EPFL

Thèse n° 10 417

Some Mordell-Weil lattices and applications to sphere packings

Présentée le 9 février 2024

Faculté des sciences de base
Chaire d'Arithmétique
Programme doctoral en mathématiques

pour l'obtention du grade de Docteur ès Sciences

par

Gauthier LETERRIER

Acceptée sur proposition du jury

Prof. T. Mountford, président du jury
Prof. M. Viazovska, directrice de thèse
Dr R. Griffon, rapporteur
Dr A. Kumar, rapporteur
Prof. Ph. Michel, rapporteur

École polytechnique fédérale de Lausanne

2024

À ma famille.

L'homme moderne, universel, c'est l'homme pressé, il n'a pas le temps, il est prisonnier de la nécessité, il ne comprend pas qu'une chose puisse ne pas être utile ; il ne comprend pas non plus que, dans le fond, c'est l'utile qui peut être un poids inutile, accablant. Si on ne comprend pas l'utilité de l'inutile, l'inutilité de l'utile, on ne comprend pas l'art.

Eugène Ionesco, *Notes et contre-notes*, 1962.
(Gallimard, Folio Essais, p. 211).

Abstract

We provide new explicit examples of lattice sphere packings in some dimensions that are the densest known so far, using Kummer families of elliptic curves over global function fields. For instance, in the paper [Let22], we get lattices of rank 54, 55, 162, 163, 486 and 487, which give the densest sphere packings known to this date.

In some cases, these families of elliptic curves have unbounded Mordell–Weil rank, and using the Néron–Tate height on the Mordell–Weil group, one can obtain lattices in high-dimensional euclidean spaces. In one case however, the rank of the curves happens to be bounded and non-zero in the Kummer family of (isotrivial) elliptic curves. In any case, these results rely on the explicit determination of the L-function of these curves, via Jacobi sums. This allows, under certain assumptions, to obtain formulas for the (analytic) rank of those curves.

Keywords: elliptic curves over global fields, L-functions of elliptic curves, Néron–Tate height, function fields in positive characteristic, Jacobi sums, Mordell–Weil lattices, sphere packings, kissing number.

MSC 2020 (Math. Subject Classification): 11G05, 11M38, 11T24, 11H31.

Résumé

Nous présentons de nouveaux exemples explicites de réseaux donnant lieu à des empilements de sphères qui sont les plus denses connus jusqu'ici, dans certaines dimensions, en utilisant des familles de Kummer de courbes elliptiques sur des corps de fonctions globaux. Par exemple, dans l'article [Let22], nous obtenons des réseaux de rang 54, 55, 162, 163, 486 et 487, qui donnent les plus empilements de sphères les plus denses connus à ce jour.

Dans certains cas, le rang de Mordell–Weil dans les familles de courbes elliptiques considérées est non borné, et en utilisant la hauteur de Néron–Tate sur le groupe de Mordell–Weil, on obtient des réseaux dans des espaces euclidens de grande dimension. A contrario, dans un cas, le rang des courbes est en fait borné et non-nul dans la famille de Kummer de courbes elliptiques (isotriviales). Dans tous les cas, ces résultats reposent sur la détermination explicite de la fonction L de ces courbes, à l'aide de sommes de Jacobi. Cela permet, sous certaines hypothèses, d'obtenir des expressions pour le rang (analytique) de ces courbes.

Mots-clés : courbes elliptiques sur les corps globaux, fonctions L de courbes elliptiques, hauteur de Néron–Tate, corps de fonctions en caractéristique positive, sommes de Jacobi, réseaux de Mordell–Weil, empilements de sphères, nombre de contact.

MSC 2020 (Math. Subject Classification): 11G05, 11M38, 11T24, 11H31.

Acknowledgements

In mathematics you don't understand things, you just get used to them.

John VON NEUMANN

First and foremost, I would like to express my deep gratitude to Prof. Maryna Viazovska, who agreed to supervise my doctoral thesis. This work on a fascinating topic would not have been possible without her suggestions and support. I feel utterly fortunate to have benefited from her generosity.

I would like to extend my most sincere thanks to the members of the jury: the president Prof. Thomas Mountford, the internal examiner Prof. Philippe Michel, as well as the two external examiners Dr. Richard Griffon and Dr. Abhinav Kumar. I am grateful to Richard for inviting me to Clermont–Ferrand in November 2021 and giving me the opportunity to discuss some of the present work.

It is also a pleasure to thank the members of the chair of Number Theory. The discussions I could have with my (former or current) colleagues Martin Stoller and Nihar Gargava were always enriching. I am also thankful to Vlad Serban, Matthew de Courcy-Ireland, Riccardo Maffucci, Maxim Mornev, Maria Dostert and Monique Kiener for their support and help.

I am sincerely grateful to Dimitar Jetchev, for his constantly renewed interest in my project, and for his help. I thank Prof. Philippe Michel for his support already after my master studies. I also thank Prof. Vahid Tarokh who gave me helpful advice for the computation of Gram matrices in chapter 3. I am grateful to Prof. Douglas Ulmer who helped me with the calculation of a descent map in chapter 3.

During these four years, I had the opportunity to spend some time with a number of people (mostly from "the third floor"!) with whom it was always enjoyable to share a coffee, lunch or mathematical ideas: thank you to Bruno, Quentin, Guillaume, Vignesh, Svenja, Ilaria, Tanguy, Katie, Moritz, Samuel, Jefferson (and others, but the margin is too tiny to contain all the names!).

Il m'est plus naturel de m'adresser ici en français pour remercier quelques personnes ayant contribué, plus ou moins directement, à la démarche individuelle que représente ce travail de recherche. Je dois beaucoup à mes parents et à ma famille, en particulier ma soeur Agathe, Bruno et bien sûr Anabelle ! J'ai une pensée également pour Mamette, qui avait "côtoyé" les mathématiques de par son métier, et m'a fait remarquer que la dimension 54 de l'un de mes réseaux, c'est le numéro départemental de la Meurthe-et-Moselle !

Je remercie aussi quelques amis avec lesquels j'ai partagé agréablement une partie des études universitaires : Alexis, Arnaud, Aurélien, Gabriel, Hugo, Nicolas, ... Enfin, un petit mot pour Maurice Mischler : merci de m'avoir fait découvrir les courbes elliptiques il y a une dizaine d'années déjà !

The author of this thesis was financially supported by the Swiss National Science Foundation (SNSF), Project funding (Div. I-III), "Optimal configurations in multidimensional spaces", grant number 184927.

Contents

This work can be cited in **bibtex** format as

```
@PHDTHESIS{Leterrier_thesis_2023,
  author = {{Leterrier, Gauthier}},
  title = {{Some Mordell--Weil lattices and applications to sphere
      packings}},
  school = {\'Ecole Polytechnique F\'ed\'erale de Lausanne (EPFL)},
  type = {PhD thesis},
  year = {2023},
  note = {Available at \url{https://gitlab.com/gauthierleterrier/maths}}
}
```

Any comment, remark, suggestion (especially about typographic misprints, possible mistakes, ...) can be sent to the author at **gauthier [dot] leterrier [at] gmail [dot] com**.

Introduction

Quand une curiosité intense anime une recherche, nous avançons comme portés par des ailes impatientes. Ne sommes-nous alors téméraire esquif aux voiles tendues qui avidement laboure l'inépuisable océan ?

Alexandre GROTHENDIECK, En guise de programme, pour le cours « Introduction à la recherche », 1978/79

The main goals of this thesis are, on the one hand, to provide new explicit examples of lattice sphere packings in some dimensions which are the densest known so far, and on the other hand, to compute the analytic rank of some Kummer families of elliptic curves over global function fields. Despite the appearance, these two aims (one in discrete geometry and the other in arithmetic geometry) are actually related, which we are going to make clearer in the following paragraphs.

While quadratic forms have been studied for several centuries, some aspects of their geometry is still not well-understood. The typical question is to determine how the minimal non-zero value of a real positive-definite quadratic form on $\mathbb{Z}^n$ behaves with respect to its discriminant. More precisely, a notable open problem is to determine the value of the *Hermite constant* γ_n in a given dimension $n \geqslant 1$, defined as

$$\gamma_n := \sup\left\{ \frac{\min(q(\mathbb{Z}^n \smallsetminus \{0\}))}{\mathrm{disc}(q)^{1/n}} \;\middle|\; q : \mathbb{R}^n \to \mathbb{R} \text{ positive-definite quadratic form} \right\},$$

where $\mathrm{disc}(q)$ denotes the discriminant of q. This supremum is finite, as shown by Charles Hermite [Her50, p. 263] himself around 1847, and is in fact a maximum. However, determining the exact value of γ_n is notoriously difficult, and has been solved only if $1 \leqslant n \leqslant 8$ or $n = 24$, the latter case having been settled a few years ago by H. Cohn and A. Kumar [CK04, CK09] using the help of a computer.

There is an equivalent formulation of the problem in terms of lattice sphere packings. Namely, given a (full-rank) lattice $L \subset \mathbb{R}^n$, we can consider a collection of non-overlapping open euclidean balls of fixed radius, centered all the lattice points. The maximal possible radius for the balls is $\frac{\lambda_1(L)}{2}$, where $\lambda_1(L)$ is the L^2-norm of a shortest non-zero vector in L. In other words, we get a packing of balls (sometimes simply called *sphere packing*) $\mathcal{P} = \{B + x \;:\; x \in L\}$ where $B = B^n(0, \lambda_1(L)/2) \subset \mathbb{R}^n$ is the open euclidean ball of radius $\lambda_1(L)/2$ centered at 0 and $B + x$ denotes the translate by $x \in \mathbb{R}^n$. Let us denote by

$$D(L) := \frac{\mathrm{vol}\left(B^n(0, \lambda_1(L)/2)\right)}{\mathrm{vol}(\mathbb{R}^n/L)} \;\in]0, 1]$$

the proportion (or so-called *packing density*) of the euclidean space covered by the balls (that is, the ratio of the volume of the balls inside a fundamental parallelepiped $P \subset \mathbb{R}^n$ for

$\mathbb{R}^n/L$ by the volume of P). Then we have

$$D_\ell(n) := \sup\{\, D(L) \;:\; L \subset \mathbb{R}^n \text{ lattice} \,\} = \mathrm{vol}(B^n) \cdot 2^{-n} \cdot \gamma_n^{n/2},$$

where $\mathrm{vol}(B^n)$ denotes the Lebesgue measure of any open L^2-ball of radius 1 in $\mathbb{R}^n$. Thereby, we see that determining the maximal *lattice* packing density $D_\ell(n)$ is equivalent to finding the value of the Hermite constant γ_n. We point out that this question is more specific and quite different from the maximal density of an *arbitrary* packing of balls of equal radius (i.e., not necessarily coming from a lattice), where the exact answer is only known in dimensions 1, 2, 3, 8 and 24, the latter two cases being solved quite recently in [Via17, CKM+17]. This question was already asked in 1900 by David Hilbert as his 18th problem.

Apart from the specific dimensions $\{1, ..., 8\} \cup \{24\}$ where the value $D_\ell(n)$ and γ_n have been determined exactly, very little is known on these constants. For instance, the best known lower and upper bounds are exponentially far apart, when the dimension n goes to infinity. Namely, Minkowski and Hlawka proved that $D_\ell(n) \geqslant 2 \cdot 2^{-n}$ for all $n \geqslant 1$, which was subsequently improved by a linear factor by K. Ball in [Bal92] and further improved in some dimensions in [Van11, Ven13]. On the other hand, Kabatiansky–Levenshtein's upper bound [KL78, Corollary 2] behaves asymptotically as $D_\ell(n) \leqslant 2^{-0.59905576 \cdot n(1+o(1))}$.

Most importantly, Minkowski–Hlawka lower bound does not give insights on which lattices have a "large" sphere packing density, since this bound relies on an averaging argument (the underlying probabilistic result being Siegel's mean value theorem). It is actually difficult to produce explicitly lattices that achieve this lower bound, as soon as the dimension becomes large enough. As mentioned in [ACH+20, §3.1], « no explicit construction in dimension 2048 or greater has been shown to achieve the Minkowski–Hlawka bound ». Another source confirms this lack of understanding, as [CS98, p. 16] shows: « We still do not know how to construct packings that are as good as [Minkowski–Hlawka bound] ».

On the other hand, in dimensions n at most 1000, there are explicit lattices that reach this lower bound, or even have a packing density much larger than $2 \cdot 2^{-n}$. For instance, $\mathbb{Z}^n$ has better packing density than Minkowski–Hlawka bound up to dimension 10. The known families of lattices which are "asymptotically good", i.e., with packing density of the form $2^{-an+o(n)}$ for some $0 < a \leqslant 1$ (as in [Tsf91]), are in general not very dense in low dimensions and are not helpful to improve on the known lower bounds on packing density. The plot on page 13 shows what are the best packings known so far up to dimension $\leqslant 2048$.

In this thesis, one of the goals will be to give new examples of lattice sphere packings (e.g., in dimensions 54, 55, 162, 163, 486, 487) for which the density is the best known so far, and in particular, exceeds Minkowski–Hlawka lower bound. This is notable in view of the fact that « we know very little about [the] range » of dimensions 80 to 4096, as pointed out by N. Sloane in his 1998 ICM report [Slo98]. Thus, even small improvements on Minkowski's bound are welcome.

Roughly speaking, our lattices will be constructed using the Néron–Tate height $\hat{h}$ on elliptic curves E over global function fields like $K = \mathbb{F}_q(t)$. It is defined as $\hat{h}(P) := \lim_{n \to +\infty} n^{-2} h(nP)$ where $h(Q)$ is the degree of the x-coordinate of a rational point $Q \in E(K)$, seen as a rational map $x(Q) : \mathbb{P}^1 \to \mathbb{P}^1$ (we fix here a Weierstrass equation to get an embedding $E \hookrightarrow \mathbb{P}^2$). If we consider the free abelian group of finite rank $L := E(K)/E(K)_{\mathrm{tors}}$, then $\hat{h}$ is a positive-definite quadratic form on $L \otimes_{\mathbb{Z}} \mathbb{R}$ so it gives a structure of lattice on L, the so-called

Mordell–Weil lattice of E over K. This point of view initially originated from independent works of N. Elkies [Elk94, Elk97, Elk01] and T. Shioda [Shi91, Shi90] in the 1990s, where lattice packings were obtained in some dimensions like 80, 104, 128, 256, 512; these packings are still having the best known density in these dimensions, as of now.

In [Oes90, §3], J. Oesterlé explains how this interest for Mordell–Weil lattices began: in 1989, M. Tsfasman asked in [Tsf91, §9, question 10] how to estimate the sphere packing density of these lattices (and more generally he studied lattice packings coming from algebraic geometry or number theory). More recently, the book [SS19] by Shioda and Schütt got published, providing us with a great reference on Mordell–Weil lattices[1].

It is convenient to define a certain sublattice $E(K)^0$ of $E(K)$, called the *narrow Mordell–Weil lattice*, consisting of all the points $P \in E(K)$ such that, for every place v of K, the reduction $\overline{P_v}$ is a non-singular point of the reduction $\overline{E_v}$ of E modulo v.

We now summarize here the strategy used by Elkies in [Elk94] and the methods used by Shioda in [Shi91], to compute a lower bound on the the packing densities of their Mordell–Weil lattices $E(K)^0$. This requires three steps:

① Determine the rank of $E(K)^0$. In [Elk94], the computation of the rank relies on the fact that E is a *quadratic* twist of a constant curve. Then one can use proposition 2.5.2 and remark 2.4.1 stated later in this work. In [Shi91], the method to compute the rank uses the fact that the so-called Lefschetz number of the elliptic surface $\mathscr{E}$ attached to E is zero, as showed in [Shi86, corollary 4].

② Get an upper bound on the covolume of $E(K)^0$. In [Elk94], the L-function is computed explicitly using proposition 2.5.3. Then the special value $L^*(E/K)$ allows to determine the regulator $\mathrm{Reg}(E/K) = \mathrm{disc}(E(K))$ via the Birch–Swinnerton-Dyer formula (1.3.13). In [Shi91, proposition 4.3, corollary 4.7], the strategy involves crystalline cohomology, which also allows to get information on the Tate–Shafarevich group of E over K.

③ Finally, get a lower bound on the minimal non-zero norm $\lambda_1(E(K)^0)$ in $E(K)^0$. In [Elk94], an *ad-hoc* computation, using the fact that the characteristic is 2, shows that the Néron–Tate height $\hat{h}$ equals the naive height, allowing to deduce directly a lower bound on the minimal non-zero height. In [Shi91], Shioda uses his result which we will state later as theorem 1.3.24.

Generally, we will work with the *center packing density* of a given lattice $L \hookrightarrow \mathbb{R}^n$, defined by

$$\delta(L) := \mathrm{vol}(B^n(0,1))^{-1} \cdot D(L),$$

where $D(L) \in]0,1]$ is the density introduced earlier. More specifically, here is the result obtained by Elkies (some of the terminology and notation will be defined in chapter 1):

Theorem 0.1 ([Elk94]). *Let $n \geqslant 1$ be an integer and set $q = 2^n, k = \mathbb{F}_{q^2}$. Let $a := 0$ if n is odd, and if n is even, fix $a \in k^\times$ such that $\mathrm{tr}_{k/\mathbb{F}_2}(a) = 1$. Consider the elliptic curve $\Gamma_{n,a} : y^2 + y = x^3 + t^{2^n+1} + a$ over $K := k(t)$. Then:*

[1] Let us also mention the works [Shi08, Shi00] which deal with other lattices coming from algebraic geometry. Moreover, in MAGMA [BCP97], there are commands like `GeometricMordellWeilLattice` to compute with some of these lattices.

1. *The rank of* $\Gamma_{n,a}$ *over* $k(t)$ *is* $r := 2q = 2^{n+1}$. *The L-function of* $\Gamma_{n,a}$ *is* $L(\Gamma_{n,a}/k(t), T) = (1-q^2T)^{2q}$ *and the special value is* $L^*(\Gamma_{n,a}/k(t)) = 1$.

2. *We have* $\deg(\Delta_{\min}(\Gamma_{n,a}/K)) = 12\lceil q/6\rceil$ *and* $f(\Gamma_{n,a}/K) = 2q+4$. *As* $n \to \infty$, *Brumer's bound (theorem 2.2.6) is asymptotically achieved, and the Szpiro ratio (introduced in definition 2.2.1) tends to 1.*

3. *The center packing density of the narrow Mordell–Weil lattice* $L_{n,a}$ *of* $\Gamma_{n,a}$ *over* K *satisfies the following lower bound:*

$$\delta(L_{n,a}) \geqslant \begin{cases} \frac{1}{2} q^{-\frac{q-2}{6}} \left(\frac{q+4}{12}\right)^q & \text{if } n \text{ odd} \\ q^{-\frac{q-4}{6}} \left(\frac{q+2}{12}\right)^q & \text{if } n \text{ even.} \end{cases}$$

   In particular, we have the asymptotic lower bound $D(L_{n,a}) \geqslant r^{-\frac{r}{12}(1+o(1))}$ *as the rank* r *goes to infinity (equivalently,* $n \to +\infty$*).* ⌟

Here is a table giving some values[2]. In ranks 128, 256, 512, 1024, these Mordell–Weil lattices provide the densest known lattice sphere packings in their respective dimensions.

n	5	6	7	8	9	10	11	12
$\mathrm{rk}(L_n)$	64	128	256	512	1024	2048	4096	8192
$\log_2(\delta(L_n)) \geqslant$	24.718	97.403	294.807	797.123	2012.24	4871.88	11439.76	26286.87

- When $n = 1$, the rank is $r = 4$ and $L_{1,a}$ is homothetic to D_4, with center density $\delta = 1/8$. When $n = 2$, the rank is $r = 8$ and $L_{2,a}$ is homothetic to E_8, with center density $\delta = 1/16$.
- When $n = 3$, the 16-dimensional lattice $L_{3,a}$ has center density $\delta = 1/16$, and for $n = 4$, the 32-dimensional lattice $L_{4,a}$ has center density $\delta = (9/8)^8$.

Here is the result obtained by Shioda; we refer to remark 4.1.11 for more details (in particular for a table of explicit values).

Theorem 0.2 ([Shi91]). *For any prime* $p \equiv -1 \bmod 6$ *and any odd integer* $e > 0$, *let* E *be the elliptic curve given by* $y^2 = x^3 + 1 + t^{p^e+1}$ *over* $K := \mathbb{F}_{p^{2e}}(t)$. *Then the rank of* E *over* K *equals* $r := 2p^e - 2$ *and the center packing density of its narrow Mordell–Weil lattice is lower-bounded by*

$$\delta(E(K)^0) \geqslant \frac{((p^e+1)/12)^{p^e-1}}{p^{e\cdot(p^e-5)/6}}.$$

Moreover, as $q \to \infty$, *Brumer's bound (theorem 2.2.6) is asymptotically achieved, and the Szpiro ratio (introduced in definition 2.2.1) tends to 1.* ⌟

This leads us to the second topic of interest that underlies this work. Apart from getting better lower bounds on Hermite constants, another rich source of open problems is the arithmetic of elliptic curves: while they have been studied for a long time, their rational

[2] For $n \in \{9, 10, 11\}$, better lower bounds on the order of the Tate–Shafarevich group can improve the lower bound on the packing density. See the (unproven) values given in [Elk94, p. 354].

points are still not fully understood. For instance, it is a challenging task to compute the Mordell–Weil rank of a given elliptic curve over $\mathbb{Q}$ in general (especially when the rank is $\geqslant 2$). More generally, an important open problem is to know whether the rank of elliptic curves over a fixed number field can be arbitrarily large.

By contrast, Tate and Shafarevich showed in [TS67] that for every odd prime $p \geqslant 3$ and any $R > 0$, there is an (isotrivial) elliptic curve E over $\mathbb{F}_p(t)$ such that $E(\mathbb{F}_p(t))$ has rank $\geqslant R$. Later on, many other examples of this phenomenon of unbounded rank have been discovered, as the list from remark 1.3.47 will show. Let us simply cite some relevant works: [Shi91, Shi86, Ulm02, Ber08, BDS04, DO16].

In that setting, it makes sense to focus on elliptic curves over global function fields and study the rank of their Mordell–Weil group, or rather their analytic rank, i.e., the order of vanishing of the L-function at the "central point".

In this thesis, we will compute the L-function and thus the (analytic) rank of two families of elliptic curves over $k(t)$, where k is a finite field, namely:

- $E_{m,b,b'} : y^2 = x^3 + bx + b't^m$ over $k(t)$, where $\mathrm{char}(k) \geqslant 3$
- $E'_{m,b,b'} : y^2 = x^3 + b + b't^m$ over $k(t)$, where $\mathrm{char}(k) \geqslant 5$.

These families were chosen based on a result of ours, stated as theorem A below, which provides some sufficient conditions to get the best possible asymptotic behavior of the lower bound on the packing density, *among Mordell–Weil lattices*.

Both curves $E_{m,b,b'}$ and $E'_{m,b,b'}$ are known to satisfy the Birch–Swinnerton-Dyer conjecture, and the L-function can be expressed in terms of certain Jacobi sums (see theorems B and F below for a precise statement), so the algebraic rank can be related to those exponential sums occurring in the corresponding L-function. In the family $E_{m,b,b'}$, some interesting packings arise, especially in characteristic 3 and for $m = 3^n + 1$, where the corresponding narrow Mordell–Weil lattices are particularly dense. For instance, when $n \in \{3, 4, 5\}$ we obtain packings with current record densities in dimensions $2 \cdot 3^n$ and $2 \cdot 3^n + 1$ (using laminated lattices).

We will take this opportunity to compute the kissing number of one of these lattices (in dimension 54), and point out some probabilistic methods to compute the corresponding Gram matrix, thus showing that one can compute very explicitly these lattices. The techniques used there are also useful to compute the Tate–Shafarevich group of some of the curves $E_{3^n+1,b,b'}$ in characteristic 3.

In the other family $E'_{m,b,b'}$ (studied by Shioda over $\overline{\mathbb{F}_p}(t)$), it turns out that the rank is unbounded if and only if $p \equiv -1 \pmod 3$. When $p \equiv 1 \pmod 3$, we will actually prove that the rank over $\mathbb{F}_{p^{2160}}(t)$ is a *non-zero* constant. This contrasts with the previously known examples of Kummer families having bounded rank, as in [Ber12] and [Ulm07a, §5, §6] because all of them had rank *zero* (we note that even though $E'_{m,b,b'}$ is isotrivial, is it not a constant elliptic curve).

Main results

We now review the main results of this thesis, before making them more detailed and proving them in the following chapters.

In chapter 2, we will give sufficient conditions that ensure (conditionally on Birch–Swinnerton-Dyer conjecture) that the narrow Mordell–Weil lattices of given elliptic curves have reasonably large packing density, from an asymptotic point of view, as in Elkies' and Shioda's examples described in theorems 0.1 and 0.2 above (even though the asymptotic lower bound is much worse than Minkowski–Hlawka's bound). This also provides some conceptual understanding as to why these two authors picked these specific families of elliptic curves.

Theorem A (Theorem 2.3.1)**.** *Consider a collection of elliptic curves* $\{E_j/\mathbb{F}_{q_j}(t) \,:\, j \geqslant 1\}$ *such that the degree* f_j *of the conductor of* E_j *grows to* $+\infty$ *when* $j \to \infty$ *(and* q_j *are prime powers). Let* $K_j := \mathbb{F}_{q_j}(t)$ *and denote by* L_j *the narrow Mordell–Weil lattice* $E_j(K_j)^0$ *of* E_j/K_j*. Let* r_j *be the (algebraic) rank of* L_j *and let* $d_j := \deg(\Delta_{\min}(E_j))$ *be the degree of the minimal discriminant of* E_j/K_j*. Assume that:*

1) *The Birch–Swinnerton-Dyer conjecture 1.3.34 holds for the elliptic curves* E_j/K_j*.*

2) *There is a constant* $c_0 \geqslant 1$ *such that* $q_j \leqslant f_j^{c_0}$ *for all* $j \geqslant 1$ *(i.e., the size of the fields of constants grows at most polynomially with the conductor).*

3) *The so-called Szpiro ratio* $\sigma_j := \sigma(E_j/K_j) := \dfrac{d_j}{f_j}$ *tends to* 1 *when* $j \to \infty$*.*

4) *The so-called Brumer's bound is asymptotically sharp, i.e. the rank of* E_j/K_j *satisfies*

$$r_j \;\sim\; \frac{f_j \log(q_j)}{2\log(f_j)} \qquad (j \to \infty).$$

Then we have the following asymptotic lower bound on the packing density of L_j*, when the rank* r_j *goes to infinity:*

$$D(L_j) \;\geqslant\; r_j^{-\frac{1}{12} r_j (1+o(1))}.$$ ⌟

This theorem easily follows from an upper bound on the Brauer–Siegel ratio

$$\mathrm{BS}(E/K) := \frac{\log(|Ш(E/K)| \cdot \mathrm{Reg}(E/K))}{\log\left(|k|^{\deg(\Delta_{\min}(E/K))/12}\right)} \;\leqslant\; 1 + o(1)$$

(as the the degree of the discriminant goes to infinity), proved in [HP16]. There is one subtlety: in the paper [HP16], the size q of the field of constants is fixed, but we checked that the result holds true even if we allow $q = q_j$ to vary (as in the examples from [Elk94, Shi91]), by making all the implicit constants as explicit as possible, in appendix A. The difficulty of theorem A does not lie in the proof, but in the discovery of the suitable sufficient conditions so that the desired conclusion holds. Likewise, a difficult part of theorem C below was to discover which curves to take in order to possibly get interesting (i.e., with high density) lattice packings; this is a place where theorem A was useful.

Several families satisfy the conditions from the above proposition, as the ones considered in theorems 0.1 and 0.2 above; see also example 2.3.2.

In chapter 3, we will prove the following results. First, we explicitly compute the L-function of the curves $E_{m,b,b'} : y^2 = x^3 + bx + b't^m$ over $k(t)$ (we point out that the statements of theorem 3.1.3 and theorem B are equivalent by remark 1.4.18). In order to state the result, let us introduce some notation, also used in the rest of this introduction (we refer to section 1.4 for more details). Given a finite field k, we denote by $k_n \subset \overline{k}$ its extension of degree $n \geqslant 1$ and by $\widehat{k^\times}$ its group of multiplicative characters. If k has odd characteristic, we denote by $\lambda_k : k^\times \to \{\pm 1\}$ the Legendre symbol. Finally, given three multiplicative characters $\chi_1, \chi_2, \chi_3 \in \widehat{k^\times}$, we define the *Jacobi sums* as

$$J(\chi_1, \chi_2) := \sum_{x \in k} \chi_1(x)\chi_2(1-x), \qquad J(\chi_1, \chi_2, \chi_3) := \sum_{x,y \in k} \chi_1(x)\chi_2(y)\chi_3(1-x-y).$$

Theorem B (Theorem 3.1.3). *Let k be a finite field of odd characteristic p, let $m \geqslant 1$ be coprime to p and $b, b' \in k^\times$. Set $d := 4m/\gcd(2,m)$ and fix a generator γ of $k^\times_{\phi(d)}$, where ϕ is the Euler totient function. Given $r \in \mathbb{Z}/d\mathbb{Z}$, let $u(r)$ be the multiplicative order of $|k|$ modulo $\frac{d}{\gcd(d,r)}$ and define the character*

$$\chi_r : k^\times_{u(r)} \to \mathbb{C}^\times, \quad \gamma_{u(r)} \mapsto \exp(2\pi i r/d)$$

where $\gamma_{u(r)} := \mathrm{N}_{k_{\phi(d)}/k_{u(r)}}(\gamma)$ is a generator of $k^\times_{u(r)}$ and $\mathrm{N}(\cdot)$ denotes the norm map. Define

$$Z(m) := \begin{cases} \mathbb{Z}/d\mathbb{Z} \smallsetminus \frac{m}{2}\mathbb{Z}/2m\mathbb{Z} & \text{if } m \text{ is even and } 6 \nmid m \\ \mathbb{Z}/d\mathbb{Z} \smallsetminus (\frac{m}{2}\mathbb{Z}/2m\mathbb{Z} \cup \frac{2m}{3}\mathbb{Z}/2m\mathbb{Z}) & \text{if } m \text{ is even and } 6 \mid m \\ \mathbb{Z}/d\mathbb{Z} \smallsetminus (2\mathbb{Z}/4m\mathbb{Z} \cup m\mathbb{Z}/4m\mathbb{Z}) & \text{if } m \text{ is odd} \end{cases}$$

$$\epsilon_{m,b,b',k}(T) := \begin{cases} (1-|k|T)^2 & \text{if } m \text{ is even and } -b \in k^{\times,2} \text{ and } b' \in k^{\times,2} \\ (1+|k|T)^2 & \text{if } m \text{ is even and } -b \in k^{\times,2} \text{ and } b' \notin k^{\times,2} \\ 1-|k|^2T^2 & \text{if } m \text{ is even and } -b \notin k^{\times,2} \\ 1 & \text{if } m \text{ is odd.} \end{cases}$$

Finally, let us define the map

$$\alpha_{b,b'} : \bigsqcup_{n \geqslant 1} \widehat{k_n^\times} \longrightarrow \mathbb{C}, \qquad \alpha_{b,b'}(\theta) := \lambda_{k_n}(-b')\theta(-b^3b'^{-2}) \cdot J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot J(\theta, \theta^2) \quad \text{if } \theta \in \widehat{k_n^\times}.$$

Then the L-function of $E_{m,b,b'}$ is equal to

$$L(E_{m,b,b'}/k(t), T) = \epsilon_{m,b,b',k}(T) \cdot \prod_{[r] \in Z(m)/\langle |k| \rangle^\times} \Big(1 - \alpha_{b,b'}(\chi_r)T^{u(r)}\Big),$$

where $[r]$ denotes the orbit of $r \in \mathbb{Z}/d\mathbb{Z}$ under the action of the multiplication by the powers of $|k|$ on $\mathbb{Z}/d\mathbb{Z}$. ⌟

If m is chosen in a suitable way, one can compute explicitly the Jacobi sums appearing in the coefficient $\alpha_{b,b'}(\chi_r)$ above, thanks to a result of Tate and Shafarevich from [TS67] (see theorem 1.4.8). This allows us to get elliptic curves with arbitrarily large (analytic) ranks, as asserted by the following corollary. We can actually get more precise formulas for the rank in such cases (see corollary 3.1.14).

Corollary A (Corollary 3.1.20). *Fix any odd prime p and $b, b' \in \mathbb{F}_p^\times$. Then the rank of $E_{m,b,b'}$ over $\mathbb{F}_p(t)$ is unbounded as $m \geqslant 1$ varies.* ⌟

In characteristic 3, it turns out that an interesting phenomenon happens. The following corollary of theorem B was originally given in our paper [Let22], where we proved it using the basic fact that the map $x \mapsto x^3 + bx$ is additive in characteristic 3 (see subsection 3.1.7 for more details about this alternative proof).

Corollary B (Corollary 3.1.22). *Let $n \geqslant 1$ be an integer and set $q = 3^n$. Let $b \in \mathbb{F}_q^\times$ be any element such that $b^{\frac{q-1}{2}} = (-1)^{n+1}$. Let $E = E_{3^n+1,b,1}$ be the elliptic curve given by $y^2 = x^3 + bx + t^{3^n+1}$. Then the L-function of E over $\mathbb{F}_{q^2}(t)$ is equal to $L\left(E/\mathbb{F}_{q^2}(t),\ T\right) = (1 - q^2T)^{2\cdot 3^n}$. In particular, the analytic rank of E over $\mathbb{F}_{q^2}(t)$ is equal to $2 \cdot 3^n$.* ⌟

From there, one can deduce a lower bound on the packing density of the corresponding narrow Mordell–Weil lattices, as in [Let22].

Theorem C (Theorem 3.2.7). *Let $n \geqslant 1$ be an integer, fix $b \in \mathbb{F}_{3^n}^\times$ such that $b^{(3^n-1)/2} = (-1)^{n+1}$, and set $q = 3^n, K = \mathbb{F}_{q^2}(t)$. Let $L'_{n,b} := E_{3^n+1,b,1}(K)^0$ be the narrow Mordell–Weil lattice of the elliptic curve $E_{3^n+1,b,1}$ over K, i.e., the set of all rational points $P \in E_{3^n+1,b,1}(K)$ such that the reduction P_v is a non-singular point of the reduction $\overline{E_{3^n+1,b,1}}$ modulo v, for every place v of K.*

Then the rank of $L'_{n,b}$ is $2 \cdot 3^n$ and its center packing density satisfies the lower bound

$$\delta(L'_{n,b}) \geqslant \left(\frac{3^{n-1}+1}{4}\right)^{3^n} \cdot 3^{-n\left(\frac{3^{n-1}-1}{2}\right)-\frac{1}{2}}.$$

⌟

In particular, for $n \in \{1, ..., 7\}$, we get the following values, gathered in the table below.

n	rank of $L'_{n,b}$	$\log_2\left(\delta(L'_{n,b})\right) \geqslant$	Best *lattice* packing density known so far
1	6	$\log_2\left(\sqrt{3}/24\right) \simeq -3.79248$	$\delta(E_6) = \frac{\sqrt{3}}{24}$ ([CS98], p. xix)
2	18	$\log_2\left(\frac{\sqrt{3}}{27}\right) \simeq -3.962406$	-3.79248 [CS98], p. xix
3	54	$\log_2\left(\frac{\sqrt{3}\cdot 5^{27}}{2^{27}\cdot 3^{13}}\right) \simeq 15.88002$	15.88 (Elkies [CS98], p. xviii)
4	162	144.1852	130.679 [FIdD11]
5	486	741.1001	703.05 [Bal92]
6	1458	3172.032	3236.6 [Bal92]

In dimension 54, it equals the currently densest known sphere packings, and in dimensions 162, 486, it improves on the previously known packings; in other words, in these two dimensions, the lattices from theorem C provide the densest sphere packings known so far.

Moreover, we use laminated lattices in proposition 3.2.22 to construct lattices L of rank 55, 163, 487 with center packing densities satisfying respectively

$$\log_2(\delta(L)) \geqslant 16.833, \qquad 145.88, \qquad 743.57.$$

These lattices thus provide the densest sphere packings known so far in their respective dimensions. Let us also mention that some dense packings in ranks 150 and 306 are obtained in example 3.2.3.

Moreover, we computed the kissing number of the 54-dimensional lattice found above (using $n = 3$ in theorem C). The main point is to show that one can compute quite explicitly with these lattices, at least with the help of a computer. Unfortunately, it is quite far from being a record kissing number; already in dimension 48 there is a lattice with much larger kissing number. The following result was obtained using SAGE [The21], and the code of the corresponding programs is available at `https://gitlab.com/gauthierleterrier/maths`.

Computational theorem D (Computational theorem 3.3.1)**.** *The kissing number of the 54-dimensional lattice $L'_{3,1}$ (from theorem C) is equal to* $15309000 = 2^3 \cdot 3^7 \cdot 5^3 \cdot 7$. ⌟

In this computational context, we were also interested in a method to determine the Gram matrices of those lattices coming from the curves in characteristic 3 (and the lattices coming from Elkies' curves, defined in [Elk94], as well). We are not going to state a precise result here, but we will explain in section 3.3 how this approach works. At least, let us mention that we have found a Gram matrix for $L'_{3,1}$, which therefore gives a very explicit description of this Mordell–Weil lattice (see computational proposition 3.3.10). This relies on the fact that the Tate–Shafarevich group of the curve $y^2 = x^3 + x + t^{28}$ over $\mathbb{F}_{3^6}(t)$ is trivial, which is a result obtained in the final section of chapter 3.

Theorem E (theorem 3.4.1)**.** *If $n \in \{1, 2, 3\}$ and $b \in \mathbb{F}_{3^n}^\times$ is such that $b^{(3^n-1)/2} = (-1)^{n+1}$ then the Tate–Shafarevich group of $y^2 = x^3 + bx + t^{3^n+1}$ over $\mathbb{F}_{3^{2n}}(t)$ is trivial.* ⌟

This is proved using a 3-descent involving an inseparable isogeny, which required to use Amitsur–Čech's description of flat cohomology.

Finally, in chapter 4, we will prove the following results. We determine explicitly the L-function of the curves $E'_{m,b,b'} : y^2 = x^3 + b + b't^m$ over $k(t)$. We state the result under the hypothesis that $|k| \equiv 1 \bmod 3$ for simplicity, but we obtained an analogous statement in the case $|k| \equiv -1 \bmod 3$ as well (see theorem 4.1.2 for the exact formulation and remark 1.4.18 which ensures that this formulation is indeed equivalent to theorem F below). We keep the notation introduced before the statement of theorem B.

Theorem F (Theorem 4.1.2)**.** *Let k be a finite field of characteristic $p \geqslant 5$ such that $|k| \equiv 1 \bmod 3$, let $b, b' \in k^\times$ and $m \geqslant 1$ be an integer coprime to p. Fix a generator $\gamma \in k^\times_{\phi(m)}$. For each $r \in \mathbb{Z}/m\mathbb{Z}$, let $u(r)$ be the multiplicative order of $|k|$ modulo $\frac{m}{\gcd(m,r)}$,*

define the generator $\gamma_{u(r)} := \mathrm{N}_{k_{\phi(m)}/k_{u(r)}}(\gamma)$ *of* $k_{u(r)}^\times$ *and define the characters*[3]

$$\chi_r : k_{u(r)}^\times \to \mathbb{C}^\times, \quad \gamma_{u(r)} \mapsto \exp(2\pi i r/m),$$
$$\psi_r : k_{u(r)}^\times \to \mathbb{C}^\times, \quad \gamma_{u(r)} \mapsto \exp(2\pi i/3).$$

Given $\epsilon \in \{\pm 1\}$, *we define*

$$\alpha'_{b,b',\epsilon}(\chi_r) := \lambda_{k_{u(r)}}(b) \cdot \chi_r(-bb'^{-1}) \cdot \psi_r^\epsilon(-b) \cdot J\big(\psi_r^\epsilon,\ \chi_r,\ \lambda_{k_{u(r)}}\big)$$
$$X(m,\epsilon) := \begin{cases} \mathbb{Z}/m\mathbb{Z} \smallsetminus \{0\} & \text{if } 6 \nmid m \\ \mathbb{Z}/m\mathbb{Z} \smallsetminus \{0, \epsilon\frac{m}{6}\} & \text{if } 6 \mid m. \end{cases}$$

Then we have

$$L(E'_{m,b,b'}/k(t), T) = \prod_{\epsilon\in\{\pm1\}} \prod_{[r]\in X(m,\epsilon)/\langle |k|\rangle^\times} (1 - \alpha'_{b,b',\epsilon}(\chi_r) T^{u(r)})$$

where $[r]$ *denotes the orbit of* $r \in \mathbb{Z}/m\mathbb{Z}$ *under the action of the multiplication of the powers of* $|k|$ *on* $\mathbb{Z}/m\mathbb{Z}$. ⌟

Having in hand a concrete expression for the L-function, one can study the (analytic) rank of the curves $E'_{m,b,b'}$ over $k(t)$. When the characteristic of k is $p \equiv -1 \bmod 3$, we get a family of unbounded rank, giving some interesting sphere packings from the corresponding Mordell–Weil lattice as studied in [Shi91]. However, in characteristic $p \equiv 1 \bmod 3$, the situation is radically different, as the next statement shows.

Theorem G (Theorem 4.2.1). *For any prime* $p \equiv 1 \pmod 3$, *for all* $b, b' \in \mathbb{F}_p^\times$ *and all integers* $m' \geqslant 1$ *(not necessarily coprime to* p*), the rank of the elliptic curve* $E' := E'_{360m',b,b'} : y^2 = x^3 + b + b't^{360m'}$ *over* $\mathbb{F}_{p^{2160}}(t)$ *is equal to a non-zero constant, namely 68, which is also equal the geometric rank (i.e., the rank of* E' *over* $\overline{\mathbb{F}_p}(t)$*).* ⌟

In other words, this provides an example of an (isotrivial but non-trivial) elliptic curve $E'_{360,b,b'}$ with constant *non-zero* rank over $k(t^{1/m})$ for every $m \geqslant 1$, where $k := \mathbb{F}_{p^{2160}}$ and $p \equiv 1 \pmod 3$, which contrasts with previously known examples of Kummer families of elliptic curves with bounded rank, where the rank is actually always 0. We mention that one can also use theorem F to compute efficiently the analytic rank of some of these curves $E'_{m,b,b'}$, for instance to gather data supporting conjecture 4.2.30.

The proof of theorem G relies on Stickelberger's theorem, which tells us how the principal ideal generated by a Jacobi sum (inside some ring of cyclotomic integers) factors into prime ideals. This is related to the geometric rank of elliptic curves as follows. In general, the analytic rank is twice the number of orbits $[r]$ such that $\alpha'_{b,b',\epsilon}(\chi_r)$ is a positive integer (using theorem F), hence fixed by the Galois group of some corresponding cyclotomic field. We obtain an upper bound on the rank is only considering those $[r]$ such that the ideal generated by $\alpha'_{b,b',\epsilon}(\chi_r)$ is Galois-invariant (by considering only the *ideal*, we miss the knowledge of the sign of the Jacobi sums, since we work only up to units of the ring of cyclotomic integers). This is where Stickelberger's theorem plays a role.

[3] We note that ψ_r is a well-defined character of order 3 on $k_{u(r)}^\times$, because we assumed that $|k| \equiv 1 \bmod 3$, so that 3 divides $k_{u(r)}^\times$ for every r. Here ϕ is Euler totient function and $\mathrm{N}(\cdot)$ denotes the norm map.

Let us also mention a side result, proved in chapter 2. It provides the analogue in characteristic 2 of Tate–Shafarevich's theorem from [TS67] on unboundedness of rank of families of isotrivial elliptic curves in odd characteristic. It is relevant also in the context of sphere packings, as it uses Elkies' curves considered in [Elk94] — the only difference being the base field $\mathbb{F}_2(t)$ instead of $\overline{\mathbb{F}_2}(t)$. This fills a missing case in the table from [BDS04, page 488] (namely the assumption that p must be odd in Tate–Shafarevich's result can be removed).

Theorem H (Theorem 2.5.1)**.** *Let n be an* odd *integer and consider the elliptic curve given by the Weierstrass equation $A_n : y^2 + y = x^3 + t^{2^n+1}$ over $\mathbb{F}_2(t)$.*

Then the rank of A_n over $\mathbb{F}_{2^n}(t)$ equals 2^n. Moreover, if $n = 1$ or if n is an odd prime number, then the rank of the finitely generated abelian group $A_n(\mathbb{F}_2(t))$ is given by

$$\operatorname{rk} A_n\left(\mathbb{F}_2(t)\right) = 2 \cdot \left(1 + \frac{2^{n-1} - 1}{n}\right).$$

Finally, let us mention that some other small results, not easily found explicitly in the literature, are also written down in this work; for instance see propositions 1.1.6, 1.2.9 and 2.5.3.

Organization of the text

Overall, the chapters are essentially independent of each other (except the background chapter 1 which is freely used in the other parts of the text).

In the first chapter, we review some standard tools and useful results about lattices in section 1.1, packings in section 1.2, elliptic curves in section 1.3 (especially Shioda's lower bound on the minimal non-zero Néron–Tate height of points in the narrow Mordell–Weil lattice stated as theorem 1.3.24) and character sums (especially Jacobi sums, Hasse–Davenport lifting relation stated as theorem 1.4.7, Stickelberg's theorem 1.4.22 and Tate–Shafarevich theorem 1.4.8) in section 1.4.

In chapter 2, we study (a lower bound on) the packing density of (narrow) Mordell–Weil lattices from an asymptotic point of view, that is, when the dimension goes to infinity. First, in section 2.1, we give a general lower bound on the packing density, which relies on the use of Birch–Swinnerton-Dyer formula and Shioda's theorem 1.3.24. Then we introduce in section 2.2 some of the invariants needed to state theorem A, like Brauer–Siegel and Szpiro ratios. After proving theorem A in section 2.3, we discuss some generalizations to abelian varieties and to constant elliptic curves in section 2.4. Finally, in section 2.5, we prove theorem H.

In chapter 3, we first prove theorem B, corollary A, corollary B in section 3.1. In section 3.2, we prove theorem C. In section 3.3, we prove computational theorem D and explain how to compute Gram matrices associated with our Mordell–Weil lattices in characteristic 3. We end the chapter by proving theorem E in section 3.4.

In chapter 4, we prove theorem F in section 4.1, while in section 4.2 we give the proof of theorem G.

In chapter 5, we list some unanswered questions related to the various results discussed in this thesis.

In appendix A, we give a detailed proof of theorem 2.2.4, to make sure that we can allow the field of constants $\mathbb{F}_q$ to vary. We simply follow the proof given in [HP16], but having in mind that we shall make sure that the implicit constants do not depend on q.

For the convenience of the reader, some frequently used notation are gathered in a list of symbols (list of notation) at the end of this document, on page 239. For completeness, let us mention that:

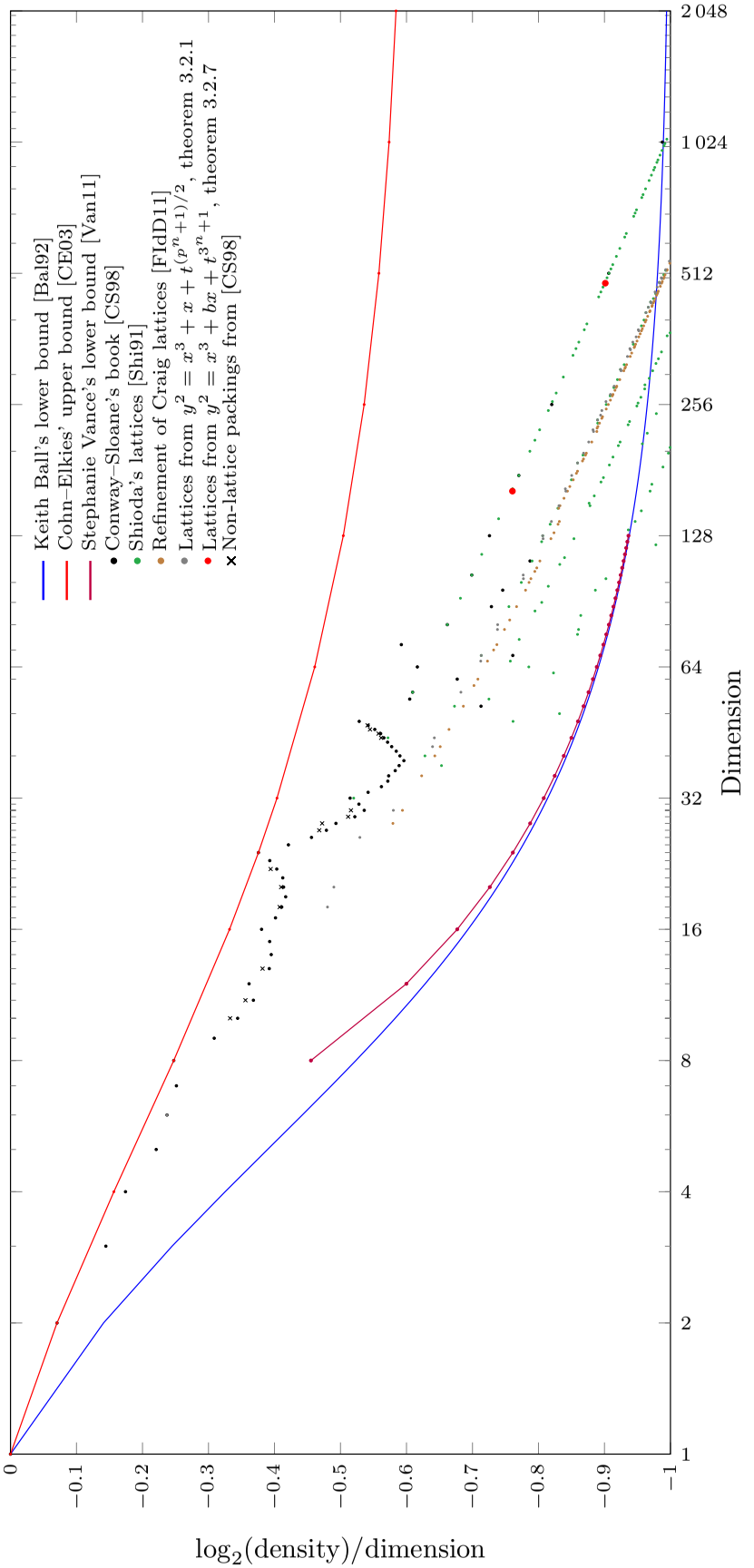
- Given a set E, we denote its cardinality by $|E|$ or by $\#E$ and by $\mathbb{1}_E$ its indicator function (sometimes we may write $\mathbb{1}_{x\in E}$ for $\mathbb{1}_E(x)$).
- We sometimes denote by $\mathbb{1}_{u=v}$ the Kronecker symbol $\delta_{u,v}$.
- Given a complex number $z \in \mathbb{C}$, its complex modulus is denoted by $|z|$.
- Given an integer $n \geqslant 1$, we denote by $\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ the Euler totient function.
- Given two integers $a, b \geqslant 1$, we sometimes denote by (a, b) their greatest common divisor.

On the following page, a plot[4] shows what we know about the (lattice) sphere packing density in dimensions $\leqslant 2048$. The density of a packing is always between 0 and 1, and Minkowski–Hlawka lower bound tells us that there are lattices in dimension n with packing density at least 2^{-n}, which corresponds to $\log_2(\text{density})/\text{dimension} \geqslant -1$.

The blue "top" curve is Cohn–Elkies' upper bound from [CE03] (theorem 1.2.25); the values being taken from [ACH+20, table 3.1]. The red "bottom" curve is Keith Ball's lower bound from [Bal92] (theorem 1.2.16). The "dots" in between correspond to lattices[5].

[4] The data used to produce the graph is available at https://gitlab.com/gauthierleterrier/maths.

[5] (To be precise, some dots are *lower bounds* on the packing density of a certain lattice). We observe that some dots form a line with slope $-\frac{1}{12}$. This is explained by theorem 2.3.1: we have $\frac{\log(D(L_j))}{\mathrm{rk}(L_j)} \geqslant -\frac{1}{12}\log \mathrm{rk}(L_j)$ for some narrow Mordell–Weil lattices L_j, and since the x-axis shows the dimension in an logarithmic scale, we get a line of slope $-\frac{1}{12}$.


Keith Ball's lower bound [Bal92]
Cohn–Elkies' upper bound [CE03]
Stephanie Vance's lower bound [Van11]
Conway–Sloane's book [CS98]
Shioda's lattices [Shi91]
Refinement of Craig lattices [FIdD11]
Lattices from $y^2 = x^3 + x + t^{(p^n+1)/2}$, theorem 3.2.1
Lattices from $y^2 = x^3 + bx + t^{3^n+1}$, theorem 3.2.7
Non-lattice packings from [CS98]
0
−0.1
−0.2
−0.3
−0.4
−0.5
−0.6
−0.7
−0.8
−0.9
−1
$\log_2(\text{density})/\text{dimension}$
2 048
1 024
512
256
128
64
32
16
8
4
2
1
Dimension

Chapter 1

Background material

In this chapter, we give some useful material on lattice packings and on elliptic curves over function fields, which we will need in the following chapters. Most of the notions gathered in this chapter are classical and well-known, we review them only for convenience and completeness.

1.1 · Lattices

1.1.1 General definitions

Definition 1.1.1. A *lattice* is a pair $(L, \langle -,- \rangle_L)$ where L is a free abelian group of finite rank and $\langle -,- \rangle_L : L \times L \to \mathbb{R}$ is a symmetric $\mathbb{Z}$-bilinear form such that[1] $\langle -,- \rangle_L \otimes_{\mathbb{Z}} \mathbb{R}$ is positive-definite (i.e., it is an inner product). In other words, the quadratic form $q_L : x \mapsto \langle x, x \rangle_L$ is positive-definite on $L \otimes_{\mathbb{Z}} \mathbb{R}$. ⌟

Remark 1.1.2. 1. In the above definition, it is not sufficient to require the positive-definiteness on L, i.e., $\langle z, z \rangle > 0$ for every $z \in L \smallsetminus \{0\}$, because this only implies positive semi-definiteness on $L \otimes_{\mathbb{Z}} \mathbb{R}$. For instance, if we set $L = \mathbb{Z} + \sqrt{2}\mathbb{Z} \subset \mathbb{R}$ then L is a free abelian group of rank 2, but is not a discrete subgroup; the quadratic form $q_L : L \to \mathbb{R}, x \mapsto |x|^2$ is not positive definite on $L \otimes_{\mathbb{Z}} \mathbb{R}$ (we have $|m + n\sqrt{2}|^2 = 0 \implies m = n = 0$ if $m, n \in \mathbb{Z}$ but not if $m, n \in \mathbb{R}$).

2. Some authors do not demand the condition of positive-definiteness, in which case they are using the terminology "non-degenerate lattice", or "indefinite lattice". For instance, the Néron–Severi lattice of an elliptic surface has signature $(1, \rho - 1)$, by Hodge index theorem (see [SS19, Theorem 4.14]). ⌟

A morphism $f : (L, \langle -,- \rangle) \to (L', \langle -,- \rangle')$ between two lattices is just an additive group morphism preserving the bilinear forms. There is clearly a bijection between the set of isomorphism classes of lattices of given rank $n \geqslant 1$ and the set of $\mathrm{GL}_n(\mathbb{Z})$-equivalence classes of positive-definite quadratic forms on $\mathbb{Z}^n$:

$$\left\{ \text{lattices } (L, \langle -,- \rangle) \text{ of rank } n \right\} / \cong \quad \longleftrightarrow \quad \left\{ \begin{array}{c} \text{positive-definite} \\ \text{quadratic forms } q : \mathbb{Z}^n \to \mathbb{R} \end{array} \right\} \Big/ \mathrm{GL}_n(\mathbb{Z})$$

One direction is obvious: given $q : \mathbb{Z}^n \to \mathbb{R}$, we consider the lattice $(\mathbb{Z}^n, b_q)$ where $b_q(x, y) := \frac{1}{2} \cdot (q(x+y) - q(x) - q(y))$ for any $x, y \in \mathbb{Z}^n$. Conversely, if $(L, \langle -,- \rangle)$ is a lattice of rank n and $\phi : \mathbb{Z}^n \to L$ is a group isomorphism, then we associate the positive-definite

[1] The $\mathbb{R}$-linear map $\langle -,- \rangle_L \otimes_{\mathbb{Z}} \mathbb{R} : (L \otimes_{\mathbb{Z}} \mathbb{R})^2 \cong L^2 \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R}$ is obtained from the universal property of tensor products applied to the $\mathbb{Z}$-bilinear map $L^2 \times \mathbb{R} \to \mathbb{R}$ given by $((v, w), \lambda) \mapsto \lambda \cdot \langle v, w \rangle_L$.

quadratic form $q := q_L \circ \phi$. It is clear that the $\mathrm{GL}_n(\mathbb{Z})$-equivalence class of q is independent of ϕ, and that the two maps we described are inverse of each other.

More importantly, we have a natural bijection relating lattices and discrete subgroups of $\mathbb{R}^n$. First, it is known that a discrete subgroup $L' \subset \mathbb{R}^n$ is a free abelian group of some rank $\leqslant n$. When the rank equals n, we have $L' = B\mathbb{Z}^n$ for some $B \in \mathrm{GL}_n(\mathbb{R})$. Therefore, the map $[B] \mapsto B\mathbb{Z}^n$ gives a bijection

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}) \longleftrightarrow \left\{ \begin{array}{c} \text{discrete additive subgroups} \\ L \subset \mathbb{R}^n \text{ of rank } n \end{array} \right\} =: \mathcal{D}_n.$$

Secondly, we have a bijection between the set of isometry classes of discrete subgroups of rank n and the set of $\mathrm{GL}_n(\mathbb{Z})$-equivalence classes of positive-definite quadratic forms:

$$\mathrm{O}_n(\mathbb{R})\backslash \mathrm{GL}_n(\mathbb{R}) \longleftrightarrow \left\{ \begin{array}{c} \text{positive-definite} \\ \text{quadratic forms } q : \mathbb{Z}^n \to \mathbb{R} \end{array} \right\} =: \mathcal{Q}_n \tag{1.1.1}$$

which can be defined as follows. First, the set $\mathcal{Q}_n$ of positive-definite quadratic forms $q : \mathbb{Z}^n \to \mathbb{R}$ is in one-to-one correspondence with the cone Sym_n^{++} of positive-definite symmetric real $n \times n$ matrices: on the one hand, a quadratic form q corresponds to its Gram matrix with respect to the canonical basis of $\mathbb{Z}^n$, and on the other hand, given $G \in \mathrm{Sym}_n^{++}$, we set $q(x) := {}^{\mathrm{t}}xGx$ for all $x \in \mathbb{Z}^n$. (Note that the action of $g \in \mathrm{GL}_n(\mathbb{Z})$ on $\mathcal{Q}_n$ by pre-composition corresponds to the action $g \cdot A := {}^{\mathrm{t}}gAg$ on $A \in \mathrm{Sym}_n^{++}$).

Then we check that the map $\mathrm{O}_n(\mathbb{R})\backslash \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathrm{Sym}_n^{++}$ given by $[A] \mapsto {}^{\mathrm{t}}AA$ is bijective. Only surjectivity requires a justification: one can argue either via Sylvester's theorem on signatures (law of inertia), or more concretely using Cholesky decomposition.

This finally shows that we have two bijections, whose composition is denoted by σ:

$$\sigma : \left\{ \text{lattices } (L, \langle -, - \rangle) \text{ of rank } n \right\} / \cong \quad \xrightarrow{\simeq} \quad \mathcal{Q}_n/\mathrm{GL}_n(\mathbb{Z}) \quad \xrightarrow{\simeq} \quad \mathrm{O}_n(\mathbb{R})\backslash\mathcal{D}_n. \tag{1.1.2}$$

Therefore, when talking about lattices, we may also refer to (isometry classes) of discrete subgroups $L \hookrightarrow \mathbb{R}^n$ of full rank in $\mathbb{R}^n$ (using the bijection σ) — this may lead to a slight abuse of terminology.

We also have the following identifications:

$$\begin{aligned} \mathcal{D}_n &\simeq \mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}) \\ \mathcal{D}_n/\text{isometries} &\simeq \mathrm{O}_n(\mathbb{R})\backslash\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}) \\ \mathcal{D}_n/\text{homotheties} &\simeq \mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})\mathbb{R}^\times \simeq \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z}) \end{aligned} \tag{1.1.3}$$

We explain how to get the bijection (1.1.3). First, the inclusion $\mathrm{GL}_n^+(\mathbb{R}) := \{ A : \det(A) > 0 \} \hookrightarrow \mathrm{GL}_n(\mathbb{R})$ induces a map $j : \mathrm{GL}_n^+(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$ which is easily seen to be bijective (for the surjectivity, given $A \in \mathrm{GL}_n(\mathbb{R})$ with $\det(A) < 0$, we have $j([A \cdot \mathrm{diag}(-1, 1, ..., 1)]) = [A]$). Now, for all $n \geqslant 1$ we have a group isomorphism $\mathrm{GL}_n^+(\mathbb{R}) \cong \mathrm{SL}_n(\mathbb{R}) \times \mathbb{R}_{>0}$. From this, (1.1.3) follows.

Definition 1.1.3. Let $L \hookrightarrow \mathbb{R}^n$ be a lattice, seen as the isometry class $\sigma(L)$ of a discrete subgroup of full rank in $\mathbb{R}^n$ via the bijection σ defined in equation (1.1.2).

1. Given an ordered $\mathbb{Z}$-basis $B = (b_1, ..., b_n)$ of L, the Gram matrix[2] $G_B(L)$ attached to B is the symmetric $n \times n$-matrix with coefficients $\langle b_i, b_j \rangle_L$ for $1 \leqslant i, j \leqslant n$. In other words, $G_B(L) = {}^t M_B \cdot M_B$ where $M_B \in \mathrm{GL}_n(\mathbb{R})$ is such that $M_B\mathbb{Z}^n$ is any representative of the isometry class $\sigma(L)$.

2. The *covolume* of a lattice L is the Lebesgue measure of any fundamental parallelepiped of $\mathbb{R}^n/\sigma(L)$. In other words if $\sigma(L) = [M\mathbb{Z}^n]$, then $\mathrm{covol}(L) = |\det(M)|$; this is independent of the matrix $M \in \mathrm{GL}_n(\mathbb{R})$ and of the choice of a representative $M\mathbb{Z}^n$ of the isometry class. We say that L is *unimodular* if $\mathrm{covol}(L) = 1$.

   The space of unimodular lattices will be denoted by $X_n := \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$, in view of (1.1.3).

3. The *discriminant* of L is the square of its covolume and is denoted by $\mathrm{disc}(L)$. Alternatively, it is the determinant[3] of the Gram matrix attached to any basis of the lattice.

4. The *minimal norm* of $(L, \langle -, - \rangle_L)$ is $\lambda_1(L) := \min\{ q_L(x)^{1/2} \ : \ x \in L \smallsetminus \{0\} \}$. If $\sigma(L)$ is the isometry class of some discrete subgroup $L' \subset \mathbb{R}^n$, then $\lambda_1(L) = \min\{ \|v\|_2 \ : \ v \in L' \smallsetminus \{0\} \}$.

5. A *minimal vector* of L is a lattice point $v \in L$ such that $q_L(v)^{1/2} = \lambda_1(L)$. The *kissing number* $\kappa(L)$ of L is the number of minimal vectors.

6. The dual[4] of $L \hookrightarrow \mathbb{R}^n$ is $L^\vee = L^* := \{x \in \mathbb{R}^n \ : \ \langle x, y \rangle_L \in \mathbb{Z}, \forall y \in L\}$. It is a lattice: if $L = B\mathbb{Z}^n$ for some $B \in \mathrm{GL}_n(\mathbb{R})$, then $L^\vee = {}^t B^{-1}\mathbb{Z}^n$. We say that L is *self-dual* if $L = L^\vee \subset \mathbb{R}^n$.

7. We say that L is *integral* if $\langle -, - \rangle_L$ takes values in $\mathbb{Z}$ on $L \times L$, that is, $L \subset L^\vee$.

   We say that L is *even* if q_L takes values in $2\mathbb{Z}$ (this implies that L is integral). ⌟

Remark 1.1.4. Here are some basic facts, which are easy to prove (see [Mar02, proposition 1.3.7] for details; note that his definition of unimodularity includes integrality).

1. If $L = B\mathbb{Z}^n$ is unimodular, then $L^\vee = {}^t B^{-1}\mathbb{Z}^n$ is also unimodular.

2. If L is integral, then $[L^\vee : L] = \mathrm{covol}(L)/\mathrm{covol}(L^\vee) = \mathrm{disc}(L)$, since $\mathbb{R}^n/L^\vee \cong \frac{\mathbb{R}^n/L}{L^\vee/L}$. More generally, if $L \subset L'$ then $\mathrm{covol}(L) = [L' : L]\,\mathrm{covol}(L')$.

3. A lattice L is self-dual if and only if it is integral and unimodular.

4. We note that if $L \subset \mathbb{R}^n$ is integral, it does not mean that $L \subset \mathbb{Z}^n$ or that the covolume is an integer. For instance, if L is spanned by $(a_1, a_2), (b_1, b_2) \in \mathbb{R}^2$ then the corresponding quadratic form $\|-\|^2 : L \to \mathbb{R}$ is such that

$$\|n(a_1, a_2) + m(b_1, b_2)\|^2 = n^2(a_1^2 + a_2^2) + nm(2a_1b_1 + 2a_2b_2) + m^2(b_1^2 + b_2^2)$$

[2] The Gram matrix of a lattice is not unique, but is well-defined up to the action of $\mathrm{GL}_n(\mathbb{Z})$ on the cone Sym_n^{++}, considered above.

[3] We prefer to *not* use the notation $|\det(L)|$ which could be either the determinant of a $\mathbb{Z}$-basis of L, or the determinant of a Gram matrix of L.

[4] Under the identification $\beta : V \to V^*, \quad \beta(v) : w \mapsto \langle v, w \rangle$, where $V = \mathbb{R}^n$, the dual lattice corresponds to the set of linear forms on V that are integral on L, i.e., $L^* = \beta^{-1}(\{\phi \in V^* \ : \ \forall x \in L, \phi(x) \in \mathbb{Z}\})$.

for all $n, m \in \mathbb{Z}$. In particular, if $L := \langle (1, \sqrt{3}); (0, 2\sqrt{3}) \rangle$, then the quadratic form takes values in $2\mathbb{Z}$, so L is an even lattice, so is integral, but $\mathrm{covol}(L) = 2\sqrt{3} \notin \mathbb{Q}$. ⌟

Here are some important examples of lattices. Namely, we define the following root lattices, where $n \geqslant 1$ is an integer. Some of them, especially E_6, will reappear later on in our work (see remarks 3.2.6 and 3.2.12).

$$\begin{aligned}
A_n &:= \{ (x_1, ..., x_{n+1}) \in \mathbb{Z}^{n+1} \ : \ x_1 + \cdots + x_{n+1} = 0 \}, && \mathrm{disc}(A_n) = n+1 \\
D_n &:= \{ (x_1, ..., x_n) \in \mathbb{Z}^n \ : \ x_1 + \cdots + x_n \in 2\mathbb{Z} \}, && \mathrm{disc}(D_n) = 4 \\
E_8 &:= \{ (x_1, ..., x_8) \in \mathbb{Z}^8 \cup \left(\tfrac{1}{2} + \mathbb{Z}\right)^8 \ : \ x_1 + \cdots + x_8 \in 2\mathbb{Z} \}, && \mathrm{disc}(E_8) = 1 \\
E_7 &:= \{ (x_1, ..., x_8) \in E_8 \ : \ x_1 + \cdots + x_8 = 0 \}, && \mathrm{disc}(E_7) = 2 \\
E_6 &:= \{ (x_1, ..., x_8) \in E_8 \ : \ x_1 + x_8 = x_2 + \cdots + x_7 = 0 \}, && \mathrm{disc}(E_6) = 3.
\end{aligned}$$

All these root lattices L listed above satisfy $\lambda_1(L) = 2^{1/2}$. Note that the root system of type B_n generates a lattice isomorphic to $\mathbb{Z}^n$ and the root system of type C_n generates a lattice isomorphic to D_n. See [CS98, Chapter 4, §6–§8] or [Mar02, chapter 4] for more details about root lattices. Another important lattice is the Leech lattice Λ_{24}, which is given various definitions in [CS98, Chapter 24] or in [CS98, Theorem 3b), chapter 26, p. 526] (where it is easily defined using a Lorentzian space). Up to isometries, it is the unique even unimodular lattice $L \subset \mathbb{R}^{24}$ such that $\lambda_1(L) = 2$.

1.1.2 Minimal norm of random lattices

If we define the Hermite constant of a lattice $L \hookrightarrow \mathbb{R}^n$ as $\gamma(L) := \lambda_1(L)^2 / \mathrm{disc}(L)^{1/n}$, then a major open problem, as mentioned in the introduction, is to determine the value of the n-dimensional Hermite constant

$$\gamma_n := \sup_{\substack{L \leqslant \mathbb{R}^n \\ \text{lattice}}} \gamma(L). \tag{1.1.4}$$

Equivalently, we are looking for unimodular lattices L having the largest possible $\lambda_1(L)$. We explain in the following paragraphs how the moduli space X_n of unimodular lattices in $\mathbb{R}^n$ is endowed with a probability measure, and how it allows to say something about the distribution of $\lambda_1(L)$.

Any left Haar measure on the locally compact group $\mathrm{SL}_n(\mathbb{R})$ is bi-invariant[5] and induces an $\mathrm{SL}_n(\mathbb{R})$-left-invariant measure on the quotient topological space $X_n := \mathrm{SL}_n(\mathbb{R}) / \mathrm{SL}_n(\mathbb{Z})$ (see [Bou04], chap. VII, §2, corollary 2, page 44). It was shown by Siegel that the measure of X_n is finite (see [Mor15, theorem 7.0.1] for a modern exposition), and therefore we may scale it to get a unique $\mathrm{SL}_n(\mathbb{R})$-left-invariant probability measure μ_n on X_n. In this way we can consider the probability space (X_n, μ_n) and talk about random (unimodular) lattices.

Using this probabilistic point of view, we can state here a result, often referred to as *Gaussian heuristic*, which gives the asymptotic behavior of the expected length of a shortest non-zero vector in a random unimodular lattice, when the dimension goes to infinity. In what follows, $B^n(0,1)$ denotes the L^2-ball in $\mathbb{R}^n$ of radius 1 centered at 0.

[5] In fact, if λ is the Lebesgue measure on $\mathbb{R}^{n^2}$, then $\mu(E) := \lambda(\{ tg \ : \ g \in E, t \in [0,1] \})$ defines a bi-invariant measure on $\mathrm{SL}_n(\mathbb{R}) \hookrightarrow \mathbb{R}^{n^2}$. See also [Bou04, chap. VII, §3, proposition 6, p. 68] for a proof of unimodularity of $\mathrm{SL}_n(\mathbb{R})$.

Theorem 1.1.5 (Rogers). *Consider the length of a shortest non-zero vector in a random unimodular lattice as a random variable $\lambda_1 : X_n \to \mathbb{R}_{>0}$. When $n \to +\infty$, its expected value (taken over $L \in X_n$, with respect to the probability measure μ_n) behaves as*

$$\mathrm{E}_{X_n}[\lambda_1(L)] := \int_{X_n} \lambda_1(L)\,\mathrm{d}\mu_n(L) \quad \sim \quad \mathrm{vol}(B^n(0,1))^{-1/n} \sim \sqrt{\frac{n}{2\pi e}}.$$

Proof. — See theorem 9 in [AEN]. The proof is based on a result of Rogers on higher moments of $L \mapsto |L \cap B \smallsetminus \{0\}|$ where $B \subset \mathbb{R}^n$ is an origin-centered ball. He proved in [Rog56, theorem 3] that for any volume $V > 0$, the distribution of $|(L \smallsetminus \{0\}) \cap B_V|$, where $B_V \subset \mathbb{R}^n$ is the origin-centered ball of volume V and $L \in X_n$ is random, converges weakly to the Poisson distribution of mean $V/2$ as $n \to +\infty$. ■

We can also prove the following version, which gives a lower bound on $\lambda_1(L)$ for a large proportion of the unimodular lattices.

Proposition 1.1.6. *For every $\epsilon > 0$ and all integers $n > 0$, there is a subset $Y_{n,\epsilon} \subset X_n$ of measure $\mu_n(Y_{n,\epsilon}) \geqslant 1 - \frac{\epsilon}{2}$ and such that for all $L \in Y_{n,\epsilon}$ we have*

$$\lambda_1(L) \geqslant \epsilon^{1/n}\,\mathrm{vol}(B^n(0,1))^{-1/n} > \epsilon^{1/n}\sqrt{\frac{n}{2\pi e}} \geqslant (1-\epsilon)\cdot\sqrt{\frac{n}{2\pi e}} \tag{1.1.5}$$

where the last inequality holds for all large enough $n \geqslant n_0(\epsilon) = \frac{\log(\epsilon)}{\log(1-\epsilon)}$.

So for instance by taking $\epsilon = 10^{-2}$ and $n > 1000$, we get that 99 % of unimodular lattices L in $\mathbb{R}^n$ have $\|v\| \geqslant \lambda_1(L) > 0.9954\sqrt{\frac{n}{2\pi e}}$ for all $v \in L \smallsetminus \{0\}$.

The proof of the above proposition relies on the following important result:

Theorem 1.1.7 (Siegel mean value theorem, [Sie45]). *For any compactly supported Riemann-integrable function $f : \mathbb{R}^n \to \mathbb{R}$ we have*

$$\int_{X_n} \Phi_f(L)\,\mathrm{d}\mu_n(L) = \int_{\mathbb{R}^n} f$$

where $\Phi_f(L) := \sum_{v \in L \smallsetminus \{0\}} f(x)$.

Proof of proposition 1.1.6. — We can take $f = \mathbb{1}_B$ where $B := B^n(0,r)$ is some euclidean ball. Then Siegel mean value theorem computes the average $E[\#(B \cap L \smallsetminus \{0\})]$ of the number of non-zero lattice points in B over all unimodular lattices L. Namely, it says that this average is $\mathrm{vol}(B)$.

Let us take $r > 0$ such that $\mathrm{vol}(B) = \epsilon = r^n\,\mathrm{vol}(B^n(0,1))$, that is $r = \epsilon^{1/n}\,\mathrm{vol}(B^n(0,1))^{-1/n}$. Consider the discrete random variable $Z_B : L \mapsto \#(B \cap L \smallsetminus \{0\})$. Note that Z_B only takes *even* values because of the symmetry: $x \in L \iff -x \in L$. Let us denote $\mathrm{P}(Z_B = k) := \mu_n(\{\, L \in X_n \;:\; Z_B(L) = k \,\})$ for any integer $k \geqslant 0$. Then we have

$$\begin{aligned}\mathrm{vol}(B) = \epsilon = \mathrm{E}[Z_B] &= \sum_{k' \geqslant 0} k'\mathrm{P}(Z_B = k') = \sum_{k \geqslant 0} 2k\mathrm{P}(Z_B = 2k) = \sum_{k \geqslant 1} 2k\mathrm{P}(Z_B = 2k) \\ &\geqslant 2\sum_{k \geqslant 1} \mathrm{P}(Z_B = 2k) = 2(1 - \mathrm{P}(Z_B = 0)).\end{aligned}$$

Thus $\mathrm{P}(Z_B = 0) \geqslant 1 - \frac{\epsilon}{2}$. But note that $Z_B(L) = 0 \iff B(0,r) \cap L = \{0\} \iff \lambda_1(L) \geqslant r$. Thus we proved that we probability at least $1 - \frac{\epsilon}{2}$, we have $\lambda_1(L) \geqslant r = \epsilon^{1/n} \operatorname{vol}(B^n(0,1))^{-1/n}$. The rest follows from Stirling's approximation, see remark 1.2.13. ■

We give here a few computational remarks.

Remark 1.1.8. 1. It is surprisingly difficult to exhibit lattices achieving the lower bound as in proposition 1.1.6, when the dimension n gets large (and for fixed $\epsilon > 0$), see remark 1.2.22 below for more details.

2. Given a lattice $L \subset \mathbb{R}^n$, where n is large, determining $\lambda_1(L)$ or finding a minimal vector is a difficult computational problem, known as the "shortest vector problem" or SVP, which underlies some post-quantum cryptosystems like NTRU. All known algorithms to compute $\lambda_1(L)$ (or $\kappa(L)$), e.g. Schnorr–Euchner or Kannan–Fincke–Pohst algorithms, run in exponential time, i.e., the required number of bit operations grows exponentially with the dimension n.

   Given a lattice $L \hookrightarrow \mathbb{R}^n$, the LLL algorithm [LLL82, proposition 1.26] can find in *polynomial* time a non-zero vector $v \in L$ such that $\|v\|_2 \leqslant a^{n-1}\lambda_1(L)$ for any $a > \sqrt{4/3} \simeq 1.15470$, which is *exponentially* far from $\lambda_1(L)$.

   To give some examples of current records, in [GNR10, p. 259] the authors found a shortest vector in a 110-dimensional lattice in 62 days, while [DSvW21, §7.3, table 1] solved an approximate SVP on lattices in dimensions 155 to 180, with an error of at most 5 % within the expected value of $\lambda_1(L)$ given in theorem 1.1.5 — the 180-dimensional case took 51 days. At any rate, this is very far from providing us with an explicit lattice in dimension > 2048 which achieves Minkowski–Hlawka lower bound, as mentioned in the introduction.

3. One strategy to determine γ_n for some fixed (large) dimension $n > 0$ would be to produce unimodular lattices uniformly at random with respect to the probability measure μ_n introduced above. This is not obvious how to proceed, but it can be done (with an error that can be made arbitrarily small) for instance using the work [GM03, §1] on equidistribution of Hecke points.

   Then computing $\lambda_1(L)$ for each such random L is quite long as mentioned in the previous item, and in any case we would only expect to find a result as in theorem 1.1.5, which does not necessarily tell us much about the Hermite constant γ_n itself.

4. A more "efficient" way to compute γ_n would be to run *Voronoi's algorithm* as explained in [Mar02, chapter 7]. It relies on Voronoi's theorem [Mar02, Theorem 3.4.6], which characterizes *extreme lattices*, i.e., lattices at which $\gamma(L)$ attains a local maximum, with respect the euclidean topology on X_n. But going through all extreme lattices is exponentially slow as the dimension increases; even in dimension 9, the algorithm has been running for years but γ_9 is still unknown. ⌟

1.2 · Packings

1.2.1 General notions

We review here some general results on packings, mostly to give a broader point of view on certain questions in discrete geometry. In our setting, we will only consider packings in some euclidean space $\mathbb{R}^n$ (endowed with the L^2-norm $\|\cdot\|_2$), where $n \geqslant 1$, even though packings in compact spaces like $\mathbb{F}_q^n$, an euclidean ball or a sphere can also be studied.

We denote by $\mathrm{vol}(\cdot)$ the Lebesgue measure on $\mathbb{R}^n$. Given $x \in \mathbb{R}^n$ and real numbers $r > 0, p \geqslant 1$, we denote by $B_p^n(x, r)$ the open L^p-ball centered at x of radius r. When $x = 0$ and $r = 1$, we simply denote the origin-centered unit ball by B_p^n. When $p = 2$, we generally omit the subscript p.

Definition 1.2.1. 1. A *body* is a connected subset $C \subset \mathbb{R}^n$ with non-empty interior and compact closure.

2. A collection $\mathcal{C}$ of bodies in $\mathbb{R}^n$ is a *packing* if for every distinct sets $E, E' \in \mathcal{C}$, the interiors of E and E' are disjoint.

3. Given a body $C \subset \mathbb{R}^n$, we define:

   - a *packing of* C as a packing $\mathcal{C}$ consisting of isometric copies of C, i.e. there is a subset $F \subset \mathrm{Isom}(\mathbb{R}^n, \|\cdot\|_2) \cong \mathbb{R}^n \rtimes \mathrm{O}_n(\mathbb{R})$ such that $\mathcal{C} = \{\, f(C) \;:\; f \in F \,\}$.
   - a *packing of translates of* C as a packing $\mathcal{C}$ consisting only of translates of C. In other words, there is a subset $T \subset \mathbb{R}^n$ such that $\mathcal{C} = \mathcal{C} + T := \{C + x \;:\; x \in T\}$, where $C + x := \{\, c + x \;:\; c \in C \,\}$ is the Minkowski sum.
   - a *lattice packing of* C as a packing $\{\, C + t \;:\; t \in T \,\}$ of translates of C where $T \subset \mathbb{R}^n$ is a lattice.

4. A packing of a body C is *periodic* if it is a finite union of translates of a given lattice packing of C.

5. Let $B \subset \mathbb{R}^n$ be a fixed body. If $\mathcal{C}$ is a countable collection of subsets of $\mathbb{R}^n$, then we define the *density* of $\mathcal{C}$ with respect to B as

$$D(\mathcal{C}, B) := \frac{\sum_{E \in \mathcal{C}} \mathrm{vol}(E \cap B)}{\mathrm{vol}(B)} \in [0, \infty].$$

6. Fix a point $x_0 \in \mathbb{R}^n$ and a family $\mathcal{C}$ of subsets of $\mathbb{R}^n$. We set

$$\overline{D}(\mathcal{C}) = \limsup_{r \to +\infty} D(\mathcal{C}, B^n(x_0, r)), \qquad \underline{D}(\mathcal{C}) = \liminf_{r \to +\infty} D(\mathcal{C}, B^n(x_0, r)). \tag{1.2.1}$$

   If these two numbers coincide in $[0, \infty]$, then we call their common value the *density* of the collection $\mathcal{C}$, denoted by $D(\mathcal{C})$.

7. Given a body $C \subset \mathbb{R}^n$, we define the *packing density* $D(C)$ of C, resp. the *translative packing density* $D_T(C)$, resp. the *lattice packing density* $D_\ell(C)$ as:

$$D(C) = \sup_{\substack{\mathcal{C} \text{ packing} \\ \text{of } C}} \overline{D}(\mathcal{C}), \qquad D_T(C) = \sup_{\substack{\mathcal{C} \text{ packing} \\ \text{of translates of } C}} \overline{D}(\mathcal{C}), \qquad D_\ell(C) = \sup_{\substack{\mathcal{C} \text{ lattice} \\ \text{packing of } C}} \overline{D}(\mathcal{C}). \quad \lrcorner$$

Remark 1.2.2. • Given a convex body $C \subset \mathbb{R}^n$, the definitions of $\overline{D}(\mathcal{C})$ and $\underline{D}(\mathcal{C})$ do not depend on the choice of $x_0 \in \mathbb{R}^n$ (see e.g., [CE03, appendix A, p. 708] and the references therein). Moreover, if the convergence of $D(C, B(x_0, r))$ to $\overline{D}(\mathcal{C})$ (as $r \to +\infty$) is uniform in $x_0 \in \mathbb{R}^n$, then for any $x_0 \in \mathbb{R}^n$ and any convex body $P \subset \mathbb{R}^n$ containing 0 in its *interior*, we have

$$\overline{D}(\mathcal{C}) = \limsup_{r \to +\infty} D(\mathcal{C}, rP + x_0).$$

(see e.g., [CE03, appendix A, p. 708]), where $rP := \{ rx \ : \ x \in P \}$. Note that this is wrong if 0 is in the boundary of P, as pointed out in [PA11, exercise 3.4].

- When C is an euclidean ball of radius $r > 0$, then a packing for C is simply called a *sphere packing*; it is characterized by the subset $X \subset \mathbb{R}^n$ of centers of the balls, such that $\|x - y\|_2 \geqslant 2r$ for any distinct points $x \neq y \in X$. ⌟

As mentioned in [Tó17, p. 34], for $d \geqslant 3$, « all methods establishing the existence of dense packings rely on the theory of lattices, thus providing the same lower bounds for $D(C)$ and $D_T(C)$ as for $D_\ell(C)$ ». This is for us a further motivation to specifically study *lattice* packings, in which case the density admits an easy expression.

Proposition 1.2.3. *Given a convex body $C \subset \mathbb{R}^n$ and a lattice $L \subset \mathbb{R}^n$ such that $\mathcal{C} := \{ C + x \ : \ x \in L \}$ is a packing, we have*

$$\overline{D}(\mathcal{C}) = \underline{D}(\mathcal{C}) = \frac{\mathrm{vol}(C)}{\mathrm{covol}(L)}$$

where $\mathrm{covol}(L)$ is the Lebesgue measure of any fundamental parallelepiped of L. ⌟

Proof. — See [Gru07, Corollary 30.1, p. 442] or [Mar02, Proposition 1.8.2]. ■

Proposition 1.2.4. *Let $C \subset \mathbb{R}^n$ be any convex body.*

1. *The packing density $D(C)$ is attained by some packing, that is, $D(C)$ is a maximum.*
2. *The lattice packing density $D_\ell(C)$ is attained.*
3. *The translative packing density $D_T(C)$ is attained.*
4. *The translative packing density $D_T(C)$ is the* supremum *of $\overline{D}(\mathcal{C})$ over* periodic *packings $\mathcal{C}$ of C.* ⌟

Proof. — 1. See [Gro86, theorem §2, p. 186] applied to the full group G of isometries of $(\mathbb{R}^n, \|\cdot\|_2)$.

2. See [Gru07, theorem 30.1] or [Oes90, corollaire, p. 382] when C is an euclidean ball. This is a consequence of Mahler's compactness theorem.

3. See [Gro86, theorem §2, p. 186] applied to the group $G \cong \mathbb{R}^n$ of translations acting on $\mathbb{R}^n$.

4. See for instance the argument given in [CE03, appendix A, p. 709] or [Rog64, theorem 1.7]. ■

Remark 1.2.5. It is not known whether, given a convex body $C \subset \mathbb{R}^n$, $D_T(C)$ is a *maximum* over periodic packings. Hans Zassenhaus conjectured that it is indeed a maximum, see [Gru07, conjecture 30.2]. ⌟

1.2.2 Lattice packings

For any lattice $L \subset \mathbb{R}^n$ and any centrally symmetric convex body $C \subset \mathbb{R}^n$ with compact closure, we define the following invariants:

Definition 1.2.6. 1. The Minkowski functional[6] $\|x\|_C := \inf\{ s \geqslant 0 \ : \ x \in sC \}$, for every $x \in \mathbb{R}^n$.

2. The minimal norm of L with respect to C is $\lambda_1(C, L) := \min\{ \|x\|_C \ : \ x \in L \smallsetminus \{0\} \}$.

3. The Hermite constant of L with respect to C is $\gamma(C, L) := \dfrac{\lambda_1(C, L)^2}{\operatorname{covol}(L)^{2/n}}$.

4. The center density of L with respect to C is

$$\delta(C, L) := \frac{(\lambda_1(C, L)/2)^n}{\operatorname{covol}(L)} = 2^{-n} \cdot \gamma(C, L)^{n/2}.$$

5. The (packing) density of L with respect to C is $D(C, L) := \delta(C, L) \operatorname{vol}(C)$. ⌟

When $C = B^n(0, 1)$ is the unit origin-centered euclidean ball, we omit it from the notation; for instance we set $\lambda_1(L) := \lambda_1(B^n(0, 1), L)$, which is consistent with definition 1.1.3, 4). The idea behind introducing $\lambda_1(C, L)$ is that given $C \subset \mathbb{R}^n$, we want to rescale L so that the packing $\{ C + x \ : \ x \in L \}$ is optimal in the sense that for any $a > 1$, the collection[7] $\{ aC + x \ : \ x \in L \}$ is not a packing. This is made precise in the following statement.

Proposition 1.2.7. *Let $C \subset \mathbb{R}^n$ be a convex body which is centrally symmetric around 0 (i.e., $C = -C := \{ -x \ : \ x \in C \}$). Then*

$$D_\ell(C) = \sup_{\substack{L \hookrightarrow \mathbb{R}^n \\ \text{lattice}}} D(C, L).$$ ⌟

Proof. — Note that for any lattice L, $\{ C + x \ : \ x \in L \}$ is a packing if and only if $L \cap \operatorname{int}(2C) = \{0\}$ if and only if[8] $\lambda_1(C, L) \geqslant 2$ (see [Gru07, Proposition 30.4]).

We know that $D_\ell(C)$ is the supremum of $\dfrac{\operatorname{vol}(C)}{\operatorname{covol}(L)}$ over lattices $L \hookrightarrow \mathbb{R}^n$ *such that* $\{ C + x \ : \ x \in L \}$ is a packing. For any such lattice L, if we rescale it to get the lattice $L' :=$

[6] It is sometimes referred to as Minkowski gauge. It is a norm on $\mathbb{R}^n$, and any norm can be obtained in this way, see for instance [Sie89, Lecture I, Theorem 7].

[7] Here $aC := \{ ac \ : \ c \in C \} \subset \mathbb{R}^n$ denotes a homothetic copy of C.

[8] Let us explain the equivalence $L \cap \operatorname{int}(D) = \{0\} \iff \lambda_1(D, L) \geqslant 1$ for a centrally symmetric convex body D. On the one hand, if $L \cap \operatorname{int}(D) = \{0\}$ then for any $x \in L \smallsetminus \{0\}$, we must have $\|x\|_D \geqslant 1$, because $sD \subset \operatorname{int}(D)$ for any $0 \leqslant s < 1$; thus $\lambda_1(D, L) \geqslant 1$. Conversely, if $\lambda_1(D, L) \geqslant 1$ and $x \in L \cap \operatorname{int}(D) \smallsetminus \{0\}$, then $\overline{B}_2(x, \epsilon) \subset D$ for some $\epsilon > 0$. Then $\lambda x \in D$ where $\lambda := 1 + \epsilon \cdot \|x\|_2^{-1} > 1$, so that $\|x\|_D < 1$, contradicting the hypothesis $\lambda_1(D, L) \geqslant 1$.

$2\lambda_1(C,L)^{-1}L$, then $\{\, C + x \;:\; x \in L' \,\}$ is still a packing (and is "optimal" in the sense that the translates of $\overline{C}$ are touching). We have

$$\frac{\mathrm{vol}(C)}{\mathrm{covol}(L')} = \frac{\mathrm{vol}(C)}{\mathrm{covol}(L)(2\lambda_1(C,L)^{-1})^n} = D(C,L) \geqslant \frac{\mathrm{vol}(C)}{\mathrm{covol}(L)}.$$

Taking the supremum over L yields the claim. ■

In particular, it follows[9] that $D(C,L) \leqslant 1$ for all centrally symmetric convex bodies C and every lattice L. It is convenient to normalize the lattice packing density as follows.

Definition 1.2.8. The *center (lattice) density* of a centrally symmetric convex body C is

$$\delta_\ell(C) := \mathrm{vol}(C)^{-1} D_\ell(C) = \sup_{\substack{L \hookrightarrow \mathbb{R}^n \\ \text{lattice}}} \delta(C,L). \qquad \lrcorner$$

We now say a few words about *laminated lattices*; we focus on the case of packings of euclidean balls for simplicity. The idea is simple: given an n-dimensional lattice packing L, one can create an $(n+1)$-dimensional periodic packing of unit by translating copies of L in $\mathbb{R}^{n+1}$ and "stacking" them as closely as possible to still get a packing.

Proposition 1.2.9. *Suppose that we have a sublattice $L \subset L'$ of (finite) index $N \geqslant 2$ in a lattice $L' \hookrightarrow \mathbb{R}^n$ (we could have for instance $L' = L^\vee$ or $L' = \frac{1}{2}L$). Let $a_0 = 0, ..., a_{N-1} \in L'$ be representatives of* smallest *length in each coset of the quotient L'/L (in particular $Na_i \in L$ for all i). Let S be the set of indices $1 \leqslant j \leqslant N-1$ such that $\|a_j\|_2 < \lambda_1(L)$. Assume that $S \neq \varnothing$ and define*

$$h := \max_{j \in S} \left(\lambda_1(L)^2 - \|a_j\|_2^2\right)^{1/2} > 0,$$
$$\mathcal{P}_0 := \bigcup_{j=0}^{N-1} \left((L + a_j) \times (Nh\mathbb{Z} + jh)\right) \subset \mathbb{R}^n \times \mathbb{R} \cong \mathbb{R}^{n+1}.$$

Then the set $\mathcal{P}$ of open euclidean balls of equal radius $\frac{1}{2}\lambda_1(L)$ centered at points of $\mathcal{P}_0$ is a periodic packing in $\mathbb{R}^{n+1}$ and has density

$$\overline{D}(\mathcal{P}) = \underline{D}(\mathcal{P}) = \frac{\lambda_1(L)}{2h} D(L).$$

Moreover, if L'/L is a cyclic group, then we may re-order the a_i's so that $\mathcal{P}$ is a lattice packing. $\lrcorner$

Remark 1.2.10. In the above proposition, if $S = \varnothing$ happens (e.g., take $L = \mathbb{Z} \times 2\mathbb{Z}$ as an index-2 sublattice of $L' = \mathbb{Z} \times 4\mathbb{Z}$), then it just means that $\lambda_1(L) = \lambda_1(L')$ and so L' gives a lattice packing in dimension n denser than L, since $D(L') = D(L)[L : L']$ by remark 1.1.4.2. Thus we may take $h = 0$ and there is no need to go to an $(n+1)$-dimensional space. $\lrcorner$

[9] This also follows from Minkowski's first theorem. If we let $a := 2(\mathrm{covol}(L)/\mathrm{vol}(C))^{1/n}$ and $C' := aC$, then $\mathrm{vol}(C') = a^n \mathrm{vol}(C) = 2^n \mathrm{covol}(L)$, so there is some $x \in L \cap \overline{C'} \smallsetminus \{0\} \neq \varnothing$, which means that $\lambda_1(C,L) \leqslant a$, or equivalently $D(C,L) \leqslant 1$.

Proof. —

- We first show that $\mathcal{P}$ is indeed a packing. Observe that we have

$$\forall x \in L,\ \forall j > 0,\ \forall r \in \mathbb{Z} \smallsetminus \{0\}, \quad \| \underbrace{(x + a_j, rh)}_{\in \mathbb{R}^{n+1}} \|_2 \geqslant \lambda_1(L). \tag{1.2.2}$$

  Indeed, one has $\|(x + a_j, rh)\|_2^2 = \|x + a_j\|_2^2 + r^2h^2 \geqslant \|a_j\|_2^2 + r^2h^2$ because the a_i's are representatives of shortest possible length in their coset. Now we have either $\|a_j\|_2 \geqslant \lambda_1(L)$, or $j \in S$ in which case $\|a_j\|_2^2 + h^2 \geqslant \lambda_1(L)$ holds anyway thanks to the definition of h.

  We want to show that for every $P \neq Q \in \mathcal{P}_0$, we have $\|P - Q\|_2 \geqslant \lambda_1(L)$. Let $P := (\ell + a_i, i' \cdot h)$ and $Q := (\ell' + a_k, k' \cdot h) \in \mathcal{P}_0 \subset \mathbb{R}^{n+1}$ be two *distinct* points, where $\ell, \ell' \in L$ and $i', k' \in \mathbb{Z}$ are such that $i' \equiv i \pmod N, k' \equiv k \pmod N$. We may write $(\ell + a_i) - (\ell' + a_k) = x + a_j \in L'$ for some unique $x \in L$ and $0 \leqslant j \leqslant N - 1$. Now there are two cases.

  – If $i' = k'$, then we must have $i = k$, which implies that $j = 0$. Thus $\|P - Q\|_2 = \|(x, 0)\|_2 \geqslant \lambda_1(L)$ holds since $x \in L \smallsetminus \{0\}$.

  – If $i' \neq k'$, then we must have $j \neq 0$ and so we may use equation (1.2.2) to conclude that $\|P - Q\|_2 \geqslant \lambda_1(L)$ holds in this case as well.

  This means that the open balls of radius $\rho_L := \lambda_1(L)/2$ centered at points of $\mathcal{P}_0$ are disjoint, i.e., $\mathcal{P}$ is a packing as claimed.

- The packing $\mathcal{P}$ is periodic; it is a (disjoint) union of N translates of the lattice sphere packing with balls centered at points of $L \times Nh\mathbb{Z}$. Therefore we may use proposition 1.2.3 to compute its density (since the Lebesgue measure is additive on finite disjoint unions):

$$\overline{D}(\mathcal{P}) = \underline{D}(\mathcal{P}) = \mathrm{vol}(B^{n+1}(0,1)) \cdot \frac{\rho_L^{n+1} N}{\mathrm{covol}(L) N h} = \frac{\lambda_1(L)}{2h} D(L).$$

- Note that we have

$$\mathcal{P}_0 = \bigcup_{j=0}^{N-1} \left((L \times Nh\mathbb{Z}) + (b_j, j \cdot h) \right)$$

  for *any* set $\{b_0, ..., b_{N-1}\}$ of representatives for L'/L — not necessarily of minimal length in their coset — provided that $b_j \equiv a_j \bmod L$ for all j. If L'/L is cyclic, say generated by the class of some $b_1 \in L$, then we re-arrange the a_i's so that $a_i \equiv i \cdot b_1 = b_i \bmod L$ for all i. Then $\mathcal{P} \subset \mathbb{R}^{n+1}$ is a lattice, generated by $L \times \{0\}$ and $(b_1, h) \in \mathbb{R}^n \times \mathbb{R}$. ■

1.2.3 Packings of euclidean balls

We state here what is known about the densest sphere packings, in some dimensions. For simplicity, from now on, we will denote $D_\ell(n) := D_\ell(B^n(0,1))$ and $\delta_\ell(n) := \delta_\ell(B^n(0,1))$ the lattice packing density (resp. center density) of L^2-balls in $\mathbb{R}^n$. Similarly, we will use the notations $D(L) := D(B^n(0,1), L)$ and $\delta(L) := \delta(B^n(0,1), L)$ given a lattice $L \hookrightarrow \mathbb{R}^n$. Note that $\delta_\ell(n) = 2^{-n} \cdot \gamma_n^{n/2}$.

Proposition 1.2.11. *The lattices $A_1, A_2, A_3, D_4, D_5, E_6, E_7, E_8, \Lambda_{24}$ maximize the density of lattice packing of euclidean balls in their respective dimensions $n \in \{1, 2, ..., 8, 24\}$, with values of $D_\ell(n)$ given in the table below. Moreover, up to similitudes (i.e., up to isometries and homotheties), they are the unique such lattices.*

In dimensions 1, 2, 3, 8, 24, these lattices also maximize the density of (arbitrary) packing of balls. In dimensions 8 and 24 respectively, E_8 and Λ_{24} are the unique periodic *packings (up to similitudes) achieving the maximal packing density.* ⌟

n	1	2	3	4	5	6	7	8	24
$D_\ell(n)$	1	$\frac{\pi}{2\sqrt{3}}$ $\simeq 0.90689$	$\frac{\pi}{\sqrt{18}}$ $\simeq 0.74048$	$\frac{\pi^2}{16}$ $\simeq 0.61685$	$\frac{\pi^2}{15\sqrt{2}}$ $\simeq 0.46525$	$\frac{\pi^3}{48\sqrt{3}}$ $\simeq 0.37294$	$\frac{\pi^3}{105}$ $\simeq 0.29529$	$\frac{\pi^4}{384}$ $\simeq 0.25366$	$\frac{\pi^{12}}{12!}$ $\simeq 0.00192$
$\delta_\ell(n)$	$\frac{1}{2}$	$\frac{1}{2\sqrt{3}}$	$\frac{1}{4\sqrt{2}}$	$\frac{1}{8}$	$\frac{1}{8\sqrt{2}}$	$\frac{1}{8\sqrt{3}}$	$\frac{1}{16}$	$\frac{1}{16}$	1
Attained by the lattice	A_1	A_2	A_3	D_4	D_5	E_6	E_7	E_8	Λ_{24}

Proof. — See the references given in [CK09, p. 1004] for the statements about the optimality among lattices and the uniqueness (for dimensions 3 and 4, a modern proof is available in [CS88, CS89, Theorem 6], and [Mar02, Theorem 6.2.1, Corollary 6.4.4, Theorem 6.5.4, 7), Theorem 6.6.1] for dimensions[10] $n \leqslant 8$. We simply mention explicitly here the work [Bli35] which proves that E_6, E_7, E_8 have the largest possible lattice packing density in their respective dimensions.

For the statements about optimality and uniqueness among *all* packings, see [PA11, Corollary 3.4] for a modern proof in dimension 2 (the result being originally due to A. Thue and L. Fejes Tóth), [Hal05] in dimension 3, [Via17] in dimension 8 and [CKM+17] in dimension 24. It is also worth mentioning the Bourbaki seminars [Oes98, Oes19] for an overview of the proofs in dimensions 3 and 8, 24 respectively. ■

Remark 1.2.12. • The lattices $A_1 \cong \sqrt{2}\mathbb{Z}, A_2, A_3, D_4, D_5, E_6, E_7, E_8$ are *laminated lattices*, see [CS98, chapter 6, theorem 2] for more details.

- In dimensions $n \in \{3, 4, 5, 6, 7\}$, there are infinitely many non-similar *periodic* packings achieving the maximal packing density of balls. This is because the optimal lattice L in dimension $n-1$ satisfies $|L^\vee/L| = \mathrm{disc}(L) > 2$ in each of those cases.
- In dimension 3, the lattice A_3 (similar to D_3) is sometimes called the "face-centered cubic" or fcc arrangement, while the "body-centered cubic" or bcc arrangement (corresponding to the lattice $D_3^\vee$) has lower packing density. The "hexagonal close packing" (or hcp) is a periodic but non-lattice packing; see [CS98, p. 113-117].
- In dimension 9, there is an uncountable family of periodic packings (one of which being a lattice packing) achieving the best *known* packing density, see [CS98, Preface p. xviii].

[10] The optimality of E_8 among lattice packings can be deduced from the optimality of E_7, together with Mordell's inequality (proposition 1.2.17). Similarly, optimality of D_4 can be deduced from the one of A_3.

Dimension 10 is the first one where the best *known* packing is *not* a lattice packing: it is a periodic packing discovered by Marc Best, consisting of 40 translates of a lattice packing (see [CS98, chapter 5, p. 140]).

- According to [CS98, p. 13], it is « a reasonable guess » that when $n \leqslant 8$, we should have $D(B^n(0,1)) = D_\ell(n)$. But it was conjectured in [Rog64, p. 15] that $D(n) > D_\ell(n)$ for all large enough dimensions. ⌟

Remark 1.2.13. For every real number $p \geqslant 1$, the Lebesgue measure of any L^p-ball of radius 1 equals $2^n \cdot \Gamma\left(1+\frac{1}{p}\right)^n \cdot \Gamma\left(1+\frac{n}{p}\right)^{-1}$. In particular, when $p = 2$, we have $\Gamma(3/2) = \frac{\sqrt{\pi}}{2}$ so that one gets $\mathrm{vol}(B^n(0,1)) = \pi^{n/2} \cdot \Gamma\left(\frac{n}{2}+1\right)^{-1}$.

When $n \to +\infty$, Stirling's approximation yields $\mathrm{vol}(B^n(0,1)) \sim (\pi n)^{-1/2} \cdot (2\pi e/n)^{n/2}$, which implies in particular that[11]

$$\mathrm{vol}(B^n(0,1))^{1/n} \sim \sqrt{\frac{2\pi e}{n}}, \qquad \log \mathrm{vol}(B^n(0,1)) = -\frac{n}{2}\log(n) \cdot (1+o(1))$$

as $n \to +\infty$. ⌟

Remark 1.2.14. 1. It is known, from Voronoi's theorem and a result of Korkine–Zolotareff, that $D_\ell(B^n(0,1))$ is attained by an integral lattice. In particular, $\delta_\ell(B^n(0,1))^2$ is a rational number. See [Mar02, Corollary 3.4.7].

2. From [Rog56, theorem 3] (cited in theorem 1.1.5), one can deduce that the variables $L \in X_n \mapsto \mathrm{vol}[B^n(0,\lambda_1(L))] = \lambda_1(L)^n \,\mathrm{vol}(B^n(0,1)) = 2^n D(L)$ converge weakly to an exponential law $\mathrm{Exp}(1/2)$ with parameter $1/2$ (i.e., mean 2), see for instance [AEN, Corollary 4]. In particular, the expected value of the lattice sphere packing density function $L \in X_n \mapsto D(L)$ is asymptotic to $2^{-n} \cdot 2$ as $n \to +\infty$.

   Note that from proposition 1.1.6 we have $D(L) \geqslant \epsilon \cdot 2^{-n}$ for unimodular lattices L in a subset of X_n of measure at least $1 - \frac{\epsilon}{2}$.

3. There is a notion of "covering" of balls (or more generally of convex bodies), which is somehow dual to the notion of "packing". The thinnest coverings of balls are only known in dimensions 1 and 2, and the thinnest lattice coverings of euclidean balls are known in dimensions $n \leqslant 5$, where $A_n^\vee$ is optimal. See [CS98, Table 1.1, p. 12]. ⌟

1.2.4 Lower and upper bounds on the sphere packing density

1.2.4.1 Lower bounds

There is a general lower bound, valid not only for balls, but for any convex centrally symmetric body, due to Minkowski and Hlawka. The proof relies on Siegel's mean value theorem 1.1.7, so this probabilistic argument does not tell us precisely which lattices achieve a large packing density.

[11] We also have an inequality $\mathrm{vol}(B^n(0,1))^{1/n} > \sqrt{\frac{2\pi e}{n}}$ for every $n \geqslant 1$, which can be shown using refined versions of Stirling's approximation, see for instance [Mor10, Corollary 1].

Theorem 1.2.15 (Minkowski–Hlawka theorem). *Let $n \geqslant 2$. For any star-shaped (e.g., convex) and centrally symmetric body $C \subset \mathbb{R}^n$, we have $D_\ell(C) \geqslant 2\zeta(n) \cdot 2^{-n}$.* ⌟

Proof. — See Siegel's proof in [Sie89, Lecture XV, §7–8] or [PA11, Corollary 7.10]. ■

This lower bound was further improved by a linear factor by Schmidt (see [PA11, p. 86]). On the other hand, Venkatesh's superlinear improvement in some[12] dimensions, given in [Ven13], is specific to L^2-balls and does not apply to general convex centrally symmetric bodies. The best known bound on $D_\ell(n)$ valid in *all* dimensions is due to Keith Ball:

Theorem 1.2.16 ([Bal92]). *For every $n \geqslant 1$, we have $D_\ell(n) \geqslant 2\zeta(n)\dfrac{n-1}{2^n}$.* ⌟

In dimensions $n \geqslant 8$ divisible by 4, this was slightly improved by [Van11]. Let us mention here a useful result, the so-called Mordell's inequality: given a lattice $L \hookrightarrow \mathbb{R}^n$ and $m \leqslant n$, one can get a lower bound on $\delta_\ell(m)$ in terms of $\delta(L)$. Some applications will be mentioned in remark 3.2.4.

Proposition 1.2.17 (Mordell). *For all $n \geqslant m \geqslant 2$, we have $\delta_\ell(m) \geqslant \Big(2^{m-n}\delta_\ell(n)^{\frac{m-1}{n}}\Big)^{\frac{m}{n-1}}$.* ⌟

Proof. — We simply apply [Mar02, Theorem 2.3.1], which is stated in terms of Hermite constants, namely $4 \cdot \delta_\ell(n)^{2/n} = \gamma_n \leqslant \gamma_m^{\frac{n-1}{m-1}}$. It follows that

$$\begin{aligned}\delta_\ell(n) &= 2^{-n}\gamma_n^{n/2} \leqslant 2^{-n}\big(\gamma_m^{\frac{n-1}{m-1}}\big)^{n/2} = 2^{-n}\big(4 \cdot \delta_\ell(m)^{2/m}\big)^{\frac{n(n-1)}{2(m-1)}} \\ &= \big(2^{n-m} \cdot \delta_\ell(m)^{\frac{n-1}{m}}\big)^{\frac{n}{m-1}},\end{aligned}$$

which easily implies the claimed inequality. For the case $m = n-1$, one can also refer to [CS98, equation (19), chap. 6, p. 167], which reads $\delta_\ell(n-1) \geqslant \frac{1}{2}\delta_\ell(n)^{\frac{n-2}{n}}$. ■

Remark 1.2.18. Using laminated lattices, we see that we also have

$$\delta_\ell(n) \geqslant \frac{1}{2}\delta_\ell(n-1). \tag{1.2.3}$$

Indeed, given a lattice $L \subset \mathbb{R}^{n-1}$ with maximal density, let $L' \subset \mathbb{R}^n$ be the lattice generated by $L \times \{0\} \subset \mathbb{R}^n$ and $e_n := (0, ..., 0, \lambda_1(L))$. We have $\lambda_1(L') = \lambda_1(L)$ and so

$$\delta_\ell(n) \geqslant \delta(L') = \frac{(\lambda_1(L')/2)^n}{\operatorname{covol}(L')} = \frac{\lambda_1(L)}{2} \cdot \frac{(\lambda_1(L)/2)^{n-1}}{\operatorname{covol}(L)\lambda_1(L)} = \frac{1}{2}\delta(L).$$

There is an analogous result about lattice kissing numbers. Given any dimension $n > 0$, let $\kappa_\ell(n) := \sup\{\, \kappa(L) \;:\; L \hookrightarrow \mathbb{R}^n \text{ lattice} \,\}$; it is finite and we even have $\kappa_\ell(n) \leqslant 2^{n+1} - 2$ (see [BMP06, §2.4, p. 94]). Now we claim that $\kappa_\ell(n+1) \geqslant \kappa_\ell(n) + 2$. Indeed, let $L \subset \mathbb{R}^n$ be a lattice with maximal kissing number $\#\{\, x \in L \;:\; \|x\| = \lambda_1(L) \,\} = \kappa_\ell(d)$. Let

[12] More specifically, it was proved that $D_\ell(2 \cdot \phi(m)) \geqslant m \cdot 2^{-2\phi(m)}$ for all $m \geqslant 1$, where ϕ is Euler totient function. This implies that for any $c < e^\gamma/2 \simeq 0.8905$ and any $x \geqslant 1$, we have $D_\ell(n) \geqslant cn\log(\log(n))2^{-n}$, where $n = 2\prod_{p \leqslant x \text{ prime}}(p-1) \in \{2, 4, 16, 96, 960, ...\}$ is a sparse sequence of dimensions. (This was also proved by other methods in [Mou17, Aut16]).

$L' \subset \mathbb{R}^{n+1}$ be the lattice generated by L and $e_{n+1} := (0, ..., 0, \lambda_1(L)) \in \mathbb{R}^{n+1}$. Then we have $\lambda_1(L') = \lambda_1(L)$ and

$$\kappa_\ell(n+1) \geqslant \#\{ x \in L' : \|x\| = \lambda_1(L') \} \geqslant \kappa_\ell(n) + 2. \qquad \lrcorner$$

Remark 1.2.19. For L^2-balls, Minkowski–Hlawka lower bound can be achieved *asymptotically* by an odd (hence integral) unimodular lattice, and by an even unimodular lattice in dimensions divisible by 8. The precise statements — originally proved by Conway and Thompson — are given in [MH73, theorem II.9.5, p. 46–47] or in [CS98, theorem 25, chapter 7, p. 197].

On the other hand, the sphere packing density of any unimodular integral lattice L in dimension n (which needs to be a multiple of 8 if the lattice is moreover *even*) is asymptotically upper bounded by $D(L) \leqslant 2^{n(\alpha+o(1))}$ where $\alpha := \log_2\left(\sqrt{\pi e/24}\right) \simeq -0.74538$, see [RS98, theorem 1]. $\lrcorner$

Remark 1.2.20. In view of theorem 1.1.5, we note that Minkowski–Hlawka lower bound from theorem 1.2.15 implies (using the identity $\lambda_1(L) = 2\left(\frac{D(L)}{\mathrm{vol}(B^n(0,1))}\right)^{1/n} \mathrm{covol}(L)^{1/n}$ and remark 1.2.13) that for all $n \geqslant 1$, there *exists* a lattice $L_n \subset \mathbb{R}^n$ of covolume 1 such that

$$\lambda_1(L_n) \geqslant 2^{1/n} \,\mathrm{vol}(B^n(0,1))^{-1/n} = \sqrt{\frac{n}{2\pi e}} \cdot (1 + o(1)). \tag{1.2.4}$$

On the other hand, from theorem 1.2.23 below we know that for all lattices $L \subset \mathbb{R}^n$ we have:

$$\lambda_1(L) \leqslant \sqrt{\frac{4^{1-\alpha_{\mathrm{KL}}} n}{2\pi e}} \,\mathrm{covol}(L)^{1/n} \cdot (1 + o(1)),$$

as $n \to +\infty$, where $4^{1-\alpha_{\mathrm{KL}}} \simeq 1.743381$. $\lrcorner$

Remark 1.2.21. The lower bounds given in theorems 1.2.15 and 1.2.16 is far from the truth in *low* or *medium* dimensions. For instance, if we look at $\mathbb{Z}^n$, it has unit covolume and $\lambda_1(\mathbb{Z}^n) = 1$, so it does better than the lower bound (1.2.4) if and only if $1 > 2^{1/n} \,\mathrm{vol}(B^n(0,1))^{-1/n}$, or equivalently $\mathrm{vol}(B^n(0,1)) > 2$, which happens if and only if $n \leqslant 10$. The root lattices A_n (if $2 \leqslant n \leqslant 12$) and D_n (if $3 \leqslant n \leqslant 16$) have a sphere packing density greater than the lower bound in theorem 1.2.16.

In slightly higher dimensions $n \leqslant 48$, the densest known lattices, listed in [CS98, p. xix-xx, p. 17], all have a packing density larger than Minkowski bound.

Some families of lattices have a packing density larger than Minkowski bound in medium dimensions. We mention here Maurice Craig's cyclotomic lattices defined in [CS98, Chapter 8, §6, §7.3c)] and its improvements as in[13] [FIdD11]; they are the densest lattices known in *some* dimensions $148 \leqslant n \leqslant 3000$ such that $n + 1$ is prime ([CS98, Chapter 8, §6, p. 224]), and they have greater density than Minkowski's bound if $n \leqslant 508$.

[13] There are some typographic mistakes in table 1, p. 1442 of the cited paper: we found for instance $\mu_2 = 64, \mu_3 = 109, \mu_4 = 225, \mu_5 = 551, \mu_6 = 1384$.

In some dimensions[14] $\leqslant 1024$, the densest known lattice sphere packings are obtained using Mordell–Weil lattices, initially studied in [Elk94, Shi91]. This is a motivation for our work: we are going to investigate more of these lattices in the following chapters (see especially theorem 3.2.7). We note that Elkies' 64-dimensional lattice from [Elk94, Theorem 1, p. 352, for $n = 5$] (with $\log_2(\delta) = 24.718$) has been superseded by a denser lattice constructed by G. Nebe in [Neb98] (with $\log_2(\delta) = 25.36$, see [CS98, page xx]), as mentioned in the introduction of [Elk01].

Finally, let us point out that applying Mordell's inequality (proposition 1.2.17) to some dense lattice in dimension n can be used to improve Minkowski–Hlawka lower bound in dimension $n-1$, even though not in a very explicit way (see example 3.2.3). ⌟

Remark 1.2.22. On the other hand, when n is large enough, finding explicitly lattices achieving the lower bound (1.2.4) is very challenging: Minkowski's argument goes through an averaging argument (over random lattices, using theorem 1.1.7), so it is not constructive, and we have no idea how to produce some L_n with "large" $\lambda_1(L)$ as soon as $n > 2048$ (or even > 1040), as mentioned in the introduction.

However, moreless explicit constructions (using number fields or algebraic curves) due to Tsfasman in [Tsf91, Theorem 5.5, Theorem 6.2] yield lattices L'_n of covolume 1 (for some sequence of dimensions n going to $+\infty$), that achieve $D(L'_n) \sim 2^{-\alpha' n(1+o(1))}$ for some $\alpha' > 0$, for instance we can take $\alpha' = 1.3888$ (equivalently, $\lambda_1(L'_n) \geqslant c'\sqrt{n}$ for some $c' > 0$ since $\lambda_1(L) = 2\Big(\frac{D(L)}{\mathrm{vol}(B^n(0,1))}\Big)^{1/n} \mathrm{covol}(L)^{1/n}$; compare this to proposition 1.1.6). However, they do not give dense lattices in low or medium dimensions (e.g., when we apply [Tsf91, Lemma 5.2] to the tower of curves $(X_n/\mathbb{F}_{q^2})_{n\geqslant 3}$ defined by Garcia and Stichtenoth in [GS95a, theorem 2.10, proposition 3.1, remark 3.4] with $q^2 = 9$, we get lattices in dimensions $|X_n(\mathbb{F}_{q^2})| - 1 \in \{77, 221, 653, ...\}$ with a packing density much lower than Minkowski–Hlawka bound).

In fact, producing lattices L_n in an infinite sequence of dimensions satisfying $D(L_n) \sim 2^{-\alpha n(1+o(1))}$ for some $\alpha > 0$ — sometimes referred to as *asymptotically good families* — is already hard. In comparison, Craig's cyclotomic lattices L''_n mentioned in the previous remark 1.2.21 satisfy $D(L''_n) \geqslant n^{-\log(\log n)(1/2+o(1))}$ which yields $\lambda_1(L''_n) \geqslant n^{1/2-\frac{\log(\log n)}{2n}(1+o(1))}$. Elkies or Shioda's narrow Mordell–Weil lattices MW_n (see theorems 0.1 and 0.2) achieve $D(\mathrm{MW}_n) \geqslant n^{-n(1/12+o(1))}$ which yields $\lambda_1(\mathrm{MW}_n) \geqslant n^{5/12(1+o(1))}$, for a suitable infinite sequence of dimensions n. Let us also mention the asymptotic behavior of the packing density of some root lattices: $D(\mathbb{Z}^n) \sim D(A_n) \sim D(D_n) \sim n^{-\frac{n}{2}(1+o(1))}$. ⌟

1.2.4.2 Upper bounds

The only known upper bounds on $D_\ell(n)$ (valid for all $n \geqslant 1$) are actually also upper bounds on $D(B^n(0,1))$, and they are all exponentially far from the best known lower bound valid in all dimensions, given in theorem 1.2.16. Currently, the best known upper bound on $D(B^n(0,1))$ is due to Kabatiantsky and Levenshtein.

[14] On the other hand, in some dimensions $3332 \leqslant n \leqslant 4096$, the paper [Che13] exhibits lattices with larger density than Shioda's or Elkies' Mordell–Weil lattices. But in that range of dimensions, all these lattice packings are outperformed by Minkowski lower bound anyway.

Theorem 1.2.23 ([KL78, Corollary 2, p. 13]). *Let* $\alpha_{\mathrm{KL}} := 0.59905576$. *Then as* $n \to +\infty$, *one has* $D(B^n(0,1)) \leqslant 2^{-n(\alpha_{\mathrm{KL}}+o(1))}$. ⌟

Remark 1.2.24. Kabatiansky and Levenshtein actually proved that, when $n \to +\infty$, we have

$$\forall \theta \in]\pi/3, \pi/2[, \quad \frac{1}{n}\log_2[D(B^n(0,1))] \leqslant \log_2(\sin(\theta/2)) + B_{\mathrm{KL}}(\theta) + o(1),$$
$$B_{\mathrm{KL}}(\theta) := b_+(\theta)\log_2(b_+(\theta)) \; - \; b_-(\theta)\log_2(b_-(\theta)), \qquad b_\pm(\theta) := \frac{1 \pm \sin(\theta)}{2\sin(\theta)}.$$

The optimal value of θ which minimizes the right-hand side is about $\theta \simeq 1.0995124 \simeq 62.99^\circ \in]\pi/3, \pi/2[$, for which the right-hand side attains a value of $\simeq -0.59905576$.

In the same paper [KL78], they also got an upper bound on the maximal kissing number $\kappa(n)$ in dimension n, namely $\kappa(n) \leqslant 2^{n(B_{\mathrm{KL}}(\pi/3)+o(1))}$, where $B_{\mathrm{KL}}(\pi/3) \simeq 0.401413$. Note that Chabauty–Shannon–Wyner lower bound (which has the best known exponent so far) reads $\kappa(n) \geqslant 2^{n(0.2075-o(1))}$. The value $\kappa(n)$ is known for $n \in \{1, 2, 3, 4, 8, 24\}$.

The asymptotic behavior of the largest *lattice* kissing number $\kappa_\ell(n)$ in dimension n (introduced in remark 1.2.18) is more difficult to study; it is only recently that an exponential lower bound $\kappa_\ell(n) \geqslant 2^{n(0.021937-o(1))}$ has been found in [Vlă19, Theorems 1.1 and 1.5]. The value $\kappa_\ell(n)$ is known for $n \in \{1, ..., 8, 9, 24\}$. ⌟

Another central result giving an upper bound on the packing density, valid for centrally symmetric convex bodies, was found by H. Cohn and N. Elkies. One of its notable features is that it is sharp for the 8- and 24-dimensional euclidean balls (see [Via17, CKM+17]).

Theorem 1.2.25 ([CE03, appendix B]). *For all centrally symmetric convex bodies* $C \subset \mathbb{R}^n$, *we have*[15]

$$D_T(C) \leqslant \Delta_{\mathrm{LP}}(C) := \inf\Big\{ \frac{\mathrm{vol}(C) f(0)}{2^n \hat{f}(0)} \; : \; f \in \mathcal{F}_C \Big\}$$

where (denoting by $\hat{f}$ *the Fourier transform of* f*)*

$$\mathcal{F}_C := \Big\{ f : \mathbb{R}^n \to \mathbb{R} \text{ Schwartz function} \Big| f \neq 0, \;\; \forall x \notin C, f(x) \leqslant 0, \;\; \forall t \in \mathbb{R}^n, \hat{f}(t) \in \mathbb{R}_{\geqslant 0} \Big\}.$$

⌟

Remark 1.2.26. 1. The best *known* upper bounds for $D(B^n(0,1))$ for $4 \leqslant n \leqslant 9$ are given in the recent work [CdLS22].

2. It is not know whether the limits $\lim\limits_{n\to+\infty} \dfrac{\log_2[D(B^n(0,1))]}{n}$ and $\lim\limits_{n\to+\infty} \dfrac{\log_2(D_\ell(n))}{n}$ exist (see [PBM05, Problem 4, p. 50]), but they are probably both equal to 1 (see for instance the last paragraph of [Ven13, p. 1629]).

3. The asymptotics behavior of the linear programming bound $\Delta_{\mathrm{LP}}(B^n(0,1))$ as $n \to +\infty$ has been conjectured in [ACH+20, Conjecture 3.2]. If true, it would give the following improvement on Kabatiantsky–Levenshtein upper bound: $D(n) \leqslant 2^{-(\lambda+o(1))n}$ where $\lambda = -\frac{1}{2}\log_2(e/(2\pi)) \simeq 0.60440$. ⌟

[15] If $\hat{f}(0) = 0$ then we set $f(0)/\hat{f}(0) := +\infty$.

1.3 · Elliptic curves

1.3.1 General notions

We first review very standard material about elliptic curves.

In what follows, an *algebraic variety* X over a field K is a separated integral (i.e., reduced and irreducible) scheme of finite type over K. We will denote by $|X|$ the set of closed points of X. A *curve* is an algebraic variety of dimension 1. A *surface* is an algebraic variety of dimension 2. In the rest of this work, when q is a power of prime number, we denote by $\mathbb{F}_q$ a finite field with q elements (it is unique up to isomorphism), and we denote by $\overline{K}$ and K^{sep} an algebraic and separable closures of a given field K (both are unique up to field isomorphisms). We denote by $\mathbb{P}^n_K$ the projective n-space over K.

Definition 1.3.1. Let K be a field. An elliptic curve over K is a pair[16] (E, O_E) where E is a smooth projective geometrically[17] irreducible algebraic curve over K of genus 1, and $O_E \in E(K)$. ⌟

It is known from Riemann–Roch theorem that any such curve admits a closed embedding as a smooth cubic curve in $\mathbb{P}^2_K$, via a Weierstrass equation like $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$. For simplicity, we will generally write the equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ of the affine open subset of the elliptic curve given by $E \smallsetminus \{[0:1:0]\}$. In that case, we take $O_E = [0:1:0]$ to be the distinguished point, and we will generally omit it from the notation (E, O_E) for elliptic curves.

It is well-known that an elliptic curve is a commutative projective algebraic group, in other words a 1-dimensional abelian variety, so that $E(K')$ is an abelian group for every field extension K'/K.

We will mostly focus on the case where K is a global function field, which are somehow the analogues[18] of number fields in positive characteristic.

Definition 1.3.2. A global function field K is a field isomorphic to the function field $k(C)$ of some smooth projective geometrically[19] irreducible curve C over a *finite* field k (note that C is uniquely determined by K, up to isomorphism, by [GW20, Theorem 15.21]). ⌟

[16] The existence of the K-rational point O_E is essential: for every prime $p > 3$, $X^3 + pY^3 + p^2Z^3 = 0$ defines a smooth projective plane cubic curve over $\mathbb{Q}$, so it has genus 1, but has no points over $\mathbb{Q}$ (not even in $\mathbb{Q}_p$), so it is not an elliptic curve over $\mathbb{Q}$. More relevant examples are given by non-trivial elements of the Tate–Shafarevich group Ш of an elliptic curve, e.g., Selmer's curve $S : 3X^3 + 4Y^3 + 5Z^3 = 0$ in the 3-torsion of Ш of its jacobian $\mathrm{Jac}(S) : X^3 + Y^3 + 3 \cdot 4 \cdot 5Z^3 = 0$.

[17] In fact, geometric irreducibility follows from the fact that E is smooth, irreducible and $E(K) \neq \varnothing$, see [Poo17, Proposition 2.3.24] and [GW20, Exercise 6.20]. On the other hand, the projective line $\mathbb{P}^1_{\mathbb{F}_{q^2}}$ considered as a smooth irreducible (but not geometrically irreducible) curve of genus 0 over $\mathrm{Spec}(\mathbb{F}_q)$ has no $\mathbb{F}_q$-rational point.

[18] For instance, both of these classes of fields are *global fields*: they are the fraction field of an infinite integrally closed domain A of finite type over $\mathbb{Z}$ (as a ring) such that A/I is finite for any non-zero ideal $I \trianglelefteq A$. Equivalently, it is the fraction field of a finitely generated $\mathbb{Z}$-algebra which is an integral domain of Krull dimension 1 (see [Poo17, §1.1.3]).

[19] By [Liu06, corollary 2.14, p. 91], this ensures that $k(C) \cap k^{\mathrm{sep}} = k$.

There are several reasons for choosing global function fields as setting, instead of taking K to be a number field:

- One reason is that the Néron–Tate height takes rational values (see remark 1.3.18), and we have a very explicit lower bound on the minimal non-zero height of a point in the Mordell–Weil lattice of E over K (see theorem 1.3.24).
- Another reason is that over function fields, the rank of elliptic curves happens to be unbounded (see theorem 1.3.44), and this can yield high-dimensional lattice sphere packings, while this is far from being known (and perhaps not even true) over number fields.
- Finally, it is more difficult to compute the L-function of an elliptic curve over a number field, which is just a Dirichlet series, while over function fields it is a rational function (or even a polynomial) in some variable T (see theorem 1.3.30). Also, much more is known on the Birch–Swinnerton-Dyer conjecture over function fields compared to the situation over number fields.

In the case where $K = k(C)$ is a global function field, there are two "special" classes of elliptic curves over K.

Definition 1.3.3. Let E be an elliptic curve over $K = k(C)$. We say that E is:

- *constant* if there is an elliptic curve E_0 over k and an isomorphism $E_0 \times_k k(C) \cong E$ over $k(C)$.
- *isotrivial* (or potentially constant or split) if there is a finite extension K'/K such that the base change $E \times_K K'$ is a constant elliptic curve over K'. Equivalently, its j-invariant $j(E)$ lies in k. ⌟

Example 1.3.4. For instance, for every prime $p \geqslant 5$ and any $a \in \mathbb{F}_p^\times$, both $E_0 : y^2 = x^3 + a$ and $E_1 : y^2 = x^3 + at^6$ are constant curves over $\mathbb{F}_p(t)$ (we actually have $E_1 \cong E_0$), $E_2 : y^2 = x^3 + t$ is isotrivial (we have $E_2 \cong E_0$ over $\mathbb{F}_p(t^{1/6})$) but not constant (see [Sil08a, proposition III.3.1.b)]) and $E_3 : y^2 = x^3 + x + t$ is not isotrivial since $j(E_3) = 12^3 \cdot \frac{4}{4+27t^2}$ does not lie in $\mathbb{F}_p$. ⌟

There are several invariants attached to an elliptic curve E over a field K. We already mentioned briefly the j-invariant, which characterizes the $\overline{K}$-isomorphism class of E (see [Sil08a, III.1.4.b)]). We recall that the j-invariant of an elliptic curve E given (when possible, e.g., if $\mathrm{char}(K) \neq 2, 3$) by a *short* Weierstrass equation $y^2 = x^3 + ax + b$ is $j(E) = 12^3 \cdot \dfrac{4a^3}{4a^3 + 27b^2}$, where the discriminant $\Delta(a, b) := -16(4a^3 + 27b^2)$ does not vanishes (see [Sil08a, III.§1, p. 42] for the general definitions).

Now we turn to local invariants of E over K, i.e., which are defined used local data at each place of K. We recall that a place of a global field K is a topological equivalence class of non-trivial absolute values $K \to \mathbb{R}_{\geqslant 0}$.

Definition 1.3.5. We denote by V_K a set of representatives of all places of K, and by $V_K^0 \subset V_K$ the subset of the non-archimedean absolute values (the "finite" places). Note that when K has positive characteristic (i.e., is a global function field), all places are non-archimedean (i.e., ultrametric). Given $v \in V_K$ we denote by K_v the completion of K with respect to v, and by $\mathcal{O}_{K_v} \subset K_v$ the valuation ring when v is non-archimedean. ⌟

For a global function field $K = k(C)$, the set $V_K = V_K^0$ is in bijection with the set $|C|$ of closed points of C, which is itself in bijection with the set of Galois orbits of $\bar{k}$-rational points in $C(\bar{k})$ (see [GW20, Proposition 5.4, Remark 15.23]): given a closed point $x \in |C|$, the local ring $\mathcal{O}_{C,x} = \mathcal{O}_x$ is a discrete valuation ring (see [GW20, Proposition 11.39]), with finite residue field $\mathbb{F}_x$ and valuation $v_x : k(C) \to \mathbb{Z}$, which yields an ultrametric absolute value[20] $|\cdot|_x : s \mapsto (\#\mathbb{F}_x)^{-v_x(s)}$. The degree of a place, seen as a closed point $x \in |C|$, is defined as $\deg(x) := [\mathbb{F}_x : k]$ (the extension $k \hookrightarrow \mathbb{F}_x$ is finite by [GW20, Proposition 3.33]).

Example 1.3.6. For instance, when $C = \mathbb{P}^1_k$, the places of $k(C) = k(t)$ are of two types: on the one hand, we have the closed point "at infinity" $\infty := [1 : 0] \in \mathbb{P}^1_k$, whose associated valuation v_∞ is given by[21] $-\deg$ on $k[t] \subset k(t)$. We have $\mathcal{O}_{v_\infty} \cong k[\![t]\!]$ and $k_{v_\infty} \cong k$. All the other places are the closed points of $\mathbb{A}^1_k$, which are given by irreducible monic polynomials P over k and their "P-adic" valuation. ⌟

In the context of number fields, we typically think of the non-archimedean places as prime ideals (and then take products of these), while in the context of function fields, we think of the places as closed points (and then take sums of these). In the latter case, by "sum" of closed points, we simply mean a divisor[22] D on the curve C defined over a field k, i.e., a (formal) finite $\mathbb{Z}$-linear combination $D = \sum_{x \in |C|} n_x \cdot x$ of closed points. Its *degree* is $\deg(D) := \sum_{x \in |C|} n_x [\mathbb{F}_x : k]$.

We can now define the following quantities, attached to an elliptic curve E over a global field K.

Definition 1.3.7. • Given a non-archimedean place $v \in V_K^0$, we define the *reduction* $\overline{E_v}$ *of* E *modulo* v as follows. We fix a minimal integral Weierstrass equation for E, of the form $Y^2Z + a_{1,v}XYZ + a_{3,v}YZ^2 = X^3 + a_{2,v}X^2Z + a_{4,v}XZ^2 + a_{6,v}Z^3$ for some $a_{i,v}$ in the discrete valuation ring $\mathcal{O}_{K_v}$. We will denote by $\overline{E_v}$ the plane projective curve over $\mathbb{F}_v$ defined by reducing the coefficients $a_{i,v}$ modulo the maximal ideal of $\mathcal{O}_{K_v}$. The isomorphism class of this (possibly singular) cubic projective curve $\overline{E_v}$ does not depend on the choice of a minimal integral Weierstrass model[23], and we have a "reduction modulo v" map $E \to \overline{E_v}$ coming from the reduction map $\mathbb{P}^2(K) \hookrightarrow \mathbb{P}^2(K_v) \to \mathbb{P}^2(\mathbb{F}_v)$ (this follows from [Sil08a, proposition VII.1.3 (b)]; see [Sil08b, VII.2, p. 187]).

• The *minimal discriminant* $\Delta_{\min}(E/K)$ is defined for number fields in [Sil08a, VIII.8] and for function fields in [Sil08b, exercise 3.35]. As opposed to the discriminant attached to a Weierstrass equation for E (which depends on the chosen equation, see [Sil08a,

[20] Some authors define, especially in the case of function fields in positive characteristic, $|s| := \exp(-v_x(s))$. This has the effect of changing the height by the multiplicative constant $\log(\#k)$ (see remark 1.3.17 below).

[21] The v_∞-valuation of a rational fraction f/g with $f, g \in k[t]$ and $\gcd(f, g) = 1$ is therefore $\deg(g) - \deg(f) \in \mathbb{Z}$. It is *not* the degree of f/g seen as a rational map $\mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ (which is always non-negative), as done in equation (1.3.1). Note that the place attached to v_∞ is called "place at infinity" even though it is a non-archimedean place (for number fields, "infinite" places generally refer to the archimedean ones).

[22] Some authors define a divisor on C as being a finite $\mathbb{Z}$-linear combination of $\bar{k}$-rational points (which for us would be a divisor on $C \times_k \bar{k}$), in which case our definition of divisor would deserve the name of "k-rational divisor" (i.e., Galois-invariant).

[23] It is important here to take a minimal integral *Weierstrass* model. For instance for any prime $p > 3$, the smooth plane cubic projective curve $XY(X - Y) = pZ^3$ is an elliptic curve over $\mathbb{Q}$, and its reduction mod p is *not* given by $XY(X - Y) = 0$ in $\mathbb{P}^2_{\mathbb{F}_p}$ (this curve has $3p + 1$ $\mathbb{F}_p$-rational points!).

Table 3.1]), the minimal discriminant only depends on the isomorphism class of E over K. In the case of function fields, we see $\Delta_{\min}(E/K)$ as an effective divisor on C.

- Another important invariant is the conductor, defined in [Sil08b, IV.10] and [Sil08b, exercise 3.36]. More specifically, for each non-archimedean place v of a global field K, one can attach a sum of two non-negative integers $f_v(E/K) = \epsilon_v(E/K) + \delta_v(E/K)$ (which is 0 if and only if E has good reduction at v), defined using the Galois action on some ℓ-adic Tate module of E. Here δ_v is called the wild part (or Swan conductor; it is 0 if $\mathrm{char}(k) \geqslant 5$) and $\epsilon_v \in \{0, 1, 2\}$ is the tame part of the conductor. In the case of function fields, we then define the *conductor* as the effective divisor $\mathfrak{f}(E/K) := \sum_{x \in |C|} f_x(E/K) \cdot x$ on C. We denote by $f(E/K)$ its degree.

- We will need to use the *Tamagawa numbers*. Given a non-archimedean place $v \in V_K^0$, we define $c_v(E/K) := [E(K_v) : E(K_v)^0]$, where $E(K_v)^0$ is the set of points $P \in E(K_v)$ such that their reduction $\overline{P} \in \overline{E_v}(\mathbb{F}_v)$ is a non-singular point. See [Sil08b, Corollary IV.9.2] for more details (in particular, for the fact that this index is finite). We have $c_v(E/K) = 1$ at every place v of good reduction for E. Thereby we may define the integer $c(E/K) := \prod_{v \in V_K^0} c_v(E/K)$.

- Finally, an important object measuring the failure of the local-global principle for E-torsors is the *Tate–Shafarevich group*. For each place (archimedean or not), we fix a K-embedding $i_v : K^{\mathrm{sep}} \hookrightarrow K_v^{\mathrm{sep}}$ of the separable closures, where K_v is the completion of K with respect to the absolute value induced by v. This induces a injective[24] morphism between the absolute Galois groups $i_v^* : G_{K_v} := \mathrm{Gal}(K_v^{\mathrm{sep}}/K_v) \hookrightarrow G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$, using "conjugation" by i_v. These are profinite groups, endowed with the Krull topology (in particular they are compact, and in fact G_{K_v} is finite when v is archimedean). In any case, they act continuously on the discrete abelian groups $E(K_v^{\mathrm{sep}})$ and $E(K^{\mathrm{sep}})$ respectively.

  To this data, we can associate the Galois cohomology groups (by taking continuous cocycles and coboundaries) and the restriction maps $\mathrm{res}_v : \mathrm{H}^1(G_K, E(K^{\mathrm{sep}})) \longrightarrow \mathrm{H}^1(G_{K_v}, E(K^{\mathrm{sep}})) \longrightarrow \mathrm{H}^1(G_{K_v}, E(K_v^{\mathrm{sep}}))$, which do not depend[25] on the choice of the embedding i_v. This prompts us to introduce the Tate–Shafarevich group of E over K as:

$$Ш(E/K) := \ker\Big(\mathrm{H}^1(G_K, E(K^{\mathrm{sep}})) \xrightarrow{(\mathrm{res}_v)_{v \in V_K}} \prod_{v \in V_K} \mathrm{H}^1(G_{K_v}, E(K_v^{\mathrm{sep}}))\Big). \qquad \lrcorner$$

Remark 1.3.8. In practice, the conductor, the Tamagawa numbers, the reduction types

[24] It is not difficult to see that i_v^* is well-defined, i.e., $\sigma(i_v(K^{\mathrm{sep}})) \subset i_v(K^{\mathrm{sep}})$ for any $\sigma \in G_{K_v}$. Injectivity of i_v follows from Krasner's lemma, which asserts that the subset $K^{\mathrm{sep}} \subset K_v^{\mathrm{sep}}$ is *dense* (for the topology induced by the unique extension to $\overline{K_v}$ of the absolute value $|\cdot|_v$ on K_v), and the fact that any element $\sigma \in G_{K_v}$ defines a *continuous* bijection of the topological Hausdorff (but not locally compact) field K_v^{sep}, namely it acts by isometries on K_v^{sep}.

[25] Two embeddings i_v, i_v' differ by multiplication by some $g \in G_K$, which imply that $(i_v')^* = g i_v^* g^{-1}$ are conjugate. Note that conjugation by g gives an isomorphism $\phi_g : H := G_{K_v} \xrightarrow{\cong} gHg^{-1}$. Let $A := E(K^{\mathrm{sep}})$ and $c : G_K \to A$ be a 1-cocycle. Then $c' := c|_{gHg^{-1}} \circ \phi_g : H \to A$ is generally not a 1-cocycle, but $g^{-1}c'$ is. An easy computation (using the fact that $c(g^{-1}) = -g^{-1}c(g)$) shows that $g^{-1}c'$ and $c|_H$ are cohomologous, so they are equal as cohomology classes in $H^1(H, A)$.

(good, additive, multiplicative) and other local invariants (e.g., the Kodaira symbols) can be computed using Tate's algorithm described in [Sil08b, IV.9, p. 364–369]. ⌟

Remark 1.3.9 (Elliptic surfaces). Elliptic curves over a function field $k(C)$ are strongly related to elliptic surfaces over C.

- More specifically, given an elliptic curve E over $k(C)$ (where k is any perfect field), there is, up to isomorphism, a unique pair $(\mathscr{E}, \pi : \mathscr{E} \to C)$ consisting of a surface $\mathscr{E}$ over k and of a morphism $\mathscr{E} \to C$, such that:
  - $\mathscr{E}$ is smooth over k, projective and geometrically irreducible,
  - $\pi : \mathscr{E} \to C$ is a surjective morphism with generic fiber $\mathscr{E}_\eta$ isomorphic to E over k.
  - For any pair $(\mathscr{E}', \pi' : \mathscr{E}' \to C)$ satisfying the above two properties, if $f : \mathscr{E} \to \mathscr{E}'$ is a birational morphism such that $\pi' \circ f = \pi$, then f is an isomorphism.

  Its existence and uniqueness are given in [SS19, theorem 5.19], [Ulm11, Lecture 3, Proposition 1.1] or in [SS10, §3.2]. See also [Ulm14a, proposition 2.1.1] (which mentions that $\pi : \mathscr{E} \to C$ is flat, with connected — but not necessarily irreducible or reduced — fibers). In general, $\mathscr{E}$ can be constructed by resolving singularities of a "Weierstrass model" of E.

  We will say that $\mathscr{E}$ (together with the fibration π) is the *elliptic surface associated to* E *over* $k(C)$; it is the minimal regular model of E.

  The *Néron model* $\mathcal{E}$ of E is the smooth locus of $\pi : \mathscr{E} \to C$, i.e., $\mathcal{E} \hookrightarrow \mathscr{E}$ is the open (quasi-projective) subscheme obtained by removing from $\mathscr{E}$ the finite set of points $x \in \mathscr{E}$ that are singular in the fiber $\pi^{-1}(\pi(x))$ (see [Sil08b, theorem IV.6.1]).

  For example, the elliptic surface attached to the elliptic curve $E \hookrightarrow \mathbb{P}^2_k$ given by $X^3 + Y^3 + Z^3 = tXYZ$ is the *smooth*[26] surface $\mathscr{E} \subset \mathbb{P}^2 \times \mathbb{P}^1$ given by (see [SS19, example 5.7], see also the remarks in [Sil08b, p. 200])

  $$\left\{ ([x : y : z], [t_0 : t_1]) \in \mathbb{P}^2 \times \mathbb{P}^1 \ : \ t_0(x^3 + y^3 + z^3) - t_1 xyz = 0 \right\}.$$

  A more delicate example is computed in [Ulm02, §3].

- There is a natural one-to-one correspondence between $k(C)$-rational points of E and sections of $\pi : \mathscr{E} \to C$ defined over k (see [SS19, proposition 5.4] or [Sil08b, proposition III.3.10]) : given a section $\sigma : C \to \mathscr{E}$ of π (i.e., $\pi \circ \sigma = \mathrm{id}_C$), we attach the point $P = \mathscr{E}_\eta \cap \sigma(C)$. Conversely, we will denote by σ_P the unique section corresponding to $P \in E(k(C))$ and we will denote by

  $$(P) := \sigma_P(C) \subset \mathscr{E}$$

  its image. It is a smooth irreducible divisor on $\mathscr{E}$, which is isomorphic to C.

- Almost all the fibers $F_v := \pi^{-1}(v)$ of π (above $v \in |C|$) are elliptic curves. In general, fibers are classified according to their Kodaira symbol (see [Sil08b, table 4.1, p. 365]).

[26] In general, the construction from [Sil08b, p. 200] does not give a smooth surface. For instance, if we consider the projective surface $-Y^2Z^{m-2} + X^3Z^{m-3} + Z^m + T^m = 0$ in $\mathbb{P}^3_k$, then it is singular at all points of the form $[X : Y : 0 : 0]$.

We denote by m_v the number of irreducible components of a fiber F_v over $\overline{k} = \overline{\mathbb{F}_v}$, counted without multiplicity (note that in general we have an equality $m_v \geqslant c_v(E/K)$ which is not always an inequality, compare the 3rd and 4th rows of table 4.1 in [Sil08b, p. 365]). See also [Ulm14a, §2.3] for the notion of multiplicity. We will denote by $\{\,\Theta_{v,i} : 0 \leqslant i \leqslant m_v - 1\,\}$ the set of irreducible components of F_v, where $\Theta_{v,0}$ is the unique irreducible component that intersects the zero section (O).

- We will denote by $\mathrm{Div}(\mathscr{E})$ the free abelian group of divisors (or 1-cycles) on $\mathscr{E}$, generated by closed irreducible curves $C \subset \mathscr{E}$. An element in $\mathrm{Div}(\mathscr{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$ will be called a $\mathbb{Q}$-divisor (this will be used in proposition 1.3.26).
- Given a smooth projective surface S, we will denote by $D \cdot D'$ the intersection product of two divisors $D, D' \in \mathrm{Div}(S)$ (see e.g., [SS19, §4.3]). It induces a symmetric bilinear pairing $\mathrm{Pic}(S) \times \mathrm{Pic}(S) \to \mathbb{Z}$ and actually this descends to a bilinear map $\mathrm{NS}(S) \times \mathrm{NS}(S) \to \mathbb{Z}$ where $\mathrm{NS}(S)$ denotes the Néron–Severi group of S (i.e., the intersection product is invariant under algebraic equivalence and not only linear equivalence).
- Given a smooth projective surface S over a perfect field k, we define the *Euler characteristic* as $\chi(S) := \sum_{i=0}^{2} (-1)^i \dim_k \mathrm{H}^i(S, \mathcal{O}_S)$, using sheaf cohomology (see [SS19, §4.3, p. 63]).

  We define the *topological Euler number* of a proper variety X as follows: we fix a prime $\ell \neq \mathrm{char}(k)$ and set $e(X) := \sum_{i \geqslant 0} (-1)^i \dim_{\mathbb{Q}_\ell} \big(\mathrm{H}^i_{\text{ét}}(X \times_k \overline{k}, \mathbb{Q}_\ell)\big)$ (see [SS19, §4.7, p. 70] and [Dol72, §1] which will be needed in the proof of item 4 of proposition 1.3.26). ⌟

1.3.2 Heights and Mordell–Weil lattices

One of the most important results on the arithmetic of elliptic curves over global fields is the following finiteness statement.

Theorem 1.3.10 (Mordell, Weil, Lang, Néron). *Let E be an elliptic curve over a field K. Then the abelian group $E(K)$ of K-rational points, called the* Mordell–Weil group *of E over K, is finitely generated in the following cases:*

- *K is a global field (i.e., a number field or a global function field),*
- *$K = k(C)$ is a function field of some smooth projective geometrically irreducible curve C over a field k, and E is non-constant.* ⌟

Proof. — For the first item, see [Sil08a, theorem VIII.6.7] or [HS00, Theorem C.0.1] for "modern proofs" over number fields and [Con06, corollary 7.2] or [Kah06, corollaire 3] over global function fields (the latter two references prove Lang–Néron theorem, which asserts in particular that $A(K)$ is finitely generated for any abelian variety A over a field K which is finitely generated over its prime subfield). See [Sil08b, theorem III.6.1] or [Con06, example 2.2, theorem 2.3] for the second item. For a sketch of the proof in the case of global function fields, see remark 1.3.19 below. ■

Definition 1.3.11. 1. Let K be a field as in the above theorem 1.3.10 and E be an elliptic curve over K, so that $E(K) \cong \mathbb{Z}^r \oplus T$ for some unique integer $r \geqslant 0$ and a unique finite abelian group T.

The integer $r = \dim_{\mathbb{Q}}(E(K) \otimes_{\mathbb{Z}} \mathbb{Q})$ is called the *algebraic rank* or *Mordell–Weil rank* of E over K and is denoted $\mathrm{rk}_{\mathbb{Z}}(E(K))$ or $\mathrm{rk}(E(K))$ or $\mathrm{rk}(E/K)$. The subgroup $T \hookrightarrow E(K)$ is the torsion subgroup, which we will denote by $E(K)_{\mathrm{tors}}$.

2. If $K = k(C)$ is any function field and E is a *non-constant* elliptic curve over K, then the *geometric rank* of E is defined as the Mordell–Weil rank of E over $\overline{k}(C)$. ⌟

When K is a global field, an important feature of the Mordell–Weil group $E(K)$ is that it is endowed with a quadratic form $\hat{h} : E(K) \to \mathbb{R}$, which we now describe in the case of global function fields (and it can somehow be used to prove theorem 1.3.10, see remark 1.3.19).

Given a Weierstrass equation for $E \hookrightarrow \mathbb{P}^2_K$ over $K = k(C)$, we have a degree-2 cover map $x : E \to \mathbb{P}^1$ given by the x-coordinate[27]. Moreover, any element $f \in k(C) \smallsetminus \overline{k} = k(C) \smallsetminus k$ determines a unique dominant rational map $C \dashrightarrow \mathbb{P}^1$ over k (see [GW20, corollary 15.22]), which has to be a surjective morphism since C is a normal curve and $\mathbb{P}^1$ is projective (see [GW20, propositions 15.5, 15.16]). Thus, its degree $\deg(f : C \to \mathbb{P}^1)$ is well-defined. We extend this definition to the constants by setting $\deg(a) := 0$ for any $a \in k$. Now, for every $P \in E(k(C)) \smallsetminus \{O_E\}$, we can see the element $x(P) \in \mathbb{P}^1(k(C)) \smallsetminus \{[1:0]\} = \mathbb{A}^1(k(C)) = k(C)$ as a rational map $C \dashrightarrow \mathbb{P}^1$. Following [Sil08b, III.§4], we can therefore define the *naive height* as[28]

$$\begin{array}{rccl} h : & E(K) & \longrightarrow & \mathbb{Z}_{\geqslant 0} \\ & P & \longmapsto & \begin{cases} \deg(x(P)) & \text{if } P \neq O_E \\ 0 & \text{else.} \end{cases} \end{array} \tag{1.3.1}$$

Remark 1.3.12. Note that for instance, when $C = \mathbb{P}^1$ and $x(P) = \frac{a(t)}{b(t)} \in k(t)$ for some coprime polynomials $a, b \in k[t]$, then $\deg(x(P)) = \max\{\deg(a), \deg(b)\}$ (see [Gal12, Lemma 8.1.9]). ⌟

We then define the (canonical) *Néron–Tate height* as

$$\hat{h}(P) := \lim_{n \to +\infty} n^{-2} \cdot h(nP) \in \mathbb{R}_{\geqslant 0} \tag{1.3.2}$$

for every $P \in E(K)$ (see [Sil08b, theorem III.4.3.a), b)] — or [Sil08a, proposition VIII.9.1] over number fields — for the existence of the limit). It is a quadratic form, such that $\hat{h}(P) = 0$ if and only if $P \in E(K)_{\mathrm{tors}}$ (see[29] [Sil08b, theorem III.4.3]). We can associate the $\mathbb{Z}$-bilinear pairing $\langle -, - \rangle_{\mathrm{NT}} : E(K) \times E(K) \to \mathbb{R}$ given by

$$\langle P, Q \rangle_{\mathrm{NT}} := \frac{1}{2} \cdot \left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \right). \tag{1.3.3}$$

[27] For instance if E is given by $Y^2Z = X^3 + aXZ^2 + bZ^3$ then we have a rational map $x : [X : Y : Z] \mapsto [X : Z]$ well-defined on $E \smallsetminus \{O_E\}$. When $X \neq 0 \neq Z$, we have $[X : Z] = [X^3 : ZX^2] = [Y^2Z - aXZ^2 - bZ^3 : ZX^2] = [Y^2 - aXZ - bZ^2 : X^2]$ which defines a rational map $x' : E \dashrightarrow \mathbb{P}^1$. But actually we have $x = x' : E \to \mathbb{P}^1$ as morphisms, so that $x(O_E) = [1 : 0]$.

[28] To be precise, we should denote this height by $h_{E/K,\iota}$ where $\iota : E \hookrightarrow \mathbb{P}^2$ is the embedding given by a Weierstrass equation. Indeed, the naive height is not invariant under base-change: if $K = k(C) \hookrightarrow K' = k(C')$, then an element $x \in K$ gives raise to maps $C \to \mathbb{P}^1$ and $C' \to C \to \mathbb{P}^1$ which may not have the same degree. Here we do not normalize by $1/[k(C) : k(t)]$.

[29] In part d) of [Sil08b, theorem III.4.3], the author assumed that E is not constant over $k(C)$, but here we do not need this assumption. What matters is that for each $B \geqslant 0$, there are only finitely points of height at most B, which is true when k is finite (see the end of remark 1.3.19 for the case $C = \mathbb{P}^1$).

We note that $\hat{h}$ induces a quadratic form on $E(K)/E(K)_{\mathrm{tors}}$ (that we still denote by $\hat{h}$), because we have $\hat{h}(P+T) = \hat{h}(P)$ for all $P \in E(K)$ and $T \in E(K)_{\mathrm{tors}}$; equivalently, we have $\langle P, T\rangle_{\mathrm{NT}} = 0$ for all such points (if $nT = O_E$ for some $n \geqslant 1$ then $n\langle P, T\rangle_{\mathrm{NT}} = \langle P, nT\rangle_{\mathrm{NT}} = \langle P, O_E\rangle_{\mathrm{NT}} = 0$).

It follows (from the equivalence $\hat{h}(P) = 0 \iff P \in E(K)_{\mathrm{tors}}$) that $\hat{h}$ is positive definite on $E(K)/E(K)_{\mathrm{tors}}$. In fact, more is true: $\hat{h}$ is positive-definite on $E(K) \otimes_{\mathbb{Z}} \mathbb{R}$ (see [HS00, Corollary B.5.4.1] or [Sil08a, Lemma VIII.9.5]). Henceforth, we can introduce the following terminology.

Definition 1.3.13. Given an elliptic curve E over a global field K, the *Mordell–Weil lattice* of E over K is the lattice given by the pair $\big(E(K)/E(K)_{\mathrm{tors}}, \hat{h}\big)$. ⌟

The discriminant of the Mordell–Weil lattice of E over K is known as the *regulator*:

Definition 1.3.14. The regulator of an elliptic curve E over a global field K is defined as

$$\mathrm{Reg}(E/K) := \det\Big((\langle P_i, P_j\rangle_{\mathrm{NT}})_{1\leqslant i,j\leqslant r}\Big) \in \mathbb{R}_{>0},$$

where $\{P_1, ..., P_r\}$ is any $\mathbb{Z}$-basis of the free abelian group $E(K)/E(K)_{\mathrm{tors}}$ (in particular[30], we have $\mathrm{Reg}(E/K) = 1$ if the rank is $r = 0$). ⌟

Here is the relation between the naive and the Néron–Tate heights; the following useful result actually characterizes the Néron–Tate height.

Lemma 1.3.15. *Let E be an elliptic curve over a global field K. Then:*

1. *The Néron–Tate and naive heights differ by a bounded function: $\hat{h} - h = O(1)$. In other words, there is a constant $C > 0$ such that for all $P \in E(K)$, we have $|h(P) - \hat{h}(P)| \leqslant C$.*
2. *Moreover, $\hat{h}$ is the unique quadratic form on $E(K)$ that is such that $\hat{h} - h$ is bounded. More precisely, let $d \geqslant 2$ be a given integer, $P \in E(K)$ and $h' : E(K) \to \mathbb{R}$ be a function such that $h'(d^r P) = d^{2r} h'(P)$ for all $r \geqslant 0$ and $h' - h$ is bounded on $\{\, d^r P \;:\; r \geqslant 1\,\}$. Then $h'(P) = \hat{h}(P)$.* ⌟

Proof. — 1. See [Sil08b, theorem III.4.3.b)] when K is a function field (the statement therein has a factor $\frac{1}{2}$, which we do not have; see remark 1.3.17).

2. Let $C' > 0$ be such that $\big|h'(d^r P) - \hat{h}(d^r P)\big| \leqslant C'$ for all $r \geqslant 0$ and set $C'' := \max\{C, C'\} > 0$, where C in as in the first item. Then for all integers $r > 0$ we have

$$\begin{aligned}
|\hat{h}(P) - h'(P)| &= \big|\hat{h}(P) - d^{-2r} h'(d^r P)\big| \\
&\leqslant \big|\hat{h}(P) - d^{-2r} h(d^r P)\big| + \big|d^{-2r} h(d^r P) - d^{-2r} h'(d^r P)\big| \\
&\leqslant 2 \cdot d^{-2r} \cdot C'' \to 0,
\end{aligned}$$

as $r \to +\infty$, which shows that $h'(P) = \hat{h}(P)$ as desired. ■

[30] This is not a "convention". An $r \times r$ real matrix is a map $\{1, ..., r\}^2 \to \mathbb{R}$, so when $r = 0$ there is a unique such matrix (the empty map), and its determinant is a sum over $\mathrm{Bij}(\varnothing) = \{\mathrm{id}\}$ of an empty product, so it equals 1.

Remark 1.3.16. We briefly explain here why $\hat{h} : E(K) \to \mathbb{R}_{\geqslant 0}$ is a quadratic form. It is equivalent to saying that $\hat{h}(O_E) = 0$ and for all $P_1, P_2, P_3 \in E(K)$ we have $\hat{h}(-P_1) = \hat{h}(P_1)$ and

$$\hat{h}(P_1+P_2+P_3) - \hat{h}(P_1+P_2) - \hat{h}(P_1+P_3) - \hat{h}(P_2+P_3) + \hat{h}(P_1) + \hat{h}(P_2) + \hat{h}(P_3) = 0. \tag{1.3.4}$$

Indeed, (1.3.4) corresponds to the $\mathbb{Z}$-bilinearity of $\langle -, - \rangle_{\mathrm{NT}}$, and then using the properties $\hat{h}(O_E) = 0$ and $\hat{h}(-P) = \hat{h}(P)$ for all $P \in E(K)$, one can deduce that $\hat{h}$ is $\mathbb{Z}$-homogeneous of degree 2, i.e., $\hat{h}(nP) = n^2\hat{h}(P)$ for all $n \in \mathbb{Z}$, see [HS00, lemma A.7.2.6] (so in particular — using $n = 2$ — one gets $\hat{h}(P) = \langle P, P \rangle_{\mathrm{NT}}$).

The facts that $\hat{h}(O_E) = 0$ and $\hat{h}$ is even are obvious, while (1.3.4) can be proved "by hand" as in [Sil08a, Theorem VIII.9.3] (or [Mil06, proposition IV.4.9]), but we can argue as in [HS00, Theorem B.5.1] or [Ser89, §3.3, p. 35-36] via more conceptual arguments.

Namely, the theorem of the cube (see [EvdGM, theorems 2.5, 2.7], [Mum12, II.§6, p. 52] or [HS00, A.7.2.1]) implies that for any divisor D on E, the divisor $\sum_{\varnothing \neq I \subset \{1,2,3\}} (-1)^{1+|I|} \pi_I^*(D)$ is a principal divisor on the variety E^3, where $\pi_I : E^3 \to E$ is the morphism $(x_1, x_2, x_3) \mapsto \sum_{i \in I} x_i$. This implies that $\sum_{\varnothing \neq I \subset \{1,2,3\}} (-1)^{1+\#I} h_D \circ \pi_I$ is bounded as a function $E(\overline{K})^3 \to \mathbb{R}$ (see [HS00, theorem B.3.2]), where $h_D : E(\overline{K}) \to \mathbb{R}$ is the height defined (up to a bounded function) in [HS00, Theorem B.3.2]. From there, it readily follows that (1.3.4) holds (i.e., $\sum_{\varnothing \neq I \subset \{1,2,3\}} (-1)^{1+\#I} \hat{h} \circ \pi_I = 0$) by taking the ample basepoint-free divisor $D = 2(O_E)$ (for which $h_D = h$ is the naive height, see [Ser89, §3.5, p. 39-40]: D provides a morphism $E \to \mathbb{P}(L(D)) \cong \mathbb{P}^1$ where $L(D)$ is the Riemann–Roch space of D, of dimension 2) and taking the limit defining $\hat{h}$ as in equation (1.3.2). ⌟

Remark 1.3.17. We point out that the heights are sometimes normalized in a different way. The main properties of the canonical height $\hat{h}$ (quadratic form, positive-definite on the torsion-free part, finiteness of the number of points of bounded height) are preserved under scaling by positive real numbers. However, there is a unique normalization that can make the BSD formula (1.3.13) and theorem 1.3.24 true.

- Some authors define the naive height as $h'(P) := \frac{1}{2}\deg(x(P))$ so their "canonical" height $\hat{h}'$ is half ours, i.e., $\hat{h}' = \frac{1}{2}\hat{h}$ (or for instance in [Sil08b, Theorem III.4.3], the naive height is the same as ours but Silverman defined $\hat{h}'$ with a factor $\frac{1}{2}$ in front). But in general they also define $\langle P, Q \rangle' := \hat{h}'(P+Q) - \hat{h}'(P) - \hat{h}'(Q)$ (as in [Sil08b, Theorem III.4.3.c)] or [Sil08a, VIII.§9]), which is consistent with our definition of $\langle -, - \rangle_{\mathrm{NT}}$.

  For instance, in [Oes90], the height of a point P in a constant elliptic curve E over $k(C)$ is defined as $h'(P) = \deg(\phi_P)$, where $\phi_P : C \to E$ is defined in remark 2.4.1. But then the regulator is defined with respect to the a pairing such that $\langle P, P \rangle = 2h'(P)$, so that it coincides with the one we defined[31].

- In some cases, there is a factor $\log(\#k)$ in the definition of the heights (see also the footnote on page 34). For instance, in [Gro11, Lecture 3, §2], in the case of constant

[31] However, on page 388, we point out that there is a missing factor $|k|^{\frac{1}{12}\deg(\Delta_{\min})}$ in his Birch–Swinnerton-Dyer formula. (This does not affect the rest of his paper since the author is considering constant curves).

curves $E/k(C)$, the author defines $\langle P, P\rangle' = 2\log(\#k)\deg(\phi_P : C \to E) = \log(\#k)h(P)$ (see remark 2.4.1 for the notations). See also remark 1.3.33.3. ⌟

Remark 1.3.18. It is shown in [Sil08b, theorem III.9.3] that when E is an elliptic curve over a global function field $K = k(C)$, the Néron–Tate height takes values in $\mathbb{Q}$, that is, we have a map $\hat{h} : E(K) \to \mathbb{Q}$. (Depending on the normalization mentioned in remark 1.3.17, some authors consider a height with values in $\log(\#k)\cdot\mathbb{Q} \subset \mathbb{R}$; in any case the image is contained in a 1-dimensional $\mathbb{Q}$-vector space). We will actually give soon a stronger statement for a certain sublattice of the Mordell–Weil lattice in theorem 1.3.24. This contrasts with the situation over number fields, where the Néron–Tate height is typically expected to take transcendental values. ⌟

Remark 1.3.19. With the help of the canonical height, we can sketch the proof of theorem 1.3.10 when E is any elliptic curve over $K = k(t)$ and k is finite.

- First, we show that the quotient group $E(K)/mE(K)$ is finite for every integer $m \geqslant 1$ which is coprime to $\mathrm{char}(K)$. For any finite Galois extension K'/K, the map $E(K)/mE(K) \hookrightarrow E(K')/mE(K')$ is injective by [Sil08a, VIII.1.1.1], so we may assume that $E[m] \subset E(K)$, which implies $\mu_m(\overline{K}) \subset K^\times$ by Corollary III.8.1.1 in [Sil08a] and so $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2 \cong \mu_m^2$ as Galois modules. Since the multiplication-by-m map $[m] : E \to E$ is surjective on K^{sep}-rational points (because m is coprime to $\mathrm{char}(K)$, [EvdGM, corollaries 5.10, 5.11] apply), we obtain an injective morphism

$$E(K)/mE(K) \hookrightarrow H^1(G_K, E[m]) \cong (K^\times/K^{\times,m})^2, \tag{1.3.5}$$

  from the long exact sequence in Galois cohomology and Kummer isomorphism. Now, it turns out that the image of the map (1.3.5) lies in $K(S,m)^2$, where

$$K(S,m) := \{f \in K^\times/K^{\times,m} \ : \ v(f) \equiv 0 \pmod m, \forall v \in V_K^0 \smallsetminus S\}$$

  and S is a finite set of valuations on K (see [Sil08b, p. 194] for $m = 2$). Thus we are left with proving that $K(S,m)$ is a finite set, which is just a statement about global fields (not about elliptic curves). In the case of function fields, one needs to use the facts that the m-torsion of the class group of $K = k(C)$ is finite (in general $\mathrm{Cl}(K)[m] \cong \mathrm{Pic}^0(C)[m] \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^{2g}$ where g is the genus of the curve C) and the obvious fact that $\mathcal{O}_K^\times/\mathcal{O}_K^{\times,m}$ is finite, where $\mathcal{O}_K = \mathcal{O}_{K,\varnothing} := k$.

- The second part of the proof involves heights. If $S \subset A := E(K)$ is a finite set of points whose classes modulo m generate $E(K)/mE(K)$, then one can show (see VIII.3.1 in [Sil08a] or C.0.3 in [HS00]) that $E(K)$ is generated by the set

$$S' := \{\, P \in E(K) \ : \ \hat{h}(P) \leqslant \max_{Q\in S} \hat{h}(Q) \,\}.$$

  It remains to check that there are only finitely many points with bounded Néron–Tate height, or equivalently with bounded naive height (by lemma 1.3.15). For every $B > 0$ we have $\{\, P \in E(K) \ : \ h(P) \leqslant B \,\} \subset x^{-1}(\{\, Q \in K \ : \ \deg(Q) \leqslant B \,\})$ where $x : E \to \mathbb{P}^1$ is a degree-2 morphism and $\deg(Q)$ is described in remark 1.3.12. Now, the fibers of x have size at most 2, and it is clear that there are only finitely many rational functions in $k(t)$ of degree $\leqslant B$ (because k is *finite*). From this it follows that the above set S' is finite, as desired. ⌟

We now introduce a sublattice of $\big(E(K)/E(K)_{\mathrm{tors}}, \hat{h}\big)$, which is very convenient because of theorem 1.3.24 stated later, which gives an explicit lower bound on the λ_1 of this sublattice.

Definition 1.3.20. Let E be an elliptic curve over a global field K. We define $E(K)^0 \subset E(K)$ to be the set of all the points $P \in E(K)$ such that for every non-archimedean place v of K, the reduction $\overline{P}$ is a non-singular point on the reduction $\overline{E_v}$ of a minimal integral Weierstrass model E_v of E at v. In other words, we have

$$E(K)^0 := \bigcap_{v \in V_K^0} (E(K) \cap E(K_v)^0),$$

using the notation $E(K_v)^0$ from definition 1.3.7. ⌟

It is known that $E(K)^0 \subset E(K)$ is in fact a subgroup. This follows from the fact that $E(K_v)^0 \subset E(K_v)$ is a subgroup for all $v \in V_K^0$, see the proof of [Sil08a, proposition VII.2.1] (which uses the description of the group law on elliptic curves in terms of intersection of lines with the cubic curve). Alternatively, one can use the fact that $E(K_v)^0 = \mathcal{E}_v^0(\mathcal{O}_{K_v})$ is a subgroup inside $\mathcal{E}_v(\mathcal{O}_{K_v}) \cong E(K_v)$ where $\mathcal{E}_v$ denotes the Néron model of E over K and $\mathcal{E}_v^0$ is the connected component of the neutral element (see [Sil08b, Remark IV.6.1.2, Exercise 4.25, Corollary IV.9.2]). Then we may give the following definition.

Definition 1.3.21. The *narrow Mordell–Weil lattice* of E over K is the free abelian group $E(K)^0/(E(K)^0 \cap E(K)_{\mathrm{tors}})$ endowed with the quadratic form induced by $\hat{h}$. ⌟

Remark 1.3.22. There are alternative definitions of the narrow Mordell–Weil lattice, involving the elliptic surface $\mathscr{E} \to C$ associated to C. See lemma III.9.4 and remark 9.4.1 in [Sil08b] or [SS19, §6.7]. In the latter reference, they define $E(K)^0$ as the set of all points $P \in E(K)$ such that at each closed point $v \in |C|$, the section $(P) \subset \mathscr{E}$ intersects the connected component of the fiber $\mathscr{E}_v$ that meets the identity section (O_E). ⌟

Lemma 1.3.23. *Let E be an elliptic over a global field K. Then the index $\big[E(K) : E(K)^0\big]$ is finite and divides the product $c(E/K) = \prod_{v \in V_K^0} c_v(E/K)$ of the Tamagawa numbers. In particular, the narrow Mordell–Weil lattice is a sublattice of the Mordell–Weil lattice which has the same rank.* ⌟

Proof. — We first observe that there is an exact sequence of abelian groups

$$0 \longrightarrow E(K)^0 \hookrightarrow E(K) \longrightarrow \prod_{v \in V_K^0} E(K_v)/E(K_v)^0.$$

which induces an injective group morphism $E(K)/E(K)^0 \hookrightarrow \prod_{v \in V_K^0} E(K_v)/E(K_v)^0 =: G$. In view of the properties of the Tamagawa numbers mentioned in definition 1.3.7, we know that G is finite of order $c(E/K)$ (recall that for all but finitely many places v, we have $c_v(E/K) = 1$). Thus the index $\big[E(K) : E(K)^0\big]$ is indeed finite and divides $c(E/K)$. ■

Over global *function fields* $K = k(C)$, the important features of the narrow Mordell–Weil lattice are given by following result.

Theorem 1.3.24 (Shioda). *Let E be an elliptic curve over a global function field $K = k(C)$. Then the narrow Mordell–Weil lattice is an even (hence integral) lattice: $\hat{h}(P) \in 2\mathbb{Z}_{\geqslant 0}$ for all $P \in E(K)^0$. Moreover, for every $P \in E(K)^0 \smallsetminus \{0\}$ one has*

$$\hat{h}(P) \geqslant \frac{\deg\left(\Delta_{\min}(E/K)\right)}{6}.$$

In particular, if E has at least one place of bad reduction over K, then $E(K)^0$ is torsion-free, so that $(E(K)^0, \hat{h})$ is a lattice with $\lambda_1(E(K)^0) \geqslant \left(\frac{\deg(\Delta_{\min}(E/K))}{6}\right)^{1/2} > 0$. ⌟

Proof. — See theorem 6.44, as well as theorem 6.24 and §5.12 (especially theorem 5.47 and corollary 5.50), in the book[32] [SS19]. For convenience, a sketch of the proof of Shioda's result is given after proposition 1.3.26 below (in particular, we check that the pairing $\langle -, - \rangle$ defined in [SS19, Theorem 6.20] coincides with the Néron–Tate pairing $\langle -, - \rangle_{\mathrm{NT}}$ defined in equation (1.3.3)).

Note that in [SS19, chapter 6], it is assumed that k is algebraically closed, so the lower bound on $\hat{h}(P)$ in fact holds for any $P \in E(\overline{k}(C))^0 \smallsetminus \{0\}$. The fact that $E(K)^0$ is integral is also proved in [Sil08b, Theorem III.9.5.c)]. ■

Remark 1.3.25. 1. In [SS19], all elliptic surfaces are assumed to have at least one singular fiber (by convention 2.10, *ibid.*), i.e., E has always at least one place of bad reduction over K. If $C = \mathbb{P}^1_k$, it suffices to assume that E is not constant to ensure that $\deg\left(\Delta_{\min}(E/K)\right) > 0$, see [Spr13]. For a general curve C, assuming that an elliptic curve E over $k(C)$ is non-isotrivial is sufficient (any pole of the j-invariant — seen as a rational map $j : C \to \mathbb{P}^1$ — is a place of bad reduction for E).

2. The lower bound from theorem 1.3.24 is not always attained. For instance, in [Elk97], one takes $K = k(t)$ with $k = \mathbb{F}_{2^{12}}$ and $E : y^2 + y = x^3 + t^{33} + a_6$ where $a_6 \in k$ is such that $\mathrm{tr}_{k/\mathbb{F}_2}(a_6) = 1$. Now, it is proved in [Elk97] that $E(K) = E(K)^0$ (on page 3) and that $\lambda_1(E(K))^2 = 8$ (on page 4), while we have $\frac{1}{6}\deg\left(\Delta_{\min}(E/K)\right) = \frac{36}{6} = 6$ (this then gives a Mordell–Weil lattice $E(K)$ homothetic to the Leech lattice). However, in many examples we will treat, the lower bound will be sharp (see proposition 3.2.14).

3. For the full Mordell–Weil lattice $E(K)/E(K)_{\mathrm{tors}}$, see [SS19, Theorems 6.20, 6.24, Table 6.1] for an explicit description of the height pairing. It is not true that the height takes values in the integers (see [SS19, Example 6.26] or the point Q_n in remark 3.2.21), but it always takes values in $\mathbb{Q}$, as mentioned in remark 1.3.18. More specifically, let $\mathscr{E} \to C$ be the elliptic surface attached to $E/K = k(C)$ as in remark 1.3.9, and denote by $(P) \subset \mathscr{E}$ the (image of the) section attached to a rational point $P \in E(K)$. Then [SS19, theorem 6.24] states that

$$\hat{h}(P) = 2\chi(\mathscr{E}) + 2(P) \cdot (O) - \sum_{v \in V_K^0} \gamma_v(P) \tag{1.3.6}$$

where $\gamma_v(P) \in \mathbb{Q}$ are certain rational numbers, such that $\gamma_v(P) = 0$ if v is a place of good reduction or if $P \in E(K)^0$. See [SS19, definition 6.23 and table 6.1, p. 127] for more details. (Furthermore, by proposition 1.3.26 we have $\chi(\mathscr{E}) = \frac{1}{12}\deg\left(\Delta_{\min}(E/K)\right)$).

[32] In convention 2.10 *ibid.*, it is assumed that E has at least a place of bad reduction, but the above lower bound trivially holds without this assumption, for instance when E is a constant curve.

4. Theorem 1.3.24 can be seen as a variation[33] on a conjecture of Lang (over function fields), which asserts that for any global field K, there is constant $c_K > 0$ such that for any non-torsion point P on any elliptic curve E over K, one has

$$\hat{h}(P) \geqslant c_K \cdot \begin{cases} \log\left(\mathrm{N}_{K/\mathbb{Q}}(\Delta_{\min}(E/K))\right) & \text{if } K \text{ is a number field,} \\ \deg\left(\Delta_{\min}(E/K)\right) & \text{if } K \text{ is a function field.} \end{cases}$$

   See for instance [HS88], [GS95b, theorem 7, p. 79][34] or the proof of [HP16, proposition 7.6, p. 80] for some results towards this.

   For an upper bound on $\lambda_1(E(K))$ over number fields, see [Sil08a, Conjecture VIII.10.2]. ⌟

To finish this subsection, we explain some steps towards a proof of theorem 1.3.24. Here is a quick overview that summarizes the key ingredients, where we use the notations from remark 1.3.9.

1. First, the Néron–Tate height is expressed in terms of an intersection product: $\hat{h}(P) = -D_P \cdot D_P$, where D_P is a certain $\mathbb{Q}$-divisor on the elliptic surface $\mathscr{E} \to C$ attached to E, involving the section (P) as well as other prime divisors, with the Euler characteristic $\chi(\mathscr{E}) \in \mathbb{Z}$ appearing in some coefficient. In particular, the canonical height takes values in $\mathbb{Q}$.

2. The canonical bundle formula and adjunction formula will imply the following identity for the self-intersection product of a section of a point $P \in E(K)$: $(P) \cdot (P) = -\chi(\mathscr{E})$. Using the first step, it will give us the lower bound $\hat{h}(P) \geqslant 2\chi(\mathscr{E})$ for every $P \in E(K)^0 \smallsetminus \{0\}$.

3. Finally, there is an identity $\chi(\mathscr{E}) = \dfrac{1}{12}\deg(\Delta_{\min})$. Together with the step 2 above, this allows to conclude the proof of theorem 1.3.24.

We now make these steps a bit more detailed, by stating the following results (and using notations from remark 1.3.9).

Proposition 1.3.26. *Let E be an elliptic curve over a global function field $k(C)$ as in definition 1.3.2.*

1. *Assume that E is given by $y^2 = x^3 + Ax + B$ and let $P \in E(K)$ be such that $2P \neq O$ and $x(P), y(P)$ have no poles in common with A and B. Then*

$$(P) \cdot (O) = \frac{1}{2}h(P).$$

2. *There exists a map $E(K) \to \mathrm{Div}(\mathscr{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$ denoted $P \mapsto \Gamma_P$ such that*

   (a) *The set $\{\, ((P) - (O)) \cdot \Gamma_P \;:\; P \in E(K) \,\} \subset \mathbb{Q}$ is finite.*

   (b) *If $P \in E(K)^0 \smallsetminus \{O\}$ then $((P) - (O)) \cdot \Gamma_P = 0$.*

[33] The point is that Shioda's lower bound is valid for $E(K)^0$, not for the full Mordell–Weil lattice, where bad places will play a role (see e.g. [SS19, Table 6.1] for the local contributions to the height at places of bad reduction).

[34] As pointed out in [HP16, remark 1.18], an hypothesis of separability of the j-invariant is omitted from the original statement, but is used in the proof.

(c) *If we let* $D_P := (P) - (O) + \Gamma_P$, *then the self-intersection product of* D_P *satisfies* $-D_P \cdot D_P = 2(P)\cdot(O) - (P)^2 - (O)^2 + ((P)-(O))\cdot\Gamma_P$.

(d) *The assignement* $(P,Q) \mapsto -D_P \cdot D_Q$ *is bilinear on* $E(K)\times E(K)$.

3. *For all* $P \in E(K)$, *the self-intersection of the section* (P) *equals* $(P)\cdot(P) = -\chi(\mathscr{E})$ *(in particular, it does not depend on* P*).*

4. *We have* $\chi(\mathscr{E}) = \frac{1}{12}e(\mathscr{E})$ *and* $e(\mathscr{E}) = \deg(\Delta_{\min}(E/K))$. *(In particular,* $\deg(\Delta_{\min}(E/K))$ *is an integral multiple of 12).* ⌟

Before explaining how the proof of the above proposition 1.3.26 goes, we use it to deduce Shioda's lower bound on $\lambda_1(E(K)^0)$.

Sketch of the proof of theorem 1.3.24. — • We first check that $\hat{h}(P) = -D_P \cdot D_P$ for all $P \in E(K)$, where D_P is as in item 2c above (we fix a choice of Γ_P). From items 2c and 3 we have

$$\begin{aligned} -D_P \cdot D_P &= 2\chi(\mathscr{E}) + 2(P)\cdot(O) + ((P)-(O))\cdot\Gamma_P \\ &= 2(P)\cdot(O) + \mathcal{O}(1) && \text{by item 2a} \\ &= h(P) + \mathcal{O}(1) && \text{by item 1.} \end{aligned}$$

Thus, using the bilinearity of $(P,Q) \mapsto -D_P \cdot D_Q$ stated in item 2d, we see that lemma 1.3.15 allows us to conclude that $\hat{h}(P) = -D_P \cdot D_P$. In particular, $\hat{h}(P) \in \mathbb{Q}$ for all $P \in E(K)$.

• Now, if $P \in E(K)^0 \smallsetminus \{O\}$ we have

$$\begin{aligned} \hat{h}(P) = -D_P \cdot D_P &= 2\chi(\mathscr{E}) + 2(P)\cdot(O) && \text{by item 2b} \\ &\geqslant 2\chi(\mathscr{E}) \\ &= \frac{\deg(\Delta_{\min}(E/K))}{6} && \text{by item 4} \end{aligned} \tag{1.3.7}$$

where we used the fact that if $P \neq O$, then the sections (P) and (O) are distinct irreducible curves on $\mathscr{E}$, so their intersection product is non-negative. Hence we get the desired lower bound. ■

Proof of proposition 1.3.26. — 1. See [Sil08b, proof of theorem III.9.3, p. 250] (it is assumed that k is algebraically closed of characteristic 0, but the proof of this part does not rely on these hypothesis). This is shown by writing $(P)\cdot(O)$ as a sum of local intersection numbers, and relating each of them to the valuation of $x(P)$ at the corresponding place. (Note that [Sil08b, theorem III.9.3] has a factor $\frac{1}{2}$ in the last part of the statement; see remark 1.3.17 above).

2. The map $P \mapsto \Gamma_P$ is not unique; one definition is given in [Sil08b, p. 247] using [Sil08b, proposition III.8.3], another one is given in [SS19, lemma 6.16]. In both cases, the properties stated in proposition 1.3.26, item 2 hold: see [Sil08b, proof of theorem III.9.3, p. 248-249].

Namely, we can take Γ_P as the $\mathbb{Q}$-divisor given by

$$\Gamma_P := -((P)\cdot(O) + \chi(\mathscr{E}))E \; + \sum_{v\in|C|} \overrightarrow{\Theta_v}\cdot(-A_v^{-1})\cdot\overrightarrow{J_{P,v}} \;\in\; \mathrm{Div}(\mathscr{E})\otimes_{\mathbb{Z}}\mathbb{Q},$$

where, using the notations from remark 1.3.9, $\overrightarrow{\Theta_v} := (\Theta_{v,1} \cdots \Theta_{v,m_v-1})$ is a vector of irreducible divisors on $\mathscr{E}$, $\overrightarrow{J_{P,v}} := {}^{\mathrm{t}}((P) \cdot \Theta_{v,i})_{1 \leqslant i \leqslant m_v-1}$ is a column-vector with integral entries given by intersection products, and the Gram matrix A_v is defined via $(A_v)_{i,j} = \Theta_{v,i} \cdot \Theta_{v,j}$.

3. This is [SS19, Corollary 5.45]. The proof relies on the adjunction formula (which allows to compute the self-intersection product in terms of the canonical divisor class $K_{\mathscr{E}}$ of the elliptic surface $\mathscr{E}$, see [SS19, Theorem 4.11]) and on the canonical bundle formula of Kodaira (which tells us more precisely what is $K_{\mathscr{E}}$, see [SS19, Theorem 5.44]) — the latter being specific to *elliptic* surfaces.

4. The first identity is proved as [SS19, Corollary 5.50]; it relies on Noether's formula (Riemann–Roch theorem for surfaces).

   The second identity is given in [SS19, §5.12]. It is convenient to assume that k is algebraically closed, so that all places $v \in |C|$ have degree 1. First, one can relate[35] the Euler number of a fiber F_v of $\pi : \mathscr{E} \to C$ above $v \in |C|$ to its number of components m_v. Then a result of Dolgachev [Dol72] (based on work of Grothendieck) states that

   $$e(\mathscr{E}) = \sum_{v \in |C|} (e(F_v) + \delta_v), \tag{1.3.8}$$

   where δ_v is the wild ramification part of the local conductor (as defined in [Sil08b, IV.10, p. 380]; we have $\delta_v = 0$ unless $\mathrm{char}(k) \in \{2, 3\}$). Finally, using Ogg's formula (see [Sil08b, theorem IV.§11]), one can prove that $e(F_v) + \delta_v = v(\Delta)$ for all places $v \in V_K^0$, by doing a case-by-case analysis depending on whether v is a place of good, additive or multiplicative reduction. All in all, this allows to conclude that $e(\mathscr{E}) = \deg(\Delta_{\min}(E/K))$. ■

1.3.3 L-functions, ranks and Birch–Swinnerton-Dyer conjecture

An important tool to study some arithmetic invariants of an elliptic curve E over a global field K is to look at its *L-function* $L(E/K, s)$, whose special value at $s = 1$ contains a lot of information, as the rank, at least conjecturally. We now recall how the L-function is defined. In the sequel we assume that $K = k(C)$ is a global function field as in definition 1.3.2.

Definition 1.3.27. Let E be an elliptic curve over $K = k(C)$ and let $k_n \subset \overline{k}$ be the extension of degree n over k.

1. For every place $v \in V_K^0$, define the integers

   $$\begin{aligned} A_E(v, j) &:= |k|^j + 1 - \left|\overline{E_v}(k_j)\right|, \\ a_v(E) &:= A_E(v, \deg(v)) = |\mathbb{F}_v| + 1 - \left|\overline{E_v}(\mathbb{F}_v)\right|, \end{aligned} \tag{1.3.9}$$

   where $j \geqslant 1$ is any integer multiple of $\deg(v) := [\mathbb{F}_v : k]$ (so in particular k_j is an extension of $\mathbb{F}_v$).

[35] For instance, if the fiber F_v is multiplicative with Kodaira type I_n, where $n \geqslant 2$, then $e(F_v) = m_v$, since F_v is given by "gluing" n copies of $\mathbb{P}^1$ (see [Sil08b, theorem IV.8.2, p. 353]), so

$$e(I_n) = e\Big(\bigsqcup_{i=1}^{n} \mathbb{P}^1\Big) - \underbrace{n}_{n \text{ gluings}} = n \cdot e(\mathbb{P}^1) - n = 2n - n = n = |\pi_0(F_v)|.$$

2. We define the *local factor* at v as

$$L_v(E/K,T) := \begin{cases} 1 - a_v(E)T^{\deg(v)} + |k|^{\deg(v)}T^{2\deg(v)} & \text{if } E \text{ has good reduction at } v \\ 1 - a_v(E)T^{\deg(v)} & \text{else.} \end{cases}$$

3. The L-function of E over K is defined as[36]

$$L(E/K,T) := \prod_{v \in V_K^0} L_v(E/K,T)^{-1} \in \mathbb{Z}[\![T]\!].$$ ⌟

Remark 1.3.28. 1. We explain how $a_v(E)$ behaves when v is a place of bad reduction for E. Namely, $a_v(E)$ is equal 0 if E has additive reduction at v, and ± 1 if E has multiplicative reduction at v, the sign depending on whether the reduction is split or non-split multiplicative (this follows from proposition III.2.5 in [Sil08a], see also section 2.10 in [Was08]); see also footnote 23 on page 34.

2. Over number fields, the L-function is rather defined as a function of a complex variable $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 3/2$ by taking the product of $L_v(E/K, \mathrm{N}(\mathfrak{p})^{-s})^{-1}$ over all primes $v = \mathfrak{p} \in V_K^0$. So it is not defined as a formal Laurent series in some variable T. ⌟

One can re-write the L-function as follows, by an elementary computation. This will be very useful in the sequel.

Proposition 1.3.29. *Let E be an elliptic curve over a global function field $K = k(C)$. Then we have, using the notations from definition 1.3.27:*

$$\log L(E/K,T) = \sum_{j \geqslant 1} \left(\sum_{x \in C(k_j)} A_E(v_x, j) \right) \frac{T^j}{j}.$$

where v_x is the place corresponding to the closed point attached to the rational point x (i.e., its Galois orbit under $\mathrm{Gal}(\overline{k}/k)$) and $k_j \subset \overline{k}$ is the extension of degree j of k. ⌟

Proof. — This is [Gri16, Lemme 1.3.15], which is stated only for $C = \mathbb{P}^1$, but the proof immediately generalizes. ■

In fact, we can say more about the L-function.

Theorem 1.3.30 (Grothendieck, Deligne, Raynaud). *Let E be an elliptic curve over over a global function field $K = k(C)$ and let $g_C \geqslant 0$ be the genus of C. Then:*

- *The L-function $L(E/K,T)$ is a rational function of T, i.e., $L(E/K,T) \in \mathbb{Q}(T)$. Its degree[37] is $D(E/K) := f(E/K) + 2 \cdot (2g_C - 2)$.*
- *For any root α of $L(E/K,T)$ and any complex embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, the complex modulus of $\iota(\alpha)$ is $|\iota(\alpha)| = (\#k)^{-1}$.*

[36] We explain what this infinite product of rational fractions means (see also [Lor96, VIII.§4]). By taking the Taylor expansion at $T = 0$, one can see that $L_v(E/K,T)^{-1} \in \mathbb{Z}[\![T^{\deg(v)}]\!]$ (the coefficients are integers since $L_v(E/K,0) = 1$). Then the product over $v \in V_K^0$ makes sense (as a power series) because for all $n \geqslant 1$, there are only finitely many places v of degree n.

[37] Here we take $\deg = -v_\infty$, where v_∞ is the valuation described in example 1.3.6.

- *We have a functional equation*

$$L(E/K, |k|^{-2}T^{-1}) = \epsilon \cdot (|k|T)^{-D(E/K)} \cdot L(E/K, T), \tag{1.3.10}$$

  for some $\epsilon \in \{\pm 1\}$*, where* $D(E/K)$ *is as in the first item.*

- *If moreover* E *is non-constant, then* $L(E/K, T) \in \mathbb{Z}[T]$ *is a polynomial with constant term 1.* ⌟

Proof. — See [Gro11, theorem 2.6 and appendix D (for $\mathrm{char}(k) \geqslant 5$)] and [Ulm11, Lecture 1, Theorem 9.3 and Lecture 4, §1 (Theorems 1.3.3, 1.4.1) and §2][38] for modern expositions, including the case of more general Galois representations (e.g., arising from abelian varieties).

The last item is proved by constructing, for any fixed prime $\ell \neq \mathrm{char}(k)$, a certain finite-dimensional $\mathbb{Q}_\ell[G_k]$-module $V(E/K)$, where $G_k := \mathrm{Gal}(\overline{k}/k)$ (coming from the first étale cohomology group of some lisse ℓ-adic sheaf on $C \times_k \overline{k}$) such that $L(E/K, T) = \det[\mathrm{id} - T\mathrm{Fr}_k \curvearrowright V(E/K)] \in \mathbb{Q}_\ell[T]$ is the "reciprocal" characteristic polynomial of the Frobenius $\mathrm{Fr}_k : x \mapsto x^{|k|}$ acting on $V(E/K)$. See [Ulm11, lecture 4, theorem 1.3.3] for more details. ■

Remark 1.3.31. 1. In particular, theorem 1.3.30 allows us to speak of the order of vanishing of the L-function at any[39] given value of T in $\mathbb{C}$.

2. It is not too difficult to show that the L-function is a rational function, by relating it to the zeta functions of the elliptic surface $\mathscr{E}$ attached to E (as in remark 1.3.9) and of the curve C. The details are given in [Ulm11, Lecture 3, §6] and [Shi92b, lemma 5, p. 105]. But this approach does not explain why the L-function is a polynomial when E is non-constant; this fact requires étale cohomology to be proved.

3. If $E \cong E_0 \times_k k(C)$ is constant, then the L-function can be expressed in terms over the zeta function of C over k as

$$L(E/K, T) = Z\Big(C/k, \beta_1 T\Big) Z\Big(C/k, \beta_2 T\Big) = Z\Big(C/k, \frac{|k|T}{\beta_1}\Big) Z\Big(C/k, \frac{|k|T}{\beta_2}\Big) \tag{1.3.11}$$

   where $\beta_1, \beta_2 \in \overline{\mathbb{Q}}$ are such that the numerator of the zeta function $Z(E_0/k, T)$ of E_0 over k is $(1 - \beta_1 T)(1 - \beta_2 T)$ (see [Oes90, §3.2, p. 391] and [Gro11, equation (D.3)]; recall that $\beta_1\beta_2 = |k|$). We see that, as a ratio of two coprime polynomials of degree $4g$ and 4 respectively, the L-function has degree $4g - 4$ as expected. ⌟

We now recall what the Birch–Swinnerton-Dyer (BSD) conjecture is, and what is known about it. Originally, it was stated for elliptic curves over $\mathbb{Q}$, but it was then generalized to abelian varieties over any global field. We first introduce the following notations.

Definition 1.3.32. Let E be an elliptic curve over a global function field K.

1. The (exponential differential) *height* of E/K is $H(E/K) := |k|^{\frac{\deg(\Delta_{\min}(E/K))}{12}}$.

[38] Note that the equation (1.3.1) *loc. cit.* has some typographic misprints; it should read $L(\rho, T) = \prod_v \det(1 - T^{\deg(v)}\mathrm{Fr}_v \mid V^{I_v})^{-1}$.

[39] Except possibly if $E \cong E_0 \times_k K$ is constant, in which case $T \in \{(|k| \cdot \beta_1)^{-1}, (|k| \cdot \beta_2)^{-1}, \beta_1^{-1}, \beta_2^{-1}\}$ are the 4 poles of $L(E/K, T)$, where $\beta_1^{-1}, \beta_2^{-1}$ are the 2 roots of the (numerator of the) zeta function of E_0 over k (see equation (1.3.11)).

2. The *analytic rank* $\rho(E/K)$ of E over K is the order of vanishing of $L(E/K,T)$ at $T=|k|^{-1}$, that is, $\rho(E/K) := \operatorname{ord}_{T=|k|^{-1}} L(E/K,T)$.

3. The *special value* of the L-function of E/K is the non-zero rational number

$$L^*(E/K) \;:=\; \frac{1}{\rho!}L^{(\rho)}(E/K,T)\Big|_{T=|k|^{-1}}$$

where $\rho=\rho(E/K)$ and $L^{(\rho)}$ denotes the derivative of order ρ of the L-function. ⌟

Remark 1.3.33. 1. Because the L-function is a rational function in $\mathbb{Q}(T)$ by theorem 1.3.30, we also have $L^*(E/K) = \dfrac{L(E/K,T)}{(1-|k|T)^\rho}\Big|_{T=|k|^{-1}}$ and this is a non-zero rational number.

2. From theorem 1.3.30 and equation (1.3.11) we deduce an upper bound on the analytic rank:

$$\rho(E/K) \leqslant \begin{cases} 4g_C & \text{if } E \text{ is constant} \\ f(E/K)+4g_C-4 & \text{else.} \end{cases} \tag{1.3.12}$$

   We will see in theorem 1.3.35 that $\operatorname{rk} E(K) \leqslant \rho(E/K)$ always holds, so this also gives an upper bound on the algebraic rank. When E is non-constant, this is actually a bound on the geometric rank of E over $\overline{k}(C)$ (see definition 1.3.11), since the *degree* of the conductor does not change under algebraic extensions of the field of constants.

3. We can consider the following complex-analytic version of the L-function: theorem 1.3.30 allows us to define

$$\mathcal{L}(E/K,s) := L(E/K,|k|^{-s})$$

   for any $s\in\mathbb{C}$ (we may get finitely many poles if E is constant, see footnote 39 on page 48). Since $1-|k|^{1-s}\sim \log(|k|)\cdot(s-1)$ as $s\to 1$, the leading term $\mathcal{L}^*(E/K)$ in the Taylor expansion of $\mathcal{L}(E/K,s)$ around $s=1$ (that is, $\mathcal{L}(E/K,s)\sim\mathcal{L}^*(E/K)\cdot(s-1)^\rho$) satisfies $\mathcal{L}^*(E/K)=\log(|k|)^\rho L^*(E/K)$.

   This is related to remark 1.3.17: if one uses the normalization $\hat{h}' := \log(|k|)\cdot\hat{h}$ of the Néron–Tate height then one uses the special value $\mathcal{L}^*(E/K)$ instead of $L^*(E/K)$ in the BSD formula given below, because the corresponding regulator is $\operatorname{Reg}'(E/K) := \log(|k|)^r \operatorname{Reg}(E/K)$ where $r:=\operatorname{rk}E(K)$.

4. We have $L^*(E/K)\in\mathbb{Q}_{>0}$ (see [Gri16, remarque 1.3.13]) and $\rho(E/K)\in\mathbb{Z}_{\geqslant 0}$ (this is clear if E is not constant since $L(E/K,T)$ is a polynomial in that case, and if E is constant then one can use equations (1.3.11) and (2.4.5) and the Riemann hypothesis for curves over finite fields). ⌟

The analytic rank of E/K, as the name suggests, is conjecturally related to the (algebraic) rank of the Mordell–Weil group $E(K)$ introduced in definition 1.3.11: in fact we expect them to be equal, and the special value $L^*(E/K)$ to be related to many arithmetic invariants of the elliptic curve. Here is the precise formulation of the conjecture, as given in[40] [Gro11, lecture 2, conjecture 2.10] (which includes the case of elliptic curves over number fields) or [HP16, conjecture 2.2] for abelian varieties over function fields (see also subsection 2.4.2).

[40] Beware that both of these references normalize the Néron–Tate height so that it takes values in $\mathbb{Q}\cdot\log(\#k)$, see also remarks 1.3.17 and 1.3.33.

Conjecture 1.3.34 (Birch, Swinnerton-Dyer). Let E be an elliptic curve over a global function field $K = k(C)$ as in definition 1.3.2. Let g_C be the genus of C. Then the following statements hold:

a) The algebraic rank of E over K is equal to the analytic rank of E over K. In other words, the rank of the finitely generated abelian group $E(K)$ is equal to the order of vanishing of the L-function of E/K at $T = |k|^{-1}$, i.e.,

$$\mathrm{rk}_{\mathbb{Z}}\big(E(K)\big) = \operatorname*{ord}_{T=|k|^{-1}} L(E/K, T).$$

b) The Tate–Shafarevich group $Ш(E/K)$ is finite and we have the following identity, called the BSD formula (using notations from definitions 1.3.7 and 1.3.32):

$$L^*(E/K) \;=\; \frac{|Ш(E/K)| \cdot \mathrm{Reg}(E/K) \cdot c(E/K)}{|E(K)_{\mathrm{tors}}|^2 \cdot |k|^{g_C - 1} \cdot H(E/K)}. \tag{1.3.13}$$

⌟

While this conjecture remains widely open, many cases are known, for instance:

- The case where the elliptic curve E is isotrivial (see definition 1.3.3 and theorem 1.3.35).
- The case where E has a Weierstrass equation given by a sum of 4 monomials (see theorem 1.3.40).

See also the works [Ber08, theorem 2.3] and [PU16, Corollary 3.1.4] for other proved cases of conjecture 1.3.34. Let us also mention that one finds in [Gro11, lecture 2, §5] an explicit example where the BSD conjecture is verified.

The first important result towards the BSD conjecture can be stated as follows.

Theorem 1.3.35 (Artin, Tate, Milne). *Let E be an elliptic curve over a global function field $K = k(C)$. Then:*

1. *The statements a) and b) in conjecture 1.3.34 are equivalent.*
2. *We always have the inequality $\mathrm{rk}(E(K)) \leqslant \rho(E/K) := \mathrm{ord}_{T=|k|^{-1}} L(E/K, T)$. (In particular, conjecture 1.3.34 is true if the analytic rank of E over K is 0).*
3. *Assume that E is isotrivial. Then both statements of conjecture 1.3.34 are true.* ⌟

Proof. — The first part is proved in [Mil75, theorem 8.1] (which assumes $\mathrm{char}(k)$ to be odd, but using the work [Ill79] one can drop this condition), see also [Tat66b, KT03, Sch82] and [Gro11, theorem 3.1].

The second statement is originally proved in [Tat66b, proof of theorem 5.2, p. 436-437], see also [Ulm11, lecture 3, theorem 8.1].

The third claim is proved in [Ulm11, lecture 3, §8] (see also [Mil68, theorem 3, p. 100] for constant abelian varieties). Most of these results use the relation between conjecture 1.3.34 and Tate's conjecture for the elliptic surface $\mathscr{E}$. ■

Another important class of elliptic curves over $k(t)$ for which the BSD conjecture 1.3.34 is known is described as follows. Following the terminology of [SS19, §13.2.1.2] for surfaces named after Jean Delsarte, we introduce the following notion.

Definition 1.3.36. Let $K = k(t)$ be the function field of $\mathbb{P}^1_k$, where k is any field. A *Delsarte elliptic curve* is an elliptic curve over K which is birational to the affine plane curve given by $g(X, Y) = 0$ where

$$g = \sum_{i=1}^{4} c_i t^{e_{i1}} X^{e_{i2}} Y^{e_{i3}} \in k[t][X, Y] \subset K[X, Y]$$

is a sum of exactly 4 monomials in t, X, Y (i.e., $c_i \in k^\times$ for every i) such that the following conditions are fulfilled:

- We let $M := \max_{1 \leqslant i \leqslant 4} \sum_{j=1}^{3} e_{ij}$ and define $e_{i4} := M - \sum_{j=1}^{3} e_{ij} \geqslant 0$ for each $i \in \{1, ..., 4\}$. Then we require that for any j, there is some i such that $e_{ij} = 0$.
- We consider the 4×4 integer matrix $A := (e_{ij})_{1 \leqslant i,j \leqslant 4}$. Then we require the image of $\det(A)$ in k to be non-zero (when $\mathrm{char}(k) = p > 0$, this means $\det(A) \not\equiv 0 \pmod{p}$). ⌟

Remark 1.3.37. We use this definition to match with [Shi86, SS19], but any g as above satisfies "Shioda's 4-monomial condition" in the terminology of [Ulm11, lecture 3, exercise 10.1]. ⌟

Example 1.3.38. For instance, for any prime $p \geqslant 5$ and any integer $m > 0$ coprime to p, the elliptic curves with (affine) Weierstrass equation

$$y^2 + xy = x^3 + t^m, \qquad y^2 = x^3 + x + t^m, \qquad y^2 = x^3 + 1 + t^m$$

over $\mathbb{F}_p(t)$ are of Delsarte type, because the associated matrices A are respectively

$$A = \begin{pmatrix} 0 & 0 & 2 & m-2 \\ 0 & 1 & 1 & m-2 \\ 0 & 3 & 0 & m-3 \\ m & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 2 & m-2 \\ 0 & 3 & 0 & m-3 \\ 0 & 1 & 0 & m-1 \\ m & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 2 & m-2 \\ 0 & 3 & 0 & m-3 \\ 0 & 0 & 0 & m \\ m & 0 & 0 & 0 \end{pmatrix}$$

and have determinant $-m^2, 4m^2, 6m^2$ respectively. Delsarte elliptic curves have been classified in [Hei11, Hei12]: there are 42 families of them. ⌟

Remark 1.3.39. We explain that the $\overline{k}(t)$-isomorphism class of a Delsarte elliptic curve E "essentially" does not depend on the coefficients $c_1, ..., c_4$.

- More precisely, assume that $E \hookrightarrow \mathbb{P}^2_K$ is given as a plane projective curve $E : \tilde{g}(X, Y, Z) = \sum_{i=1}^{4} c_i t^{e_{i1}} X^{e_{i2}} Y^{e_{i3}} Z^{e_{i4}} = 0$, using the notations from definition 1.3.36 which ensures that $\tilde{g}$ is a homogenous polynomial in $K[X, Y, Z]$ (which has degree $\leqslant 4$ because E is assumed to be an elliptic curve). Let $E_1 : \sum_{i=1}^{4} t^{e_{i1}} X^{e_{i2}} Y^{e_{i3}} Z^{e_{i4}} = 0$. Then we claim that there is a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E_1 \\ \downarrow & & \downarrow \\ \mathrm{Spec}(\overline{k}(t)) & \xrightarrow{\psi} & \mathrm{Spec}(\overline{k}(t)) \end{array}$$

where $\phi : E \to E_1$ is an isomorphism and ψ is induced by an automorphism of $\overline{k}(t)$ of the form $t \mapsto \lambda_1 t$ for some $\lambda_1 \in \overline{k}$.

First, the assumption $\det(A) \not\equiv 0 \bmod p$ certainly implies $\det(A) \neq 0$ so that $A \in \mathrm{GL}_4(\mathbb{Q})$. Write $A^{-1} = \det(A)^{-1}A'$ for some integral matrix $A' = (a'_{ij}) \in M_{4\times 4}(\mathbb{Z})$. Then we can find $\lambda_1, ..., \lambda_4 \in \overline{k}^\times$ such that

$$\forall i \in \{1, ..., 4\}, \qquad \lambda_1^{e_{i1}}\lambda_2^{e_{i2}}\lambda_3^{e_{i3}}\lambda_4^{e_{i4}} = c_i^{-1}.$$

Namely, let $c'_i \in \overline{k}$ be such that $c_i'^{\det(A)} = c_i^{-1}$ and let $\lambda_j = \prod_{r=1}^4 c_r'^{a'_{jr}}$; this implies

$$\prod_{j=1}^4 \lambda_j^{e_{ij}} = \prod_{r=1}^4 c_r'^{\sum_{j=1}^4 e_{ij}a'_{jr}} = c_i'^{\det(A)} = c_i^{-1}.$$

Now, the change of variables $(t, X, Y, Z) \mapsto (\lambda_1 t, \lambda_2 X, \lambda_3 Y, \lambda_4 Z)$ shows that E is isomorphic to E_1 over $\overline{k}(t)$ as desired.

- We point out however that E and E_1 do not need to be isomorphic over $\overline{k(t)}$ if we do not allow any automorphism of $\overline{k}(t)$: for instance take $k = \mathbb{F}_5$, then $E_1 : y^2 = x^3 + x + t$ has j-invariant $j(t) = \frac{1}{t^2+2}$ while $E : y^2 = x^3 + x + 2t$ has j-invariant $\frac{-1}{t^2+3} = j(2t) \neq j(t)$.

  Nevertheless, the algebraic rank and the L-function of E and E_1 over $k'(t)$ are equal, where $k' = k(\lambda_1, \lambda_2, \lambda_3, \lambda_4) \subset \overline{k}$ and λ_i are as above. In particular, the geometric rank of E and E_1 are equal (if they are non-constant). ⌟

Theorem 1.3.40 (Shioda). *Let E be a Delsarte elliptic curve over $k(t)$. The Birch–Swinnerton-Dyer conjecture 1.3.34 is true.* ⌟

Proof. — See [Ulm11, lecture 1, theorem 12.4 and lecture 3, §10] or [Ulm07b, theorem 6.2] for a more general statement about jacobians. The strategy is to show that the associated elliptic surface $\mathscr{E}$ (as in remark 1.3.9) is dominated by a Fermat surface (via a morphism that can be explicitly defined, see [Shi86, p. 421]), and then to apply Tate's conjecture which is known for Fermat surfaces (because they are dominated by a product of Fermat curves). ■

We also recall the following well-known facts.

Proposition 1.3.41. *Let E, E' be two elliptic curves over a global function field K.*

1. *If E' is isogenous to E over K, then they have the same L-function, i.e., $L(E/K, T) = L(E'/K, T) \in \mathbb{Q}(T)$. In particular, they have the same analytic rank.*
2. *If $L_v(E/K, T) = L_v(E'/K, T)$ for all places $v \in V_K^0$ then E and E' are isogenous over K.*
3. *The algebraic rank is also invariant under isogenies: if E' is isogenous to E over K, then $\mathrm{rk}\, E(K) = \mathrm{rk}\, E'(K)$.* ⌟

Proof. — 1. One method is to see that an isogeny $f : E \to E'$ induces, for any prime $\ell \nmid \mathrm{char}(k) \cdot \deg(f)$, an isomorphism of $\mathbb{Z}_\ell[G_K]$-modules $T_\ell(E) \cong T_\ell(E') := \varprojlim_n E'[\ell^n]$ between the ℓ-adic Tate modules. But the L-function of E is entirely determined by

$T_\ell(E)$, so that isogenous curves must have equal L-functions, as explained in [Gro11, lecture 2, p. 13 and appendix C]. See also [Dok13, §3, p. 218-219] (in the case of number fields) to see in particular why the local factors of the L-function at bad places v are indeed given by the action of an *arithmetic* Frobenius $\mathrm{Fr}_v \in G_K$ on the inertia-invariant subspace of $V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

2. This is due to Parshin, Zahrin (in characteristic $\neq 2$) and Mori; see [MB85, théorème XII.2.5, p. 244] and apply ideas of Tate given in [Tat66a, §3, theorem 1] or in [EvdGM, corollary 16.25]. (Over number fields, the statement of item 2 above is also true; this is due to Faltings' work on Mordell's conjecture; see also [Sil93, theorem 3.3]).

3. If $f : E \to E'$ is an isogeny of elliptic curves defined over a global field K, then the group morphism $E(\overline{K}) \to E'(\overline{K})$ is surjective with finite kernel. Hence the (non-necessarily surjective) group morphism $E(K) \to E'(K)$ has finite kernel (say of size n), and induces a morphism $E(K)/E(K)_{\mathrm{tors}} \hookrightarrow E'(K)/E'(K)_{\mathrm{tors}}$ which has to be injective (if $f(P) \in E'(K)_{\mathrm{tors}}$, say $m \cdot f(P) = O_{E'}$, then $nm \cdot P = O_E$ so $P \in E(K)_{\mathrm{tors}}$). Therefore $\mathrm{rk}\, E(K) \leqslant \mathrm{rk}\, E'(K)$.

   Applying the same reasoning to the dual isogeny $\hat{f} : E' \to E$ yields $\mathrm{rk}\, E'(K) \leqslant \mathrm{rk}\, E(K)$, so we finally get the desired equality. ■

Remark 1.3.42. In general, it is *not* true that if $L(E/K, T) = L(E'/K, T)$ then the two elliptic curves E and E' are isogenous over K. While this is true over $\mathbb{Q}$, it fails over $\mathbb{Q}(i)$ (see the explicit example given in [Sil93, remark 3.4]) and also over global function fields, even over the function field of $\mathbb{P}^1$.

Already proposition 1.3.29 points out what goes wrong: the equality of L-functions only gives that $\sum_{x \in \mathbb{P}^1(\mathbb{F}_{q^j})} A_E(v_x, j) = \sum_{x \in \mathbb{P}^1(\mathbb{F}_{q^j})} A_{E'}(v_x, j)$ holds for all $j \geqslant 1$, while being isogenous means that $A_E(v, \deg(v)) = A_{E'}(v, \deg(v))$ for all places $v \in V_K^0$.

Here is an explicit example (see also remark 4.1.12): for any prime $p \equiv -1 \pmod{12}$, if we let $q = p^n$ for some odd integer $n > 0$, then the curves $E_2 : y^2 = x^3 + t^{q+1} + 1$ and $E_{11} : y^2 = x^3 + t^q - t$ have the same L-function over $\mathbb{F}_{q^2}(t)$, namely $(1 - q^2T)^{2(q-1)}$, but they are not isogenous since they have different conductors: E_2 has good reduction at $t = 0$, while E_{11} does not. ⌟

Proposition 1.3.43. *Let E be a non-constant elliptic curve over a global field $K = k(C)$ (where k is a finite field). For each $n \geqslant 1$, let $k_n \subset \overline{k}$ be the extension of k of degree n.*

By theorem 1.3.30, we may write the L-function of E as a polynomial $L(E/k(C), T) = \prod_{i=1}^{D}(1 - \alpha_i T)$ for some $\alpha_i \in \overline{\mathbb{Q}}$. Then

$$L(E/k_n(C), T) = \prod_{i=1}^{D}(1 - \alpha_i^n T).$$ ⌟

Proof. — This is stated in [Ulm19, item (4), p. 1088]. Essentially, this relies on the fact that $L(E/K, T)$ is the "reciprocal" characteristic polynomial $\det[\mathrm{id} - T \cdot \mathrm{Fr}_k \curvearrowright V(E/K)]$, using the notations from the proof of theorem 1.3.30, and on the fact that $\mathrm{Fr}_{k_n} = \mathrm{Fr}_k^n$. (For a constant elliptic curve, this can be proved using equation (1.3.11) and the corresponding fact for zeta functions). See also remark 4.2.10 for a more direct proof in some cases. ■

1.3.4 Families of elliptic curves with unbounded rank

We will be interested in Mordell–Weil lattices of large rank, to get sphere packings in high-dimensional euclidean spaces. As mentioned in subsection 1.3.1, one reason to work over a global function field K (of positive characteristic) is that the algebraic rank of elliptic curves over K can be arbitrary large, as asserted by the following result.

Theorem 1.3.44 (Tate–Shafarevich, Ulmer). *For every global function field K, the set of Mordell–Weil ranks of elliptic curves over K is unbounded. More precisely, for every prime p, if we set $K = \mathbb{F}_p(t)$, then we have*

$$\sup\{\, \mathrm{rk}(E(K)) \;:\; E \in \mathcal{E} \,\} = +\infty,$$

where $\mathcal{E}$ is either the set of (isomorphism classes of) isotrivial elliptic curves over K, or the set of non-isotrivial elliptic curves over K. ⌟

Proof. — For the isotrivial case when $p \neq 2$, see [TS67, theorem 2], where it is shown that, given a supersingular elliptic curve A_0 over $\mathbb{F}_p$, the rank is unbounded among the quadratic twists A_n of $A := A_0 \times_{\mathbb{F}_p} \mathbb{F}_p(t)$ by quadratic extensions $\mathbb{F}_p(C_n)/\mathbb{F}_p(t)$ where C_n is a hyperelliptic curve given by an affine equation $u^2 = t^{p^n+1} + 1$ and $n \geqslant 3$ is an odd prime. In fact, Tate and Shafarevich prove that $\mathrm{rk}[A_n(\mathbb{F}_p(t))] = \frac{p^n-p}{n} + p - 1$. See also [SS19, §13.3.1].

For the isotrivial case when $p = 2$, see our theorem H (= theorem 2.5.1) and its corollary 2.5.5.

For the non-isotrivial case, see [Ulm02, theorems 1.5, 9.2] where it is shown that for every $n \geqslant 1$, the rank of the Delsarte elliptic curve

$$\Gamma_{1,p^n+1} : y^2 + xy = x^3 - t^{p^n+1}$$

over $\mathbb{F}_p(t)$ is $\geqslant \frac{p^n-1}{2n}$. ■

The main source of elliptic curves with unbounded rank over $k(t)$ (where k is a finite field) is obtained by base-change. This prompts us to introduce the following terminology, following [Ulm19, §2.3].

Definition 1.3.45. Let k be a finite field and E be an elliptic curve over $K = k(t)$.

1. Given a non-constant rational fraction $b \in K \smallsetminus k$, we denote by $\phi_b : K \to K$ the unique k-algebra endomorphism of K such that $\phi_b(t) = b(t) \in K$. It induces a scheme morphism $\Phi_b : \mathrm{Spec}(K) \to \mathrm{Spec}(K)$ and we denote by $E(b)$ the elliptic curve obtained as the fiber product (the pull-back) $E(b) := E \times_{K,\Phi_b} K$ as in the following cartesian diagram:

$$\begin{array}{ccc} E(b) & \dashrightarrow & E \\ \vdots & & \downarrow \\ \mathrm{Spec}(K) & \xrightarrow{\Phi_b} & \mathrm{Spec}(K) \end{array}$$

   where the right-vertical arrow $E \to \mathrm{Spec}(K)$ is the structural morphism.

More concretely, if $E \hookrightarrow \mathbb{P}^2_K$ is given by a Weierstrass equation $f(X,Y,Z) = f(t,X,Y,Z) = 0$, where $f \in k[t,X,Y,Z] \subset K[X,Y,Z]$ is a homogeneous cubic polynomial[41] over $k(t)$, then $E(b)$ is defined by the affine Weierstrass equation $f(b(t),X,Y,Z) = 0$.

2. The *Kummer family* attached to E is the set of elliptic curves $\{ E(t^m) \ : \ m \geqslant 1 \}$ over $k(t)$.

3. The *Artin–Schreier family* attached to E is the set of elliptic curves $\{ E(t^{q^m} - t) \ : \ m \geqslant 1 \}$ over $k(t)$, where $q = |k|$. ⌟

For instance, if E is the elliptic curve given by $f(X,Y) = Y^2 - (X^3 + 1 + t) = 0$ then $E(t^m)$ has a Weierstrass equation given by $Y^2 = X^3 + 1 + t^m$ over $k(t)$.

We state here some useful results. The first item allows us to think of Kummer families of elliptic curves over $k(t)$ as the base change of a fixed elliptic curve over a family of function fields $k(t^{1/m})$, as $m \geqslant 1$ varies (a similar result holds for Artin–Schreier families).

Proposition 1.3.46. *Let E be an elliptic curve over $k(t)$ where k is a finite field. For any integer $m > 0$, we set $E_{(m)} := E(t^m)$ as in definition 1.3.45.*

1. We have an isomorphism $E_{(m)}(k(t)) \cong E(k(t^{1/m}))$ of abelian groups. In particular, if $m, m' \geqslant 1$ are integers such that m divides m', then

$$\mathrm{rk}(E_{(m')}) \geqslant \mathrm{rk}(E_{(m)}).$$

2. Consider the integer $m = m' \cdot |k|^e$ for some integer m' coprime to $|k|$ and $e \geqslant 0$. Then

$$\mathrm{rk}\, E_{(m')}(k(t)) = \mathrm{rk}\, E_{(m)}(k(t)).$$ ⌟

Proof. — 1. To clarify the exposition we write $b(t) = t^m$, we let K_m be the K-algebra given by the ring morphism $\phi_b : K \to K$ (i.e., $K_m = K$ as a ring, and its K-algebra structure is given by t acting as t^m on 1_K) and let $\Phi_b : \mathrm{Spec}(K_m) \to \mathrm{Spec}(K)$ be the corresponding scheme morphism. Define $K'_m := k(t^{1/m})$, which is a K-algebra via the inclusion $\iota : K \hookrightarrow K_m$. Note that the morphism $t \mapsto t^{1/m}$ from K_m to K'_m defines a K-algebra isomorphism $(K_m, \phi_b) \cong (K'_m, \iota)$.

Now $E(b)$ is an elliptic curve over K_m and for any field extension L/K_m, we have a group isomorphism $\mathrm{Hom}_{K_m}(\mathrm{Spec}(L), E(b)) \cong \mathrm{Hom}_K(\mathrm{Spec}(L), E) = E(L)$, where we consider $\mathrm{Spec}(L) \to \mathrm{Spec}(K_m) \xrightarrow{\Phi_b} \mathrm{Spec}(K)$ (see [GW20, equation (4.7.1)]). When we take $L = K_m$, we find

$$E_{(m)}(K) = E_{(m)}(K_m) \cong E(K_m, \phi_b) \cong E(K'_m, \iota) = E(k(t^{1/m})).$$

Finally, if m divides m' then we clearly have an embedding of fields $k(t^{1/m}) \hookrightarrow k(t^{1/m'})$, so from the previous observation, we deduce the inequality $\mathrm{rk}(E_{(m)}) \leqslant \mathrm{rk}(E_{(m')})$.

2. If $\mathrm{char}(k) = p$ then the Frobenius morphism $\phi_{p^f} : E_{(m')} \to E_{(m')}^{(p^f)}$ is an isogeny for any $f \geqslant 0$. Moreover, when $p^f = |k|^e$ is a power of $|k|$, then $E_{(m')}^{(p^f)}$ and $E_{(m)}$ are isomorphic

[41] It is an elliptic curve since the discriminant $\Delta_{E(b)} \in k(t) = K$ of this Weierstrass equation for $E(b)$ is just $\Delta_E(b(t)) \neq 0$.

over K. Thus $E_{(m')}$ and $E_{(m)}$ are isogenous, so that proposition 1.3.41 tells us that these two curves have the same Mordell–Weil rank (as well as the same analytic rank). ■

Remark 1.3.47. Many other cases of families of elliptic with unbounded rank over global function fields have been discovered.

1. Shioda deals in [Shi91, theorem 1.2] with an isotrivial family of Delsarte elliptic curves with arbitrarily large *geometric* rank, i.e. Mordell–Weil rank over $\overline{\mathbb{F}_p}(t)$ (see definition 1.3.11). He showed that given a prime $p \equiv -1 \pmod 6$ and an odd integer $n \geqslant 1$, the rank of
$$\Gamma_{2,p^n+1} : y^2 = x^3 + 1 + t^{p^n+1}$$
over $\mathbb{F}_{p^{2n}}(t)$ equals $2(p^n+1) - 4 = 2p^n - 2$.

   (For the rank of Γ_{2,p^n+1} over $\mathbb{F}_p(t)$, and for the case $p \equiv 1 \pmod 6$, see theorem F and theorem G).

   Moreover, in [Shi86, remark 10], Shioda gives a non-isotrivial family of Delsarte elliptic curves with unbounded geometric rank, namely given a prime $p \equiv -1 \pmod 4$ and an odd integer $n \geqslant 1$, the rank of
$$\Gamma_{3,\frac{p^n+1}{2}} : y^2 = x^3 + x + t^{\frac{p^n+1}{2}}$$
over $\overline{\mathbb{F}_p}(t)$ is $p^n - 1$ if $p \equiv 1 \pmod 3$ and is $p^n - 3$ is $p \equiv -1 \pmod 3$.

   (For the rank of $\Gamma_{3,\frac{p^n+1}{2}}$ over $\mathbb{F}_p(t)$, and for the cases $p \equiv 1 \pmod 4$ or $p = 3$, see theorem B and corollary 3.1.20).

2. Elkies found in [Elk94, p. 347-348] an isotrivial family of Delsarte elliptic curves with unbounded rank over $\overline{\mathbb{F}_2}(t)$. Namely, for any odd integer $n \geqslant 1$, the curve
$$\Gamma_{4,2^n+1} : y^2 + y = x^3 + t^{2^n+1}$$
has rank 2^{n+1} over $\mathbb{F}_{2^{2n}}(t)$. This is an analogue in characteristic 2 (over the algebraic closure) of the work [TS67], since $\Gamma_{4,2^n+1}$ is a quadratic twist of a constant supersingular curve by the quadratic extension of $\mathbb{F}_2(t)$ defined by the hyperelliptic curve $u^2+u = t^{2^n+1}$. See also [SS19, example 13.39].

   (For the rank of $\Gamma_{4,2^n+1}$ over $\mathbb{F}_2(t)$, see our theorem H).

3. In [Ulm14c, corollaries 4.3, 5.3], Ulmer proves that for any odd prime p, the rank of
$$\Gamma_{5,d} : y^2 = x(x+1)(x+t^d)$$
over $\mathbb{F}_p(t)$ is unbounded as $d = p^n + 1$ and $n \geqslant 1$. See also [CHU13, Ulm14b, PU13] and [Gri16, proposition 4.3.5].

4. In the work [Ulm07b, theorems 1.3, 4.7 and §9], Ulmer gives conditions to ensure that elliptic curves (or more general L-functions) over global function fields have a large *analytic* rank (see theorem 1.3.48 below). Concrete applications of these results are given in [Ulm11, corollary 3.4.2] and also in [Gri16, proposition 5.3.5], where the rank is unbounded in the family of Delsarte elliptic curves
$$\Gamma_{6,d} : y^2 + 3t^d xy + y = x^3$$

(with short Weierstrass equation $y^2 = x^3 + (3xt^d + 4)^2$, see [Gri16, lemme 5.2.3]).

5. Lisa Berger gives in [Ber08, theorem 4.1] other examples of families of (non-Delsarte) elliptic curves with unbounded algebraic rank over global fields (see also [Ulm11, theorem 4.2.1]), by proving the BSD conjecture 1.3.34 for these curves and applying the aforementioned result [Ulm07b, theorem 4.7] (stated as theorem 1.3.48 below). See also [Gri16, remarque 8.1.1, §8.2.1, corollaire 8.3.13], where it is proved that for every prime $p \geqslant 5$, the curves

$$\Gamma_{7,d} : y^2 = (x - 2t^d)(x^2 + t^d(t^d - 4)x - 2t^{3d})$$

have unbounded rank over $\mathbb{F}_p(t)$ as $d \geqslant 1$ varies over integers coprime to p (which also follows from theorem 1.3.48).

This work is used in [Ulm13, theorem 8.1] (see also [Ulm11, lecture 5, §3]), where Ulmer proves that for any prime p and any integer $n \geqslant 1$, if we let $d = p^n + 1$ then the rank of

$$\Gamma_{8,d} : y^2 + xy + t^d y = x^3 + t^d x^2$$

(with short Weierstrass equation $y^2 = (x + 4t^d)(x^2 + x + 4t^d)$, see [Gri16, §6.2.1]) has rank $d - 1$ over $\overline{\mathbb{F}_p}(t)$ if $p = 2$ and geometric rank $d - 2$ if $p > 2$ (moreover, explicit generators for a subgroup of finite index in the Mordell–Weil group are described, and the Mordell–Weil lattice is described in [Ulm13, remark 8.10] as being homotethic to $A_{d/2}^\vee \oplus A_{d/2}^\vee$ if $p > 2$). See also [Gri16, Proposition 6.3.4].

Moreover, by [Ulm11, lecture 5, §5], the geometric rank is also unbounded in the family given over $\mathbb{F}_p(t)$, for any odd prime p, by

$$\Gamma_{9,d} : y^2 + 2t^d xy = x^3 - t^{2d} x.$$

6. In [BDS04] and [DS07], Bouw, Diem and Scholten prove the existence of (isotrivial) elliptic curves with large rank, which are quadratic twists of base change of a constant *ordinary* elliptic curve.

7. Griffon proved in [Gri20] that for every odd prime p, the rank of

$$\Gamma_{10,d} : y^2 = x(x^2 + t^{2d}x - 4t^{2d})$$

over $\mathbb{F}_p(t)$ is unbounded as $d \geqslant 1$ ranges over integers coprime to p.

8. All the examples above are *Kummer families*, obtained by base-changing a curve over $k(t)$ to $k(t^{1/d})$. On the other hand, in the paper [GU20, proposition 8.4.1], it is proved that the *Artin–Schreier family* of isotrivial Delsarte elliptic curves

$$\Gamma_{11,p^n} : y^2 = x^3 + t^{p^n} - t \tag{1.3.14}$$

has unbounded rank over $\mathbb{F}_p(t)$ for every prime $p \equiv -1 \bmod 6$, as $n \geqslant 1$ varies. See also [PU16, corollary 2.7.3 and §§4.3, 6.4, 6.5] and [Gri19, corollary 4.8]: for any odd prime p, the family

$$\Gamma_{12,p^n} : y^2 = x(x + 1)(x + (t^{p^n} - t)^2)$$

has unbounded rank over $\mathbb{F}_p(t)$ as $n \geqslant 1$ varies.

9. Davis and Occhipinti show in [DO16, proposition 3.7] that, given a power q of a prime $p \geqslant 5$, the curve
$$\Gamma_{13,q+1} : y^2 + xy - t^{q+1}y = x^3$$
has rank q over $\mathbb{F}_{q^2}(t)$ if $q \equiv 1 \bmod 3$ and rank $q-2$ over $\mathbb{F}_{q^2}(t)$ if $q \equiv 2 \bmod 3$. See also [Gri16, proposition 7.3.5].

   Moreover, the paper [Occ12, theorem 2] provides, based on Lisa Berger's work, for each prime p, an example of elliptic curve E over $\mathbb{F}_p(t)$ such that $\operatorname{rk} E(\overline{\mathbb{F}_p}(t^{1/d})) \geqslant d$ for *all* d coprime to p.

10. In [Ulm07b, §1, §7.11], it is proved in particular (by taking $g = 1$ in *loc. cit.*) that for any prime $p \geqslant 5$, the Delsarte elliptic curve with affine equation $y^2 = x^4 + x^3 + t^{p^n+1}$ has unbounded rank over $\mathbb{F}_p(t)$ as $n \geqslant 1$ varies. A short Weierstrass equation for this curve is
$$\Gamma_{14,d} : y^2 = x^3 + (-4t^d)x + t^d$$
where $d = p^n + 1$. ⌟

Here is a result that ensures that some elliptic curves have large *analytic* rank.

Theorem 1.3.48 (Ulmer). *Let E be an elliptic curve over $K = k(t)$ where k is a finite field with q elements. Let $\mathfrak{f}'(E/K) = \mathfrak{f}(E/K) - \epsilon_0(E/K)[0:1] - \epsilon_\infty(E/K)[1:0] \in \operatorname{Div}(\mathbb{P}^1)$ be the conductor of E where we remove the tame parts at the places $0, \infty$ (see definition 1.3.7).*

If $\deg(\mathfrak{f}'(E/K))$ is odd, then there is a constant $c \in \mathbb{Z}$ such that for all $n \geqslant 1$, the analytic rank of E over $k(t^{1/d})$ is at least $\frac{q^n+1}{2n} - c$, where $d := q^n + 1$. ⌟

Proof. — See [Ulm07b, theorem 4.7 and §9] and [Ulm11, theorem 3.1.1 and §3.3]. ■

Remark 1.3.49. 1. If k is a field of characteristic 0 (for instance $\mathbb{Q}, \overline{\mathbb{Q}}, \mathbb{C}$), then the rank of non-constant elliptic curves over $K = k(t)$ (which is finite by theorem 1.3.10) is not known to be unbounded (despite some claims by A. I. Lapin, see [SS19, Remark 13.20]). The largest *known* rank for an elliptic curve over $\overline{\mathbb{Q}}(t)$ is given by the isotrivial Delsarte elliptic curve $y^2 = x^3 + 1 + t^{360}$ of Mordell–Weil rank 68, see [SS19, theorem 13.26] (for a non-isotrivial curve, $y^2 = x^3 + x + t^{1260}$ has the largest known rank over $\overline{\mathbb{Q}}(t)$, namely 56, see [Shi86, corollary 9, p. 431]).

   In fact, the rank of any *Delsarte* elliptic curve over $k(t)$ is proved to be at most 68, when $\operatorname{char}(k) = 0$ (see [Hei12, theorem 1.2 and §6] or [Hei11]).

   We note that if the ranks of non-constant elliptic curves over $\mathbb{Q}(t)$ are unbounded, this would imply that the ranks of elliptic curves over $\mathbb{Q}$ are unbounded, by Silverman's specialization theorem [Sil08b, theorem III.11.4].

2. In view of the analogy between function fields and number fields, we may wonder whether the rank of elliptic curves over a given number field should be bounded or not (which is, as of now, a notorious open question). An interesting observation is made in [PPVW19, remark 12.3.1]: all *known* families $\{E_i : i \geqslant 1\}$ of elliptic curves over $\mathbb{F}_q(t)$ with unbounded rank have the property that for all but finitely many $i \geqslant 1$, the curve E_i is defined over a *proper* subfield of $\mathbb{F}_q(t)$ (typically, $\mathbb{F}_q(t^d)$ or $\mathbb{F}_q(t^{q^d} - t)$ for some $d > 1$).

We say that E is defined over a subfield $F \subset K$ if it is the base change of a curve E_0 over F, i.e., $E \cong E_0 \times_F K$. In that case, we have $j(E) \in F$; in other words, if $j(E)$ does not belong to a proper subfield of K then E is not defined over a proper subfield. However, the converse does not hold, because the j-invariant only characterizes an elliptic curve up to $\overline{K}$-isomorphism: for instance the curve $E : y^2 = x^3 + t$ over $k(t)$ (where $\mathrm{char}(k) \neq 2, 3$) has j-invariant 0, but E cannot be defined over k (but the base change of E to $k(t^{1/6})$ can be defined over k).

In fact, if $E : y^2 = x^3 + Ax + B$ is an elliptic curve over $k(t)$ not defined over proper subfield, where $A, B \in k[t]$, then either $A = 0$ and B is a polynomial of degree 1 or $A^{-3}B^2 = f$ is a Möbius transformation (i.e., a non-constant ratio of two polynomials of degree $\leqslant 1$). When $f \in k[t]$, this implies that $A = f^{-1}Q^2, B = \pm f^{-1}Q^3$ for some $Q \in k[t]$.

When $\epsilon \in \{\pm 1\}$, $f(t) = t^\epsilon$ and $Q(t) = t^r$, we get the elliptic curves $y^2 = x^3 + t^{\epsilon+3r}x + t^{\epsilon+2r}$ which are not defined over a proper subfield of $k(t)$. These are the curves $y^2 = x^3 + t^n x + t^m$ for $|2m - 3n| = 1$ (which implies that $\gcd(n, m) = 1$ but not conversely) studied in [Shi86, theorem 8], where it is proved that they have bounded rank over $\mathbb{F}_p(t)$ for any odd prime p.

In [PPVW19, §12.5], it is guessed that for any global function field K, the rank of elliptic curves E/K *not defined over a proper subfield of* K is bounded.

3. It is proved in [Gri20, theorem 7.9] that for any odd prime p, every positive odd integer occurs as the Mordell–Weil rank of some elliptic curve E over $\mathbb{F}_p(t)$, *provided* that there is a prime $\ell \neq 2, p$ such that p generates $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ (in fact, E can be taken of the form $y^2 = x^3 + t^{2d}x^2 - 4t^{2d}x$ for some $d > 0$).

4. The examples of Kummer families from remark 1.3.47 exhibit elliptic curves E over $k(t)$ such that[42] $\sup_{d \geqslant 1} \mathrm{rk}\, E(k(t^{1/d})) = +\infty$. The function field $k(t^{1/d})$ has genus 0. One could look at the rank of $E(k(C))$ for more general curves. This is for instance done in [Oes90, proposition 4, §3.3] in the case where E is constant and C is a Fermat curve.

5. The rank of families of abelian varieties (especially jacobians) has also been studied. For instance, [Ulm07b, theorem 1.1, §7.1.1] provides families of simple abelian varieties of any dimension $g \geqslant 1$ having arbitrarily large rank over $\mathbb{F}_p(t)$ for any prime p.

   See also [UZ10] (where jacobians with large rank over function fields of characteristic 0 are found — but not families with unbounded rank!), or [Shi92a, §3], [BHP+20, Ulm13, PU16, AGTT21].

6. One can point out some results about the "average" rank of elliptic curves, when ordered by (some notion of) height. Despite results like theorem 1.3.48 or [Ulm07b, theorem 1.3] (which give many examples of families of elliptic curves with unbounded rank), the average rank of elliptic curves over $\mathbb{F}_q(t)$ is finite. In fact, De Jong showed in [Jon02, corollary 1.3] that the average rank of elliptic curves over $\mathbb{F}_q(t)$ is bounded above by $\frac{3}{2} + \mathcal{O}(1/q)$, improving Brumer's bound of 2.3 (see [Bru92, theorem 7.11]). Moreover, it

[42] We can mention that it is not too difficult to show that $\sup\{\mathrm{rk}\, E(L) \ : \ L/K \text{ finite}\} = +\infty$ when $K = k(t)$ by taking successive quadratic extensions.

is conjectured that for elliptic curves over $\mathbb{Q}$ or over $\mathbb{F}_q(t)$, the average rank is $\frac{1}{2}$. See also Brumer's bound stated as theorem 2.2.6 in the next chapter. ⌟

Remark 1.3.50. There are also examples of Kummer or Artin–Schreier families of elliptic curves with *bounded* rank.

For Kummer families with bounded rank, see [Ulm07a]:

- Theorem 4.5 states that a certain quadratic twist E of an ordinary constant elliptic curve (base-changed to $\mathbb{F}_p(t)$) is such that the rank of $E(\mathbb{F}_p(t^{1/d}))$ is bounded as $d \geqslant 1$ varies[43]. However the rank is not explicitly given.
- Theorem 5.2 shows that the curve $E_1 : y^2 + xy = x^3 - t$ has rank 0 in a certain "$\mathbb{Z}_\ell$-tower" of $\overline{\mathbb{F}_p}(t)$, given by $\overline{\mathbb{F}_p}(t^{1/\ell^n})$ where $n \geqslant 1$ varies and $\ell > 5$ is a prime dividing $p - 1$.
- Theorem 6.2 proves that if $p \leqslant 11$ is prime, then there is a non-isotrivial elliptic curve E over $\mathbb{F}_p(t)$ such that $E(\overline{\mathbb{F}_p}(t^{1/d}))$ has rank 0 for any $d \geqslant 1$ (so the parity condition on the conductor in theorem 1.3.48 is not fulfilled for those E).

  Moreover, Ulmer conjectured in [Ulm07a, §6.6] that there should be such examples for any prime p. This was later proved by Lisa Berger in [Ber12, theorem 1.2].

As stated in theorem G, we found that the (isotrivial) elliptic curve $E_2 : y^2 = x^3 + 1 + t$ over $\mathbb{F}_p(t)$, with $p \equiv 1 \pmod 6$, has *constant* (hence bounded) non-zero rank over $k(t^{1/d})$ where k is a certain finite extension of $\mathbb{F}_p$ and $d \geqslant 1$ is any integer.

For Artin–Schreier families, all known examples with bounded rank seem to actually have rank 0; see [GU20] (curves E_{11} defined in equation (1.3.14), for $p \equiv 1 \pmod 6$), [Gd21, Corollary 5.4] or [PU16, §6.2]. ⌟

Remark 1.3.51. The work [Shi86] allows to compute the geometric rank of Delsarte elliptic surfaces. See remark 4.2.33. ⌟

1.4 · Character sums

1.4.1 General defintions and results on Gauss and Jacobi sums

We will be interested in computing explicitly the L-function of some elliptic curves, which allows to determine the analytic rank of those curves. These computations will involve character sums (mostly Jacobi sums), so we recall some facts above those exponential sums. First we setup some notations used in the rest of this work.

Definition 1.4.1. Let k be a field.

1. A multiplicative character of k is a group morphism $\chi : k^\times \to \overline{\mathbb{Q}}^\times$. The set of multiplicative characters on k forms a group, denoted by $\widehat{k^\times}$ (this is the Pontryagin dual for the discrete topology on $k^\times$). In particular, the set of characters on $k^\times$ of order divisible by d is the d-torsion subgroup $\widehat{k^\times}[d]$.

[43] It is assumed in [Ulm07a, theorem 4.5] that $\gcd(d, p) = 1$, but this is not necessary, see proposition 1.3.46.

2. The trivial character $\mathbb{1}$ is the constant map $k^\times \to \{1\}$.

3. Given $\chi \in \widehat{k^\times}$, we set $\chi(0) := 0$ if χ is non-trivial and $\mathbb{1}(0) := 1$.

4. If k is finite of odd characteristic, the Legendre symbol is the unique character of order 2 on $k^\times$, and is denoted by λ_k. We have $\lambda_k(x) = \iota\big(x^{\frac{|k|-1}{2}}\big)$ for all $x \in k^\times$, where ι denotes the isomorphism $k^\times[2] = \{\pm 1\} \cong \mathbb{Z}^\times \subset \overline{\mathbb{Q}}^\times$.

5. Given a finite extension k'/k, we denote by $\mathrm{N}_{k'/k} : k'^\times \to k^\times$ the norm map and by $\mathrm{tr}_{k'/k} : k' \to k$ the trace map.

6. If k is finite, then for every integer $n \geqslant 1$, we denote by $k_n \subset \overline{k}$ its unique extension of degree n.

7. For every integer $n \geqslant 1$, we write $\mu_n(k) := k^\times[n]$ for the subgroup of n-th roots of unity in $k^\times$ (it has order $\leqslant n$). We also define $\zeta_n := \exp(2\pi i/n) \in \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, which is a primitive n-th root of unity.

8. Given an element $a \in (\mathbb{Z}/d\mathbb{Z})^\times$, we denote by $\mathrm{ord}^\times(a \mod d)$ its (multiplicative) order and by $(\mathbb{Z}/d\mathbb{Z})/\langle a\rangle^\times$ the quotient *set* where the cyclic subgroup $\langle a\rangle^\times := \{\, a^j \,:\, j \in \mathbb{Z}\,\} \leqslant (\mathbb{Z}/d\mathbb{Z})^\times$ acts by multiplication on the set $\mathbb{Z}/d\mathbb{Z}$.

9. Given a real number $x \in \mathbb{R}$, we let $\{x\} := x - \lfloor x \rfloor \in [0, 1[$ be the fractional part of x. ⌟

Remark 1.4.2. When $k \hookrightarrow k'$ is a quadratic extension of finite fields of odd characteristic, we do not have $\lambda_k(x) = \lambda_{k'}(x)$ for all $x \in k$, since $\lambda_{k'}$ is trivial on $k^\times$.

On the other hand, if $k \hookrightarrow k'$ is any extension of finite fields of odd characteristic, then one has $\lambda_{k'} = \lambda_k \circ \mathrm{N}_{k'/k}$, where $\mathrm{N}_{k'/k} : (k')^\times \to k^\times$ denotes the norm map (indeed, $\mathrm{N}_{k'/k}$ is a surjective group morphism, so $\lambda_k \circ \mathrm{N}_{k'/k}$ has order exactly 2). In particular, $\lambda_{k'}(x) = \lambda_k(x)^{[k':k]}$ for all $x \in k$.

Let us mention that both the trace and norm maps are surjective and we have $\mathrm{N}_{k'/k}(x) = x^{|k'^\times|/|k^\times|}$ for all $x \in k'^\times$. ⌟

We can use characters to count solutions of simple equations over finite fields, as the following standard results show.

Proposition 1.4.3. *Let k be a finite field.*

1. For all $w \in k$ and all integers $d \geqslant 1$, we have

$$\#\{\, t \in k \,:\, t^d = w \,\} = \sum_{\chi \in \widehat{k^\times}[d]} \chi(w),$$

2. More generally, for every $z, w \in k^\times$ and all integers $n, m \geqslant 1$, we have

$$\#\{\, t \in k^\times \,:\, t^n = z,\ t^m = w \,\} = \frac{1}{|k^\times|} \sum_{\substack{\chi,\chi' \in \widehat{k^\times} \\ \chi^n \chi'^m = \mathbb{1}}} \chi(z)\chi'(w).$$

3. Fix a prime power q and an integer $n \geqslant 1$ such that $k = \mathbb{F}_{q^n}$. For all $w \in k$, we have

$$\#\{\, x \in k \,:\, x^q - x = w \,\} = \sum_{\psi : \mathbb{F}_q \to \overline{\mathbb{Q}}^\times} \psi(\mathrm{tr}_{k/\mathbb{F}_q}(w)), \tag{1.4.1}$$

where the sum runs over all additive *characters of $\mathbb{F}_q$ (not of k). In particular, we have*

$$\exists x \in k, x^q - x = w \iff \mathrm{tr}_{k/\mathbb{F}_q}(w) = 0. \tag{1.4.2}$$

⌟

Proof. — 1. When $w = 0$, both sides are equal to $1 = \mathbb{1}(0)$ (since we set $\chi(0) := 0$ when $\chi \neq \mathbb{1}$). When $w \neq 0$, the left-hand side is

$$\begin{cases} 0 & \text{if } w \notin \mathrm{Im}(f_d) \\ |\ker(f_d)| = |k^\times|/|\mathrm{Im}(f_d)| & \text{if } w \in \mathrm{Im}(f_d), \end{cases}$$

where f_d is the group morphism $f_d : k^\times \to k^\times, x \mapsto x^d$. On the other hand, let $H := \mathrm{Im}(f_d) \leqslant G := k^\times$, so that we have

$$\{\, \chi \in \widehat{G} \,:\, \chi^d = \mathbb{1} \,\} = H^\perp := \{\, \chi \in \widehat{G} \,:\, \chi|_H = \mathbb{1} \,\} \tag{1.4.3}$$

Let us denote by $\pi : G \to G/H$ the quotient morphism. It is known that the map $\widehat{G/H} \to H^\perp, \overline{\chi} \mapsto \overline{\chi} \circ \pi$ is an isomorphism and consequently, we may rewrite the right-hand side as

$$\sum_{\chi^d = \mathbb{1}} \chi(w) = \sum_{\overline{\chi} \in \widehat{G/H}} \overline{\chi}([w]) = |G/H| \cdot \mathbb{1}_{w \in H} = |\ker(f_d)| \cdot \mathbb{1}_{w \in H} = \#\{\, x \in k \,:\, x^d = w \,\}.$$

2. The proof is similar to the previous case. Consider the group $G := k^\times \times k^\times$ and the group morphism $\phi : k^\times \to G, t \mapsto (t^n, t^m)$ as well as its image $H := \mathrm{Im}(\phi)$. We have (using the fact $k^\times / \ker(\phi) \cong H$)

$$\begin{aligned} \#\{\, t \in k^\times \,:\, t^n = z,\ t^m = w \,\} &= |\ker(\phi)| \cdot \mathbb{1}_{(z,w) \in \mathrm{Im}(\phi)} \\ &= \frac{1}{|k^\times|} \cdot \left|G/H\right| \cdot \mathbb{1}_{(\bar{z},\bar{w}) \equiv (\bar{1},\bar{1}) \bmod H} \\ &= \frac{1}{|k^\times|} \sum_{\overline{\chi} \in \widehat{G/H}} \bar{\chi}(\bar{z}, \bar{w}) \\ &= \frac{1}{|k^\times|} \sum_{\chi \in H^\perp} \chi(z, w) \end{aligned}$$

where

$$H^\perp := \{\, \chi \in \widehat{G} \,:\, \chi|_H = \mathbb{1} \,\} = \{\, \chi \in \widehat{G} \,:\, \forall t \in k^\times,\ \chi(t^n, t^m) = 1 \,\}.$$

Note that there is an isomorphism $\widehat{G} \cong \left(\widehat{k^\times}\right)^2$ where a pair (χ, χ') of multiplicative characters on k is mapped to the character $(z, w) \mapsto \chi(z)\chi'(w)$. Under this isomorphism, $H^\perp$ corresponds to the set of pairs (χ, χ') such that $\chi^n \chi'^m = \mathbb{1}$, whence the claim.

3. We first prove (1.4.2) (additive version of Hilbert 90 theorem), because it is equivalent to (1.4.1). Indeed, from (1.4.2) we deduce that $x^q - x = w$ has 0 solution if $\mathrm{tr}(w) \neq 0$, and has q solutions otherwise (if it has at least one solution x_0, then $x_0 + \alpha$ is a solution for any $\alpha \in \mathbb{F}_q$). By orthogonality of characters, the same holds for $\sum_{\psi:\mathbb{F}_q\to\mathbb{C}^\times} \psi(\mathrm{tr}_{k/\mathbb{F}_q}(w))$, so the conclusion follows.

   We actually prove a more general fact than (1.4.2). Namely, given any finite cyclic Galois extension L/K of fields, given a generator σ of $\mathrm{Gal}(L/K)$ and given $w \in L$, we have

$$\sigma(x) - x = w \text{ has a solution in } L \iff \mathrm{tr}_{L/K}(w) = 0. \tag{1.4.4}$$

   Here is a first (cohomological) proof. One has $H^r(\mathrm{Gal}(L/K), (L,+)) = \{0\}$ for all $r \geqslant 1$ (even for non-cyclic extensions), and when G is a *cyclic* group acting on some G-module A, then $H^1(G,A) \cong H_T^{-1}(G,A) := \ker(\sum_{g\in G} g)/\langle ga - a \ : \ a \in A\rangle$ (the latter group comes from Tate cohomology), from which the equivalence (1.4.4) immediately follows.

   We can also give a direct proof of (1.4.4). The implication $\implies$ is clear, so assume that $\mathrm{tr}_{L/K}(w) = 0$. Define the map $g : L \to L, x \mapsto \sigma(x) - x$. It is a K-linear map, with kernel $\ker(g)$ equal to K, since $\mathrm{Gal}(L/K)$ is generated by σ. As we just noticed, we have $\mathrm{Im}(g) \subset \ker(\mathrm{tr}_{L/K})$.

   Moreover, we have $\mathrm{Im}(\mathrm{tr}_{L/K}) = K$, i.e., $\mathrm{tr}_{L/K} : L \to K$ is surjective (indeed, by K-linearity, proving surjectivity of the trace amounts to showing that $\mathrm{tr}_{L/K} \neq 0$; this is in fact equivalent to L/K being separable). But then comparing K-dimensions, we conclude that $\mathrm{Im}(g) = \ker(\mathrm{tr}_{L/K})$. Thus equations (1.4.2) and (1.4.4) hold. ■

Remark 1.4.4. In proposition 1.4.3, the second item is indeed a generalization of the first one because we may take $z = w$ and $n = m$. Also, if we assume that $n = m$, then when $z \neq w$, or when $z = w$ is not an n-th power in $k^\times$, the sum $\sum_{\chi,\chi'\in\widehat{k^\times},\ \chi^n\chi'^m=\mathbb{1}} \chi(z)\chi'(w)$ vanishes, which can be checked directly:

$$\begin{aligned}\sum_{\chi\in\widehat{k^\times}} \Big(\chi(z) \sum_{\substack{\chi'\in\widehat{k^\times}\\(\chi\chi')^n=\mathbb{1}}} \chi'(w)\Big) &= \sum_{\chi\in\widehat{k^\times}} \chi(zw^{-1}) \sum_{\substack{\chi'=:\chi^{-1}\tilde{\chi}\in\widehat{k^\times}\\(\chi\chi')^n=\mathbb{1}}} (\chi\chi')(w)\\ &= [k^\times : k^{\times,n}] \cdot \sum_{\tilde{\chi}\in\widehat{k^\times}} \tilde{\chi}(zw^{-1})\mathbb{1}_{w\in k^{\times,n}}\\ &= [k^\times : k^{\times,n}] \cdot |k^\times| \cdot \mathbb{1}_{w\in k^{\times,n}} \cdot \mathbb{1}_{z=w}.\end{aligned}$$

⌟

Definition 1.4.5. Let k be a finite field of characteristic p and let $\chi, \chi_1, ..., \chi_n : k^\times \to \overline{\mathbb{Q}}^\times$ be multiplicative characters on k.

1. We define the Gauss sum of χ as[44] $G(\chi) := \sum_{x\in k^\times} \chi(x) \exp\left(2\pi i \frac{\mathrm{tr}_{k/\mathbb{F}_p}(x)}{p}\right)$.

2. We define the Jacobi sum of $\chi_1, ..., \chi_n$ as

$$J(\chi_1, ..., \chi_n) := \sum_{\substack{x_1,...,x_n\in k\\ x_1+...+x_n=1}} \chi_1(x_1)\cdots\chi_n(x_n).$$

⌟

[44] Here we view the algebraic closure of $\mathbb{Q}$ as the set of complex numbers which are algebraic over $\mathbb{Q}$, so that $\exp\left(2\pi i \frac{\mathrm{tr}_{k/\mathbb{F}_p}(x)}{p}\right)$ lies in $\overline{\mathbb{Q}}$.

Note that $G(\chi)$ is a sum over $k^\times$, not over k. When $n = 1$, we have $J(\chi_1) = \chi_1(1) = 1$. When $n = 3$, we sometimes speak of "triple Jacobi sum". Here are some basic properties of these sums.

Proposition 1.4.6. *Let k be a finite field of characteristic p and let $\chi, \chi_1, ..., \chi_n \in \widehat{k^\times}$.*

1. *We have $G(\mathbb{1}) = -1$ and if $\chi \neq \mathbb{1}$, then $|\iota(G(\chi))| = |k|^{1/2}$ for any field embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$.*
2. *If $\chi_i \neq \mathbb{1}$ for all i, then we have*
$$J(\chi_1, ..., \chi_n) = \begin{cases} -\chi_n(-1)J(\chi_1, ..., \chi_{n-1}) & \text{if } \chi_1 \cdot \chi_2 \cdots \chi_n = \mathbb{1}, \\ \dfrac{G(\chi_1) \cdots G(\chi_n)}{G(\chi_1 \cdot \chi_2 \cdots \chi_n)} & \text{else.} \end{cases}$$
In particular, if $\chi_1 \cdot \chi_2 \cdots \chi_n \neq \mathbb{1}$ and $\chi_i \neq \mathbb{1}$ for all i, then $|\iota(J(\chi_1, ..., \chi_n))| = |k|^{\frac{n-1}{2}}$ for any embedding $\iota : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Moreover, if some of the characters χ_i are trivial but not all, then $J(\chi_1, ..., \chi_n) = 0$.
3. *We have $G(\chi^p) = G(\chi)$ and $J(\chi_1^p, ..., \chi_n^p) = J(\chi_1, ..., \chi_n)$ (hence, applied successively, we have $J(\chi_1^{|k|}, ..., \chi_n^{|k|}) = J(\chi_1, ..., \chi_n)$).* ⌟

Proof. — See [Coh07, §2.5.2, §2.5.3] or [BEW98, theorem 1.1.4] for the first two items. The third item follows from the fact that $x \mapsto x^p$ is a field automorphism of k and preserves the trace map (i.e., $\mathrm{tr}_{k/\mathbb{F}_p}(x) = \mathrm{tr}_{k/\mathbb{F}_p}(x^p)$ for all $x \in k$). ■

Note that when $n = 2$, the second item of proposition 1.4.6 yields[45] $J(\chi, \chi^{-1}) = -\chi(-1)$ for any non-trivial $\chi \in \widehat{k^\times}$.

1.4.1.1 Hasse–Davenport and Tate–Shafarevich theorems

An important fact is the following relation between the Gauss or Jacobi sums over various extensions of a finite field.

Theorem 1.4.7 (Hasse–Davenport lifting relation). *Let k be a finite field and, for every $n \geqslant 1$, let $k_n \subset \overline{k}$ be its extension of degree n. Let $\chi, \chi_1, ..., \chi_m \in \widehat{k^\times}$ be non-trivial characters. Then we have:*
$$-G(\chi \circ \mathrm{N}_{k_n/k}) = (-G(\chi))^n,$$
$$J(\chi_1 \circ \mathrm{N}_{k_n/k}, ..., \chi_m \circ \mathrm{N}_{k_n/k}) = (-1)^{(n-1)(m-1)} J(\chi_1, ..., \chi_m)^n.$$ ⌟

Proof. — See [Coh07, theorem 3.7.4, corollary 3.7.5]. Note that the second identity follows from the first, by proposition 1.4.6. One strategy to prove the first identity is to make use of the Dirichlet L-function $L(\eta_\chi, T)$ (especially the fact that it is a polynomial in T) attached to a certain Dirichlet character $\eta_\chi : k_M^\times := \big(k[X]/(M(X))\big)^\times \cong (k, +) \times k^\times \longrightarrow \mathbb{C}^\times$ where $M(X) = X^2$ and $\eta_\chi([f]) = \chi(f(0)) \cdot \psi(f'(0)/f(0))$ for all $[f] \in k_M^\times$, where $\psi(x) := \exp(2\pi i \,\mathrm{tr}_{k/\mathbb{F}_p}(x)/p)$ for all $x \in k$. ■

[45] This can be proved directly: Note that the map $x \mapsto \frac{x}{1-x}$ is injective from $k \smallsetminus \{1\}$ to $k \smallsetminus \{-1\}$ (indeed, $\frac{x}{1-x} = \frac{x'}{1-x'}$ implies $x - xx' = x' - xx'$ so $x = x'$), thus is bijective and then we have, when χ is not trivial: $J(\chi, \chi^{-1}) = \sum_{x \in k \smallsetminus \{1\}} \chi(x(1-x)^{-1}) = \sum_{x' \in k \smallsetminus \{-1\}} \chi(x') = -\chi(-1)$.

The following crucial result computes *explicitly* some Gauss sums and Jacobi sums, in particular giving a sufficient condition for a Jacobi sum to be equal to a *positive integer*. This will be important to compute (as in corollary 3.1.14, for instance) the analytic rank of some elliptic curves over $k(t)$ whose L-function can be written (essentially) as a product $\prod_r(1-\alpha_r T)$ where each α_r is (related) to a Jacobi sum: the analytic rank is the number of indices r such that $\alpha_r = |k|$ (which is a positive integer).

Theorem 1.4.8 (Tate–Shafarevich). *Let k_2/k be a quadratic extension of finite fields and $\chi \in \widehat{k_2^\times}$ be non-trivial. Assume that the restriction $\chi|_{k^\times} = \mathbb{1}$ is trivial. Then one has $G(\chi) = \chi(z)|k|$, where $z \in k_2^\times$ is any non-zero element such that $\mathrm{tr}_{k_2/k}(z) = z + z^{|k|} = 0$.*

Consequently, if $\chi_1, ..., \chi_m \in \widehat{k_2^\times}$ are non-trivial characters that are trivial on $k^\times$ and such that $\chi_1 \cdots \chi_m \neq \mathbb{1}$, then

$$J(\chi_1, ..., \chi_m) = |k_2|^{\frac{m-1}{2}}.$$

⌟

Proof. — See [TS67, lemma, p. 918] or [Ulm02, lemma 8.3] (note that in the latter reference, the Gauss sum is defined with a minus sign in front). Note that $\chi(z)$ is independent of z, since any two elements in $k_2^\times$ of trace 0 differ by some multiplicative constant in $k^\times$ (the kernel of the trace is 1-dimensional over k) and χ is trivial on $k^\times$. The second claim about Jacobi sums readily follows from the first part and from proposition 1.4.6. ■

Remark 1.4.9. Assume that k is a finite field of odd cardinality q. If g generates the group $k_2^\times$, then the element $z := g^{\frac{q+1}{2}}$ has trace 0 over k. Indeed, we have a chain of equivalences:

$$\begin{aligned} \mathrm{tr}_{k_2/k}(z) = z + z^q = 0 &\iff g^{\frac{q+1}{2}} = -g^{q\cdot\frac{q+1}{2}} = g^{\frac{q^2-1}{2}+\frac{q(q+1)}{2}} \\ \iff q+1 \equiv q^2-1+q^2+q \pmod{q^2-1} &\iff 2(q^2-1) \equiv 0 \bmod q^2-1. \end{aligned}$$

⌟

1.4.2 Teichmüller character

Let k be a finite field. The groups $\widehat{k_n^\times}$ are cyclic for any $n \geqslant 1$, and there is actually a way to have a "compatible" family of generators, thanks to the *Teichmüller character*. There are several equivalent ways to define it. We start with the following observation.

Lemma 1.4.10. *Let R be an integral domain (e.g., $R = \mathbb{Z}$) with field of fractions K. Fix a maximal ideal $\mathfrak{m} \trianglelefteq R$. Denote by $\overline{K}$ an algebraic closure of K, and let $\overline{R}$ be the integral closure of R in $\overline{K}$. Then there exists a maximal ideal $\overline{\mathfrak{m}} \trianglelefteq \overline{R}$ above $\mathfrak{m}$ (that is, $\mathfrak{m} = \overline{\mathfrak{m}} \cap R$), and for any such ideal, the quotient ring $\overline{R}/\overline{\mathfrak{m}}$ is an algebraic closure $R/\mathfrak{m}$.* ⌟

Proof. — The existence of $\overline{\mathfrak{m}}$ follows from the "lying over" property for prime ideals applied to the integral extension $R \subset \overline{R}$ and by using Zorn's lemma.

Note that we have an injection $R/\mathfrak{m} \hookrightarrow \overline{R}/\overline{\mathfrak{m}}$ since $\mathfrak{m} = \overline{\mathfrak{m}} \cap R$, and this extension is algebraic. It remains to check that $\overline{R}/\overline{\mathfrak{m}}$ is algebraically closed. Let $\widetilde{F} \in (\overline{R}/\overline{\mathfrak{m}})[X]$ be a polynomial, which we may assume to be monic. We can lift $\widetilde{F}$ to some *monic* polynomial

$F \in \overline{R}[X]$. Since $\overline{K}$ is algebraically closed, F splits over $\overline{K}$, but we shall show that all roots of F belong to $\overline{R}$, and hence $\widetilde{F}$ splits completely over $\overline{R}/\overline{\mathfrak{m}}$.

Fix a root $a \in \overline{K}$ of F. If we write $F(x) = x^n + f_{n-1}x^{n-1} + \cdots + f_1 x + f_0$, then $S := R[f_0, ..., f_{n-1}] \subset \overline{R}$ is finitely generated as R-module. Moreover, $S[a]$ is finitely generated as R-module, since $a^n = -(f_{n-1}a^{n-1} + \cdots + f_1 a + f_0)$. Thus $S[a]$ is finite over R, and so is $R[a]$, which implies that $a \in \overline{R}$ is an algebraic integer over R as desired. ■

In particular for $R = \mathbb{Z}$ and any[46] maximal ideal $P \trianglelefteq \overline{\mathbb{Z}}$ (in the ring of algebraic integers $\overline{\mathbb{Z}}$) above $p\mathbb{Z}$, we have $\overline{\mathbb{Z}}/P \cong \overline{\mathbb{F}_p}$. Now we denote by $\pi_P : \overline{\mathbb{Z}} \longrightarrow \overline{\mathbb{Z}}/P \cong \overline{\mathbb{F}_p}$ the reduction morphism. The main claim to construct the Teichmüller character is the following lemma.

Lemma 1.4.11. *Consider the subgroup*

$$\mu^{(p)} := \left\{ x \in \overline{\mathbb{Q}}^\times \ : \ \exists m \in \mathbb{Z}, x^m = 1, \gcd(m, p) = 1 \right\} \ \leqslant \ \overline{\mathbb{Z}}^\times$$

Then π_P restricts to an isomorphism $\pi_P|_{\mu^{(p)}} : \mu^{(p)} \xrightarrow{\cong} \overline{\mathbb{F}_p}^\times$. ⌟

Definition 1.4.12. Given a prime p, we fix once and for all a maximal ideal $P \trianglelefteq \overline{\mathbb{Z}}$ above p. The Teichmüller character $\Theta = \Theta_P : \overline{\mathbb{F}_p}^\times \to \mu^{(p)} \subset \overline{\mathbb{Q}}^\times$ is the inverse of the morphism $\pi_P|_{\mu^{(p)}}$ defined in lemma 1.4.11. ⌟

Proof of lemma 1.4.11. —

- We first prove the surjectivity of $\pi|_{\mu^{(p)}}$. We fix $y \in \overline{\mathbb{F}_p}^\times$ so that $y \in \mathbb{F}_{p^r}^\times$ for some $r \geqslant 1$. If we set $m = p^r - 1$, then $y^m = 1$. Since $\gcd(m, p) = 1$, it follows that y is a *simple* root of the polynomial $T^m - 1 \in \mathbb{F}_{p^r}[T]$. There is a (unique unramified) extension K_r of $\mathbb{Q}_p$ with residue field $\mathcal{O}_{K_r}/\mathfrak{p} \cong \mathbb{F}_{p^r}$; in fact we may take $K_r = \mathbb{Q}_p(\zeta_{p^r-1})$. Applying Hensel's lemma to it, we get an element $x \in K_r$ such that $x^m = 1$ and $x \equiv y \pmod{\mathfrak{p}}$. Then $x \in \mu^{(p)} \hookrightarrow \overline{\mathbb{Z}}^\times$ is a preimage of y under π, showing the claimed surjectivity.
- We now check the injectivity of $\pi|_{\mu^{(p)}}$. Assume that x belongs to the kernel, that is: $x^m = 1$ for some integer $m \geqslant 2$ coprime to p and $x \equiv 1 \pmod{P}$. We want to show that $x = 1$. We may write $x = 1 + y$ for some $y \in P$, and then

$$1 = x^m = (1 + y)^m = 1 + my + \cdots + y^m \tag{1.4.5}$$

  so that $y(m + \cdots + y^{m-1}) = 0$. If $y \neq 0$, then we see that m can be expressed as sums of powers of y, so $m \in P$ since P is an ideal and $y \in P$. But then $m \in P \cap \mathbb{Z} = p\mathbb{Z}$, contradicting the fact that $\gcd(m, p) = 1$ ↯. Thus this forces $y = 0$ and $x = 1$ as desired. ■

Remark 1.4.13. 1. The injectivity of π_P fails on the p-th roots of unity. Namely, consider $\mathbb{Z}[\zeta_p] \subset \overline{\mathbb{Z}}$, and the prime ideal $\mathfrak{p} = (1 - \zeta_p)$ which lies above p. Then $\zeta_p \neq 1$ but $\zeta_p \equiv 1 \pmod{\mathfrak{p}}$, so π_P is not injective on μ_p.

[46] There are infinitely many such ideals, and the absolute Galois group $G_\mathbb{Q}$ of $\mathbb{Q}$ acts transitively on those; see [Was97, Appendix §2, Lemma, p. 394]. Since $\mathbb{Z} \subset \overline{\mathbb{Z}}$ is integral, they both have the Krull dimension 1, so any non-zero prime ideal of $\overline{\mathbb{Z}}$ is maximal.

2. There are other ways to define the Teichmüller character. Let k be a finite field with $q = p^r$ elements.

   - Following [Was97, chap. 6, p. 95], if we fix a prime ideal $\mathfrak{p}$ of (the ring of integers of) $\mathbb{Q}(\zeta_{q-1})$ lying above p, then $\mathbb{Z}[\zeta_{q-1}]/\mathfrak{p} \cong \mathbb{F}_q \cong k$ and the $(q-1)$-st roots of unity are distinct modulo $\mathfrak{p}$ (see [Was97, lemma 2.12] or [Coh07, lemma 3.6.1]), so this yields an isomorphism $k^\times \to \mu_{q-1}(\overline{\mathbb{Q}})$ which is nothing but the restriction $\Theta|_{k^\times}$.
   - Alternatively, one may use a purely p-adic approach: as before we let $\mathcal{O}_r = \mathbb{Z}_p[\zeta_{q-1}]$ be (the ring of Witt vectors of k or equivalently) the ring of integers of the unique unramified extension K_r of $\mathbb{Q}_p$ with residue field $\mathcal{O}_r/\mathfrak{p} \cong \mathbb{F}_q \cong k$. For $a = [z]_{\mathfrak{p}} \in k^\times$ we define the value[47] $\omega_q(a) := \lim_{n\to\infty} z^{q^n}$, which is the unique $(q-1)$-th root of unity in $\mathcal{O}_r$ such that $\omega_q(a) \equiv a \pmod{\mathfrak{p}}$. We get a section $\omega_q : k^\times \to \mu_{q-1}(\overline{\mathbb{Z}}) \subset \mathcal{O}_r^\times$ of $\pi_q : \mathcal{O}_r^\times \to k^\times$. One can check that $\Theta|_{k^\times} = \omega_q$.
   - Finally, one can mention that given an integer $m \geqslant 1$ not divisible by some prime p, if we let a prime $\mathfrak{p} \trianglelefteq \mathbb{Z}[\zeta_m]$ above p, then $k := \mathbb{Z}[\zeta_m]/\mathfrak{p}$ has $q = p^f$ elements, where $f = \mathrm{ord}^\times(p \mod m)$ and $\Theta|_{k^\times}^{\frac{|k^\times|}{m}}$ is the m-th power residue symbol (or reciprocity symbol), see e.g. [Coh07, definition 3.6.2, lemma 3.6.24]: it is the unique multiplicative character $\chi_{\mathfrak{p},m} : k^\times \to \mu_m(\overline{\mathbb{Z}})$ of order m such that $\chi_{\mathfrak{p},m}(x) \equiv x^{\frac{q-1}{m}} \pmod{\mathfrak{p}}$ for all $x \in \mathbb{Z}[\zeta_m] \smallsetminus \mathfrak{p}$. In particular when $m = q-1$, we get $\Theta(x) \equiv x \bmod \mathfrak{p}$ for all $x \in \mathbb{Z}[\zeta_{q-1}] \smallsetminus \mathfrak{p}$. ⌟

Proposition 1.4.14. *Let $\Theta : \overline{\mathbb{F}_p}^\times \hookrightarrow \overline{\mathbb{Q}}^\times$ be the Teichmüller character. Let $k \supset \mathbb{F}_p$ be a finite field. Then $\Theta|_{k^\times}$ generates the cyclic group $\widehat{k^\times}$ and there is a unique generator g of $k^\times$ such that $\Theta(g) = \exp\left(\frac{2\pi i}{|k^\times|}\right)$.*

More generally, if d divides $|k^\times|$ then the restriction of $\Theta^{\frac{|k^\times|}{d}}$ to $k^\times$ is a character of order exactly d which generates $\widehat{k^\times}[d]$, and its value on the generator g from above is $\Theta^{\frac{|k^\times|}{d}}(g) = \exp\left(\frac{2\pi i}{d}\right)$. ⌟

Proof. — The fact that $\Theta|_{k^\times}$ generates the cyclic group $\widehat{k^\times}$ is proved in [Gri16, lemme 2.1.2]. The existence of an element $g \in k^\times$ such that $\Theta(g) = \exp\left(\frac{2\pi i}{|k^\times|}\right)$ is clear since the image of $\Theta|_{k^\times}$ is the subgroup $\mu_{|k^\times|} \subset \overline{\mathbb{Q}}^\times$. Then g must be a generator of $k^\times$ since its order is at least as large as the order of $\Theta(g) = \exp\left(\frac{2\pi i}{|k^\times|}\right)$ which equals $|k^\times|$. Uniqueness of such a $g \in k^\times$ is clear as Θ is injective. The rest of the statement of the proposition is easily deduced from the previous claims. See also remark 1.4.18. ■

1.4.2.1 Characters of order dividing d

It is convenient to introduce some notations in order to classify the characters of order dividing d (namely the elements of $\widehat{k_n^\times}[d]$).

Definition 1.4.15. Let us fix a power q of some prime p and an integer $d \geqslant 1$ coprime to q.

[47] One easily shows that the sequence $(z^{q^n})_{n\geqslant 1}$ is Cauchy (it suffices to check that $|z^{q^{n+1}} - z^{q^n}| \to 0$ as $n \to \infty$ by the ultrametric property of $\mathcal{O}_r$), so it converges in $\mathcal{O}_r$ by completeness.

1. We define the map
$$\begin{array}{rccc} u_{q,d}: & \mathbb{Z}/d\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & r \bmod d & \longmapsto & \min\{\, j \geqslant 1 \;:\; d \mid (q^j-1)r \,\}. \end{array} \tag{1.4.6}$$
Note that it is indeed well-defined on $\mathbb{Z}/d\mathbb{Z}$. In other words, $u_{q,d}(r)$ is the cardinality of the orbit $r \in \mathbb{Z}/d\mathbb{Z}$ under the action of the group $\langle q \rangle \leqslant (\mathbb{Z}/d\mathbb{Z})^\times$ of powers of q by multiplication on $\mathbb{Z}/d\mathbb{Z}$.

2. Given $r \in \mathbb{Z}/d\mathbb{Z}$ and an integer $n \in u_{q,d}(r)\mathbb{Z}_{>0}$, we define the character
$$\begin{array}{rccc} \theta_{\mathbb{F}_{q^n},d,r}: & \mathbb{F}_{q^n}^\times & \longrightarrow & \overline{\mathbb{Q}}^\times \\ & x & \longmapsto & \Theta(x)^{\frac{(q^n-1)r}{d}} \end{array}$$
Note that this definition does not make sense for every $n \in \mathbb{Z}_{>0}$, but only for those n which are integer multiples of $u_{q,d}(r)$ because then we have $\frac{(q^n-1)r}{d} \in \mathbb{Z}$ (as proposition 1.4.16.3 will show). ⌟

We state a few properties of $u_{q,d}$ and $\theta_{\mathbb{F}_{q^n},d,r}$ in the following two easy propositions.

Proposition 1.4.16. *Let q and $d \geqslant 1$ be as in definition 1.4.15.*

1. *For every $r \in \mathbb{Z}/d\mathbb{Z}$, the value $u_{q,d}(r)$ is equal to the multiplicative order of q in the group $\left(\mathbb{Z}\Big/\frac{d}{(d,r)}\mathbb{Z}\right)^\times$. Here (d,r) denotes the gcd between d and r.*
2. *We have $u_{q,d}(r) = u_{q,d}(q^j r)$ for all $j \in \mathbb{Z}$. (Note that q is invertible in $\mathbb{Z}/d\mathbb{Z}$ so that $q^j r$ makes sense even when $j < 0$).*
3. *Given $r \in \mathbb{Z}/d\mathbb{Z}$ and $j \geqslant 1$, we have $d \mid r \cdot (q^j-1) \iff u_{q,d}(r) \mid j$.*
4. *Given an integer $A \geqslant 1$, we have $\#\{\, r \in \mathbb{Z}/d\mathbb{Z} \;:\; d \mid A \cdot r \,\} = \gcd(d,A)$. In fact, we have the equivalences $d \mid A \cdot r \iff \frac{d}{\gcd(d,A)} \,\Big|\, r \iff \frac{d}{\gcd(d,r)} \,\Big|\, A$.* ⌟

Proof. — We first prove item 4 and then the rest will follow.

4. It suffices to check the first equivalence, because the second one follows by symmetry (swap A and r), and it also follows that $\{\, r \in \mathbb{Z}/d\mathbb{Z} \;:\; d \mid A \cdot r \,\} = \frac{d}{(d,A)}\mathbb{Z}\Big/d\mathbb{Z}$. Now the equivalence $d \mid A \cdot r \iff \frac{d}{\gcd(d,A)} \,\Big|\, r$ can be checked by considering the ℓ-adic valuations v_ℓ for all primes ℓ, which amounts to checking that $v_\ell(A) + v_\ell(r) \geqslant v_\ell(d) \iff v_\ell(r) \geqslant v_\ell(d) - \min\{v_\ell(A), v_\ell(d)\}$ for all primes ℓ, which is clear (since $v_\ell(r) \geqslant 0$).

1. From item 4 we get $d \mid r \cdot (q^j-1) \iff \frac{d}{(d,r)} \,\Big|\, (q^j-1)$, so that $u_{q,d}(r)$ is indeed the multiplicative order of q modulo $\frac{d}{(d,r)}$.

3. This is clear from items 1 and 4.

2. This also follows from item 1, since $\gcd(d,q) = 1$. ■

It is also useful to note that for all $N \geqslant 1$, we have $u_{q^N,d}(r) = \operatorname{ord}\left(q^N \bmod \frac{r}{(d,r)}\right) = \frac{u_{q,d}(r)}{\gcd(N, u_{q,d}(r))}$ (recall that in for any element g of a finite group we have $\operatorname{ord}(g^N) = \frac{\operatorname{ord}(g)}{\gcd(N,\operatorname{ord}(g))}$).

Proposition 1.4.17. *Let q and $d \geqslant 1$ be as in definition 1.4.15. Fix $r \in \mathbb{Z}/d\mathbb{Z}$.*

1. *Let $n, N \in u_{q,d}(r)\mathbb{Z}$. Assume $n \mid N$ so that $\mathbb{F}_{q^n} \subset \mathbb{F}_{q^N}$. Then we have*

$$\theta_{\mathbb{F}_{q^N},d,r} = \theta_{\mathbb{F}_{q^n},d,r} \circ \mathrm{N}_{\mathbb{F}_{q^N}/\mathbb{F}_{q^n}} \tag{1.4.7}$$

2. *Let $n \in u_{q,d}(r)\mathbb{Z}$. The character $\theta_{\mathbb{F}_{q^n},d,r} \in \widehat{\mathbb{F}_{q^n}^\times}$ has order exactly $\dfrac{d}{(d,r)}$.*

3. *Let k be a finite field. We have*

$$\widehat{k_n^\times}[d] = \left\{ \theta_{k_n,d,r} \ : \ r \in \mathbb{Z}/d\mathbb{Z} \text{ such that } u_{|k|,d}(r) \mid n \right\}, \tag{1.4.8}$$

and consequently we have the equality of sets

$$\bigsqcup_{n \geqslant 1} \widehat{k_n^\times}[d] = \bigsqcup_{r \in \mathbb{Z}/d\mathbb{Z}} \left\{ \theta_{k_n,d,r} \ : \ n \in u_{|k|,d}(r)\mathbb{Z}_{>0} \right\}. \tag{1.4.9}$$

In particular, when $|k| \equiv 1 \pmod{d}$, then $u_{|k|,d}(r) = 1$ for all r and

$$\widehat{k_n^\times}[d] = \left\{ \theta_{k,d,r} \circ \mathrm{N}_{k_n/k} \ : \ r \in \mathbb{Z}/d\mathbb{Z} \right\} = \left\{ \chi \circ \mathrm{N}_{k_n/k} \ : \ \chi \in \widehat{k^\times}[d] \right\}. \qquad \lrcorner$$

The second equality in item 3 is especially interesting: we can express an infinite union of finite sets as a *finite* union of infinite sets of characters given by pre-composing with the *norm map* of arbitrary finite extensions of $k_{u(r)}$, which will be the key to get the rationality of the L-function.

Proof. — 1. To ease the notation, let $k = \mathbb{F}_{q^n}$ and write $m = N/n \in \mathbb{Z}$, so that $k_m := \mathbb{F}_{q^N}$ is the extension of k of degree m. The main point is to observe that the norm is given by

$$\mathrm{N}_{k_m/k}(x) = \prod_{\sigma \in \mathrm{Gal}(k_m/k)} \sigma(x) = x \cdot x^{q^n} \cdot x^{q^{2n}} \cdots x^{q^{(m-1)n}} = x^{1+q^n+\cdots+q^{(m-1)n}} = x^{\frac{q^N-1}{q^n-1}}$$

for all $x \in k_m$. Thus we get

$$\begin{aligned} \theta_{\mathbb{F}_{q^N},d,r}(x) &= \Theta(x)^{\frac{(q^N-1)r}{d}} = \Theta(x)^{\frac{q^N-1}{q^n-1}\frac{(q^n-1)r}{d}} \\ &= \Theta\big(\mathrm{N}_{\mathbb{F}_{q^N}/\mathbb{F}_{q^n}}(x)\big)^{\frac{(q^n-1)r}{d}} = \theta_{\mathbb{F}_{q^n},d,r}\Big(\mathrm{N}_{\mathbb{F}_{q^N}/\mathbb{F}_{q^n}}(x)\Big). \end{aligned}$$

2. By proposition 1.4.14, there is a unique generator g of $\mathbb{F}_{q^n}^\times$ such that

$$\theta_{\mathbb{F}_{q^n},d,r}(g) = \exp\left(\frac{2\pi i}{q^n-1} \cdot \frac{r \cdot (q^n-1)}{d}\right) = \exp\left(\frac{2\pi i r}{d}\right).$$

Let A be the order of $\theta_{\mathbb{F}_{q^n},d,r}$. Then $\exp\left(\frac{2\pi i r}{d}\right)^A = 1$ so that $d \mid A \cdot r$ and proposition 1.4.16.4 implies that A is a multiple of $\frac{d}{(d,r)}$. On the other hand, it is clear that $\theta_{\mathbb{F}_{q^n},d,r}^{\frac{d}{(d,r)}} = \mathbb{1}$ from the above equation, so we can conclude that $A = \frac{d}{(d,r)}$.

3. The inclusion $\supset$ in equation (1.4.8) follows from the previous item since $\theta_{k_n,d,r}$ has order exactly $d/(d,r)$. Now we show that the sets on both sides of equation (1.4.8) have the same cardinality. We know that $\widehat{k_n^\times}[d]$ has cardinality $\gcd(|k_n^\times|, d)$. On the other hand, the characters $\theta_{k_n,d,r}$ in the set on the right-hand side of (1.4.8) are pairwise distinct (as it can be seen by evaluating them at a generator of $k_n^\times$, see proposition 1.4.14). Note that this implies that the set on the right-hand side of equation (1.4.9) is indeed a disjoint union. But now, we know from items 3 and 4 of proposition 1.4.16 that

$$\#\{\, r \in \mathbb{Z}/d\mathbb{Z} \;:\; u_{|k|,d}(r) \mid n \,\} = \#\{\, r \in \mathbb{Z}/d\mathbb{Z} \;:\; d \mid \#k_n^\times \cdot r \,\} = \gcd(|k_n^\times|, d),$$

which concludes the proof. Finally, in the case $|k| \equiv 1 \pmod d$, one can use item 1 to deduce the claimed description of $\widehat{k_n^\times}[d]$. ■

Remark 1.4.18. We explain here a more concrete approach to proposition 1.4.17, which can be important for computational reasons. Fix a finite field k and a "norm-compatible" family of generators $(\gamma_n)_{n\geqslant 1} \in \prod_{n\geqslant 1} k_n^\times$ in the sense that for any $n \mid N$, we have $\gamma_n = \mathrm{N}_{k_N/k_n}(\gamma_N)$. Such families exist since the norm maps are surjective; in more conceptual terms, if $E_n \subset k_n^\times$ denotes the set of generators of $k_n^\times$, then we have surjective[48] maps given by the (restriction of the) norm $\mathrm{Nr}_{n,N} : E_N \to E_n$ whenever $n \mid N$ and then the projective limit of the inverse system $\big((E_n)_{n\geqslant 1}, (\mathrm{Nr}_{n,N})_{n|N}\big)$ is non-empty.

Fix an integer $d \geqslant 2$, an element $r \in \mathbb{Z}/d\mathbb{Z}$ and an integer $n \in u_{|k|,d}(r)\mathbb{Z}_{>0}$. Then we may define a character $\theta'_{k_n,d,r} \in \widehat{k_n^\times}$ be setting

$$\theta'_{k_n,d,r}(\gamma_n) := \exp\Big(\frac{2\pi i r}{d}\Big). \tag{1.4.10}$$

Note that $\theta'_{k_n,d,r}$ has order exactly $d/(d,r)$ (and it is well-defined because we assumed $n \in u_{|k|,d}(r)\mathbb{Z}_{>0}$). Moreover, if $n \mid N$, then

$$\theta'_{k_N,d,r}(\gamma_N) = \theta'_{k_n,d,r}(\gamma_n) = \theta'_{k_n,d,r}(\mathrm{N}_{k_N/k_n}(\gamma_N))$$

so that the same property as item 1 in proposition 1.4.17 is satisfied. Finally, (1.4.8) also holds if we consider the characters $\theta'_{k_n,d,r}$ instead of $\theta_{k_n,d,r}$; the same proof applies. Therefore, in most of the applications (especially in proposition 1.4.26), we could work with the characters $\theta'_{k_n,d,r}$ instead of $\theta_{k_n,d,r}$. ⌟

Remark 1.4.19. Let us mention that for any finite field k of odd characteristic, the Legendre symbol can be written as $\lambda_k = \theta_{k,2,1}$. If 3 divides $|k^\times|$ (i.e., $|k| \equiv 1 \bmod 3$), then $\theta_{k,3,\pm 1}$ are the two characters of order exactly 3 in $\widehat{k^\times}$. ⌟

[48] We use the fact that for every surjective morphism of cyclic groups $\mathbb{Z}/ab\mathbb{Z} \to \mathbb{Z}/a\mathbb{Z}, [x] \mapsto [dx]$ (with $a, b \geqslant 1$), any generator $[h] \in \mathbb{Z}/a\mathbb{Z}$ can be lifted to a generator of $\mathbb{Z}/ab\mathbb{Z}$. First, we may assume that the surjective morphism is given by a canonical quotient map, since $\gcd(d, a) = 1$. Without loss of generality we can suppose that $\gcd(a, b) = 1$. Then we just use Chinese remainder theorem.

Concretely, in SAGE [The21], the command `GF(q).multiplicative_generator()` can be used to get norm-compatible families of generators. In practice (e.g., in proposition 1.4.26) we may assume that $n = u_{|k|,d}(r)$ divides $\phi(d)$ for some fixed integer $d \geqslant 1$.

1.4.2.2 Stickelberger's theorem

It is clear that given a finite field k and any multiplicative characters $\chi_1, ..., \chi_n \in \widehat{k^\times}$ of order dividing some integer $D \geqslant 2$ (for instance $D = |k^\times|$), the Jacobi sum $J(\chi_1, ..., \chi_n) \in \mathbb{Z}[\zeta_D]$ is an algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_D)$. An important question is to know how the principal ideal generated by $J(\chi_1, ..., \chi_n)$ decomposes as a product of prime ideals. The answer is given by Stickelberger theorem 1.4.22, stated below, which requires the following notations.

Definition 1.4.20. Let us fix a prime p and a primitive D-root of unity ζ_D, where $D \geqslant 2$ is coprime to p. Fix a power $q = p^e$ of p.

1. We denote by $\mathfrak{p} = P \cap \mathbb{Z}[\zeta_D]$ the prime ideal of $\mathbb{Z}[\zeta_D]$ above p which is below the maximal ideal $P \trianglelefteq \overline{\mathbb{Z}}$ used in definition 1.4.12. For any $t \in (\mathbb{Z}/D\mathbb{Z})^\times$, we define $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ to be the unique element such that $\sigma_t(\zeta_D) = \zeta_D^t$.

2. We define the character
$$\omega_{q,D} := \theta_{\mathbb{F}_{q^m},D,1} : \mathbb{F}_{q^m}^\times \longrightarrow \overline{\mathbb{Q}}^\times$$
where $m := u_{q,D}(1) = \mathrm{ord}^\times(q \bmod D)$.

3. Given a vector $\vec{b} = (b_1, ..., b_n) \in (\mathbb{Z}/D\mathbb{Z} \smallsetminus \{0\})^n$, we define
$$\beta(\vec{b}) = \beta_{q,D}(\vec{b}) := \sum_{j=0}^{f-1} \Big(-1 + \sum_{i=1}^{n+1} \left\{ \frac{-b_i \cdot p^j}{D} \right\} \Big)$$
where $b_{n+1} := -\sum_{i=1}^n b_i$, $f \geqslant 1$ is such that $p^f = q^{\mathrm{ord}^\times(q \bmod D)}$ (that is, $f = e \cdot \mathrm{ord}^\times(q \bmod D)$) and $\{x\}$ is the fractional part of x as in definition 1.4.1. ⌟

Remark 1.4.21. 1. We note that $\omega_{q,D}$ is a character of order exactly D on $\mathbb{F}_{q^{\mathrm{ord}(q \bmod D)}}^\times$ by proposition 1.4.17.

2. Moreover, given an integer $d \geqslant 1$ coprime to q and $r \in \mathbb{Z}/d\mathbb{Z}$, we set $D := \frac{d}{\gcd(d,r)}$ so that $n := u_{q,d}(r) = u_{q,D}(1)$ by proposition 1.4.16.1. Then we find
$$\theta_{\mathbb{F}_{q^n},d,r} = \Theta^{\frac{(q^n-1)\cdot r}{d}} = \Theta^{\frac{(q^n-1)\cdot r/\gcd(d,r)}{D}} = \omega_{q,D}^{\frac{r}{\gcd(d,r)}}. \tag{1.4.11}$$

3. It can be checked that $\beta(\vec{b})$ is an *integer* (see [Gri16, remarque 3.3.4]). ⌟

We are now ready to state how the principal ideal generated by a Jacobi sum decomposes into a product of prime ideals.

Theorem 1.4.22 (Stickelberger). *Let $q = p^e$ be a power of a prime p, where $e \geqslant 1$. Let $D \geqslant 2$ be coprime to p and let $\vec{a} = (a_1, ..., a_n) \in (\mathbb{Z}/D\mathbb{Z} \smallsetminus \{0\})^n$ be such that $\sum_{i=1}^n a_i \neq 0$. Then, using the notations from definition 1.4.20, we have*
$$J(\omega_{q,D}^{a_1}, ..., \omega_{q,D}^{a_n})\mathbb{Z}[\zeta_D] = \prod_{[t] \in (\mathbb{Z}/D\mathbb{Z})^\times/\langle p \rangle^\times} \sigma_{t^{-1}}(\mathfrak{p})^{\beta_{q,D}(t \cdot \vec{a})}$$ ⌟

Proof. — See [Gri16, théorème 3.3.9] (the result is deduced, using proposition 1.4.6, from a similar statement about Gauss sums; see also [BEW98, theorems 11.2.2, 11.2.3] or [Coh07, proposition 3.6.10]). ■

Remark 1.4.23. We check that the product over $[t] \in (\mathbb{Z}/D\mathbb{Z})^\times/\langle p\rangle^\times$ appearing in theorem 1.4.22 is well-defined in the sense that the factors do not depend on which representative $t \in (\mathbb{Z}/D\mathbb{Z})^\times$ we choose.

Namely, we have $\beta_{q,D}(p\vec{b}) = \beta_{q,D}(\vec{b})$ (this is clear since β is defined using a sum over elements in $\langle p\rangle \leqslant (\mathbb{Z}/D\mathbb{Z})^\times$, repeated $\frac{e}{\gcd(\mathrm{ord}(p \bmod D),e)}$ times) and $\sigma_p(\mathfrak{p}) = \mathfrak{p}$ (because σ_p is the Frobenius element at $\mathfrak{p}$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$; it actually generates the decomposition subgroup at $\mathfrak{p}$ which is the stabilizer of $\mathfrak{p}$ under the action of the Galois group). ⌟

Stickelberger's result will be important to us in the following way. In a nutshell, it gives an upper bound on the geometric rank of *some* elliptic curves. If the L-function of an elliptic curve E over a global function field $K = k(C)$ is expressed as a product $L(E/K,T) = \prod_{j=1}^{d}(1-\alpha_j T)$, then computing the order of vanishing of this L-function at $T = |k|^{-1}$ amounts to counting how many α_j are equal to $|k|$. All such α_j are rational (and conversely, if $\alpha_j \in \mathbb{Q}$ then $\alpha_j = \pm|k|$ by theorem 1.3.30), and thus the ideal $(\alpha_j) \trianglelefteq \mathbb{Z}[\zeta_{q-1}]$ is Galois-invariant (but not conversely; we miss roots of unity by passing to the ideal!). If the α_j's are related to Jacobi sums, then we see that Stickelberger's theorem 1.4.22 tells us how this principal ideal factors into prime ideals. For more details, see section 4.2 in chapter 4.

1.4.3 Characters and L-functions

A general strategy to compute the L-function of an elliptic curve E over $k(t)$ is to first *try* to express it via character sums. Namely, we *wish* to find some integers $d \geqslant 1$, $\delta \mid d$ and a function (using the notations from definition 1.4.1)

$$\alpha : \bigsqcup_{n\geqslant 1} \widehat{k_n^\times}[d] \longrightarrow \mathbb{C}$$

satisfying some properties (stated in proposition 1.4.26) and such that

$$\log L(E/k(t),T) = -\sum_{n\geqslant 1}\left(\sum_{\chi\in \widehat{k_n^\times}[d]\smallsetminus\widehat{k_n^\times}[\delta]} \alpha(\chi)\right)\frac{T^n}{n}. \tag{1.4.12}$$

Remark 1.4.24. We point out that it is *not* always possible to take α so that its image lies in the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_n; n \geqslant 1)$ of $\mathbb{Q}$ (which would be reasonable to have if α is defined in terms of character sums like Jacobi sums, for instance). Here is a concrete example inspired by [Ulm07a, §6.5]. We take $p = 5, d = 3, k = \mathbb{F}_p$ and we consider the elliptic curve

$$E : y^2 = x^3 + (t^d-1)^4 x + (t^d+1)(t^d-1)^5 \tag{1.4.13}$$

over $K = \mathbb{F}_p(t)$. The L-function of E over K is $390625T^8 - 2500T^6 - 150T^4 - 4T^2 + 1 \in \mathbb{Z}[T]$ which is an irreducible polynomial, and the Galois group of its splitting field is a non-abelian group of order 16 (e.g., using MAGMA [BCP97]), so its roots cannot lie in some cyclotomic field, in particular they cannot be sums of roots of unity. ⌟

Remark 1.4.25. Assume that at each place $v \in V_K \smallsetminus \{v_\infty\} \simeq |\mathbb{A}^1_k|$, the elliptic curve E has a minimal integral Weierstrass model of the form $y^2 = f_v(x,t)$ for some monic polynomial $f_v(x,t) \in K[t,x]$ of degree 3 in x. Then proposition 1.3.29 allows us to write

$$\log L(E/K,T) = \sum_{j \geqslant 1} \left(A_E(v_\infty, j) - \sum_{x,t \in k_j} \lambda_{k_j}(f_v(x,t)) \right) \frac{T^j}{j}.$$

If we have $f_v(x,t) = g_v(x,t^d)$ for some polynomials g_v and some integer $d \geqslant 1$ coprime to $\mathrm{char}(k)$ (independent of v), then we may use proposition 1.4.3 to get an expression of the L-function as in equation (1.4.12). ⌟

The following result, which is proved (with different notations) in [Gri16, Proposition 2.1.15], will be essential to express the L-function $L(E/k(t),T)$ of some elliptic curves E over $k(t)$ as a *polynomial* (as in theorem 1.3.30) with explicit roots, which will then allow to determine the order of vanishing at $T = |k|^{-1}$.

Proposition 1.4.26. *Fix a finite field k and two integers $d, \delta \geqslant 1$ coprime to $|k|$ such that $\delta \mid d$. Assume that we have a map*

$$\alpha : \bigsqcup_{n \geqslant 1} \widehat{k_n^\times}[d] \longrightarrow \mathbb{C}$$

satisfying the following two properties:

1. *(Compatibility with the Frobenius morphism). For every $n \geqslant 1$ and every $\chi \in \widehat{k_n^\times}[d]$, one has $\alpha(\chi) = \alpha(\chi^{|k|})$.*
2. *(Hasse–Davenport relation). For every finite extensions $L \supset F \supset k$ of k and any character $\chi \in \widehat{F^\times}[d]$, we have $\alpha(\chi \circ \mathrm{N}_{L/F}) = \alpha(\chi)^{[L:F]}$.*

Then the following identity holds in $\mathbb{C}[\![T]\!]$:

$$\sum_{n \geqslant 1} \left(\sum_{\chi \in \widehat{k_n^\times}[d] \smallsetminus \widehat{k_n^\times}[\delta]} \alpha(\chi) \right) \frac{T^n}{n} = - \sum_{[r] \in (\mathbb{Z}/d\mathbb{Z} \smallsetminus \frac{d}{\delta}\mathbb{Z}/d\mathbb{Z})/\langle |k| \rangle^\times} \log\left(1 - \alpha(\theta_{k_{u(r)},d,r}) T^{u(r)}\right) \tag{1.4.14}$$

where $u(r) := u_{|k|,d}(r)$ is as in definition 1.4.15. The sum on the right-hand side runs over the orbits of the action of the group $\langle |k| \rangle^\times \leqslant (\mathbb{Z}/d\mathbb{Z})^\times$ of powers of $|k|$ on $\mathbb{Z}/d\mathbb{Z} \smallsetminus \frac{d}{\delta}\mathbb{Z}/d\mathbb{Z}$ (note that d is coprime to $|k|$ so $|k|$ is invertible in $\mathbb{Z}/d\mathbb{Z}$). ⌟

Proof. — We first point out that the right-hand side of equation (1.4.14) is well-defined. Namely, we show that $1 + \alpha(\theta_{k_{u(r)},d,r}) T^{u(r)}$ is independent of the representative of the orbit $[r] = \{\, |k|^j \cdot r \ : \ j \in \mathbb{Z} \,\} \subset \mathbb{Z}/d\mathbb{Z}$. First of all, proposition 1.4.16.2 indicates that $u(r) = u(|k|^j r)$ for any $j \in \mathbb{Z}$. While the character $\theta_{k_{u(r)},d,r}$ might depend on the choice of a representative r, the value $\alpha(\theta_{k_{u(r)},d,r})$ only depends on the orbit $[r]$. Indeed, it is clear that $\theta_{k_{u(qr)},d,qr} = \theta^q_{k_{u(r)},d,r}$, where $q := |k|$. Then, from hypothesis 1 on α, one deduces that

$$\alpha(\theta_{k_{u(q^j r)},d,q^j r}) = \alpha(\theta_{k_{u(r)},d,r})$$

holds for every $j \in \mathbb{Z}$.

Now we compute the series on the left-hand side of equation (1.4.14), mainly using proposition 1.4.17. First, notice that given $r' \in \mathbb{Z}/\delta\mathbb{Z}$, we have

$$u_{|k|,\delta}(r') = \mathrm{ord}^{\times}\Big(|k| \bmod \frac{\delta}{(\delta, r')}\Big) = \mathrm{ord}^{\times}\Big(|k| \bmod \frac{d}{(\delta, r') \cdot d/\delta}\Big) = u_{|k|,d}(\frac{d}{\delta}r')$$

and for each $n \in u_{|k|,\delta}(r')\mathbb{Z}_{>0}$ we have

$$\theta_{k_n,\delta,r'} = \Theta^{|k_n^{\times}|\cdot r'/\delta} = \Theta^{|k_n^{\times}|\cdot r'\cdot \frac{d}{\delta}/d} = \theta_{k_n,d,\frac{d}{\delta}r'}$$

Therefore, the elements $r' \in \mathbb{Z}/\delta\mathbb{Z}$ can be replaced by $r = \frac{d}{\delta}r' \in \frac{d}{\delta}\mathbb{Z}/d\mathbb{Z}$ and we compute:

$$\begin{aligned}
\sum_{n\geqslant 1}\Bigg(\sum_{\chi\in\widehat{k_n^{\times}}[d]\smallsetminus\widehat{k_n^{\times}}[\delta]}\alpha(\chi)\Bigg)\frac{T^n}{n} &= \sum_{r\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\frac{d}{\delta}\mathbb{Z}/d\mathbb{Z}}\Bigg(\sum_{n\in u_{|k|,d}(r)\mathbb{Z}_{>0}}\alpha(\theta_{k_n,d,r})\Bigg)\frac{T^n}{n} && (\star)\\
&= \sum_{r\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\frac{d}{\delta}\mathbb{Z}/d\mathbb{Z}}\sum_{\nu\geqslant 1}\alpha(\theta_{k_{u(r)\cdot\nu},d,r})\frac{T^{u(r)\cdot\nu}}{u(r)\cdot\nu}\\
&= \sum_{r\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\frac{d}{\delta}\mathbb{Z}/d\mathbb{Z}}\sum_{\nu\geqslant 1}\alpha(\theta_{k_{u(r)},d,r}\circ \mathrm{N}_{k_{u(r)\nu}/k_{u(r)}})\frac{T^{u(r)\cdot\nu}}{u(r)\cdot\nu} && (\star\star)\\
&= \sum_{r\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\frac{d}{\delta}\mathbb{Z}/d\mathbb{Z}}\sum_{\nu\geqslant 1}\alpha(\theta_{k_{u(r)},d,r})^{\nu}\frac{T^{u(r)\cdot\nu}}{u(r)\cdot\nu} && (\diamondsuit)\\
&= \sum_{r\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\frac{d}{\delta}\mathbb{Z}/d\mathbb{Z}}\Bigg[\sum_{\nu\geqslant 1}\frac{\big(\alpha(\theta_{k_{u(r)},d,r})T^{u(r)}\big)^{\nu}}{u(r)\cdot\nu}\Bigg]\\
&= -\sum_{r\in\mathbb{Z}/d\mathbb{Z}\smallsetminus\frac{d}{\delta}\mathbb{Z}/d\mathbb{Z}}\frac{1}{u(r)}\log\Big(1-\alpha(\theta_{k_{u(r)},d,r})T^{u(r)}\Big) && (\triangle)\\
&= -\sum_{[r]\in(\mathbb{Z}/d\mathbb{Z}\smallsetminus\frac{d}{\delta}\mathbb{Z}/d\mathbb{Z})/\langle|k|\rangle}\log\Big(1-\alpha(\theta_{k_{u(r)},d,r})T^{u(r)}\Big)
\end{aligned}$$

where the last step follows because $u_{|k|,d}(r)$ is (by definition) the cardinality of the orbit $[r]$ of $r \in \mathbb{Z}/d\mathbb{Z}$ under the action of the powers of $|k|$ on $\mathbb{Z}/d\mathbb{Z}$. Equality $(\star)$ uses proposition 1.4.17.3, $(\star\star)$ uses proposition 1.4.17.1, $(\diamondsuit)$ uses hypothesis 2 on α, and $(\triangle)$ uses the identity $\log(1-aT) = -\sum_{\nu\geqslant 1}(aT)^{\nu}/\nu$. ■

The following lemma determines explicitly the number of factors appearing in equation (1.4.14).

Lemma 1.4.27. *Let $a, n \geqslant 2$ be two coprime integers, and let the cyclic group $\langle a\rangle^{\times} \subset (\mathbb{Z}/n\mathbb{Z})^{\times}$ of powers of a act on the set $\mathbb{Z}/n\mathbb{Z}$. Then*

1. The number of orbits for this action is equal to

$$\Big|\mathbb{Z}/n\mathbb{Z}\Big/\langle a\rangle^{\times}\Big| = \sum_{e|n}\frac{\phi(e)}{\mathrm{ord}^{\times}(a \bmod e)} = \sum_{e|n}[(\mathbb{Z}/e\mathbb{Z})^{\times} : \langle a\rangle^{\times}].$$

2. Moreover, we have $\Big|\mathbb{Z}/(a+1)\mathbb{Z}\Big/\langle a\rangle^{\times}\Big| = g + \frac{a+1-g}{2}$ where $g := \gcd(a-1, 2)$ and $\Big|\mathbb{Z}/(a+1)\mathbb{Z}\Big/\langle a^2\rangle^{\times}\Big| = a+1$. More generally, $\Big|\mathbb{Z}/n\mathbb{Z}\Big/\langle a\rangle^{\times}\Big| \geqslant \frac{n}{\mathrm{ord}^{\times}(a \bmod n)}$.

3. *Assume that $n = a^\ell + 1$ where ℓ is either some odd prime. Define $g := \gcd(a-1, 2)$. Then*
$$\left|\mathbb{Z}/n\mathbb{Z}\Big/\langle a\rangle^\times\right| = g \ + \ \frac{a+1-g}{2} \ + \ \frac{a^\ell - a}{2\ell}.$$ ⌟

Proof. — 1. First, note that the additive order of any element $x \in \mathbb{Z}/n\mathbb{Z}$ is a divisor e of n. We claim that if the *additive* order of x equals $\mathrm{ord}^+(x \bmod n) = e$, then the orbit of x has size $|\operatorname{orb}(x)| = \mathrm{ord}^\times(a \bmod e)$ equal to the *multiplicative* order of a mod e. Then the formula will immediately follow since given a group action $G \curvearrowright X$, the number of orbits is $|X/G| = \sum_{A\in X/G} 1 = \sum_{A\in X/G}\sum_{x\in A}\frac{1}{|A|} = \sum_{x\in X}\frac{1}{|\operatorname{orb}(x)|}$.

The orbit of x is $\{x, ax, a^2x, a^3x, ...\} \subset \mathbb{Z}/n\mathbb{Z}$. Since $ex \equiv 0 \pmod n$ and $a^{\mathrm{ord}^\times(a \bmod e)} = 1 + e\alpha$ for some $\alpha \in \mathbb{Z}$, we get $a^{\mathrm{ord}^\times(a \bmod e)}x \equiv x \pmod n$, so the orbit has size at most $\mathrm{ord}^\times(a \bmod e)$. In fact we have

$$a^j x \equiv x \pmod n \iff a^j - 1 \equiv 0 \pmod e \iff \mathrm{ord}^\times(a \bmod e) \mid j,$$

so this proves $|\operatorname{orb}(x)| = \mathrm{ord}^\times(a \bmod e)$. (We note that $e = \frac{n}{\gcd(x,n)}$, so we can generalize the proof of proposition 1.4.16.1 to conclude that $|\operatorname{orb}(x)| = \mathrm{ord}^\times(a \bmod e)$).

2. Assume now that $n = a + 1$. Then $a \equiv -1 \bmod n$ implies that all the orbits have size 2, except the orbits of $x \in \mathbb{Z}/n\mathbb{Z}$ such that $x \equiv -x$, i.e. $x \equiv 0$ or $x \equiv \frac{n}{2}$ if a is odd (i.e., $g = 2$). Thus, if a is even we have $\frac{a}{2} + 1$ orbits and if a is odd we have $\frac{a-1}{2} + 2$ orbits, which shows the claim.

The second identity is obvious: $\langle a^2\rangle$ acts trivially on $\mathbb{Z}/(a+1)\mathbb{Z}$ since $a^2 \equiv 1 \bmod (a+1)$.

The last inequality follows from the fact that we have a reduction map $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/e\mathbb{Z})^\times$ for any divisor $e \mid n$, and this implies that $\mathrm{ord}^\times(a \bmod e) \mid \mathrm{ord}^\times(a \bmod n)$. Now it suffices to recall that $\sum_{e|n}\phi(e) = n$.

3. We start with the case where ℓ is an odd prime. Consider the action $\mathbb{Z} \curvearrowright \mathbb{Z}/n\mathbb{Z}$ defined by $j \cdot x := a^j x$ for all $j \in \mathbb{Z}$. We have $a^\ell x \equiv -x \mod n$ for all $x \in \mathbb{Z}/n\mathbb{Z}$ (since $n = a^\ell + 1$), so $a^{2\ell}x \equiv x \mod n$, which implies that the action factors through $\mathbb{Z}/2\ell\mathbb{Z} \curvearrowright \mathbb{Z}/n\mathbb{Z}$. In particular, all orbits have size dividing 2ℓ. Since ℓ is prime, the sizes are among $\{1, 2, \ell, 2\ell\}$. Given $k \geqslant 1$, let

$$a_k := \#\{\, x \in \mathbb{Z}/n\mathbb{Z} \ : \ a^k x \equiv x \mod n \,\}, \qquad A_k := \#\{\, x \in \mathbb{Z}/n\mathbb{Z} \ : \ |\operatorname{orb}(x)| = k \,\},$$

so that the number of orbits of size k is $\dfrac{1}{k}A_k$. We have (by inclusion-exclusion principle)

$$A_1 = a_1, \quad A_2 = a_2 - a_1, \quad A_\ell = a_\ell - a_1, \quad A_{2\ell} = a_{2\ell} - a_\ell - a_2 + a_1,$$

since ℓ is an *odd* prime. Moreover, define the endomorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $f(x) := (a^k - 1)x$. We have

$$a_k = \#\ker(f) = \frac{n}{\#\operatorname{Im}(f)} = \frac{n}{[(a^k-1)\mathbb{Z} + n\mathbb{Z} : n\mathbb{Z}]} = \frac{n}{n/\gcd(n, a^k-1)} = \gcd(n, a^k - 1).$$

One concludes that

$$a_1 = \gcd(a^\ell + 1, q - 1) = \gcd\Big(\frac{a^\ell - 1}{a-1}(a-1) + 2, a - 1\Big) = \gcd(a-1, 2),$$

$$a_2 = \gcd(a^\ell + 1, a^2 - 1) \overset{\ell \text{ odd}}{=} \gcd\left(a\left(\tfrac{a^{\ell-1}-1}{a^2-1}(a^2-1)+1\right)+1, a^2-1\right) = a+1,$$
$$a_\ell = \gcd(a^\ell + 1, a^\ell - 1) = \gcd(a^\ell + 1, 2) = \gcd(a-1, 2),$$
$$a_{2\ell} = \gcd(a^\ell + 1, a^{2\ell} - 1) = a^\ell + 1.$$

Hence the total number of orbits is

$$\left|\mathbb{Z}/n\mathbb{Z}\Big/\langle a\rangle^\times\right| = \sum_{k\in\{1,2,\ell,2\ell\}} \frac{A_k}{k} = g \;+\; \frac{a+1-g}{2} \;+\; 0 \;+\; \frac{a^\ell - a}{2\ell},$$

where $g := \gcd(a-1, 2)$ as desired.

(Note also that in general if $a = q$ is a prime power and $\gcd(n, q) = 1$, the number of $\langle q\rangle^\times$-orbits on $\mathbb{Z}/n\mathbb{Z}$ is the number of irreducible factors of $X^n - 1$ in $\mathbb{F}_q[X]$: such a factor corresponds to a Galois-orbit of an n-th root of unity in $\mathbb{F}_q^\times$, and $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is generated by $\mathrm{Fr}_q : x \mapsto x^q$ whose iterates are given by powers of q, namely $\mathrm{Fr}_q^j : x \mapsto x^{q^j}$). ■

1.4.4 Explicit Jacobi sums

We now give some examples where the hypothesis of Tate–Shafarevich's theorem 1.4.8 are fulfilled. To this end, we start with a small lemma.

Lemma 1.4.28. *Let $a \geqslant 2, \nu \geqslant 1$ be integers and D be a divisor of $a^\nu + 1$ (in particular, $\gcd(a, D) = 1$). Assume that $D \geqslant 3$. Then:*

1. *The multiplicative order $\mathrm{ord}(a) := \mathrm{ord}^\times(a \bmod D)$ of a modulo D is even and*
$$a^{\mathrm{ord}(a)/2} \equiv -1 \pmod{D}.$$
2. *Moreover, $\dfrac{\mathrm{ord}(a)}{2}$ divides ν and the ratio $\dfrac{\nu}{\mathrm{ord}(a)/2}$ is odd.*
3. *Finally, we have*
$$\frac{a^{\mathrm{ord}(a)} - 1}{D \cdot (a-1)} \in \mathbb{Z}.$$ ⌟

Proof. — We prove the first two items simultaneously. Let us write $\mathrm{ord}(a) = 2\alpha + \epsilon$ for some $\alpha \geqslant 1$ and $\epsilon \in \{0, 1\}$. Then

$$1 \equiv a^{\mathrm{ord}(a)\cdot\nu} = (a^\nu)^{2\alpha+\epsilon} \equiv (-1)^{2\alpha+\epsilon} \equiv (-1)^\epsilon \pmod{D}$$

and since $D \geqslant 3$, this implies that $\epsilon = 0$, i.e. $\mathrm{ord}(a)$ is even.

Moreover, we know that $a^{2\nu} \equiv 1 \pmod{D}$, so the order of a divides 2ν, which means that $\nu = \alpha\nu_1$ for some integer $\nu_1 \geqslant 1$. Let us write $\nu_1 = 2\nu' + \epsilon'$ for some $\nu' \geqslant 0$ and $\epsilon' \in \{0, 1\}$. Then

$$-1 \equiv a^\nu = (a^\alpha)^{2\nu'+\epsilon'} = 1^{\nu'} \cdot a^{\alpha\epsilon'} \pmod{D},$$

which means (again because $D \geqslant 3$) that $\epsilon' = 1$ and $a^\alpha = a^{\mathrm{ord}(a)/2} \equiv -1 \pmod{D}$ as desired. This also proves that $\nu = \frac{\mathrm{ord}(a)}{2} \cdot \nu_1$ for some *odd* integer $\nu_1 \geqslant 1$.

Finally let us check that $\frac{a^{\mathrm{ord}(a)}-1}{D\cdot(a-1)}$ is an integer. From item 1, we know that $\mathrm{ord}(a)=2\alpha$ is even and that $a^\alpha \equiv -1 \pmod D$. Now, we have

$$\frac{a^{\mathrm{ord}(a)}-1}{a-1} = \sum_{i=0}^{\mathrm{ord}(a)-1} a^i \equiv \sum_{i=1}^{\alpha} a^i + \sum_{i=\alpha+1}^{2\alpha} a^i \equiv \sum_{i=1}^{\alpha} a^i + \sum_{i=1}^{\alpha}(-a^i) = 0 \pmod D,$$

which confirms that $\frac{a^{\mathrm{ord}(a)}-1}{a-1}$ is an integer divisible by D. ■

We get the following corollary.

Corollary 1.4.29. *Let $d \geqslant 1$ be an integer and $r \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ such that $r \neq \frac{d}{2}$ if d is even. Let k be a finite field. Assume that[49] there is some integer $\nu \geqslant 1$ such that $|k|^\nu \equiv -1 \pmod d$.*

Then $u(r) := u_{|k|,d}(r)$ is even, so that $k_{u(r)}$ has a (unique) quadratic subfield. Moreover, the restriction of the non-trivial character $\theta_{k_{u(r)},d,r}$ to this quadratic subfield is trivial. ⌟

Proof. —

- Since $r \neq 0, d/2 \bmod d$, we have $D := \frac{d}{(d,r)} \geqslant 3$ and by proposition 1.4.16 we have $u_{|k|,d}(r) = \mathrm{ord}^\times(|k| \bmod D)$. Since $|k|^\nu \equiv -1 \bmod d$, we also have $|k|^\nu \equiv -1 \bmod D$ and so we may apply lemma 1.4.28, which asserts that $u(r) := u_{|k|,d}(r) \in 2\mathbb{Z}$ is even and that $|k|^{u(r)/2}+1 \equiv 0 \pmod D$. From proposition 1.4.16.4 we get

$$r\cdot(q^{u_{q,d}(r)/2}+1) \equiv 0 \pmod d. \tag{1.4.15}$$

- We now prove that $\theta := \theta_{k_{u(r)},d,r}$ is trivial on $k^\times_{u(r)/2}$. Note also that $\theta_{k_{u(r)},d,r}$ is non-trivial on $k_{u(r)}$, since $r \not\equiv 0 \pmod d$, by proposition 1.4.17.2. Now, there is a unique generator g of $k^\times_{u(r)}$ such that $\theta(g) = \exp(2\pi i r/d)$ by proposition 1.4.14. Note that $g' := g^{q^{u(r)/2}+1} = \mathrm{N}_{k_{u(r)}/k_{u(r)/2}}(g)$ is a generator of $k^\times_{u(r)/2}$. We have

$$\theta(g') = \exp\Big(\frac{2\pi i r}{d}(q^{u(r)/2}+1)\Big) = 1 \tag{1.4.16}$$

  where the second equality follows from equation (1.4.15). This concludes the proof. ■

We can generalize slightly the above results to get the following. The point is that we do not assume that $|k|^\nu \equiv -1 \pmod d$ but only $p^\nu \equiv -1 \pmod d$ (for some $\nu \geqslant 1$).

Lemma 1.4.30. *Let p be any prime, $d, e \geqslant 1$ be integers, set $k = \mathbb{F}_{p^e}$ and let $r \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ such that $r \neq d/2$ if d is even. Set $\theta := \theta_{k_{u(r)},d,r}$ where $u(r) := u_{|k|,d}(r)$.*

Assume that $p^\nu \equiv -1 \bmod d$ for some integer $\nu \geqslant 1$. Then:

1. *For any $M \geqslant 2$ there is a sign $\epsilon \in \{\pm 1\}$ such that for any $a_1, ..., a_M \in \mathbb{Z}/\frac{d}{(d,r)}\mathbb{Z} \smallsetminus \{0\}$ satisfying $a_1 + \cdots + a_m \neq 0$, we have*

$$J(\theta^{a_1}, ..., \theta^{a_M}) = \epsilon \cdot |k|^{(M-1)\cdot u(r)/2}.$$

   Moreover, we may take $\epsilon = +1$ if M is odd.

[49] For instance, this is fulfilled if $k = \mathbb{F}_{p^e}$ for some prime p and some *odd* integer $e \geqslant 1$ such that there is some integer $\nu' \geqslant 1$ satisfying $p^{\nu'} \equiv -1 \pmod d$.

2. *If $k' \subset k$ is a subfield such that the degree $c := [k' : \mathbb{F}_p]$ is* odd[50]*, then the restriction of θ to k' is trivial and the degree $[k_{u(r)} : k']$ is even.* ⌟

Proof. — 1. Here we may not be able[51] to use the Tate–Shafarevich theorem 1.4.8 directly on θ (unless we assume that e divides ν which implies $|k|^\nu \equiv -1 \bmod d$, in which case corollary 1.4.29 applies). But we will use Tate–Shafarevich theorem 1.4.8 on a different character and then apply the Hasse–Davenport relation (theorem 1.4.7).

Namely, we apply corollary 1.4.29 to $k' = \mathbb{F}_p$ in order to get that $u'(r) := u_{p,d}(r)$ is even and $\theta' := \theta_{k'_{u'(r)},d,r}$ is trivial on the quadratic subfield of $k'_{u'(r)}$. Then so is θ'^{a_i} for any $1 \leqslant i \leqslant M$. Note that none of the θ'^{a_i} nor $\theta'^{a_1+\cdots+a_M}$ are trivial on $k'_{u'(r)}$ since $a_i \not\equiv 0 \not\equiv a_1 + \cdots + a_m \bmod \frac{d}{(d,r)}$ and θ' has order $\frac{d}{(d,r)}$. By theorem 1.4.8, we find

$$J(\theta'^{a_1}, ..., \theta'^{a_M}) = p^{(M-1)\cdot u'(r)/2}$$

Now, we compute

$$[k_{u(r)} : \mathbb{F}_p] = e \cdot u_{|k|,d}(r) = e \cdot \operatorname{ord}\left(p^e \bmod \frac{d}{(d,r)}\right) = \frac{e}{\gcd(e, u_{p,d}(r))} \cdot u_{p,d}(r). \quad (1.4.17)$$

Hence $k_{u(r)}$ is an extension of $k'_{u'(r)}$ of degree

$$n := \frac{e}{\gcd(e, u_{p,d}(r))}.$$

Thus, theorem 1.4.7 together with proposition 1.4.17.1 yield

$$J(\theta^{a_1}, ..., \theta^{a_M}) = (-1)^{(n-1)(M-1)} p^{(M-1)\cdot n\cdot u'(r)/2} = (-1)^{(n-1)(M-1)} |k|^{(M-1)\cdot u(r)/2} \quad (1.4.18)$$

which concludes the proof, by setting $\epsilon := (-1)^{(n-1)(M-1)}$ (which does not depend on the a_i's).

2. Since $k' = \mathbb{F}_{p^c}$ is a subfield of $k = \mathbb{F}_{p^e}$, we may write $e = c \cdot e'$ for some $e' \geqslant 1$. By proposition 1.4.14, there is a unique generator $g \in k^\times_{u(r)}$ such that $\theta(g) = \exp(2\pi i r/d)$. Now, $g' := \mathrm{N}_{k/k'}(g) = g^{|k^\times|/|k'^\times|}$ is a generator of $k'^\times$ and

$$\theta(g') = \exp(2\pi i X), \qquad X := \frac{r \cdot (p^{ce'u(r)} - 1)}{d \cdot (p^c - 1)}$$

so we want to prove that $X \in \mathbb{Z}$. Let $a := p^c$ and $D := \frac{d}{(d,r)}$; we have $D \geqslant 3$ in view of the hypothesis on r. We have

$$X = \frac{r}{(d,r)} \cdot \frac{a^{e' \operatorname{ord}(a^{e'} \bmod D)} - 1}{D \cdot (a-1)}.$$

[50] The character θ does not need to be trivial on k' if c is even. For instance, if $k = \mathbb{F}_{2^4}$ and g is a generator of $k^\times$ such that $\theta_{k,3,1}(g) = \exp(2\pi i/3)$, then $k'^\times = \mathbb{F}_{2^2}^\times$ is generated by g^5 and $\theta_{k,3,1}(g^5) = \exp(10\pi i/3) \neq 1$.

[51] It is always true that $e \cdot u_{|k|,d}(r)$ is even (i.e., $k_{u(r)}$ has a quadratic subfield), but when $4 \mid e$, it may not be true that $d \mid r \cdot (|k|^{u(r)/2} + 1)$ which is needed for the triviality of θ over that quadratic subfield. For instance, take $p = 2, d = 3, r = 1, |k| = p^4$: we have $u_{|k|,d}(r) = 1$ and $d \nmid (p^2 + 1)$.

Now, observe that $a^{e' \operatorname{ord}(a^{e'} \bmod D)} - 1$ is an integer multiple of $a^{\operatorname{ord}(a \bmod D)} - 1$ and that $a^\nu = (p^\nu)^c \equiv -1 \mod D$ because c is *odd*. Henceforth lemma 1.4.28 allows us to conclude that $X \in \mathbb{Z}$ as desired. Finally, from equation (1.4.17) and the fact that $u_{p,d}(r)$ is even (as seen above), we deduce that $e \cdot u_{|k|,d}(r) = c \cdot e' \cdot u(r)$ is even. Since c is odd, this means that $[k_{u(r)} : k'] = e' \cdot u(r)$ is even, which finishes the proof. ■

We will also need the following generalization of corollary 1.4.29.

Lemma 1.4.31. *Let $d \geqslant 1$ be an integer, let $\delta \mid d$ be a divisor of d and let $r \in \mathbb{Z}/d\mathbb{Z}$ be such that r is not a multiple of $\frac{\delta}{\gcd(\delta,2)}$ and is a multiple of $\frac{d}{\delta}$. Let $k = \mathbb{F}_q$ be a finite field with q elements. Assume that there is some integer $\nu \geqslant 1$ such that $q^\nu \equiv -1 \pmod{\delta}$.*

Then $u(r) := u_{q,d}(r)$ is even and

$$q^{u(r)/2} \equiv -1 \mod \tfrac{d}{(d,r)}$$

and the restriction of character $\theta_{k_{u(r)},d,r}$ to $k^\times_{u(r)/2}$ is trivial. ⌟

Proof. — The assumption implies that $q^\nu \equiv -1 \bmod \delta'$ where $\delta' := \frac{\delta}{(\delta,r)}$. Note that $\delta' \geqslant 3$, because $\delta' = 1$ would give that $\delta \mid r$, and $\delta' = 2$ would give that δ is even and $\delta/2$ divides r. Both cases are excluded by hypothesis.

Then by lemma 1.4.28, we deduce that the multiplicative order $\operatorname{ord}^\times(q \bmod \delta')$ of $q \bmod \delta'$ is even. We claim that δ' divides $\frac{d}{(d,r)}$, from which we can easily conclude that $u_{q,d}(r) = \operatorname{ord}^\times(q \bmod \frac{d}{(d,r)})$ is even. As far as the divisibility is concerned, the hypothesis ensures that we can write $r = \frac{d}{\delta} r'$ for some integer $r' \geqslant 1$. Then $d \cdot (\delta, r) = d \cdot (\delta, \frac{d}{\delta} r')$ is a multiple of

$$d \cdot (\delta, r') = (d\delta, dr') = (d\delta, r\delta) = \delta \cdot (d, r) \tag{1.4.19}$$

and this is equivalent to saying that $\delta' = \frac{\delta}{(\delta,r)}$ divides $\frac{d}{(d,r)}$.

We now check that $q^{u(r)/2} \equiv -1 \mod \frac{d}{(d,r)}$. First, observe that $d/(d,r)$ divides δ, as can be seen from equation (1.4.19). The assumption $q^\nu \equiv -1 \bmod \delta$ implies that $q^\nu \equiv -1 \bmod d'$ where $d' := d/(d,r)$. Then we can apply lemma 1.4.28 to d' (note that $d' \geqslant 3$ since we cannot have $r \in \{0, d/2, d\}$). This ensures that $r \cdot (q^{u(r)/2} + 1) \equiv 0 \pmod{d}$, which is exactly what we needed in the proof of corollary 1.4.29 to check that $\theta_{k_{u(r)},d,r}$ is trivial on $k^\times_{u(r)/2}$ (see equation (1.4.16)). ■

Chapter 2

Packing density of Mordell–Weil lattices and asymptotics

In this chapter, we first give a general lower bound on the sphere packing density of (narrow) Mordell–Weil lattices of elliptic curves over global function fields like $\mathbb{F}_q(t)$ satisfying the Birch–Swinnerton-Dyer conjecture 1.3.34 (see proposition 2.1.1), which relies on Shioda's theorem 1.3.24.

Moreover, we analyze the asymptotic behavior of this lower bound as the rank goes to infinity (see theorem 2.3.1). This requires an upper bound on the Brauer–Siegel ratio of elliptic curves as given in [HP16]. As a result, we get sufficient conditions on a sequence of elliptic curves $(E_n)_{n\geqslant 1}$ so that the packing density of the corresponding narrow Mordell–Weil lattices $(L_n)_{n\geqslant 1}$ satisfies $D(L_n) \geqslant r_n^{-\frac{r_n}{12}(1+o(1))}$ where r_n is the rank of L_n. This includes the families studied by Elkies and Shioda in [Elk94] and [Shi91] respectively, hence providing some conceptual explanation behind the choice of these curves to get "interesting" sphere packings. In section 2.4, we mention how some of the ideas can be generalized to abelian varieties, and to constant elliptic curves.

Finally, in section 2.5, we answer a natural question raised by the work [Elk94]: when $n \geqslant 1$ is odd, what is the rank of the elliptic curve $y^2 + y = x^3 + t^{2^n+1}$ over $\mathbb{F}_2(t)$ (instead of $\mathbb{F}_{2^{2n}}(t)$ as done in the Elkies' paper)? Even though the lower bound on the packing density of the corresponding narrow Mordell–Weil lattices is asymptotically "as good as" the lattices from [Elk94, Shi91], they do not give rise to very dense sphere packings in low dimensions. In any case, these elliptic curves provides an explicit example of a family of isotrivial elliptic curves in characteristic 2 with unbounded rank, in analogy with the work [TS67] which deals with isotrivial curves in odd characteristic.

We remind the reader that a list of symbols can be found at the end of this work, on page 239.

2.1 · Lower bound on the packing density

We start by giving a general lower bound on the sphere packing density of narrow Mordell–Weil lattices.

Proposition 2.1.1. *Let E be an elliptic curve over a global function field $K = k(C)$ as in definition 1.3.2. Let g be the genus of C and r be the Mordell–Weil rank of $E(K)$. Assume that E/K satisfies the BSD conjecture 1.3.34.*

Then the center (sphere packing) density of the narrow Mordell–Weil lattice $E(K)^0 \subset E(K)$ is bounded from below by

$$\delta\left(E(K)^0\right) \geqslant \frac{\left(\frac{\deg\left(\Delta_{\min}(E/K)\right)}{24}\right)^{r/2}}{c(E/K)^{1/2} \cdot L^*(E/K)^{1/2} \cdot |E(K)_{\mathrm{tors}}| \cdot |k|^{\frac{g-1}{2}} \cdot H(E/K)^{1/2}}. \tag{2.1.1}$$

Moreover, this lower bound is an equality if and only if the following equalities hold:

$$\lambda_1(E(K)^0)^2 = \frac{1}{6}\deg\left(\Delta_{\min}(E/K)\right), \qquad |Ш(E/K)| = 1, \qquad [E(K) : E(K)^0] = c(E/K).$$

Proof. — We apply BSD formula (item a) from conjecture 1.3.34) to get an upper bound on the discriminant of $E(K)$, by simply using the fact $|Ш(E/K)| \geqslant 1$:

$$\mathrm{Reg}(E/K) \leqslant L^*(E/K) \cdot |E(K)_{\mathrm{tors}}|^2 \cdot |k|^{g-1} \cdot H(E/K) \cdot c(E/K)^{-1}. \tag{2.1.2}$$

From theorem 1.3.24, we have

$$\lambda_1\left(E(K)^0\right) \geqslant \left(\frac{\deg\left(\Delta_{\min}(E/K)\right)}{6}\right)^{1/2}. \tag{2.1.3}$$

Now, using remark 1.1.4.2, the covolume of $E(K)^0$ is given by

$$\mathrm{covol}\left(E(K)^0\right) = [E(K) : E(K)^0] \cdot \mathrm{covol}(E(K)) = [E(K) : E(K)^0] \cdot \mathrm{Reg}(E/K)^{1/2}.$$

Using lemma 1.3.23, together with equation (2.1.2), we deduce

$$\mathrm{covol}\left(E(K)^0\right) \leqslant c(E/K)^{1/2} \cdot L^*(E/K)^{1/2} \cdot |E(K)_{\mathrm{tors}}| \cdot |k|^{g/2-1/2} \cdot H(E/K)^{1/2}$$

(Note that $L^*(E/K) > 0$ by remark 1.3.33.4, so taking its square root makes sense).

Combining the above inequalities yields the claimed lower bound on $\delta(E(K)^0)$. The case of equality is clearly attained exactly when the lower bounds (2.1.3), $|Ш(E/K)| \geqslant 1$ and $[E(K) : E(K)^0] \leqslant c(E/K)$ (which are the only ones we used to get a lower bound on $\delta(E(K)^0)$) are all equalities. In general, the right-hand side of equation (2.1.1) can be multiplied by $|Ш(E/K)|^{1/2} \in \mathbb{Z}_{>0}$. ■

Remark 2.1.2. Here is the strategy to compute the lower bound on $\delta(E(K)^0)$ from proposition 2.1.1.

① Compute the L-function $L(E/K, T)$ as explicitly as possible. This gives the analytic rank, and also the algebraic rank (since E satisfies the BSD conjecture by assumption). From this, we can also compute the special value $L^*(E/K)$.

② Using Tate's algorithm (see [Sil08b, IV.9, p. 364–369]), one can compute $\deg(\Delta_{\min}(E/K))$ (and hence $H(E/K)$) and $c(E/K)$.

③ It only remains to determine $|E(K)_{\mathrm{tors}}|$, which can be done in various ways (for instance using the injectivity of reduction maps, see [Sil08a, VII.3.1(b)], or using a function field analogue of Nagell–Lutz theorem [Sil08a, VIII.7.2]). We mention another method in the following proposition 2.1.3. ⌟

Proposition 2.1.3. *Let E be an elliptic curve over a global function field K with at least one place of bad reduction (in particular[1], E is non-constant). Then $|E(K)_{\mathrm{tors}}|^2$ divides $c(E/K)$. Moreover, there is an injective group morphism $E(K)_{\mathrm{tors}} \hookrightarrow \prod_{v\in V_K^0} E(K_v)/E(K_v)^0$.* ⌟

Proof. — See [SS19, proposition 6.31] (where the authors use notations from §5.4, p. 87 *ibid.*; note in particular that their convention 5.10 corresponds to our hypothesis about bad reduction) or [SS10, corollary 7.5] for the second claim. ■

We also have the following uniform bound.

Proposition 2.1.4. *Let $g \geqslant 0$ be an integer. Then there is a constant $T_g > 0$ such that for every global function field $K = k(C)$ where C has genus g and every* non-constant *elliptic curve E over K, one has $|E(K)_{\mathrm{tors}}| \leqslant T_g$.* ⌟

Let us mention that when E is constant over $k(C)$, we have $E(K)_{\mathrm{tors}} = E(k)$ as mentioned in remark 2.4.1; so it has size $|k| + 1 - a$ for some $a \in \mathbb{Z}$ such that $|a| \leqslant 2|k|^{1/2}$.

Proof. — See [Lev68, theorem 1, p. 460] and [Ulm11, lecture 1, proposition 7.1] for the case where E is non-isotrivial. The proof of [Ulm11, lecture 1, proposition 7.1] only relies on the fact that E is *non-constant*. (Also, as pointed out in [Sch05] after the proof of proposition 1.9, if E is isotrivial but not constant and if $p = \mathrm{char}(k)$, then the p-primary part of $E(K)_{\mathrm{tors}}$ (i.e., the p-Sylow subgroup) has size $\leqslant 2$).

See [McD18, McD19] for the full (finite) list of groups that occur as $E(K)_{\mathrm{tors}}$ for some non-isotrivial curve E/K, when K has genus 0 or 1: while the list might depend on $\mathrm{char}(k)$, there is indeed an upper bound on $|E(K)_{\mathrm{tors}}|$ that is independent of k.

See also [GS95b, theorem 13] for a bound that depends on the inseparability degree of $j_E : C \to \mathbb{P}^1$. ■

2.2 · Brauer–Siegel and Szpiro ratios, Brumer's bound

In order to study the asymptotic behavior of the lower bound from proposition 2.1.1 (as the rank goes to infinity), we need some tools which we introduce now.

We first define two notions, following [HP16, definition 1.2 and §7.2, p. 80]

Definition 2.2.1. Let E be an elliptic curve over a global function field K. Assume that $f(E/K) > 0$ (in particular E is non-constant).

[1] See also remark 1.3.25.

1. The *Szpiro ratio* of E over K is the positive rational number
$$\sigma(E/K) := \frac{\deg\left(\Delta_{\min}(E/K)\right)}{f(E/K)}.$$

2. Assume that $Ш(E/K)$ is finite. The *Brauer–Siegel* ratio of E over K is the non-negative real number
$$\mathrm{BS}(E/K) := \frac{\log(|Ш(E/K)| \cdot \mathrm{Reg}(E/K))}{\log(H(E/K))}.$$ ⌟

Observe that $\mathrm{BS}(E/K)$ is well-defined since the assumption $f(E/K) > 0$ implies that there is at least one place of bad reduction for E, so that $H(E/K) > 1$ (thus $\log(H(E/K)) \neq 0$). Let us mention here some results about these invariants. First, we deal with the Szpiro ratio.

Theorem 2.2.2 (Ogg, Pesenti–Szpiro). *Let E be an elliptic curve over a global function field $K = k(C)$ such that $f(E/K) > 0$.*

1. *We have $\sigma(E/K) \geqslant 1$ (or equivalently $f(E/K) \leqslant \deg\left(\Delta_{\min}(E/K)\right)$), with equality if and only if for every place $v \in V_K^0$, the reduction type of E at v has Kodaira symbol $\mathrm{I}_0, \mathrm{I}_1$ or II.*

2. *Let g be the genus of C and let p^e be the degree of inseparability of the j-invariant $j_E : C \to \mathbb{P}^1$. Assume that E is not constant if $g = 0$. Then we have the inequality $\deg\left(\Delta_{\min}(E/K)\right) \leqslant 6p^e \cdot (f(E/K) + 2g - 2)$.* ⌟

Proof. — 1. The inequality follows from Ogg's formula (see [Sil08b, IV.11.1, p. 389]), which reads $v(\Delta_{\min}(E/K)) = f_v + m_v - 1 \geqslant f_v$, where $m_v \geqslant 1$ is the number of irreducible components, defined over $\overline{k}$ and counted without multiplicity, of the fiber of $\pi : \mathscr{E} \to C$ over v (we use the notations from remark 1.3.9). The other claim is given in [Sil08b, corollary IV.11.2, p. 396], see also [Sil08b, exercise 3.36, p. 287].

2. See [PS00, theorem 0.1] (this is an analogue over function fields of a famous conjecture of Szpiro, itself related to the *abc* conjecture, see [Sil08a, VIII.11]). ■

Remark 2.2.3. The degree of inseparability of j_E plays an essential role in the bound from theorem 2.2.2.2, as the following example shows. We use Frobenius twists $E \to E^{(p^n)}$ (these are isogenies over $K = \mathbb{F}_p(t)$, so the conductor is preserved). Let $p = 31$ so that the equations $\alpha^3 = -4 \bmod p, \beta^2 = -27 \bmod p$ have a solution, for instance $(\alpha, \beta) = (3, 2)$, and $3^{-1} \equiv 21, 2^{-1} \equiv 16 \bmod p$. Define $E_n : y^2 = x^3 + 21t^{p^n}x + 16$. We have $j(E_n) = 12^3 \frac{4a^3}{4a^3+27b^2} = -12^3 \frac{t^{3p^n}}{t^{3p^n}+1} = -12^3\left(\frac{t^3}{t^3+1}\right)^{p^n}$. We have $f(E_n/K) = 5$ while $\deg(\Delta_{\min}(E_n/K)) \sim 3p^n$ as $n \to \infty$. ⌟

Now, we deal with some known results on the Brauer–Siegel ratio.

Theorem 2.2.4 (Hindry–Pacheco). *Fix real numbers $\epsilon > 0, c_0 \geqslant 1$ and an integer $g \geqslant 0$. Then there are constants $B_{\epsilon,g,c_0}, B'_{\epsilon,g,c_0} > 0$ such that for every global function field $K = k(C)$ where C has genus g, and every elliptic curve E over K with finite Tate–Shafarevich group and with $f(E/K)^{c_0} \geqslant |k|$ and $f(E/K) \geqslant B_{\epsilon,g,c_0}$, we have*
$$|Ш(E/K)| \cdot \mathrm{Reg}(E/K) \leqslant B'_{\epsilon,g,c_0} \cdot H(E/K)^{1+\epsilon}.$$

Therefore, if $(E_n/k_n(C_n))_{n\geqslant 1}$ is a sequence of elliptic curves with finite Tate–Shafarevich groups such that $\lim_{n\to\infty} H(E_n/K_n) = +\infty$, the genus of C_n stays bounded and $|k_n| \leqslant f(E_n/K_n)^{c_0}$ for some absolute $c_0 \geqslant 1$, then we have

$$\limsup_{n\to+\infty} \mathrm{BS}(E_n/K_n) \leqslant 1.$$

Proof. — See [HP16, theorem 1.10 and its proof on page 54] for a statement where the constant B'_{ϵ,g,c_0} actually might depend on q (this is also why they do not assume explicitly that the curves are non-constant). For safety, we make a detailed proof that allows K to vary (with a fixed genus g), which can be found in the appendix A. ■

Remark 2.2.5. 1. Corollary 1.13 and proposition 7.6 in [HP16] give a lower bound on the Brauer–Siegel ratio: namely, for all $\epsilon > 0$ and all global function fields K, there is $C_{\epsilon,K} > 0$ such that for all elliptic curves E over K with finite Tate–Shafarevich group, we have

$$|Ш(E/K)| \cdot \mathrm{Reg}(E/K) \geqslant \mathrm{Reg}(E/K) \geqslant C_{\epsilon,K} \cdot H(E/K)^{-\epsilon},$$

which yields $\liminf_E \mathrm{BS}(E/K) \geqslant 0$, where the liminf is taken over the collection of elliptic curves over K with finite Tate–Shafarevich group, ordered by increasing height $H(E/K)$. However, in all the known examples (given for instance in [HP16, Gri16, Gri17]), the inequality $\limsup_{n\to+\infty} \mathrm{BS}(E_n/K_n) \leqslant 1$ is an equality! As of now, there is no example of families of elliptic curves where the limit of the Brauer–Siegel ratio is < 1, even though such examples are believed to exist, according to [HP16, conjecture 1.7]. (We also note that the results from [HP16] are actually more general: they hold for abelian varieties[2]).

2. Theorem 2.2.4 provides an analogue over function fields of Lang's conjecture in [Lan83, p. 159].

3. Theorem 2.2.4 may fail if we allow the genus to vary in an unbounded fashion. For instance, [Oes90, proposition 4c)] gives an example of constant elliptic curves E_n over $\mathbb{F}_{q^2}(X_{q+1})$ (so $H(E_n) = 1$) with $|Ш(E_n)\,\mathrm{Reg}(E_n)| \to +\infty$ as $n \to +\infty$. Here the Fermat curves X_{q+1} have genus going to infinity as $q \to +\infty$. See the work [KT08] and its erratum.

Another tool that we will need is a bound on the *analytic* rank of an elliptic curve in terms of its conductor. Recall also that the Mordell–Weil rank is always bounded from above by the analytic rank (theorem 1.3.35), that is: $\mathrm{rk}\, E(K) \leqslant \rho(E/K)$.

Theorem 2.2.6 (Brumer). *Let $K = \mathbb{F}_q(C)$ be a global function field and let g_C be the genus of the curve C. Then there are explicit constants $\beta_K, c_K > 0$ such that for any elliptic curve E over K such that the degree f_E of the conductor of E/K is > 1 (in particular, E is non-constant), the analytic rank of E/K satisfies:*

$$\rho(E/K) \leqslant \frac{f_E + 4g_C - 4}{2\log(f_E)}\log(q) + \frac{f_E \log(q)^2}{\log(f_E)^2(1-q^{-1/2})^2} + 1 + 2\beta_K + \frac{c_K \log(q)}{2\log(f_E)}.$$

[2]We note that the full generality of proposition 7.6 from [HP16] relies on some unpublished work (or work in progress) of A. Pacheco and S. David (see page 80 *ibid.*).

In particular, if q is fixed and $f_E \to +\infty$ we get

$$\rho(E/K) \leqslant \frac{f_E + 4g_C - 4}{2\log(f_E)} \log(q) + \mathcal{O}_{q,C}\left(\frac{f_E}{\log^2(f_E)}\right). \qquad \lrcorner$$

Proof. — See [Bru92, proposition 6.9] (where it is assumed that $p \geqslant 5$ at the beginning of §6, but the proof does not require this assumption) and [Paz22, lemma 3.1] (where the result can be improved by noticing that $q^{Y/2} \leqslant f_E \cdot q^{1/2}$ just after equation (11)). See also [Ulm07b, §11].

More specifically, Brumer shows in [Bru92] (using Weil's explicit formulas and some trigonometric polynomials as the Féjer kernel) that if we define the constants

$$\begin{aligned} \beta_K &:= (2g_C + 1)(1 - q^{-1})^{-1} \\ c_K &:= \frac{4\beta_K}{q^{1/2} - 1} + \frac{4}{\sqrt{q}(1 - q^{-1/2})^2} + \frac{4\beta_K}{(q-1)(1 - q^{-1/2})} \end{aligned}$$

then we have[3]

$$\rho(E/K) \leqslant \frac{f_E + 4g_C - 4}{Y} + \frac{4q^{Y/2}}{q^{1/2}Y^2(1 - q^{-1/2})^2} + 1 + 2\beta_K + \frac{c_K}{Y} \tag{2.2.1}$$

for every integer $Y \geqslant 1$. Observe that since $q \geqslant 2$, we have $\beta_K \leqslant 4g_C + 2$ and $c_K \leqslant 4\beta_K(3 + 2\sqrt{2}) + 4(3\sqrt{2} + 4) = \mathcal{O}(g_C)$.

Let $Y := \left\lceil \frac{2\log(f_E)}{\log(q)} \right\rceil$. We have $Y \geqslant 1$ (since $f_E \geqslant 2$ by assumption) and $\frac{Y}{2} \leqslant \frac{\log(f_E)}{\log(q)} + \frac{1}{2} = \log_q(f_E) + \frac{1}{2}$ so that $q^{Y/2} \leqslant q^{\log_q(f_E) + \frac{1}{2}} = f_E q^{1/2}$. This yields the desired upper bound. ■

Finally, the following result will be useful to get an upper bound the index of the narrow Mordell–Weil lattice in the full Mordell–Weil lattice.

Proposition 2.2.7. *Let $\epsilon > 0$ and $g \geqslant 0$. Then there is a constant $d(\epsilon, g) > 0$ such that for all elliptic curves E over any global function field $K = k(C)$ where C has genus g and $\deg(\Delta_{\min}(E/K)) \geqslant d(\epsilon, g)$, we have*

$$\log(c(E/K)) \leqslant \epsilon \log(q) \deg(\Delta_{\min}(E/K)).$$

In particular, we have $c(E/K) = o(H(E/K))$ as $\deg(\Delta_{\min}(E/K)) \to +\infty$. $\lrcorner$

Proof. — This is proven as [Gri16, théorème 1.5.4]. More specifically, on page 82 *ibid.*, one has (given $\epsilon > 0$)

$$\log(c(E/K)) \leqslant \max\left\{\frac{\epsilon}{2} \cdot \Delta \cdot \left(1 + \frac{\log(5)}{\log(\Delta)}\right), \log(q) \cdot \Delta \cdot 12(g+1) \cdot \frac{\log(10/\epsilon) + \log\log(\Delta)}{\log(\Delta)}\right\},$$

where we set $\Delta := \deg(\Delta_{\min}(E/K))$ for simplicity. We now choose $d = d(\epsilon, g) > 0$ so that $12(g+1) \cdot \left(\frac{\log(10/\epsilon) + \log\log(\Delta)}{\log(\Delta)}\right) \leqslant \epsilon$ and $1 + \frac{\log(5)}{\log(\Delta)} \leqslant 2\log(2)$ for all $\Delta \geqslant d$. It follows that

$$\log(c(E/K)) \leqslant \max\{\epsilon \cdot \Delta \cdot \log(2), \epsilon \cdot \Delta \cdot \log(q)\} \leqslant \epsilon \cdot \log(q) \cdot \deg(\Delta_{\min}(E/K))$$

as soon as $\deg(\Delta_{\min}(E/K)) \geqslant d(\epsilon, g)$ as desired. ■

[3] This is obtained just before the statement of [Bru92, proposition 6.9], but there is possibly a typographic error: it is written β_K instead of $2\beta_K$ in the sum (see also the proof of [Paz22, lemma 3.1] where there is indeed $2\beta_K$ as well).

2.3 · Asymptotic behavior of the lower bound

We are now ready to analyze how the lower bound from proposition 2.1.1 behaves in terms of the rank of the Mordell–Weil lattice. We give *sufficient* conditions to get a "large" packing density among packings obtained from narrow Mordell–Weil lattices.

Theorem 2.3.1 (Theorem A). *Consider a collection of elliptic curves* $\{ E_j/K_j \ : \ j \geqslant 1 \}$ *where* $K_j = \mathbb{F}_{q_j}(C_j)$ *is the function field of a smooth projective geometrically irreducible curve* C_j *with bounded genus, and such that the degree* $f_j := f(E_j/K_j)$ *of the conductor goes to* $+\infty$ *when* $j \to \infty$.

Denote by $L_j := E_j(K_j)^0$ *the narrow Mordell–Weil lattice of* E_j/K_j. *Let* r_j *be the (algebraic) rank of* L_j *and let* $d_j := \deg\left(\Delta_{\min}(E_j/K_j)\right)$ *be the degree of the minimal discriminant of* E_j/K_j.

Assume that:

1) *The Birch–Swinnerton-Dyer conjecture 1.3.34 holds for the elliptic curves in the family (in particular, the Tate–Shafarevich groups* $Ш(E_j/K_j)$ *are finite).*

2) *There is a constant* $c_0 \geqslant 1$ *(independent of* j*) such that* $q_j \leqslant f_j^{c_0}$ *for all* $j \geqslant 1$.

3) *The Szpiro ratio* $\sigma_j := \sigma(E_j/K_j) = \dfrac{d_j}{f_j}$ *tends to a finite value*[4] $\sigma \geqslant 1$ *when* $j \to \infty$.

4) *The ratio between the rank of* E_j/K_j *and Brumer's bound stays away from zero, that is, there exists a constant* $\beta \in]0, 1]$ *such that*

$$r_j \ \sim \ \beta \cdot \frac{f_j \log(q_j)}{2 \log(f_j)} \qquad (j \to \infty),$$

Then we have the following asymptotic lower bound as $j \to +\infty$ *(hence the rank* r_j *goes to infinity):*

$$\log(\delta(L_j)) \geqslant (1 + o(1)) \cdot \Big(r_j \log(r_j) \Big(\frac{1}{2} - \frac{\sigma}{12\beta} \Big) + \frac{1}{2} \log(|Ш(E_j/K_j)|) \Big).$$

In particular when $\sigma = 1$ *and* $\beta = 1$ *(i.e., Brumer's bound is asymptotically sharp*[5]*), we get*

$$D(L_j) \ \geqslant \ r_j^{-\frac{1}{12} r_j (1 + o(1))}.$$ ⌟

Before proving this result, let us mention some examples of families of elliptic curves that satisfy the conditions from the above theorem 2.3.1, showing that this result provides some conceptual explanation as to why these families might be interesting for sphere packings.

Example 2.3.2. We use the notations from remark 1.3.47.

[4] We have $\sigma \geqslant 1$ by theorem 2.2.2.1.

[5] This is a slight abuse of terminology: since we allow q_j to vary, the main term of Brumer's bound as in theorem 2.2.6 may not be the one indicated in the last part of theorem 2.2.6.

- In [Elk94], the isotrivial elliptic curves $E_n := \Gamma_{4,2^n+1}$ over $K_n := \mathbb{F}_{q_n}(t)$ (where $q_n := 2^{2n}$ and $n \geqslant 1$ is odd) have rank 2^{n+1} and satisfy $\deg(\Delta_{\min}(E_n/K_n)) = 12\lceil 2^n/6 \rceil$ and $f(E_n/K_n) = 2^{n+1} + 4$ (see theorem 0.1). We see that $q_n \leqslant f(E_n/K_n)^2$ for all $n \geqslant 1$, that Brumer's bound is asymptotically achieved and that the Szpiro tends to 1 as $n \to +\infty$. Morevoer, these curves are isotrivial so they satisfy the Birch–Swinnerton-Dyer conjecture 1.3.34 by theorem 1.3.35. See also remark 2.5.9.
- In [Shi91], the isotrivial elliptic curves $E_p := \Gamma_{2,p+1}$ over $K_p := \mathbb{F}_{p^2}(t)$ (where $p \equiv -1 \pmod 6$ is prime) have rank $2p-2$ and satisfy $\deg(\Delta_{\min}(E_p/K_p)) = 2(p+1)$ and $f(E_p/K_p) = 2(p+1)$ (see proposition 4.1.4). Thus one checks easily that the 4 conditions of theorem 2.3.1 are fulfilled, as $p \to +\infty$.
- The family of non-isotrivial elliptic curves $\Gamma_{3,\frac{p^n+1}{2}}$ with arbitrarily large rank (from remark 1.3.47), satisfies the conditions of theorem 2.3.1, as we will explain at the beginning of section 3.2. ⌟

Proof of theorem 2.3.1. — By definition 1.2.6, the center sphere packing density of the lattice L_j is

$$\delta(L_j) = \frac{(\lambda_1(L_j)/2)^{r_j}}{[E_j(K_j) : L_j] \cdot \mathrm{Reg}(E_j/K_j)^{1/2}},$$

for any $j \geqslant 1$. Using lemma 1.3.23 and theorem 1.3.24 as well as the identity $|Ш(E_j/K_j)| \cdot \mathrm{Reg}(E_j/K_j) = H(E_j/K_j)^{\mathrm{BS}(E_j/K_j)}$, we get

$$\delta(L_j) \geqslant \frac{(d_j/24)^{r_j/2} \cdot |Ш(E_j/K_j)|^{1/2}}{c(E_j/K_j) \cdot H(E_j/K_j)^{\mathrm{BS}(E_j/K_j)/2}}, \tag{2.3.1}$$

which yields

$$\log(\delta(L_j)) \geqslant \frac{r_j}{2}\log\left(\frac{d_j}{24}\right) + \frac{1}{2}\log(|Ш(E_j/K_j)|) - \log(c(E_j/K_j)) - \frac{\mathrm{BS}(E_j/K_j)\cdot d_j}{24}\log(q_j). \tag{2.3.2}$$

Notice that when $j \to \infty$, the rank r_j, the (degree of the) conductor f_j and the minimal discriminant d_j all tend to infinity (because $f_j \leqslant d_j$ from theorem 2.2.2.1 and by assumptions **2)** and item **4)**). Because of the condition **4)** and the assumption **2)** — which implies that $\log(\log(q_j)) = o(\log(f_j))$ — we can express the degree $f(E_j)$ of the conductor of E_j/K_j in terms of the rank r_j:

$$f_j \sim \frac{2r_j\log(r_j)}{\beta\cdot\log(q_j)}. \tag{2.3.3}$$

Indeed, we have

$$\log(r_j) \sim \log(\beta) + \log(f_j) + \log\log(q_j) - \log(2\log f_j) \sim \log(f_j) + \log\log(q_j) \sim \log(f_j)$$

so that $r_j \sim \dfrac{\beta\cdot f_j\log(q_j)}{2\log(r_j)}$ from which equation (2.3.3) follows.

Let us denote $B := \limsup_{j\to+\infty} \mathrm{BS}(E_j/K_j)$. We know that $B \leqslant 1$ by theorem 2.2.4. Then, using the fact that $d_j \sim \sigma\cdot f_j$, equation (2.3.2) becomes

$$\log(\delta(L_j)) \geqslant (1+o(1))\cdot\left(\frac{r_j}{2}\log\left(\frac{\sigma\cdot 2r_j\log(r_j)}{24\beta\cdot\log(q_j)}\right) + \frac{1}{2}\log(|Ш(E_j/K_j)|)\right.$$

$$
\begin{aligned}
&\quad - \log(c(E_j/K_j)) - \frac{B\cdot\sigma\cdot 2r_j\log(r_j)}{24\beta}\Big)\\
&= (1+o(1))\cdot\Big(r_j\log(r_j)\Big(\frac{1}{2}-\frac{B\cdot\sigma}{12\beta}\Big)+o(r_j\log(r_j))\\
&\quad + \frac{1}{2}\log(|Ш(E_j/K_j)|) - \log(c(E_j/K_j))\Big)\\
&= (1+o(1))\cdot\Big(r_j\log(r_j)\Big(\frac{1}{2}-\frac{B\cdot\sigma}{12\beta}\Big)+\frac{1}{2}\log(|Ш(E_j/K_j)|)\Big), \qquad (2.3.4)
\end{aligned}
$$

where we used the fact that $\log\log(q_j) = o(\log(r_j))$ in the second equality and proposition 2.2.7 in the third equality, which ensures that

$$\log(c(E_j/K_j)) = o(\log(q_j)d_j) = o(\sigma\cdot\log(q_j)\cdot f_j) = o(\sigma\cdot r_j\log(r_j)).$$

This concludes the proof of the main inequality of theorem 2.3.1, by using the inequality $B\leqslant 1$.

Moreover, if we now assume that $\sigma = 1$ and $\beta = 1$, then the trivial bound $|Ш(E_j/K_j)|\geqslant 1$ yields

$$\log(\delta(L_j))\geqslant (1+o(1))\cdot r_j\log(r_j)\Big(\frac{1}{2}-\frac{1}{12}\Big).$$

Recalling that $D(L_j) = \mathrm{vol}(B^{r_j}(0,1))\delta(L_j)$ and using remark 1.2.13 (which tells us that $\log\mathrm{vol}(B^r(0,1))\sim -\frac{r}{2}\log(r)$ as $r\to+\infty$), we finally deduce

$$D(L_j)\ \geqslant\ r_j^{-\frac{1}{12}r_j(1+o(1))}. \qquad \blacksquare$$

Remark 2.3.3. 1. We note that the lower bound $D(L_j)\geqslant r_j^{-\frac{1}{12}r_j(1+o(1))}$ from theorem 2.3.1 is *very* far from Minkowski lower bound stated in theorem 1.2.15. In fact, any bound on the form $D(L'_n)\geqslant\alpha^n$ for some $\alpha\in]0,\frac{1}{2}[$ and some lattices $L'_n\hookrightarrow\mathbb{R}^n$ yields (by remark 1.2.13, as $n\to+\infty$)

$$\log\delta(L'_n)\sim\frac{n}{2}\log(n)+\log D(L_n)\geqslant\frac{n}{2}\log(n)+\alpha\cdot n=\frac{1}{2}n\log(n)\cdot(1+o(1)).$$

while we obtained $\log\delta(L_j)\geqslant\frac{5}{12}r_j\log(r_j)\cdot(1+o(1))$. Note that a family of lattices $L'_n\hookrightarrow\mathbb{R}^n$ satisfying $\log\delta(L'_n)\sim\frac{n}{2}\log(n)\cdot(1+o(1))$ does not necessarily achieve Minkowski lower bound: we could have for instance $\log D(L'_n)\sim\alpha n\log\log n$ (as for Craig's lattices mentioned in remarks 1.2.21 and 1.2.22).

2. It is difficult to give a general asymptotic *upper* bound. First one would need an upper bound on $\lambda_1(E(K)^0)$ (see [Sil08a, conjecture VIII.10.2]) and also on $Ш(E/K)$. Instead, we may want to use some "trivial" upper bounds on the packing density to say something about some invariants of elliptic curves with large ranks.

   - For instance, if we have a family $\{E_j/K\ :\ j\geqslant 1\}$ of elliptic curves over $K:=\mathbb{F}_q(t)$ satisfying the 4 conditions of theorem 2.3.1, then we cannot have $|Ш(E_j/K)|\sim q^{\tau\cdot f(E_j)\cdot(1+o(1))}$ for a constant $\tau>\frac{\sigma}{12}$. Indeed, if this was the case then theorem 2.3.1 would yield

$$\log\delta(E_j(K)^0)\geqslant(1+o(1))\cdot r_j\log(r_j)\cdot\left(\frac{1}{2}-\frac{\sigma}{12\beta}+\frac{\tau}{\beta}\right)$$

But the obvious bound $D(E_j(K)^0) \leqslant 1$ yields

$$\log \delta(E_j(K)^0) \leqslant \frac{1}{2} r_j \log(r_j)(1+o(1)) \tag{2.3.5}$$

by remark 1.2.13, so the above (asymptotic) inequality forces $\frac{1}{2} \geqslant \frac{1}{2} - \frac{\sigma}{12\beta} + \frac{\tau}{\beta}$, which means $\tau \leqslant \frac{\sigma}{12}$ as claimed.

- As mentioned in remark 2.3.6 below, Shioda found an example of a family $\{E_j\}$ with $\beta = \sigma = 1$ and such that, with $e := 3$, we have

$$\log |Ш(E_j/K_j)| \sim r_j \log(r_j) \frac{1}{6^e} \left(1 - \frac{1}{e}\right) \sim \frac{f(E_j)\log(q_j)}{2 \cdot 6^e} \left(1 - \frac{1}{e}\right) = f(E_j)\log(q_j) \cdot \frac{1}{648}.$$

- Similarly, families of curves $\{ E_j/K_j \ : \ j \geqslant 1 \}$ satisfying the 4 conditions of theorem 2.3.1 must have a Brauer–Siegel ratio lower bounded by 0, i.e., $\mathrm{BS}(E_j/K_j) \geqslant 0 - o(1)$ as it follows from equations (2.3.4) and (2.3.5). Such a lower bound actually holds for any family of abelian varities with conductor going to infinity, as shown in [HP16, corollary 1.13].

3. It is likely that condition $q_j \leqslant f_j^{c_0}$ in theorem 2.3.1 could be relaxed by using different values of the parameter Y in the proof of Brumer's bound (see theorem 2.2.6). ⌟

Remark 2.3.4. The result of theorem 2.3.1 only tells us something about the asymptotics, when the rank goes to infinity, so it does not ensure that we get "interesting" sphere packings in *low* dimensions.

On the one hand, it might happen that the asymptotic of the (lower bound on the) packing density $D(L_n)$ of some Mordell–Weil lattices $(L_n)_{n\geqslant 1}$ of ranks r_n is *worse* than $D(L_n) \geqslant r_n^{-\frac{1}{12} r_n (1+o(1))}$, but some lattice L_n are quite dense. For instance, the family of lattices $(L_{p,n})$ from [Oes90] mentioned in remark 2.4.2 satisfies $D(L_{p,n}) \geqslant r_n^{-\frac{3}{8} r_n (1+o(1))}$, but for $(p,n) \in \{(2,1),(3,1),(2,2)\}$ we get respectively the D_4, Coxeter-Todd and Leech lattices.

On the other hand, even if the four sufficient conditions from theorem 2.3.1 are fulfilled, it might not be true that in medium dimensions, the Mordell–Weil lattices are denser than Minkowski–Hlawka lower bound. See remark 2.5.9 for an explicit example over $\mathbb{F}_2(t)$. ⌟

Remark 2.3.5. All the families of elliptic curves in remark 1.3.47 have unbounded rank (and for most of them Brumer's bound from theorem 2.2.6 is asymptotically achieved as the conductor grows to infinity). However, for most of these families, the Szpiro ratio tends to an integer $\geqslant 2$ so that the lower bound on the packing density is not as good as for families having a Szpiro ratio tending to 1, as theorem 2.3.1 tells us (this also applies to the family Γ_{1,p^n+1} considered in theorem 1.3.44: its Szpiro ratio tends to 2, so this seems to give a negative answer to a question from [Ulm02, §1.9] which asks whether these curves give dense packings). Notable exceptions are the families $\Gamma_{2,p^n+1}, \Gamma_{3,\frac{p^n+1}{2}}, \Gamma_{4,2^n+1}$ and Γ_{11,p^n} (see remark 4.1.12). ⌟

Remark 2.3.6. The size of the Tate–Shafarevich group is of great interest in view of the asymptotic lower bound on $\delta(E(K)^0)$ from theorem 2.3.1.

1. For instance, Shioda was able to prove a lower bound on $|Ш(E/K)|$ for his family of elliptic curves $\Gamma_{2,m} : y^2 = x^3 + 1 + t^m$ (given in remark 1.3.47.1) which is enough to improve the lower bound $\log_2 \delta(E(K)^0) \geqslant \frac{5}{12} r \log(r) \cdot (1 + o(1))$, but not sufficient to get $\frac{1}{2} r \log(r)$. More specifically, [Shi91, proposition 4.3, corollary 4.6] imply that for every *odd* integer $e \geqslant 1$ and all primes $p \equiv -1 \pmod 6$, if we let $m = p^e + 1$ and $K := \mathbb{F}_{p^{2e}}(t)$, then
$$|Ш(\Gamma_{2,m}/K)| \geqslant p^{2(e-1)n_0}$$
where $n_0 := \left(\frac{p-5}{6}\right)^e$. This implies that
$$\log_2 \delta(\Gamma_{2,m}(K)^0) \geqslant r \log_2(r) \left(\frac{1}{2} - \frac{1}{12} + \frac{1}{2 \cdot 6^e}\left(1 - \frac{1}{e}\right)\right) \cdot (1 + o(1)),$$
when $p \to \infty$ (and e is fixed), where the rank of the (narrow) Mordell–Weil lattice is given by $r = 2 \cdot (p^e - 1)$. When e runs over the odd integers, then $\frac{1}{2 \cdot 6^e}\left(1 - \frac{1}{e}\right)$ is maximal at $e = 3$, with value $\frac{1}{3 \cdot 6^3} = \frac{1}{648}$, and the lower bound on $|Ш(\Gamma_{2,m}/K)|$ is actually sharp (see [Shi91, proposition 4.3, corollary 4.6]), as is the lower bound on the minimal norm (see [Shi91, proposition 5.2]), so in this case we get $\log \delta(\Gamma_{2,m}(K)^0) \sim r \log(r)(\frac{1}{2} - \frac{1}{12} + \frac{1}{648}) = \frac{271}{648} r \log(r) \simeq 0.4182 r \log(r)$.

2. In general, it is known that $|Ш(E/K)| \ll_\epsilon |k|^{f(E/K)\left(\frac{1}{2}+\epsilon\right)}$ when $f(E/K) \to \infty$ (see [HP16, corollary 1.17] and also [GS95b, theorem 15]). Examples of families with $\log |Ш(E/K)| \sim \log H(E/K)$ and $\log |Ш(E/K)| \sim \log\left(|k|^{f(E/K)\left(\frac{1}{4}+\epsilon\right)}\right)$ are given in [Gd21, theorem C, proposition 1.2, equation (2.3)], but the algebraic rank of those elliptic curves is 0 (see proof of proposition 2.1, *ibid.*). ⌟

Remark 2.3.7. In remark 3.1.21 we will see an example where the Szpiro ratio is asymptotic to 1, but Brumer's bound does not seem to be achieved; the rank is only (at least) half of Brumer's upper bound.

More examples can be obtained as follows: as explained at the end of [Ulm07b, §11], the lower bound on the analytic rank from theorem 1.3.48 is asymptotic to Brumer's bound (i.e., $\beta = 1$ in the notations of theorem 2.3.1) if and only if $\deg(\mathfrak{f}'(E/K)) = 1$, using the notation from theorem 1.3.48. ⌟

2.4 · Some generalizations

2.4.1 Mordell–Weil lattices of constant elliptic curves

We point out that theorem 2.3.1 does not apply to constant elliptic curves E over K, since we require the degree of the conductor to go to infinity. In fact, we note that the lower bound from proposition 2.1.1 in the case of a constant curve is trivial, since $\deg(\Delta_{\min}(E/K)) = 0$. The following remark gives some details about Mordell–Weil lattices of constant elliptic curves, and especially how to get a non-trivial lower bound on $\lambda_1(E(K))$ (observe that we have $E(K)^0 = E(K)$ if E is constant).

Remark 2.4.1. Let E be a *constant* elliptic curve over a global function field $K = k(C)$, that is, E is defined over k. We note that under this hypothesis, the elliptic surface $\mathscr{E}$ attached to E (in remark 1.3.9) splits, i.e., $\mathscr{E} \cong C \times_k E$. The main properties of the Mordell–Weil lattice of E over K are discussed in [Oes90], [Gro11, Lecture 3, §2].

1. First we describe the abelian group $E(K)$. There is a group isomorphism

$$\phi : E(k(C)) \cong \mathrm{Hom}_k(C, E), \qquad P \mapsto \phi_P, \tag{2.4.1}$$

described as follows. Given a point $P = (x, y) \in E(k(C))$ we define the rational map $\phi_P : t \mapsto (x(t), y(t))$ which is actually a morphism $C \to E$ since C and E are smooth projective curves (see [GW20, proposition 15.5]). Under the isomorphism (2.4.1), the torsion subgroup $E(k(C))_{\mathrm{tors}} \cong E(k)$ is identified with the constant morphisms $c_P : C \to E, t \mapsto P$ (see for instance [Ulm11, Lecture 1, Proposition 6.1]).

Moreover, we have a morphism $f_* : \mathrm{Hom}_k(C, E) \longrightarrow \mathrm{Hom}_{\mathsf{AV}_k}(\mathrm{Jac}(C), E)$ (where we consider the category AV_k of abelian varieties over k), given by the universal property of the Albanese functor. In general, it has a finite cokernel, but when k is a finite field (which is the case as $k(C)$ is a global function field), there is[6] a divisor of degree 1 on C, used to define an Abel–Jacobi map $C \hookrightarrow \mathrm{Jac}(C)$ which in turn can be used to show that f_* is surjective. In other words, we get a short exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(k) & \longrightarrow & \mathrm{Hom}_k(C, E) & \longrightarrow & \mathrm{Hom}_{\mathsf{AV}_k}(\mathrm{Jac}(C), E) & \longrightarrow & 0 \\ & & P & \longmapsto & c_P & & f & \longmapsto & f_* \end{array} \tag{2.4.2}$$

(see [Ulm11, Lecture 2, Proposition 6.1] and [BDS04, §1]). This implies that

$$E(K)/E(K)_{\mathrm{tors}} \cong \mathrm{Hom}_{\mathsf{AV}_k}(\mathrm{Jac}(C), E) \tag{2.4.3}$$

and this free abelian group has rank at most $g \cdot \mathrm{rk}_{\mathbb{Z}} \mathrm{End}_k(E) \leqslant 4g$, where g is the genus of C. In fact, if $\mathrm{Jac}(C)$ is isogenous to $E^r \times \prod_{i=1}^s A_i$ for some simple abelian varieties A_i not isogenous to E, then $E(K)$ has rank $r \cdot \mathrm{rk}_{\mathbb{Z}} \mathrm{End}_k(E)$ (see [EvdGM, exercise 1.4, p. 15]). Moreover, if the numerator of the zeta function of C over k is written as $\prod_{i=1}^{2g}(1 - \alpha_i T)$ and the numerator of the zeta function of E over k is denoted $(1 - \beta_1 T)(1 - \beta_2 T)$, then using Tate's theorem from [Tat66a, theorem 1(a), p. 139], one finds (see [EvdGM, corollary 16.23] or [Oes90, proposition 3]):

$$\mathrm{rk}\, E(K) = \#\{\, (i, j) \in \{1, ..., 2g\} \times \{1, 2\} \ : \ \alpha_i = \beta_j \,\}. \tag{2.4.4}$$

2. Secondly, we describe the Néron–Tate height. We claim that $\hat{h}(P) = h(P) = 2\deg(\phi_P)$ for any $P \in E(K) \cong \mathrm{Hom}_k(C, E)$. The second equality is clear, since $h(P) = \deg(x \circ \phi_P : C \to \mathbb{P}^1_k) = 2\deg(\phi_P) \in 2\mathbb{Z}_{\geqslant 0}$ (recall that the degree of a constant morphism is set to be 0).

To show that the naive and the Néron–Tate heights coincide, it suffices, by lemma 1.3.15, to show that the naive height, or the map $\deg : \mathrm{Hom}_k(C, E) \to \mathbb{Z}$, is a quadratic form. This follows from [Ser89, Theorem p. 32] (and from [Sil08a, corollary III.6.3] if C is an

[6] This is a theorem of F. K. Schmidt, see [Lor96, Proposition VIII.6.2].

elliptic curve); the reasoning is analogous to the one in remark 1.3.16. Namely, one can show that for all $f, g, h \in \mathrm{Hom}_k(C, E)$ we have

$$\deg(f+g+h) - \deg(f+g) - \deg(f+h) - \deg(g+h) + \deg(f) + \deg(g) + \deg(h) = 0.$$

Fix a line bundle L on E of positive degree. Then [EvdGM, Corollary 2.8] or [HS00, corollary A.7.2.4] states that

$$(f+g+h)^*L \otimes (f+g)^*L^{-1} \otimes (f+h)^*L^{-1} \otimes (g+h)^*L^{-1} \otimes f^*L \otimes g^*L \otimes h^*L$$

is isomorphic to the trivial line bundle on C. Since $\deg(f^*L) = \deg(f)\deg(L)$ holds whenever C, E are curves, and since $\deg(L \otimes L') = \deg(L) + \deg(L')$, we get the desired result.

To get a lower bound on the Néron–Tate height of $\phi : C \to E$, one notices that whenever one has finite subsets $S \subset C(\overline{k}), T \subset E(\overline{k})$ such that $\phi(S) \subseteq T$ we have

$$\deg(\phi) \geqslant \frac{\#S}{\#T}.$$

(For instance, we may take $S = X(k_n), T = E(k_n)$ for some extension k_n/k of degree n; see [Gro90, corollary 11.12] for other examples). Indeed, we have

$$\#T \cdot \deg(\phi) = \sum_{Q \in T} \deg(\phi) \geqslant \sum_{Q \in T} \#\phi^{-1}(\{Q\}) \geqslant \#S.$$

3. The L-function of E over K was described in equation (1.3.11) in terms of the zeta functions of E and C over k:

$$L(E/K, T) = \prod_{j=1}^{2} \frac{\prod_{i=1}^{2g}(1 - |k|\alpha_i T/\beta_j)}{(1 - |k|T/\beta_j) \cdot (1 - |k|^2 T/\beta_j)}. \tag{2.4.5}$$

In view of equation (2.4.4), it follows that the analytic rank is actually equal to the algebraic rank, $\rho(E/K) = \mathrm{rk}\, E(K)$, so that part a) of the BSD conjecture 1.3.34 is true. Recalling that $\beta_1\beta_2 = |k|$ and $|E(k)| = (1-\beta_1)(1-\beta_2)$, we find that $\prod_{j=1}^{2}(1 - |k|T/\beta_j) \cdot (1 - |k|^2 T/\beta_j) = |E(k)|^2/|k|$ and therefore

$$L^*(E/K) = \frac{|k|}{|E(k)|^2} \cdot \prod_{\substack{i,j \\ \alpha_i \neq \beta_j}} (1 - \frac{\alpha_i}{\beta_j}). \tag{2.4.6}$$

4. In the end, using BSD formula (item b) of conjecture 1.3.34; it reads $\mathrm{Reg}(E/K) \cdot |Ш(E/K)| = L^*(E/K) \cdot |k|^{g-1} \cdot |E(k)|^2$ in our case) and the fact $E(K)_{\mathrm{tors}} \cong E(k)$, we find that the center density of the Mordell–Weil lattice $L := \big(E(K)/E(K)_{\mathrm{tors}}; \hat{h}\big)$ is bounded below by

$$\delta(L) \geqslant \frac{(|X(k')|/2|E(k')|)^{r/2}}{\Big(|k|^g \prod\limits_{\substack{i,j \\ \alpha_i \neq \beta_j}} (1 - \frac{\alpha_i}{\beta_j})\Big)^{1/2}} \tag{2.4.7}$$

where r is the rank of $E(K)$ and where $k' \supset k$ is any finite extension.

5. It is unclear how to study the asymptotic behavior of the lower bound (2.4.7) in terms of the rank r, as $r \to +\infty$. This is because the rank is, as in equation (2.4.4), the number the pairs (i,j) such that $\alpha_i = \beta_j$ but relating it to the product over $\alpha_i \neq \beta_j$ appearing in (2.4.7) does not seem very easy. ⌟

Remark 2.4.2. In [Oes90], Oesterlé used constant elliptic curves over a Fermat curve over $\mathbb{F}_{p^2}$ to get Mordell–Weil lattices $(L_{p,n})_{n\geqslant 1, p \text{ prime}}$ (some of them being homothetic to D_4 or the Leech lattice), satisfying $\delta(L_{p,n}) \geqslant r_n^{\frac{1}{8}r_n\cdot(1+o(1))}$ where $r_n = 2p^n(p^n-1)$ is the rank of $L_{p,n}$. In other words, $D(L_{p,n}) \geqslant r_n^{-\frac{3}{8}r_n\cdot(1+o(1))}$ as $n \to +\infty$. (In fact, using a lower bound on $|Ш(E/K)|$ for those curves given in [Gro90, proposition 14.10], one can improve this asymptotic lower bound on the packing density; see also [Dum95]).

The idea was to use a *maximal curve* C over $k = \mathbb{F}_{q^2}$, i.e., a curve with as many points as allowed by Hasse–Weil bound $|X(k)| \leqslant |k| + 1 + 2g|k|^{1/2}$. Instead, one could try to look at families of curves achieving the so-called *Drinfeld–Vladut bound* such as the tower $(C_n)_{n\geqslant 1}$ defined Garcia and Stichtenoth in [GS95a]. The difficulty to estimate the packing density of $E(k(C_n))$ is then to compute explicitly the zeta function of C_n, which is not known in general, despite the work [MZ10]. ⌟

2.4.2 Higher dimensional abelian varieties and jacobians

We mention here a few remarks about Mordell–Weil lattices of abelian varieties in general (but these remarks do not lead to new results). Indeed, *most of* the theory explained in section 1.3 can be generalized to abelian varieties A over a global function field $K = k(C)$.

Remark 2.4.3. 1. The abelian group $A(K)$ is finitely generated and there is an L-function $L(A/K,T) \in \mathbb{Q}(T)$ attached to the ℓ-adic representation $G_K \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A))$ coming from the Tate module, where $\ell \neq \mathrm{char}(k)$ is any prime.

Moreover, the Birch–Swinnerton-Dyer conjecture can be formulated in this setting (see [HP16, conjecture 2.2] or [KT03, Sch82]). Let $\rho = \rho(A/K)$ be the analytic rank of A over K, i.e., the order of vanishing of $L(A/K,T)$ at $T = |k|^{-1}$. Then it is conjectured that $\mathrm{rk}\, A(K) = \rho(A/K)$, that the Tate–Shafarevich group $Ш(A/K)$ is finite, and that

$$L^*(A/K,1) := \frac{L^{(\rho)}(A,1)}{\rho!} = \frac{|Ш(A/K)| \cdot \mathrm{Reg}(A/K) \cdot c(A/K)}{H(A/K)\cdot |k|^{d\cdot(g-1)} \cdot |A(K)_{\mathrm{tors}}| \cdot |A^\vee(K)_{\mathrm{tors}}|},$$

where:

- $c(A/K)$ denotes the product of the Tamagawa numbers,
- $A^\vee$ is the dual abelian variety,
- g is the genus of C and $d := \dim(A)$,
- $H(A/K) := |k|^{\deg(\omega_{A/K})}$ where $\omega_{A/K} := e_{\mathcal{A}}^*(\Omega^1_{\mathcal{A}/C})$, $\phi : \mathcal{A} \to C$ is the Néron model and $e_{\mathcal{A}} : C \to \mathcal{A}$ the zero section of ϕ (see [HP16, definition 2.1]; in the case of an elliptic curve $A = E$, it coincides with the definition 1.3.32 of $H(E/K)$: by [GS95b, lemma 5, p. 79] we have $\deg(\omega_{E/K}) = \chi(\mathscr{E})$ and then we apply proposition 1.3.26.4),

- $\mathrm{Reg}(A/K) := |\det((\langle P_i, Q_j\rangle)_{1\leqslant i,j\leqslant r})|$ where $P_1, ..., P_r$ is any $\mathbb{Z}$-basis of $A(K)/A(K)_{\mathrm{tors}}$, $Q_1, ..., Q_r$ is any $\mathbb{Z}$-basis of $A^\vee(K)/A^\vee(K)_{\mathrm{tors}}$ and $\langle -, -\rangle : A(K) \times A^\vee(K) \to \mathbb{Q}$ is the Néron–Tate pairing defined via the Poincaré line bundle $\mathcal{P}_A$ on $A \times A^\vee$ (see [HS00, theorems B.5.8 and A.7.3.4]), i.e.,

$$\langle -, -\rangle : A(K) \times A^\vee(K) \to \mathbb{R}, \qquad (a, \mathscr{L}) \longmapsto \hat{h}_{A\times A^\vee, \mathcal{P}_A}(a, \mathscr{L}) = \hat{h}_{A,\mathscr{L}}(a).$$

  The conjecture is known for isotrivial abelian varieties by [Mil68, theorem 3, p. 100 and §4.(2), p. 103] and [KT03].

2. When A is a Jacobian, the height $H(A/K)$ and the global Tamagawa number $c(A/K)$ can be computed using a generalization of Tate's algorithm developed in [Dok21]. Moreover, some examples of computations of L-functions $L(A/K, T)$, as well as of the invariants $H(A/K)$ and $c(A/K)$ can be found in [AGTT21, §2.3, §2.5, §4].

3. We can endow $A(K)$ with several lattice structures using heights: by [HS00, proposition B.5.3] (only stated for number fields), any ample symmetric divisor D on A induces a quadratic form $\hat{h}_{A,D} : A(K) \to \mathbb{R}$ which is positive-definite on $A(K) \otimes_{\mathbb{Z}} \mathbb{R}$. Then we may define the bilinear pairing on $A(K)$ by $\langle P, Q\rangle_D := \frac{1}{2}(\hat{h}_{A,D}(P+Q) - \hat{h}_{A,D}(P) - \hat{h}_{A,D}(Q))$. The corresponding Gram matrix has determinant denoted by $\mathrm{Reg}_D(A/K)$.

   According to[7] [AHP18, §2.3], it relates to the regulator $\mathrm{Reg}(A/K)$ defined above as follows:

$$\mathrm{Reg}_D(A/K) = [A^\vee(K) : \Phi_D(A(K))] \cdot 2^{-\operatorname{rk} A(K)} \cdot \mathrm{Reg}(A/K), \tag{2.4.8}$$

   where $\Phi_D : A \to A^\vee, p \mapsto [t_p^* D - D]$ is the polarization attached to D (and $t_p : A \to A$ is the translation by p).

   When $A = E$ is an elliptic curve, the Néron–Tate height as defined in equation (1.3.2) is associated to the ample symmetric divisor $2(O_E)$ (see remark 1.3.16). We have $\hat{h} = \hat{h}_{E,2(O)} = 2\hat{h}_{E,(O)}$ (see [Ser89, §3.5, p. 39-40]). Now, the polarization $\Phi_{(O)}$ attached to (O) has[8] degree 1 (this is a principal polarization), so the isomorphism $\Phi_{(O)} : E \to E^\vee$ over K ensures that the index is $[E^\vee(K) : \Phi_{(O)}(E(K))] = 1$. Thus

$$\begin{aligned}\mathrm{Reg}_{2(O)}(E/K) &= 2^{\operatorname{rk} E(K)} \mathrm{Reg}_{(O)}(E/K) \\ &\overset{(2.4.8)}{=} 2^{\operatorname{rk} E(K)} \cdot (1 \cdot 2^{-\operatorname{rk} E(K)} \cdot \mathrm{Reg}(E/K)) = \mathrm{Reg}(E/K),\end{aligned} \tag{2.4.9}$$

   so that the two definitions of regulator coincide when $A = E$ is an elliptic curve.

4. Let us discuss the case of jacobian varieties. If $A = \mathrm{Jac}(X)$ is the jacobian of a curve X over $k(C)$, or more generally a principally polarized abelian variety (PPAV), then there is an isogeny $A \to A^\vee$ (in fact a polarization, so the isogeny is "coming from an ample line bundle") of degree 1, so that we get an isomorphism $A \cong A^\vee$; see [HS00, corollary A.8.2.3]. In particular, we have $|A(K)_{\mathrm{tors}}| = |A^\vee(K)_{\mathrm{tors}}|$.

[7] See also [HS00, remark F.4.1.3, p. 459], but there is probably a typographic error: the equality $\hat{h}_D(P) = \langle P, \phi_D(P)\rangle_{\mathcal{P}}$ should use the polarization $\Phi_D : A \to A^\vee$ (instead of the map $\phi_D : A \to \mathbb{P}(L(D))$) and we actually have $\hat{h}_D(P) = \frac{1}{2}\langle P, \phi_D(P)\rangle_{\mathcal{P}}$, according to the proof of theorem B.5.8 (p. 208), *ibid.*

[8] In general, see [EvdGM, theorem 9.11]: the degree of Φ_D is the square of the Euler characteristic of $\mathcal{O}_A(D)$. On a curve X, we have $\chi(\mathcal{O}_X(D)) = 1 - g(X) + \deg(D)$ by Riemann–Roch theorem.

The BSD conjecture is known in the case of jacobians of certain plane curves defined by a sum of exactly 4 monomials as in theorem 1.3.40, see [Ulm07b, theorem 6.2].

In the case of a jacobian $A = \mathrm{Jac}(X)$, the theta divisor Θ provides a principal polarization $\lambda_\Theta : A \xrightarrow{\cong} A^\vee$ over K. Then the divisor $\Theta' := \Theta + [-1]^*\Theta$ is ample and symmetric and can be used to get a Néron–Tate height on A, as in [HS00, Proof of theorem B.6.5, p. 216] or see [BG06, §9.4], which is a quadratic form $\hat{h}_{\Theta'} : A(K) \to \mathbb{R}$, positive-definite on $A(K) \otimes_{\mathbb{Z}} \mathbb{R}$. When $A = X = E$ is an elliptic curve, then $\Theta = (O_E)$ and $\Theta' = 2(O_E)$ so this corresponds to the Néron–Tate height as defined in equation (1.3.2).

5. Now that we have lattices $(A(K), \hat{h}_{A,D})$, the main question is how to get a lower bound on the height of non-torsion points, analogous to Shioda's theorem 1.3.24. To be short, no such generalization is known as of now, but we mention some approaches.

   In general, Lang–Silverman conjecture predicts (as in [Pazar, conjecture 4.1] over number fields) that given a global function field K and an integer $g \geqslant 1$, there is a constant $c(K, g) > 0$ such that for any *simple* abelian variety A over K of dimension g, any ample symmetric divisor D on A and any non-torsion point $P \in A(K)$, one has

   $$\hat{h}_{A,D}(P) \geqslant c(K, g) \cdot \max\{\log_{|k|} H(A/K), 1\}.$$

   Some cases are known, as mentioned in [HP16, proof of proposition 7.6, p. 80].

   However, one would need a very explicit (and optimal) expression for $c(K, g)$. We now assume that $A = J := \mathrm{Jac}(X)$ is the jacobian of some curve X over k. In [Shi92a, theorem 2.4] and [Shi99a, theorem 7], Shioda found a generalization of the formula $\hat{h}(P) = -D_P \cdot D_P$ given in proposition 1.3.26 and its proof. One would have to check whether the height defined by Shioda coincides with the Néron–Tate height $\hat{h}_{J,\Theta'}$ (as showed for elliptic curves in [Sil08b, III.9.3, p. 247-248]). See also the works [Shi15, Ngu00].

   Also, it is worth working with the narrow Mordell–Weil sublattice $J(K)^0 \subset J(K)$ as in definition 1.3.20, where an explicit lower bound on the height may be easier to get (as in theorem 1.3.24). It is defined in [Shi92a, Shi99a] in a slightly different way, but the two definitions should be equivalent by an argument similar as [SS19, theorem 6.47]. In any case, Shioda shows that $\langle P, P\rangle = -D_P \cdot D_P$ for any $P \in J(K)^0$ where D_P is a certain divisor on a certain surface $S \to C$ with generic fiber X.

   The difficulty in generalizing theorem 1.3.24 lies in the task of analyzing certain self-intersection products on the surface S, as in item 3 of proposition 1.3.26, which relied on the use of Kodaira's canonical bundle formula which is specific to *elliptic* surfaces.

   However, if S happens to be birational to a quotient $\mathcal{F}/\Gamma$ of a Fermat surface $\mathcal{F}$ by some finite group Γ, then one may use known facts on the intersection theory on $\mathcal{F}$ and functorial properties of the intersection product (e.g., push-forward under $\mathcal{F} \dashrightarrow S$) to get information on $D_P \cdot D_P$. ⌟

Remark 2.4.4. In the case of a constant abelian variety A over $k(C)$, i.e. $A \cong A_0 \times_k K$ for some abelian variety A_0 over k, we should have $A(k(C)) \simeq \mathrm{Hom}_k(C, A)$ and $A(K)_{\mathrm{tors}} = A(k)$ (indeed, if $f : C \to A$ is torsion, say $N \cdot f = 0$, then $\mathrm{Im}(f) \subset A[N]$, but since $A[N]$ is a 0-dimensional subvariety, this forces f to be constant). The height $\hat{h}_{\Theta'}$ is related to the

degree map on $\mathrm{Hom}_k(C, A)$ (or at least to the degree of the divisor $f^*\Theta'$ over C; see [Mil68, §3, lemma 2] and [Kel14, Theorem 4.2.17]).

Moreover, if we let g be the genus of C then similarly to remark 2.4.1, we have

$$|Ш(A/K)| \cdot \mathrm{Reg}(A/K) = |k|^{g\cdot\dim(A)} \cdot \prod_{\substack{1\leqslant i\leqslant 2g \\ 1\leqslant j\leqslant 2\dim(A) \\ \alpha_i\neq\beta_j}} (1 - \frac{\alpha_i}{\beta_j})$$

where β_j are the roots of the characteristic polynomial of the Frobenius endomorphism of A (see [Mil68, theorem 3] and [EvdGM, theorem 12.18]). ⌟

Remark 2.4.5. Let us discuss how theorem 2.3.1 can be generalized to higher dimensional abelian varieties A over a global function field $K = k(C)$ where $|k| = q$.

- First, Brumer's bound still holds, see [Ulm07b, equation (11.2)]: we have

$$\rho(A/K) \leqslant \frac{f(A/K)\log(|k|)}{2\log(f(A/K))} + \mathcal{O}_{q,C}\left(\frac{f(A/K)}{\log^2(f(A/K))}\right)$$

  where $f(A/K)$ is the degree of the conductor of A (seen as a divisor on the curve C).

- Secondly, the Brauer–Siegel ratio of a family of abelian varieties A_j/K of fixed dimension (here we fix K) such that $f(A_j/K) \to +\infty$ is upper-bounded by 1: $\limsup_{j\to+\infty} \mathrm{BS}(A_j/K) \leqslant 1$, as showed in [HP16, Ulm19].

- In general, we consider the higher-dimensional Szpiro ratio (assuming that A has at least one place of bad reduction, i.e., $f(A/K) > 0$)

$$\sigma'(A/K) = \frac{h(A/K)}{f(A/K)},$$

  where $h(A/K) := \log_q(H(A/K))$. Note that when $A = E$ is an elliptic curve we have $\sigma'(E/K) = \frac{\frac{1}{12}\deg(\Delta_{\min}(E/K))}{f(E/K)} = \frac{1}{12}\sigma(E/K)$. By theorem 2.2.2.1, we have $\sigma'(E/K) \geqslant \frac{1}{12}$ for any elliptic curve E/K.

- Let us assume that for all $i \geqslant 1$, we have a jacobian $A_i = J_i := \mathrm{Jac}(X_i)$ of a curve X_i over K and that J_i is simple (as an abelian variety). Consider the height $\hat{h}_{\Theta'}$ as in remark 2.4.3.4. By equation (2.4.9), this quadratic form $\hat{h}_{\Theta'}$ on $J_i(K)$ has discriminant equal to the regulator $\mathrm{Reg}(J_i/K)$.

  In view of Lang–Silverman conjecture mentioned in item 5 of remark 2.4.3, we assume that $\hat{h}_{\Theta'}(P) \geqslant c_1 \cdot h(J_i/K)$ for all non-torsion points $P \in J_i(K)$ and some constant $c_1 > 0$ independent of P.

  Assume that:

  – The conductor f_i of J_i/K goes to infinity as $i \to +\infty$.

  – The Birch–Swinnerton-Dyer conjecture holds for J_i, for all $i \geqslant 1$.

  – Brumer's bounded is asymptotically achieved, and the generalized Szpiro ratio tends to some $\sigma' > 0$. In other words, as $i \to +\infty$, we have $r_i := \mathrm{rk}\, J_i(K) \sim \frac{f_i\log(|k|)}{2\log(f_i)}$ and $h(J_i/K) \sim \sigma' \cdot f_i$.

If we denote by r_i the rank of $J_i(K)$, then we have, as in proof of theorem 2.3.1:

$$\delta(J_i(K)) \geqslant \frac{(c_1^{1/2} \cdot h(J_i/K)^{1/2}/2)^{r_i} \cdot |Ш(J_i/K)|^{1/2}}{H(J_i/K)^{\mathrm{BS}(J_i/K)/2}}$$

so this gives

$$\begin{aligned}\log \delta(J_i(K)) \cdot (1+o(1)) &\geqslant \frac{r_i}{2} \cdot \log\Big(\frac{c_1 \sigma' f_i}{4}\Big) + \frac{1}{2}\log|Ш(J_i/K)| - \frac{\mathrm{BS}(J_i/K)}{2}\sigma' f_i \log(|k|) \\ &\geqslant \frac{r_i}{2} \cdot \log\Big(\frac{c_1 \sigma' r_i \log(r_i)}{2\log(|k|)}\Big) + \frac{1}{2}\log|Ш(J_i/K)| - \mathrm{BS}(J_i/K) \cdot \sigma' \cdot r_i \log(r_i) \\ &\geqslant r_i \log(r_i) \cdot \big(\frac{1}{2} - \sigma'\big).\end{aligned}$$

2.5 · Isotrivial elliptic curves over $\mathbb{F}_2(t)$ with arbitrarily large rank

In this section, we give an answer to a natural question raised by the work [Elk94] of Elkies, where he considered Mordell–Weil lattices of the elliptic curves $y^2 + y = x^3 + t^m + a$ over $\mathbb{F}_{q^2}(t)$ where $q = 2^n$ (for any integer $n \geqslant 1$), $m = q + 1 = 2^n + 1$ and finally $a = 0$ if n is odd, while if n is even, $a \in \mathbb{F}_{q^2}$ is any element such that $\mathrm{tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(a) = 1$. The rank of these lattices is 2^{n+1}.

When n is odd, we may wonder what can be said about the Mordell–Weil lattice of

$$A_n \ : \ y^2 + y = x^3 + t^{2^n+1} \tag{2.5.1}$$

over $\mathbb{F}_2(t)$, instead of taking it over $\mathbb{F}_{q^2}(t)$? In particular, does it give rise to some dense sphere packings in low or medium dimensions?

We show that the rank still grows to infinity, but the answer to the latter question about packings is *no*, even though the lower bound on the packing density of $A_n(\mathbb{F}_2(t))$ is asymptotically "as good as" the one for $A_n(\mathbb{F}_{2^{2n}}(t))$ (at least if n is an odd prime). Namely, using the notations from theorem 2.3.1, we have $\sigma = 1$ and $\beta = 1$ which means that Brumer's bound is asymptotically sharp and the Szpiro ratios converge to 1 (see also remark 2.3.4).

We first determine the rank of A_n over $\mathbb{F}_2(t)$ in the following way.

Theorem 2.5.1 (Theorem H). *Let $n \geqslant 1$ be an integer, and consider the elliptic curve A_n over $\mathbb{F}_2(t)$ given by the equation (2.5.1). Let $k \supset \mathbb{F}_2$ be a finite extension of* odd *degree dividing n. Then the rank of the abelian group $A_n(k(t))$ is given by*

$$\mathrm{rk}\, A_n(k(t)) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 2 \cdot \displaystyle\sum_{\substack{e \mid (2^n+1) \\ e \neq 1}} \frac{\phi(e)}{\mathrm{ord}^{\times}(|k| \bmod e)} & \text{if } n \text{ is odd.} \end{cases}$$

In particular, we have $\mathrm{rk}\, A_n(\mathbb{F}_{2^n}(t)) = 2^n$ when n is odd, and when $n = 1$ or when n is an odd prime, *we have*

$$\mathrm{rk}\, A_n(\mathbb{F}_2(t)) = 2 \cdot \Big(1 + \frac{2^{n-1} - 1}{n}\Big).$$

We first sketch the proof of theorem 2.5.1. Consider the unique smooth projective curves[9] given by the affine equations

$$A : y^2 + y = x^3, \qquad C'_n : u^2 + u = t^{2^n+1} \tag{2.5.2}$$

over $\mathbb{F}_2$. There are two key properties:

- The first one is that A_n is a quadratic twist of $A \times_{\mathbb{F}_2} \mathbb{F}_2(t)$ over the quadratic extension $\mathbb{F}_2(C'_n)/\mathbb{F}_2(t)$ corresponding to the hyperelliptic degree-2 cover $C'_n \to \mathbb{P}^1$ given by the x-coordinate of a point of the hyperelliptic curve C'_n (see the proof of corollary 2.5.5).
- The second important fact is that the numerator $Z_1(A/\mathbb{F}_2, T) = 1 + 2T^2$ of the zeta function of A appears with high multiplicity (when $n \to +\infty$) in the numerator $Z_1(C'_n/\mathbb{F}_2, T)$ of the zeta function of C'_n. We will compute explicitly the zeta function of C'_n over $\mathbb{F}_2$ using Gauss sums. A classical result of Tate [Tat66a] will then allow us to conclude the proof of theorem 2.5.1.

2.5.1 Quadratic twists

To make the above two items more precise, we mention a few (well-known) facts on quadratic twists.

Proposition 2.5.2. *Let K be a field and let E be an elliptic curve over K.*

1. *Assume that K is a field of characteristic $\neq 2$ and fix $u \in K^\times \smallsetminus K^{\times,2}$. If E has a Weierstrass equation of the form $E : y^2 = f(x)$, then the curve $E' : uy^2 = f(x)$ over K is a quadratic twist of[10] E over $K' := K(u^{1/2})$ and we have an isomorphism of $\mathbb{Q}$-vector spaces*

$$E(K') \otimes_{\mathbb{Z}} \mathbb{Q} \;\cong\; E(K) \otimes_{\mathbb{Z}} \mathbb{Q} \;\oplus\; E'(K) \otimes_{\mathbb{Z}} \mathbb{Q}. \tag{2.5.3}$$

2. *Assume that $\mathrm{char}(K) = 2$. Fix an element $d \in K$ such that $P(X) := X^2 + d'X + d \in K[X]$ is irreducible separable and let $K' = K[X]/(P(X)) = K(\alpha)$, where $\alpha \in \overline{K}$ is a root of P. If E is given by a Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, then*

$$E' : y^2 + a_1xy + a_3y = x^3 + (a_2 + dd'^{-2}a_1^2)x^2 + a_4x + a_6 + dd'^{-2}a_3^2$$

is a quadratic twist of E over K' and the isomorphism (2.5.3) also holds. ⌟

Proof. — 1. The extension $K' = K(u^{1/2})/K$ has degree 2, and its Galois group is generated by an element σ such that $\sigma(u^{1/2}) = -u^{1/2}$. The map

$$g : E(K') \xrightarrow{\simeq} E'(K'), \quad (x, y) \longmapsto (x, u^{\frac{1}{2}}y)$$

provides an isomorphism of algebraic curves $E \times_K K' \cong E' \times_K K'$ over K', so that E' is indeed a quadratic twist of E.

[9] Existence and uniqueness (up to isomorphism) follow from [GW20, theorem 15.21]. Namely, there is a unique smooth projective curve C'_n such that $\mathbb{F}_2(C'_n) \cong \mathbb{F}_2(t)[u]/(u^2 + u - t^{2^n+1})$. Notice that in general C'_n will not be given by the projective closure of $u^2 + u = t^{2^n+1}$ in $\mathbb{P}^2$, which is singular!

[10] If $f(x) = x^3 + a_2x^2 + a_4x + a_6$ then E' has a Weierstrass equation $y'^2 = x'^3 + ua_2x'^2 + u^2a_4x' + u^3a_6$, by writing $y = u^{-2} \cdot y'$ and $x = u^{-1} \cdot x'$.

Now, consider the $\mathbb{Q}$-vector space $V := E(K') \otimes_{\mathbb{Z}} \mathbb{Q}$, endowed with the action of the Galois group $\mathrm{Gal}(K'/K) = \langle\sigma\rangle$. We can decompose V into eigenspaces for σ. Indeed we have $\sigma^2 = \mathrm{id}_{K'}$, the eigenvalues of the $\mathbb{Q}$-linear map induced by σ on V are -1 and $+1$, and this yields

$$V = V^{\sigma=1} \oplus V^{\sigma=-1}.$$

We have[11] $V^{\sigma=1} = E(K) \otimes_{\mathbb{Z}} \mathbb{Q}$. Moreover,

$$\begin{aligned} E(K')^{\sigma=-1} &= \{(x,y) \in E(K') \ : \ \sigma \cdot (x,y) = -(x,y)\} \\ &= \{(x,y) \in E(K') \ : \ (\sigma(x), \sigma(y)) = (x,-y)\} \end{aligned}$$

Notice that $\sigma(y) = -y \iff \sigma(u^{1/2}y) = u^{1/2}y \iff u^{1/2}y \in K$, so we deduce that $g(E(K')^{\sigma=-1}) = E'(K)$. Finally, we conclude that the isomorphism (2.5.3) holds.

2. Let us deal with the case where K has characteristic 2. The extension K'/K has degree 2 with Galois group generated by an element σ such that $\sigma(\alpha) = \alpha + d'$. Note that $d' \neq 0$ since $P(X)$ is separable (by replacing X with $d'X$ and d with $d'^{-2}d$, we may assume that $d' = 1$). The map

$$g : E(K') \to E'(K') \qquad (x,y) \mapsto (x, y + \alpha d'^{-1}(a_1 x + a_3))$$

is an isomorphism which proves that E' is a quadratic twist of E. Moreover, one easily sees that

$$E(K')^{\sigma=-\mathrm{id}} = \{(x,y) \in E(K') \ : \ (\sigma(x), \sigma(y)) = (x, y + a_1 x + a_3)\}$$

from which it easily follows that $g(E(K')^{\sigma=-\mathrm{id}}) = E'(K)$. Once again, we obtain as before a decomposition (2.5.3). ■

The following result is a standard fact, but we include a proof here since it does not seem easy to find a complete proof in the literature.

Proposition 2.5.3. *Let K be a global function[12] field and K'/K be a separable quadratic extension. Let E be an elliptic curve over K. Then there is a unique (up to K-isomorphism) quadratic twist E'/K of E over K' and we have*

$$L(E/K', T) = L(E/K, T) \cdot L(E'/K, T). \qquad \lrcorner$$

Proof. — • In general, we may write $K' = K(\alpha)$ for some root α of an irreducible polynomial $P(X) = X^2 + d'X + d \in K[X]$ (this is due to the primitive element theorem, since K'/K is separable). Without loss of generality, we may assume that $P \in \mathcal{O}_K[X]$. When $\mathrm{char}(K) \neq 2$, we may also assume that $d' = 0$. When $\mathrm{char}(K) \notin \{2,3\}$, [Sil08a, proposition X.5.4] implies that E has a unique quadratic twist over K'. When $\mathrm{char}(K) \in \{2,3\}$ and $j(E) \neq 0$, we have $\mathrm{Aut}_{\overline{K}}(E) = \{\pm 1\}$ by [Sil08a, proposition A.1.2, p. 410],

[11] This seems obvious, but if we replaced $\mathbb{Q}$ by $S := \mathbb{F}_2$, this could become wrong (namely, if $G := \mathbb{Z}/2\mathbb{Z}$ acts on $M := \mathbb{Z}$ via multiplication by -1, then $M^G = \{0\}$ but G acts trivially on $M \otimes_{\mathbb{Z}} S \cong \mathbb{F}_2$ — here we assume that G acts trivially on S, as it does on $\mathbb{Q}$). The key here is that $\mathbb{Q}$ is torsion-free, so that $\mathrm{Tor}_1^{\mathbb{Z}}(-, \mathbb{Q}) = 0$ and the universal coefficient theorem applies since $\mathbb{Z}$ is a PID.

[12] An analogous statement holds over number fields, in which case one has to work with the "complex-analytic" L-function $\mathcal{L}(E/K, s)$.

so that E has also a unique[13] quadratic twist over K'. If $\mathrm{char}(K) = 2$ and $j(E) = 0$, then E can be defined over $\mathbb{F}_2$ and [KST17, proposition 3.1] implies that it has a unique *quadratic* twist over K'. Finally, if $\mathrm{char}(K) = 3$ and $j(E) = 0$, then E can be defined over $\mathbb{F}_3$ and [KST17, proposition 2.1] implies once again that it has a unique quadratic twist over K'.

It follows that E' is isomorphic over K to the curve described in proposition 2.5.2.

- Fix a prime $\ell \neq \mathrm{char}(k)$ and denote by $\rho_{E,\ell} : G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$ the ℓ-adic Galois representation of E, and same for $\rho_{E',\ell}$. Denote by

$$\chi : G_K \twoheadrightarrow \mathrm{Gal}(K'/K) \cong \{\pm 1\} \subset \mathbb{Q}_\ell^\times \tag{2.5.4}$$

the quadratic character of kernel $G_{K'}$. We claim that we have an isomorphism

$$\rho_{E'} \cong \rho_E \otimes \chi, \tag{2.5.5}$$

and we will explain in the next item that it implies the main claim of proposition 2.5.3.

Let $S \subset V_K^0$ be the union of the places ramified in K', the places above the infinite place v_∞, the places v where the Weierstrass equations defining E and E' (given in proposition 2.5.2) are not integral at v, and the places v for which the valuation of the discriminants of the Weierstrass equations defining E and E' in proposition 2.5.2 is positive (in particular, this includes the bad places for E and the bad places for E'). Note that S is a finite set. Moreover, the Weierstrass models for E, E' as given in proposition 2.5.2 are minimal integral at each $v \notin S$ (since $v(\Delta_E) = v(\Delta_{E'}) = 0$).

By [Lan91, lemma IV.4.4, p. 113], the isomorphism (2.5.5) holds once we prove that the traces of Frobenius conjugacy classes $\mathrm{Frob}_v \subset G_{K_v}/I_v$ at each $v \notin S$ agree (where I_v is the inertia subgroup at v), which amounts to checking that

$$a_v(E') = a_v(E) \cdot \chi(\mathrm{Frob}_v) \tag{2.5.6}$$

for all $v \in V_K \smallsetminus S$, where $a_v(E)$ is defined in equation (1.3.9). Recall that for every $v \in V_K \smallsetminus S$, we have

$$\chi(\mathrm{Frob}_v) = 1 \iff \mathrm{Frob}_v \in G_{K'} \iff \mathrm{Frob}_v|_{K'} = \mathrm{id}_{K'} \iff v \text{ splits in } K'. \tag{2.5.7}$$

Fix $v \in V_K \smallsetminus S$ and let us show the equality (2.5.6). Since S contains the ramified places of K'/K and since K'/K is quadratic, we know that either v is inert or (totally) split in K'.

– Assume that v is split in K'. This means that $P(X)$ splits modulo v, i.e., has roots in $\mathbb{F}_v = \mathcal{O}_K/\mathfrak{p}_v$. Therefore, the reductions $\overline{E_v}$ and $\overline{E'_v}$ are isomorphic over $\mathbb{F}_v$, in view of the proof fo proposition 2.5.2. Thus $a_v(E') = a_v(E) = a_v(E) \cdot \chi(\mathrm{Frob}_v)$, in view of (2.5.7). This proves equation (2.5.6) in that case.

– Assume now that v is inert in K'.

[13] Namely, these twists are classified by the cohomology set $H^1(\mathrm{Gal}(K'/K), \mathrm{Aut}_{K'}(E))$ (which is a group in that case), and it is just $\mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$.

∗ Assume that $\mathrm{char}(K) \neq 2$ (and $d' = 0$). Then d is not a square modulo v, i.e., its Legendre symbol is $\lambda_{\mathbb{F}_v}(d) = -1$. Since E, E' are given by $y^2 = f(x), y^2 = d^{-1}f(x)$ respectively which are minimal integral Weierstrass models at v, we compute:

$$\begin{aligned} a_v(E) + a_v(E') &= |\mathbb{F}_v| + 1 - |\overline{E_v}(\mathbb{F}_v)| \quad + \quad |\mathbb{F}_v| + 1 - |\overline{E'_v}(\mathbb{F}_v)| \\ &= -\sum_{x \in \mathbb{F}_v} \lambda_{\mathbb{F}_v}(f(x)) - \sum_{x \in \mathbb{F}_v} \lambda_{\mathbb{F}_v}(d^{-1} \cdot f(x)) = 0 \end{aligned}$$

which yields $a_v(E') = -a_v(E) = a_v(E) \cdot \chi(\mathrm{Frob}_v)$, hence also proving equation (2.5.6) in this case.

∗ Assume that $\mathrm{char}(K) = 2$. By replacing α with $d^{-1}\alpha$, we may assume that $P(X) = X^2 + X + d$, i.e., $d' = 1$. We know that P has no roots modulo v, since v is inert, which is equivalent to saying $\mathrm{tr}_{\mathbb{F}_v/\mathbb{F}_2}(d) \neq 0$ by proposition 1.4.3.3. We claim that

$$|\overline{E_v}(\mathbb{F}_v)| + |\overline{E'_v}(\mathbb{F}_v)| = 2|\mathbb{P}^1(\mathbb{F}_v)| = 2(|\mathbb{F}_v| + 1) \tag{2.5.8}$$

We pick $x \in \mathbb{F}_v$ and let $A_x := a_1 x + a_3, B_x := x^3 + a_2 x^2 + a_4 x + a_6 \in \mathbb{F}_v$. In view of the equation for E' in proposition 2.5.2, we need to show

$$\#\{\, y \in \mathbb{F}_v \;:\; y^2 + A_x y + B_x = 0 \,\} + \#\{\, y \in \mathbb{F}_v \;:\; y^2 + A_x y + B_x + dA_x^2 = 0 \,\} = 2.$$

If $A_x = 0$ then this amounts to $\#\{\, y \in \mathbb{F}_v \;:\; y^2 = B_x \,\} = 1$ which is true since in a finite field of characteristic 2, any element has a unique square root. If $A_x \neq 0$, we find that

$$\begin{aligned} \#\{\, y \in \mathbb{F}_v \;:\; y^2 + A_x y + B_x = 0 \,\} &= \#\{\, y \in \mathbb{F}_v \;:\; A_x^{-2}(y^2 + A_x y + B_x) = 0 \,\} \\ &= \#\{\, y \in \mathbb{F}_v \;:\; (A_x^{-1}y)^2 + A_x^{-1}y + A_x^{-2}B_x = 0 \,\} \\ &= \#\{\, y' \in \mathbb{F}_v \;:\; y'^2 + y' + A_x^{-2}B_x = 0 \,\} \\ &= 2 \cdot \mathbb{1}_{\mathrm{tr}(A_x^{-2}B_x)=0} \end{aligned}$$

where the last equality comes from proposition 1.4.3.3. Similarly,

$$\#\{\, y \in \mathbb{F}_v \;:\; y^2 + A_x y + B_x + dA_x^2 = 0 \,\} = 2 \cdot \mathbb{1}_{\mathrm{tr}(A_x^{-2}B_x + d)=0}$$

Now, the trace down to $\mathbb{F}_2$ is either 0 or 1, and we know that $\mathrm{tr}(d) \neq 0$ since v is inert. From there, we deduce that equation (2.5.8) holds, which implies once again that $a_v(E') = -a_v(E) = a_v(E) \cdot \chi(\mathrm{Frob}_v)$, which shows equation (2.5.6) in this case.

- Now we explain how equation (2.5.5) implies that $L(E/K', T) = L(E/K, T)L(E'/K, T)$ (see also [Ulm07b, §4.4]). In general, if we take a Galois representation $\rho : G = G_K \to \mathrm{GL}(W)$ for some finite-dimensional $\mathbb{Q}_\ell$-vector space W, where $\ell \neq \mathrm{char}(k)$, we may consider its restriction $\mathrm{Res}^G_H \rho$ to the normal subgroup $H = \mathrm{Gal}(K^{\mathrm{sep}}/K') \trianglelefteq G$. Given another Galois representation $H \to \mathrm{GL}(V)$, we always have

$$\mathrm{Ind}^G_H(V \otimes \mathrm{Res}^G_H W) \cong (\mathrm{Ind}^G_H V) \otimes W$$

and since Artin L-functions behave well with respect to *induction* (see [Neu99, proposition VII.10.4]), this yields (using $V = \mathbb{1}$):

$$L(\mathrm{Res}^G_H \rho, T) = L(\mathrm{Ind}^G_H \mathrm{Res}^G_H \rho, T) = L(\mathrm{Ind}^G_H(\mathbb{1} \otimes \mathrm{Res}^G_H \rho), T) = L((\mathrm{Ind}^G_H \mathbb{1}) \otimes \rho, T).$$

Now, $\mathrm{Ind}_H^G(V)$ has degree $[G : H]\dim(V) = [K' : K]$ since $V = \mathbb{1}$, and is actually isomorphic to $\mathbb{Q}_\ell[G/H] = \mathbb{Q}_\ell[\mathrm{Gal}(K'/K)]$. The subspace $\mathbb{Q}_\ell\,\mathrm{id}_{K'} \subset \mathbb{Q}_\ell[\mathrm{Gal}(K'/K)]$ is the trivial subrepresentation, and we can decompose

$$\mathbb{Q}_\ell[\mathrm{Gal}(K'/K)] = \mathbb{1} \oplus \chi,$$

where χ is the quadratic character defined above in equation (2.5.4) (seen as one-dimensional representation). Thus we get[14] (using [Neu99, proposition VII.10.4]):

$$L(\mathrm{Res}_H^G \rho, T) = L((\mathbb{1} \oplus \chi) \otimes \rho, T) = L(\rho, T)L(\rho \otimes \chi, T)$$

Now, if we take $\rho = \rho_{E,\ell}$ for some prime $\ell \neq p$, it is known that $L(\rho_{E,\ell}, T) = L(E/K, T)$ and similarly $L(\rho_{E',\ell}, T) = L(E'/K, T)$ (see [Gro11, lecture 2, p. 13 and appendix C] and [Dok13, §3, p. 218-219]). Thus the statement of the proposition indeed follows from the isomorphism (2.5.5). ■

Proposition 2.5.4. *Let k be a finite field and E_0 be an elliptic curve over k. Set $K = k(t)$ and consider the constant curve $E := E_0 \times_k K$ over K. Choose a square-free polynomial $d(t) \in k[t] \hookrightarrow K$ and define the hyperelliptic curve C_d over k by an affine open subset (see also footnote 9 on page 99) so that:*

- *If $\mathrm{char}(k) \neq 2$, then $d \in K^\times \smallsetminus K^{\times,2}$ and $C_d : y^2 = d(t)$.*
- *If $\mathrm{char}(k) = 2$, then $X^2 + X + d \in K[X]$ is irreducible and $C_d : y^2 + y = d(t)$.*

Let g be the genus of C_d and let us write the numerators of the zeta functions of C_d and E_0 respectively as

$$Z_1(C_d/k, T) = \prod_{i=1}^{2g}(1 - \alpha_i T), \qquad Z_1(E_0/k, T) = (1 - \beta_1 T)(1 - \beta_2 T).$$

Consider the quadratic twist E' of E over $K' := K(C_d)/K$ as in proposition 2.5.2. Then we have

$$\mathrm{rk}\, E'(k(t)) = \mathrm{rk}\, E(k(C_d)) = \#\{\,(i,j) \in \{1,...,2g\} \times \{1,2\} \;:\; \alpha_i = \beta_j\,\} \tag{2.5.9}$$

$$L(E'/k(t), T) = Z_1(C, \beta_1 T)Z_1(C, \beta_2 T) = \prod_{\substack{1 \leqslant i \leqslant 2 \\ 1 \leqslant j \leqslant 2g}} (1 - \alpha_i \beta_j T) \tag{2.5.10}$$

and BSD conjecture 1.3.34 holds for E' over $k(t)$. ⌟

Proof. — From the exact sequence (2.4.2), we know[15] that $E(K)$ has rank 0, since $\mathrm{Jac}(\mathbb{P}^1) = 0$. Then we deduce from proposition 2.5.2 (especially the isomorphism (2.5.3)) that the finitely generated abelian groups $E(K')$ and $E'(K)$ have the same rank.

[14] More generally, given a finite Galois extension K'/K, we have $L(E/K', T) = \prod_\chi L(\rho_{E,\ell} \otimes \chi, T)^{\dim(\chi)}$ where the product runs over the irreducible representations χ of the Galois group. See also remark 3.1.25.

[15] In other words, the only morphisms $\mathbb{P}^1 \to E$ are constant. This can be seen for separable morphisms using Riemann–Hurwitz formula, since the genus of E is 1 and $\mathbb{P}^1$ has genus 0. More generally, see [EvdGM, corollary 1.7].

Now, equation (2.4.4) implies that

$$\operatorname{rk} E'(k(t)) = \operatorname{rk} E(K') = \operatorname{rk} \operatorname{Hom}_k(\operatorname{Jac}(C_d), E) = \#\{\,(i,j) \in \{1,...,2g\} \times \{1,2\} \;:\; \alpha_i = \beta_j\,\}.$$

It remains to compute the L-function of the quadratic twist E' over K. The L-function of E over K' and over K are given by equations (1.3.11) and (2.4.5):

$$L(E/K',T) = \prod_{j=1}^{2} \frac{\prod_{i=1}^{2g}(1-|k|\alpha_i T/\beta_j)}{(1-|k|T/\beta_j)\cdot(1-|k|^2 T/\beta_j)}.$$

The L-function of E/K is simpler, as the numerator is just equal to 1, since the genus of $K = k(t) = k(\mathbb{P}^1)$ is 0. Since K'/K is a separable quadratic extension, we have $L(E/K',T) = L(E/K,T)L(E'/K,T)$ by proposition 2.5.3. Therefore, we obtain:

$$L(E'/K,T) = \frac{L(E/K',T)}{L(E/K,T)} = \prod_{\substack{1\leqslant i\leqslant 2\\ 1\leqslant j\leqslant 2g}} (1-|k|\alpha_i T/\beta_j) = \prod_{\substack{1\leqslant i\leqslant 2\\ 1\leqslant j\leqslant 2g}} (1-\alpha_i\beta_j T),$$

since $\beta_1\beta_2 = |k|$. In particular, we see that the analytic rank of E' over K is equal to the algebraic rank, so that (the "rank part" of) BSD conjecture 1.3.34 holds (this also follows from (2.5.3) in proposition 2.5.2). ■

An immediate consequence of theorem 2.5.1 is that the analogue of the main result of [TS67] cited in theorem 1.3.44 holds in characteristic 2.

Corollary 2.5.5. *The rank of isotrivial elliptic curves over $\mathbb{F}_2(t)$ is unbounded.* ⌟

Proof. — Thanks to theorem 2.5.1, the only thing left to prove is that the curves A_n over $\mathbb{F}_2(t)$ are isotrivial. In fact, they are quadratic twists of constant curves. More precisely, A_n is a quadratic twist of $A \times_{\mathbb{F}_2} \mathbb{F}_2(t)$ over the quadratic extension $\mathbb{F}_2(C'_n)/\mathbb{F}_2(t)$, using the notations of equation (2.5.2). This follows from proposition 2.5.2.2 with $d := t^{2^n+1} \in K := \mathbb{F}_2(t)$ and $a_3 := 1, a_1 = a_2 = a_4 = a_6 := 0$. ■

2.5.2 Zeta function of some hyperelliptic curves

We now compute explicitly the zeta function[16] of the hyperelliptic curves C'_n in terms of Gauss sums.

Proposition 2.5.6. *Let $m \geqslant 1$ be any odd integer and C_m be the hyperelliptic curve defined by the affine open subset $u^2 + u = t^m$ over $\mathbb{F}_2$ (see footnote 9 on page 99).*

Then the zeta function of C_m over a finite extension $k/\mathbb{F}_2$ is given by

$$Z(C_m/k,T) = ((1-T)(1-|k|T))^{-1} \cdot \prod_{[r]\in((\mathbb{Z}/m\mathbb{Z})\smallsetminus\{0\})/\langle|k|\rangle^\times} \left(1 + G(\theta_{k_{u(r)},m,r})T^{u(r)}\right),$$

where $u(r) = u_{|k|,m}(r)$ is as in definition 1.4.15. ⌟

[16] The work [Kob91] contains an expression the zeta function of C_n in terms of certain Jacobi sums, at least when $2^n + 1$ is prime. We found out that a similar computation is now given in [Waw21, §3], where it is assumed that $|k| \equiv 1 \pmod m$. Note also that Elkies showed in [Elk94, Proposition 1] that $Z_1(C'_n/\mathbb{F}_{q^2},T) = (1+qT)^q$.

Proof of proposition 2.5.6. — Let C_m^{aff} be the affine plane curve $u^2+u=u^2-u=t^m$ over $\mathbb{F}_2$. Then C_m is the unique smooth projective geometrically[17] irreducible curve such that $\mathbb{F}_2(C_m)\cong\mathbb{F}_2(C_m^{\mathrm{aff}})$. We note that C_m has a unique point at infinity, that is $|C_m\smallsetminus C_m^{\mathrm{aff}}|=1$, and C_m has genus $\frac{m-1}{2}$ since m is odd (see [Gal12, §10.1.1] or [GPS02, proposition 2]).

Now, for every $j\geqslant 1$, we compute

$$\begin{aligned}
|C_m(k_j)| = 1+|C_m^{\mathrm{aff}}(k_j)| &= 1+\sum_{t\in k_j}\#\{\,u\in k_j\ :\ u^2-u=t^m\,\}\\
&= 1+\sum_{t\in k_j}\sum_{\psi\in\widehat{\mathbb{F}_2}}\psi(\mathrm{tr}_{k_j/\mathbb{F}_2}(t^m)) && \text{proposition 1.4.3.3}\\
&= 1+|k_j|+\sum_{t\in k_j}(-1)^{\mathrm{tr}(t^m)}\\
&= 1+|k_j|+\sum_{t'\in k_j}\sum_{\chi\in\widehat{k_j^\times}[m]}(-1)^{\mathrm{tr}(t')}\chi(t') && \text{proposition 1.4.3.1}\\
&= 1+|k_j|+\sum_{\chi\in\widehat{k_j^\times}[m]}(G(\chi)+\chi(0)) && \text{definition 1.4.5.1}\\
&= 1+|k_j|+\sum_{\chi\in\widehat{k_j^\times}[m]\smallsetminus\{\mathbb{1}\}}G(\chi).
\end{aligned}$$

Now, the map $\alpha:\chi\longmapsto -G(\chi)$ satisfies the hypothesis of proposition 1.4.26 thanks to theorem 1.4.7.1 and proposition 1.4.6.3. Thus we get

$$\begin{aligned}
\log(Z(C_m/k,T)) &= \sum_{j\geqslant 1}|C(k_j)|\frac{T^j}{j}\\
&= -\log((1-T)(1-|k|T))-\sum_{j\geqslant 1}\sum_{\chi\in\widehat{k_j^\times}[m]\smallsetminus\{\mathbb{1}\}}(-G(\chi))\frac{T^j}{j}\\
&= -\log((1-T)(1-|k|T))+\sum_{[r]\in((\mathbb{Z}/m\mathbb{Z})\smallsetminus\{0\})/\langle|k|\rangle^\times}\log\left(1+G(\theta_{k_{u(r)},m,r})T^{u(r)}\right),
\end{aligned}$$

which concludes the proof. ∎

Let us deduce some consequences of proposition 2.5.6.

Corollary 2.5.7. *Let $n\geqslant 1$ be an integer and set $C_n':=C_m$ where $m:=2^n+1$. Then for any finite extension $k/\mathbb{F}_2$ of degree dividing n, we have*

$$Z(C_n'/k,T)=((1-T)(1-|k|T))^{-1}\cdot\prod_{[r]\in((\mathbb{Z}/m\mathbb{Z})\smallsetminus\{0\})/\langle|k|\rangle^\times}\left(1+(|k|^{1/2}T)^{u_{|k|,m}(r)}\right).$$ ⌟

Proof. — Using proposition 2.5.6, the identity for $Z(C_n'/k,T)$ follows from theorem 1.4.8 and corollary 1.4.29, which can be applied since $[k:\mathbb{F}_2]\mid n$ (namely, there is an integer

[17] Here C_m^{aff} is smooth over $\mathbb{F}_2$ (the jacobian matrix reads $\nabla=[mt^{m-1},1]$), but it is not needed to get a projective model. For instance, $y^2=x^3$ is singular but it is birational to $\mathbb{P}^1$. However, smoothness of C_m^{aff} ensures that C_m^{aff} embeds in C_m, see [GW20, proposition 15.5]. See also footnote 9 on page 99. Moreover, geometric irreducibility is discussed in footnote 17 on page 32.

$\nu \geqslant 1$ such that $|k|^\nu \equiv -1 \pmod{2^n+1}$). This tells us that for all $r \in \mathbb{Z}/m\mathbb{Z} \smallsetminus \{0\}$, $u(r)$ is even and we have

$$G(\theta_{k_{u(r)},m,r}) = \theta_{k_{u(r)},m,r}(z) \cdot |k|^{\frac{u(r)}{2}}$$

where $z \in k_{u(r)}$ is any non-zero element such that its trace to $k_{u(r)/2}$ is zero, i.e., $z+z^{\frac{u(r)}{2}} = 0$. We may take $z = 1$, since $\mathrm{char}(k) = 2$, so that $G(\theta_{k_{u(r)},m,r}) = |k|^{\frac{u(r)}{2}}$. This finishes the proof. ■

2.5.3 Proof of theorem 2.5.1

From there, we can prove theorem 2.5.1 (= theorem H).

Proof of theorem 2.5.1. — Since the curve $A : y^2+y = x^3$ satisfies $|A(\mathbb{F}_2)| = 3$, one deduces that the numerator of its zeta function over $\mathbb{F}_2$ is $Z_1(A/\mathbb{F}_2, T) = 1+2T^2 = (1-\beta_1 T)(1-\beta_2 T)$ with $\beta_1 = i\sqrt{2} = -\beta_2 = \overline{\beta_2}$ (indeed, we have $\beta_1\beta_2 = 2$ and $|A(\mathbb{F}_2)| = 2+1-(\beta_1+\beta_2)$).

In general, the numerator of the zeta function of A over $k \supset \mathbb{F}_2$ is $(1-\beta_1^{[k:\mathbb{F}_2]}T)(1-\beta_2^{[k:\mathbb{F}_2]}T)$ (see [Gri16, proposition 1.3.7] or [Lor96, lemma VIII.5.7]), so

$$Z_1(A/k,T) = \begin{cases} 1+|k|T^2 & \text{if } [k:\mathbb{F}_2] \text{ is odd} \\ (1-(-1)^j|k|^{1/2}T)^2 & \text{if } [k:\mathbb{F}_2] =: 2j \text{ is even.} \end{cases} \tag{2.5.11}$$

Let $m := 2^n+1$. For all $r \in \mathbb{Z}/m\mathbb{Z} \smallsetminus \{0\}$, we know that $u_{|k|,m}(r)$ is even by corollary 1.4.29: indeed $[k:\mathbb{F}_2]$ divides n by assumption, so there is an integer $\nu \geqslant 1$ such that $|k|^\nu \equiv -1 \pmod{m}$. Moreover, for every $u \in 2\mathbb{Z}_{\geqslant 1}$, the polynomial $1+|k|T^2$ divides $1+(|k|^{1/2}T)^u$ in $\mathbb{Z}[T]$ if and only $u/2$ is odd, in which case the factor $1+|k|T^2$ occurs with multiplicity 1 in $1+(|k|^{1/2}T)^u$.

Assume now that $[k:\mathbb{F}_2]$ is odd. Then using proposition 2.5.4 (especially equation (2.5.9)) and corollary 2.5.7, we deduce that the rank of A_n over $k(t)$ is (recall that $m = 2^n+1$)

$$\mathrm{rk}\, A_n(k(t)) = 2 \cdot \#\left\{ [r] \in (\mathbb{Z}/m\mathbb{Z} \smallsetminus \{0\}) \Big/ \langle |k| \rangle^\times \ : \ \frac{u_{|k|,m}(r)}{2} \text{ is odd} \right\}.$$

Using lemma 1.4.28 on $D := \frac{m}{\gcd(m,r)} \geqslant 3$, we see that $\frac{n}{u(r)/2}$ is always an odd integer. If n is odd, then $u(r)/2$ is odd for any r. If n is even, then $u(r)/2$ is even for any r. Thus, we find

$$\mathrm{rk}\, A_n(k(t)) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 2 \cdot \left| (\mathbb{Z}/m\mathbb{Z} \smallsetminus \{0\}) \Big/ \langle |k| \rangle^\times \right| & \text{if } n \text{ is odd.} \end{cases}$$

Lemma 1.4.27.1 gives a general formula for the number of orbits of $\langle |k| \rangle^\times$ on $\mathbb{Z}/m\mathbb{Z}$, while lemma 1.4.27.2 gives the case $k = \mathbb{F}_{2^n}$.

Finally, when $m = 2^n+1$ and n is either an odd prime or $n = 1$, lemma 1.4.27.3 yields

$$\left| (\mathbb{Z}/m\mathbb{Z} \smallsetminus \{0\}) \Big/ \langle 2 \rangle^\times \right| = 1 + \frac{2}{2} + \frac{2^n-2}{2n} - 1 = 1 + \frac{2^{n-1}-1}{n}$$

and this concludes the proof. ■

Remark 2.5.8. Note that when $[k : \mathbb{F}_2] = 2n$ (i.e., $k = \mathbb{F}_{2^{2n}}$) and n is odd, we recover the result from [Elk94, p. 347-348] which asserts that $\operatorname{rk} A_n(\mathbb{F}_{2^{2n}}(t)) = 2^{n+1}$.

Indeed, if we let $k' = \mathbb{F}_{2^n}$ then all the orbits of the multiplicative action of $\langle 2^n \rangle^\times$ on $\mathbb{Z}/(2^n+1)\mathbb{Z} \smallsetminus \{0\}$ have size 2 (see lemma 1.4.27), so corollary 2.5.7 implies that the numerator of $Z(C'_n/k', T)$ equals $(1 + |k'|T^2)^{\frac{m-1}{2}}$.

Then the numerator of $Z(C'_n/k, T)$ equals

$$Z_1(C'_n/k, T) = \left((1 - (i|k'|^{1/2})^2 T) \cdot (1 - (-i|k'|^{1/2})^2 T)\right)^{\frac{m-1}{2}} = (1 + |k'|T)^{m-1}.$$

Now, from equation (2.5.11) we have $Z_1(A/k, T) = (1 + |k'|T)^2$ so proposition 2.5.4 yields

$$\operatorname{rk} A_n(\mathbb{F}_{2^{2n}}(t)) = 2 \cdot (m-1) = 2^{n+1}$$

as claimed. ⌟

Remark 2.5.9. We expand a bit on remark 2.3.4. The family $\{ A_n/\mathbb{F}_2(t) \ : n \geqslant 1 \text{ odd prime} \}$ satisfies the conditions of theorem 2.3.1. Namely, we have $\deg(\Delta_{\min}(A_n)) = 2 \cdot 2^n + 8$ and $f(A_n) = 2 \cdot 2^n + 4$, so the Szpiro ratio tends to 1 as $n \to +\infty$. Moreover, from theorem 2.5.1, we know that Brumer's bound is asymptotically achieved:

$$\operatorname{rk} A_n(\mathbb{F}_2(t)) \sim \frac{2^n}{n} = \frac{2 \cdot 2^n \cdot \log(2)}{2 \cdot \log(2^n)} \sim \frac{f(A_n)\log(2)}{2\log f(A_n)}.$$

Therefore, the asymptotic lower bound on the packing density of $A_n(\mathbb{F}_2(t))^0$ is the same as for Elkies' and Shioda's examples from [Elk94, Shi91] (see theorems 0.1 and 0.2). However, in low dimensions, we do *not* get sphere packing records. Assume that n is odd.

- Over $\mathbb{F}_2(t)$, for $n = 11$ we get a 188-dimensional lattice L with $\log_2 \delta(L) \geqslant 16.05$, much worse than Minkowski–Hlawka lower bound from theorem 1.2.15 (which reads $\log_2 \delta_\ell(188) \geqslant 142.88$). For $n = 13$ we get a 632-dimensional lattice, for $n = 9$ we get a 60-dimensional lattice; both are very far from achieveing Minkowski bound.
- Let $k' = \mathbb{F}_{2^n}$. When n is odd, we have $Z_1(C'_n/k', T) = (1 + 2^n T^2)^{2^{n-1}} =: \prod_{j=1}^{2g_n}(1 - \alpha_j T)$ as explained in remark 2.5.8, where $g_n = 2^{n-1}$ is the genus of C'_n. Moreover we have $Z_1(A/k', T) = 1 + 2^n T^2 =: (1 - \beta_1)(1 - \beta_2)$ by equation (2.5.11). We have $L(A_n/\mathbb{F}_{2^n}(t), T) = (1 - 2^{2n}T^2)^{2^n}$ by equation (2.5.10). Then the special value of A_n over $\mathbb{F}_{2^n}(t)$ is

$$L^*(A_n/\mathbb{F}_{2^n}(t)) = \prod_{\alpha_i\beta_j \neq |k'|} (1 - \alpha_i\beta_j|k'|^{-1}) = \prod_{j=1}^{g_n}(1+1)^2 = 2^{2g_n} = 2^{2^n}.$$

  (Compare this with $L^*(A_n/\mathbb{F}_{2^{2n}}(t)) = 1$: changing the field of constants to a quadratic subextension heavily changes the special value and the rank). Using proposition 2.1.1, if we let $L_n := A_n(\mathbb{F}_{2^n}(t))^0$ then we find:

  – For $n = 7$, the rank of L_n is 128 and $\log_2 \delta(L_n) \geqslant 82.903$.

  – For $n = 9$, the rank of L_n is 512 and $\log_2 \delta(L_n) \geqslant 749.623$.

The density exceeds Minkowski lower bound only when $n = 7$, but both densities are smaller than the ones found by Elkies in [Elk94] (see theorem 0.1). ⌟

Remark 2.5.10. Let $k = \mathbb{F}_{2^{2n}}$ where $n \geqslant 1$ is odd and set $q = 2^n$. We have $A_n(k(C'_n)) \cong A(k(C'_n))$ since A_n is a quadratic twist of $A : y^2 + y = x^3$ over $k(C'_n)$. We find by equation (1.3.11)

$$L(A_n/k(C'_n), T) = Z(C'_n/k, -qT)^2 = \frac{(1-q^2T)^{2^n \cdot 2}}{((1+qT)(1+q^3T))^2}$$

so $A_n(k(C'_n))$ has rank 2^{n+1}. The special value at $T = |k|^{-1} = q^{-2}$ is

$$L^*(A_n/k(C'_n)) = ((1+q^{-1})(1+q))^{-2} = \frac{q^2}{(1+q)^4}$$

and we can compute a lower bound on $\delta[A_n(k(C'_n))]$ by equation (2.4.7). For $n = 1$, we get a 4-dimensional lattice with the same density as the root lattice D_4, but as soon as $n \geqslant 3$, the lower bound is very far from beating Minkowski lower bound. ⌟

2.5.4 Alternative proof of theorem 2.5.1

In this subsection, we give a slightly different computation of the zeta function of $C'_n : u^2 + u = t^{2^n+1}$ when $n = 1$ or is an odd prime, which allows us to deduce the last equality of theorem 2.5.1.

Proposition 2.5.11. *Let n be an odd prime or $n = 1$, and $r \geqslant 1$ be an integer.*

1. We have

$$|C'_n(\mathbb{F}_{2^r})| = \begin{cases} 2^r + 1 & \text{if } r \text{ odd} \\ 2^r + 1 + (-2)^{\frac{r}{2}+1} & \text{if } r \text{ even and } [n \nmid r \text{ or } n = 1] \\ 2^r + 1 - (-1)^{\frac{r}{2n}} 2^{n+\frac{r}{2}} & \text{if } r \text{ even and } [n \mid r \text{ and } n > 1]. \end{cases}$$

2. Write $n = 2n' + 1$. The numerator of the zeta function of C'_n over $\mathbb{F}_2$ is

$$Z_1(C'_n/\mathbb{F}_2, T) = \prod_{j=0}^{n-1} ((1 - a_j T)(1 - \overline{a_j} T))^{d_j}$$

where

$$a_j := \sqrt{2} e^{\frac{i(2j+1)\pi}{2n}}, \qquad 0 \leqslant j \leqslant n-1$$
$$d_j = d_0 := \frac{2^{n-1} - 1}{n} \quad \forall j \neq n', \qquad d_{n'} := d_0 + 1. \qquad ⌟$$

Observe that the degrees d_j satisfy $\sum_{j=0}^{n-1} 2d_j = 2g_n = 2^n$, where $g_n = 2^{n-1}$ is the genus of C'_n (see the proof of proposition 2.5.6), since $d_{n'} = 2^{n-1} - (n-1)d_0$.

Now, if we assume proposition 2.5.11, then the rank of A_n over $\mathbb{F}_2(t)$ is $2d_{n'}$ (by proposition 2.5.4), because from equation (2.5.11) we have $Z_1(A/\mathbb{F}_2, T) = 1 + 2T^2 = (1 -$

$\beta_1 T)(1-\beta_2 T)$ with $\beta_1 = i\sqrt{2} = -\beta_2$. Now $a_{n'} = i\sqrt{2} = \beta_1$ occurs with multiplicity $d_{n'}$ in $Z_1(C'_n/\mathbb{F}_2, T)$, and the same holds for $\overline{a_{n'}} = \beta_2$, so we obtain the last claim from theorem 2.5.1.

It remains to prove proposition 2.5.11, which occupies the rest of this subsection. It is not difficult to see that item (2) implies (1) in proposition 2.5.11, as we shall see here. The converse is not obvious to prove directly, but it follows by uniqueness of the zeta function given the number of points on all field extensions (by definition of the zeta function). Afterwards, we will prove part (1) itself.

Proof of (2) $\implies$ (1) in proposition 2.5.11. — If we assume (2) in proposition 2.5.11, then we have $|C'_n(\mathbb{F}_{2^r})| = 2^r + 1 - \sum_{j=0}^{n-1} d_j(a_j^r + \overline{a_j}^r)$. Almost all d_j are equal to d_0, except for $d_{n'}$, so it makes sense to start with looking at the sum $\sum_{j=0}^{n-1}(a_j^r + \overline{a_j}^r) = 2\operatorname{Re}\left(\sum_{j=0}^{n-1} a_j^r\right)$.

Let $\zeta = \zeta_{n,r} := \exp\left(\frac{ri\pi}{2n}\right)$. We compute (using the notations from proposition 2.5.11):

$$\begin{aligned} 2^{-r/2}\sum_{j=0}^{n-1} a_j^r &= \sum_{j=0}^{n-1} \exp\left(\frac{r(2j+1)i\pi}{2n}\right) \\ &= \sum_{j=0}^{n-1} \zeta^{2j+1} \\ &= \begin{cases} \zeta \cdot \dfrac{1-(-1)^r}{1-\zeta^2} & \text{if } \zeta_{n,r}^2 \neq 1 \ \ (\iff 2n \nmid r) \\ n\zeta = n(-1)^{\frac{r}{2n}} & \text{if } \zeta_{n,r}^2 = 1 \ \ (\iff 2n \mid r) \end{cases} \end{aligned}$$

Notice that $\zeta^{2n} = (-1)^r$ was used in the last equality, and that this sum is 0 if r is even and not divisible by n (since $1-(-1)^r = 0$).

Now we have

$$\begin{aligned} \sum_{j=0}^{n-1} d_j(a_j^r + \overline{a_j}^r) &= d_0 \sum_{j \neq n'} (a_j^r + \overline{a_j}^r) + (d_0+1)(a_{n'}^r + \overline{a_{n'}}^r) \\ &= d_0 \sum_{j=0}^{n-1} (a_j^r + \overline{a_j}^r) \ + \ (a_{n'}^r + \overline{a_{n'}}^r). \end{aligned} \tag{$\star$}$$

- If r is even and $n \nmid r$, then the above sum ($\star$) simplifies to

$$d_0 \cdot 0 + 2^{r/2}(i^r + (-i)^r) = 2^{r/2} \cdot 2 \cdot (-1)^{r/2},$$

  i.e., $|C'_n(\mathbb{F}_{2^r})| = 2^r + 1 - 2^{r/2} \cdot 2 \cdot (-1)^{r/2}$ in that case, as wanted.

- If r is even and $n \mid r$, we immediately get

$$\begin{aligned} |C'_n(\mathbb{F}_{2^r})| &= 2^r + 1 - 2^{r/2}\left(2d_0 n(-1)^{\frac{r}{2n}} \ + \ 2 \cdot (-1)^{r/2}\right) \\ &= 2^r + 1 - 2^{r/2+1}((2^{n-1}-1)(-1)^{\frac{r}{2}} \ + \ (-1)^{r/2}) \\ &= 2^r + 1 - (-1)^{r/2} 2^{r/2+1} \cdot 2^{n-1}. \end{aligned}$$

- If r is odd, then the sum $(\star)$ simplifies to

$$2\operatorname{Re}\left(d_0\zeta\cdot\frac{1-(-1)^r}{1-\zeta^2}\right)+2^{r/2}\underbrace{(i^r+(-i)^r)}_{=0}=4d_0\operatorname{Re}\left(\frac{\zeta}{1-\zeta^2}\right)=0,$$

  where the last equality holds because $|\zeta|=1$ implies

$$\frac{\zeta}{1-\zeta^2}=\frac{\zeta(1-\overline{\zeta}^2)}{|1-\zeta^2|^2}=\frac{\zeta-\overline{\zeta}}{|1-\zeta^2|^2}\in i\mathbb{R}.$$

  Therefore $|C_n'(\mathbb{F}_{2^r})|=2^r+1$ in that case, as desired. ■

Finally, we prove the first part of proposition 2.5.11, which we have seen to be equivalent to the second statement.

Proof of (1) in proposition 2.5.11. — First of all, notice that C_n' has a single point at infinity (see the proof of proposition 2.5.6).

- Assume that r is odd. When Q is a prime power, we start by letting $\psi:\mathbb{F}_Q^\times\to\mathbb{F}_Q^\times$ be the multiplicative map $t\mapsto t^N$. Its kernel has size $d:=\gcd(N,Q-1)$. When $N=2^n+1, n\geqslant 1$ and $Q=2^r$, where r is odd, we have $d=\gcd(2^n+1,2^r-1)=1$. Indeed, we have $2^n\equiv -1 \pmod d, 2^r\equiv 1 \pmod d$. Then the order of 2 modulo d divides $\gcd(r,2n)=\gcd(r,n)\mid n$ (since r is odd). Therefore $-1\equiv 2^n\equiv 1 \mod d$. Thus d must divide 2, and since it is an odd integer, we conclude $d=\gcd(2^n+1,2^r-1)=1$.

  Therefore, ψ is injective and therefore surjective, so that

$$|C_n'(\mathbb{F}_{2^r})|=1+\sum_{t\in\mathbb{F}_{2^r}}\#\{y\in\mathbb{F}_{2^r}\ :\ y^2+y=t^{2^n+1}\}=1+\sum_{z\in\mathbb{F}_{2^r}}\#\{y\in\mathbb{F}_{2^r}\ :\ y^2+y=z\}.$$

  Proposition 1.4.3.3 states that $y^2+y=y^2-y=z$ has a solution for y if and only if $\operatorname{tr}_{k/\mathbb{F}_2}(z)=0$, in which case there are exactly two solutions $\{y,y+1\}$.

  Hence, since the trace is surjective, we have $|C_n'(\mathbb{F}_{2^r})|=1+2|\ker(\operatorname{tr})|=1+2\cdot 2^{r-1}=1+2^r$, as claimed.

- For $r=2n$, we can see that $C_n'(\mathbb{F}_{2^{2n}})$ has $2q^2+1=1+q^2-2g_n\cdot(-q)$ rational points, where $q=2^n$ and $g_n=2^{n-1}$, as proved in [Elk94, proposition 1, p. 345]. This implies that the numerator of the zeta function of C_n' over $\mathbb{F}_{q^2}$ is $(1+qT)^{2g_n}$. Therefore, when $2n\mid r=2nr'$ (for some $r'\geqslant 1$), we have

$$\begin{aligned}|C_n'(\mathbb{F}_{2^r})|=|C_n'(\mathbb{F}_{(q^2)^{r'}})|&=2^r+1-\sum_{i=1}^{2g_n}(-q)^{r'}=2^r+1-q^{1+r'}(-1)^{r'}\\&=2^r+1-(-1)^{r/(2n)}2^{n+r/2}.\end{aligned}$$

- Finally, assume that $r=2r'$ is even but not divisible by n. Proposition 1.4.3.3 states that the equation $x^2+x=b$ has a solution for x (in which case it has exactly two solutions $\{x,x+1\}$) if and only if $\operatorname{tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(b)=0$. We have

$$|C_n'(\mathbb{F}_{2^r})|=1+\sum_{t\in\mathbb{F}_{2^r}}\#\{y\in\mathbb{F}_{2^r}\ :\ y^2+y=t^{2^n+1}\}$$

$$= 1 + 2\#\{t \in \mathbb{F}_{2^r} \ : \ \mathrm{tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(t^{2^n+1}) = 0\}$$

For $a \in \mathbb{F}_2$, define

$$T(a) = T_{n,r}(a) := \#\{t \in \mathbb{F}_{2^r} \ : \ \mathrm{tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(t^{2^n+1}) = a\}.$$

We claim that if r is even and coprime to n (which is automatic if n is an odd prime or $n = 1$, as soon as $n \nmid r$), then

$$T(0) - T(1) = (-2)^{r/2+1}. \tag{2.5.12}$$

Since $T(0) + T(1) = 2^r$, we will get

$$|C_n'(\mathbb{F}_{2^r})| = 1 + 2T(0) = 1 + (T(0) + T(1)) + (T(0) - T(1)) = 1 + 2^r + (-2)^{r/2+1},$$

as claimed in proposition 2.5.11.

Let us show equation (2.5.12), in order to conclude the proof. Define the additive character

$$\begin{array}{rccc} \psi : & \mathbb{F}_{2^r} & \longrightarrow & \mathbb{C}^\times \\ & x & \longmapsto & \exp\left(\frac{2\pi i}{2}\,\mathrm{tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(x)\right) = (-1)^{\mathrm{tr}_{\mathbb{F}_{2^r}/\mathbb{F}_2}(x)} \end{array}$$

Then proposition 1.4.3 yields

$$T(0) - T(1) = \sum_{t \in \mathbb{F}_{2^r}} \psi(t^{2^n+1}) = \sum_{x \in \mathbb{F}_{2^r}} \sum_{\substack{\chi : \mathbb{F}_{2^r}^\times \to \mathbb{C}^\times \\ \chi^{2^n+1} = \mathbb{1}}} \psi(x)\chi(x) = \sum_{\substack{\chi : \mathbb{F}_{2^r}^\times \to \mathbb{C}^\times \\ \chi^{2^n+1} = \mathbb{1}}} G(\chi)$$

where $G(\chi)$ denotes the Gauss sum attached to the multiplicative character χ.

We are summing characters such that

$$\chi^{2^n+1} = \mathbb{1} = \chi^{2^r-1}$$

so that $\chi^g = \mathbb{1}$, where $g := \gcd(2^n + 1, 2^r - 1)$. The key point now is that $g = 3$. Indeed, we can write a Bézout relation $nu + r'v = 1$ (since n is an odd prime and $n \nmid r = 2r'$, the case $n = 1$ also works), so the identities $2^n \equiv -1 \mod g, 2^r \equiv 1 \mod g$ yield $2^{2nu+rv} = 4 \equiv 1 \mod g$, i.e. $g \mid 3$. One easily sees that in fact $g = 3$: since $n = 2k + 1$ is odd, we have $2^n + 1 = 2 \cdot 4^k + 1 \equiv 2 + 1 = 0 \mod 3$ and $2^r - 1 = 4^{r'} - 1 \equiv 1 - 1 = 0 \mod 3$.

Therefore, if χ_3 denotes any of the two cubic characters of $\mathbb{F}_{2^r}^\times$, then

$$T(0) - T(1) = G(\mathbb{1}) + G(\chi_3) + G(\chi_3^2) = G(\chi_3) + G(\chi_3^2).$$

The explicit computation of those cubic Gauss sums in characteristic 2 is now possible, either by using Hasse–Davenport relation (see remark 2.5.12), or by direct methods as in [DS11, theorem 1, corollary 1]. Namely, we have $G(\chi_3) = G(\chi_3^2) = -(-2)^{r/2}$ (recall that r is even in our case). This proves the result (2.5.12) about $T(0) - T(1)$, and therefore about $|C_n'(\mathbb{F}_{2^r})|$. ■

Remark 2.5.12. We explain how the cubic Gauss sums can be sometimes computed using the Hasse–Davenport relation. The key point is that if $q \equiv 1 \pmod{m}$, then for every $s \geqslant 1$, we have by the last equality of proposition 1.4.17.3

$$\{\chi \in \widehat{\mathbb{F}_{q^s}^\times} \ : \ \chi^m = \mathbb{1}\} = \{\chi' \circ \mathrm{N}_{\mathbb{F}_{q^s}/\mathbb{F}_q} \ : \ \chi'^m = \mathbb{1}\}$$

(notice that $\chi^m = \mathbb{1}$ if and only if the order of χ divides m). In particular, since $4 \equiv 1 \pmod{3}$, it suffices to describe cubic Gauss sums over $\mathbb{F}_4$ to determine those sums over $\mathbb{F}_{4^s} = \mathbb{F}_{2^{2s}}$.

Now we compute the cubic Gauss sums explicitly. Write $\mathbb{F}_4 = \{0, 1, a, a+1\}$ where $a^2 = a+1$. Define a cubic character $\chi : \mathbb{F}_4^\times = \langle a \rangle \to \mathbb{C}^\times$ by $\chi(a) = \exp(2\pi i/3) =: \zeta_3$. Recall that $\zeta_3^2 + \zeta_3 + 1 = 0$. Define the additive character $\phi : \mathbb{F}_4 \to \mathbb{C}^\times, x \mapsto \exp(\pi i \operatorname{tr}_{\mathbb{F}_4/\mathbb{F}_2}(x)) = (-1)^{\mathrm{tr}(x)}$. We can now evaluate

$$\begin{aligned} G(\chi) = \sum_{x \in \mathbb{F}_4} \chi(x)\psi(x) &= \chi(0)\psi(0) \ + \ \chi(1)\psi(1) \ + \ \chi(a)\psi(a) \ + \ \chi(a+1)\psi(a+1) \\ &= 0 \ + \ 1 \ + \ \zeta_3 \cdot (-1) \ + \ \zeta_3^2 \cdot (-1) \\ &= 1 - \zeta_3 - \zeta_3^2 = 1 - (-1) = 2 \end{aligned}$$

Similarly, $G(\chi^2) = 2$. Therefore, over $\mathbb{F}_{4^s}$, we have $-G_{\mathbb{F}_{4^s}}(\chi \circ \mathrm{N}_{\mathbb{F}_{4^s}/\mathbb{F}_4}) = (-G_{\mathbb{F}_4}(\chi))^s = (-2)^s$ by Hasse–Davenport relation stated in theorem 1.4.7. ⌟

Chapter 3

The family $y^2 = x^3 + bx + b't^m$

In this chapter, we study the Mordell–Weil lattices attached to the elliptic curves given by $y^2 = x^3 + bx + b't^m$ over $\mathbb{F}_q(t)$ for some odd prime power q, some $b, b' \in \mathbb{F}_q^\times$ and $m \geqslant 1$.

In section 3.1, we first compute its L-function in terms of Jacobi sums (theorem 3.1.3) and give some formulas for the rank (corollaries 3.1.14 and 3.1.16). In particular, we deduce in corollary 3.1.20 that for any fixed odd prime p, the rank of these curves is unbounded as we vary m (however, Brumer's bound from theorem 2.2.6 seems to be asymptotically achieved only if $p \equiv -1 \bmod 4$). In characteristic 3, an alternative computation of the L-function is given in corollary 3.1.22, using the fact that the map $x \mapsto x^3 + bx$ is additive.

In section 3.2, we study some dense sphere packings we can get from these Mordell–Weil lattices (e.g., in dimensions 150 and 306 as in example 3.2.3). The curves in characteristic 3 provide lattices in dimensions $2 \cdot 3^n = 54\ ;\ 162\ ;\ 486$ (for $n \in \{3, 4, 5\}$) which are the densest known so far; see theorem 3.2.7. Using laminated lattices, we also get lattice packings in dimensions 55, 163, 487, which are the densest known so far in their respective dimensions (proposition 3.2.22).

In section 3.3, we focus on the 54-dimensional lattice mentioned in the previous paragraph and discuss some computational aspects related to its kissing number and its Gram matrices. We end the chapter by proving (in section 3.4) the triviality of the Tate–Shafarevich group of the some of the above elliptic curves in characteristic 3.

As mentioned in remark 3.1.17, the *geometric* rank of these curves was computed in [Shi86, remark 10], provided that the characteristic is $p \equiv -1 \bmod 4$. Our method gives the rank over $\mathbb{F}_q(t)$ for *any* power of p, including when $p \equiv 1 \bmod 4$, so the results we obtain are more general.

Let k be a finite field of odd characteristic. For any integer $m \geqslant 1$ and any $b, b' \in k^\times$ we let $E_{m,b,b'}$ be the elliptic curve over $k(t)$ given by the Weierstrass equation

$$E_{m,b,b'} : \quad Y^2Z = X^3 + bXZ^2 + b't^mZ^3. \tag{3.0.1}$$

Its j-invariant is $j(E_{m,b,b'}) = 12^3 \cdot \dfrac{4b^3}{4b^3 + 27b'^2t^{2m}}$ so we see that $E_{m,b,b'}$ is isotrivial if and only if $\mathrm{char}(k) = 3$, in which case it has j-invariant equal to 0.

This is a Delsarte elliptic curve as in definition 1.3.36 and example 1.3.38. In particular, Shioda's theorem 1.3.40 ensures that $E_{m,b,b'}$ satisfies the Birch–Swinnerton-Dyer conjecture 1.3.34 over $k(t)$.

When q is a power of an odd prime, we also define the narrow Mordell–Weil lattice (see definition 1.3.20)

$$L_{m,b,b',q} := E_{m,b,b'}(\mathbb{F}_q(t))^0.$$

In the specific case where $m = 3^n + 1, q = 3^{2n}, b' = 1$ and $b \in \mathbb{F}_{3^n}^\times$ satisfies $b^{(3^n-1)/2} = (-1)^{n+1}$ (for some integer $n \geqslant 1$), we will obtain some dense lattice sphere packings, denoted $L'_{n,b}$ for simplicity, in dimension $2 \cdot 3^n$: when $n \in \{3, 4, 5\}$, they are currently the densest *known* packings in their respective dimensions.

We remind the reader that a list of symbols can be found at the end of this work, on page 239. In particular, we will use the notations from definitions 1.4.1, 1.4.5 and 1.4.15; for instance k_j denotes the extension of degree $j \geqslant 1$ of a finite field k.

3.1 · L-function of $E_{m,b,b'}$

In view of the lower bound on the packing density of Mordell–Weil lattices given in proposition 2.1.1, we need to compute the L-function of $E_{m,b,b'}$ as explicitly as possible (see also remark 2.1.2). To give such a description, we introduce the following notations.

Definition 3.1.1. Given an integer $m \geqslant 1$, a finite field k and elements $b, b' \in k^\times$, we define

$$d = d(m) := \frac{4m}{\gcd(2,m)} = \begin{cases} 2m & \text{if } m \text{ is even} \\ 4m & \text{if } m \text{ is odd} \end{cases}$$

$$Z(m) := \begin{cases} \mathbb{Z}/2m\mathbb{Z} \smallsetminus \frac{m}{2}\mathbb{Z}/2m\mathbb{Z} & \text{if } m \text{ is even and } 6 \nmid m \\ \mathbb{Z}/2m\mathbb{Z} \smallsetminus (\frac{m}{2}\mathbb{Z}/2m\mathbb{Z} \cup \frac{2m}{3}\mathbb{Z}/2m\mathbb{Z}) & \text{if } m \text{ is even and } 6 \mid m \\ \mathbb{Z}/4m\mathbb{Z} \smallsetminus \left(2\mathbb{Z}/4m\mathbb{Z} \cup m\mathbb{Z}/4m\mathbb{Z}\right) & \text{if } m \text{ is odd} \end{cases}$$

$$\epsilon_{m,b,b',k}(T) := \begin{cases} (1 - |k|T)^2 & \text{if } m \text{ is even and } -b \in k^{\times,2} \text{ and } b' \in k^{\times,2} \\ (1 + |k|T)^2 & \text{if } m \text{ is even and } -b \in k^{\times,2} \text{ and } b' \notin k^{\times,2} \\ 1 - |k|^2T^2 & \text{if } m \text{ is even and } -b \notin k^{\times,2} \\ 1 & \text{if } m \text{ is odd.} \end{cases}$$

Finally, let us define the map

$$\alpha_{b,b'} : \bigsqcup_{n \geqslant 1} \widehat{k_n^\times} \longrightarrow \mathbb{C}, \qquad \alpha_{b,b'}(\theta) := \lambda_{k_n}(-b')\theta(-b^3b'^{-2}) \cdot J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot J(\theta, \theta^2) \quad \text{if } \theta \in \widehat{k_n^\times}.$$

⌟

Remark 3.1.2. In general, we have $Z(m) \subset \mathbb{Z}/d(m)\mathbb{Z}$. Note that when $6 \mid m$ we have

$$Z(m) = \mathbb{Z}/2m\mathbb{Z} \smallsetminus \left\{0, \frac{m}{2}, \frac{2m}{3}, m, \frac{3m}{2}, \frac{4m}{3}\right\}.$$

When $6 \nmid m$ is even, we have $Z(m) = \mathbb{Z}/2m\mathbb{Z} \smallsetminus \{0, m/2, m, 3m/2\}$. ⌟

We now state the main result of this section, proved in subsection 3.1.3.

Theorem 3.1.3 (theorem B). *Let k be a finite field of odd characteristic and let $E_{m,b,b'}$ be the elliptic curve over $k(t)$ as in equation (3.0.1). Assume that m is coprime to $\mathrm{char}(k)$. Then, using the notations from definition 3.1.1, the L-function of $E_{m,b,b'}$ is*

$$L(E_{m,b,b'}/k(t),T) = \epsilon_{m,b,b',k}(T) \cdot \prod_{[r]\in Z(m)/\langle|k|\rangle^\times} \left(1-\alpha_{b,b'}(\theta_{k_{u(r)},d,r})T^{u(r)}\right)$$

where $u(r) = u_{|k|,d}(r)$ and $\theta_{k_{u(r)},d,r}$ were introduced in definition 1.4.15. ⌟

Remark 3.1.4. 1. When m is not coprime to p, one can use proposition 1.3.46 to compute the L-function of $E_{m,b,b'}$. More precisely, let $v_p(m)$ be the p-adic valuation of m and set $m_1 := m/p^{v_p(m)}$. Let $b_1, b_1' \in k^\times$ be the unique elements such that ${b_1}^{p^{v_p(m)}} = b$ and ${b_1'}^{p^{v_p(m)}} = b'$ (recall that the p-th power Frobenius map is a bijection on k; when $b, b' \in \mathbb{F}_p^\times$ we may take $b_1 = b$ and $b_1' = b'$). Then the Frobenius morphism $\mathrm{Fr}_p^{v_p(m)} : E_{m_1,b_1,b_1'} \longrightarrow E_{m,b,b'}$ is an isogeny over $k(t)$, so the curves have the same L-function.

2. As we have explained at the beginning of the proof of proposition 1.4.26, the coefficient $\alpha_{b,b'}(\theta_{k_{u(r)},d,r})$ appearing in theorem 3.1.3 does not depend on the choice of a representative r of the orbit $[r] \in Z(m)/\langle|k|\rangle^\times$. ⌟

3.1.1 Reduction types and local term at the infinite place

We start by analyzing the places of bad reduction of $E_{m,b,b'}$; this is a routine calculation using Tate's algorithm as in [Sil08b, IV.§9]. We use the notations from definition 1.3.7.

Proposition 3.1.5. *Let k be a finite field of odd characteristic $p \geqslant 3$ and let $E_{m,b,b'}$ be the elliptic curve over $k(t)$ as in equation (3.0.1). Assume that m is coprime[1] to p. Then the places of bad reductions of $E_{m,b,b'}$ are given by:*

- *The places v above $\Delta := 4b^3 + 27b'^2t^{2m}$ (there are none if $p = 3$), with $f_v = c_v = v(\Delta) = 1$. Moreover, (3.0.1) is a minimal integral Weierstrass model at v.*
- *The place at infinity $v = \infty$ if[2] $6 \nmid m$, in which case the reduction is of additive type. Further, if we let $\pi := 1/t \in k(t)$, $a := \lceil m/6 \rceil$ and $\alpha = 6a - m$ then $y'^2 = x'^3 + b\pi^{4a}x' + b'\pi^{6a-m}$ is a minimal integral Weierstrass model at $v = \infty$ for $E_{m,b,b'}$, and*

$$f_v = v(\Delta) - 2(\alpha - 1), \qquad v_\infty(\Delta) = \begin{cases} 2\alpha = 12\lceil m/6\rceil - 2m & \text{if } p > 3 \\ 12a = 12\lceil m/6\rceil & \text{if } p = 3. \end{cases}$$

The other local invariants at ∞ are given in the table below.

$m \equiv 1 \bmod 6$	II*	$f_v = v(\Delta) - 8$	$c_v = 1$
$m \equiv 2 \bmod 6$	IV*	$f_v = v(\Delta) - 6$	$c_v = \begin{cases} 3 & \text{if } b' \text{ is a square in } k \\ 1 & \text{otherwise} \end{cases}$
$m \equiv 3 \bmod 6$	I$_0^*$	$f_v = v(\Delta) - 4$	$c_v = 1 + \#\{\, x \in k \,:\, x^3 = -b' \,\}$
$m \equiv 4 \bmod 6$	IV	$f_v = v(\Delta) - 2$	$c_v = \begin{cases} 3 & \text{if } b' \text{ is a square in } k \\ 1 & \text{otherwise} \end{cases}$
$m \equiv 5 \bmod 6$	II	$f_v = v(\Delta)$	$c_v = 1$

[1] If $\gcd(m,p) > 1$, then all bad places $\neq \infty$ are of multiplicative type with Kodaira symbol I$_p$.
[2] This also happens if $p = 3$, but in that case we must have $6 \nmid m$ since we assumed $\gcd(m,p) = 1$.

In particular, we have

$$\deg\left(\Delta_{\min}(E_{m,b,b'}/k(t))\right) = 12\lceil m/6\rceil,$$
$$f(E_{m,b,b'}/k(t)) = \begin{cases} 2m & \text{if } 6 \mid m \\ 2m+2 & \text{if } 6 \nmid m \end{cases}$$

and the Szpiro ratio $\sigma(E_{m,b,b'}/k(t))$ tends to 1 as $m \to \infty$.

Moreover we always have $c(E_{m,b,b'}/k(t)) \in \{1,2,3,4\}$. In fact, if $6 \mid m$ then $c(E_{m,b,b'}/k(t)) = 1$, while if $m \equiv 2, 4 \bmod 6$ and b' is a square in k then

$$c(E_{m,b,b'}/k(t)) = 3. \qquad \lrcorner$$

Proof. — We prove the various claims simultaneously. For simplicity we write $E = E_{m,b,b'}$. The discriminant of the Weierstrass equation (3.0.1) is $-16\Delta = -16(4b^3 + 27b'^2t^{2m})$.

- We first analyze the reduction type at a place $v \mid \Delta$ (we may see this valuation as an irreducible polynomial over k). Since there are no such places if $p = 3$, we may assume that $p > 3$ in this item. The assumption $\gcd(m,p) = 1$ ensures that $\Delta \in k[t]$ is separable, so $v(\Delta) = 1$ and this implies that $\overline{E_v}$ has Kodaira type I_1, by table IV.4.1, p. 365 in [Sil08b]. We can however be more precise by doing explicit computations.

  Let $\pi \in \mathcal{O}_{\mathbb{P}^1,v}$ denote a uniformizer at v. The jacobian matrix of E reads

  $$\nabla = [-(3X^2 + bZ^2) \qquad 2YZ \qquad Y^2 - 2bXZ - 3b't^mZ^2]$$

  If we define $s := -\frac{3b'}{2b}t^m$, then $3s^2 + b = \frac{1}{4b^2} \cdot \Delta \equiv 0 \pmod{\pi}$, so that ∇ vanishes modulo π at the point $[s : 0 : 1]$. One easily checks that $(\bar{s}, \bar{0}) \in \overline{E_v}$ lies on the reduction modulo π of E, so it is a singular point. In other words, $(\bar{0}, \bar{0})$ is a singular point of the reduction modulo π of

  $$E' : \quad y^2 = (x+s)^3 + x + s + t^m = x^3 + 3sx^2 + (\underbrace{3s^2+1}_{\equiv 0 \bmod \pi})x + \underbrace{s^3 + s + t^m}_{\equiv 0 \bmod \pi}.$$

  Write a_1, a_2, a_3, a_4, a_6 for the coefficients of this Weierstrass equation of E' as in [Sil08b, p. 364]. From the table III.3.1 in [Sil08a], we have $\Delta(E') = \Delta(E)$, so we still have $v(\Delta) = 1$. Moreover, if we set $b_2 = 4a_2 = 12s = -18b'b^{-1}t^m$, we have $\pi \nmid b_2$ so the reduction type is I_1 according to Step 2 of [Sil08b, IV.§9, p. 366] so that $f_v = 1$. Because $v(\Delta) = 1$ is odd, we have $c_v = 1$ in any case (whether we have split or non-split multiplicative reduction). Moreover, this shows that $y^2 = x^3 + bx + b't^m$ is a *minimal* integral Weierstrass model at v (see also [Sil08a, remark VII.1.1]).

- We now focus on the place at infinity $v = \infty$ (corresponding to $[1 : 0] \in \mathbb{P}^1(k)$). Let $\pi = t^{-1} \in k(t)$ be a uniformizer of the discrete valuation ring $\mathcal{O}_{\mathbb{P}^1,v}$ and define

  $$a := \lceil m/6\rceil = \min\{a' \geqslant 0 \ : \ 6a' - m \geqslant 0\}.$$

  The change of variables $(x,y) = (\pi^{-2a}x', \pi^{-3a}y')$ shows that E has Weierstrass equation

  $$E_v : \quad y'^2 = x'^3 + b\pi^{4a}x' + b'\pi^{6a-m} \tag{3.1.1}$$

which is integral at v. The associated discriminant is

$$\Delta_v = -16 \cdot (4b^3\pi^{12a} + 27b'^2\pi^{2(6a-m)})$$

We have $\pi \mid \Delta$ if and only if $6 \nmid m$ or $p = 3$. Define $\alpha := 6a - m \in \{0, 1, 2, 3, 4, 5\}$. If $p > 3$, we have $v(\Delta) = 2 \cdot \alpha < 12$ so that equation (3.1.1) is a *minimal* integral Weierstrass model at $v = \infty$ by [Sil08b, remark VII.1.1]. If $p = 3$ then $v(\Delta) = 12a$. We have the following coefficients, as defined in [Sil08b, IV.9, p. 364]:

$$b_2 = 0, \qquad b_4 = 2b\pi^{-4a}, \qquad b_6 = 4b'\pi^{6a-m}, \qquad b_8 = -b^2\pi^{8a}$$

We also let $a_4 := b\pi^{4a}, a_6 := b'\pi^{6a-m}$. Now we distinguish several cases.

- Suppose that $m \equiv 0 \bmod 6$. If $p > 3$ then $\pi \nmid \Delta_v$ so E has good reduction I_0 at $v = \infty$. (If $p = 3$ then $\gcd(m, p) > 1$ so we do not consider this case; the reduction type is IV or IV*).

- From now on we suppose that $6 \nmid m$, which means that $\alpha = 6a - m > 0$. Moreover, the reduction modulo π of E is $\bar{y}^2 = \bar{x}^3$, so the only singular point is $(\bar{0}, \bar{0}) \in \overline{E_v}$. Further, we always have $\pi \mid b_2 = 0$ so we can proceed with step 4 of Tate algorithm as written in [Sil08b, IV.9, p. 366].

  Suppose that $m \equiv 5 \bmod 6$ so $\alpha = 1$. Then $\pi^2 \nmid a_6$, so the reduction type is II and $f_v = v(\Delta)$ and $c_v = 1$. If we assume $m \not\equiv 5 \bmod 6$, then $\pi^2 \mid a_6$ and $\pi^3 \mid b_8$ since $\alpha = 6a - m \geqslant 2$ and $a \geqslant 1$.

- Suppose that $m \equiv 4 \bmod 6$ so $\alpha = 2$. Then $\pi^3 \nmid b_6$ and the reduction type is IV with $f_v = v(\Delta) - 2$. Moreover, the polynomial $T^2 - \pi^{-2}a_6 = T^2 - b'$ splits over $\mathbb{F}_v = k$ if and only if b' is a (non-zero) square in k, if and only $c_v = 3$. Otherwise $c_v = 1$.

  Now we assume that $\alpha \geqslant 3$. Then $\pi^3 \mid b_6$ and define the polynomial $P(T) := T^3 + b\pi^{4a-2}T + b'\pi^{\alpha-3}$ as in [Sil08b, p. 367, step 6].

- Suppose that $m \equiv 3 \bmod 6$, so $\alpha = 3$ and $p > 3$ (since we assumed $\gcd(m, p) = 1$). Then P has distinct roots in $\overline{\mathbb{F}_v} = \overline{k}$ and so the reduction type is $\mathrm{I}_0{}^*$ with $f_v = v(\Delta) - 4$ and $c_v = 1 + \#\{\, x \in k \;:\; x^3 + b' = 0 \,\}$.

  Now we assume that $\alpha \geqslant 4$. Then P has a triple root $T = \bar{0}$ modulo π. Consider the polynomial $Q(Y) := Y^2 - b'\pi^{\alpha-4}$.

- Suppose that $m \equiv 2 \bmod 6$. Then Q has distinct roots modulo π in $\overline{k}$ so the reduction type is IV* with $f_v = v(\Delta) - 6$. Moreover, $c_v = 3$ if and only if b' is a square in k, otherwise $c_v = 1$.

- Suppose finally that $m \equiv 1 \bmod 6$. Then Q has a double root $Y = \bar{0}$ modulo π, and we conclude that the reduction type is II* with $f_v = v(\Delta) - 8$ and $c_v = 1$.

Moreover, in all those cases, this proves that (3.1.1) is a *minimal* integral Weierstrass model (even when $p = 3$, provided that $\gcd(m, p) = 1$).

The other claims about $\deg\left(\Delta_{\min}(E/k(t))\right), f(E/k(t)), c(E/k(t))$ and the Szpiro ratio immediately follow from the above analysis. ■

Coming back to the L-function, proposition 1.3.29 allows us to write

$$\log L(E_{m,b,b'}/k(t), T) = \sum_{n \geqslant 1} a_{m,b,b'}(n) \frac{T^n}{n}$$

where (using the notations[3] from equation (1.3.9) in definition 1.3.27)

$$\begin{aligned} a_{m,b,b'}(n) &:= \sum_{w \in \mathbb{P}^1(k_n)} a_w(E_{m,b,b'}) \\ &= \sum_{w \in \mathbb{P}^1(k_n)} \left(|\mathbb{F}_w| + 1 - |\overline{(E_{m,b,b'})_w}(\mathbb{F}_w)| \right). \end{aligned}$$

Here we see the rational points w as places of $k(t)$ by taking their Galois orbits. We mention that while the notation does not make it explicit, the values $a_{m,b,b'}(n)$ depend on the field of constants k that we fixed.

For each $n \geqslant 1$, denote by

$$A_{E_{m,b,b'}}(\infty, n) := |k_n| + 1 - |\overline{(E_{m,b,b'})_\infty}(k_n)| \tag{3.1.2}$$

the local term at the place $v = v_\infty = [1:0] \in \mathbb{P}^1_k$ (see example 1.3.6), as in equation (1.3.9).

From propositions 1.4.3 and 3.1.5 we get

$$a_{m,b,b'}(n) = A_{E_{m,b,b'}}(\infty, n) - \sum_{t \in k_n} \sum_{x \in k_n} \lambda_{k_n}(x^3 + bx + b't^m) \tag{3.1.3}$$

$$= A_{E_{m,b,b'}}(\infty, n) - \sum_{\chi \in \widehat{k_n^\times}[m]} S_{b,b'}(\chi, n) \tag{3.1.4}$$

where the sum runs over multiplicative characters $\chi : k_n^\times \to \mathbb{C}^\times$ such that $\chi^m = \mathbb{1}$ and where we set

$$S_{b,b'}(\chi, n) := \sum_{z,x \in k_n} \lambda_{k_n}(x^3 + bx + b'z)\chi(z). \tag{3.1.5}$$

First, let us study the local term $A_{m,b}(\infty, k_n)$ at the place at infinity of $k(t)$.

Proposition 3.1.6. *Let $n \geqslant 1$. Let k be a finite field of odd characteristic, $b, b' \in k^\times$ and $m \geqslant 1$ be coprime to* $\mathrm{char}(k)$.

- *If $6 \nmid m$ or if $|k|^n \not\equiv 1 \pmod 3$, then $A_{E_{m,b,b'}}(\infty, n) = 0$.*
- *If $6 \mid m$ and if $|k|^n \equiv 1 \pmod 3$, then*

$$\begin{aligned} A_{E_{m,b,b'}}(\infty, n) &= - \sum_{\psi \in \widehat{k_n^\times}[3]} \psi(-b')\lambda_{k_n}(b')J(\lambda_{k_n}, \psi) \\ &= -\lambda_{k_n}(-1) \sum_{\psi \in \widehat{k_n^\times}[3] \smallsetminus \{\mathbb{1}\}} \psi(-b')\lambda_{k_n}(b')J(\lambda_{k_n}, \lambda_{k_n}\psi^{-1}). \end{aligned}$$

⌟

[3]There is a slight conflict of notation here (the use of the letter "a" twice), but it will not be harmful.

Proof. — When $6 \nmid m$, the curve $E_{m,b,b'}$ has bad reduction of additive type at $v = \infty$ according to proposition 3.1.5, so that $A_{E_{m,b,b'}}(\infty, n) = 0$ for all $n \geqslant 1$ by remark 1.3.28.

When $6 \mid m$, the curve $E_{m,b,b'}$ has good reduction at ∞ with minimal integral Weierstrass model $E_\infty : y^2 = x^3 + b\pi^{4m/6}x + b'$ where $\pi = 1/t$ is a uniformizer at ∞ (thanks to proposition 3.1.5). Denoting the Legendre symbol λ_{k_n} simply by λ, we have

$$\begin{aligned} A_{E_{m,b,b'}}(\infty, n) &= |k_n| + 1 - |\overline{E_\infty}(k_n)| \\ &= -\sum_{x \in k_n} \lambda(x^3 + b') \\ &= -\sum_{z \in k_n} \sum_{\psi \in \widehat{k_n^\times}[3]} \lambda(z + b')\psi(z) \\ &= -\sum_{z' \in k_n} \sum_{\psi \in \widehat{k_n^\times}[3]} \lambda(-b'z' + b')\psi(-b'z') \\ &= -\sum_{\psi \in \widehat{k_n^\times}[3]} \psi(-b')\lambda(b')J(\lambda, \psi). \end{aligned}$$

Observe that

$$\gcd(3, |k_n^\times|) = \gcd(3, |k|^n - 1) = \begin{cases} 3 \text{ if } |k|^n \equiv 1 \pmod 3 \\ 1 \text{ if } |k|^n \equiv -1 \pmod 3. \end{cases}$$

In particular, if $|k|^n \equiv -1 \pmod 3$ then $A_{E_{m,b,b'}}(\infty, n) = 0$. When $|k|^n \equiv 1 \pmod 3$, there is a character $\theta_3 : k_n^\times \to \mathbb{C}^\times$ of order 3, and

$$\begin{aligned} -A_{E_{m,b,b'}}(\infty, n) &= \underbrace{\mathbb{1}(-b')\lambda(b')J(\lambda, \mathbb{1})}_{=0} + \theta_3(-b')\lambda(b')J(\lambda, \theta_3) + \theta_3^2(-b')\lambda(b')J(\lambda, \theta_3^2) \\ &= \lambda(b') \cdot \big(\theta_3(-b')J(\lambda, \theta_3) \ + \ \theta_3^2(-b')J(\lambda, \theta_3^2)\big) \end{aligned}$$

Finally, theorem 2.1.5 in [BEW98] states that

$$\chi, \psi, \chi\psi \text{ non-trivial} \implies J(\chi, \psi) = \chi(-1)J(\chi^{-1}\psi^{-1}, \chi) = \psi(-1)J(\chi^{-1}\psi^{-1}, \psi) \tag{3.1.6}$$

and so $J(\lambda, \lambda\theta_3) = \lambda(-1)J(\theta_3^{-1}, \lambda) = \lambda(-1)J(\theta_3^2, \lambda)$ which yields

$$J(\lambda, \lambda\theta_3^2) + J(\lambda, \lambda\theta_3) = \lambda(-1)\big(J(\theta_3, \lambda) + J(\theta_3^2, \lambda)\big). \qquad \blacksquare$$

3.1.2 Expressing $S_{b,b'}(\chi, n)$ in terms of Jacobi sums

Throughout we let k be a finite field of odd characteristic. Given an integer $n \geqslant 1$ and a multiplicative character $\chi : k_n^\times \to \mathbb{C}^\times$, we wish to express the character sum $S_{b,b'}(\chi, n)$ defined in equation (3.1.5) in terms of well-known Jacobi sums (or Gauss sums).

We can perform an explicit computation if $\chi^2 = \mathbb{1}$.

Lemma 3.1.7. *Let $n \geqslant 1$. We have $S_{b,b'}(\mathbb{1}, n) = 0$ and*

$$S_{b,b'}(\lambda_{k_n}, n) = \lambda_{k_n}(b') \cdot 2|k|^n \cdot \mathbb{1}_{-b \in k_n^{\times,2}}. \tag{3.1.7}$$

Here $\mathbb{1}_{x \in E}$ denotes the value of the indicator function of a set E at x. ⌟

Proof. — • We first treat the case where $\chi = \lambda$. According to [Gri16, lemme 2.2.3], we have

$$\sum_{z\in k_n} \lambda(z^2 + d\cdot z) = \begin{cases} -1 & \text{if } d \neq 0 \\ |k_n| - 1 & \text{if } d = 0. \end{cases}$$

In particular, we get

$$\begin{aligned} S_{b,b'}(\lambda_{k_n}, n) &= \sum_{z,x\in k_n} \lambda_{k_n}(b'z^2 + z(x^3+bx)) \\ &= \lambda_{k_n}(b')\cdot\Big(\sum_{\substack{x\in k_n \\ b'^{-1}(x^3+bx)\neq 0}} (-1) + (|k_n|-1)\cdot(1 + 2\cdot \mathbb{1}_{-b\in k_n^{\times,2}})\Big) \\ &= \lambda_{k_n}(b')\cdot\Big(-(|k_n|-1-2\cdot\mathbb{1}_{-b\in k_n^{\times,2}}) \;+\; |k_n|-1+2\cdot(|k_n|-1)\cdot\mathbb{1}_{-b\in k_n^{\times,2}}\Big) \\ &= \lambda_{k_n}(b')\cdot 2|k|^n\cdot\mathbb{1}_{-b\in k_n^{\times,2}}. \end{aligned}$$

• As for the case $\chi = \mathbb{1}$, we simply have

$$S_{b,b'}(\mathbb{1}, n) = \sum_{x\in k_n}\sum_{z\in k_n} \lambda(x^3+bx+b'z) = \sum_{x\in k_n} 0 = 0. \qquad \blacksquare$$

From now on, we can focus on the case where $\chi^2 \neq \mathbb{1}$, which means $\chi \neq \mathbb{1}, \lambda_{k_n}$. We will first express $S_{b,b'}(\chi, n)$ (defined in equation (3.1.5)) in terms of another sum given as follows. For a multiplicative character ψ on k_n, we set

$$C_b(\psi, n) := \sum_{x\in k_n} \psi(x^3 + bx) \tag{3.1.8}$$

which we may call a "ψ-Jacobsthal sum".

Lemma 3.1.8. *Let $n \geqslant 1$ and $\chi \in \widehat{k_n^\times}$ be such that $\chi^2 \neq \mathbb{1}$. Then the sums from equations (3.1.5) and (3.1.8) satisfy the following identity (involving a Jacobi sum as given in definition 1.4.5)*

$$S_{b,b'}(\chi, n) = \chi(-b'^{-1})J(\lambda_{k_n}, \chi)\cdot C_b(\lambda_{k_n}\chi, n). \qquad \lrcorner$$

Proof. — In what follows, we will generally denote the Legendre symbol λ_{k_n} by λ for simplicity. The terms with $x = 0$ in $S_{b,b'}(\chi, n)$ form the sum of the values of the *non-trivial* character $\lambda\chi$ over $k_n^\times$, so this contributes nothing, since $\chi \neq \lambda$. Then we may consider the sum over the *non-zero* $x \in k_n$, and do a change of variables $z = b'^{-1}xz'$ to get

$$\begin{aligned} S_{b,b'}(\chi, n) &= \sum_{\substack{z', x\in k_n \\ x\neq 0}} \lambda_{k_n}(x^3 + bx + xz')\chi(xz')\chi(b'^{-1}) \\ &= \chi(b'^{-1})\sum_{\substack{x\in k_n \\ x\neq 0}} \Big((\lambda\chi)(x)\chi(-1)\sum_{z'\in k_n}\lambda(x^2+b+z')\chi(-z')\Big). \end{aligned}$$

When $x^2 = -b$, the inner sum over z' vanishes, since $\chi \neq \lambda$ (so that $\chi\lambda$ is not trivial). Therefore, we may assume that $x^2 \neq -b$ and consider the elements $\alpha_x = (b+x^2)^{-1} \in k_n^\times$ to get

$$\chi(-b')S_{b,b'}(\chi, n) = \sum_{x\in k_n, x^2\neq 0, -b} \Big((\lambda\chi)(x\alpha_x^{-1})\sum_{z'\in k_n}\lambda(\alpha_x(x^2+b+z'))\chi(-\alpha_x z')\Big)$$

$$= \sum_{x\in k_n, x^2\neq 0,-b} \Big((\lambda\chi)(x^3+bx)\sum_{z\in k_n}\lambda(1-z)\chi(z)\Big)$$
$$= J(\lambda_{k_n},\chi)\cdot\sum_{x\in k_n}(\lambda\chi)(x^3+bx)$$

which gives the desired result. ∎

We now evaluate the character sums $C_b(\psi,n)$ (defined in equation (3.1.8)) in terms of Jacobi sums.

Proposition 3.1.9. *Let $n\geqslant 1$ and $\psi\in\widehat{k_n^\times}$. We have*

$$C_b(\psi,n)=\psi(b)\sum_{\substack{\theta\in\widehat{k_n^\times}\\ \theta^2=\psi}}\theta(-b)J(\theta,\psi)=\psi(b)\sum_{\substack{\theta\in\widehat{k_n^\times}\\ \theta^2=\psi}}\theta(-b)J(\theta,\theta^2).$$

In particular, if ψ is an odd character, i.e. $\psi(-1)=-1$, then $C_b(\psi,n)=0$, because then there is no character θ such that $\theta^2=\psi$, so the sum vanishes. ⌟

Proof. —

- If $\psi(-1)=-1$ then by setting $x=-x'$ we obtain

$$C_b(\psi,n)=\sum_{x'\in k}\psi(-x'^3-bx')=\psi(-1)\sum_{x'\in k}\psi(x'^3+bx')=-C_b(\psi,n) \tag{3.1.9}$$

  so that $C_b(\psi,n)=0$.

- If $\psi(-1)=1$ then by [Gri16, lemme 2.1.1], there is a character $\theta\in\widehat{k_n^\times}$ such that $\theta^2=\psi$ (and there are exactly two such characters, the other being $\theta\lambda$). Then

$$\begin{aligned}C_b(\psi,n)&=\sum_{x\in k_n}\theta(x^2)\psi(x^2+b)\\&=\sum_{s\in k_n}\theta(s)\psi(s+b)(1+\lambda_{k_n}(s))\\&=\sum_{s'\in k_n}\theta(-1)\theta(-bs')\psi(bs'+b)(1+\lambda_{k_n}(bs'))\\&=\theta(-1)(\theta\psi)(b)\sum_{s'\in k_n}\theta(-s')\psi(s'+1)(1+\lambda_{k_n}(bs'))\\&=\psi(b)\theta(-b)\Big(J(\theta,\psi)\ +\ \lambda_{k_n}(-b)J(\theta\lambda,\psi)\Big)\end{aligned}$$

  which is indeed equal to the claimed formulas (the second formula is obtained by replacing ψ by θ^2). ∎

We can now summarize the above results in order to express the coefficients $a_{m,b,b'}(n)$ of the L-function (as given in equation (3.1.4)) in terms of Jacobi sums. To this end, it is convenient to introduce the following set of characters on $k_n^\times$.

Definition 3.1.10. Given an integer $n\geqslant 1$, we let

$$X_m(n):=\begin{cases}\widehat{k_n^\times}[2m]\smallsetminus\big(\widehat{k_n^\times}[4]\cup\widehat{k_n^\times}[3]\big) & \text{if } m \text{ is even}\\ \widehat{k_n^\times}[4m]\smallsetminus\big(\widehat{k_n^\times}[2m]\cup\widehat{k_n^\times}[4]\big) & \text{if } m \text{ is odd.}\end{cases}$$ ⌟

Note that when m is even, the subgroup $\widehat{k_n^\times}[3]$ is non-trivial if and only if $6 \mid m$ (which is related to the condition we have in proposition 3.1.6).

Corollary 3.1.11. *Let k be a finite field of odd characteristic and fix $b, b' \in k^\times$. Let $m \geqslant 1$ be an integer coprime to $\mathrm{char}(k)$. Then for all $n \geqslant 1$, the coefficient $a_{m,b,b'}(n)$ from equation (3.1.4) can be expressed as*

$$\begin{aligned} a_{m,b,b'}(n) &= -\lambda_{k_n}(b') \cdot 2|k|^n \cdot \mathbb{1}_{-b \in k_n^{\times,2}} \cdot \mathbb{1}_{m \text{ even}} \\ &\quad - \lambda_{k_n}(-b') \sum_{\theta \in X_m(n)} \theta^2(b'^{-1})\theta^3(-b) J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot J(\theta, \theta^2) \end{aligned} \tag{3.1.10}$$

where $\mathbb{1}_{m \text{ even}}$ equals 1 if m is even and 0 otherwise. ⌟

Proof. — • The first step is to combine equation (3.1.4), lemmas 3.1.7 and 3.1.8, and proposition 3.1.9. We find

$$\begin{aligned} a_{m,b,b'}(n) = A_{E_{m,b,b'}}(\infty, n) \\ - \lambda_{k_n}(b') \cdot 2|k|^n \cdot \mathbb{1}_{-b \in k_n^{\times,2}} \cdot \mathbb{1}_{m \text{ even}} \quad - \sum_{\chi \in \widehat{k_n^\times}[m] \smallsetminus \widehat{k_n^\times}[2]} S_{b,b'}(\chi, n), \end{aligned}$$

and for all $\chi \in \widehat{k_n^\times}[m] \smallsetminus \widehat{k_n^\times}[2]$ we have

$$\begin{aligned} S_{b,b'}(\chi, n) &= \chi(-b'^{-1}) J(\lambda_{k_n}, \chi) \cdot (\lambda_{k_n}\chi)(b) \sum_{\theta^2 = \lambda_{k_n}\chi} \theta(-b) J(\theta, \theta^2) \\ &= \sum_{\theta^2 = \lambda_{k_n}\chi} \Big((\lambda_{k_n}\theta^2)(-b'^{-1}) J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot \theta^2(b)\theta(-b) J(\theta, \theta^2) \Big) \\ &= \lambda_{k_n}(-b'^{-1}) \sum_{\theta^2 = \lambda_{k_n}\chi} \theta^2(b'^{-1})\theta^3(-b) J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot J(\theta, \theta^2). \end{aligned}$$

It is easy to check the following equality of sets of characters

$$X'_m(n) := \left\{ \theta \in \widehat{k_n^\times} \ : \ \exists \chi \in \widehat{k_n^\times},\ \theta^2 = \lambda_{k_n}\chi,\ \chi^m = \mathbb{1}, \chi^2 \neq \mathbb{1} \right\} \tag{3.1.11}$$

$$= \begin{cases} \widehat{k_n^\times}[2m] \smallsetminus \widehat{k_n^\times}[4] & \text{if } m \text{ is even} \\ \widehat{k_n^\times}[4m] \smallsetminus (\widehat{k_n^\times}[2m] \cup \widehat{k_n^\times}[4]) & \text{if } m \text{ is odd.} \end{cases} \tag{3.1.12}$$

This allows to re-write the coefficients $a_{m,b,b'}(n)$ as follows:

$$\begin{aligned} a_{m,b,b'}(n) = A_{E_{m,b,b'}}(\infty, n) - \lambda_{k_n}(b') \cdot 2|k|^n \cdot \mathbb{1}_{-b \in k_n^{\times,2}} \cdot \mathbb{1}_{m \text{ even}} \\ - \lambda_{k_n}(-b'^{-1}) \sum_{\theta \in X'_m(n)} \theta^2(b'^{-1})\theta^3(-b) J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot J(\theta, \theta^2). \end{aligned} \tag{3.1.13}$$

- The second step is to take care of the local term at infinity. In the above sum, none of $\lambda_{k_n}, \lambda_{k_n}\theta^2, \theta^2$ is trivial (since $\theta^4 \neq \mathbb{1}$). On the other hand, the second Jacobi sum $J(\theta, \theta^2)$ is a root of unity if and only if $\theta^3 = \mathbb{1}$ by proposition 1.4.6 (since none of θ, θ^2 can be trivial). We now distinguish two cases.

– Assume that $3 \nmid m$ or that $|k_n| \equiv -1 \pmod 3$. Then there is no character of order 3 in $X'_m(n)$. In other words, in this case, we have $X'_m(n) = X_m(n)$ and proposition 3.1.6 tells us that in this case we have $A_{m,b}(\infty, k_n) = 0$. Then we see that equation (3.1.13) is exactly the same as equation (3.1.10).

– Assume that $3 \mid m$ and m is odd and $|k_n| \equiv 1 \pmod 3$. Then there is indeed a character $\theta_3 \in \widehat{k_n^\times}[m]$ of order 3, but $\chi := \theta_3^2\lambda_{k_n}$ satisfies $\chi^m = \lambda_{k_n} \neq \mathbb{1}$, so $\theta_3 \notin X'_m(n)$. In other words, in that case, we have $X'_m(n) = X_m(n)$ and furthermore we have $A_{m,b,b'}(\infty, k_n) = 0$ by proposition 3.1.6. Hence we see that equation (3.1.13) is exactly the same as equation (3.1.10).

– Assume that $3 \mid m$ and m is even (equivalently $6 \mid m$) and $|k_n| \equiv 1 \pmod 3$. Then there is indeed a character $\theta_3 \in \widehat{k_n^\times}[m]$ of order 3, and $\chi := \theta_3^2\lambda_{k_n}$ satisfies $\chi^m = \mathbb{1}$, so $\theta_3, \theta_3^{-1} \in X'_m(n)$. The above sum (appearing in (3.1.13)) over the two terms $\{\theta_3, \theta_3^{-1}\} \subset X'_m(n)$ reduces to, in view of proposition 1.4.6 (recall that $\theta_3^2 = \theta_3^{-1}$):

$$\begin{aligned} &- \lambda_{k_n}(-b'^{-1}) \sum_{\theta \in \{\theta_3^{\pm 1}\}} \theta^2(b'^{-1})\theta^3(-b)J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot J(\theta, \theta^2) \\ =& - \lambda_{k_n}(-b') \sum_{\theta \in \{\theta_3^{\pm 1}\}} \theta^2(b'^{-1})J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot (-\theta(-1)) \\ =& \ \lambda_{k_n}(-b') \sum_{\theta \in \{\theta_3^{\pm 1}\}} \theta(-b')J(\lambda_{k_n}, \lambda_{k_n}\theta^2). \end{aligned}$$

Furthermore, in this case we have by proposition 3.1.6:

$$A_{E_{m,b,b'}}(\infty, n) \ = \ -\lambda_{k_n}(-b') \sum_{\psi \in \widehat{k_n^\times}[3] \smallsetminus \{\mathbb{1}\}} \psi(-b')J(\lambda_{k_n}, \lambda_{k_n}\psi^{-1}).$$

Thereby we find

$$\begin{aligned} a_{m,b,b'}(n) = &-\lambda_{k_n}(b') \cdot 2|k|^n \cdot \mathbb{1}_{-b \in k_n^{\times,2}} \cdot \mathbb{1}_{m \text{ even}} \\ &- \lambda_{k_n}(-b') \sum_{\substack{\theta \in X'_m(n) \\ \theta^3 \neq \mathbb{1}}} \theta^3(-b)\theta^2(b'^{-1})J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot J(\theta, \theta^2) \end{aligned}$$

which means that formula (3.1.10) holds, as claimed. ∎

Remark 3.1.12. Given a non-trivial character $\chi \in \widehat{k^\times}$ such that $\chi^2, \chi^3 \neq \mathbb{1}$, proposition 1.4.6 gives

$$J(\lambda_k, \lambda_k\chi^2)J(\chi, \chi^2) = \frac{G(\lambda_k)G(\lambda_k\chi^2)}{G(\chi^2)} \frac{G(\chi)G(\chi^2)}{G(\chi^3)} = J(\lambda_k, \chi, \lambda_k\chi^2). \qquad ⌟$$

3.1.3 Proof of theorem 3.1.3

Now that we have computed the coefficients $a_{b,b',m}(n)$ explicitly in terms of Jacobi sums, we can apply proposition 1.4.26 to express the L-function of the elliptic curve $E_{m,b,b'}$ as a rational function.

Proof of theorem 3.1.3. — Let us check the two assumptions from proposition 1.4.26 on the map $\alpha_{b,b'}$ considered in definition 3.1.1. For simplicity, we will simply denote this map by α in the sequel.

- Let $n \geqslant 1$ and $\theta \in \widehat{k_n^\times}$. We want to prove that $\alpha(\theta) = \alpha(\theta^{|k|})$. Since $b \in k$, we have $b^{|k|} = b$ so $\theta^3(-b) = (\theta^{|k|})^3(-b)$. Moreover, since $|k|$ is odd we have $\lambda_{k_n}^{|k|} = \lambda_{k_n}$, so that proposition 1.4.6.3 yields

$$J(\lambda_{k_n}, \lambda_{k_n}\theta^2) = J(\lambda_{k_n}^{|k|}, \lambda_{k_n}^{|k|}\theta^{2|k|}) = J(\lambda_{k_n}, \lambda_{k_n} \cdot (\theta^{|k|})^2).$$

  The same holds for the other Jacobi sum occurring in $\alpha(\theta)$, so this proves the first needed hypothesis.

- Let us fix two finite extensions $L \supset F \supset k$ and a character θ on $F^\times$. We wish to show that $\alpha(\theta \circ \mathrm{N}_{L/F}) = \alpha(\theta)^{[L:F]}$. We perform a direct computation, applying Hasse–Davenport relation 1.4.7 (recalling that $b \in k$ so that $\mathrm{N}_{L/F}(b) = b^{[L:F]}$ and using remark 1.4.2):

$$\begin{aligned}\alpha(\theta \circ \mathrm{N}_{L/F}) &= \lambda_L(-1)\theta^3(\mathrm{N}_{L/F}(-b)) \cdot J(\lambda_F \circ \mathrm{N}_{L/F}, (\lambda_F \cdot \theta^2) \circ \mathrm{N}_{L/F}) \cdot J(\theta \circ \mathrm{N}_{L/F}, \theta^2 \circ \mathrm{N}_{L/F}) \\ &= \big(\lambda_F(-1)\theta^3(-b)\big)^{[L:F]} \cdot (-1)(-J(\lambda_F, \lambda_F\theta^2))^{[L:F]} \cdot (-1)(-J(\theta, \theta^2))^{[L:F]} \\ &= \alpha(\theta)^{[L:F]}.\end{aligned}$$

Then a direct application of proposition 1.4.26 gives the result, in view of definition 3.1.10 and corollary 3.1.11, since

$$\log L(E_{m,b,b'}/k(t), T) = \sum_{n \geqslant 1} a_{m,b,b'}(n)\frac{T^n}{n},$$

$$a_{m,b,b'}(n) = -\lambda_{k_n}(b') \cdot 2|k|^n \cdot \mathbb{1}_{-b \in k_n^{\times,2}} \cdot \mathbb{1}_{m \text{ even}} - \sum_{\theta \in X_m(n)} \alpha_{b,b'}(\theta)$$

We explain in detail how to compute the factor $\epsilon_{m,b,b',k}(T)$ given by

$$\log(\epsilon_{m,b,b',k}(T)) = -\sum_{n \geqslant 1} \lambda_{k_n}(b') \cdot 2|k|^n \cdot \mathbb{1}_{-b \in k_n^{\times,2}} \cdot \mathbb{1}_{m \text{ even}} \cdot \frac{T^n}{n}.$$

- First, if m is odd then $-\lambda_{k_n}(b') \cdot 2|k|^n \cdot \mathbb{1}_{-b \in k_n^{\times,2}} \cdot \mathbb{1}_{m \text{ even}} = 0$ for all b, b', n so we get $\epsilon_{m,b,b',k}(T) = 1$.

- From now on, we assume that m is even. If $-b$ and b' are both squares in $k^\times$, then

$$\log(\epsilon_{m,b,b',k}(T)) = -2\sum_{n \geqslant 1} \frac{(|k|T)^n}{n} = \log((1 - |k|T)^2).$$

- If $-b$ is a square in $k^\times$ and b' is not a square in $k^\times$, then we split the sum according to whether n is odd or even:

$$\begin{aligned}\log(\epsilon_{m,b,b',k}(T)) &= -2\sum_{n' \geqslant 1} \frac{(|k|T)^{2n'}}{2n'} + (-2)\sum_{n' \geqslant 0}(-1)\frac{(|k|T)^{2n'+1}}{2n'+1} \\ &= \log(1 - (|k|T)^2) + 2\operatorname{arctanh}(|k|T) = \log(1 - (|k|T)^2) + \log\left(\frac{1+|k|T}{1-|k|T}\right) \\ &= \log((1 + |k|T)^2).\end{aligned}$$

- Finally, if $-b$ is not a square in $k^\times$, then

$$\log(\epsilon_{m,b,b',k}(T)) = -2\sum_{n'\geqslant 1} |k|^n \cdot \frac{T^{2n'}}{2n'} = \log(1-(|k|T)^2).$$

This finishes the proof of theorem 3.1.3. ■

Remark 3.1.13. We can make a sanity check about the degree of the L-function (as a polynomial in T), say in the case where m is even and $6 \nmid m$. On the one hand, it is equal to

$$2+\sum_{r\in Z(m)/\langle|k|\rangle} u_{|k|,d(m)}(r) = 2+\#(\mathbb{Z}/2m\mathbb{Z}\smallsetminus\{0,m/2,m,3m/2\}) \quad = \quad 2+(2m-4) = 2m-2.$$

On the other hand, it should be equal to $f(E_{m,b,b'})-4$ by theorem 1.3.30. Since we assumed $6 \nmid m$, we get from proposition 3.1.5 that $f(E_{m,b,b'}) = 2m+2$, which is consistent with our computation. ⌟

3.1.4 Explicit Jacobi sums and analytic rank

In view of theorem 3.1.3, we know that the analytic rank of $E_{m,b,b'}$ over $k(t)$, i.e. the order of vanishing of its L-function at $T = |k|^{-1}$, is given by (using the notations from definition 3.1.1)

$$\begin{aligned}\rho(E_{m,b,b'}/k(t)) &= \operatorname*{ord}_{T=|k|^{-1}} \epsilon_{m,b,b',k}(T) + \#\{\,[r]\in Z(m)/\langle|k|\rangle \;:\; \alpha_{b,b'}(\theta_{k_{u(r)},d,r}) = |k|^{u(r)}\,\} \\ &= \operatorname*{ord}_{T=|k|^{-1}} \epsilon_{m,b,b',k}(T) + \#\{\,[r]\in Z(m)/\langle|k|\rangle \;:\; \alpha_{b,b'}(\theta_{k_{u(r)},d,r}) \in \mathbb{R}_{>0}\,\}\end{aligned} \tag{3.1.14}$$

(The second equality follows because $\alpha_{b,b'}(\theta_{k_{u(r)},d,r})$ has complex modulus equal to $|k|^{u(r)}$; see proposition 1.4.6 or theorem 1.3.30).

In some cases, *all* the coefficients $\alpha_{b,b'}(\theta)$ are actually positive integers, which allows an explicit formula for the rank of $E_{m,b,b'}$.

Corollary 3.1.14. *Let k be a finite field of odd characteristic $p\geqslant 3$ and fix $b,b'\in k^\times$. Let $m\geqslant 1$ be an integer and set $d=d(m) := \frac{4m}{\gcd(2,m)}$ as in definition 3.1.1. Assume that:*

1. *Either $|k|^\nu \equiv -1 \bmod d(m)$ for some integer $\nu\geqslant 1$ (in particular, m is coprime to $|k|$).*
2. *Or $p^\nu \equiv -1 \bmod d(m)$ for some integer $\nu\geqslant 1$ and the degrees of b and b' over $\mathbb{F}_p$ are both odd (that is, $[\mathbb{F}_p(b,b'):\mathbb{F}_p]$ is odd).*

Then the (algebraic) rank of $E_{m,b,b'}(k(t))$ is equal to

$$\sum_{\substack{e\mid d(m)\\ e\nmid 4, e\nmid \delta_m}} \frac{\phi(e)}{\operatorname{ord}^\times(|k| \bmod e)} + \begin{cases} 2 & \text{if } m \text{ is even and } -b\in k^{\times,2} \text{ and } b'\in k^{\times,2}\\ 0 & \text{if } m \text{ is even and } -b\in k^{\times,2} \text{ and } b'\notin k^{\times,2}\\ 1 & \text{if } m \text{ is even and } -b\notin k^{\times,2}\\ 0 & \text{if } m \text{ is odd.}\end{cases}$$

where

$$\delta_m := \begin{cases} 3 & \text{if } m \text{ is even} \\ 2m & \text{if } m \text{ is odd} \end{cases}$$

In particular when m is even, we have

$$\operatorname{rk} E_{m,b,b'}(k(t)) \geqslant \frac{2m-6}{\operatorname{ord}^\times(|k| \bmod 2m)}.$$

Proof. — As mentioned at the beginning of the chapter, theorem 1.3.40 ensures that $E_{m,b,b'}$ satisfies the Birch–Swinnerton-Dyer conjecture 1.3.34, so the algebraic rank coincides with the analytic rank.

Let us fix $r \in Z(m) \subset \mathbb{Z}/d(m)\mathbb{Z}$ and set $u(r) := u_{|k|,d}(r)$. We have $r \not\equiv 0$ and $r \not\equiv \frac{d}{2} \bmod d$ (see remark 3.1.2). To ease the notation, let us write the Legendre symbol of $k_{u(r)}$ as $\lambda := \lambda_{k_{u(r)}}$ and set $\theta := \theta_{k_{u(r)},d,r}$.

We check that none of $\lambda\theta^2, \theta^2, \theta^3$ is trivial. Recall from proposition 1.4.17 that θ has order exactly $\frac{d}{(d,r)}$. Since $r \in Z(m)$, it can be seen (using definition 3.1.1 and remark 3.1.2) that $\frac{d}{(d,r)} \notin \{2,3,4\}$. It follows that $\lambda\theta^2, \theta^2, \theta^3 \neq \mathbb{1}$.

- In the case where $|k|^\nu \equiv -1 \pmod d$, we may apply corollary 1.4.29, which ensures that $u(r)$ is even so that $k_{u(r)}$ has a unique quadratic subfield $k_{u(r)/2}$ (which contains k) and also that the restriction of θ to $k_{u(r)/2}$ is trivial.

  Observe that the Legendre symbol $\lambda_{k_{u(r)}}$ is trivial on $k_{u(r)/2}$. In particular, the restrictions of $\lambda, \lambda\theta^2$ and θ^2 to $k_{u(r)/2}$ are all trivial.

  Thus, the characters $\lambda, \lambda\theta^2$ and θ, θ^2 satisfy the hypothesis of Tate–Shafarevich theorem 1.4.8, which yields

$$\begin{aligned} \alpha_{b,b'}(\theta) &= \lambda(-b')\theta(-b^3b'^{-2}) \cdot J(\lambda, \lambda\theta^2) \cdot J(\theta, \theta^2) && \text{definition 3.1.1} \\ &= 1 \cdot 1 \cdot |k_{u(r)}|^{1/2} \cdot |k_{u(r)}|^{1/2} && \text{theorem 1.4.8} \\ &= |k|^{u(r)} \end{aligned}$$

- In the case where hypothesis 2 holds, we rather apply lemma 1.4.30 to get

$$\begin{aligned} \alpha_{b,b'}(\theta) &= \lambda(-b')\theta(-b^3b'^{-2}) \cdot (\pm 1) \cdot |k_{u(r)}|^{1/2} \cdot (\pm 1) \cdot |k_{u(r)}|^{1/2} \\ &= |k_{u(r)}| \end{aligned}$$

  since θ is trivial on $k' := \mathbb{F}_p(b,b')$ by lemma 1.4.30 because this field has *odd* degree over $\mathbb{F}_p$, and $\lambda_{k_{u(r)}}$ is trivial on k' since the degree $[k_{u(r)} : k']$ is even once again by lemma 1.4.30.

Thus from equation (3.1.14) and lemma 1.4.27 we deduce that

$$\begin{aligned} \operatorname{rk} E_{m,b,b'}(k(t)) &= \rho(E_{m,b,b'}/k(t)) \\ &= \left| Z(m) \Big/ \langle |k| \rangle^\times \right| + \operatorname*{ord}_{T=|k|^{-1}} \epsilon_{m,b,b',k}(T) \end{aligned} \tag{3.1.15}$$

$$= \begin{cases} \sum_{\substack{e \mid 2m \\ e \nmid 4}} \frac{\phi(e)}{\mathrm{ord}^\times(|k| \bmod e)} & \text{if } m \text{ is even and } 6 \nmid m \\ \sum_{\substack{e \mid 2m \\ e \nmid 4, e \nmid 3}} \frac{\phi(e)}{\mathrm{ord}^\times(|k| \bmod e)} & \text{if } m \text{ is even and } 6 \mid m \\ \sum_{\substack{e \mid 4m \\ e \nmid 2m, e \nmid 4}} \frac{\phi(e)}{\mathrm{ord}^\times(|k| \bmod e)} & \text{if } m \text{ is odd} \end{cases}$$

$$+ \begin{cases} 2 & \text{if } m \text{ is even and } -b \in k^{\times,2} \text{ and } b' \in k^{\times,2} \\ 0 & \text{if } m \text{ is even and } -b \in k^{\times,2} \text{ and } b' \notin k^{\times,2} \\ 1 & \text{if } m \text{ is even and } -b \notin k^{\times,2} \\ 0 & \text{if } m \text{ is odd.} \end{cases}$$

For the last equality, note for instance that when m is even and $6 \nmid m$, then the *additive* order of any $r \in \mathbb{Z}/2m\mathbb{Z}$ divides 4 if and only if $r \in \frac{m}{2}\mathbb{Z}/2m\mathbb{Z}$. Looking at the proof of lemma 1.4.27 we see that we need the condition $e \nmid 4$ in the above sum, since $r \in Z(m)$. The other cases are treated in a similar way. (Observe also that when $6 \nmid m$ is even and $e \mid 2m, e \nmid 4$, then we automatically have $e \nmid 3$).

The last inequality follows from item 2 of lemma 1.4.27: when m is even, we have

$$\sum_{\substack{e \mid d(m) \\ e \nmid 4, e \nmid \delta_m}} \frac{\phi(e)}{\mathrm{ord}^\times(|k| \bmod e)} \geqslant \frac{d(m) - \phi(1) - \phi(2) - \phi(3) - \phi(4)}{\mathrm{ord}^\times(|k| \bmod d(m))}. \qquad \blacksquare$$

Remark 3.1.15. Because $d(m)$ is a multiple of 4 for any $m \geqslant 1$ (we keep the notations from definition 3.1.1), the condition $p^\nu \equiv -1 \bmod d(m)$ given in item 2 of corollary 3.1.14 forces $p \equiv -1 \pmod 4$ and ν to be odd. ⌟

When $p \equiv -1 \bmod 4$ is prime and e is odd, we can say more about the rank of $E_{m,b,b'}$ over $\mathbb{F}_{p^{2e}}(t)$, for instance if $m = \frac{p^e+1}{2}$ (which is even) or if $m = \frac{p^e+1}{4}$ and $p^e \equiv 3 \pmod 8$ (so that m is odd).

Corollary 3.1.16. *Let p be a prime such that $p \equiv -1 \pmod 4$, $e \geqslant 1$ be an odd integer. Let $m \geqslant 1$ be an integer and set $d = d(m) = \frac{4m}{\gcd(2,m)}$. Let $b, b' \in \mathbb{F}_{p^e}^\times$ be any elements.*

If $p^e \equiv -1 \pmod d$, then we have

$$L(E_{m,b,b'}/\mathbb{F}_{p^{2e}}(t), T) = (1 - p^{2e}T)^{|Z(m)| + 2 \cdot \mathbb{1}_{m \text{ even}}}$$

so the rank of $E_{m,b,b'}$ over $\mathbb{F}_{p^{2e}}(t)$ is

$$\mathrm{rk}\, E_{m,b,b'}(\mathbb{F}_{p^{2e}}(t)) = \begin{cases} 2m - 4 & \text{if } 6 \mid m \\ 2m - 2 & \text{if otherwise.} \end{cases}$$

Moreover, the algebraic rank over $\mathbb{F}_{p^{2e}}(t)$ is equal to the geometric rank, and when $m = \frac{p^e+1}{2}$, Brumer's bound from theorem 2.2.6 is asymptotically attained as $m \to +\infty$. ⌟

Proof. — We notice that $\langle p^{2e} \rangle^\times$ acts trivially on $Z(m) \subset \mathbb{Z}/d(m)\mathbb{Z}$ since $p^e \equiv -1 \pmod d$. Note that $b, b' \in \mathbb{F}_{p^e}^\times$ are necessarily both squares in $\mathbb{F}_{p^{2e}}$, so that $\epsilon_{m,b,b',\mathbb{F}_{p^{2e}}}(T) = (1 - p^{2e}T)^2$ if m is even and $\epsilon_{m,b,b',\mathbb{F}_{p^{2e}}}(T) = 1$ if m is odd. Observe that b, b' have odd degree over

$\mathbb{F}_p$ since e is odd. By equations (3.1.14) and (3.1.15) and theorem 3.1.3, we know that the L-function $L(E_{m,b,b'}/\mathbb{F}_{p^{2e}}(t), T)$ is as displayed above. The rank $\operatorname{rk} E_{m,b,b'}(\mathbb{F}_{p^{2e}}(t))$ is therefore equal to

$$\begin{cases} 2 & \text{if } m \text{ is even} \\ 0 & \text{if } m \text{ is odd} \end{cases} + \begin{cases} 2m-4 & \text{if } m \text{ is even and } 6 \nmid m \\ 2m-6 & \text{if } m \text{ is even and } 6 \mid m \\ 4m-(2m+4)+2 = 2m-2 & \text{if } m \text{ is odd.} \end{cases}$$

Moreover, the same reasoning applies if we replace $\mathbb{F}_{p^{2e}}(t)$ by $k(t)$ for any finite extension $k \supset \mathbb{F}_{p^{2e}}$, so the geometric rank is equal to $\operatorname{rk} E_{m,b,b'}(\mathbb{F}_{p^{2e}}(t))$. This can be also be proved by noticing (thanks to proposition 3.1.5) that $\operatorname{rk} E_{m,b,b'}(\mathbb{F}_{p^{2e}}(t)) = f(E_{m,b,b'}) - 4$, so that the upper bound from equation (1.3.12) in remark 1.3.33 is an equality. Since the *degree of* the conductor does not depend on the field of constants, the fact that this upper bound is an equality shows that the geometric rank must also be equal to $f(E_{m,b,b'}) - 4$.

Finally, Brumer's bound indicates that

$$\begin{aligned} p^e + \mathcal{O}(1) = \operatorname{rk} E_{m,b,b'}(\mathbb{F}_{p^{2e}}(t)) &\leqslant \frac{f(E_{m,b,b'})\log(p^{2e})}{2\log(f(E_{m,b,b'}))}(1+o(1)) \\ &= \frac{2m\log(p^{2e})}{2\log(2m)}(1+o(1)) = \frac{2e\cdot p^e\log(p)}{2e\log(p)}(1+o(1)), \end{aligned}$$

so we see that this upper bound is asymptotically sharp (in the sense that the ratio between the rank and Brumer's upper bound tends to 1), as $m \to +\infty$. ■

Remark 3.1.17. Corollary 3.1.16 generalizes and makes more precise a result stated in [Shi86, remark 10]. Namely, Shioda showed (using other techniques) that if $p \equiv -1 \bmod 4$ and e is odd, then the rank of $y^2 = x^3 + x + t^{\frac{p^e+1}{2}}$ over $\overline{\mathbb{F}_p}(t)$ equals

$$\begin{cases} p^e - 3 & \text{if } p \equiv -1 \bmod 12 \\ p^e - 1 & \text{if } p \not\equiv -1 \bmod 12. \end{cases}$$

Indeed, $m := \frac{p^e+1}{2}$ is even so $d(m) = p^e + 1$ and $6 \mid m \iff p^e \equiv -1 \mod 12$.

We showed that this rank is achieved over $\mathbb{F}_{p^{2e}}(t)$, which is an unproven claim in [Ulm02, §1.8]. ⌟

Example 3.1.18. When m is even, there are always the obvious solutions $(0, \pm t^{m/2}) \in E_{m,b,1}(K)$ on $y^2 = x^3 + bx + t^m$. We give here an example when m is odd, by taking $p = 5$, $m = \frac{p+1}{2} = 3$ and $b = -1$. We thus consider the curve

$$E := E_{3,-1,1} : y^2 = x^3 - x + t^3 \quad \text{over } \mathbb{F}_5(t).$$

Notice that $p \equiv 1 \bmod 4$ so that corollary 3.1.14 does not apply. However theorem 3.1.3 can be used to get $L(E/\mathbb{F}_5(t), T) = (5T)^4 + 1 = \prod_{\zeta^8=1\neq\zeta^4}(1 - 5\zeta T)$. From proposition 1.3.43 we find, for any $n \geqslant 1$:

$$L(E/\mathbb{F}_{5^n}(t), T) = \prod_{\zeta^8=1\neq\zeta^4}(1 - (5\zeta)^n T),$$

so the rank is 0 over $\mathbb{F}_{5^4}(t)$ and is 4 over $\mathbb{F}_{5^8}(t)$.

Can we even give an example of a point on E over $K := \mathbb{F}_{5^8}(t)$? Since the discriminant of this Weierstrass equation is $3t^6 + 4$, Shioda's theorem 1.3.24 indicates that any point in the narrow Mordell–Weil lattice has height $\geqslant \deg(\Delta)/6 = 1$. We may then try to find an *integral* point $P = (x, y) \in E(K)$ where x has degree 1, say $x(t) = at + b$. We want

$$x^3 - x + t^3 = (a^3 + 1)t^3 + 3a^2bt^2 + (3ab^2 - a)t + b^3 - b$$

to be a square in K, which can only happen if $a^3 = -1$, so we may set $a = -1$. We wish to find $b, c, d \in \mathbb{F}_{5^8}$ so that $3bt^2 + (1 - 3b^2)t + b^3 - b = (ct + d)^2 = c^2t^2 + 2cdt + d^2$.

We find

$$b = \frac{c^2}{3} = 2c^2, \quad 2cd = 1 - 3(2c^2)^2, \quad d^2 = b^3 - b = (2c^2)^3 - 2c^2,$$

and since $c \neq 0$ we get $d = \frac{1-12c^4}{2c}$ from the second equation. Replaced in the third equation, we get $d^2 = \frac{(1-2c^4)^2}{-c^2} = 8c^6 - 2c^2$. This is an equation of degree 8 in c over $\mathbb{F}_5$, so it has a solution in $\mathbb{F}_{5^8}$, hence there is a point $P = \left(-t + 2c^2, ct + \frac{1-12c^4}{2c}\right)$ in $E(\mathbb{F}_{5^8}(t))$. ⌟

Example 3.1.19. Corollary 3.1.14 predicts that $y^2 = x^3 + x + t^7$ has rank 2 over $\mathbb{F}_3(t)$, since $p^3 \equiv -1 \bmod d(m)$ where $p := 3$ and $m := 7$ (so $d(m) = 28$). Can we exhibit some rational points? This can be done for instance using techniques described in section 3.3. We found no *integral* points with $\deg(x(t)) \leqslant 14$, and the rational point with the smallest $\deg(x)$ we found is

$$P = \left(\frac{t^6 + 2t^5 + t^4 + t^2 + 1}{t^2}\ ,\ \frac{2t^9 + 2t^6 + t^4 + 2}{t^3}\right).$$

We also found the point

$$Q = \left(\frac{t^{18} + t^{15} - t^{13} + t^{12} + t^6 + 1}{t^6}\ ,\ \frac{-t^{27} + t^{18} - t^{12} + 1}{t^9}\right).$$

Using lemma 3.2.15 to be stated later, one can check that $\hat{h}(P) = h(P) = 6$ and $\hat{h}(Q) = h(Q) = 18$. From this it can be shown that P, Q are linearly independent in $E(K)$. Indeed, if we had $aP = bQ$ for some integers a, b then we would get (by taking the heights on both sides) $6a^2 = 18b^2$, but $\sqrt{3}$ is irrational. ⌟

3.1.5 Unbounded ranks

We explain here that the curves $E_{m,b,b'}$ provide a Kummer family of (non-isotrivial if $p > 3$) elliptic curves with unbounded rank over $\mathbb{F}_p(t)$, for any odd prime p.

Corollary 3.1.20. *Fix any odd prime p and $b, b' \in \mathbb{F}_p^\times$. Then the rank in the Kummer family $\{E_{m,b,b'}/\mathbb{F}_p(t); m \geqslant 1\}$ is unbounded, that is*

$$\sup\{\operatorname{rk} E_{m,b,b'}(\mathbb{F}_p(t)) \ :\ m \geqslant 1\} = +\infty.$$ ⌟

Proof. — • Assume first that $p \equiv -1 \bmod 4$. For any odd integer $\nu \geqslant 1$, consider the even integer $m_\nu := \frac{p^\nu+1}{2}$. Note that $\operatorname{ord}^\times(p \bmod 2m_\nu)$ divides 2ν. Therefore, the last inequality in corollary 3.1.14 yields

$$\operatorname{rk} E_{m_\nu,b,b'}(\mathbb{F}_p(t)) \geqslant \frac{2m_\nu - 6}{2\nu} = \frac{p^\nu - 5}{2\nu},$$

which proves the claim in that case, by letting $\nu \to +\infty$ (among odd integers).

- Suppose now that $p \equiv 1 \bmod 4$ and let $k = \mathbb{F}_p$. Consider an *even* integer $\nu \geqslant 1$ and set $m = m_\nu = p^\nu + 1$. We have $d := d(m) = 2m$; moreover m is even, $6 \nmid m$ and $m/2$ is odd. Recall from equation (3.1.14) that the analytic rank satisfies

$$\rho(E_{m,b,b'}/k(t)) \geqslant \#\{\, [r] \in Z(m)/\langle |k| \rangle \;:\; \alpha_{b,b'}(\theta_{k_{u(r)},d,r}) = |k|^{u(r)} \,\}.$$

While corollary 3.1.14 does *not* apply (as mentioned in remark 3.1.15), we claim that *at least* roughly "half" of the classes $[r] \in Z(m)/\langle |k| \rangle^\times$ are such that $\alpha_{b,b'}(\theta_{k_{u(r)},d,m}) = |k|^{u(r)}$.

We have $p^\nu \equiv -1 \pmod{\delta}$ where $\delta := d/2 = m$ divides d. Applying lemma 1.4.31, we deduce that if $r \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/4, 2d/4, 3d/4\}$ is *even*, then the restriction of $\theta_{k_{u(r)},d(m),r}$ to $k^\times_{u(r)/2}$ is trivial. In particular, for all $b, b' \in k^\times$, we get from Tate–Shafarevich theorem 1.4.8 that

$$\alpha_{b,b'}(\theta_{k_{u(r)},d,r}) = |k_{u(r)}|$$

if $r \in Z(m) \smallsetminus \{0, d/4, 2d/4, 3d/4\}$ is even (since $u(r)$ is even, $\lambda_{k_{u(r)}}$ is also trivial on $k = \mathbb{F}_p$). Thereby the analytic rank of $E_{m,b,b'}$ over $k(t)$ is *at least*

$$\rho(E_{m_\nu,b,b'}/k(t)) \geqslant \Big| Z'(m) \Big/ \langle |k| \rangle \Big|, \qquad \text{where } Z'(m) := 2\mathbb{Z}/2m\mathbb{Z} \smallsetminus \{0, m\}.$$

The argument from lemma 1.4.27 shows that

$$\begin{aligned} \rho(E_{m_\nu,b,b'}/k(t)) &\geqslant \sum_{\substack{e \mid m_\nu \\ e \nmid 2}} \frac{\phi(e)}{\mathrm{ord}^\times(p \bmod e)} \\ &\geqslant \sum_{\substack{e \mid m_\nu \\ e \nmid 2}} \frac{\phi(e)}{2\nu} = \frac{m_\nu - \phi(1) - \phi(2)}{2\nu} = \frac{p^\nu - 1}{2\nu}. \end{aligned}$$

This can be made arbitrarily large as $\nu \to +\infty$ (among even integers). ∎

Remark 3.1.21. 1. We point out that the parity condition stated in theorem 1.3.48 is *not* satisfied here when $p \geqslant 5$, so that unboundedness of rank in the Kummer family $\{E_{m,b,b'}; m \geqslant 1\}$ does not follow from this general result. Indeed, proposition 3.1.5 ensures that the conductor has even degree and the tame part at the place at infinity $\epsilon_\infty = f_\infty(E_{m,b,b'})$ is also even (when $p \geqslant 5$), so that $\deg(\mathfrak{f}')$ is *not* odd, using the notation from theorem 1.3.48.

2. We have seen in corollary 3.1.16 that Brumer's bound is asymptotically sharp if $p \equiv -1 \bmod 4$. However, if $p \equiv 1 \bmod 4$ it is not clear whether is it achieved; rather the above argument only indicates that the rank only attains *at least* "half" of Brumer's bound:

$$\frac{p^\nu}{2\nu} \cdot (1 + o(1)) \leqslant \mathrm{rk}\, E_{m_\nu,b,b'}(\mathbb{F}_p(t)) \leqslant \frac{f(E_{m_\nu,b,b'}) \log(p)}{2 \log(f(E_{m_\nu,b,b'}))} \cdot (1 + o(1)) \leqslant \frac{p^\nu}{\nu}.$$

Proving that Brumer's bound is *not* asymptotically achieved would require to show that most of the coefficients $\alpha_{b,b'}(\theta_{k_{u(r)},d,r})$ are not positive integers when $r \in Z(m)$ is *odd*.

This would yield an upper bound on the (analytic) rank. Detecting whether *some power* of $\alpha_{b,b'}(\theta_{k_{u(r)},d,r})$ is an integer can be done using Stickelberger's theorem 1.4.22. More details will be given in chapter 4, see for instance lemma 4.2.11 (about another family of curves, though). ⌟

3.1.6 Case of characteristic 3

We focus here on the case of a finite field k of characteristic 3 and assume that $m = 3^n + 1$ for some integer $n \geqslant 1$ (so $d(m) = 2m$). We look at the elliptic curve $E_{m,b,b'} : y^2 = x^3 + bx + b't^{3^n+1}$ over $k(t)$. Notice that[4] we *do not* have $3^\nu \equiv -1 \mod d(m)$ for some $\nu \geqslant 1$, i.e., the conditions of corollary 3.1.14 are not fulfilled. However, we are going to show that the L-function is of the form $(1 - |k|T)^\rho$ when $k = \mathbb{F}_{3^{2n}}$ so that the analytic rank is "as large as possible", using specifically the fact that the base field has characteristic 3. This will then give dense sphere packings as studied in the next section 3.2.

More specifically, we prove that a consequence of theorem 3.1.3 is the following corollary. We will also give an alternative and more direct proof in subsection 3.1.7.

Corollary 3.1.22 (corollary B)**.** *Let $n \geqslant 1$ be an integer and set $q = 3^n$. Let $b \in \mathbb{F}_q^\times$ be any element such that*[5] $b^{\frac{q-1}{2}} = (-1)^{n+1}$.

Then the L-function of the elliptic curve $E_{3^n+1,b,1}$ over $\mathbb{F}_{q^2}(t)$ is equal to

$$L\left(E_{3^n+1,b,1}/\mathbb{F}_{q^2}(t),\ T\right) = (1 - q^2T)^{2\cdot 3^n}.$$

In particular, the analytic and algebraic ranks of $E_{3^n+1,b,1}$ over $\mathbb{F}_{q^2}(t)$ are equal to $2 \cdot 3^n$. ⌟

Proof. — • Note that $m := 3^n + 1$ is even and $6 \nmid m$. We have $d := d(m) = 2m$ from definition 3.1.1. Let us write $k := \mathbb{F}_{q^2} = \mathbb{F}_{3^{2n}}$ and notice that -1 and b are squares in $k^\times$ (since $b \in \mathbb{F}_{3^n}^\times$). Observe that we have $3^{2n} - 1 = (3^n - 1) \cdot m \equiv 0 \mod d$ which implies that $u_{|k|,d}(r) = \mathrm{ord}^\times(|k| \bmod \frac{d}{(d,r)}) = 1$ for any $r \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$. From theorem 3.1.3, we deduce

$$L(E_{m,b,1}/k(t), T) = (1 - |k|T)^2 \cdot \prod_{[r]\in Z(m)/\langle|k|\rangle^\times} \Big(1 - \alpha_{b,1}(\theta_{k,d,r})T\Big),$$
$$\alpha_{b,1}(\theta) := \theta(-b^3) \cdot J(\lambda_{k_n}, \lambda_{k_n}\theta^2) \cdot J(\theta, \theta^2) \quad \text{if } \theta \in \widehat{k_n^\times}.$$

where $\theta_{k_{u(r)},d,r}$ was introduced in definition 1.4.15.

Fix $r \in Z(m) = \mathbb{Z}/2m\mathbb{Z} \smallsetminus \{0, m/2, m, 3m/2\}$. We claim that $\alpha_{b,1}(\theta_{k,d,r}) = |k| = q^2 = 3^{2n}$.

[4] Indeed, $2n$ is the multiplicative order of 3 modulo $m = 3^n + 1$. If $3^\nu \equiv -1 \pmod{2m}$, then $3^{2\nu} \equiv 1 \pmod m$ so that $2n$ divides 2ν. Since -1 is not a square modulo 4 and m is even, ν must be odd. Then $r := \nu/n$ is an odd integer and $3^\nu + 1 = (3^n + 1)\sum_{k=0}^{r-1}(-3^n)^k$ is the product of m by an *odd* integer, so it cannot be 0 mod $2m$.

[5] In other words, if n is odd, b is a square in $\mathbb{F}_q^\times$ (for instance $b = 1$), and if n is even, $b \in \mathbb{F}_q^\times$ is not a square.

- Observe that we cannot apply Tate–Shafarevich theorem 1.4.8 directly to compute the Jacobi sum $J(\theta_{k,d,r}, \theta_{k,d,r}^2)$ because the restriction of $\theta_{k,d,r} \in \widehat{k^\times}$ to $\mathbb{F}_q^\times$ is *not* trivial when r is odd (using the notation from definition 1.4.12):

$$\theta_{k,d,r} = \Theta|_k^{\frac{|k^\times|\cdot r}{2m}} = \Theta|_k^{\frac{r\cdot(q^2-1)}{2\cdot(q+1)}} = \Theta|_k^{r\cdot\frac{q-1}{2}}.$$

  While Θ^{q-1} is trivial on $\mathbb{F}_q^\times$, the above character is not when r is odd (its restriction to $\mathbb{F}_q^\times$ is the Legendre symbol over $\mathbb{F}_q$). But this computation shows that $\theta_{k,d,r}^2$ *is* trivial over $\mathbb{F}_q^\times$.

- Set $\theta := \theta_{k,d,r}$ for simplicity. The key point is that when $r \in Z(m)$, we have $J(\theta, \theta^2) = \frac{G(\theta)G(\theta^2)}{G(\theta^3)}$ by proposition 1.4.6 and because k has characteristic 3, we have $G(\theta) = G(\theta^3)$ by proposition 1.4.6.3, and now $G(\theta^2)$ can be determined using Tate–Shafarevich theorem 1.4.8.

  Because $r \in Z(m)$ we have $r \not\equiv 0, m/2, m, 3m/2 \bmod d$ so none of the characters $\lambda_k, \theta, \theta^2$ is trivial, and θ^3 is non-trivial since the order of θ is $\frac{d}{(r,d)}$, which divides $d = 2m$ and $6 \nmid m$. Then we find:

$$\begin{aligned}
\alpha_{b,1}(\theta_{k,d,r}) &= \theta(-b)^3 J(\lambda_k, \lambda_k\theta^2) J(\theta, \theta^2) \\
&= \theta(-b)^3 \cdot \frac{G(\lambda_k)G(\lambda_k\theta^2)}{G(\theta^2)} \cdot \frac{G(\theta)G(\theta^2)}{G(\theta^3)} && \text{proposition 1.4.6} \\
&= \theta(-b)^3 G(\lambda_k)G(\lambda_k\theta^2) && \text{proposition 1.4.6} \\
&= \theta(-b)^3 \cdot \lambda_k(z)3^n \cdot (\lambda_k\theta^2)(z)3^n && \text{theorem 1.4.8} \\
&= \theta(-b)^3 \cdot \theta^2(z)3^{2n} && (\star)
\end{aligned}$$

  where $z \in k^\times$ is any non-zero element such that $\mathrm{tr}_{k/\mathbb{F}_q}(z) = z + z^q = 0$.

- It remains to evaluate $\theta(-b)^3 \cdot \theta^2(z)$. While the value $\theta(z)$ might depend on z (such that $\mathrm{tr}_{k/\mathbb{F}_q}(z) = 0$), the value $\theta^2(z)$ does not, since we have seen above that θ^2 is trivial on $\mathbb{F}_q^\times$.
  - We claim that $\theta^2(z) = (-1)^r$. By proposition 1.4.14, let g be the generator of $k^\times$ such that $\theta(g) = \exp\left(\frac{2\pi i r}{d}\right)$. According to remark 1.4.9 we may take $z = g^{\frac{q+1}{2}}$. Then we find, recalling that $m = q + 1$:

$$\theta^2(z) = \exp\left(2 \cdot \frac{2\pi i(q+1)\cdot r}{2d}\right) = \exp\left(\frac{\pi i(q+1)\cdot r}{m}\right) = \exp(\pi i r) = (-1)^r.$$

  - In order to determine $\theta(-b)$, we let $\beta \in \mathbb{Z}$ be an integer such that $b = g^{(q+1)\beta}$. Such an integer always exists since $b \in \mathbb{F}_q^\times$ and $g^{q+1} = \mathrm{N}_{k/\mathbb{F}_q}(g)$ generates the multiplicative subgroup $\mathbb{F}_q^\times$ of $k^\times$. We have

$$\begin{aligned}
\theta(-b) &= \theta\left(g^{\frac{q^2-1}{2}} \cdot g^{(q+1)\beta}\right) \\
&= \exp\left(\frac{2\pi i r\left(\frac{q^2-1}{2} + (q+1)\beta\right)}{2m}\right) \\
&= \exp\left(\pi i r\left(\tfrac{q-1}{2} + \beta\right)\right)
\end{aligned}$$

which is always ± 1, and we have (recalling that $q = 3^n$)

$$\theta(-b) = (-1)^r \iff r \cdot \left(\tfrac{q-1}{2} + \beta - 1\right) \text{ is even} \impliedby \begin{cases} \beta \text{ is odd and } n \text{ is even, or} \\ \beta \text{ is even and } n \text{ is odd.} \end{cases}$$

- All in all, we found that $\theta(-b)^3 \cdot \theta^2(z) = 1$ if

$$\begin{cases} b \text{ is a non-square in } \mathbb{F}_{3^n}^\times \text{ and } n \text{ is even, or} \\ b \text{ is a square in } \mathbb{F}_{3^n}^\times \text{ and } n \text{ is odd.} \end{cases}$$

In both cases, we deduce from equation $(\star)$ that $\alpha_{b,1}(\theta_{k,d,r}) = 3^{2n}$ for all r, which is what we wanted. This finally implies that the L-function of $E_{3^n+1,b,1}$ over $\mathbb{F}_{3^{2n}}(t)$ is given by

$$\begin{aligned} L(E_{m,b,1}/k(t), T) &= (1 - |k|T)^2 \cdot (1 - |k|T)^{|Z(m)|} \\ &= (1 - |k|T)^{2+(2m-4)} = (1 - 3^{2n}T)^{2m-2} \end{aligned}$$

which means that the analytic rank of $E_{m,b,1}$ over $\mathbb{F}_{3^{2n}}(t)$ is equal to $2(m-1) = 2 \cdot 3^n$, if $m = 3^n + 1$ and $\lambda_{\mathbb{F}_{3^n}}(b) = (-1)^{n+1}$. The algebraic rank is equal to the analytic rank by theorem 1.3.40. This concludes the proof. ■

Remark 3.1.23. Fix any sequence $b_n \in \mathbb{F}_{3^n}^\times$ satisfying $b^{(3^n-1)/2} = (-1)^{n+1}$ for all $n \geqslant 1$. Then the family $\{ E_{3^n+1,b_n,1}/\mathbb{F}_{3^{2n}}(t) \ : \ n \geqslant 1 \}$ attains Brumer's bound from theorem 2.2.6 asymyptotically when $n \to +\infty$. Indeed, we have (using proposition 3.1.5):

$$\rho(E_{3^n+1,b_n,1}/\mathbb{F}_{3^{2n}}(t)) = 2 \cdot 3^n \leqslant \frac{f(E_{3^n+1,b_n,1}) \cdot \log(3^{2n})}{2 \cdot \log f(E_{3^n+1,b_n,1})}(1 + o(1)) \sim \frac{2 \cdot 3^n \cdot 2n \cdot \log(3)}{2\log(2 \cdot 3^n)}. \quad ⌟$$

Remark 3.1.24. We will see in proposition 3.4.3 that for *any* $m \geqslant 1$ coprime to 3 and $b \in \mathbb{F}_{3^n}^\times$, the rank of $E_{m,b,1}$ over $\mathbb{F}_{3^{2n}}(t)$ is an even integer (for every $n \geqslant 1$). ⌟

3.1.7 Alternative proof of corollary 3.1.22

In this subsection, we give an alternative proof to corollary 3.1.22. Throughout, we fix an integer $n \geqslant 1$, an odd prime p, set $q = p^n, m = p^n + 1, k = \mathbb{F}_{q^2}$ and fix $b \in \mathbb{F}_q^\times$ such that $\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(b) = (-1)^{n+1}$. When $p = 3$, the sums of Legendre symbols appearing in the L-function of $E_{m,b,1}$ over $\mathbb{F}_{q^2}(t)$ (as in remark 1.4.25 and equation (3.1.3)) can be determined thanks to an auxiliary superelliptic curve over $\mathbb{F}_q$ (see subsection 3.1.7.1), and using the fact that $x \mapsto x^p + bx$ is an additive map in characteristic p (see lemmas 3.1.27 and 3.1.28). Moreover, the number of points over $\mathbb{F}_{q^2}$ of this auxiliary superelliptic curve can be computed essentially because its jacobian is isogenous to a power of a *supersingular* elliptic curve.

The idea behind this approach was inspired by the work of N. Elkies [Elk94], where a counting argument about hyperelliptic curves has been used. In our case, this will get replaced by a *superelliptic* curve (see subsection 3.1.7.1). In both works, the elliptic curves (over function fields of characteristic 2 and 3 respectively) are isotrivial. But in our case

$E_{3^n+1,b,1}$ is a *cubic* twist of a constant curve (see proposition 3.2.9), while the elliptic curves studied in [Elk94] were *quadratic* twists of a constant curve, which allowed to use proposition 2.5.3 to compute the L-function.

This alternative approach is useful because many of the steps can be performed in arbitrary (odd) characteristic p. However, the case $p = 3$ is specifically related to elliptic curves; in general one would need to work with jacobians of hyperelliptic curves of the form $y^2 = x^p + bx + t^{p^n+1}$ (see also remark 2.4.3).

Some of the content in this subsection has been published my paper [Let22].

Remark 3.1.25. In [Elk94], the method is slightly different, because *quadratic twists* are being used. This does not seem to have an analogue in our setting: while we could consider cubic twists of the L-functions of our elliptic curve, they do *not* correspond to the L-function of cubic twists. Assume that $b = b' = 1$ and $p = 3$ for simplicity. We consider the (smooth projective models of the) curves

$$\begin{aligned} E_0 &: \ y^2 = x^3 + x && \text{over } \mathbb{F}_{q^2} \\ E_{m,1,1} &: \ y^2 = x^3 + x + t^m && \text{over } \mathbb{F}_{q^2}(t) \\ C &: \ u^3 + u = t^m && \text{over } \mathbb{F}_{q^2} \end{aligned}$$

The field extension $F := \mathbb{F}_{q^2}(C) \ / \ K := \mathbb{F}_{q^2}(t)$ has degree 3, and is Galois, with cyclic Galois group generated by the field automorphism $u \mapsto u + i$, where $i \in \mathbb{F}_{q^2}$ is a square root of -1. The elliptic curve E is a cubic twist of E_0: they are isomorphic over $\mathbb{F}_{q^2}(C)$ (see proposition 3.2.9). Under the assumptions of corollary 3.1.22, the jacobian of C is supersingular: it is in fact isogenous to a power of E_0. Therefore, by remark 2.4.1, we have

$$\operatorname{rk} E_0(F) = \operatorname{rk} \operatorname{Hom}(C, E_0) = \operatorname{rk}(\operatorname{End}(E_0)^{g(C)}) = 4 \cdot 3^n.$$

Then we wish to decompose $E_0(F)$ into eigenspaces for the Galois action, and ideally we would have

$$E_0(F) \cong E_0(K) \oplus E(K) \oplus E'(K),$$

where $K = \mathbb{F}_{q^2}(t)$ and E' is another cubic twist of E_0 over F (different from E), and finally we would hopefully prove that $\operatorname{rk} E(K) = \operatorname{rk} E'(K) = 2 \cdot 3^n$ (knowing that $E_0(K)$ has rank 0). But this is not possible: E_0 has only 2 twists over F.

Indeed, the set of isomorphism classes of elliptic curves over K which are isomorphic to E_0 over F is in one-to-one correspondence with the Galois cohomology set $H^1(\mathrm{Gal}(F/K); \mathrm{Aut}_F(E_0))$. But we have $\mathrm{Aut}_F(E_0) = \mathrm{Aut}_{\mathbb{F}_{3^2}}(E_0)$ so the Galois action is trivial, and $\mathrm{Aut}_{\mathbb{F}_{3^2}}(E_0)$ is the dicyclic group Dic_{12} of order 12. Therefore, $H^1(\mathrm{Gal}(F/K); \mathrm{Aut}_F(E_0))$ is in bijection with the 3-torsion part of Dic_{12} *up to conjugacy*, and this set has 2 elements. So the only corresponding twists are E_0 and E.

Alternatively, we can write $L(E/F, T) = \prod_\chi L(E/K, \chi, T)$ where χ runs over the complex characters of the Galois group of F/K, which is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ (see footnote 14 on page 103). But those twisted L-functions do *not* correspond to L-functions of twists of E_0: the local factors of the former may involve complex cubic roots of unity, while the latter only involve integers. ⌟

We now explain the alternative proof of corollary 3.1.22. We start by re-using equation (3.1.3), which reads

$$\log L(E_{m,b,1}/k(t)) = -\sum_{j\geqslant 1} R_b(n,j)\frac{T^j}{j} \tag{3.1.16}$$

where we define

$$R_b(n,j) := \sum_{w,x\in k_j} \lambda_{k_j}\left(x^3+bx+w^{3^n+1}\right). \tag{3.1.17}$$

Notice that we can discard the terms with $w=[1:0]$ since we have $A_{E_{m,b,1}}(\infty,j)=0$ for every $j\geqslant 1$ by proposition 3.1.5.

The strategy to evaluate those sums $R_b(n,j)$ consists of two steps:

① First, we will compute the number of points on a certain superelliptic curve $C_{n,b}$, given by $v^{3^n+1}=u^3+bu$ over k_j for every $j\geqslant 1$, where $b\in\mathbb{F}_{3^n}^\times$ is chosen as in corollary 3.1.22.

② Secondly, we study the sums

$$\sigma_b(j,t) := \sum_{x\in k_j} \lambda_{k_j}(x^3+bx+t), \tag{3.1.18}$$

where $t\in k_j$ and $j\geqslant 1$ is any integer.

3.1.7.1 Number of points on the superelliptic curve $C_{n,b}$

We fix an odd prime number p and set $k=\mathbb{F}_{p^{2n}}$. For any $n\geqslant 1$, let $C_{n,b}^{\mathrm{aff}}$ be the affine curve

$$C_{n,b}^{\mathrm{aff}}: \quad v^{p^n+1}=u^p+bu, \tag{3.1.19}$$

defined over $\mathbb{F}_{p^n}$, where $b\in\mathbb{F}_{p^n}^\times$. Note that $C_{n,b}^{\mathrm{aff}}$ is smooth.

There is a smooth projective irreducible curve $C_{n,b}$ over $\mathbb{F}_{p^n}$ (unique up to isomorphism) such that its function field is the same as the one of $C_{n,b}^{\mathrm{aff}}$ (by [GW20, theorem 15.21]): in fact $C_{n,b}$ is a superelliptic curve.

In this paragraph, we compute the zeta function of $C_{n,b}$ over $\mathbb{F}_{p^{2n}}$, which completes the step ① announced above (by specializing to $p=3$).

Proposition 3.1.26. *Let $n\geqslant 1$ be an integer and let $b\in\mathbb{F}_{p^n}^\times$ be such that $\mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(b) = b^{\frac{p^n-1}{p-1}} = (-1)^{n+1}$. Then the zeta function of the superelliptic curve $C_{n,b}$ over $k=\mathbb{F}_{p^{2n}}$ is given by*

$$Z\big(C_{n,b}/k,\ T\big) \ = \ \frac{(1+p^nT)^{(p-1)\cdot p^n}}{(1-T)(1-p^{2n}T)}.$$

In particular, for every $r\geqslant 1$, we have

$$|C_{n,b}(k_r)| = p^{2nr}+1-(p-1)\cdot p^n\cdot(-p^n)^r. \qquad \lrcorner$$

It turns out that $C_{n,b}$ has a unique point at infinity, defined over $\mathbb{F}_{p^n}$, so that $|C_{n,b}(k')| = \left|C_{n,b}^{\mathrm{aff}}(k')\right|+1$ for every finite extension k' of $\mathbb{F}_{p^n}$. Moreover, $C_{n,b}$ has genus $g(C_{n,b})=\frac{p-1}{2}\cdot p^n$ (see proposition 2 in [GPS02]).

The key point is that we will be able to deduce the number of points $|C_{n,b}(k_r)|$, for all $r\geqslant 1$, just from the computation of $|C_{n,b}(k)|$. We start with an elementary fact.

Lemma 3.1.27. *Let p be an odd prime, $n \geqslant 1$ be an integer, set $q = p^n$ and let $b \in \mathbb{F}_{p^n}^\times$ be any element such that*

$$\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(b) \;=\; b^{\frac{p^n-1}{p-1}} = (-1)^{n+1}. \tag{3.1.20}$$

Then all the roots of $X^p + bX \in \mathbb{F}_q[X]$ belong to $\mathbb{F}_{q^2}$ and we have

$$\#\{x \in \mathbb{F}_{q^2} \;:\; x^p + bx \in \mathbb{F}_q\} = p^{n+1} = p \cdot q. \qquad \lrcorner$$

Proof. — Consider the maps $f, g_b : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ defined by $f : x \mapsto x^q - x$ and $g_b : x \mapsto x^p + bx$. The key point is that these maps are endomorphisms of the additive group $(\mathbb{F}_{q^2}, +)$ seen as vector space over $\mathbb{F}_p$, and we can describe the set $\{x \in \mathbb{F}_{q^2} \;:\; x^p + bx \in \mathbb{F}_q\}$ as the kernel of $f \circ g_b$. Thereby, the proof essentially boils down to a basic argument of linear algebra. A direct computation shows that $f \circ g_b = g_b \circ f$ (using the fact that $b \in \mathbb{F}_q^\times$).

The rank-nullity theorem yields

$$\dim(\ker(g_b \circ f)) = \dim(\ker(f)) + \dim(\ker(g_b) \cap \mathrm{Im}(f)), \tag{3.1.21}$$

where the dimensions are taken over $\mathbb{F}_p$.

It is clear that $\dim(\ker(f)) = n$, since $q = p^n$, and that $\ker(g_b)$ has dimension 1 since it consists of roots in $\overline{\mathbb{F}_p}$ of the separable polynomial $X^p + bX$ which has degree p, and all those roots actually lie in $\mathbb{F}_{q^2}$. Indeed, if $x^p = -bx$ then

$$\begin{aligned} x^{p^n} \;&=\; (-b)^{1+p+\cdots+p^{n-1}} \cdot x = (-b)^{\frac{p^n-1}{p-1}} \cdot x \overset{(3.1.20)}{=} (-1)^{\frac{p^n-1}{p-1}} \cdot (-1)^{n+1} x \\ &\overset{p \text{ odd}}{=} (-1)^n \cdot (-1)^{n+1} x \;=\; -x, \end{aligned} \tag{3.1.22}$$

which implies that $x^{q^2} = (x^q)^q = (-x)^q = x$, i.e., $x \in \mathbb{F}_{q^2}$ as claimed.

The above computation (3.1.22) also shows that any element $x \in \ker(g_b)$ satisfies $x^{p^n} = -x$, so that $f(x) = -2x$, which shows that $x \in \mathrm{Im}(f)$ (recall that p is odd, so $-2 \in \mathbb{F}_p^\times$ is invertible). In other words, we have $\ker(g_b) \cap \mathrm{Im}(f) = \ker(g_b)$. Finally we get $\dim(\ker(f \circ g_b)) = \dim(\ker(g_b \circ f)) = n + 1$ from equation (3.1.21), which yields

$$\#\{x \in \mathbb{F}_{q^2} \;:\; x^p + bx \in \mathbb{F}_q\} = |\ker(f \circ g_b)| = p^{n+1},$$

which is what we wanted to prove. ■

Proof of proposition 3.1.26. — We first compute $|C_{n,b}(k)|$. The norm map

$$k^\times \longrightarrow \mathbb{F}_{p^n}^\times, \qquad v \longmapsto v^{p^n} \cdot v = v^{p^n+1} =: w$$

is a surjective morphism, with kernel of size $\dfrac{p^{2n}-1}{p^n-1} = p^n + 1$. Furthermore, by lemma 3.1.27, $X^p + bX$ has p roots over k. Therefore, we get

$$\begin{aligned} |C_{n,b}(k)| &= 1 + p + (p^n+1) \sum_{w \in \mathbb{F}_{p^n}^\times} \#\{u \in k \;:\; u^p + bu = w\} \\ &= 1 + p + (p^n+1)\,(\#\{u \in k \;:\; u^p + bu \in \mathbb{F}_{p^n}\} - p) \\ &= 1 + p^n \cdot p^{n+1} \end{aligned} \tag{3.1.23}$$

where the last line follows from lemma 3.1.27.

We now consider $C_{n,b}$ as a curve over $k = \mathbb{F}_{p^{2n}}$ (instead of a curve over $\mathbb{F}_{p^n}$). Let us write $\{\,\omega_j \;:\; 1 \leqslant j \leqslant 2g(C_{n,b})\,\}$ for the reciprocal of the roots of the numerator (in $\mathbb{Z}[T]$) of zeta function $Z(C_{n,b}/k, T)$; in particular, they can be seen as complex numbers and their modulus is known to be equal to $|\omega_j| = \sqrt{|k|} = p^n$. Thereby, Lefschetz trace formula tells us that

$$\begin{aligned}|C_{n,b}(k)| &= |k| + 1 - \sum_{j=1}^{2g(C_{n,b})} \omega_j \\ &= 1 + p^{2n+1} = p \cdot p^{2n} + 1 = p^{2n} + 1 - \sum_{j=1}^{(p-1)\cdot p^n} \omega_j,\end{aligned}$$

which implies $-(p-1)\cdot p^{2n} = \sum_{j=1}^{(p-1)\cdot p^n} \omega_j$. Because the $\omega_j \in \mathbb{C}$ satisfy $|\omega_j| = p^n$, this forces $\omega_j = -p^n$ for every j (e.g., by taking the real part of the latter sum). We conclude that for every $n \geqslant 1$ and every $r \geqslant 1$:

$$|C_{n,b}(k_r)| = |k|^r + 1 - (p-1)p^n \cdot (-p^n)^r. \qquad \blacksquare$$

3.1.7.2 Evaluating the sums $\sigma_b(j,t)$

This paragraph is devoted to the explicit computation of (a generalization of) the sums $\sigma_b(j,t)$ defined in equation (3.1.18), as required by step ② above. Namely, for an odd prime number p, an integer $n \geqslant 1$ and $b \in \mathbb{F}_{p^n}^\times$, we define

$$\sigma_b(j,t) := \sum_{x \in k_j} \lambda_{k_j}(x^p + bx + t)$$

where $k := \mathbb{F}_{p^{2n}}$, $j \geqslant 1$ and $t \in k_j$ (when $p = 3$, we recover the sums from equation (3.1.18)).

Lemma 3.1.28. *Let $n \geqslant 1$ be an integer and fix $b \in \mathbb{F}_{p^n}$ such that $\mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(b) = (-1)^{n+1}$. Let $j \geqslant 1$ be any integer. Consider the map $g_{b,j} : k_j \to k_j$ defined by $g_{b,j} : x \mapsto x^p + bx$.*

Then for every $t \in k_j$ we have :

$$\sigma_b(j,t) = \begin{cases} -(p-1)\cdot(-p^n)^j & \text{if } t \in \mathrm{Im}(g_{b,j}) \\ (-p^n)^j & \text{otherwise.} \end{cases} \qquad \lrcorner$$

Proof. — Step 1 – The first key point here is to use again the fact that the map $g_{b,j}$ is additive, in order to deduce that $\sigma_b(j,t)$ takes only two values (for fixed j, b and variable t).

Indeed, if we pick any $x_0 \in k_j$, then

$$\begin{aligned}\sigma_b(j,t) &= \sum_{x \in k_j} \lambda_{k_j}(g_{b,j}(x) + t) = \sum_{x' \in k_j} \lambda_{k_j}(g_{b,j}(x' + x_0) + t) \\ &= \sum_{x' \in k_j} \lambda_{k_j}\left(g_{b,j}(x') \;+\; g_{b,j}(x_0) + t\right) = \sigma_b(j, t + g_{b,j}(x_0)).\end{aligned}$$

In other words, $\sigma_b(j,t)$ only depends on the class of t in the quotient additive group $k_j/\operatorname{Im}(g_{b,j})$. Moreover, notice that for any $\alpha \in \mathbb{F}_p^\times$ one has

$$\begin{aligned}\sigma_b(j,t) &= \sum_{x' \in k_j} \lambda_{k_j}\big(g_{b,j}(\alpha x') + t\big) = \sum_{x' \in k_j} \lambda_{k_j}\big(\alpha g_{b,j}(x') + t\big) \\ &= \lambda_{k_j}(\alpha) \cdot \sigma_b(j, \alpha^{-1}t) = \sigma_b(j, \alpha^{-1}t),\end{aligned}$$

where the last equality holds because α is a square in $\mathbb{F}_{p^2}$ and hence in $k = \mathbb{F}_{p^{2n}}$.

Since $[k_j : \operatorname{Im}(g_{b,j})] = |\ker(g_{b,j})| = p$ by lemma 3.1.27 (which can be applied since we assumed $\mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(b) = (-1)^{n+1}$), we deduce that $\sigma_b(j,t)$ only takes (at most) two values, for fixed j, b and variable t. The first value occurs when $t \in \operatorname{Im}(g_{b,j})$ in which case $\sigma_b(j,t) = \sigma_b(j,0)$. Let us denote by σ^* the other value of $\sigma_b(j,t)$, which occurs when $t \notin \operatorname{Im}(g_{b,j})$. Observe that the value of σ^* can be deduced from the sum

$$\sum_{t \in k_j} \sigma_b(j,t) = |\operatorname{Im}(g_{b,j})| \cdot \sigma_b(j,0) \; + \; \big(p^{2nj} - |\operatorname{Im}(g_{b,j})|\big) \cdot \sigma^* = p^{2nj}\left(\frac{1}{p}\sigma_b(j,0) \; + \; \frac{p-1}{p}\sigma^*\right)$$

because the left-hand side sum vanishes :

$$\sum_{t \in k_j} \sigma_b(j,t) \; = \sum_{x \in k_j} \sum_{t \in k_j} \lambda_{k_j}(x^p + bx + t) = 0,$$

since all the inner sums are 0 (they are sums of a non-trivial multiplicative character over the whole group – recall also that $\lambda_{k_j}(0) = 0$). Therefore $\sigma^* = -\frac{1}{p-1}\sigma_b(j,0)$, so it is enough to determine the value of $\sigma_b(j,0)$.

Step 2 – Now we compute the sum $\sigma_b(j,0) = \sum_{x \in k_j} \lambda_{k_j}(x^p + bx)$.

The most conceptual (and easiest, or shortest) proof relies on the fact that if $\pi : Y \to X$ is a surjective morphism between two smooth irreducible projective algebraic curves (or even varieties) defined over a finite field, then the numerator of the zeta function of X divides the one of Y in $\mathbb{Z}[T]$. This can be argued using the Tate modules of the jacobians of these curves, see for instance proposition 5 in [AP04].

In our case, we have the morphism

$$\pi : C_{n,b} \to H_b \qquad (u,v) \mapsto \left(u, v^{\frac{p^n+1}{2}}\right)$$

where H_b is the hyperelliptic curve given by $y^2 = x^p + bx$ over $\mathbb{F}_{p^n}$ (we defined the morphism on affine open subsets, but it extends uniquely to a morphism between the smooth projective curves $C_{n,b} \to H_b$ by [GW20, proposition 15.5]). Being a non-constant morphism between irreducible curves, π must be surjective.

The numerator of $Z(C_{n,b}/\mathbb{F}_{p^{2n}}, T)$ is $(1 + p^n T)^{(p-1)\cdot p^n}$ by proposition 3.1.26. Therefore, the numerator of $Z(H_b/\mathbb{F}_{p^{2n}}, T)$ is $(1 + p^n T)^{p-1}$ since H_b has genus $\frac{p-1}{2}$. Notice that H_b has a unique point at infinity. Thus we deduce from standard arguments that

$$1 + p^{2nj} + \sigma_b(j,0) \; = \; |H_b(k_j)| \; = \; 1 + p^{2nj} - (p-1)(-p^n)^j, \tag{3.1.24}$$

which gives the claimed value for $\sigma_b(j,0)$. Therefore, from step 1 we get the value $\sigma^* = (-p^n)^j$ and this finishes the proof. ∎

Remark 3.1.29. When $p = 3$, it is possible to give more concrete and elementary (but computationally longer) proofs of the identity $\sigma_b(j, 0) = -2 \cdot (-3^n)^j$ from lemma 3.1.28, via quartic Jacobi sums.

— A second proof of lemma 3.1.28 when $p = 3$ is based on [IR90, exercise 11, p. 170]. Let $\mathcal{D}_b$ be the affine quadric $u^2 - v^4 = -4b \equiv -b$ over $\mathbb{F}_{3^n}$. Let $\mathcal{E}_b$ be the elliptic curve given by (the projective closure of) the affine equation $y^2 = x^3 + bx$ over $\mathbb{F}_{3^n}$, where $\mathrm{N}_{\mathbb{F}_{3^n}/\mathbb{F}_3}(b) = \lambda_{\mathbb{F}_{3^n}}(b) = (-1)^{n+1}$.

The key here is to use the morphism of affine curves

$$\begin{array}{rccc} \phi : & \mathcal{D}_b & \longrightarrow & \mathcal{E}_b \smallsetminus \{[0:1:0]\} \\ & (u, v) & \longmapsto & \left(x = \frac{1}{2}(u + v^2)\ ;\ y = vx = \frac{1}{2}v(u + v^2)\right) \end{array}$$

and that the number of points of $\mathcal{D}_b$ can be computed via quartic Jacobi sums. The map ϕ is well-defined since $y^2 = v^2x^2 = x(x^2 + b) = x^3 + bx \iff xv^2 = x^2 + b \iff \frac{1}{2}(u + v^2)v^2 = \frac{1}{4}(u^2 + 2uv^2 + v^4) + b \iff 2uv^2 + 2v^4 = u^2 + 2uv^2 + v^4 + 4b \iff v^4 = u^2 + 4b$. Moreover, ϕ is an isomorphism onto its image $\mathcal{E}_b \setminus \{[0:1:0], [0:0:1]\}$, the inverse being $(x, y) \longmapsto (2x - (y/x)^2\ ,\ y/x)$ (where $x \neq 0$).

Let $\alpha \geqslant 1$ be any integer and set $Q = 3^{n\alpha}$. Now, by proposition 1.4.3 one has

$$|\mathcal{D}_b(\mathbb{F}_Q)| = \sum_{v \in \mathbb{F}_Q} (1 + \lambda_{\mathbb{F}_Q}(v^4 - 4b)) = Q + \sum_{w \in \mathbb{F}_Q} \sum_{\chi^4 = \mathbb{1}} \chi(w)\lambda(w - 4b),$$

where $\chi : \mathbb{F}_Q^\times \to \mathbb{C}^\times$ runs over multiplicative characters of order dividing 4. Moreover,

$$\begin{aligned} \sum_{w \in \mathbb{F}_Q} \chi(w)\lambda(w - 4b) &= \sum_{w' \in \mathbb{F}_Q} \chi(-4bw')\lambda(-4bw' - 4b) \\ &= \chi(4b)\lambda_{\mathbb{F}_Q}(-4b) \sum_{w' \in \mathbb{F}_Q} \chi(-w')\lambda(w' + 1) \\ &= \chi(4b)\lambda_{\mathbb{F}_Q}(-4b) \cdot J(\chi, \lambda). \end{aligned}$$

In short, we get

$$|\mathcal{D}_b(\mathbb{F}_Q)| = Q + \lambda_{\mathbb{F}_Q}(-4b) \sum_{\chi^4 = \mathbb{1}} \chi(4b) \cdot J(\chi, \lambda). \tag{3.1.25}$$

– If $n \cdot \alpha$ is odd, then there are only 2 characters $\mathbb{F}_Q^\times \to \mathbb{C}^\times$ of order dividing 4, namely the trivial one and the Legendre symbol, because $\gcd(|\mathbb{F}_Q^\times|, 4) = \gcd(3^{n\alpha} - 1, 4) = 2$. The above identity (3.1.25) then yields

$$|\mathcal{D}_b(\mathbb{F}_Q)| = Q + \lambda_{\mathbb{F}_Q}(-4b)\lambda_{\mathbb{F}_Q}(4b) \cdot J(\lambda_{\mathbb{F}_Q}, \lambda_{\mathbb{F}_Q}) = Q - 1,$$

where we used the fact $J(\mathbb{1}, \lambda) = 0$ and $J(\lambda, \lambda) = -\lambda(-1)$. (We see that the identity $|\mathcal{D}_b(\mathbb{F}_Q)| = Q - 1$ actually holds for any $Q = p^{n\alpha}$ and any $b \in \mathbb{F}_Q^\times$ such that $n \cdot \alpha$ is odd and $p \equiv -1 \pmod 4$).

– If $n \cdot \alpha$ is even, then there exists a character $\chi_4 : \mathbb{F}_Q^\times \to \mathbb{C}^\times$ of order exactly 4 (since 4 divides $|\mathbb{F}_Q^\times| = 3^{n\cdot\alpha} - 1$, as $n\alpha$ is even). In particular, $\chi_4^2 = \lambda_{\mathbb{F}_Q}$.

From equation (3.1.25) we get (recall that $J(\mathbb{1}, \lambda) = 0$, so in the sum below, the term for $k = 0$ vanishes):

$$|\mathcal{D}_b(\mathbb{F}_Q)| = Q + \lambda_{\mathbb{F}_Q}(-4b) \sum_{k=1}^{3} \chi_4^k(4b) \cdot J(\chi_4^k, \lambda)$$

$$= Q + \lambda_{\mathbb{F}_Q}(-4b)\Big(\lambda(4b) \cdot \underbrace{J(\lambda,\lambda)}_{=-\lambda(-1)} + 2\,\mathrm{Re}(\chi_4(4b) \cdot J(\chi_4,\lambda))\Big)$$
$$= Q - 1 + 2\lambda_{\mathbb{F}_Q}(-4b)\,\mathrm{Re}(\chi_4(4b) \cdot J(\chi_4,\lambda)) \tag{3.1.26}$$

When $\alpha \cdot n = n$ is even, then $\chi_4(b)^2 = \lambda_{\mathbb{F}_{3^n}}(b) = -1$ by assumption, so $\chi_4(4b) = \lambda_{\mathbb{F}_{3^n}}(2)\chi_4(b)$ is purely imaginary. On the other hand, $J(\chi_4,\lambda)$ is a real number. Indeed, we have $J(\chi_4, \lambda_{\mathbb{F}_{3^n}}) = \dfrac{G(\chi_4)\cdot G(\lambda)}{G(\chi_4\lambda)}$ by proposition 1.4.6. Since χ_4 and $\chi_4\lambda = \chi_4^{-1}$ have both order 4, and since $p := 3 \equiv -1 \pmod 4$, theorem 11.6.3 in [BEW98] yields

$$G(\chi_4) = G(\chi_4\lambda) = p^{n/2} \cdot (-1)^{\frac{n}{2}-1+\frac{(p+1)n}{8}}.$$

Moreover, it is well-known (see [BEW98, theorem 11.5.4]) that $G(\lambda_{\mathbb{F}_Q}) = (-1)^{n-1}Q^{1/2}i^n = -(-3)^{n/2}$ since $p \equiv 3 \pmod 4$ and n is even (here $i \in \mathbb{C}$ denotes a square root of -1).

All in all, when $\alpha \cdot n = n$ is even, equation (3.1.26) finally implies that

$$|\mathcal{D}_b(\mathbb{F}_{3^n})| = 3^n - 1 + 2\lambda_{\mathbb{F}_{3^n}}(-4b) \cdot 0 = 3^n - 1.$$

Finally, $|\mathcal{E}_b(\mathbb{F}_Q)| = |\mathcal{D}_b(\mathbb{F}_Q)| + 2$ yields $|\mathcal{E}_b(\mathbb{F}_{3^n})| = 3^n - 1 + 2 \cdot 0 + 2 = 3^n + 1$ for every n (even or odd). By Hasse–Weil theorem we can write the number of points as $|\mathcal{E}_b(\mathbb{F}_{3^n})| = 3^n + 1 - (t_1 + t_2)$ with $t_1 t_2 = 3^n$ so $t_1 = -t_2 = 3^{n/2}i \in \mathbb{C}$ and therefore

$$|\mathcal{E}_b(\mathbb{F}_{3^{2nj}})| = 1 + 3^{2nj} - 3^n(i^{2j} + (-i)^{2j}) = 1 + 3^{2nj} - 2(-3^n)^j,$$

as we had in equation (3.1.24).

— The third and last proof of lemma 3.1.28, when $p = 3$ and n is even (and $\lambda_{\mathbb{F}_{3^n}}(b) = -1$), is similar to the previous one, but is more enlightening about the appearance of the quartic curve $\mathcal{D}_b$ (or rather the character χ_4 of order 4), which seemed to be just a clever trick.

The idea to compute $T(b) := \sigma_b(1,0) = \sum_{x\in\mathbb{F}_{3^{2n}}} \lambda_{\mathbb{F}_{3^{2n}}}(x^3 + bx)$ is to let $b \in \mathbb{F}_{3^n}^\times$ vary (and then we will be able to deduce $\sigma_b(j,0)$ for all $j \geqslant 1$). We observe that for any $u \in \mathbb{F}_{3^n}^\times$, one has

$$T(b) = \sigma_b(1,0) = \sum_{x'\in\mathbb{F}_{3^{2n}}} \lambda((ux')^3 + bux')$$
$$= \lambda(u^3)\sigma_{u^{-2}b}(1,0) = \lambda(u)T(u^{-2}b)$$

In particular, we have $T(b) = T(v^4 b)$ for every $v \in \mathbb{F}_{3^n}^\times$, that is: $T(b)$ only depends on the class of b in $\mathbb{F}_{3^n}^\times/\mathbb{F}_{3^n}^{\times,4}$, i.e. modulo the 4-th powers. If n is even, then this group has size 4 (equal to the kernel of the endomorphism $x \mapsto x^4$ of $\mathbb{F}_{3^n}^\times$).

We show that for every prime $p \equiv 3 \pmod 4$, every even integer $n \geqslant 2$ and every $b \in \mathbb{F}_{p^n}^\times$ such that $\lambda_{\mathbb{F}_{p^n}}(b) = -1$, we have

$$S(b) := \sum_{x\in\mathbb{F}_{p^n}} \lambda_{\mathbb{F}_{p^n}}(x^3 + bx) = 0. \tag{3.1.27}$$

This is *not* the same as $T(b)$ because we are summing over $\mathbb{F}_{3^n}$ and not over $\mathbb{F}_{3^{2n}}$, but it will be sufficient, by Hasse–Weil theorem, to deduce[6] $T(b)$. Similarly to $T(b)$, we see that $S(b) = S(u^4 b)$ for every $u \in \mathbb{F}_{p^n}^\times$. Then

$$\begin{aligned}
(p^n-1)S(b) &\underset{\boxed{S(0)=0}}{=\!\!\uparrow} \sum_{u\in\mathbb{F}_{p^n}} S(bu^4) \\
&\underset{\boxed{\lambda(0)=0}}{=\!\!\uparrow} \sum_{x\in\mathbb{F}_{p^n}^\times}\sum_{u\in\mathbb{F}_{p^n}} \lambda(x^3)\lambda(1+bx^{-2}u^4) \\
&= \sum_{x\in\mathbb{F}_{p^n}^\times}\sum_{z\in\mathbb{F}_{p^n}}\sum_{\chi^4=\mathbb{1}} \lambda(x^3)\lambda(1+bx^{-2}z)\chi(z) \\
&= \sum_{x\in\mathbb{F}_{p^n}^\times} \lambda(x)\sum_{\chi^4=\mathbb{1}} \chi(-b^{-1}x^2)\sum_{z\in\mathbb{F}_{p^n}} \chi(-bx^{-2}z)\lambda(1+bx^{-2}z) \\
&= \sum_{x\in\mathbb{F}_{p^n}^\times} \lambda(x)\sum_{\chi^4=\mathbb{1}} \chi(-b^{-1}x^2) J(\chi,\lambda) \\
&\underset{\boxed{n \text{ even} \implies \chi_4 \text{ exists}}}{=\!\!\uparrow} \sum_{k=0}^{3} J(\chi_4^k,\lambda)\chi_4^k(-b^{-1}) \sum_{x\in\mathbb{F}_{p^n}^\times} \lambda^{1+k}(x)
\end{aligned}$$

Now notice that

$$\sum_{x\in\mathbb{F}_{p^n}^\times} \lambda^{1+k}(x) = \begin{cases} 0 & \text{if } k\in\{0,2\} \\ p^n-1 & \text{if } k\in\{1,3\} \end{cases}$$

This yields

$$\begin{aligned}
S(b) &= \sum_{k\in\{1,3\}} J(\chi_4^k,\lambda)\chi_4^k(-b^{-1}) \\
&= 2\,\mathrm{Re}\left(J(\chi_4,\lambda)\chi_4(-b^{-1})\right) = 2\,\mathrm{Re}\left(J(\chi_4,\lambda)\overline{\chi_4}(-b)\right),
\end{aligned}$$

which reminds us of equation (3.1.26). We conclude as before that $S(b) = 0$ since $-b$ is not a square in $\mathbb{F}_{p^n}$ by assumption (so that $\chi_4(-b)$ is purely imaginary), while the Jacobi sum $J(\chi_4,\lambda)$ is a real number. This terminates the proof. ⌟

3.1.7.3 Conclusion of the proof

We are now in position to give a new proof of corollary 3.1.22.

Second proof of corollary 3.1.22. — Recall from equations (3.1.16) to (3.1.18) that we have

$$\log L(E_{m,b,1}/k(t)) = -\sum_{j\geqslant 1} R_b(n,j)\frac{T^j}{j}, \qquad R_b(n,j) = \sum_{w\in k_j} \sigma_b(j, w^{3^n+1}). \tag{3.1.28}$$

[6] Indeed, if $S(b) = 0$ then the elliptic curve $A : y^2 = x^3 + bx$ satisfies $|A(\mathbb{F}_{p^n})| = p^n + 1 - (\alpha+\beta)$ where $\alpha+\beta = 0, \alpha\beta = p^n$ so that $\alpha = -\beta = ip^{n/2}$ and then $T(b) = |A(\mathbb{F}_{p^{2n}})| - (p^{2n}+1) = -(\alpha^2+\beta^2) = 2\cdot 3^n$.

For general odd prime p, assume that $b \in \mathbb{F}_{p^n}^\times$ satisfies $\mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(b) = (-1)^{n+1}$, define the set

$$\Gamma_b(n,j) := \left\{ w \in k_j \ : \ w^{p^n+1} \in \mathrm{Im}(g_{b,j}) \right\},$$

where $g_{b,j} : k_j \to k_j$ denotes the map $x \mapsto x^p + bx$ as in lemma 3.1.28. Recall that we introduced the affine curve $C_{n,b}^{\mathrm{aff}} : v^{p^n+1} = u^p + bu$ in equation (3.1.19). Observe that all the fibers of the map

$$C_{n,b}^{\mathrm{aff}}(k_j) \longrightarrow \Gamma_b(n,j), \qquad (u,v) \longmapsto v$$

have size p since $\ker(g_{b,j})$ is 1-dimensional over $\mathbb{F}_p$ by lemma 3.1.27; it can be applied thanks to our assumption on b. Thereby, we deduce from proposition 3.1.26 that

$$|\Gamma_b(n,j)| = \frac{1}{p}(|C_{n,b}(k_j)| - 1) = \frac{1}{p}(p^{2nj} - (p-1)\cdot p^n \cdot (-p^n)^j). \tag{3.1.29}$$

Therefore, using lemma 3.1.28 and the above expression (3.1.28) of $R_b(n,j)$, we get

$$\begin{aligned} R_b(n,j) &= -(p-1)\cdot(-p^n)^j \cdot |\Gamma_b(n,j)| \quad + \quad (-p^n)^j \cdot \left(p^{2nj} - |\Gamma_b(n,j)|\right) \\ &= (-p^n)^j \cdot \left(p^{2nj} - p \cdot |\Gamma_b(n,j)|\right) \\ &\overset{(3.1.29)}{=} (-p^n)^j \cdot (p-1)\cdot p^n \cdot (-p^n)^j \\ &= (p-1)\cdot p^{n(1+2j)} = (p-1)q^{1+2j}, \end{aligned}$$

Finally, we conclude that

$$-\sum_{j \geqslant 1} R_b(n,j)\frac{T^n}{n} = -(p-1)q\sum_{j\geqslant 1}\frac{(q^2T)^j}{j} = (p-1)p^n \cdot \log(1-q^2T). \tag{3.1.30}$$

We now specialize to the case where $p = 3$ so that $q = 3^n$ and $k = \mathbb{F}_{3^{2n}}$. Notice that the hypothesis in corollary 3.1.22 reads[7] $b^{\frac{p^n-1}{2}} = \mathrm{N}_{\mathbb{F}_{3^n}/\mathbb{F}_3}(b) = (-1)^{n+1}$, in which case (3.1.28) becomes $L\left(E_{m,b,1}/\mathbb{F}_{q^2}(t),\ T\right) = (1-q^2T)^{(p-1)\cdot p^n} = (1-q^2T)^{2\cdot 3^n}$, as desired. This finishes the proof[8]. ■

3.2 · Sphere packings from $E_{m,b,b'}$

We are looking for some examples of elliptic curves satisfying the asymptotic conditions of theorem 2.3.1 and it turns out that $E_{m,b,b'}/\mathbb{F}_{p^{2e}}(t)$ verifies[9] them if $m = (p^e+1)/2, p \equiv -1 \bmod 4$ and $e > 0$ is odd. Indeed, as mentioned in proposition 3.1.5, the Szpiro ratio of $E_{m,b,b'}$ tends to 1 when $m \to +\infty$. Moreover, corollary 3.1.16 asserts that Brumer's bound is asymptotically attained (but *probably* not if $p \equiv 1 \bmod 4$, see remark 3.1.21).

[7] The norm map $\mathrm{N} : \mathbb{F}_{3^n}^\times \to \mathbb{F}_3^\times \cong \{\pm 1\}$ is surjective, so it gives a non-trivial character of order two: the Legendre symbol.

[8] We see that one should expect the rank of the jacobian of $y^2 = x^p + bx + t^{p^n+1}$ over $\mathbb{F}_{p^{2n}}(t)$ to be $(p-1)\cdot p^n$ if $\mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(b) = (-1)^{n+1}$ (however a complete proof would require the analysis of the reduction type at $v = \infty$). See also remark 2.4.3.

[9] The cardinality of the field of constants satisfies $q_j := p^{2e} \sim (2m)^2 \sim f(E_{m,b,b'})^2$, so we may take $c_0 := 2$ in the statement of theorem 2.3.1.

3.2.1 Case $m = \frac{p^e+1}{2}$

When $m := \frac{p^e+1}{2}$, we compute the lower bound on the center density of the narrow Mordell–Weil lattice $L_{m,b,b',q}$ of $E_{m,b,b'}$ over $\mathbb{F}_{p^{2e}}(t)$.

Theorem 3.2.1. *Let p be a prime number such that $p \equiv -1 \pmod 4$ and let $e > 0$ be an odd integer. Fix $b, b' \in \mathbb{F}_{p^e}^\times$ and set $m = \dfrac{p^e+1}{2}$ as well as $k := \mathbb{F}_{p^{2e}}$. Then:*

- *The rank of the lattice $L_{m,b,b',p^{2e}} = E_{m,b,b'}(k(t))^0$ is given by*

$$r = \begin{cases} p^e - 1 & \text{if } p \equiv 1 \pmod 3, \text{ or } p = 3 \\ p^e - 3 & \text{if } p \equiv -1 \pmod 3 \end{cases}$$

- *The center sphere packing density of $L_{m,b,b',p^{2e}}$ (introduced in definition 1.2.6) satisfies*

$$\delta(L_{m,b,b',p^{2e}}) \geqslant \frac{(D/24)^{r/2}}{c^{1/2} \cdot p^{e\cdot(D/12-1)}}$$

where

$$D := 12\left\lceil \frac{p^e+1}{12} \right\rceil = \begin{cases} p^e+1 & \text{if } p \equiv 11 \pmod{12}, \\ p^e+5 & \text{if } p \equiv 7 \pmod{12}, \\ p^e+9 & \text{if } p \equiv 3 \pmod{12} \end{cases} \qquad c := \begin{cases} 1 & \text{if } p \equiv -1 \pmod{12}, \\ 3 & \text{otherwise} \end{cases}$$

Following the strategy sketched in remark 2.1.2, we first study the torsion subgroup of $E_{m,b,b'}(k(t))$.

Lemma 3.2.2. *Let p be an odd prime, $b, b' \in \overline{\mathbb{F}_p}^\times$ and $m \geqslant 1$ be an even integer coprime to p. Then the abelian group $E_{m,b,b'}(\overline{\mathbb{F}_p}(t))$ is torsion-free.*

Proof. — From proposition 3.1.5, we know that $c(E_{m,b,b'}/k(t)) \in \{1, 3\}$ for any finite field $k \supset \mathbb{F}_p(b, b')$; in particular this global Tamagawa number is square-free. Thanks to proposition 2.1.3, we deduce that $E_{m,b,b'}(k(t))$ is torsion-free for all such k. Then $E_{m,b,b'}(\overline{\mathbb{F}_p}(t))$ is torsion-free as well. ■

Proof of theorem 3.2.1. — The result on the rank readily follows from corollary 3.1.16. The lower bound on the center density comes from proposition 2.1.1. Indeed, corollary 3.1.16 ensures that the special value of the L-function is $L^*(E_{m,b,b'}/k(t)) = 1$. Moreover, we have just seen that $E_{m,b,b'}(k(t))_{\text{tors}}$ is trivial. Finally $D = \deg\left(\Delta_{\min}(E_{m,b,b'}/k(t))\right)$ and $c = c(E_{m,b,b'}/k(t))$ have been determined in proposition 3.1.5. A direct computation then yields the claimed inequality (notice that $b' \in \mathbb{F}_{p^e}^\times$ is always a square in $k = \mathbb{F}_{p^{2e}}$). ■

Example 3.2.3. The following table shows some dimensions for which the lattice above has "interesting" center density. For simplicity we let $L(p, e) := L_{(p^e+1)/2,\,1,\,1,p^{2e}}$ when $p \equiv -1 \bmod 4$ and $e > 0$ is odd. The last two columns compare our bound for $r = 150$ and $r = 306$ to the previously known results of Keith Ball [Bal92] (theorem 1.2.16 which improves on Minkowski–Hlawka lower bound from theorem 1.2.15) and the improvements of Craig's lattices from [FIdD11] discussed in remark 1.2.21. Our values therefore seem to be the best known lattice sphere packing densities in these two dimensions.

rank r	p	$\log_2 \delta(L(p,1)) \geqslant$	[Bal92] $\delta_\ell(n) \geqslant$	[FIdD11] $\delta_\ell(n) \geqslant$
2	3	$\log_2(\delta(A_2))$		
6	7	$\log_2(\delta(E_6))$		
8	11	$\log_2(\delta(E_8))$		
150	151	114.8796	97.758	114.6448
306	307	358.8224	345.18	357.5522

Here are a few other values:

rank r	p	$\log_2 \delta(L(p,1)) \geqslant$	rank r	p	$\log_2 \delta(L(p,1)) \geqslant$
66	67	21.1808	162	163	131.0698
68	71	23.1399	164	167	134.2149
78	79	31.8717	176	179	151.033
80	83	34.044	188	191	168.3386
102	103	56.3817	198	199	182.6803
104	107	58.9044	248	251	261.2165
126	127	84.2649	356	359	449.2792
128	131	87.0694	416	419	562.7234
138	139	99.2616	464	467	657.25672

Moreover, $L(3,5)$ has rank 242, $\log_2 \delta(L(3,5)) \geqslant 251.1816$ and $L(7,3)$ has rank 342 and $\log_2 \delta(L(7,3)) \geqslant 423.1044$.

- Applying Mordell's inequality from proposition 1.2.17 (with $n = 72 > m = 66$) to the even unimodular 72-dimensional lattice with minimal norm $8^{1/2}$ found by G. Nebe in [Neb12] gives $\log_2 \delta_\ell(66) \geqslant 24.6338 > \log_2 \delta(L(67,1))$. So our 66-dimensional lattice $L(67,1)$ is not the densest possible; however Mordell's inequality does not provide *explicitly* a lattice achieving the bound 24.6338.

  We observe that $L(67,1)$ is denser than the narrow Mordell–Weil lattice obtained from [Shi91, theorem 1.2] with $m = 34, p = 101$ (which has $\log_2(\delta) \simeq 18.220$), and is also denser than Craig's lattice $A_{66}^{(8)}$ (which has $\log_2(\delta) \simeq 20.504$; see [CS98, Chapter 8, §6, §7.3c)] and remark 1.2.21). But the improvement of Craig's lattice given in [FIdD11] satisfies $\log_2(\delta) \simeq 21.504$, which is slightly better than what we found.

- In fact, most of the packing densities in the second table are superseded by applying Mordell's inequality to some Mordell–Weil lattices from [Shi91, theorem 1.2] or to some improvement of Craig's lattices from [FIdD11]. However, all the packing densities in the second table are greater than the values obtained from Ball's lower bound (theorem 1.2.16) in their respective dimensions. ⌟

Remark 3.2.4. We point out that one can use Mordell's inequality (proposition 1.2.17) to improve some of the packing densities obtained in [Shi91, example 1.3] and remark 4.1.11 stated later, which are the best known so far in their respective dimensions.

- Using $p = 257, m = p+1$ in [Shi91, proposition 1.2] yields a 512-dimensional lattice with $\log_2(\delta) = 796.8875$, and then Mordell's inequality gives $\log_2 \delta_\ell(508) \geqslant 780.4962$, much better than the density of the 508-dimensional lattice L obtained using $p = 509, m = (p+1)/2$ which satisfies $\log_2(\delta(L)) \simeq 745.6273$.

- In fact, [Elk94] exhibits a 512-dimensional lattice with $\log_2(\delta) \geqslant 797.1237$, which implies $\log_2 \delta_\ell(508) \geqslant 780.7287$.
- Similarly, using $p = 263, m = p + 1$ in [Shi91, proposition 1.2] yields a 524-dimensional lattice with $\log_2(\delta) = 822.6975$, and then Mordell's inequality gives $\log_2 \delta_\ell(520) \geqslant 806.1962$, improving by far the density of the 520-dimensional lattice L obtained using $p = 521, m = (p+1)/2$ which satisfies $\log_2(\delta(L)) \simeq 770.3712$. ⌟

3.2.1.1 Sharpness of the lower bound on the packing density of $L_{m,b,b',q}$

We discuss here some results related to the equality case of the inequality on the packing density of $L_{m,b,b',q}$ given in theorem 3.2.1. Namely, proposition 2.1.1 states necessary and sufficient conditions for the displayed lower bound on $\delta(L_{m,b,b',q})$ to be sharp. Two of them are:

- The index of the narrow Mordell–Weil lattice in the full Mordell–Weil lattice equals the global Tamagawa number.
- There is a point $P \in L_{m,b,b',q}$ with $\hat{h}(P) = \frac{1}{6}\deg\left(\Delta_{\min}(E_{m,b,b'}/\mathbb{F}_q(t))\right)$ (i.e., the lower bound on the minimal non-zero height from Shioda's theorem 1.3.24 is attained).

We fix a prime $p \equiv -1 \bmod 4$ and an odd integer $e > 0$. We consider the even integer $m := \frac{p^e+1}{2}$ and fix $b, b' \in \mathbb{F}_{p^e}^\times$, let $k = \mathbb{F}_{p^{2e}}$ and $K = k(t)$.

When $p \equiv -1 \bmod 12$ then from proposition 3.1.5, we know that $c(E_{m,b,b'}/K) = 1$, so by lemma 1.3.23 we must have $[E_{m,b,b'}(K) : E_{m,b,b'}(K)^0] = 1 = c(E_{m,b,b'}/K)$. In other words, the condition in the first item above is satisfied. We now check that the condition in the second item is also fulfilled, when $p \equiv -1 \bmod 12$ and $b = b' = 1$.

Proposition 3.2.5. *Let p, e, m, K be as above. Let $\epsilon \in \{-i, 0, i\}$ where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. For simplicity we denote by $E = E_{m,1,1}$ the elliptic curve $y^2 = x^3 + x + t^m$ over K.*

1. *The point $P_\epsilon := (\epsilon, t^{m/2}) \in E(K)$ lies in the narrow Mordell–Weil lattice $E(K)^0 \subset E(K)$, if and only if $6 \mid m$.*
2. *If $m \equiv 0 \pmod 6$ (i.e., if $p \equiv -1 \bmod 12$), then the Néron–Tate height of P_ϵ is $\hat{h}(P_\epsilon) = \frac{m}{3} = \frac{1}{6}\deg\left(\Delta_{\min}(E/K)\right)$.*
3. *In general, $Q := P_0 - P_i \in E(K)^0$ and when $m = 2$ (i.e., $p = 3, e = 1$), we have $\hat{h}(Q) = 2 = \frac{1}{6}\deg\left(\Delta_{\min}(E/K)\right)$.* ⌟

Proof. — 1. At all (bad) places v above $4 + 27t^{2m}$, we know that $c_v = 1$ according to proposition 3.1.5. So we only need to study which points reduce to smooth points at the bad place $v = \infty$ (with uniformizer $\pi = t^{-1}$).

Let $a := \lceil m/6 \rceil$, so that the transformation

$$(x, y) \mapsto (x' := t^{-2a}x, y' := t^{-3a}y) \tag{3.2.1}$$

gives a Weierstrass model $y'^2 = x'^3 + x't^{-4a} + t^{m-6a}$ which is minimal integral at $v = \infty$ by proposition 3.1.5. Now P_ϵ gets mapped to

$$(\epsilon t^{-2a}, t^{m/2-3a}) \equiv \begin{cases} (\overline{0}, \overline{0}) & (\text{mod } t^{-1}) \quad \text{if } 6 \nmid m \\ (\overline{0}, \overline{1}) & (\text{mod } t^{-1}) \quad \text{if } 6 \mid m. \end{cases}$$

When $6 \nmid m$, $(\overline{0}, \overline{0})$ is the unique singular point of the reduction $\overline{E_v} : \overline{y}^2 \equiv \overline{x}^3$. When $6 \mid m$, the reduction is $\overline{y}^2 \equiv \overline{x}^3 + 1 \pmod{t^{-1}}$, so this is smooth (because $p \neq 3$, since otherwise $m \equiv 2 \pmod 6$). We deduce that $P_\epsilon = (\epsilon, t^{m/2}) \in E(K)^0$ if and only if $6 \mid m$.

2. This follows from proposition 5.1 in [Shi91], with $\chi := \lceil m/6 \rceil = m/6$. The coefficients of the Weierstrass equation of E satisfy the condition (5.2) *ibid.* (especially $\deg(4+27t^{2m}) > 12(\chi - 1)$ because $p \neq 3$). For $(x(t), y(t)) = (\epsilon, t^{m/2})$, we have $\deg(x) \leqslant 2\chi, \deg(y) = 3\chi$, so that
$$\hat{h}(P_\epsilon) = 2\chi + 2(P_\epsilon) \cdot (O) = 2\chi = \frac{1}{6} \deg\left(\Delta_{\min}(E/K)\right) = \frac{m}{3},$$
by equation (1.3.7) and proposition 1.3.26.4, using notations from remark 1.3.9.

3. Consider the point
$$Q := P_0 - P_i = \left(-4t^m - i \; ; \; 8it^{3m/2} - 3t^{m/2}\right) \in E(K).$$
Under the change of variables (3.2.1), the point Q is mapped to
$$Q_\infty := \left[(-4t^m - i)t^{a-3m/2} \; : \; (8it^{3m/2} - 3t^{m/2})t^{-3m/2} \; : \; t^{3a-3m/2}\right].$$
If $m = 2a$ (equivalently, $m = 2, a = 1$), the reduction of this point modulo t^{-1} is $[-4 : 8i : 1]$, and otherwise it is $[0 : 1 : 0]$. Both points are smooth on the reduction $\overline{E_v}$, so that $Q \in E_m(\mathbb{F}_{p^2}(t))^0$ for every (even) $m = (p^e + 1)/2$. Now the conditions $\deg(x) = m \leqslant 2\chi = 2\lceil m/6 \rceil, \deg(y) = 3m/2 \leqslant 3\chi$ from proposition 5.1 in [Shi91] for the point $Q = (x(t), y(t))$ are satisfied if and only if $m = 2$. In that case, the height of Q is $\hat{h}(Q) = 2\chi = 2$. Therefore, the lower bound from theorem 1.3.24 is sharp, according to the value $\deg\left(\Delta_{\min}(E/K)\right) = 12$ in that case. ■

Remark 3.2.6. The lower bound on the packing density displayed in the first table of example 3.2.3 for $p = 3, 7, 11$ tell us that the Tate–Shafarevich group Ш of $E_{(p+1)/2,1,1}$ over $\mathbb{F}_{p^2}(t)$ is trivial for these three primes. Indeed, using the optimality of A_2, E_6, E_8 among *lattice* packings stated in proposition 1.2.11, we must have equalities $\delta(L(3,1)) = \delta(A_2), \delta(L(7,1)) = \delta(E_6)$ and $\delta(L(11,1)) = \delta(E_8)$, where $L(p,1) := L_{(p+1)/2,1,1,p^2}$ is as in example 3.2.3. Then we conclude by using the last part of proposition 2.1.1. ⌟

3.2.2 Case $m = 3^n + 1$: lattice packings in dimensions $2 \cdot 3^n$ from characteristic 3

We now focus on the case where $m = p^n + 1$ and the characteristic is $p = 3$. The following result appeared in my paper [Let22].

Theorem 3.2.7 (theorem C). *Let $n \geqslant 1$ be an integer, set $q = 3^n$ and fix $b \in \mathbb{F}_{3^n}^\times$ such that $b^{\frac{q-1}{2}} = (-1)^{n+1}$. Consider the narrow Mordell–Weil lattice $L'_{n,b} := L_{3^n+1,b,1,3^{2n}}$ of*

$y^2 = x^3 + bx + t^{3^n+1}$ over $\mathbb{F}_{3^{2n}}(t)$. Then the rank of $L'_{n,b}$ is $2 \cdot 3^n$ and its center density satisfies the lower bound

$$\delta(L'_{n,b}) \geqslant \left(\frac{3^{n-1}+1}{4}\right)^{3^n} \cdot 3^{-n\left(\frac{3^{n-1}-1}{2}\right)-\frac{1}{2}}.$$

In particular, for $n \in \{1, ..., 7\}$, we get the following values, gathered in the table below.

n	rank of $L'_{n,b}$	$\log_2\left(\delta(L'_{n,b})\right) \geqslant$	Best *lattice* packing density known so far
1	6	$\log_2\left(\sqrt{3}/24\right) \simeq -3.79248$	$\delta(E_6) = \frac{\sqrt{3}}{24}$ ([CS98], p. xix)
2	18	$\log_2\left(\frac{\sqrt{3}}{27}\right) \simeq -3.962406$	-3.79248 [CS98], p. xix
3	54	$\log_2\left(\frac{\sqrt{3}\cdot 5^{27}}{2^{27}\cdot 3^{13}}\right) \simeq 15.88002$	15.88 (Elkies [CS98], p. xviii)
4	162	144.1852	130.679 [FIdD11]
5	486	741.1001	703.05 [Bal92]
6	1458	3172.032	3236.6 [Bal92]

We see that in dimension 54, we get the same density as the densest lattice packings of balls known so far (in fact no construction is explained for the 54-dimensional lattice MW_{54} listed in [CS98], p. xx). Moreover, in dimensions 162 and 486, we improve the current records. But in dimension 18, another construction achieves a higher packing density, and in dimensions above 1458, non-constructive lower bounds (as in theorems 1.2.15 and 1.2.16) are the best known so far. Observe that in dimension 6, we get the same density as the E_6 lattice; see also remark 3.2.12.

Remark 3.2.8. By applying Mordell's inequality (proposition 1.2.17) to the above lattices, we get the following lower bounds for the maximal lattice packing densities in dimensions 52, 53, 160, 161, 484, 485:

n	52	53	160	161	484	485
$\log_2(\delta_\ell(n)) \geqslant$	12.7525	14.2918	138.648	141.405	733.010	737.050

Before proving theorem 3.2.7, we first point out that in characteristic 3, the curves $E_{m,b,b'}$ are isotrivial. The proof also gives information on the torsion subgroup of $E_{m,b,b'}(\mathbb{F}_{3^{2n}}(t))$.

Proposition 3.2.9. *Let k be a finite field of characteristic 3. Let $m \geqslant 1$ be an integer coprime to 3. Let $b, b' \in k^\times$. Then the elliptic curve $E_{m,b,b'}$ over $K = k(t)$ is isotrivial. More precisely, it is a* cubic twist *of the constant curve $E' : y'^2 = x'^3 + bx'$ over k.*

Moreover, the Mordell–Weil group $E_{m,b,b'}(K)$ is torsion-free.

Proof. — The first statement is immediate from the change of variables $y = y', x = x' - u$ where $u \in \overline{k(t)}$ satisfies $u^3 + bu = b't^m$ (this exactly defines the superelliptic curve from subsection 3.1.7.1 when $b' = 1, m = 3^n + 1$). Indeed, if we consider the cubic extension $K' := K(u)$ of K, with $u \in \overline{K}$ as above, then we have an isomorphism

$$f : E'(K') \xrightarrow{\cong} E_{m,b,b'}(K'), \quad (x', y') \mapsto (x' - u, y'). \tag{*}$$

One can also see that the j-invariant of $E_{m,b,b'}$ is 0, so it must be an isotrivial elliptic curve.

Finally, $E_{m,b,b'}(K)$ is torsion-free directly follows from lemma 3.2.2 when m is even, but we can provide an alternative argument anyway. We have $E'(K')_{\text{tors}} = E'(k)$ by [Ulm11, Proposition 6.1, lecture 1] (see also remark 2.4.1). Since $x' - u \notin K$ whenever $x' \in k$, this proves that $E_{m,b,b'}(K)_{\text{tors}}$ has to be trivial by the isomorphism (*). ■

Remark 3.2.10. Let $E := E_{3^n+1,b,1}$, $K := k(t)$ where $k := \mathbb{F}_{3^{2n}}$. From corollary 3.1.22, we know the special value: $L^*(E/K) = 1$. Moreover, we have $\deg(\Delta_{\min}(E/K)) = 12\lceil(3^n+1)/6\rceil = 2 \cdot (3^n + 3)$ and $c(E/K) = 3$ by proposition 3.1.5. From BSD formula (see conjecture 1.3.34), we get

$$\begin{aligned} |Ш(E/K)| \cdot \mathrm{Reg}(E/K) &= c(E/K)^{-1} \cdot |E(K)_{\text{tors}}|^2 \cdot |k|^{-1} \cdot H(E/K) \\ &= 3^{-1} \cdot 3^{-2n} \cdot 3^{2n \cdot \frac{3^n+3}{6}} = 3^{n(3^{n-1}-1)-1} \end{aligned} \tag{3.2.2}$$

Moreover, we know that $E(K)^0$ is an integral lattice, so its discriminant is an integer, and since $[E(K) : E(K)^0] = c(E/K) = 3$ by proposition 3.2.14, it follows that $\mathrm{Reg}(E/K) \in \frac{1}{3^2}\mathbb{Z}_{>0}$. We will discuss the Tate–Shafarevich groups further in section 3.4. ⌟

Proof of theorem 3.2.7. — For ease of notation, in what follows, we write $K_n := \mathbb{F}_{3^{2n}}(t)$. First of all, we notice that the rank of the lattice $L'_{n,b}$ is equal to $r = 2 \cdot 3^n$. Indeed, theorem 1.3.35 and proposition 3.2.9 imply that the BSD conjecture 1.3.34 is fulfilled (we already knew this thanks to theorem 1.3.40, as mentioned at the beginning of the chapter). In particular, the algebraic rank of $E_{3^n+1,b,1}$ over K_n agrees with the analytic rank, which equals $2 \cdot 3^n$ by corollary 3.1.22.

In fact, corollary 3.1.22 also tells us that the special value of the L-function is equal to 1, i.e., $L^*(E_{3^n+1,b,1}/K_n) = 1$. Now we may apply proposition 2.1.1 using the values from proposition 3.1.5 (see also remark 3.2.10) and the last statement of proposition 3.2.9 to deduce the lower bound stated in theorem 3.2.7. This concludes the proof. ■

Remark 3.2.11. We mention here that when $n \to +\infty$, we have the asymptotic lower bound $\log_2(\delta(L'_{n,b})) \geqslant 3^n \cdot n \cdot \log_2(3) - \frac{n \cdot 3^{n-1}}{2}\log_2(3) + o(n \cdot 3^n)$ from theorem 3.2.7. Because the rank of $L'_{n,b}$ is $r = 2 \cdot 3^n$, this reads

$$\log_2(\delta(L'_{n,b})) \geqslant \left(\frac{1}{2} - \frac{1}{12}\right) r \log_2(r) + o(r \log_2(r)),$$

which implies

$$D(L'_{n,b}) \geqslant 2^{-\frac{1}{12} r \log_2(r) \cdot (1+o(1))} = r^{-r/12 \cdot (1+o(1))}, \tag{3.2.3}$$

where $D(L'_{n,b}) \in [0,1]$ is the packing density as introduced in definition 1.2.6. Although this is far from attaining Minkowski–Hlawka lower bound $\geqslant 2^{-r}$, we get the same asymptotic density as in [Elk94, theorem 1] and [Shi91, equation (1.12)].

This observation actually follows from theorem 2.3.1, together with proposition 3.1.5 (which asserts that the Szpiro ratio of our elliptic curves tends to 1 when the conductor goes to infinity) and remark 3.1.23 (which shows that Brumer's bound is asymptotically sharp). ⌟

Remark 3.2.12. When $n = 1$ and $b = 1$ (which is the only square in $\mathbb{F}_3^\times$), theorem 3.2.7 provides a 6-dimensional lattice $L'_{1,1}$ which has a sphere packing density greater than or equal to the one of the E_6 lattice. Since the latter is optimal among lattice packings by proposition 1.2.11, we must actually have equality $\delta(L'_{1,1}) = \delta(E_6)$. Then the last part of proposition 2.1.1 tells us (in particular) that the Tate–Shafarevich group of $E_{4,1,1} : y^2 = x^3 + x + t^{3^1+1}$ over $\mathbb{F}_{3^2}(t)$ is trivial: $|Ш(E_{4,1,1}/\mathbb{F}_{3^2}(t))| = 1$. ⌟

3.2.2.1 Discussion of the sharpness of the lower bound on the packing density

In this paragraph, we shorty study some of the necessary conditions under which the inequality in theorem C is actually an equality.

Proposition 3.2.13. *If $n \in \{1,2,3\}$ and $b \in \mathbb{F}_{3^n}^\times$ is such that $b^{\frac{3^n-1}{2}} = (-1)^{n+1}$, then the lower bound from theorem 3.2.7 on the packing density of $L'_{n,b}$ is an equality.* ⌟

Proof. — We have to check the three conditions stated at the end of proposition 2.1.1. Consider the curve $E := E_{3^n+1,b,1}$ over $K := \mathbb{F}_{3^{2n}}(t)$ so that $L'_{n,b} = E(K)^0$. The condition $\lambda_1(E(K)^0) = \frac{1}{6}\deg(\Delta_{\min}(E/K))$ and $[E(K) : E(K)^0] = c(E/K)$ are given in the next proposition 3.2.14, since $n \leqslant 5$. Finally, since $n \leqslant 3$, we will see later (in theorem 3.4.1) that the Tate–Shafarevich group of E/K is trivial. This concludes the proof. ■

Proposition 3.2.14. *Let $n \geqslant 1$ be an integer and for a given element $b \in \mathbb{F}_{3^n}^\times$ such that $b^{\frac{3^n-1}{2}} = (-1)^{n+1}$, we consider the elliptic curve $E := E_{3^n+1,b,1}$ over $K := \mathbb{F}_{3^{2n}}(t)$. Then:*

1. *The index $[E(K) : E(K)^0]$ is equal to $c(E/K) = 3$. In fact, if we let*

$$Q_n := \left(0, t^{(3^n+1)/2}\right) \in E_{3^n+1,b,1}(\mathbb{F}_3(t)) \hookrightarrow E(K)$$

   then $\{-Q_n, O, Q_n\}$ is a set of representatives for $E(K)/E(K)^0$.

2. *If $n \leqslant 5$, then there is some $b \in \mathbb{F}_{3^n}^\times$ as above such that there exists a point $P_n \in E(K)^0$ such that $\hat{h}(P_n) = \dfrac{1}{6}\deg(\Delta_{\min}(E/K)) = 3^{n-1} + 1$.* ⌟

We start with a useful lemma, which works specifically in the case of characteristic 3.

Lemma 3.2.15. *Let k be a finite field of characteristic 3, let $b, b' \in k^\times$ and $m \geqslant 1$ be an integer coprime to 3. Set $K := k(t)$. Fix a point $P = (x,y) \in E_{m,b,b'}(K)$ such that $\deg(x_1) > \frac{m}{3} + \deg(x_2)$, where $x = x_1/x_2 \in K$ is written as the ratio of two coprime polynomials $x_1, x_2 \in k[t]$. Then the naive and the canonical heights coincide at P, that is, $h(P) = \hat{h}(P)$.* ⌟

Proof. — The idea is to use lemma 1.3.15.2: it tells us that if $h' : E(K) \to \mathbb{R}$ is a function such that $h'(3^r P) = 9^r h'(P)$ for all $r \geqslant 0$ and $h' - h$ is bounded on $\{ 3^r P \ : \ r \geqslant 0 \}$, then $h'(P) = \hat{h}(P)$.

Since $\mathrm{char}(k) = 3$, the multiplication-by-3 map on $E_{m,b,b'}$ is given by

$$Q = (x, y) \longmapsto 3Q = (b^{-4}x^9 + b^{-4}b'^3t^{3m} - b^{-1}b't^m \ , \ y \cdot r(x)) \tag{3.2.4}$$

where $r \in K[x]$ is a polynomial of degree 12, see lemma 3.2.16 below. If $x = x_1/x_2 \in K$ and $\deg(x_1) > \frac{3m}{9} + \deg(x_2)$ then

$$\begin{aligned} \deg(b^{-4}x^9 + b^{-4}b'^3t^{3m} - b^{-1}b't^m) &= \max\{\deg(x_1^9 + x_2^9(b'^3t^{3m} - b^3b't^m)), \deg(x_2^9)\} \\ &= 9\max\{\deg(x_1), \deg(x_2)\} \end{aligned}$$

which means that $h(3P) = 9h(P)$ whenever $P = (x, y)$ satisfies the condition given in the statement.

Since $x_1(3P) = b^{-4}x_1(P)^9 + x_2(P)^9(b^{-4}b'^3t^{3m} - b^{-1}t^m)$ has degree $9\deg(x_1(P))$ and $x_2(3P) = x_2(P)^9$, we get that the inequality

$$\deg(x_1(3P)) > 9 \cdot \frac{m}{3} + 9\deg(x_2(P)) = \frac{m}{3} + \deg(x_2(3P))$$

so we may apply the same reasoning to $3P$ instead of P. By induction, we can conclude that $h(3^r P) = 9^r h(P)$ for all integers $r \geqslant 0$. Thus we may apply lemma 1.3.15 to the naive height $h : E(K) \to \mathbb{R}$ to get the conclusion. ■

Lemma 3.2.16. *Consider an elliptic curve $y^2 = x^3 + Ax + B =: f(x)$ over a field K of characteristic 3 and fix $Q = (x_Q, y_Q) \in E(K) \smallsetminus E[6]$. Then the x and y-coordinates of $3Q$ are*

$$\begin{aligned} x(3Q) &= A^{-4}x_Q^9 + A^{-4}B^3 - A^{-1}B, \\ y(3Q) &= -A^{-6}y_Q \cdot f(x_Q)^4. \end{aligned}$$

Proof. — This is a tedious but direct computation. Since $Q \notin E[2]$, we notice that $y_Q \neq 0$ and $y_Q^{-1} = \frac{y_Q}{f(x_Q)}$. By [Sil08a, p. 54], we find

$$\begin{aligned} x(2Q) &= x_Q + \frac{A^2}{f(x_Q)}, \\ y(2Q) &= -\frac{A \cdot x(2Q)}{2y_Q} - \frac{x_Q^3 - Ax_Q + B}{y_Q} \\ &= y_Q^{-1} \cdot \Big(A \cdot (x_Q + \tfrac{A^2}{f(x_Q)}) - x_Q^3 + Ax_Q - B \Big) \\ &= \frac{y_Q}{f(x_Q)} \Big(- f(x_Q) + \frac{A^3}{f(x_Q)} \Big) = -y_Q + \frac{A^3 y_Q}{f(x_Q)^2}. \end{aligned}$$

Since $2Q \neq \pm Q$, we may set

$$\begin{aligned} \lambda &:= \frac{y(2Q) - y_Q}{x(2Q) - x_Q} = A^{-2}y_Q f(x_Q) \cdot (1 + A^3 \cdot f(x_Q)^{-2}) \\ \nu &:= \frac{y_Q \cdot x(2Q) - y(2Q) \cdot x_Q}{x(2Q) - x_Q} \end{aligned}$$

and then

$$\begin{aligned} x(3Q) &= \lambda^2 - x(2Q) - x(Q) = \lambda^2 + x_Q - A^2 f(x_Q)^{-1} \\ &= A^{-4} y_Q^2 f(x_Q)^2 \cdot (1 + 2A^3 \cdot f(x_Q)^{-2} + A^6 \cdot f(x_Q)^{-4}) \ + \ x_Q - A^2 f(x_Q)^{-1} \\ &= A^{-4} f(x_Q)^3 - A^{-1} f(x_Q) + A^2 f(x_Q)^{-1} \ + \ x_Q - A^2 f(x_Q)^{-1} \\ &= A^{-4}(x_Q^9 + A^3 x_Q^3 + B^3) \ - \ A^{-1}(x_Q^3 + A x_Q + B) \ + \ x_Q \\ &= A^{-4} x_Q^9 + A^{-4} B^3 - A^{-1} B. \end{aligned} \tag{3.2.5}$$

Finally, we compute

$$\begin{aligned} \nu &= \frac{f(x_Q)}{A^2} \cdot \Big(y_Q \cdot \Big(x_Q + \frac{A^2}{f(x_Q)} \Big) - x_Q \cdot \Big(- y_Q + \frac{A^3 y_Q}{f(x_Q)^2} \Big) \Big) \\ &= \frac{f(x_Q) \cdot y_Q}{A^2} \cdot \Big(- x_Q + \frac{A^2}{f(x_Q)} - \frac{A^3 x_Q}{f(x_Q)^2} \Big) \end{aligned}$$

so we find (for simplicity we denote $f := f(x_Q), x := x_Q, y := y_Q$)

$$\begin{aligned} y(3Q) &= -\lambda \cdot x(3Q) - \nu \\ &\overset{(3.2.5)}{=} -\lambda \cdot (A^{-4} f - A^{-1} f + x) - \nu \\ &= -A^{-2} y \cdot f \cdot \Big(A^{-4} f^3 + A^{-1} f \ - \ A^{-1} f - A^2 f^{-1} \ + \ x + A^3 f^{-2} x \Big) \\ &\quad - \big(f y A^{-2} \cdot (-x) + y - A \cdot xy \cdot f^{-1} \big) \\ &= -A^{-6} y_Q \cdot f(x_Q)^4. \end{aligned}$$

■

We also state a useful result which tells us more about points of integral Néron–Tate height.

Lemma 3.2.17. *Let k be a finite field of characteristic 3, let $b, b' \in k^\times$ and $m \geqslant 1$ be an* even *integer coprime to 3. Set $K := k(t)$ and $E := E_{m,b,b'}$. Fix a point $P = (x, y) \in E_{m,b,b'}(K)$ such that $\hat{h}(P) \in \mathbb{Z}$ (e.g., $\hat{h}(P) = \frac{1}{6} \deg(\Delta_{\min}(E/K))$). Then:*

1. *The point P lies in the narrow Mordell–Weil lattice, i.e., $P \in E(K)^0$.*
2. *If $\hat{h}(P) = \frac{1}{6} \deg(\Delta_{\min}(E/K))$ then both coordinates of P are polynomials, i.e., $x, y \in k[t]$.*
3. *We have $\hat{h}(P) = h(P)$.* ⌟

Proof. — 1. From equation (1.3.6) we have

$$\hat{h}(P) = \frac{1}{6} \deg(\Delta_{\min}(E/K)) + 2(P) \cdot (O) - \gamma_\infty(P) \cdot \mathbb{1}_{P \notin E(K)^0}$$

where $\gamma_\infty(P) \in \{\frac{2}{3}, \frac{4}{3}\}$ are the values given in [SS19, table 6.1, p. 127], depending on whether $E_{m,b,b'}$ has reduction type IV or IV* at the place at infinity ∞ according to proposition 3.1.5, since $m \equiv 2, 4 \bmod 6$. Because $\gamma_\infty(P)$ is never an integer, the assumption $\hat{h}(P) \in \mathbb{Z}$ implies that $P \in E(K)^0$.

2. The above argument shows that if $\hat{h}(P) = \frac{1}{6} \deg(\Delta_{\min}(E/K))$ then we must have $(P) \cdot (O) = 0$. We prove that $x, y \in k[t]$. First observe that it is enough to check that either x or y is a polynomial because the relation $y^2 = x^3 + bx + b't^m$ and the fact that $k[t]$ is integrally closed will ensure that both x and y are polynomials. Inspecting the

proof of [Sil08b, theorem III.9.3, p. 250], the fact that $(P) \cdot (O) = 0$ implies that x cannot have a pole at any $t \in \mathbb{A}^1$ (that is, we must have $v_t(x) \geqslant 0$). This forces x to be a polynomial.

3. By lemma 3.2.15, the equality $\hat{h}(P) = h(P)$ holds as soon as $\deg(x_1) > \frac{m}{3} + \deg(x_2)$, where x is written as a ratio $x = \frac{x_1}{x_2}$ of two coprime polynomials $x_1, x_2 \in k[t]$. Therefore it is sufficient to prove that the equality $\deg(x_1) < \frac{m}{3} + \deg(x_2)$ can never occur, provided that $\hat{h}(P) \in \mathbb{Z}$ (we have a strict inequality since $3 \nmid m$). For the sake of a contradiction, assume that such an inequality holds. By equation (3.2.4), we have

$$x(3P) = \frac{z_1}{z_2}, \quad z_1 := b^{-4}x_1^9 + (b^{-4}b'^3t^{3m} - b^{-1}b't^m) \cdot x_2^9, \quad z_2 := x_2^9.$$

Note that $z_1, z_2 \in k[t]$ are coprime since x_1, x_2 are, and using the assumption $\deg(x_1) < \frac{m}{3} + \deg(x_2)$, we get $\deg(z_1) = 3m + 9\deg(x_2) > \frac{m}{3} + \deg(z_2)$. In particular, we may apply lemma 3.2.15 to the point $3P$, which asserts that $\hat{h}(3P) = h(3P) = \deg(z_1) = 3m + 9\deg(x_2)$. Thus $\hat{h}(P) = \frac{1}{9}\hat{h}(3P) = \frac{m}{3} + \deg(x_2)$ is not an integer (since $\gcd(m, 3) = 1$), so this yields a contradiction, which concludes the proof. ■

It is worth mentioning an important consequence of lemma 3.2.17.

Corollary 3.2.18. *We keep the notations k, b, b', m from lemma 3.2.17. Then the Néron–Tate and naive heights coincide on the* narrow *Mordell–Weil lattice $E_{m,b,b'}(k(t))^0$.* ⌟

Proof. — This is immediate from the above lemma, recalling that the Néron–Tate height takes *integral* values on the narrow Mordell–Weil lattice by theorem 1.3.24. ■

Proof of proposition 3.2.14. — 1. First, we know from lemma 1.3.23 that $[E(K) : E(K)^0]$ must divide $c(E/K)$ and we have $c(E/K) = 3$ by proposition 3.1.5, so the index $[E(K) : E(K)^0]$ is either 1 or 3. We prove that the index cannot be equal to 1 by noticing that the point Q_n does not belong to $E(K)^0$. Indeed, if we set $\mu := \left\lceil \frac{3^n+1}{6} \right\rceil$, then the point Q_n gets mapped to the point $(Q_n)_\infty := \left(0, t^{(3^n+1)/2-3\mu}\right)$ on the minimal integral Weierstrass model $E_\infty : y^2 = x^3 + bxt^{-4\mu} + t^{3^n+1-6\mu}$ of E at the place at infinity (via the map $(x, y) \mapsto (xt^{-2\mu}, yt^{-3\mu})$), as in proposition 3.1.5. Then $(Q_n)_\infty$ modulo t^{-1} is the singular point $(\overline{0}, \overline{0})$ of $\overline{E_\infty}$ (because $m := 3^n + 1$ is not a multiple of 6). Therefore, $Q_n \notin E(K)^0$, as claimed. It follows that $[E(K) : E(K)^0] = 3$ and therefore $\{-Q_n, O, Q_n\}$ is a set of representatives for $E(K)/E(K)^0$.

2. We first exhibit those rational points P_n explicitly, and then prove that they lie in the narrow Mordell–Weil sublattice and finally explain how to compute their Néron–Tate height. Some of these points can be found for instance using techniques described in section 3.3.

   — When $n = 1$ and $b = 1$, there is the rational point of height 2

   $$P_1 = (t^2, -t^3 + t) \in E_{4,b,1}(\mathbb{F}_3(t)) \hookrightarrow E_{4,b,1}(K).$$

   — If $n = 2$, let us write $\mathbb{F}_{3^2} \cong \mathbb{F}_3[X]/(X^2 - X - 1)$ and let z be the class of X in $\mathbb{F}_{3^2}$. One can take $b := z$ since $z^{(3^n-1)/2} = z^4 = -1$. There is a point of height 4:

   $$P_2 := \left(t^4 + (z+1)t^2 - 1\ ,\ -t^6 + t^4 - t^2 - z + 1\right) \in E_{10,b,1}(\mathbb{F}_{3^2}(t)) \hookrightarrow E_{10,b,1}(\mathbb{F}_{3^{2n}}(t))$$

— If $n = 3$ and $b = 1$, then there is a point of height $10 = 3^{n-1} + 1$:

$$P_3 = \left(t^{10} + t^8 + t^2\ ,\ -t^{15} + t^{13} - t^{11} - t^7 - t^5 + t\right) \in E_{28,b,1}(K)$$

— If $n = 4$, let $q = 3^n$, $\mathbb{F}_{q^2} \cong \mathbb{F}_3[X]/(f_8(X))$ and z be the class of X, where $f_8 = X^8 - X^5 + X^4 - X^2 - X - 1 \in \mathbb{F}_3[X]$ is the Conway polynomial of degree 8 over $\mathbb{F}_3$. Let $b = z^{q+1} = \mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(z)$, which is a generator of $\mathbb{F}_q^\times$ and in particular it is not a square in $\mathbb{F}_q^\times$. Then the following rational point has height $28 = 3^{n-1} + 1$:

$$\begin{aligned} P_4 = \big(&t^{28} + b^{52}t^{26} + b^{56}t^{24} + b^{52}t^{22} + b^{35}t^{20} + b^{75}t^{18} + b^{70}t^{16} \\ &+ b^{28}t^{14} + b^{54}t^{12} + b^{71}t^{10} + b^{71}t^8 + b^{15}t^6 + b^{29}t^4 + b^{60}t^2 - 1\ , \\ &- t^{42} + t^{40} - t^{38} + b^{39}t^{36} + b^{67}t^{34} - t^{32} + b^{47}t^{30} \\ &+ b^{49}t^{28} + b^{70}t^{24} + b^{70}t^{22} + bt^{20} + b^3t^{18} + b^{46}t^{16} - t^{14} \\ &+ b^{51}t^{12} + b^5t^{10} + b^{76}t^6 + b^{18}t^4 + b^{27}t^2 + b^{74}\big) \in E_{82,b,1}(\mathbb{F}_q(t)). \end{aligned}$$

— If $n = 5$ and $b = 1$, then there is a point[10] of height $82 = 3^{n-1} + 1$:

$$\begin{aligned} P_5 = \big(&t^{82} - t^{76} + t^{68} - t^{66} - t^{64} + t^{60} + t^{58} + t^{56} - t^{52} - t^{48} + t^{46} - \\ &t^{44} - t^{42} + t^{36} - t^{34} - t^{32} + t^{30} - t^{26} + t^{24} + t^{16} + t^{12} - t^8 - t^4 + t^2\ , \\ &t^{123} - t^{121} + t^{119} + t^{117} - t^{115} + t^{113} - t^{105} + t^{101} - t^{99} \\ &+ t^{95} - t^{87} + t^{85} + t^{81} - t^{67} - t^{61} + t^{59} - t^{57} - t^{55} + t^{51} + t^{45} \\ &- t^{43} + t^{41} + t^{37} + t^{33} - t^{31} - t^{27} - t^{19} - t^{11} + t^9 - t^7 - t^3 - t\big) \in E_{244,b,1}(\mathbb{F}_3(t)). \end{aligned}$$

It readily follows from[11] lemma 3.2.15 that for each $n \leqslant 5$, we have $\hat{h}(P_n) = h(P_n) = 3^{n-1} + 1 \in \mathbb{Z}$.

We check that for each $n \leqslant 5$, the point P_n lies in the *narrow* Mordell–Weil sublattice $E(K)^0$, i.e., its reduction modulo the place at infinity is not the singular point $(\overline{0}, \overline{0})$ of $\overline{E_\infty} : \bar{y}^2 = \bar{x}^3$. This follows from lemma 3.2.17, but we give a direct argument. Recall from equation (3.2.1) and proposition 3.1.5 that if we let $m := 3^n + 1$ and $a := \lceil m/6 \rceil$ then the transformation

$$(x, y) \mapsto (x' := t^{-2a}x, y' := t^{-3a}y)$$

gives a Weierstrass model $E_\infty : y'^2 = x'^3 + x't^{-4a} + t^{m-6a}$ which is minimal integral at $v = \infty$. If we are given a point $P = (x, y) \in E(K)$ such that $x, y \in \mathbb{F}_{3^{2n}}[t]$ are polynomials with $\deg(x) = 2a, \deg(y) = 3a$, then the corresponding point $(x', y') \in E_\infty$ is such that both x' and y' have a non-zero constant term in t^{-1}, so their reduction modulo t^{-1} is not $(\overline{0}, \overline{0})$. In particular, this applies to the points $P_1, ..., P_5$ above. ■

[10] See the file `SAGE_computation_check_for_Proposition_3.2.14__2_.ipynb` available at https://gitlab.com/gauthierleterrier/maths.

[11] One could also argue as in the proof of Proposition 5.1 of [Shi91] (even though the exact statement from there does not directly apply in characteristic 3; one has to work with $\deg(\Delta_{\min}(E/K))$ in equation (5.2) *ibid*). The idea is to use equation (1.3.7), proposition 1.3.26.4 and the fact that $P_n \in E(K)^0$, to get $\hat{h}(P_n) = \frac{1}{6}\deg(\Delta_{\min}(E/K)) + 2(P_n) \cdot (O)$ where, using notations from remark 1.3.9, $\mathscr{E} \to \mathbb{P}^1$ is the elliptic fibration attached to E over K and $(P_n), (O) \subset \mathscr{E}$ are the sections corresponding to the rational points $P_n, O \in E(K)$. Then [Shi91, Proposition 5.1] gives a condition so that (P_n) and (O) do not intersect.

Remark 3.2.19. Let E and K be as in proposition 3.2.14. For every $Q \in E(K)$, we have

$$\boxed{\hat{h}(Q) = \frac{1}{9}h(3Q)}.$$

Indeed, since $[E(K) : E(K)^0] = 3$ by proposition 3.2.14, we know that $3Q \in E(K)^0$. Thus by corollary 3.2.18 we have $9\hat{h}(Q) = \hat{h}(3Q) = h(3Q)$, whence the above identity. ⌟

Remark 3.2.20. We keep the notations from proposition 3.2.14. If we fix an element $\beta \in \mathbb{F}_{3^{2n}}^\times$ such that $\beta^2 = -b$, then for every $\epsilon \in \{-\beta, 0, \beta\}$, the six points $(\epsilon, \pm t^{(3^n+1)/2})$ belong to $E(K) \smallsetminus E(K)^0$, but this does not contradict the fact that $E(K)^0$ has index 3 in $E(K)$. For instance, we have $(\beta, t^{(3^n+1)/2}) - (0, t^{(3^n+1)/2}) \in E(K)^0$ (i.e. those two points give the same element in the quotient $E(K)/E(K)^0 \cong \mathbb{Z}/3\mathbb{Z}$).

For instance, if $n = 1$ and $b = 1$, this difference is equal to $Q' := (2t^4 + 2\beta, \beta t^6)$. At $v = \infty$, it gets mapped to

$$(Q')_\infty = (2t^2 + 2\beta t^{-2}, \beta t^3) = [2t^{-1} + 2\beta t^{-4} : \beta : t^{-3}] \equiv [0 : \beta : 0] = O_{\overline{E_\infty}} \mod \pi,$$

where $\pi := t^{-1}$. Therefore we have $Q' \in E(K)^0$ as claimed, since Q' reduces to a regular point modulo all places v of K (at $v \neq \infty$, E has good reduction, so this is obvious, and at $v = \infty$, it reduces the point at infinity mod π, which is a smooth point). ⌟

Remark 3.2.21. The densities of the narrow and the full Mordell–Weil lattices of $E_{3^n+1,b,1}$ over $\mathbb{F}_{3^{2n}}(t)$, denoted $L'_{n,b}$ and $M_{n,b}$ respectively, compare as follows. Define $Q_n := \left(0, t^{(3^n+1)/2}\right)$ as in proposition 3.2.14. One can show[12] that $\hat{h}(Q_n) = 3^{n-1} + 1 - \frac{2}{3}$. Indeed, by lemma 3.2.16 we have $x(3Q_n) = b^{-4}t^{3m} - b^{-1}t^m$ where $m := 3^n + 1$ so that lemma 3.2.15 applies. We find $9 \cdot \hat{h}(Q_n) = \hat{h}(3Q_n) = h(3Q_n) = 3m$, whence the result. Now, we have

$$\delta(M_{n,b}) \leqslant \frac{\left(\hat{h}(Q_n)^{1/2}/2\right)^{2\cdot 3^n}}{\operatorname{covol}(M_{n,b})}.$$

By proposition 3.2.14, we have $[M_{n,b} : L'_{n,b}] = 3$ so we get

$$\frac{\delta(M_{n,b})}{\delta(L'_{n,b})} \leqslant 3 \cdot \left(\frac{\hat{h}(Q_n)}{\lambda_1(L'_{n,b})^2}\right)^{3^n} \leqslant 3 \cdot \left(\frac{3^{n-1} + 1 - 2/3}{3^{n-1} + 1}\right)^{3^n} = 3 \cdot \left(1 - \frac{2}{3^n + 3}\right)^{3^n}.$$

Thus the narrow Mordell–Weil lattice $L'_{n,b}$ is always denser than the full Mordell–Weil lattice $M_{n,b}$, and the ratio of the densities tends to $3e^{-2} \simeq 0.406$ as $n \to +\infty$. ⌟

3.2.3 Laminated lattices

We now laminate the lattices obtained in theorem 3.2.7 to get sphere packings in dimension $2 \cdot 3^n + 1$ for $n \leqslant 5$, using "holes" of the narrow Mordell–Weil lattices $L'_{n,b}$ introduced in theorem 3.2.7 (i.e., points in the euclidean space $\mathbb{R}^{2\cdot 3^n}$ that are "far" from lattice points).

[12] This can also be proved using equation (1.3.6) and [SS19, Table 6.1, p. 127] and the fact that the reduction of $E_{3^n+1,b,1}$ at $v = \infty$ has type IV (by proposition 3.1.5), via an argument similar as in footnote 11 (namely one shows that the sections (Q_n) and (O) do not intersect in the elliptic surface $\mathscr{E} \to \mathbb{P}^1$ attached to $E_{3^n+1,b,1}$).

Proposition 3.2.22. *For each $n \leqslant 5$, there is a lattice packing $\mathcal{P}_n$ of euclidean balls in dimension $2 \cdot 3^n + 1$ with center density at least $\delta(L'_{n,b}) \cdot \frac{1}{2} \left(\frac{3^n+3}{2}\right)^{1/2}$, where $L'_{n,b}$ is a lattice described in theorem 3.2.7.* ⌟

We get the following values:

n	dimension of $\mathcal{P}_n$	$\log_2(\delta(\mathcal{P}_n)) \geqslant$
1	7	-4
2	19	-3.669925
3	55	16.833472
4	163	145.88137
5	487	743.57141

To our knowledge, in dimensions 55, 163 and 487, the above lattices are the densest sphere packings known so far.

Observe that the 7-dimensional lattice packing $\mathcal{P}_1$ has a density at least as big as the one of the E_7 root lattice. Since the latter maximizes the sphere packing density among lattices by proposition 1.2.11, it follows that $\delta(\mathcal{P}_1)$ is *equal* to 2^{-4}. In dimension 19, we get a density a bit worse than the best known lattice packing which gives $\log_2 \delta_\ell(19) \geqslant -3.5$ (see [CS98, p. xix]).

Proof. — Let $n \in \{1, ..., 5\}$ and fix $b \in \mathbb{F}_{3^n}^\times$ such that $b^{(3^n-1)/2} = (-1)^{n+1}$. We apply proposition 1.2.9 to the sublattice $L'_{n,b} \subset M_{n,b}$ of the full Mordell–Weil lattice $M_{n,b} := E_{3^n+1,b,1}(\mathbb{F}_{3^{2n}}(t))$.

We know that $\{-Q_n, O, Q_n\}$ are representatives for the quotient $M_{n,b}/L'_{n,b}$, as proposition 3.2.14 shows and each of them has the smallest possible height in their coset. In fact, we can see from equation (1.3.6) that any point $Q \in M_{n,b}$ satisfies

$$\hat{h}(Q) \geqslant \frac{1}{6} \deg\left(\Delta_{\min}(E/K)\right) - \gamma_\infty(Q) \cdot \mathbb{1}_{Q \notin L'_{n,b}}$$

where $\gamma_\infty(Q) = \frac{2}{3}$ is the value given in [SS19, table 6.1, p. 127], using the fact $E_{3^n+1,b,1}$ has bad additive reduction at the place at infinity ∞, with Kodaira symbol IV as stated in proposition 3.1.5. Since we assumed that $n \leqslant 5$, proposition 3.2.14 ensures that $\lambda_1(L'_{n,b})^2 = 3^{n-1} + 1$, and from the equalities $\hat{h}(Q_n) = \hat{h}(-Q_n) = 3^{n-1} + 1 - \frac{2}{3}$ (see remark 3.2.21), we get the value $h = (\frac{2}{3})^{1/2}$ introduced in proposition 1.2.9. Thus the open balls of radius $\lambda_1(L'_{n,b})/2$ centered at the points of

$$\mathcal{P}_n := L'_{n,b} \times 3h\mathbb{Z} \;\cup\; (L'_{n,b} + Q_n) \times (3h\mathbb{Z} + h) \;\cup\; (L'_{n,b} - Q_n) \times (3h\mathbb{Z} - h)$$

form a packing by proposition 1.2.9, which also tells us that $\mathcal{P}_n$ is a *lattice* packing and not only a periodic packing (since $M_{n,b}/L'_{n,b}$ is cyclic, of order 3). Moreover, one has

$$\delta(\mathcal{P}_n) = \frac{\lambda_1(L'_{n,b})}{2 \cdot (2/3)^{1/2}} \cdot \delta(L'_{n,b}) = \delta(L'_{n,b}) \cdot \frac{1}{2} \left(\frac{3^n + 3}{2} \right)^{1/2}. \qquad \blacksquare$$

3.3 · Kissing numbers and Gram matrices

We now discuss some computational results regarding the narrow Mordell–Weil lattices $L'_{n,b} \hookrightarrow \mathbb{R}^{2 \cdot 3^n}$ we introduced in theorem 3.2.7. Some of these algorithmic aspects are useful because they show that it is possible to work quite concretely with those lattices, for instance by finding rational points on the corresponding elliptic curve $E_{3^n+1,b,1}$. Recall that given $n \geqslant 1$ and $b \in \mathbb{F}_{3^n}^\times$ such that $b^{(3^n-1)/2} = (-1)^{n+1}$, we consider the curve $E_{3^n+1,b,1} : y^2 = x^3 + bx + t^{3^n+1}$ over $\mathbb{F}_{3^{2n}}(t)$ and the lattice $L'_{n,b} = E_{3^n+1,b,1}\big(\mathbb{F}_{3^{2n}}(t)\big)^0$.

More specifically, with the help of the computer algebra system SAGE [The21], we can determine the kissing number of our 54-dimensional lattice $L'_{3,1}$ which is the densest lattice sphere packing known so far in $\mathbb{R}^{54}$.

Computational theorem 3.3.1 (Computational theorem D)**.** *The kissing number of the 54-dimensional lattice $L'_{3,1}$ is equal to $\kappa(L'_{3,1}) = 15309000 = 2^3 \cdot 3^7 \cdot 5^3 \cdot 7$.* ⌟

The proof is given in subsection 3.3.1.3; the SAGE code is available at `https://gitlab.com/gauthierleterrier/maths` and can be tested on `https://www.cocalc.com`. This value is not a record because in dimension 48, there is a lattice with kissing number 52416000 (see [CS98, p. xxii]), and we have $\kappa_\ell(d+1) \geqslant \kappa_\ell(d) + 2$ for every dimension $d > 0$ by remark 1.2.18. However, it is interesting to see that it is possible to compute the kissing number of these Mordell–Weil lattices. It is also possible to do so with the Mordell–Weil lattices in characteristic 2 from [Elk94, p. 360]: it is stated that the 64-dimensional lattice has kissing number 89413632 (see remark 3.3.5).

3.3.1 Kissing number of a 54-dimensional Mordell–Weil lattice

Computing the kissing number can be done by producing minimal vectors in the lattice. Thereby, a first step to compute $\kappa(L'_{3,1})$ is to have a criterion to exhibit rational points on the elliptic curve $E_{28,1,1} : y^2 = x^3 + x + t^{28}$ over $\mathbb{F}_{3^6}(t)$.

Lemma 3.3.2. *Let k be a finite field of prime characteristic $p \geqslant 2$ and fix $b \in k^\times$. Let $z(t) = \sum_{j=0}^d z_j t^j \in k[t]$ be of degree d divisible by p. Then the following are equivalent:*

1. *There exists a polynomial $s \in k[t]$ such that $z = s^p + bs$.*
2. *We have $z_0 = s_0^p + bs_0$ for some $s_0 \in k$ and for every integer $j \geqslant 1$ coprime to p, we have*

$$f_j := \sum_{r=0}^{R(j)} (-1)^r b^{-\frac{p^{r+1}-1}{p-1}} z_{p^{R(j)-rj}}^{p^r} = 0 \tag{3.3.1}$$

where $R(j) := \lfloor \log_p(d/j) \rfloor$.

Moreover, if 2) holds, then the polynomial s in 1) is uniquely determined by z up to an additive constant *in k, and for each $j \geqslant 1$ coprime to p its j-th coefficient is $s_j = b^{-1}z_j$.*

Finally, an analogous statement holds for Laurent series $z \in k((t^{-1}))$: if 1) holds for some $s \in k((t^{-1}))$ then 2) holds. ⌟

Note that $\frac{p^{r+1}-1}{p-1} = 1 + p + p^2 + \cdots + p^r$ and that $R(j) = 0$ whenever $j > d/p$, in which case the equation reads $b^{-1}z_j = 0$ (if $\gcd(j,p) = 1$), i.e., $z_j = 0$, which is automatically true when $j > d$.

Proof. — • We first prove 1) $\implies$ 2). Let us write $s(t) = \sum_{j=0}^{d/p} s_j t^j$ so that

$$s^p + bs = \sum_{j=0}^{d/p}(s_j^p t^{pj} + bs_j t^j) = \sum_{j=0}^{d}(s_{j/p}^p + bs_j)t^j$$

where we set $s_{j'} := 0$ if $j' \notin \mathbb{Z}$ or $j' > d/p$. Thus we get $z_j = s_{j/p}^p + bs_j$ for all $j \geqslant 0$. In particular, when $j \notin p\mathbb{Z}$ we get $z_j = bs_j$.

Let us fix some $j \geqslant 1$ coprime to p. Then we get successively

$$\begin{aligned} s_j^p + bs_{pj} = z_{pj} &\implies s_{pj} = b^{-1}(z_{pj} - s_j^p) = b^{-1}(z_{pj} - b^{-p}z_j^p) \\ s_{pj}^p + bs_{p^2j} = z_{p^2j} &\implies s_{p^2j} = b^{-1}(z_{p^2j} - s_{pj}^p) = b^{-1}z_{p^2j} - b^{-p-1}z_{pj}^p + b^{-p^2-p-1}z_j^{p^2}. \end{aligned}$$

By induction on $R \geqslant 0$, we deduce

$$s_{p^Rj} = b^{-1}z_{p^Rj} - b^{-(p+1)}z_{p^{R-1}j}^p + b^{-(p^2+p+1)}z_{p^{R-2}j}^{p^2} - \cdots \pm b^{-(p^R+p^{R-1}+\cdots+1)}z_j^{p^R}. \tag{3.3.2}$$

When $R = R(j) > \log_p(d/j) - 1 = \log_p\left(\frac{d}{pj}\right)$ we have $p^{R(j)}j > d/p$ which means that $s_{p^{R(j)}j} = 0$, i.e., equation (3.3.1) holds.

- The converse 2) $\implies$ 1) follows from the discussion above. Let $z \in k[t]$ be a polynomial as in 2). The coefficient s_0 is given by assumption. Given $j \notin p\mathbb{Z}$, we set $s_j := b^{-1}z_j$. If $j \geqslant 1$ is coprime to p, then we have to define $s_{p^r \cdot j}$ for all $r \geqslant 1$. This can be done using equation (3.3.2) and the other equations displayed above; for instance $s_{p\cdot j} = b^{-1}(z_{pj} - b^{-p}z_j^p)$. One can then check using (3.3.2) that $z_j = s_{j/p}^p + bs_j$ for every $j \geqslant 0$ (not necessarily coprime to p), which proves that $z = s^p + bs$.

  Finally, note that a polynomial $s \in k[t]$ such that $s^p + bs = z$ must be unique up to an additive constant, because if s_1, s_2 are two such polynomials then $(s_1 - s_2)^p = -b(s_1 - s_2)$ so taking degrees on both sides shows that $s_1 - s_2$ must be constant.

- The proof of 1) $\implies$ 2) from above immediately generalizes to the case of Laurent series $z = \sum_{j=-\infty}^{d} z_j t^j \in k((t^{-1}))$ and $s \in k((t^{-1}))$. ■

Remark 3.3.3. When $b = -1$, the condition $z_0 = s_0^p + bs_0$ for some $s_0 \in k$ is equivalent to $\mathrm{tr}_{k/\mathbb{F}_p}(z_0) = 0$ by proposition 1.4.3. See also lemma 3.1.27. ⌟

Recall from corollary 3.1.22 that the narrow Mordell–Weil lattice $L'_{3,1} = E_{28,1,1}(\mathbb{F}_{3^6}(t))^0$ of $E_{28,1,1}$ has rank 54 and from proposition 3.2.14 that $\lambda_1(L'_{3,1})^2 = 3^{3-1} + 1 = 10$. In other words, we want to count the number of points $P \in L'_{3,1}$ with $\hat{h}(P) = 10$.

By lemma 3.2.17, all points $P = (x, y) \in E_{28,1,1}(\mathbb{F}_{3^6}(t))$ with Néron–Tate height 10 must lie in the narrow Mordell–Weil lattice and both x, y are polynomials with $\deg(x) = h(P) = \hat{h}(P) = 10$. Moreover, from the relation $y^2 = x^3 + x + t^{3^n+1}$ and $\deg(x) = 3^{n-1} + 1$ we deduce that $\deg(y) = \frac{3^n+3}{2}$ (for any $n \geqslant 1$); when $n = 3$ this implies that $\deg(y) = 15$. In other words, we want to compute

$$\kappa(L'_{3,1}) = \#\{\, (x, y) \in \mathbb{F}_{3^6}[t] \times \mathbb{F}_{3^6}[t] \;:\; \deg(x) = 10, y^2 = x^3 + x + t^{28} \,\}. \tag{3.3.3}$$

In what follows, we will denote $k := \mathbb{F}_{3^6}$ and $E := E_{28,1,1}$ for simplicity. We have $|k| = 729$ and it is not reasonable to do a naive "brute-force" approach to list all the solutions as in equation (3.3.3) (e.g., the space of polynomials $x(t)$ of degree 10 over k has size $|k|^{11} > 3 \cdot 10^{31}$, so running over x and checking whether $x^3 + x + t^{28}$ is a square in $k[t]$ gives an extremely inefficient strategy).

3.3.1.1 Polynomial equations in the coefficients y_j

Instead, we will run over $y \in k[t]$ (despite having larger degree, namely 15) and check for solutions in x thanks to lemma 3.3.2. Given $y = \sum_{j=0}^{15} y_j t^j \in k[t]$ of degree 15, we are looking for polynomials $x \in k[t]$ of degree 10 such that $(x, y) \in E(k(t))$. Consider the polynomial $z(t) := y^2 - t^{28} = \sum_{j=0}^{30} z_j t^j$ of degree 30. By lemma 3.3.2, there is a polynomial $x \in k[t]$ such that $z = x^3 + x$ if and only if the equations (3.3.1) are satisfied, and $z_0 = y_0^2 = s_0^3 + s_0$ for some $s_0 \in k$.

We can express each coefficient z_j in terms of the 16 unknowns y_j. For instance,

$$z_{30} = y_{15}^2, \quad z_{29} = -y_{14}y_{15}, \quad z_{28} = y_{14}^2 - y_{13}y_{15} - 1, \quad z_{26} = y_{13}^2 - y_{12}y_{14} - y_{11}y_{15}. \tag{3.3.4}$$

Assume now that there is a polynomial $x = \sum_{j=0}^{10} x_j t^j \in k[t]$ with $z = x^3 + x$. Lemma 3.3.2 gives us equations $f_j = 0$ for each integer $j \geqslant 1$ coprime to 3. In particular, they tell us that:

- For every $j \geqslant 1$ coprime to 3, we have $z_j = x_j$. This holds exactly when $j \in \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29\}$.
- In particular, for all $j > 30/3 = 10$ coprime to 3, we have $z_j = x_j = 0$. In other words, we have

$$z_{11} = z_{13} = z_{14} = z_{16} = z_{17} = z_{19} = z_{20} = z_{22} = z_{23} = z_{25} = z_{26} = z_{28} = z_{29} = 0. \tag{3.3.5}$$

- Moreover, lemma 3.3.2 will give us equations involving the 7 variables $z_1, z_2, z_4, z_5, z_7, z_8, z_{10}$ and the corresponding indices multiplied by powers of 3. (e.g., z_3, z_9, z_{27}; z_6, z_{18}, etc.)
- The polynomial x is necessarily unique up to an additive constant in k. More precisely, there are exactly 3 solutions to the equation $\alpha^3 + \alpha = 0$ in $\mathbb{F}_{3^2} \hookrightarrow k$, so there are exactly 3 polynomials $x(t)$ such that $x^3 + x = z(t)$.

Using equation (3.3.5) and remembering that $y_{15} \neq 0$, we find successively:

$$\begin{aligned}
z_{29} &= -y_{14}y_{15} = 0 && \Longrightarrow\ y_{14} = 0\\
z_{28} &= -y_{13}y_{15} - 1 = 0 && \Longrightarrow\ y_{13} = -y_{15}^{-1}\\
z_{26} &= y_{15}^{-2} - y_{11}y_{15} = 0 && \Longrightarrow\ y_{11} = y_{15}^{-3}\\
z_{25} &= (-y_{10}y_{15}^2 + y_{12})/y_{15} = 0 && \Longrightarrow\ y_{10} = y_{12}y_{15}^{-2}\\
z_{23} &= -y_8y_{15} = 0 && \Longrightarrow\ y_8 = 0\\
z_{22} &= (-y_7y_{15}^7 - y_{12}^2y_{15}^4 + y_9y_{15}^5 + 1)/y_{15}^6 = 0 && \Longrightarrow\ y_7 = y_{15}^{-7}(-y_{12}^2y_{15}^4 + y_9y_{15}^5 + 1)\\
z_{20} &= (-y_5y_{15}^9 + 1)/y_{15}^8 && \Longrightarrow\ y_5 = y_{15}^{-9}\\
z_{19} &= (-y_4y_{15}^8 + y_{12}^3y_{15}^4 + y_9y_{12}y_{15}^5 + y_6y_{15}^6 - y_{12})/y_{15}^7 && \Longrightarrow\ y_4 = y_{15}^{-8}(y_{12}^3y_{15}^4 + y_9y_{12}y_{15}^5 + y_6y_{15}^6 - y_{12})\\
z_{17} &= (-y_2y_{15}^6 - y_{12}^3)/y_{15}^5 = 0 && \Longrightarrow\ y_2 = -y_{15}^{-6}y_{12}^3
\end{aligned} \tag{3.3.6}$$

Moreover, from the equation $z_{16} = 0$ we can deduce that:

$$\begin{aligned}
y_1 &= y_{15}^{-13}(-y_{12}^4y_{15}^8 - y_9^2y_{15}^{10} + y_6y_{12}y_{15}^{10} + y_3y_{15}^{11} + y_{12}^2y_{15}^4 - y_9y_{15}^5 - 1)\\
z_{14} &= 0
\end{aligned}$$

and from the equation $z_{13} = 0$ we can deduce that:

$$\begin{aligned}
y_0 &= -y_{15}^{-12}(y_{12}^5y_{15}^8 - y_9y_{12}^3y_{15}^9 + y_6y_9y_{15}^{11} + y_3y_{12}y_{15}^{11} - y_9y_{12}y_{15}^5 - y_6y_{15}^6 + y_{12})\\
z_{11} &= 0.
\end{aligned}$$

From these computations, we see that we are left with 5 free variables, namely $y_3, y_6, y_9, y_{12}, y_{15}$ in k. This is still too large for a brute-force computation (we have $|k|^5 > 10^{14}$). We have not used the remaining 7 equations $f_1, f_2, f_4, f_5, f_7, f_8, f_{10} = 0$ from lemma 3.3.2 yet. In general, they are given as follows (but recall that we have set $b := 1 \in \mathbb{F}_{3^3}^\times$ in our case):

$$\begin{aligned}
&b \cdot f_1 = z_{27} - b^{-3}z_9^3 + b^{-12}z_3^9 - b^{-39}z_1^{27}, \quad b \cdot f_2 = z_{18} - b^{-3}z_6^3 + b^{-12}z_2^9, \quad b \cdot f_4 = z_{12} - b^{-3}z_4^3\\
&b \cdot f_5 = z_{15} - b^{-3}z_5^3, \quad b \cdot f_7 = z_{21} - b^{-3}z_7^3, \quad b \cdot f_8 = z_{24} - b^{-3}z_8^3, \quad b \cdot f_{10} = z_{30} - b^{-3}z_{10}^3.
\end{aligned}$$

Since the coefficients z_j can be expressed in terms of the y_j (as in equation (3.3.4)), these 7 equations yield (complicated) polynomial equations in $k[y_3, y_6, y_9, y_{12}, y_{15}^{\pm 1}]$. We may assume that the degree in each variable is $< |k|$ since each y_j belongs to k and $\alpha^{|k|} = \alpha$ for all $\alpha \in k$. For instance we have $f_{10} = -y_5^6 + y_4^3y_6^3 + y_3^3y_7^3 + y_2^3y_8^3 + y_1^3y_9^3 + y_0^3y_{10}^3 + y_{15}^2b^3$ which becomes

$$\begin{aligned}
f_{10} = y_{15}^{-54} \cdot (&y_{15}^{56} - y_{12}^{18}y_{15}^{36} + y_6^3y_{12}^9y_{15}^{42} - y_9^9y_{15}^{45} + y_6^3y_9^3y_{12}^3y_{15}^{45} + y_3^3y_{12}^6y_{15}^{45}\\
&+ y_6^6y_{15}^{48} - y_3^3y_9^3y_{15}^{48} - y_9^3y_{12}^6y_{15}^{27} - y_9^6y_{15}^{30} + y_3^3y_{15}^{33} - y_{12}^6y_{15}^{12} - y_9^3y_{15}^{15} - 1).
\end{aligned}$$

Therefore $f_{10} = 0$ implies $y_3^3 \cdot U_{10} + V_{10} = 0$ where

$$\begin{aligned}
U_{10} &:= y_{12}^6y_{15}^{45} + y_{15}^{33} - y_9^3y_{15}^{48},\\
V_{10} &:= y_{15}^{56} - y_{12}^{18}y_{15}^{36} + y_6^3y_{12}^9y_{15}^{42} - y_9^9y_{15}^{45} + y_6^3y_9^3y_{12}^3y_{15}^{45} + y_6^6y_{15}^{48} - y_9^3y_{12}^6y_{15}^{27} - y_9^6y_{15}^{30} - y_{12}^6y_{15}^{12} - y_9^3y_{15}^{15} - 1.
\end{aligned} \tag{3.3.7}$$

The point here is that U_{10} and V_{10} only depend on y_6, y_9, y_{12}, y_{15} but not on y_3. So we have two disjoint cases:

① Either $U_{10} = 0$, i.e., $y_{15}^{33}(y_{12}^2y_{15}^4 - y_9y_{15}^5 + 1)^3 = 0$. This implies

$$y_9 = y_{15}^{-5}(y_{12}^2y_{15}^4 + 1). \tag{3.3.8}$$

Substituting this value in the equation $f_7 = 0$ gives

$$\begin{aligned} y_3^3 \cdot U_7 + V_7 &= 0 \\ U_7 &:= -y_{12}^9 y_{15}^{15} - y_6^3 y_{15}^{21} + y_{12}^3 y_{15}^3 \\ V_7 &:= -y_{12}^3 y_{15}^{26} - y_6 y_{15}^{28} + y_6^3 y_{12}^{12} y_{15}^{12} + y_6^6 y_{12}^3 y_{15}^{18} + y_{12} y_{15}^{22} - y_6^3 y_{12}^6 \end{aligned} \tag{3.3.9}$$

Therefore:

- either $U_7 = (-y_{12}^3 y_{15}^5 - y_6 y_{15}^7 + y_{12} y_{15})^3 = 0$, which determines y_6 uniquely. In this case, the only free variables are y_3, y_{12}, y_{15}.
- or $U_7 \neq 0$ and we have a formula for $y_3^3 = -V_7 \cdot U_7^{-1}$ so that $y_3 = (-V_7 \cdot U_7^{-1})^{|k|/3}$. In this case, the only free variables are y_6, y_{12}, y_{15}.

② Or $U_{10} \neq 0$ so that $y_3^3 = -U_{10}^{-1} V_{10}$ which gives

$$y_3 = (-U_{10}^{-1} V_{10})^{\frac{|k|}{3}} \tag{3.3.10}$$

In this case, the only free variables are y_6, y_9, y_{12}, y_{15}.

3.3.1.2 Using isometries to reduce the search space

We could possibly investigate more deeply the other equations $f_j = 0$, but instead we use *symmetries* to further reduce the search space, i.e., we make use of some automorphisms (= isometries) of the lattice $E(K)^0$.

Let us consider the curves $E_{q+1,b,1}$ over $k(t)$ where $q = p^n, p := 3, n = 3, k := \mathbb{F}_{q^2}$ and $b \in \mathbb{F}_q^\times$ satisfies $\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(b) = (-1)^{n+1}$. First, the most obvious isometries are $(x, y) \mapsto (x, -y)$ and $(x, y) \mapsto (x + \beta, y)$ where $\beta^3 + b\beta = 0$ (since $b \in \mathbb{F}_{3^n}$, there are always 3 solutions $\beta \in k = \mathbb{F}_{3^{2n}}$).

Secondly, define $\sigma : K \to K$ to be the field automorphism of $K = k(t)$ such that $\sigma(t) = t$ and $\sigma(a) = a^3$ for all $a \in k$. If $b \in \mathbb{F}_3^\times$ (i.e., $\sigma(b) = b$), then

$$f_\sigma : \ (x, y) \mapsto (\sigma(x), \sigma(y))$$

is a (surjective) isometry[13] of $E(K)^0$. Finally, the map

$$g_\alpha : \ (x(t), y(t)) \mapsto (x(\alpha t), y(\alpha t)) \tag{3.3.11}$$

is well-defined onto $E(K)^0$ provided that $\alpha^{q+1} = 1$ (see remark 3.3.4 below) and this is an isometry.

Note that $f_\sigma : (x, y) \mapsto (\sigma(x), \sigma(y))$ changes the y_{15}-coefficient to y_{15}^3 and $g_\alpha : (x(t), y(t)) \mapsto (x(\alpha t), y(\alpha t))$ changes it to $\alpha^{15} y_{15}$. We check that these isometries preserve the non-vanishing of the polynomials U_{10} and U_7 (given in equations (3.3.7) and (3.3.9)) that define the two cases ① and ② above. It is clear for the isometry f_σ, since $\sigma \in \mathrm{Gal}(k(t)/\mathbb{F}_3(t))$ preserves polynomial functions of $y_6, y_9, y_{12}, y_{15} \in k$. As for g_α, where $\alpha^{3^n+1} = \alpha^{28} = 1$, we (miraculously?) find that:

[13] Observe that Néron–Tate height is preserved under this map thanks to corollary 3.2.18.

- We have $U_{10} = 0$ if and only if $y_{12}^2 y_{15}^4 - y_9 y_{15}^5 + 1 = 0$. Now, the action of g_α on a polynomial $y(t)$ changes the coefficient y_j into $\alpha^j y_j$. We have

$$\begin{aligned}(\alpha^{12} y_{12})^2 \cdot (\alpha^{15} y_{15})^4 - \alpha^9 y_9 \cdot (\alpha^{15} y_{15})^5 + 1 &= \alpha^{84} y_{12}^2 y_{15}^4 - \alpha^{84} y_9 y_{15}^5 + 1 \\ &= y_{12}^2 y_{15}^4 - y_9 y_{15}^5 + 1,\end{aligned}$$

  since $84 \equiv 0 \bmod 28$ and $\alpha^{28} = 1$.

- We have $U_7 = 0$ if and only if $-y_{12}^3 y_{15}^5 - y_6 y_{15}^7 + y_{12} y_{15} = 0$. We find

$$\begin{aligned}&- (\alpha^{12} y_{12})^3 \cdot (\alpha^{15} y_{15})^5 - \alpha^6 y_6 \cdot (\alpha^{15} y_{15})^7 + \alpha^{12} y_{12} \cdot \alpha^{15} y_{15} \\ &= -\alpha^{111} y_{12}^3 y_{15}^5 - \alpha^{27} y_6 y_{15}^7 + \alpha^{111} y_{12} y_{15} \\ &= \alpha^{-1} \cdot (-y_{12}^3 y_{15}^5 - y_6 y_{15}^7 + y_{12} y_{15}).\end{aligned}$$

Let z be a generator of $k^\times$. Then $\ker(\mathrm{N}_{k/\mathbb{F}_q})$ is a subgroup of $k^\times$ of size $q+1 = 28$, generated by $z^{q-1} = z^{26}$. We want to use the isometries g_α from equation (3.3.11), where $\alpha^{q+1} = 1$, that is, $\alpha \in \ker(\mathrm{N}_{k/\mathbb{F}_q})$. Recall that under g_α, the coefficient y_{15} becomes $\alpha^{15} y_{15}$. Now, $\alpha \mapsto \alpha^{15}$ is a bijection of $k^\times$ (because $\gcd(15, |k^\times|) = \gcd(3 \cdot 5, 2^3 \cdot 7 \cdot 13) = 1$) and hence of $\ker(\mathrm{N}_{k/\mathbb{F}_q})$. Thereby, we may assume that $y_{15} = z^{e_{15}}$ for some $0 \leqslant e_{15} < 26$; this can be achieved by applying g_α for some $\alpha \in \langle z^{26} \rangle = \ker(\mathrm{N}_{k/\mathbb{F}_q})$.

Furthermore, the isometry $(x, y) \mapsto (\sigma(x), \sigma(y))$ allows us to assume without loss of generality that $e_{15} \in \{0, 1, 2, 4, 5, 7, 8, 13, 14, 17\}$, because these 10 values from a complete set of representatives[14] for the action of the cyclic group $\langle 3 \rangle^\times \leqslant (\mathbb{Z}/26\mathbb{Z})^\times$ on $\mathbb{Z}/26\mathbb{Z}$. This leaves us with 10 values for y_{15} (instead of $q^2 - 1 = 728$ initially).

Remark 3.3.4. More generally, given $\alpha, \beta, \gamma \in k$ and $D_{b,\beta}(t) \in k[t]$, we could define[15] the automorphism of $E(k(t))$

$$(x(t), y(t)) \longmapsto \Big(x(\alpha(t+\beta)) + D_{b,\beta}(t) + \gamma, \;\; y(\alpha(t+\beta)) \Big)$$

provided that

$$\alpha^{q+1} = 1, \quad \gamma^p + b\gamma = \beta^{q+1}, \quad D_{b,\beta}(t)^p + b D_{b,\beta}(t) = \beta t^q + \beta^q t. \tag{3.3.12}$$

However we will not make use of these extra automorphisms. Notice that if $\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(b) = (-1)^{n+1}$, then for every $\beta \in k$, there is some $D_{b,\beta}(t) \in k[t]$ such that $D_{b,\beta}(t)^p + b D_{b,\beta}(t) =$

[14] There are indeed 10 representatives, as lemma 1.4.27 shows.

[15] Indeed,

$$\begin{aligned}y(\alpha(t+\beta))^2 &= x(\alpha(t+\beta))^p + b \cdot x(\alpha(t+\beta)) + (\alpha(t+\beta))^{q+1} \\ &= x(\alpha(t+\beta))^p + b \cdot x(\alpha(t+\beta)) + \alpha^{q+1}(t+\beta)(t^q + \beta^q) \\ &= x(\alpha(t+\beta))^p + b \cdot x(\alpha(t+\beta)) + \alpha^{q+1}(t^{q+1} + \beta t^q + \beta^q t + \beta^{q+1})\end{aligned}$$

and if we let $\xi(t) := x(\alpha(t+\beta)) + D_{b,\beta}(t) + \gamma$ then

$$\xi(t)^p + b\xi(t) + t^{q+1} = x(\alpha(t+\beta))^p + b \cdot x(\alpha(t+\beta)) + t^{q+1} \;\; + \;\; D_{b,\beta}(t)^p + b \cdot D_{b,\beta}(t) \;\; + \;\; \gamma^p + b\gamma.$$

We see that the two expressions match if equation (3.3.12) is satisfied.

$\beta t^q + \beta^q t$ holds, as lemma 3.3.2 shows. Indeed, in the lemma, the only relevant equation is for $j = 1$, when $R(j) = n$ and we get the condition

$$(-1)^0 b^{-1}\beta + (-1)^n b^{-\frac{p^{n+1}-1}{p-1}} \beta^{q^2} = 0.$$

Note that $\beta^{q^2} = \beta$ and we have

$$b^{-1} + (-1)^n b^{-\frac{p^{n+1}-1}{p-1}} = 0 \iff 1 + (-1)^n b^{-(p+\ldots+p^n)} = 0 \iff 1 + (-1)^n \mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(b)^{-p} = 0$$

and the latter equation holds precisely because $p = 3$ is odd and $\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(b) = (-1)^{n+1}$. ⌟

3.3.1.3 Conclusion

We can now summarize the above discussion to explain the computation of the kissing number $\kappa(L'_{3,1})$. The SAGE program used for the computation is available at https://gitlab.com/gauthierleterrier/maths.

Proof of computational theorem 3.3.1. — The general procedure for the computation of $\kappa(L'_{3,1})$ is as follows. Fix a generator g of $k^\times$. For each of the 10 integers $e_{15} \in S := \{0, 1, 2, 4, 5, 7, 8, 13, 14, 17\}$, let $y_{15} = g^{e_{15}}$ and loop over $y_{12} \in k$: there are two disjoint cases ① and ② to consider as above.

1. Either we use equation (3.3.8), in which case we solve a system of polynomial equations in either $y_3 \in k$ or in $y_6 \in k$.
2. Or we use equation (3.3.10), in which case we solve a system of polynomial equations in $y_6, y_9 \in k$.

For each solution, we get the 5 coefficients $y_3, y_6, y_9, y_{12}, y_{15}$ and then we define $y_0, y_1, y_2, y_4, y_5, y_7, y_8, y_{10}, y_{11}, y_{13}, y_{14}$ using the equations (3.3.6) and set $y := \sum_{j=0}^{15} y_j t^j \in k[t]$. We check that $y_0^2 = s_0^3 + s_0$ for some $s_0 \in k$. Then lemma 3.3.2 ensures that there are exactly 3 polynomials $x \in k[t]$ such that $P = (x, y) \in E(K)^0$ has Néron–Tate height 10 (see also discussion on page 158).

Let us say a few words about each case.

1. The first case only involves polynomial equations in 1 variable (either y_3 or y_6), so SAGE [The21] only took 40 seconds to complete the search: only $e_{15} = 0$ and $e_{15} = 13$ have a non-zero number of solutions $y(t)$, and both of them had 1458 solutions $y(t)$, corresponding to $3 \cdot 1458 = 4374$ minimal vectors $(x(t), y(t))$ in $E(K)^0$. Thus, for each multiple e_{15} of 13, we have $1458 \cdot 3$ minimal points $(x(t), y(t))$ with $y_{15} = g^{e_{15}}$. Since $(q^2 - 1)/13 = 56$, we get in total $56 \cdot 1458 \cdot 3 = 244944$ minimal vectors such that equation (3.3.8) is satisfied.
2. The second case takes longer (roughly 28 minutes on SAGE [The21]) to list all the corresponding y-coordinates with $y_{15} = g^{e_{15}}$, distributed as follows:

e_{15}	0	1	2	4	5	7	8	13	14	17
Number of $y(t)$	6561	5832	8019	8019	8019	5832	5832	6561	5832	8019

Given an integer $e \in \mathbb{Z} \cap [0, q^2 - 1]$, its orbit of its class modulo 26 under the multiplicative action of the powers of $3 \in (\mathbb{Z}/26\mathbb{Z})^\times$ has a unique representative e_{15} in

$S = \{0, 1, 2, 4, 5, 7, 8, 13, 14, 17\}$. Then the number of minimal vectors $(x, y) \in E(K)^0$ with $y_{15} = g^e$ is given by 3 times the number of $y(t)$ corresponding to e_{15} in the above table.

This allows us to deduce that there are exactly 15064056 points $(x, y) \in E(K)^0$ of height 10 such that $U_{10}(y_9, y_{12}, y_{15}) \neq 0$ (see equations (3.3.8) and (3.3.10); it just means $y_9 \neq y_{15}^{-5}(y_{12}^2 y_{15}^4 + 1)$).

All in all, the kissing number of $L'_{3,1} = E(K)^0$ is:

$$15064056 + 244944 = 15309000 = 2^3 \cdot 3^7 \cdot 5^3 \cdot 7,$$

which concludes the proof. ■

Remark 3.3.5. A similar strategy can be used to determine the kissing number of Elkies' 64-dimensional lattice obtained in [Elk94] as the narrow Mordell–Weil lattice MW_{64} of the curve $E : y^2 + y = x^3 + t^{q+1}$ over $\mathbb{F}_Q(t)$ where $n = 5, q = 2^n = 32, Q = q^2 = 1024, k = \mathbb{F}_Q$. The minimal non-zero height is 12. Here we first fix $x(t) = \sum_{j=0}^{12} x_j t^j \in k[t]$ with $x_{12} \neq 0$ and then check whether $z(t) := x(t)^3 + t^{q+1}$ can be written as $y^2 + y$, using lemma 3.3.2. There is such a polynomial y such that $(x(t), y(t)) \in E(k(t))$ if and only if $\mathrm{tr}_{k/\mathbb{F}_2}(x_0^3) = 0$ and for every odd integer $j \geqslant 1$, we have

$$f_j := \sum_{r=0}^{R(j)} z_{2^r j}^{2^{R(j)-r}} = 0.$$

where $R(j) := \lfloor \log_2(d/j) \rfloor$. For $j = 1, 3, 5, ..., 35$ this yields:

$$z_{32} + z_{16}^2 + z_8^4 + z_4^8 + z_2^{16} + z_1^{32} = 0, \quad z_3^8 + z_6^4 + z_{12}^2 + z_{24} = 0, \quad z_5^4 + z_{10}^2 + z_{20} = 0,$$
$$z_7^4 + z_{14}^2 + z_{28} = 0, \quad z_9^4 + z_{18}^2 + z_{36} = 0, \quad z_{11}^2 + z_{22} = 0, \quad \cdots, \quad z_{19}^2 + z_{38} = 0.$$

Note that $z_{19} = ... = z_{35} = 0$ and $z_{38} = 0$. Some of these equations force some relations between the coefficients x_j, as:

$$\begin{aligned}
x_6 &= (1 + x_{10}^3 x_{12}^3)/x_{12}^5 \\
x_{11} &= 0 \\
x_9 &= (x_{11}^3 + 1)/x_{12}^2 \\
x_7 &= (x_{10}^2 x_{11} + x_9 x_{11}^2)/x_{12}^2 = 0 \\
x_5 &= (x_9 x_{10}^2 + x_9^2 x_{11} + x_7 x_{11}^2)/x_{12}^2 \\
x_3 &= (x_9^3 + x_7 x_{10}^2 + x_8^2 x_{11} + x_5 x_{11}^2)/x_{12}^2 \\
x_1 &= (x_8^2 x_9 + x_7 x_9^2 + x_5 x_{10}^2 + x_7^2 x_{11} + x_3 x_{11}^2)/x_{12}^2
\end{aligned}$$

Then from $f_{17} = 0$, one can express x_4 in terms of x_8, x_{10}, x_{12}. Moreover,

- If $x_{10} \neq 0$, the equation $f_{11} = 0$ implies that one can express x_2 in terms of x_8, x_{10}, x_{12}. Thus this leaves us with 4 free variables x_0, x_8, x_{10} and $x_{12} \in k$ (and 6 equations $f_1, f_3, f_5, f_7, f_9, f_{13} = 0$, together with the condition $\mathrm{tr}_{k/\mathbb{F}_2}(x_0^3) = 0$).
- If $x_{10} = 0$, then the equation $f_9 = 0$ gives a relation between x_0, x_2, x_8, x_{12}.

Let $\sigma : K \to K$ be the field automorphism of $K = K(t)$ such that $\sigma(t) = t$ and $\sigma(a) = a^2$ for all $a \in k$. Let g be a generator of $k^\times$. Recall that $k = \mathbb{F}_{q^2}$ where $q = 2^n$ and $n = 5$.

Using the isometry $(x(t), y(t)) \mapsto (x(at), y(at))$ where $a^{q+1} = 1$, we may assume that $a = g^e$ with $0 \leqslant e < q - 1$. Using the isometry $(x, y) \mapsto (\sigma(x), \sigma(y))$, we may assume that e ranges over the set $\{0, 1, 3, 5, 7, 11, 15\}$ of 7 representatives of the action of the powers of 2 on $\mathbb{Z}/(q-1)\mathbb{Z} = \mathbb{Z}/31\mathbb{Z}$.

The procedure is then as follows: for each $e_{12} \in \{0, 1, 3, 5, 7, 11, 15\}$, we set $x_{12} = g^{e_{12}}$ and then we loop over $x_{10} \in k$ to solve a system of polynomial equations in $x_0, x_8 \in k$ (if $x_{10} = 0$, we also have the variables x_0, x_2) and one checks that the condition $\mathrm{tr}_{k/\mathbb{F}_2}(x_0^3) = 0$ is indeed satisfied.

In total, using SAGE [The21], this gives us 85155840 minimal points $(x, y) \in E(K)^0$ with $x_{10} \neq 0$, 4249080 minimal vectors with $x_{10} = 0 \neq x_8$, and $4356 \cdot 2 = 8712$ minimal vectors with $x_{10} = x_8 = 0$.

All in all, we conclude that the kissing number of MW_{64} equals

$$8712 + 4249080 + 85155840 = 89413632,$$

which is indeed the result stated in [Elk94, p. 360]. ⌟

Remark 3.3.6. The kissing number of some narrow Mordell–Weil lattices of the curves $y^2 = x^3 + 1 + t^{q+1}$ (studied in [Shi91]) has been determined in [Neb98, p. 494 (after corollary 4.7)], using techniques from group theory. For instance when $q = p = 23 \equiv -1 \pmod 6$, the corresponding 44-dimensional lattice has kissing number 2708112, which seems to still be the best known *lattice* kissing number (for non-lattice the best known is 2948552). ⌟

3.3.2 Gram matrices

In what follows, we will also describe a probabilistic algorithm to compute the Gram matrix of *certain* Mordell–Weil lattices. The computations rely on the specific shape of the Weierstrass equation, namely, there is a "linear part" like $y^2 + y$ in characteristic 2 and $x^3 + bx$ in characteristic 3 (in order to use lemma 3.3.2).

In general, computing the Gram matrix of a Mordell–Weil lattice (in a deterministic way) seems to be a difficult task. In particular, it would allow to determine the regulator of the elliptic curve, which is (by BSD formula from conjecture 1.3.34) very closely related to determining the order of the Tate–Shafarevich group Ш of the curve.

3.3.2.1 General strategy

We give here an overview of the probabilistic algorithm. We consider a lattice $L \hookrightarrow L \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^n$, which we see as a free abelian group of rank n together with an inner product $\langle -, - \rangle : L \times L \to \mathbb{R}$ (in the case of narrow Mordell–Weil lattices, this inner product is integer-valued).

1. The first step is to find n lattice points $P_1, ..., P_n \in L$ that are linearly independent over $\mathbb{R}$. In particular, they generate a full-rank sub-lattice $L_0 \subseteq L$.

Note that in the case of an integral lattice L, the equality $\mathrm{covol}(L_0) = [L : L_0]\,\mathrm{covol}(L)$ implies $\mathrm{disc}(L)$ divides $\mathrm{disc}(L_0) = [L : L_0]^2\,\mathrm{disc}(L)$.

2. The idea is that if we can produce random points Q in $L \cap B$ for some origin-centered ball B, then the probability that $Q \in L_0$ should behave like $\frac{1}{[L:L_0]}$ (this can be made precise by letting the radius of the ball go to infinity). Therefore, if $L_0 \neq L$, then the probability that among r random points $Q \in L \cap B$ at least one of them does not lie in L_0 is $1 - [L : L_0]^{-r} \geqslant 1 - 2^{-r}$. For large enough r, this is means that with very high probability we find a sublattice $L_1 \subset L$ with $\mathrm{covol}(L_1) \leqslant \mathrm{covol}(L_0)/2$ (see subsection 3.3.2.3 for more details).

   Detecting whether a point Q belongs to L_0 is easy: it suffices to express Q as a (unique) $\mathbb{R}$-linear combination of $P_1, ..., P_n$ and check whether all the coefficients are integers.

   We keep producing random points to get sublattices $L_j \subset L$ with $\mathrm{covol}(L_j) \leqslant \mathrm{covol}(L_{j-1})/2$. This process has to stop since we have the lower bound $\mathrm{covol}(L_j) \geqslant \mathrm{covol}(L)$ for any j. Eventually we get with very high probability a sublattice $L_{j_0} \subset L$ with an explicit $\mathbb{Z}$-basis, and having the same covolume as L, which means that $L_{j_0} = L$. Then we can compute a Gram matrix of L by using the basis of L_{j_0}.

3.3.2.2 Finding linearly independent points

One idea is to take random lattice points $P_1, P_2, ... \in L \cap B$ and successively compute the Gram matrix of $B_{0,d} := \{ P_i \ : \ 1 \leqslant i \leqslant d \}$ for $d \in \{1, 2, 3, ...\}$. The rank of the Gram matrix of d vectors in $\mathbb{R}^n$ equals the dimension of the space spanned by these vectors.

Assume that the Gram matrix of $B_{0,d-1}$ has non-zero determinant for some $d \geqslant 2$ (this is the case for $d = 2$). This means that $P_1, ..., P_{d-1}$ are linearly independent over $\mathbb{R}$ (hence over $\mathbb{Z}$), see [Sil08b, Lemma III.11.5]. Then we pick another point $P_d \in L \cap B$ and if the Gram matrix of $B_{0,d} := B_{0,d-1} \cup \{P_d\}$ has zero determinant, then we discard P_d and pick a new point P'_d. We repeat the process until the Gram matrix of $B_{0,d}$ has non-zero determinant. We continue like this until $d = n = \mathrm{rk}(L)$. This will give us a $\mathbb{Z}$-basis $B_0 := B_{0,n}$ of a certain sublattice $L_0 \subset L$ of finite index.

Remark 3.3.7. It may happen that we can obtain linearly independent lattice points of *minimal length* (i.e., lying in $L \cap S$ where S is the sphere of radius $\lambda_1(L)$, instead of $L \cap B$ for some origin-centered ball B).

There are several related notions for a lattice $L \subset \mathbb{R}^n$:

1. The minimal vectors of L span $\mathbb{R}^n$ as $\mathbb{R}$-vector space, i.e., L is *well-rounded*.
2. The minimal vectors of L span L as a $\mathbb{Z}$-module.
3. An *arbitrary* set of n minimal vectors of L which are $\mathbb{R}$-linearly independent span L.
4. There is a $\mathbb{Z}$-basis of L consisting of minimal vectors of L.

Here are some relations between these various properties.

- We always have 4) $\implies$ 2) $\implies$ 1). In dimension $\leqslant 4$, we have 1) $\implies$ 2), i.e., a well-rounded lattice is generated (as an abelian group) by its minimal vectors. In fact,

we even have 1) $\implies$ 3) in dimension $\leqslant 4$, except if L is homothetic[16] to D_4, see [Mar01, théorème 1.7, proposition 4.1] and [Mar02, §9.2, p. 329].

- The implication 1) $\implies$ 2) is wrong in dimensions $\geqslant 5$. For instance, $D_5^\vee$ is spanned by $e_1, ..., e_4, b_5 := \frac{1}{2}(e_1 + ... + e_5)$, where $e_i \in \mathbb{R}^5$ is the i-th vector of the canonical basis, and has kissing number 10 with minimal norm 1 with minimal vectors being $\{\pm e_i\}$ (see [CS98, p. 120]). Thus $D_5^\vee$ is well-rounded, but the minimal vectors do not span $D_5^\vee$ as an abelian group. This argument fails for $D_4^\vee$, since in that case $b_4 := \frac{1}{2}(e_1 + ... + e_4)$ has norm 1 and is among the minimal vectors!
- The implication 2) $\implies$ 4) holds in dimensions $n \leqslant 9$, but not in dimension $\geqslant 10$ (see [MS12, CS95]. ⌟

3.3.2.3 Reducing the covolume

Let $L \hookrightarrow \mathbb{R}^n$ be a lattice and assume that we are given points $P_1, ..., P_n \in L$ which are $\mathbb{R}$-linearly independent (as explained in the above step). Let $L_0 \subset L$ be the sublattice generated by the P_i's.

Given $Q \in L$, let us write $Q = \sum_{i=1}^n \alpha_i P_i$ for some $\alpha_i \in \mathbb{R}$. By substracting some integer multiple of P_i if necessary, we get a (unique) point $Q' = \sum_{i=1}^n \alpha_i' P_i$ where $-1/2 < \alpha_i' \leqslant 1/2$ for all i. Note that $Q' \equiv Q \mod L_0$. If $Q' \notin L_0$ then there is some index r such that $\alpha_r' \neq 0$; we choose such an index r. We define

$$P_i' := \begin{cases} Q' & \text{if } i = r \\ P_i & \text{if } i \neq r. \end{cases}$$

In other words, we replace P_r by Q'. We claim that $\{ P_i' \ : \ 1 \leqslant i \leqslant n \} \subset L$ are linearly independent vectors that span a sublattice $L_1 \subset L$ with $\operatorname{covol}(L_1) \leqslant \operatorname{covol}(L_0)/2$. We prove both claims at once. Without loss of generality, we may assume that $r = 1$. By embedding L into $\mathbb{R}^n$, we may consider the matrix whose columns are given by the P_i', so that

$$\begin{aligned} \operatorname{covol}(L_1) &= |\det(P_1' \ , \ P_2', \cdots, P_n')| \\ &= \left| \det(\sum_{i=1}^n \alpha_i P_i \ , \ P_2', \cdots, P_n') \right| \\ &= \left| \sum_{i=1}^n \alpha_i \det(P_i \ , \ P_2, \cdots, P_n) \right| \\ &= |\alpha_1 \det(P_1 \ , \ P_2, \cdots, P_n)| \\ &= |\alpha_1| \operatorname{covol}(L_0) \leqslant \frac{1}{2} \operatorname{covol}(L_0) \end{aligned}$$

In particular, we note that $\operatorname{covol}(L_1) > 0$ which means that the points P_i' are linearly independent.

[16] The root lattice D_4 can be generated by $a_1 = (1, 1, 0, 0)$, $a_2 = (1, -1, 0, 0)$, $a_3 = (0, 0, 1, -1)$ and $a_4 = (0, 1, -1, 0)$. The sublattice L generated by a_1, a_2, a_3 and $(0, 0, 1, 1)$ has index 2 in D_4 and is generated by minimal vectors of D_4.

Remark 3.3.8. For instance if $r = 1$, then we get two new lattices

$$\tilde{L}_1 = \mathbb{Z}Q \oplus \mathbb{Z}P_2 \oplus \cdots \oplus \mathbb{Z}P_n, \quad L_1 = \mathbb{Z}Q' \oplus \mathbb{Z}P_2 \oplus \cdots \oplus \mathbb{Z}P_n.$$

It is not necessarily true that they contain $L_0 = \mathbb{Z}P_1 \oplus \mathbb{Z}P_2 \cdots \oplus \mathbb{Z}P_n$, unless $\alpha_1 = \pm 1 \in \mathbb{Z}^\times$. Also, $\tilde{L}_1$ does not contain or is not contained in L_1 in general, because $Q = \sum_{i=1}^n \alpha_i P_i$ is a sum that involves P_1 (since $\alpha_1 \neq 0$ by our assumption that $r = 1$). Anyway if all P_i and Q are minimal vectors, it follows that $\tilde{L}_1$ and L_1 are generated by minimal vectors, but L_1 does not necessarily have a basis of minimal vectors (at least Q' might not be a minimal vector). ⌟

In practice, we do not compute explicitly the points Q' but rather work with matrices. The issue is that it can happen that Q' has very large norm, which is not convenient to work with. First, the following easy fact tells us how to compute the coefficients α_i of a point $Q \in L$ in terms of a given basis of a sublattice $L' \subset L$.

Lemma 3.3.9. *Let $v_1, ..., v_n \in \mathbb{R}^n$ be a basis and let $G = (\langle v_i, v_j \rangle)_{i,j}$ be the corresponding Gram matrix. Let $w \in \mathbb{R}^n$. Then*

$$w = \sum_{j=1}^n \alpha_j v_j, \quad \vec{\alpha} := G^{-1} \cdot (\langle w, v_i \rangle)_{i=1}^n. \qquad ⌟$$

Proof. — Since the v_i form a basis of $\mathbb{R}^n$, there are unique coefficients α_j such that $w = \sum_{j=1}^n \alpha_j v_j$. We have $\langle w, v_i \rangle = \sum_j \alpha_j \langle v_j, v_i \rangle = \sum_j G_{ij}\alpha_j = (G\vec{\alpha})_i$. Inverting G yields the conclusion. ■

Now the procedure to compute a Gram matrix of L is as follows. By subsection 3.3.2.2, we consider a basis $B_0 = \{ P_i \ : \ 1 \leqslant i \leqslant n \}$ of a sublattice $L_0 \subset L$ with Gram matrix G_0. We start by initializing a matrix A to the identity matrix: $A := I_{n \times n}$. Using lemma 3.3.9, we can compute the coefficients of a random point $Q \in L$ with respect to this $\mathbb{R}$-basis B_0.

If all the coefficients are integers, then $Q \in L_0$ so we discard the point. Otherwise we consider $Q' := Q \mod L_0 = \sum_{i=1}^n \alpha'_i P_i$, with coefficients α'_i between $-1/2$ and $1/2$, and one of these coefficients, say α'_r, is non-zero.

Then we want to replace P_r by Q' as explained before, to get a basis B_1 of a new sublattice L_1, which has a certain matrix A_1 with respect to the basis B_0: it is the identity matrix except that on the r-th row we write the $\mathbb{R}$-coefficients α'_i of Q' with respect to B_0. We set $A \leftarrow A_1 \cdot A = A_1 \cdot I_{n \times n} = A_1$. The Gram matrix gets updated as $G_1 = A_1 G_0 \, {}^t A_1$.

Continuing like this, we pick a random point $Q_2 \in L$ and we get a matrix A_2, a sublattice $L_2 \subset L$ and update $A \leftarrow A_2 \cdot A$. Eventually, we get a sublattice $L_{j_0} \subset L$ such that random points $Q \in L$ lie in L_{j_0} with very high probability, which means that we should have $L_{j_0} = L$. The final matrix $A \in \mathrm{GL}_n(\mathbb{R})$ gives the new basis with respect to B_0 and the final Gram matrix is $G = A G_0 \, {}^t A$ (which is *provably* a Gram matrix for L_{j_0}). In fact, if we know the covolume of L, we can check whether $\mathrm{covol}(L_{j_0}) = \det(G)^{1/2} = \mathrm{covol}(L)$, and in this case we *provably* have $L_{j_0} = L$.

Finally, we can apply the LLL algorithm (on the level of the Gram matrix directly) to get a "nicer" basis (with smaller coefficients).

3.3.2.4 Results

We used the method described above to compute a Gram matrix attached to sublattices of the 54-dimensional narrow Mordell–Weil lattice $L'_{3,1}$ introduced in theorem 3.2.7. Using SAGE [The21], we obtain the following result; the code is available at https://gitlab.com/gauthierleterrier/maths.

Computational proposition 3.3.10. *The narrow Mordell–Weil lattice $L'_{3,1}$ of $E : y^2 = x^3 + x + t^{28}$ over $K := \mathbb{F}_{3^6}(t)$ is* well-rounded, *i.e., there is a set of minimal vectors that spans the euclidean space $L \otimes_{\mathbb{Z}} \mathbb{R}$.*

Moreover, if[17] $|Ш(E/K)| = 1$ *then $L'_{3,1}$ is generated over $\mathbb{Z}$ by its minimal vectors and a Gram matrix G is given by:*

$$\begin{pmatrix}
10 & 5 & 4 & 1 & 0 & 1 & -3 & 4 & -2 & -4 & -3 & 3 & -3 & 5 & 3 & 4 & -1 & 3 & -4 & 3 & 1 & 1 & -3 & -2 & 0 & -3 & -5 & 3 & 4 & -5 & 4 & -3 & 5 & -1 & -2 & 3 & -3 & -2 & -5 & 4 & -3 & 4 & 4 & -1 & -2 & 2 & 2 & -1 & 1 & -3 & -3 & -1 & 1 & -4 \\
5 & 10 & -1 & -1 & 1 & -2 & 2 & 5 & -3 & -3 & 1 & 0 & -4 & 2 & 5 & 5 & 3 & -1 & 0 & -2 & -3 & 3 & -3 & 1 & 2 & -3 & 1 & 5 & 0 & -5 & -1 & 1 & 2 & -1 & -4 & 1 & -4 & -4 & -4 & -1 & -2 & -1 & 2 & 1 & -3 & 2 & -1 & -4 & -3 & -1 & -5 & -4 & -1 & 1 \\
4 & -1 & 10 & 1 & -2 & 5 & -3 & -2 & 3 & -2 & -5 & -1 & -1 & 1 & 3 & 0 & 1 & 3 & -1 & 5 & 3 & -3 & -1 & -2 & -4 & 3 & -3 & 3 & 2 & -1 & 6 & 1 & 3 & -3 & -1 & 4 & -3 & 0 & -1 & 2 & -4 & 6 & 2 & -1 & -2 & 2 & 3 & 2 & 1 & -2 & 1 & 4 & -2 & -6 \\
1 & -1 & 1 & 10 & -5 & 1 & -1 & 2 & -2 & -3 & -2 & -1 & -1 & 3 & -4 & -1 & -4 & 4 & 2 & -1 & 4 & 2 & -4 & -3 & -4 & 2 & -4 & 0 & 2 & 4 & -1 & 2 & 3 & 4 & -4 & 1 & 4 & 3 & 3 & 0 & -4 & -1 & -3 & 0 & 1 & -2 & -4 & 4 & 0 & 3 & 3 & 1 & -4 & -4 \\
0 & 1 & -2 & -5 & 10 & -1 & 1 & -1 & 0 & 0 & -1 & 3 & 3 & -3 & 3 & -2 & 1 & -3 & -1 & -3 & -3 & 1 & 3 & 2 & 2 & -1 & 1 & 1 & -4 & -1 & 1 & -2 & -3 & -4 & 2 & 0 & 0 & -1 & -2 & 3 & 0 & 1 & 0 & -2 & -3 & 1 & -1 & -1 & -3 & -5 & -4 & -4 & 5 & 3 \\
1 & -2 & 5 & 1 & -1 & 10 & 2 & -1 & 5 & 1 & -1 & -4 & 0 & 2 & -3 & 1 & -1 & 3 & 2 & 2 & 5 & -5 & -3 & 1 & 0 & 3 & 1 & -1 & 4 & 1 & 3 & 1 & 1 & 1 & 2 & 5 & -4 & 2 & -1 & 3 & -1 & 4 & -1 & 1 & -2 & 2 & 3 & 3 & 2 & -2 & 1 & 6 & 2 & -6 \\
-3 & 2 & -3 & -1 & 1 & 2 & 10 & 0 & 0 & -1 & 3 & -2 & 2 & 0 & -1 & 1 & 1 & -3 & 4 & -4 & 1 & -3 & 1 & 1 & 4 & -1 & 7 & 1 & 2 & -1 & -3 & 1 & -4 & 2 & 2 & 2 & -3 & 1 & -1 & -4 & -1 & -1 & -3 & -1 & -3 & -2 & -3 & -2 & -2 & 0 & 1 & -1 & 2 & 3 \\
4 & 5 & -2 & 2 & -1 & -1 & 0 & 10 & -5 & -1 & 1 & 0 & -3 & 3 & 0 & 3 & -1 & 2 & -3 & -1 & -1 & 2 & -3 & -1 & 2 & -2 & 0 & 1 & 2 & -2 & -1 & 1 & 1 & 4 & -4 & -1 & 2 & -4 & -4 & 1 & -3 & -2 & 0 & 2 & 0 & 3 & 0 & 0 & 2 & -1 & 0 & -4 & 0 & 2 \\
-2 & -3 & 3 & -2 & 0 & 5 & 0 & -5 & 10 & 4 & 1 & -3 & -1 & -2 & -3 & 0 & -1 & 2 & 0 & 1 & 2 & -3 & 0 & 2 & -3 & 3 & 0 & -2 & 0 & 1 & 0 & 0 & 2 & -3 & 2 & 3 & -2 & 3 & -1 & 3 & 0 & 3 & -2 & 2 & 1 & -1 & 4 & 1 & -1 & -2 & 0 & 3 & -1 & -5 \\
-4 & -3 & -2 & -3 & 0 & 1 & -1 & -1 & 4 & 10 & 5 & -1 & -1 & -1 & -5 & -2 & -1 & 1 & -3 & -1 & -3 & -3 & 1 & 0 & -2 & -1 & 3 & -3 & -2 & 1 & -3 & 0 & 0 & 2 & 3 & 0 & 2 & -1 & -2 & 2 & 2 & 0 & -3 & 1 & 3 & 3 & 3 & -1 & 1 & 0 & 0 & 3 & 0 & -1 \\
-3 & 1 & -5 & -2 & -1 & -1 & 3 & 1 & 1 & 5 & 10 & 1 & 1 & -1 & -2 & -1 & -2 & -2 & 0 & -1 & -4 & -2 & 2 & 3 & 0 & -2 & 6 & -4 & -2 & -2 & -3 & 2 & 1 & 4 & 0 & -3 & 1 & -2 & -2 & 0 & 1 & -2 & -2 & 0 & 2 & 1 & 1 & -1 & 0 & 2 & 1 & 0 & -1 & 2 \\
3 & 0 & -1 & -1 & 3 & -4 & -2 & 0 & -3 & -1 & 1 & 10 & 4 & 2 & 3 & -3 & -3 & -3 & -5 & 2 & -3 & -1 & 3 & -3 & -2 & -5 & -3 & 1 & 0 & -3 & 1 & -3 & 1 & -1 & 1 & -3 & 2 & -3 & -3 & 4 & -1 & 3 & 2 & -5 & 1 & -1 & 1 & 0 & 1 & 0 & -2 & -2 & 0 & 0 \\
-3 & -4 & -1 & -1 & 3 & 0 & 2 & -3 & -1 & -1 & 1 & 4 & 10 & 0 & -1 & -3 & -1 & -3 & 0 & 0 & -1 & -3 & 3 & -1 & 0 & -1 & 3 & -1 & 0 & 1 & 0 & -1 & -3 & -1 & 2 & -1 & 1 & 1 & 0 & -1 & 0 & 0 & -1 & -3 & 2 & -1 & 0 & 3 & 0 & -1 & 3 & 0 & 1 & 2 \\
5 & 2 & 1 & 3 & -3 & 2 & 0 & 3 & -2 & -1 & -1 & 2 & 0 & 10 & -3 & 3 & -3 & 3 & -3 & 2 & 1 & -3 & -5 & -3 & 0 & -5 & -1 & 3 & 6 & -3 & -2 & -1 & 2 & 2 & 0 & 4 & -2 & -2 & -2 & 1 & 0 & 1 & 2 & -1 & -1 & 0 & 2 & 1 & 2 & 1 & -1 & 1 & 1 & -5 \\
3 & 5 & 3 & -4 & 3 & -3 & -1 & 0 & -3 & -5 & -2 & 3 & -1 & -3 & 14 & -1 & 6 & -6 & -1 & 3 & -2 & 2 & 4 & 3 & 2 & 0 & 0 & 4 & -4 & -4 & 5 & 0 & 0 & -4 & -2 & -2 & -2 & -3 & 0 & 1 & -1 & 3 & 4 & -1 & -2 & 1 & 1 & -1 & -1 & -1 & -5 & -3 & -2 & 3 \\
4 & 5 & 0 & -1 & -2 & 1 & 1 & 3 & 0 & -2 & -1 & -3 & -3 & 3 & -1 & 10 & 1 & 1 & 1 & 1 & 1 & 1 & -5 & 0 & 2 & -1 & -1 & 1 & 4 & -3 & 0 & 0 & 0 & -2 & 0 & 3 & -5 & -1 & -2 & -1 & 0 & -1 & 3 & 2 & -2 & 2 & 1 & -2 & 1 & -1 & -2 & -2 & 2 & 0 \\
-1 & 3 & 1 & -4 & 1 & -1 & 1 & -1 & -1 & -1 & -2 & -3 & -1 & -3 & 6 & 1 & 10 & -4 & 0 & -1 & -2 & 2 & 2 & 1 & 4 & 0 & 2 & 4 & -2 & 0 & 0 & 0 & -3 & -3 & 1 & 0 & -3 & -1 & 1 & -3 & 1 & 0 & 1 & 1 & -2 & 1 & 1 & -2 & -1 & -2 & -3 & 0 & -1 & 3 \\
3 & -1 & 3 & 4 & -3 & 3 & -3 & 2 & 2 & 1 & -2 & -3 & -3 & 3 & -6 & 1 & -4 & 10 & 0 & -1 & 2 & 0 & -4 & -3 & -2 & 2 & -2 & 0 & 4 & 0 & 1 & 0 & 4 & 1 & -3 & 4 & 1 & 2 & -2 & 0 & -1 & -1 & -1 & 3 & 0 & 1 & 1 & 0 & 0 & -1 & 3 & 3 & -1 & -5 \\
-4 & 0 & -1 & 2 & -1 & 2 & 4 & -3 & 0 & -3 & 0 & -5 & 0 & -3 & -1 & 1 & 0 & 0 & 12 & -2 & 3 & 1 & -1 & 3 & 1 & 5 & 2 & -1 & 0 & 3 & 1 & 5 & -2 & 0 & 0 & 1 & -3 & 3 & 6 & -6 & 3 & -3 & 0 & 1 & -1 & -1 & -5 & -1 & -2 & 3 & 2 & 3 & 1 & 1 \\
3 & -2 & 5 & -1 & -3 & 2 & -4 & -1 & 1 & -1 & -1 & 2 & 0 & 2 & 3 & 1 & -1 & -1 & -2 & 10 & 1 & -3 & 1 & 1 & -2 & 1 & -3 & -1 & 2 & -1 & 4 & 0 & 3 & 0 & 2 & 0 & -1 & -1 & 0 & 3 & 0 & 5 & 5 & -2 & 1 & 1 & 4 & 3 & 5 & 1 & 0 & 2 & 1 & -3 \\
1 & -3 & 3 & 4 & -3 & 5 & 1 & -1 & 2 & -3 & -4 & -3 & -1 & 1 & -2 & 2 & 3 & 1 & 10 & 0 & -2 & -1 & 0 & 2 & -4 & -2 & 4 & 2 & 2 & -2 & 1 & 2 & 1 & 3 & -2 & 4 & 3 & 0 & 0 & 2 & -1 & 2 & 1 & -2 & -1 & 3 & 2 & 1 & 3 & 4 & 1 & -3 \\
1 & 3 & -3 & 2 & 1 & -5 & -3 & 2 & -3 & -3 & -2 & -1 & -3 & -3 & 2 & 1 & 2 & 0 & 1 & -3 & 0 & 10 & 0 & 1 & 0 & 0 & -4 & 0 & -4 & 2 & -1 & -1 & 2 & 0 & -3 & -3 & 2 & 1 & 2 & -1 & 1 & -4 & 0 & 3 & 1 & -1 & -3 & 0 & -3 & 0 & -1 & -3 & -2 & 3 \\
-3 & -3 & -1 & -4 & 3 & -3 & 1 & -3 & 0 & 1 & 2 & 3 & 3 & -5 & 4 & -5 & 2 & -4 & -1 & 1 & -2 & 0 & 10 & 1 & 0 & 0 & 2 & -2 & -4 & 0 & 1 & -2 & -1 & -1 & 3 & -3 & 3 & 0 & 1 & -1 & 1 & 2 & -1 & -2 & 1 & -1 & 0 & 0 & 0 & -2 & 2 & -1 & 0 & 4 \\
-2 & 1 & -2 & -3 & 2 & 1 & 1 & -1 & 2 & 0 & 3 & -3 & -1 & -3 & 3 & 0 & 1 & -3 & 3 & 1 & -1 & 1 & 1 & 10 & 2 & 3 & 3 & -3 & -4 & 1 & 1 & 2 & 0 & 0 & -1 & -1 & -2 & 1 & 2 & 1 & 4 & -2 & 1 & 2 & -1 & 0 & 0 & 1 & -2 & 0 & -1 & -1 & 1 & 2 \\
0 & 2 & -4 & -4 & 2 & 0 & 4 & 2 & -3 & -2 & 0 & -2 & 0 & 0 & 2 & 2 & 4 & -2 & 1 & -2 & 0 & 0 & 0 & 2 & 12 & -2 & 4 & 0 & 2 & -2 & -1 & -2 & -5 & 1 & 3 & 0 & -3 & 1 & 0 & -3 & 4 & -2 & 2 & 2 & -2 & -1 & 1 & -4 & 1 & -1 & -3 & -1 & 6 & 5 \\
-3 & -3 & 3 & 2 & -1 & 3 & -1 & -2 & 3 & -1 & -2 & -5 & -1 & -5 & 0 & -1 & 0 & 2 & 5 & 1 & 2 & 0 & 0 & 3 & -2 & 10 & 0 & -2 & -2 & 4 & 3 & 3 & 0 & -1 & -2 & 0 & 1 & 4 & 4 & -1 & -2 & -1 & -1 & 1 & 0 & 0 & -2 & 2 & 0 & 0 & 3 & 1 & -1 & -1 \\
-5 & 1 & -3 & -4 & 1 & 1 & 7 & 0 & 0 & 3 & 6 & -3 & 3 & -1 & 0 & -1 & 2 & -2 & 2 & -3 & -4 & 2 & 3 & 4 & 0 & 14 & 0 & -2 & -2 & -2 & 3 & -4 & 2 & 0 & 0 & -1 & -1 & -2 & -4 & 1 & -3 & -3 & 1 & -3 & 1 & 1 & -2 & -2 & 0 & 1 & -1 & 1 & 4 \\
3 & 5 & 3 & 0 & 1 & -1 & 1 & 1 & -2 & -3 & -4 & 1 & -1 & 3 & 4 & 1 & 4 & 0 & -1 & -1 & -2 & 0 & -2 & -3 & 0 & -2 & 0 & 10 & 2 & -2 & -1 & 1 & -1 & -3 & -2 & 3 & -3 & -2 & -3 & -1 & -2 & 1 & 1 & -1 & -4 & 0 & -1 & -2 & -3 & -1 & -4 & -1 & -1 & -2 \\
4 & 0 & 2 & 2 & -4 & 4 & 2 & 2 & 0 & -2 & -2 & 0 & 0 & 6 & -4 & 4 & -2 & 4 & 0 & 2 & 4 & -4 & -4 & -4 & 2 & -2 & -2 & 2 & 12 & -2 & 1 & -2 & 1 & 2 & 1 & 4 & -3 & 2 & -4 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 1 & -1 & 4 & 0 & 2 & 3 & 2 & -3 \\
-5 & -5 & -1 & 4 & -1 & 1 & -1 & -2 & 1 & 1 & -2 & -3 & 1 & -3 & -4 & -3 & 0 & 0 & 3 & -1 & 2 & 2 & 0 & 1 & -2 & 4 & -2 & -2 & -2 & 10 & -1 & 1 & -1 & 1 & 1 & -1 & 4 & 5 & 4 & 0 & 1 & -1 & -4 & 1 & 1 & -2 & -2 & 4 & 0 & 1 & 2 & 2 & -2 & 0 \\
4 & -1 & 6 & -1 & 1 & 3 & -3 & -1 & 0 & -3 & -3 & 1 & 0 & -2 & 5 & 0 & 0 & 1 & 1 & 4 & 2 & -1 & 1 & 1 & -1 & 3 & -2 & -1 & 1 & -1 & 12 & 1 & 2 & -2 & -1 & 1 & -2 & 0 & -1 & 4 & 0 & 4 & 3 & -1 & -1 & 4 & 2 & 0 & 3 & -3 & 1 & 3 & 0 & 0 \\
-3 & 1 & 1 & 2 & -2 & 1 & 1 & 1 & 0 & 0 & 2 & -3 & -1 & -1 & 0 & 0 & 0 & 0 & 5 & 0 & -2 & -1 & -2 & 2 & -2 & 3 & 3 & 1 & -2 & 1 & 1 & 12 & -3 & 1 & -2 & 0 & 1 & -2 & -3 & -1 & -1 & -2 & -1 & 1 & -1 & 2 & 0 & 0 & 0 & 2 & 1 & 0 & -2 & -1 \\
5 & 2 & 3 & 3 & -3 & 1 & -4 & 1 & 2 & 0 & 1 & 1 & -3 & 2 & 0 & 0 & -3 & 4 & -2 & 3 & 1 & 2 & -1 & 0 & -5 & 0 & -4 & -1 & 1 & -1 & 2 & -3 & 12 & 1 & -4 & 0 & 0 & 1 & -3 & 2 & -2 & 3 & 1 & 1 & 2 & 1 & 1 & 1 & 0 & -1 & 1 & 3 & -4 & -4 \\
-1 & -1 & -3 & 4 & -4 & 1 & 2 & 4 & -3 & 2 & 4 & -1 & -1 & 2 & -4 & -2 & -3 & 1 & 0 & 0 & 2 & 0 & -1 & 0 & 1 & -1 & 2 & -3 & 2 & 1 & -2 & 1 & 1 & 12 & 0 & 0 & 3 & 1 & 0 & -1 & 0 & -2 & 0 & 3 & 0 & -2 & 1 & 2 & 4 & 4 & 2 & 0 & 1 \\
-2 & -4 & -1 & -4 & 2 & 2 & 2 & -4 & 2 & 3 & 0 & 1 & 2 & 0 & -2 & 0 & 1 & -3 & 0 & 2 & 1 & -3 & 3 & -1 & 3 & -2 & 0 & -2 & 1 & 1 & -1 & -2 & -4 & 0 & 12 & 1 & -2 & 1 & 2 & 0 & 2 & 3 & 0 & -2 & 0 & -2 & 3 & 0 & 3 & -1 & -1 & 2 & 6 & -1 \\
3 & 1 & 4 & 1 & 0 & 5 & 2 & -1 & 3 & 0 & -3 & -3 & -1 & 4 & -2 & 3 & 0 & 4 & 1 & 0 & 3 & -3 & -3 & -1 & 0 & 0 & 0 & 3 & 4 & -1 & 1 & 0 & 0 & 0 & 1 & 12 & -4 & 2 & -2 & 0 & -2 & 3 & -1 & 0 & -4 & 1 & 0 & 0 & -2 & -2 & -1 & 2 & 1 & -5 \\
-3 & -4 & -3 & 4 & 0 & -4 & -3 & 2 & -2 & 2 & 1 & 2 & 1 & -2 & -2 & -5 & -3 & 1 & -3 & -1 & -2 & 2 & 3 & -2 & -3 & 1 & -1 & -3 & -3 & 4 & -2 & 1 & 0 & 3 & -2 & -4 & 14 & 2 & 2 & 3 & -3 & 0 & -4 & -1 & 3 & -1 & -1 & 4 & 1 & 1 & 1 & -4 & -3 & 2 \\
-2 & -4 & 0 & 3 & -1 & 2 & 1 & -4 & 3 & -1 & -2 & -3 & 1 & -2 & -3 & 1 & -4 & 1 & 0 & 1 & 1 & 4 & -1 & -2 & 2 & 5 & 0 & -2 & 1 & 1 & 1 & 2 & 2 & 12 & 1 & -1 & 0 & 0 & -2 & 1 & 0 & -4 & -1 & 1 & -1 & -1 & 2 & 2 & 0 & -1 \\
-5 & -4 & -1 & 3 & -2 & -1 & -1 & -4 & -1 & -2 & -2 & -3 & 0 & -2 & 0 & -2 & 1 & -2 & 6 & 0 & 3 & 2 & 1 & 2 & 0 & 4 & -2 & -3 & -4 & 4 & -1 & 3 & -3 & 0 & 2 & -2 & 2 & 1 & 14 & -4 & 3 & -2 & 1 & 0 & 3 & -3 & -3 & 3 & 0 & 5 & 2 & 1 & 0 & 1 \\
4 & -1 & 2 & 0 & 3 & 3 & -4 & 1 & 3 & 2 & 0 & 4 & -1 & 1 & 1 & -1 & -3 & 0 & -6 & 3 & 0 & -1 & -1 & 1 & -3 & -1 & -4 & -1 & 0 & 0 & 4 & -1 & 2 & -1 & 0 & 0 & 3 & -1 & -4 & 14 & -2 & 5 & 0 & -1 & 1 & 3 & 4 & 4 & 2 & -3 & -5 & 0 & 0 & -4 \\
-3 & -2 & -4 & -4 & 0 & -1 & -1 & -3 & 0 & 2 & 1 & -1 & 0 & 0 & -1 & 0 & 1 & -1 & 3 & 0 & 0 & 1 & 1 & 4 & 4 & -2 & 1 & -2 & 0 & 1 & 0 & -1 & -2 & 0 & 2 & -2 & -3 & 0 & 3 & -2 & 14 & -3 & 3 & 3 & 3 & 0 & 1 & -3 & 1 & 2 & -1 & 5 & 2 & 3 \\
4 & -1 & 6 & -1 & 1 & 4 & -1 & -2 & 3 & 0 & -2 & 3 & 0 & 1 & 3 & -1 & 0 & -1 & -3 & 5 & 2 & -4 & 2 & -2 & -2 & -1 & -3 & 1 & 1 & -1 & 4 & -2 & 3 & -2 & 3 & 3 & 0 & 0 & -2 & 5 & -3 & 12 & 2 & -4 & 0 & 1 & 4 & 1 & 2 & -3 & -3 & 3 & 0 & -5 \\
4 & 2 & 2 & -3 & 0 & -1 & -3 & 0 & -2 & -3 & -2 & 2 & -1 & 2 & 4 & 3 & 1 & -1 & 0 & 5 & -1 & 0 & -1 & 1 & 2 & -1 & -3 & 1 & 2 & -4 & 3 & -1 & 1 & -2 & 0 & -1 & -4 & -2 & 1 & 0 & 3 & 2 & 10 & -2 & 2 & 1 & 2 & -2 & 2 & 1 & -2 & 1 & 3 & 1 \\
-1 & 1 & -1 & 0 & -2 & 1 & -1 & 2 & 2 & 1 & 0 & -5 & -3 & -1 & -1 & 2 & 1 & 3 & 1 & -2 & 2 & 3 & -2 & 2 & 2 & 1 & 1 & -1 & 0 & 1 & 1 & 1 & 0 & -2 & 0 & -1 & 1 & 0 & -1 & 3 & -4 & -2 & 10 & 0 & 1 & 2 & 0 & -1 & 0 & 1 & 0 & -2 & 0 \\
-2 & -3 & -2 & 1 & -3 & -2 & -3 & 0 & 1 & 3 & 2 & 1 & -2 & -1 & -2 & -2 & -2 & 0 & -1 & 1 & 1 & 1 & -1 & -2 & 0 & -3 & -4 & 0 & 1 & -1 & -1 & 2 & 3 & 0 & -4 & 3 & 0 & 3 & 1 & 3 & 0 & 2 & 0 & 10 & -1 & 1 & 0 & 3 & 3 & 2 & 2 & -2 & 1 \\
2 & 2 & 2 & -2 & 1 & 2 & -2 & 3 & -1 & 3 & 1 & -1 & -1 & 0 & 1 & 2 & 1 & 1 & -1 & 1 & -2 & -1 & -1 & 0 & -1 & 0 & 1 & 0 & 0 & -2 & 4 & 2 & 1 & 0 & -2 & 1 & -1 & -4 & -3 & 3 & 0 & 1 & 1 & 1 & -1 & 10 & 1 & -2 & 2 & -3 & -1 & 2 & 0 & 1 \\
2 & -1 & 3 & -4 & -1 & 3 & -3 & 0 & 4 & 3 & 1 & 1 & 0 & 2 & 1 & 1 & 1 & -1 & 1 & -2 & -1 & 1 & -2 & 2 & 0 & 1 & -2 & 3 & 0 & -1 & -1 & -3 & 4 & 1 & 4 & 2 & 2 & 1 & 1 & 12 & 1 & 3 & -2 & -2 & 2 & -1 & -4 \\
-1 & -4 & 2 & 4 & -1 & 3 & -2 & 0 & 1 & -1 & -1 & 0 & 3 & 1 & -1 & -2 & -2 & 0 & -1 & 3 & 3 & 0 & 0 & 1 & -4 & 2 & -2 & -2 & -1 & 4 & 0 & 0 & 1 & 1 & 0 & 0 & 4 & 1 & 3 & 4 & -3 & 1 & -2 & 0 & 0 & -2 & 1 & 12 & 1 & 1 & 2 & 0 & -1 & -3 \\
1 & -3 & 1 & 0 & -3 & 2 & -2 & 2 & -1 & 1 & 0 & 1 & 0 & 2 & -1 & 1 & -1 & 0 & -2 & 5 & 2 & -3 & 0 & -2 & 1 & 0 & -2 & -3 & 4 & 0 & 3 & 0 & 0 & 0 & 2 & 3 & -2 & 1 & -1 & 0 & 2 & 1 & 2 & 2 & -1 & 3 & 2 & 3 & 1 & 10 & 0 & 2 & 2 & 2 & 0 \\
-3 & -1 & -2 & 3 & -5 & -2 & 0 & -1 & -2 & 0 & 2 & 0 & -1 & 1 & -1 & -2 & -1 & 3 & 1 & 1 & 0 & -2 & 0 & -1 & 0 & 0 & -1 & 0 & 1 & -3 & 2 & -1 & 4 & -1 & -2 & 1 & -1 & 5 & -3 & 2 & -3 & 1 & 0 & 3 & -3 & -2 & 1 & 0 & 10 & 1 & 1 & -2 & 0 \\
-3 & -5 & 1 & 3 & -4 & 1 & 1 & 0 & 0 & 0 & 1 & -2 & 3 & -1 & -5 & -2 & -3 & 3 & 2 & 0 & 3 & -1 & 2 & -1 & 3 & 1 & -4 & 2 & 2 & 1 & 1 & 1 & 4 & -1 & -1 & 1 & 2 & 2 & -5 & -1 & -3 & -2 & 1 & 2 & -1 & -2 & 2 & 2 & 1 & 12 & 2 & -2 & 1 \\
-1 & -4 & 4 & 1 & -4 & 6 & -1 & -4 & 3 & 3 & 0 & -2 & 0 & 1 & -3 & -2 & 0 & 3 & 3 & 2 & 4 & -3 & -1 & -1 & 1 & -1 & -1 & 3 & 2 & 3 & 0 & 3 & 2 & 2 & 2 & -4 & 2 & 1 & 0 & 5 & 3 & 1 & 0 & 2 & 2 & 2 & 0 & 2 & 1 & 2 & 14 & -1 & -4 \\
1 & -1 & -2 & -4 & 5 & 2 & 2 & 0 & -1 & 0 & -1 & 0 & 1 & 1 & -2 & 2 & -1 & -1 & 1 & 1 & -2 & 0 & 1 & 6 & -1 & 1 & -1 & 2 & -2 & 0 & -2 & -4 & 0 & 6 & 1 & -3 & 0 & 0 & 0 & 2 & 0 & 3 & -2 & -2 & 0 & -1 & -1 & 2 & -2 & -2 & -1 & 14 & 1 \\
-4 & 1 & -6 & -4 & 3 & -6 & 3 & 2 & -5 & -1 & 2 & 0 & 2 & -5 & 3 & 0 & 3 & -5 & 1 & -3 & -3 & 3 & 4 & 2 & 5 & -1 & 4 & -2 & -3 & 0 & 0 & -1 & -4 & 1 & -1 & -5 & 2 & -1 & 1 & -4 & 3 & -5 & 1 & 0 & 1 & 1 & -4 & -3 & 0 & 0 & 1 & -4 & 1 & 14
\end{pmatrix}$$

Proof. — 1. We first have to produce 54 $\mathbb{R}$-linearly independent minimal vectors in $L'_{3,1}$, that is, rational points $(x, y) \in E(K)$ with $x, y \in \mathbb{F}_{3^6}[t]$ and $\deg(x) = 10$.

[17] We will actually prove in theorem 3.4.1 that the Tate–Shafarevich group of E/K is indeed trivial. Here we prefer to state this as an assumption to emphasize how it is used in the proof.

Given two elements $y_{15} \in k^\times, y_{12} \in k$, we may use identities (3.3.6), equation (3.3.10) to solve a system of polynomial equations in $y_6, y_9 \in k$ and for each solution y_6, y_9 we can deduce coefficients $y_0, ..., y_{14} \in k$. Moreover, we check that $y_0^2 = s_0^3 + s_0$ for some $s_0 \in \mathbb{F}_{3^6}$. Then we set $y(t) := \sum_{j=0}^{15} y_j t^j \in k[t]$ and there are exactly 3 polynomials $x(t)$ such that $(x, y) \in E(K)$; we choose one of them.

In this way, we can produce ("random") points in $E(K)$ with Néron–Tate height 10. Following subsection 3.3.2.2, we compute successive Gram matrices, until we get a 54-dimensional invertible matrix. Notice that the Néron–Tate height coincides with the naive height by corollary 3.2.18, so one can easily compute the Gram matrices.

More specifically, the following 54 minimal vectors are linearly independent over $\mathbb{R}$, given by their x-coordinates as follows[18]. We write $\mathbb{F}_{3^6} = \mathbb{F}_3[X]/(X^6 - X^4 + X^2 - X - 1)$ so that the class g of X is a generator of $\mathbb{F}_{3^6}^\times$. Then for each $i \in \{0, ..., 53\}$, we give a list of 11 elements e_j which are either the discrete logarithm of the j-th coefficient of $x(t) \in \mathbb{F}_{3^6}[t]$ in base g (i.e., $x_j = g^{e_j}$), or e_j is the empty string ", in which case we set $x_j := 0$. For instance, when $i = 0$, we get the point with x-coordinate $x(t) = t^2 + t^8 + t^{10}$.

0	[", ", 0, ", ", ", ", ", ", 0, ", 0]
1	[182, ", 0, ", ", ", ", ", ", 0, ", 0]
2	[", ", 390, ", ", ", ", ", ", 468, ", 494]
3	[182, ", 390, ", ", ", ", ", ", 468, ", 494]
4	[32, 420, 532, 56, 0, 56, 448, 448, 588, ", 252]
5	[140, 420, 532, 56, 0, 56, 448, 448, 588, ", 252]
6	[", ", 52, ", ", ", ", ", ", 208, ", 260]
7	[182, ", 52, ", ", ", ", ", ", 208, ", 260]
8	[", ", 442, ", ", ", ", ", ", 676, ", 26]
9	[182, ", 442, ", ", ", ", ", ", 676, ", 26]
10	[420, 532, 140, 168, 0, 168, 616, 616, 308, ", 28]
11	[96, 532, 140, 168, 0, 168, 616, 616, 308, ", 28]
12	[", ", 104, ", ", ", ", ", ", 416, ", 520]
13	[182, ", 104, ", ", ", ", ", ", 416, ", 520]
14	[", ", 494, ", ", ", ", ", ", 156, ", 286]
15	[182, ", 494, ", ", ", ", ", ", 156, ", 286]
16	[", ", 364, 91, 364, 182, 0, 0, 546, 637, 0]
17	[182, ", 364, 91, 364, 182, 0, 0, 546, 637, 0]
18	[", ", 364, 364, 455, 546, 91, 91, 182, 182, 0]
19	[182, ", 364, 364, 455, 546, 91, 91, 182, 182, 0]
20	[", ", 364, 273, 364, 546, 0, 0, 182, 455, 0]
21	[182, ", 364, 273, 364, 546, 0, 0, 182, 455, 0]
22	[0, 273, 273, 182, 455, 455, 455, 455, 364, 273, 0]
23	[637, 273, 273, 182, 455, 455, 455, 455, 364, 273, 0]
24	[", ", 364, 364, 637, 182, 273, 273, 546, 546, 0]
25	[182, ", 364, 364, 637, 182, 273, 273, 546, 546, 0]
26	[0, 91, 91, 546, 637, 637, 637, 637, 364, 91, 0]
27	[637, 91, 91, 546, 637, 637, 637, 637, 364, 91, 0]
28	[285, 665, 44, 486, 438, 648, 530, 530, 120, 384, 486]
29	[180, 665, 44, 486, 438, 648, 530, 530, 120, 384, 486]
30	[650, 338, 189, 719, 4, 564, 90, 90, 581, 387, 486]
31	[332, 338, 189, 719, 4, 564, 90, 90, 581, 387, 486]
32	[497, 63, 243, 138, 547, 356, 202, 202, 125, 649, 486]
33	[369, 63, 243, 138, 547, 356, 202, 202, 125, 649, 486]
34	[210, 282, 410, 318, 191, 672, 127, 127, 176, 164, 486]
35	[434, 282, 410, 318, 191, 672, 127, 127, 176, 164, 486]
36	[520, 253, 377, 13, 122, 225, 245, 245, 255, 663, 486]
37	[85, 253, 377, 13, 122, 225, 245, 245, 255, 663, 486]
38	[695, 229, 235, 232, 628, 543, 16, 16, 120, 257, 486]
39	[401, 229, 235, 232, 628, 543, 16, 16, 120, 257, 486]
40	[218, 139, 486, 675, 557, 462, 56, 56, 581, 282, 486]
41	[338, 139, 486, 675, 557, 462, 56, 56, 581, 282, 486]
42	[691, 272, 658, 727, 15, 154, 620, 620, 125, 317, 486]
43	[457, 272, 658, 727, 15, 154, 620, 620, 125, 317, 486]
44	[3, 462, 618, 315, 523, 341, 530, 530, 120, 319, 486]
45	[202, 462, 618, 315, 523, 341, 530, 530, 120, 319, 486]
46	[605, 390, 122, 520, 197, 71, 363, 363, 176, 77, 486]
47	[243, 390, 122, 520, 197, 71, 363, 363, 176, 77, 486]
48	[237, 368, 218, 659, 343, 398, 363, 363, 176, 328, 486]
49	[418, 368, 218, 659, 343, 398, 363, 363, 176, 328, 486]
50	[198, 530, 306, 360, 70, 181, 473, 473, 255, 330, 486]
51	[549, 530, 306, 360, 70, 181, 473, 473, 255, 330, 486]
52	[109, 265, 297, 27, 478, 437, 127, 127, 176, 577, 486]
53	[31, 265, 297, 27, 478, 437, 127, 127, 176, 577, 486]

2. Using the method explained in subsection 3.3.2.3, one finds the Gram matrix G displayed above (within less than 15 seconds using SAGE [The21]), corresponding to a certain sublattice $L_{j_0} \subset L'_{3,1}$. We have $\det(G) = 3^{25}$. On the other hand, equation (3.2.2) from remark 3.2.10 ensures that

$$\mathrm{Reg}(E/K) = 3^{23} \cdot |Ш(E/K)|^{-1}.$$

Moreover, $[E(K) : E(K)^0] = 3$ by proposition 3.2.14 and so $\mathrm{disc}(E(K)^0) = 3^2\,\mathrm{Reg}(E/K) = 3^{25}|Ш(E/K)|^{-1}$. Thus, if the Tate–Shafarevich group of $E_{28,1,1}$ over $\mathbb{F}_{3^6}(t)$ is trivial, then the sublattice L_{j_0} is actually equal to $L'_{3,1}$ because they both have the same covolume. Then G is a Gram matrix for $L'_{3,1}$ and, as explained in remark 3.3.8, the lattice $L_{j_0} = L'_{3,1}$ is generated by minimal vectors. ■

Remark 3.3.11. 1. There is no obvious way to give very explicitly (in terms of rational points) the points in the basis giving the above Gram matrix G. Indeed, the change-

[18] See the file `Computation Gram matrix of L'_3, 1` at https://gitlab.com/gauthierleterrier/maths for a computational proof that there are indeed linearly independent.

of-basis matrix A has coefficients $1/1453$ or $1/7$ (the denominators are factors of the determinant of the initial Gram matrix), and it seems difficult for instance to explicitly divide a point in $7E(K)^0$ by 7.

2. Another interpretation of the above result is that the Tate–Shafarevich group of $E_{28,1,1}$ over $\mathbb{F}_{3^6}(t)$ is trivial "with high probability", since random points $Q \in L'_{3,1}$ lie with very high probability in the sublattice L_{j_0} described at the end of the proof of computational proposition 3.3.10.

3. We can apply the same ideas to the 64-dimensional Mordell–Weil lattice $E(K)^0$ attached to $y^2 + y = x^3 + t^{33}$ over $\mathbb{F}_{2^{10}}(t)$ given in [Elk94], since lemma 3.3.2 applies here as well. After a few minutes of computation on SAGE, we end up with a Gram matrix G of determinant 2^{52}. Note that [Elk94, Proposition 3] asserts that $\operatorname{covol}(E(K)^0) = 2^{52/2} = 2^{26}$ (in this case the Tate–Shafarevich group is proved to be trivial), so in that case G is *provably* a Gram matrix of $E(K)^0$.

4. Observe that a lattice has not a *unique* Gram matrix, but two Gram matrices G, G' are $\mathrm{GL}_n(\mathbb{Z})$-congruent, i.e., $G' = {}^tUGU$ for some $U \in \mathrm{GL}_n(\mathbb{Z})$. ⌟

3.4 · Computation of some Tate–Shafarevich groups

In this final section, we discuss a method to study the Tate–Shafarevich group of the elliptic curves $E := E_{3^n+1,b,1} : y^2 = x^3 + bx + t^{3^n+1}$ over $K := \mathbb{F}_{3^{2n}}(t)$ that appeared in theorem 3.2.7, where $n \geqslant 1$ is any integer and $b \in \mathbb{F}_{3^n}^\times$ satisfies $b^{(3^n-1)/2} = (-1)^{n+1}$. This is done via "$p$-descent in characteristic p" (where $p = 3$), in analogy with the case $p = 2$ discussed in [Elk94]. There are other methods to study Ш, involving crystalline cohomology (see [Shi91, Dum95]); we will not explain this here.

More specifically, in this section we will prove the following statement.

Theorem 3.4.1 (theorem E). *If $n \in \{1, 2, 3\}$ and $b \in \mathbb{F}_{3^n}^\times$ is such that $b^{(3^n-1)/2} = (-1)^{n+1}$ then the Tate–Shafarevich group of $y^2 = x^3 + bx + t^{3^n+1}$ over $\mathbb{F}_{3^{2n}}(t)$ is trivial.* ⌟

From remark 3.2.10, we know that

$$|Ш(E/K)| \cdot \mathrm{Reg}(E/K) = 3^{n(3^{n-1}-1)-1}.$$

and $\mathrm{Reg}(E/K) \in \frac{1}{3^2}\mathbb{Z}$. Thus $|Ш(E/K)|$ divides $3^{n(3^{n-1}-1)+1}$. In particular, $Ш(E/K)$ is a 3-group, i.e., it is equal to its 3-primary subgroup (equivalently, its 3-Sylow subgroup) denoted by $Ш(E/K)[3^\infty]$. If $Ш(E/K)$ is non-trivial, then it must have an element of order 3; in other words we have

$$Ш(E/K) = \{1\} \iff Ш(E/K)[3] = \{1\}. \tag{3.4.1}$$

When $n \in \{1, 2, 3, 4, 5\}$ we conclude that $|Ш(E/K)|$ divides $3, 3^5, 3^{25}, 3^{105}$ and 3^{401} respectively. Furthermore it is known that the order of the Tate–Shafarevich group of an elliptic curve must be a square in $\mathbb{Z}$ (see [Sil08a, corollary C.17.2.1]), so when $n = 1$, we must have $|Ш(E/K)| = 1$.

Remark 3.4.2. In fact, when $n = 1$, the lower bound on the density of the 6-dimensional lattice $E_{4,1,1}(\mathbb{F}_{3^2}(t))^0$ agrees with the density of the root lattice E_6. By optimality of the density of E_6 among *lattice* sphere packings in dimension 6 (see proposition 1.2.11), we know that the lower bound from theorem 3.2.7 must be sharp when $n = 1$. In particular we get another (somehow indirect) proof that $Ш(E_{4,1,1}/\mathbb{F}_{3^2}(t))$ is trivial, by proposition 2.1.1. ⌟

One approach to obtain upper bounds on $|Ш(E/K)|$, inspired from [Elk94], would be to use a 3-descent argument.

Proposition 3.4.3. *For an integer $m \geqslant 1$ coprime to 3 and $n \geqslant 1$, let $k := \mathbb{F}_{3^{2n}}$, fix $b \in \mathbb{F}_{3^n}^\times$ and consider the elliptic curve $E_{m,b,1} : y^2 = f(x) := x^3 + bx + t^m$ over $k(t)$. Let $\beta \in k$ be a square root of $-b^{-3}$. We may define a map*

$$\begin{array}{rccc} \phi : & E_{m,b,1} & \longrightarrow & E_{m,b,1} \\ & (x,y) & \longmapsto & (-b^{-1}x^3 - b^{-1}t^m, \beta \cdot y \cdot f(x)) = (-b^{-1}(x^3+t^m), \beta \cdot y^3) \end{array} \tag{3.4.2}$$

where $f(x) := x^3 + bx + t^m$. Then:

1. *The map ϕ is a well-defined K-isogeny of degree 3.*
2. *We have[19] $\hat{h}(\phi(P)) = 3\hat{h}(P)$ for all $P \in E_{m,b,1}(k(t))$ and $\phi^2 = \phi \circ \phi = [-3]$ is the multiplication by -3. In particular, if we consider the lattice $L := E_{m,b,1}(k(t))$, then the rank $\mathrm{rk}(L)$ is even and $|L/\phi(L)| = 3^{\mathrm{rk}(L)/2}$.* ⌟

Proof. — 1. In general, if we consider an elliptic curve of the form $y^2 = x^3 + a_4x + a_6 =: f(x)$ over a field K of characteristic 3 (in particular $a_4 \neq 0$ otherwise the curve would be singular), and if we fix a square root $\beta \in \overline{K}$ of $-a_4^{-3}$ then the $\overline{K}$-morphism

$$\begin{array}{rccc} \phi : & E & \longrightarrow & E \\ & (x,y) & \longmapsto & (-a_4^{-1}x^3 - a_4^{-1}a_6, \beta \cdot y \cdot f(x)) = (-a_4^{-1}x^3 - a_4^{-1}a_6, \beta \cdot y^3) \end{array} \tag{3.4.3}$$

is well-defined: we simply let $x' := -a_4^{-1}x^3 - a_4^{-1}a_6$ and compute

$$\begin{aligned} (\beta \cdot y \cdot f(x))^2 &= -a_4^{-3}f(x)^3 \\ &= -a_4^{-3}(x^9 + a_4^3x^3 + a_6^3) = -a_4^{-3}x^9 - x^3 - (a_4^{-1}a_6)^3 \\ f(x') &= x'^3 + a_4x' + a_6 \\ &= (-a_4^{-1}x^3 - a_4^{-1}a_6)^3 + a_4(-a_4^{-1}x^3 - a_4^{-1}a_6) + a_6 \\ &= -a_4^{-3}x^9 - a_4^{-3}a_6^3 - x^3. \end{aligned}$$

In our case, the well-defined morphism ϕ is given by:

$$\begin{aligned} &\phi([X:Y:Z]) = [-b^{-1}X^3 - b^{-1}t^mZ^3 : \beta Y^3 : Z^3] \\ &\phi([X:Y:Z]) = [0:1:0] \iff Z^3 = X^3 = 0 \end{aligned} \tag{3.4.4}$$

In particular, ϕ is an isogeny over $k(t)$ of degree 3, since it is a morphism that maps $O := [0:1:0]$ to itself (the degree of ϕ is given by the degree in x of its first coordinate, namely $-b^{-1}x^3 - b^{-1}t^m$, by [Gal12, lemma 9.6.13]).

[19] In other words, ϕ acts as a homothety of ratio (scaling factor) $\sqrt{3}$: if we define the norm $\|P\| := \hat{h}(P)^{1/2}$, then $\|\phi(P)\| = \sqrt{3}\|P\|$.

2. We observe that $\phi^2 = \phi \circ \phi$ is given by

$$\begin{aligned}\phi(\phi(x,y)) &= (-b^{-1}\phi_1^3 - b^{-1}t^m, \beta \cdot \phi_2^3)\\ &= \big(-b^{-1}(-b^{-1}(x^3+t^m))^3 - b^{-1}t^m, \beta\cdot(\beta y^3)^3\big)\\ &= \big(b^{-4}(x^9+t^{3m}) - b^{-1}t^m, \beta^4 y^9\big)\end{aligned}$$

Thanks to lemma 3.2.16 and in view of the equality $\beta^2 = -b^{-3}$, we conclude that $\phi^2 = -[3]$ is the multiplication by -3.

From this, it follows that we have a chain of sublattices $3L = \phi(\phi(L)) \subset \phi(L) \subset L$, where $L := E_{m,b,1}(k(t))$. Moreover, the map $L/\phi(L) \to \phi(L)/\phi(\phi(L))$ given by $[x] \mapsto [\phi(x)]$ is an isomorphism of abelian groups. Then $[L : 3L] = 3^{\mathrm{rk}(L)} = [L : \phi(L)]^2$ is a square, so that the rank of L is even and $|L/\phi(L)| = 3^{\mathrm{rk}(L)/2}$.

We finally check that $\hat{h}(\phi(P)) = 3\hat{h}(P)$ for all $P \in E(K)$. From remark 3.2.19, we have to check that $h(3\phi(P)) = h(\phi(3P)) = 3h(3P)$. Now, $Q := 3P$ belongs to $E(K)^0$ so by lemma 3.2.17 and the fact that $\hat{h}$ is integer-valued on $E(K)^0$ (see theorem 1.3.24), we know that $x(Q), y(Q)$ are both polynomials. Checking that $h(\phi(Q)) = 3h(Q) = 3\deg(x(Q))$ is now easy: since $Q \in E(K)^0$, we have $\deg(x(Q)) = h(Q) = \hat{h}(Q) > \frac{m}{3}$ by corollary 3.2.18, theorem 1.3.24, and proposition 3.1.5 so the first coordinate of $\phi(Q)$, given by $-b^{-1}(x(Q)^3 + t^m)$, has indeed degree $\deg(x(Q)^3) = 3\deg(x(Q))$. ■

Now let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the absolute Galois group of K. For simplicity, let us denote $Ш := Ш(E/K)$. Note that the K-isogeny ϕ induces a map in Galois cohomology

$$H^1(\phi) : H^1(G_K, E(K^{\mathrm{sep}})) \longrightarrow H^1(G_K, E(K^{\mathrm{sep}})). \tag{3.4.5}$$

If we define $Ш[\phi] := Ш \cap \ker(H^1(\phi))$, then $H^1(\phi)$ (co-)restricts to a map $Ш[\phi] \to Ш[\phi]$. Moreover, we have $Ш[\phi] \subset Ш[3]$: if $s \in Ш$ satisfies $H^1(\phi)(s) = 0$ then $-3s = 0$ since $H^1\phi \circ H^1\phi = [-3]$ on $H^1(G_K, E(K^{\mathrm{sep}}))$. In particular, if $Ш[3]$ is trivial then so is $Ш[\phi]$.

Conversely, if $Ш[\phi]$ is trivial and $s \in Ш[3]$ then $-3s = H^1\phi(s') = 0$ where $s' := H^1\phi(s) \in Ш[\phi] = \{0\}$. Because $s' = 0$ we deduce that $s \in Ш[\phi] = \{0\}$. In other words, $Ш[3]$ is trivial. In conclusion, we get, in view of (3.4.1):

$$Ш(E/K) = \{0\} \iff Ш(E/K)[3] = \{0\} \iff Ш(E/K)[\phi] = \{0\}. \tag{3.4.6}$$

3.4.1 The need of flat cohomology

One issue however is that ϕ is not separable. In fact, E is supersingular, since for $p := 3$, the coefficient of $x^{p-1} = x^2$ in $f(x)^{\frac{p-1}{2}} = f(x) = x^3 + bx + t^m$ is 0 (we apply [Sil08a, theorem V.4.1]). Therefore $E[3](\overline{K}) = \{O\}$. Since ϕ is a 3-isogeny, we have $G := E[\phi] := \ker(\phi) \leqslant E[3]$ and then the kernel of ϕ has no $\overline{K}$-rational points (which implies that ϕ is not separable by [Sil08a, theorem III.4.10]).

Consequently, we can *not* apply the descent procedure as explained in [Sil08a, chapter X, §4]. If ϕ was separable, then we would have an exact sequence

$$0 \longrightarrow G(K^{\mathrm{sep}}) \hookrightarrow E(K^{\mathrm{sep}}) \xrightarrow{\phi} E(K^{\mathrm{sep}}) \longrightarrow 0. \tag{3.4.7}$$

which would yield a short exact sequence involving the *Selmer group* as central term:

$$0 \to E(K)/\phi(E(K)) \to \mathrm{Sel}_\phi(E/K) \to Ш(E/K)[\phi] \to 0.$$

In our case, inseparability of ϕ causes the triviality of the group $G(K^{\mathrm{sep}})$, and the non-surjectivity of ϕ on K^{sep}-rational points of E (even though it is surjective on $\overline{K}$-points). Therefore, we do not have an exact sequence as in (3.4.7).

However, instead of using Galois-invariants and Galois cohomology, we can save the picture by working with *flat cohomology*. Some relevant references are [Ulm91, Vol90, Kra77, Bro97] and especially [Möh14, lemma 6.3.3]. More specifically, we consider the kernel $G := \ker(\phi)$ of ϕ as a *group scheme*: while it has no $\overline{K}$-rational point, G is not trivial as a group scheme.

Now we let $T := \mathrm{Spec}(K)$ and consider G and E as group schemes over T. In fact, they are sheaves of abelian groups on T with respect to the *flat topology*: for instance, G is obviously a presheaf $(U \to T) \mapsto G(U)$, and being representable by a scheme, it is actually a sheaf, by [Mil80, Corollary II.1.7, p. 52]. We point out that since K is a field, any morphism from a non-empty scheme X to $\mathrm{Spec}(K)$ is faithfully flat ([GW20], p. 430).

It makes sense to speak of exact sequences of sheaves of abelian groups over T (in the flat topology), and it turns out that given any isogeny $\phi : E \to E'$ between elliptic curves over K we have an exact sequence of group schemes

$$0 \longrightarrow G = \ker(\phi) \xhookrightarrow{\iota} E \xrightarrow{\phi} E' \longrightarrow 0. \tag{3.4.8}$$

Indeed, by [EvdGM, proposition 5.2], any isogeny is necessarily flat, in which case [Mil80, exercise II.2.19, p. 67] ensures that ϕ induces a surjective morphism of flat sheaves[20] on T.

It induces a long exact sequence in flat cohomology. Note that $\mathrm{H}^0_{\mathrm{flat}}(T, A) \cong \Gamma(T, A) = A(T) = A(K)$ for any group scheme A over K, so we find:

$$\begin{array}{l} 0 \longrightarrow G(K) = \{0\} \xhookrightarrow{\iota} E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} \\ \mathrm{H}^1_{\mathrm{flat}}(T, G) \xrightarrow{H^1(\iota)} \mathrm{H}^1_{\mathrm{flat}}(T, E) \xrightarrow{H^1(\phi)} \mathrm{H}^1_{\mathrm{flat}}(T, E') \longrightarrow \cdots \end{array} \tag{3.4.9}$$

By a theorem of Grothendieck, if A is a *smooth* group scheme over $T = \mathrm{Spec}(K)$ (for instance $A = E$, but *not* $A = G$), then $\mathrm{H}^1_{\mathrm{flat}}(T, A) \cong \mathrm{H}^1_{\text{ét}}(T, A) \cong \mathrm{H}^1(G_K, A(K^{\mathrm{sep}}))$ (see [Gro68, corollaire 11.9, p. 183, and p. 125] for the first isomorphism, while the second isomorphism with Galois cohomology is given in [Mil80, example III.1.7, page 86]; see also [Mil80, theorem III.3.9]). Therefore, (3.4.9) induces a short exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xhookrightarrow{\delta} \mathrm{H}^1_{\mathrm{flat}}(T, E[\phi]) \xrightarrow{H^1(\iota)} H^1(G_K, E(K^{\mathrm{sep}}))[\phi] \longrightarrow 0 \tag{3.4.10}$$

where $H^1(G_K, E(K^{\mathrm{sep}}))[\phi] := \ker(H^1(\phi))$.

[20] Moreover, by [EvdGM, proposition 5.6], ϕ is separable if and only if ϕ is étale, in which case ϕ defines a surjective morphism of *étale* sheaves (i.e., sheaves of abelian groups on the étale site of $T := \mathrm{Spec}(K)$), by [Mil80, exercise II.2.19, p. 67].

For any place $v \in V_K$, we can use the same reasoning with $T_v = \mathrm{Spec}(K_v)$ to get short exact sequences as in (3.4.10), which yield a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \xhookrightarrow{\delta} & \mathrm{H}^1_{\mathrm{flat}}(T, E[\phi]) & \xrightarrow{H^1\iota} & H^1(G_K, E(K^{\mathrm{sep}}))[\phi] & \longrightarrow & 0 \\ & & \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \\ 0 & \longrightarrow & \prod_{v\in V_K} E'(K_v)/\phi(E(K_v)) & \xhookrightarrow{(\delta_v)} & \prod_{v\in V_K} \mathrm{H}^1_{\mathrm{flat}}(T_v, E[\phi]) & \xrightarrow{(H^1\iota_v)} & \prod_{v\in V_K} H^1(G_{K_v}, E(K_v^{\mathrm{sep}}))[\phi] & \longrightarrow & 0 \end{array} \tag{3.4.11}$$

Here f_3 is defined using the restriction maps $G_{K_v} \hookrightarrow G_K, \sigma \mapsto \sigma|_{K^{\mathrm{sep}}}$ and $T_v := \mathrm{Spec}(K_v)$, and f_2 is obtained using the canonical[21] group morphisms $\mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K), \ker(\phi)) \to \mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K_v), \ker(\phi))$.

This prompts to introduce the following group.

Definition 3.4.4. We define the ϕ-Selmer group of E over K as the kernel of $(H^1(\iota_v))_{v\in V_K} \circ f_2$, i.e.,

$$\begin{aligned} \mathrm{Sel}_\phi(E/K) &:= \ker\left(\mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K), \ker(\phi)) \longrightarrow \prod_{v\in V_K} \mathrm{H}^1(G_{K_v}, E(K_v^{\mathrm{sep}}))\right) \\ &= \bigcap_{v\in V_K} \ker\left(\mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K), \ker(\phi)) \longrightarrow \mathrm{H}^1(G_{K_v}, E(K_v^{\mathrm{sep}}))\right) \\ &= \bigcap_{v\in V_K} \mathrm{Sel}_\phi(E/K_v) \end{aligned}$$

$$\mathrm{Sel}_\phi(E/K_v) := \{\, \gamma \in \mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K), \ker(\phi)) \;:\; \gamma_v \in \mathrm{Im}(\delta_v) \subset \mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K_v), \ker(\phi)) \,\}. \;\lrcorner$$

All in all, we get a short exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \xhookrightarrow{\delta} \mathrm{Sel}_\phi(E/K) \xrightarrow{H^1\iota} Ш(E/K)[\phi] \longrightarrow 0 \tag{3.4.12}$$

From equation (3.4.6) and the above exact sequence applied to the 3-isogeny $\phi : E \to E$ from proposition 3.4.3, we deduce that

$$Ш(E/K) = \{1\} \iff |E(K)/\phi(E(K))| = |\mathrm{Sel}_\phi(E/K)|. \tag{3.4.13}$$

Remark 3.4.5. The inequality $|E(K)/\phi(E(K))| \leqslant |\mathrm{Sel}_\phi(E/K)|$ always holds. $\lrcorner$

3.4.2 Computing the descent map

Now, in order to understand better the ϕ-Selmer group, we want first to determine $\mathrm{H}^1_{\mathrm{flat}}(T, G)$ where $G = E[\phi] = \ker(\phi), T = \mathrm{Spec}(K)$ and then describe explicitly the boundary map $\delta : E(K)/\phi(E(K)) \to \mathrm{H}^1_{\mathrm{flat}}(T, G)$ (appearing in (3.4.10)) as well as δ_v for all places v.

[21] Given the map $\pi : X = \mathrm{Spec}(K_v) \to Y = \mathrm{Spec}(K)$ and any group scheme $\mathcal{F}$ on Y, we have functorial maps $\mathrm{H}^i_{\mathrm{flat}}(Y, \mathcal{F}) \to \mathrm{H}^i_{\mathrm{flat}}(X, \pi^*\mathcal{F})$ extending the morphism on H^0 given by $\mathcal{F}(K) \to \mathcal{F}(K_v)$ — see [Mil80, remark III.1.6 c), p. 85].

3.4.2.1 Kernel of ϕ

In this paragraph, we find the structure of $\ker(\phi)$ as a group scheme, where $\phi : E \to E$ is the inseparable 3-isogeny as in equation (3.4.3).

Remark 3.4.6. We will need to work with rational points of E over commutative K-algebras R which are not necessarily fields. However, we will assume that their Picard group is trivial: $\mathrm{Pic}(R) = \{0\}$. The key fact is that under this assumption, the R-rational points of the projective plane $\mathbb{P}^2$ are easily described: $\mathbb{P}^2(R) \cong L(R)/R^\times$ where $L(R)$ is the set of triplets $(x, y, z) \in R^3$ such that the elements $x, y, z \in R$ generates the unit ideal $\langle x, y, z\rangle = R$. See [Sta23, Tag 01NE] (when $\mathrm{Pic}(R) = \{0\}$, all line bundles on $\mathrm{Spec}(R)$ are trivial, so we get the description of $\mathbb{P}^2(R)$ as in [GW20, exercises 3.19, 4.6]).

In particular, given an embedding $E \hookrightarrow \mathbb{P}^2_K = \mathrm{Proj}\, K[X, Y, Z]$, we get an inclusion $E(R) \hookrightarrow \mathbb{P}^2(R)$, so we can write points $P \in E(R)$ using projective coordinates. ⌟

Proposition 3.4.7. *Let K be a field of characteristic 3 and E be an elliptic curve over K given by $y^2 = x^3 + a_4x + a_6$ where $a_6 \in K$ and $-a_4 \in K$ is a square. Consider the K-isogeny $\phi : E \to E$ defined in equation (3.4.3).*

Then the kernel of ϕ (seen as a subgroup scheme of E) is isomorphic to the affine group scheme $\alpha_3 := \mathrm{Spec}(K[u]/(u^3))$. More specifically, there is a unique isomorphism of group schemes $\iota : \ker(\phi) \to \alpha_3$ such that for any K-algebra R with $\mathrm{Pic}(R) = \{0\}$, the values of ι on R-rational points are given by

$$\iota_R : \ker(\phi)(R) \xrightarrow{\cong} \alpha_3(R), \qquad [X : Y : Z] \longmapsto X/Y. \quad ⌟$$

Note that α_3 is non-reduced and that we have $\alpha_p(L) \simeq \mathrm{Hom}_{K\text{-alg}}(K[x]/(x^p), L) \simeq \{0\}$ for *any* field extension L/K.

Proof of proposition 3.4.7. — Let R be a K-algebra such that $\mathrm{Pic}(R) = 0$. Then, letting $\beta \in K$ be a square root of $-a_4^{-3}$, we have

$$\begin{aligned}(\ker(\phi))(R) &= \{\, [X : Y : Z] \in E(R) \subset \mathbb{P}^2(R) \;:\; [-a_4^{-1}(X^3 + a_6Z^3) : \beta Y^3 : Z^3] = [0 : 1 : 0] \,\} \\ &= \{\, [X : Y : Z] \in E(R) \subset \mathbb{P}^2(R) \;:\; \exists \lambda \in R^\times, (X^3 + a_6Z^3) = Z^3 = 0, \beta Y^3 = \lambda \,\}.\end{aligned}$$

In particular we have $X^3 = Z^3 = 0$ for all $[X : Y : Z] \in (\ker(\phi))(R)$. For any R-rational point $[X : Y : Z]$ of $\ker(\phi)$, we know that $Y^{-1} = \lambda^{-1}\beta Y^2 \in R^\times$ is a unit, and that $(XY^{-1})^3 = 0$, which ensures that $XY^{-1} \in \alpha_3(R)$, and thus ι_R is well-defined.

We need to study the group law on $\ker(\phi)$. Note that if $[X : Y : Z] = [X/Y : 1 : Z/Y] \in \ker(\phi)(R)$ then the equation of E yields $Y^2Z = a_4XZ^2$ which implies $Y^2Z^2 = 0$ (since $X^3 = Z^3 = 0$) and thus $Y^2Z = a_4X \cdot 0 = 0$ which finally we get $Z = 0$ (since Y is a unit in R).

Now, we can add two points $P = [x : 1 : 0], P' = [x' : 1 : 0] \in \ker(\phi)(R)$ using the formulas $X_3^{(2)}, Y_3^{(2)}, Z_3^{(2)}$ from [BL95, §5, p. 237-238], which give the addition law on elliptic curves over any commutative ring with trivial Picard group. These formulas $X_3^{(2)}, Y_3^{(2)}, Z_3^{(2)}$ are valid whenever the y-coordinate of $P - P' \in \ker(\phi)(R)$ is non-zero, which is the case here

since it is actually a unit in R as we have seen. An implementation[22] on SAGE [The21] of these formulas shows that $P + P' = [x + x' : 1 : 0]$ so that ι_R is indeed a group morphism.

Finally, ι_R is bijective: its inverse is given by $s \in \alpha_3(R) \longmapsto [s : 1 : 0]$. It is also straightforward to check that the isomorphisms ι_R are natural in R. The fact that these maps ι_R induce a unique group-scheme morphism $\iota : \ker(\phi) \to \alpha_3$ (which is an isomorphism with inverse induced by ι_R^{-1}) follows from the next lemma 3.4.8, recalling that all local rings have trivial Picard group. ■

Lemma 3.4.8. *Let K be a field and G, G' be two* finite *group schemes over K. Assume that for all local K-algebras R, we are given group morphisms $\iota_R : G(R) \to G'(R)$ which are functorial in R.*

Then there is a unique morphism $\iota : G \to G'$ of group schemes such that its values on R-rational points is ι_R, for all local K-algebras R. ⌟

Proof. — Let $\mathcal{C}$ be the category whose objects are finite disjoint union of affine schemes with local underlying ring (and morphisms are given in the obvious way). By [Mil17, proposition 11.2], we know that G and G' are objects of $\mathcal{C}$. Now there is a unique way to extend our functor to get morphisms $\iota_S : G(S) \to G'(S)$ for any $S \in |\mathcal{C}|$ (simply by using the fact that $G(\prod_{i=1}^n R_i) \cong \prod_{i=1}^n G(R_i)$). Then the claim basically follows from Yoneda's lemma. ■

3.4.2.2 Amitsur–Čech cohomology

In order to describe explicitly the descent map $\delta : E(K)/\phi(E(K)) \to \mathrm{H}^1_{\mathrm{flat}}(T, G)$ (appearing in (3.4.10)), we need to study the group $\mathrm{H}^1_{\mathrm{flat}}(T, G)$ (where $G = \ker(\phi), T = \mathrm{Spec}(K)$). By proposition 3.4.7, we know that there is an isomorphism $H^1(\iota) : \mathrm{H}^1_{\mathrm{flat}}(T, G) \longrightarrow \mathrm{H}^1_{\mathrm{flat}}(T, \alpha_3)$. The key point is that flat cohomology groups $\mathrm{H}^i_{\mathrm{flat}}(S, \mathcal{F})$ over an *affine* scheme $\mathrm{Spec}(R)$ can be described very explicitly using the Amitsur–Čech chain complex, as defined in [Sha72, chapter VI.§3, p. 204–210] or [Sha64, §2].

Given a commutative ring R, a sheaf of abelian group $\mathcal{F}$ on the flat site of $\mathrm{Spec}(R)$ and a *faithfully flat* R-algebra S, we have an exact sequence, i.e., an (augmented) *cochain complex*:

$$0 \longrightarrow \mathcal{F}(R) \longrightarrow \mathcal{F}(S) \xrightarrow{\Delta_0} \mathcal{F}(S^{\otimes 2}) \xrightarrow{\Delta_1} \mathcal{F}(S^{\otimes 3}) \xrightarrow{\Delta_2} \dots$$

where the tensor products are over R,

$$\Delta_n := \sum_{i=1}^{n+2} (-1)^i \mathcal{F}(\epsilon_{i,n+1}) : \mathcal{F}(S^{\otimes(n+1)}) \to \mathcal{F}(S^{\otimes(n+2)}) \tag{3.4.14}$$

$$\begin{array}{rccc} \epsilon_{i,n} : & S^{\otimes(n+1)} & \longrightarrow & S^{\otimes(n+2)} \\ & s_1 \otimes \cdots \otimes s_n & \longmapsto & s_1 \otimes \cdots \otimes 1 \otimes s_{i+1} \otimes \cdots \otimes s_n \end{array}$$

(we only defined $\epsilon_{i,n}$ on pure tensors but we can extend it to $S^{\otimes(n+1)}$ by R-linearity). Note that $\epsilon_{i,n}$ are R-algebra homomorphisms[23], so that $\mathcal{F}(\epsilon_{i,n})$ makes sense.

[22] See the file `"Kernel of phi and explicit descent map.ipynb"` available at https://gitlab.com/gauthierleterrier/maths.

[23] However, $\sum_{i=1}^{n+2}(-1)^i \epsilon_{i,n+1}$ is typically *not* a ring morphism; but Δ_n is well-defined since it is an alternating sum of $\mathcal{F}(\epsilon_{i,n})$.

For instance, the case $\mathcal{F} = \mathbb{G}_a$ is discussed in [Mil80, proposition I.2.18]: if $R \to S$ is a faithfully flat morphism of rings, then the sequence of R-modules

$$0 \longrightarrow R \longrightarrow S \xrightarrow{\Delta_0} S^{\otimes 2} \xrightarrow{\Delta_1} S^{\otimes 3} \xrightarrow{\Delta_2} \dots \tag{3.4.15}$$

is exact. We can now introduce the relevant cohomology groups.

Definition 3.4.9. Let $R \to S$ be a faithfully flat ring morphism and let $\mathcal{F}$ be a sheaf of abelian groups on the flat site of $\mathrm{Spec}(R)$. For each $n \geqslant 1$, we define the n-th *Amistur–Čech cohomology group* as

$$\check{\mathrm{H}}^n(S/R, \mathcal{F}) := \ker(\Delta_n)/\operatorname{Im}(\Delta_{n-1}).$$

When $n = 0$, we set $\check{\mathrm{H}}^0(S/R, \mathcal{F}) := \ker(\Delta_0) \cong \mathcal{F}(R)$. ⌟

The main theorem (see [Mil80, corollary III.2.10]) is that

$$\mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(R), \mathcal{F}) \cong \varinjlim_{S \in \mathsf{AlgF}_R} \check{\mathrm{H}}^1(S/R, \mathcal{F}) \tag{3.4.16}$$

where AlgF_R denotes the directed set of faithfully flat R-algebras of finite type. In fact, when $R = K$ is a field, there is a final object in AlgF_K, namely the algebraic closure $\overline{K}$, so we get (see [Sha72, theorem 42, p. 208] or rather [Sha64, theorem 1, p. 418])

$$\mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K), \mathcal{F}) \cong \check{\mathrm{H}}^1(\overline{K}/K, \mathcal{F}). \tag{3.4.17}$$

From here, we can give an explicit description of the cohomology group $\mathrm{H}^1_{\mathrm{flat}}(T, \alpha_p)$ where $T = \mathrm{Spec}(K)$ and K is a field of characteristic $p > 0$.

First, following [Mil80, p. 67 and p. 128], there is a short exact sequence of sheaves of abelian groups for the flat topology on S:

$$0 \longrightarrow \alpha_p \hookrightarrow \mathbb{G}_a \xrightarrow{F} \mathbb{G}_a \longrightarrow 0 \tag{3.4.18}$$

where F is the Frobenius morphism which is given by $\mathbb{G}_a(R) \cong R \to R, s \mapsto s^p$ for any K-algebra R. This yields a long exact sequence, where $K^p := \{\, x^p \ : \ x \in K \,\}$ is the additive subgroup of p-th powers in K:

$$0 \longrightarrow K/K^p \xhookrightarrow{\partial} \mathrm{H}^1_{\mathrm{flat}}(T, \alpha_p) \longrightarrow \mathrm{H}^1_{\mathrm{flat}}(T, \mathbb{G}_a) \longrightarrow \mathrm{H}^1_{\mathrm{flat}}(T, \mathbb{G}_a) \longrightarrow \cdots \tag{3.4.19}$$

Since $\mathbb{G}_a$ is smooth over S, we have — as discussed in subsection 3.4.1 — $\mathrm{H}^1_{\mathrm{flat}}(T, \mathbb{G}_a) \cong H^1_{\text{ét}}(T, \mathbb{G}_a) \cong H^1(G_K, K^{\mathrm{sep}}) = \{0\}$ (this is the additive analogue of Hilbert 90 theorem), so that $\mathrm{H}^1_{\mathrm{flat}}(T, \alpha_p) \cong K/K^p$. We are going to make explicit the following boundary map:

$$\partial : K/K^p \xrightarrow{\cong} \mathrm{H}^1_{\mathrm{flat}}(T, \alpha_p) \cong \check{\mathrm{H}}^1(\overline{K}/K, \alpha_p). \tag{3.4.20}$$

To this end, we start with some general considerations.

① We show that $\mathrm{H}^1_{\mathrm{flat}}(T, \alpha_p)$ is a subgroup of $\overline{K} \otimes_K \overline{K}$. First, for a general sheaf $\mathcal{F}$ as in definition 3.4.9, we have

$$\Delta_0 = \mathcal{F}(\epsilon_{1,1}) - \mathcal{F}(\epsilon_{2,1}) : \mathcal{F}(S) \to \mathcal{F}(S^{\otimes 2})$$
$$\Delta_0 = \mathcal{F}(s \mapsto 1 \otimes s) - \mathcal{F}(s \mapsto s \otimes 1)$$

and

$$\Delta_1 = \mathcal{F}(\epsilon_{1,2}) - \mathcal{F}(\epsilon_{2,2}) + \mathcal{F}(\epsilon_{3,2}) : \mathcal{F}(S^{\otimes 2}) \to \mathcal{F}(S^{\otimes 3})$$
$$\Delta_1 = \mathcal{F}(s \otimes s' \mapsto 1 \otimes s \otimes s') - \mathcal{F}(s \otimes s' \mapsto s \otimes 1 \otimes s') + \mathcal{F}(s \otimes s' \mapsto s \otimes s' \otimes 1).$$

Note that when $K = \mathbb{F}_p(t)$, then $\overline{K} \otimes_K \overline{K}$ is not reduced! It contains $K(t^{1/p}) \otimes_K \overline{K} \cong K[X]/(X^p - t) \otimes_K \overline{K} \cong \overline{K}[X]/((X - t^{1/p})^p)$ and the class s of $X - t^{1/p}$ satisfies $s^p = 0 \neq s$.

② In the case where $\mathcal{F} = \alpha_p$ we have

$$\ker(\Delta_1) = \langle s \otimes s' \in \overline{K} \otimes_K \overline{K} \mid (s \otimes s')^p = 0,\ 1 \otimes s \otimes s' - s \otimes 1 \otimes s' + s \otimes s' \otimes 1 = 0 \rangle$$
$$\mathrm{Im}(\Delta_0) = \{\, 1 \otimes s - s \otimes 1 \ :\ s \in \overline{K}, s^p = 0 \,\} = \{0\}.$$

Thus we see that $\check{\mathrm{H}}^1(\overline{K}/K, \alpha_p) = \ker(\Delta_1)/\mathrm{Im}(\Delta_0)$ is an additive subgroup of $\overline{K} \otimes_K \overline{K}$.

③ In general, an exact sequence of commutative group schemes of finite type over K, say

$$0 \longrightarrow A \xrightarrow{\beta} B \xrightarrow{\gamma} C \longrightarrow 0$$

induces an exact sequence of (co)chain complexes

$$0 \longrightarrow \mathcal{C}^\bullet(A) \longrightarrow \mathcal{C}^\bullet(B) \longrightarrow \mathcal{C}^\bullet(C) \longrightarrow 0$$

where $\mathcal{C}^\bullet(A) = (\mathcal{C}^r(A), \Delta_r)_{r \geqslant 0}$ and $\mathcal{C}^r(A) := A(\overline{K}^{\otimes(r+1)})$ are defined in equation (3.4.14) (see the proof of [Sha64, theorem 1, p. 418]). Concretely, we have a commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A(\overline{K}) & \xrightarrow{\beta_0} & B(\overline{K}) & \xrightarrow{\gamma_0} & C(\overline{K}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \Delta_0^A} & & \downarrow{\scriptstyle \Delta_0^B} & & \downarrow{\scriptstyle \Delta_0^C} & & \\
0 & \longrightarrow & A(\overline{K} \otimes_K \overline{K}) & \xrightarrow{\beta_1} & B(\overline{K} \otimes_K \overline{K}) & \xrightarrow{\gamma_1} & C(\overline{K} \otimes_K \overline{K}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \Delta_1^A} & & \downarrow{\scriptstyle \Delta_1^B} & & \downarrow{\scriptstyle \Delta_1^C} & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

We want to describe the boundary map $\partial^0 : \check{\mathrm{H}}^0(\overline{K}/K, C) \to \check{\mathrm{H}}^1(\overline{K}/K, A)$, using "diagram-chasing". Let $c \in \check{\mathrm{H}}^0(\overline{K}/K, C) = C(K) = \ker(\Delta_0^C)$. Let $b \in B(\overline{K})$ be such that $\gamma_0(b) = c$. Then

$$\gamma_1(\Delta_0^B(b)) = \Delta_0^C(\gamma_0(b)) = 0,$$

so that $\Delta_0^B(b) \in \ker(\gamma_1) = \mathrm{Im}(\beta_1)$, say $\Delta_0^B(b) = \beta_1(a)$ for some $a \in A(\overline{K} \otimes_K \overline{K})$. It can be checked that $a \in \ker(\Delta_1^A)$ and that the map $c \mapsto [a] \in \ker(\Delta_1^A) \big/ \mathrm{Im}(\Delta_0^A)$ is well-defined; this is the desired boundary map $\partial := \partial^0$.

We can now compute the boundary map ∂ introduced in equation (3.4.20).

Lemma 3.4.10. *The boundary map can be expressed as follows:*

$$\begin{array}{rccc} \partial : & K & \longrightarrow & \check{\mathrm{H}}^1(\overline{K}/K, \alpha_p) \subset \overline{K} \otimes_K \overline{K} \\ & c & \longmapsto & 1 \otimes c^{1/p} - c^{1/p} \otimes 1 \end{array}$$

where $c^{1/p} \in \overline{K}$ denotes the unique p-th root of a given element $c \in K$. ⌟

Proof. — Let us fix $c \in K$ and set $b := c^{1/p} \in \overline{K}$. Consider the exact sequence (3.4.18), where we use the notations from item ③ above:

$$0 \to A := \alpha_p \hookrightarrow B := \mathbb{G}_a \to C := \mathbb{G}_a \to 0.$$

The element $a := \Delta_0^B(b) = 1 \otimes b - b \otimes 1$ is easily seen to lie[24] in $\alpha_p(\overline{K} \otimes_K \overline{K})$, because $a^p = 1 \otimes c - c \otimes 1 = 1 \otimes c - 1 \otimes c = 0$ since $c \in K$ and the tensor product is over K. Now the boundary map ∂ is exactly given by $c \mapsto a = 1 \otimes c^{1/p} - c^{1/p} \otimes 1$, as the discussion from item ③ above shows. ■

3.4.2.3 Explicit descent map

Fix a field K of characteristic 3, let E be an elliptic curve over K defined by $y^2 = x^3 + a_4 x + a_6$ and let ϕ be the 3-isogeny introduced in equation (3.4.3). We can now give an explicit description of the descent map $\delta : E(K)/\phi(E(K)) \to \mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K), \ker(\phi))$ appearing in (3.4.9).

We note that in [Elk94], there is an analogous situation in characteristic 2, where it is proved (theorem 2, p. 355, *ibid.*) that the map $E'(K') \to K'/K'^2, (x, y) \mapsto [x]$ is a group morphism, where $E' : y^2 + y = x^3 + t^{2^n+1}$, $K' = \mathbb{F}_{2^{2n}}(t)$ and n is odd. However, no explanation is given in [Elk94] about how this descent map relates to the Tate–Shafarevich group. So our discussion in the above subsections fills this gap.

Definition 3.4.11. We define the map $\epsilon : E(K) \to K/K^3$ as the composition $\epsilon := \partial^{-1} \circ H^1(\iota) \circ \delta$, that is:

$$\epsilon : E(K) \xrightarrow{\delta} \check{\mathrm{H}}^1(\overline{K}/K, \ker(\phi)) \xrightarrow[\cong]{H^1(\iota)} \check{\mathrm{H}}^1(\overline{K}/K, \alpha_3) \xleftarrow[\cong]{\partial} K/K^3$$

where $\delta, H^1(\iota)$ are as in (3.4.9) and ∂ is as in (3.4.20). Note that ϵ is a group morphism, where K^3 denotes the additive subgroup of cubes in K. ⌟

In what follows, we will denote by $[z] = z \bmod K^3$ the class of an element $z \in K$ in the quotient additive group K/K^3.

Proposition 3.4.12. *Fix a field K of characteristic 3, let E be an elliptic curve over K defined by $y^2 = x^3 + a_4 x + a_6$ and let ϕ be the 3-isogeny introduced in equation (3.4.3). Assume that $-a_4$ is a square in K and that $E[2](K) = \{0\}$.*

[24] In fact, a lies in $\ker(\Delta_1)$ as we would expect:

$$1 \otimes (1 \otimes b) - 1 \otimes (b \otimes 1) \; - \; (1 \otimes 1 \otimes b - b \otimes 1 \otimes 1) \; + \; 1 \otimes b \otimes 1 - b \otimes 1 \otimes 1 = 0.$$

Then the map $\epsilon : E(K) \to K/K^3$ is given by $(x_P, y_P) \mapsto [-a_4^{-3} y_P] \in K/K^3$ on affine K-rational points, and $\epsilon([0:1:0]) = 0 \bmod K^3$. ⌟

Remark 3.4.13. We will need to consider R-rational points of E where the ring $R := \overline{K} \otimes_K \overline{K}$ has nilpotents (it is not reduced), but its Picard group is trivial, that is, $\mathrm{Pic}(R) = \{0\}$. Indeed, R is the direct limit of $A_L := \overline{K} \otimes_K L$ over finite extensions L/K. Then $\mathrm{Pic}(R)$ is the direct limit of $\mathrm{Pic}(A_L)$, and A_L is a finite-dimensional $\overline{K}$-algebra so it is a finite product of artinian local rings, and thus its Picard group is trivial.

This allows to describe the R-rational points of E using projective coordinates as mentioned in remark 3.4.6. ⌟

Proof of proposition 3.4.12. — We first describe the map δ using the discussion of item ③ above, applied to the short exact sequence (3.4.8). Namely, δ sends a point $P = [x_P : y_P : 1] \in E(K) \smallsetminus \{O\}$ to the $(\overline{K} \otimes_K \overline{K})$-rational point of $\ker(\phi) \leqslant E$ given by

$$\delta(P) = Q' := [1 \otimes x_Q : 1 \otimes y_Q : 1 \otimes 1] - [x_Q \otimes 1 : y_Q \otimes 1 : 1 \otimes 1]$$

where $Q = (x_Q, y_Q) \in E(\overline{K})$ satisfies $\phi(Q) = P$ (here we are also using remark 3.4.13). This means $-a_4^{-1}(x_Q^3 + a_6) = x_P$ and $\beta y_Q^3 = y_P$ (where β is a square root of $-a_4^{-3}$), so that $x_Q^3 = -a_4 x_P - a_6 \in K$.

In other words, we have

$$Q' = Q_1 + Q_2, \qquad Q_1 = [1 \otimes x_Q : 1 \otimes y_Q : 1 \otimes 1], \qquad Q_2 = [x_Q \otimes 1 : -y_Q \otimes 1 : 1 \otimes 1].$$

Let us set

$$x_1 := 1 \otimes x_Q, \quad y_1 := 1 \otimes y_Q, \quad x_2 := x_Q \otimes 1, \quad y_2 := -y_Q \otimes 1.$$

We have $x_1^3 = x_2^3$ and since a_4 is a square in K (so that $\beta \in K$) we have $y_1^3 = -y_2^3$. We claim that $Q_1 \neq Q_2$.

> Indeed, assume for a contradiction that $Q_1 = Q_2$ so that $x_1 = x_2$. By the exactness of (3.4.15) applied to $R = K, S = \overline{K}$, it follows that $x_Q \in K$. Then $y_Q^2 \in K$ and also we know that $y_Q^3 = \beta^{-1} y_P \in K$ since $-a_4$ is a square in K (so that $\beta \in K$). So in all cases $y_Q \in K$ (either it is 0 or otherwise write $y_Q = y_Q^3 y_Q^{-2}$), which implies that $y_2 = -y_1$. Since we assumed $Q_1 = Q_2$, we must have $y_2 = y_1 = -y_1$, so that $2y_1 = -y_1 = 0 \in \overline{K} \otimes_K \overline{K}$ (recall that $\mathrm{char}(K) = 3$).
>
> Now because $E[2](K) = \{0\}$ we have $y_Q \neq 0 \in K$. Then y_1 is a unit in the ring $\overline{K} \otimes_K \overline{K}$ with inverse $y_1^{-1} = 1 \otimes y_Q^{-1}$ and in particular $y_1 \neq 0 \in \overline{K} \otimes_K \overline{K}$, and this yields a contradiction with the previous assertion. Therefore, we conclude that $Q_1 \neq Q_2$ as desired.

Now, we can apply the formulas $X_3^{(1)}, Y_3^{(1)}, Z_3^{(1)}$ from [BL95, §5, p. 236-237], which give the addition of any two *distinct* points on E over any commutative ring with trivial Picard group (which is the case of $\overline{K} \otimes_K \overline{K}$ by remark 3.4.13). Using SAGE [The21], we find[25]

$$Q' = [y_2(x_2 - x_1)(y_1 - y_2) - a_4(x_2 - x_1)^2 : y_2^3 : 0] \tag{3.4.21}$$

[25] See the file "Kernel of phi and explicit descent map.ipynb" available at https://gitlab.com/gauthierleterrier/maths.

By proposition 3.4.7 and lemma 3.4.10, we know that once we write the X/Y-coordinate of Q' as $1 \otimes c^{1/3} - c^{1/3} \otimes 1$ (for some $c \in K$), this means that the map $\epsilon : E(K) \to K/K^3$ is given by $P \mapsto [c]$.

The key point is that $x_Q \in K + Ky_Q^2 \subset \overline{K}$: indeed from the equation $y_Q^2 = x_Q^3 + a_4 x_Q + a_6$ we have

$$x_Q = a_4^{-1} \cdot (y_Q^2 - x_Q^3 - a_6) = a_4^{-1} y_Q^2 - a_4^{-1}(x_Q^3 + a_6) = a_4^{-1} y_Q^2 + x_P.$$

It follows that (recalling that x_P and a_4^{-1} belong to K):

$$x_2 - x_1 = (x_P + a_4^{-1} y_Q^2) \otimes 1 - 1 \otimes (x_P + a_4^{-1} y_Q^2) = a_4^{-1} \cdot (y_Q^2 \otimes 1 - 1 \otimes y_Q^2).$$

From now on, we assume that $E[2](K) = \{O\}$. In particular, $y_Q \neq 0$ since $P \in E(K)$ and $\beta y_Q^3 = y_P$, which means that $y_2^{-1} = -y_Q^{-1} \otimes 1$ is a unit in the ring $\overline{K} \otimes_K \overline{K}$. Let us write

$$L := y_Q \otimes 1, \qquad R := 1 \otimes y_Q \in \overline{K} \otimes_K \overline{K}$$

(the notation stands for "left" and "right" respectively) and note that $L^3 = R^3$ (since $y_Q^3 = \beta^{-1} y_P \in K$). We finally compute

$$\begin{aligned}
\delta(Q') &= y_2^{-2}(x_2 - x_1)(y_1 - y_2) \;-\; a_4 y_2^{-3}(x_2 - x_1)^2 \\
&= a_4^{-1}(y_Q^{-2} \otimes 1) \cdot (y_1 - y_2) \cdot (y_Q^2 \otimes 1 - 1 \otimes y_Q^2) \\
&\quad - a_4 a_4^{-2}(-y_Q^{-3} \otimes 1) \cdot \left(y_Q^2 \otimes 1 - 1 \otimes y_Q^2\right)^2 \\
&= a_4^{-1} L^{-2}(L + R)(L^2 - R^2) + a_4^{-1} L^{-3}(L^2 - R^2)^2 \\
&= a_4^{-1} L^{-2}(L^3 + RL^2 - R^2 L - R^3) + a_4^{-1} L^{-3}(L^4 + L^2 R^2 + R^4) \\
&= a_4^{-1} \cdot (R - R^2 L^{-1} + L + L^{-1} R^2 + L^{-3} R^4) \\
&= a_4^{-1} \cdot (R + L + R) \\
&= a_4^{-1}(L - R) \\
&= a_4^{-1} y_Q \otimes 1 \;-\; 1 \otimes a_4^{-1} y_Q \\
&= 1 \otimes (-a_4^{-1} y_Q) \;-\; (-a_4^{-1} y_Q) \otimes 1
\end{aligned}$$

recalling that $2 = -1$ since $\mathrm{char}(K) = 3$. Thus we find that we may take $c^{1/3} = -a_4^{-1} y_Q$ which proves the claimed description of the map ϵ. ■

3.4.3 Selmer groups in characteristic 3

We are now ready to compute the ϕ-Selmer group of E over K (or more precisely, get an upper bound on its size). In view of the definition 3.4.4 of Selmer groups and of the description of the descent map

$$\epsilon = \partial^{-1} \circ H^1(\iota) \circ \delta : E(K) \to K/K^3, \qquad (x, y) \mapsto [-a_4^{-3} y]$$

from proposition 3.4.12, we introduce the following groups, where $v \in V_K$:

$$S_\phi(E/K_v) = \{\, z \in K/K^3 \;:\; z \in \mathrm{Im}(\epsilon'_v) \hookrightarrow K_v/K_v^3 \,\} \tag{3.4.22}$$

$$S_\phi(E/K) = \bigcap_{v \in V_K} S_\phi(E/K_v) \hookrightarrow K/K^3, \tag{3.4.23}$$

where

$$\epsilon'_v := -a_4^3 \cdot \epsilon_v : E(K_v) \to K_v/K_v^3, \qquad (x, y) \mapsto [y]$$

is (a normalization of) the descent map ϵ_v described in proposition 3.4.12 applied to K_v instead of K.

Since $\partial, H^1(\iota)$ and multiplication by $-a_4^3$ are isomorphisms, it follows that $S_\phi(E/K_v) \cong \mathrm{Sel}_\phi(E/K_v)$ and $S_\phi(E/K) \cong \mathrm{Sel}_\phi(E/K)$ as abelian groups.

Thanks to (3.4.11), one gets a commutative diagram[26] , where $\epsilon' := -a_4^3\epsilon : E(K) \to K/K^3$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(K)/\phi(E(K)) & \xrightarrow{\epsilon'} & K/K^3 & \xrightarrow{H^1\iota} & H^1(G_K, E(K^{\mathrm{sep}}))[\phi] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2'} & & \downarrow{\scriptstyle f_3} & & \\
0 & \longrightarrow & \prod_{v \in V_K} E(K_v)/\phi(E(K_v)) & \xrightarrow{(\epsilon'_v)} & \prod_{v \in V_K} K_v/K_v^3 & \xrightarrow{(H^1\iota_v)} & \prod_{v \in V_K} H^1(G_{K_v}, E(K_v^{\mathrm{sep}}))[\phi] & \longrightarrow & 0
\end{array} \tag{3.4.24}$$

from which we deduce a short exact sequence as in (3.4.12):

$$0 \longrightarrow E(K)/\phi(E(K)) \xrightarrow{\epsilon'} S_\phi(E/K) \xrightarrow{H^1\iota} Ш(E/K)[\phi] \longrightarrow 0.$$

Theorem 3.4.14. *Let $E : y^2 = x^3 + bx + a_6$ over $K := k(t)$ where k is a finite field of characteristic 3. Assume that $|k| > 3$, that $-b = \beta^2 \in k^\times$ is a square in $k^\times$ and that $a_6 \in k[t]$ is a polynomial of degree d coprime[27] to 3. Let $v \in V_K$.*

1. *If v is a finite place, then*

$$S_\phi(E/K_v) = \mathrm{Im}(\mathcal{O}_v \cap K \longrightarrow K/K^3), \tag{3.4.25}$$

   that is, any element $[y] \in S_\phi(E/K_v)$ has a v-integral representative.

2. *If $v = v_\infty = -\deg$, then we have an inclusion*

$$S_\phi(E/K_v) \subseteq \left\{ [z] \in K/K^3 \ : \begin{array}{c} \deg(z) = d/2 \quad \text{and} \quad z^2 \cdot a_6^{-1} \equiv 1 \pmod{t^{-1}} \\ \text{or} \\ 0 \leqslant \deg(z) < d/2 \quad \text{and} \quad \deg(z) \equiv d \bmod 3 \end{array} \right\}.$$

Before proving the theorem, we state a few preliminary results.

Lemma 3.4.15. *Let k be a field, fix $R \in K = k(t)$ and let P be a monic irreducible polynomial in $k[t]$, corresponding to a finite place v_P. Then $v_\infty(R') \geqslant v_\infty(R) + 1$ and*

$$v_P(R') \geqslant \begin{cases} v_P(R) - 1 & \text{if } v_P(R) \neq 0 \text{ in } k \\ v_P(R) & \text{else} \end{cases} \geqslant v_P(R) - 1. \tag{3.4.26}$$

In fact, (3.4.26) holds for any $R \in K_{v_P}$.

[26] Here we are using the fact that we have functorial morphisms $\mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K), \ker(\phi)) \to \mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K_v), \ker(\phi))$, in the sense that they commute with the boundary maps $\partial : K/K^3 \to \mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K), \ker(\phi))$ and $\partial_v : K_v/K_v^3 \to \mathrm{H}^1_{\mathrm{flat}}(\mathrm{Spec}(K_v), \ker(\phi))$. We are also using the fact that Amitsur–Čech cohomology is *functorially* isomorphic to the flat cohomology.

[27] Note that the assumption $E[2](K) = \{0\}$ from proposition 3.4.12 is satisfied in our case because $x^3 + bx + a_6 = 0$ cannot have a root $x \in K$ if a_6 is a polynomial of degree coprime to 3.

Remark 3.4.16. The last claim of lemma 3.4.15 holds because the derivative map $K \to K, f \mapsto f'$ is continuous with respect to the v-adic topology, for any finite place v. In fact, it is even uniformly continuous (so that it extends uniquely to a map $K_v \to K_v$). Indeed, we want to show that given any $\epsilon > 0$, there exists $\delta > 0$ such that for all $f, g \in K$ we have $|f - g|_v < \delta \implies |f' - g'|_v < \epsilon$. This amounts to showing that for all $N > 0$ there is $M \geqslant 0$ such that for all $f, g \in K$, we have $v_P(f - g) \geqslant N \implies v_P(f' - g') \geqslant M$. The above lemma 3.4.15 precisely shows that we may take $M := N - 1$. ⌟

Proof. — Write $R = A/B$ where $A, B \in k[t]$. Then $R' = \frac{A'B - AB'}{B^2}$ and

$$\begin{aligned}\deg(R') &\leqslant \max\{\deg(A'B), \deg(AB')\} - 2\deg(B) \\ &= \deg(A) + \deg(B) - 1 - 2\deg(B) = \deg(A) - \deg(B) - 1 \\ &= \deg(R) - 1.\end{aligned}$$

Let us turn to the result about v_P. First, notice that the displayed inequality holds if R is a polynomial: if $R = P^e \cdot S$ for some $e = v_P(R) \geqslant 0$ and some $S \in k[t]$ coprime to P, then $R' = eP^{e-1}S + P^eS'$ so

$$v_P(R') \geqslant \min\{e - 1 + v_P(e), e + v_P(S')\} \geqslant \begin{cases} e - 1 & \text{if } e = v_P(R) \neq 0 \text{ in } k \\ e & \text{else.} \end{cases} \tag{3.4.27}$$

In fact, the first inequality is an *equality*, since either $e = 0 \in k$ and $S' = 0$, or otherwise we have $v_P(e) \in \{0, +\infty\}$ so that $v_P(eP^{e-1}S) \neq v_P(P^eS')$.

Now let $R = A/B$ for some coprime polynomials $A, B \in k[t]$. Using the previous step for polynomials, we get $v_P(R') = v_P(A'B - AB') - 2v_P(B) \geqslant v_P(A) + v_P(B) - 1 - 2v_P(B) = v_P(R) - 1$. ■

Example 3.4.17. If $k = \mathbb{F}_2, S(t) = t^2 + 1$ and $P(t) = t$ then $R(t) = t^e(t^2 + 1)$ and $R'(t) = t^{e-1}(e(t^2+1)+2t^2) = et^{e-1}(t^2+1) \in \mathbb{F}_2[t]$. Therefore $v_t(R') = +\infty$ if e is even and $v_t(R') = e - 1$ if e is odd. If we work over $\mathbb{F}_p[t]$ with p odd and $p \mid e$, then $v_t(R') = e + 1$. ⌟

We will also need the following three lemmas.

Lemma 3.4.18. *Let k be a perfect field of characteristic p, set $K = k(t)$ and denote by K^p the additive subgroup of p-th powers in K. Then the kernel of the derivative map $K \to K, R \mapsto R'$ is exactly K^p. In particular, if $R \in K$ has zero derivative $R' = 0$, then $R \in K^p$ is a p-th power in K.* ⌟

Proof. — It is clear that any p-th power in K has a zero derivative. Conversely, let us write $R = P/Q$ for some coprime polynomials $P, Q \in k[t]$ and assume that $R' = 0$. Then $R' = \frac{P'Q - PQ'}{Q^2} = 0$ implies that $P'Q = PQ'$. Then P divides $P'Q$ and since $\gcd(P, Q) = 1$, we get $P \mid P'$, which forces $P' = 0$. Similarly, we get $Q' = 0$.

So we are left with proving the claim when $R = \sum_{i=0}^{N} a_i t^i$ is a polynomial, which is easy: if $R' = \sum_{i=0}^{N} i a_i t^{i-1} = 0$ then $ia_i = 0$ for all i, so we get $a_i = 0$ for all indices i coprime to p. Since k is perfect, $a_{pj} = b_j^p \in k$ is a p-th power for all $j \geqslant 0$, so that $R = \sum_{j=0}^{\lfloor N/p \rfloor} b_j^p t^{jp}$ is clearly a p-th power in K. ■

Lemma 3.4.19. *Let k be a finite field of characteristic p, let v be a finite place of $K = k(t)$ (corresponding to some monic irreducible polynomial $P \in k[t]$) and fix $x \in K$. Define $\mathcal{O}_{(v)} := \mathcal{O}_v \cap K$. If $v(x') \geqslant 0$ then $x \in \mathcal{O}_{(v)} + K^p$, that is: up to adding a p-th power, x is v-integral.* ⌟

Proof. — Let us write $x = x_0 + \sum_{i=1}^{N} \frac{f_i}{P^i}$ for some $x_0 \in \mathcal{O}_{(v_P)}$, $N \geqslant 0, f_i \in k[t]$ and $\deg(f_i) < \deg(P)$ for all i, as it can be done by "partial fraction decomposition" (which provides an explicit k-basis of $k(t)$) — note that possibly $f_i = 0$.

- Claim 1: $x_0' \in \mathcal{O}_{(v_P)}$.

  It is enough to show this for the elements of "the" k-basis of $k(t)$ provided by partial fraction decomposition. First, if $x_0 \in k[t]$ then it is clear that $v_P(x_0') \geqslant 0$. Now let us assume that $x_0 = \frac{f}{Q^e}$ where $f \in k[t], e \geqslant 1$ and $Q \neq P$ is irreducible (in particular, $v_P(Q) = 0$). Then $x_0' = \frac{g}{Q^{2e}}$ for some polynomial $g \in k[t]$. Thus $v_P(x_0') = v_P(g) - 2ev_P(Q) \geqslant 0 - 0 = 0$.

- Claim 2: if we let $s := \sum_{i=1}^{N} \frac{f_i}{P^i}$ then $v_P(s') \geqslant 0$ and $s \in K^p$ is a p-th power.

  If we had $v_P(s') < 0$ then, because $v_P(x_0') \geqslant 0$ (by the previous claim), it would follow that $v_P(x') = \min\{v_P(s'), v_P(x_0')\} < 0$, contradicting our assumption.

  Now, let us write $s = \frac{g}{P^N}$ for some polynomial $g \in k[t]$. Note that $g = \sum_{i=1}^{N} f_i P^{N-i}$ is not divisible by P (as the term with $i = N$ shows), i.e., $v_P(g) = 0$. Then using equation (3.4.27) (applied to $e := -N$) and the remark thereafter we get:

  $$v_P(s') = \min\{-N - 1 + v_P(-N),\ -N + v_P(g')\}.$$

  Observe that $-N-1+v_P(-N)$ is either $-N-1$, in which case it is $< -N+v_P(g')$ (since g is a polynomial), or it is $+\infty$. So we get either $v_P(s') = -N - 1 < 0$ or $v_P(s') = +\infty$. Since $v_P(s') \geqslant 0$, the only possibility is the latter, which means $s' = 0$ and thus $s \in K^p$ (by lemma 3.4.18) as desired.

Combining those two claims immediately concludes the proof. ■

Lemma 3.4.20. *Let k be a finite field of characteristic p and fix $y \in K := k(t)$. Assume that for every finite place $v \in V_K^0$, there is $s_v \in K$ such that $y - s_v^p \in \mathcal{O}_v$ (i.e., up to adding a p-th power in K, y is v-integral).*

Then there is $s \in K$ such that $y^* := y - s^p$ is a non-constant polynomial (this means that $y^* \in \mathcal{O}_v$ for every finite place $v \in V_K^0$, and that $[y] = [y^*] \in K/K^p$; said differently $[y]$ has a representative *which is a non-constant polynomial).* ⌟

Proof. — Let us write the partial fraction decomposition of $y \in K$ as

$$y = y_0 + \sum_{P} \sum_{j \geqslant 1} \frac{f_{P,j}}{P^j} \tag{3.4.28}$$

where $y_0, f_{P,j} \in k[t]$, P runs over monic irreducible polynomials, and $\deg(f_{P,j}) < \deg(P)$ for all j (and $f_{P,j} = 0$ for all but finitely many pairs P, j).

Let Q be a monic irreducible polynomial, corresponding to a finite place v_Q. Let us write $r_{v_Q} := \sum_{j\geqslant 1} \frac{f_{Q,j}}{Q^j} = \frac{f}{Q^d}$ for some $d \geqslant 1$ and where $Q \nmid f = \sum_{i=0}^{n} f_i t^i \in k[t]$. Note that f has degree $< d \cdot \deg(Q)$.

By assumption, there is some $s_{v_Q} \in K$ such that $y - s_{v_Q}^p \in \mathcal{O}_{v_Q}$. We may assume that $s_{v_Q} = \frac{g}{Q^e}$ for some $e \geqslant 1$ and $Q \nmid g = \sum_{i=0}^{m} g_i t^i \in k[t]$ (up to adding some v_Q-integral terms to s_{v_Q}). Note that g has degree $< e \cdot \deg(Q)$.

Writing $y = y_0 + r_{v_Q} + \sum_{P\neq Q} r_{v_P}$, we see that $y - r_{v_Q}$ is v_Q-integral. Then the element

$$r_{v_Q} - s_{v_Q}^p = \frac{f}{Q^d} - \frac{g^p}{Q^{p\cdot e}}$$

is v_Q-integral, which forces $d = p \cdot e$ and $v_Q(f - g^p) \geqslant p \cdot e$. If $f - g^p \neq 0$ then

$$p\cdot e\cdot \deg(Q) \leqslant \deg(f-g^p) \leqslant \max\{\deg(f), p\deg(g)\} < \deg(Q)\max\{d, pe\} \overset{d=pe}{=} p\cdot e\cdot\deg(Q),$$

which is a contradiction. Thereby, we must have $f = g^p$ and consequently $r_{v_Q} \in K^p$ is a p-th power.

Thus we get $y = y_0 + \underbrace{\sum_Q r_{v_Q}}_{\in K^p}$, we conclude that $y \equiv y_0 \pmod{K^p}$ where y_0 is a polynomial. Since all elements in k are p-th powers, we may assume that $y^* := y_0$ is non-constant, which finishes the proof. ■

We can now prove our result on the explicit description of the Selmer groups.

Proof of theorem 3.4.14. — 1. Let v be a finite place. Observe that because a_6 is a polynomial, it is v-integral.

- $\subseteq$. Let us fix $[y] \in S_\phi(E/K_v) \subset K/K^3$, which means that there is a point $P = (x, y) \in E(K_v)$ whose y-coordinate is the given element $y \in K$. We want to show that $y \in \mathcal{O}_v + K^3$ (i.e., there is some v-integral element $y^* \in \mathcal{O}_v$ such that $y \equiv y^* \mod K^3$).

  If $v(y) \geqslant 0$, then it is clear that $y \in \mathcal{O}_v \cap K$. From now on, assume that $v(y) < 0$. Then we have $v(x) < 0$ because otherwise $y^2 = x^3 + bx + a_6$ would be v-integral. Consequently,

  $$0 > 2v(y) = v(x^3 + bx + a_6) = \min\{v(x^3 + bx), v(a_6)\} = 3v(x)$$

  so there is $z \in \mathbb{Z}_{<0}$ such that $v(y) = 3z,\ v(x) = 2z < 0$.

  Differentiating both sides of the equation of E yields $2yy' = bx' + a_6'$. Therefore

  $$\begin{aligned} v(y') &= v(bx' + a_6') - v(y) \\ &\geqslant \min\{v(x'), v(a_6')\} - v(y) \\ &\geqslant 2z - 1 - 3z = -z - 1 \geqslant 0 \qquad \text{by lemma 3.4.15 applied to } x \in K_v \end{aligned} \tag{3.4.29}$$

  From lemma 3.4.19, it follows that $y \in \mathcal{O}_v + K^3$.

- $\supseteq$. Let $y \in \mathcal{O}_{(v)} := \mathcal{O}_v \cap K$ be v-integral. We prove the existence of a K_v-rational point $P_v = (x_0, y_0) \in E(K_v)$ whose y-coordinate is $y_0 \in K$ such that $y_0 \equiv y \pmod{K^3}$ (so that $\epsilon'_v(P_v) = [y] \in K/K^3$).

  We claim that there are v-integral elements $x_1, y_1 \in \mathcal{O}_{(v)}$ such that $y_1 \equiv y \mod K_v^3$ and $\eta := y_1^2 - (x_1^3 + bx_1 + a_6) \equiv 0 \bmod \mathfrak{m}_v$. From there we can check that that the point[28] (recall that $-b = \beta^2 \in k^\times$):

$$P_v := (x_0\ ,\ y_1), \quad \text{where} \quad x_0 := x_1 + \beta \sum_{m \geqslant 0} (b^{-1}\beta^{-1}\eta)^{3^m} \in \mathcal{O}_v$$

  is a K_v-rational point of E, since

$$\begin{aligned}
x_0^3 + bx_0 + a_6 &= x_1^3 + \beta^3 \sum_{m \geqslant 1} (b^{-1}\beta^{-1}\eta)^{3^m} + bx_1 + b\beta \sum_{m \geqslant 0} (b^{-1}\beta^{-1}\eta)^{3^m} + a_6 \\
&= x_1^3 - b\beta \sum_{m \geqslant 1} (b^{-1}\beta^{-1}\eta)^{3^m} + bx_1 + b\beta\Big(b^{-1}\beta^{-1}\eta + \sum_{m \geqslant 1} (b^{-1}\beta^{-1}\eta)^{3^m}\Big) + a_6 \\
&= x_1^3 - b\beta \sum_{m \geqslant 1} (b^{-1}\beta^{-1}\eta)^{3^m} + bx_1 + \eta + b\beta \sum_{m \geqslant 1} (b^{-1}\beta^{-1}\eta)^{3^m} + a_6 \\
&= x_1^3 + bx_1 + \eta + a_6 \\
&= y_1^2 \qquad \text{by definition of } \eta.
\end{aligned}$$

  Proving the existence of x_1, y_1 amounts to finding $s, x_1 \in \mathbb{F}_v := \mathcal{O}_v/\mathfrak{m}_v$ such that $(y + s^3)^2 \equiv x_1^3 + bx_1 + a_6$. The change of variables $x_1 = \tilde{x} + s^2 - \overline{y}^{1/3}s$ (where the reduction $\overline{y} \in \mathbb{F}_v$ of y has a unique cube root since $\mathbb{F}_v$ is a finite field of characteristic 3) yields:

$$y^2 + 2ys^3 + s^6 = (\tilde{x} + s^2 - \overline{y}^{1/3}s)^3 \ + \ b \cdot (\tilde{x} + s^2 - \overline{y}^{1/3}s) \ + \ a_6$$

  which can be rewritten as a cubic plane affine curve C over $\mathbb{F}_v$ in the variables $s, \tilde{x}$:

$$-bs^2 + b\overline{y}^{1/3}s = \tilde{x}^3 + b\tilde{x} + a_6 - y^2.$$

  It is easy to see that this curve is non-singular. Therefore, its projective closure $\overline{C}$ in $\mathbb{P}^2(\mathbb{F}_v)$ is an elliptic curve and so by the Hasse–Weil bound, we have

$$|C(\mathbb{F}_v)| = |\overline{C}(\mathbb{F}_v)| - 1 \geqslant |\mathbb{F}_v| - 2|\mathbb{F}_v|^{1/2} + 1 - 1 = (|\mathbb{F}_v|^{1/2} - 1)^2 - 1 > 0$$

  because we have $|\mathbb{F}_v| > 4$ (since we assumed $|k| > 3$ and $|k|$ must be a power of 3). Therefore this proves the existence of $x_1, y_1 \in \mathcal{O}_v$ as desired.

2. We now consider the infinite place $v = v_\infty$. Let $(x, y) \in E(K_v)$ be such that $y \in K$. Recall that $v_\infty(a_6) = -d < 0$ is coprime to 3. We have

$$\begin{aligned}
v(y^2) &= \min\{v(x^3 + bx), v(a_6)\} \\
&= \begin{cases} -d & \text{if } v(x^3 + bx) \geqslant -d, \\ 3v(x) < 0 & \text{else.} \end{cases}
\end{aligned}$$

  We split the analysis into 2 cases.

[28] Note that $|\eta|_v < 1$ so that x_0 indeed converges in $\mathcal{O}_v$.

- If $v(y) = -d/2$ then $v(x^3 + bx) \geqslant -d$ (because otherwise $v(y^2) = 3v(x) = -d$ would not be coprime to 3) so $v(x) \geqslant -d/3$. In fact, since d is coprime to 3 and $v(x)$ is an integer, we must have a strict inequality $v(x) > -d/3$.

  Therefore, we find

$$\begin{aligned} v(x^3 a_6^{-1}) &> -d - (-d) = 0 \\ v(x a_6^{-1}) &> -d/3 - (-d) > 0 \end{aligned}$$

  which implies that $x^3 a_6^{-1} \equiv -bx a_6^{-1} \equiv 0 \bmod \mathfrak{m}_v$ so $(x^3 + bx)a_6^{-1} = (y^2 - a_6)a_6^{-1} \equiv 0$ and hence $\boxed{y^2 a_6^{-1} \equiv 1 \bmod \mathfrak{m}_v}$ (and in particular $y^2 a_6^{-1} \in \mathcal{O}_v$ is v-integral).

- Otherwise we assume that $v(x^3 + bx) < -d$ (so that $v(y) < -\frac{d}{2}$), in which case $v(y) =: 3z < 0$ is a multiple of 3 and $v(x) = 2z$. In particular $v(x^3 + bx) = 6z < -d$ so $-3z > -\frac{d}{2}$. From equation (3.4.29) we know that

$$\begin{aligned} v(y') &\geqslant \min\{v(x'), -d + 1\} - v(y) \\ &= \begin{cases} v(x') - v(y) \geqslant 2z - 1 - 3z = -z - 1 \geqslant 0 & \text{if } v(x') \leqslant -d + 1, \\ -d + 1 - 3z > -d + 1 + \frac{d}{2} = -\frac{d}{2} + 1 & \text{else.} \end{cases} \end{aligned} \tag{3.4.30}$$

  Note that if $v(x') < -d + 1$, then we have an *equality* $v(y') = -d + 1 - 3z$.

  From lemma 3.4.20 and part 1) of theorem 3.4.14, we know that $y = y^* + s^3$ for some $y^* \in k[t] \smallsetminus k, s \in K$. We may assume (without loss of generality) that the coefficient of t^j in $y^* \in k[t]$ vanishes if $3 \mid j$, up to changing s. Since $v_\infty(y') = v_\infty((y^*)') < 0$, only the second case can occur in (3.4.30), which means that $\deg(y') = \deg((y^*)') < \frac{d}{2} - 1$, and consequently $\boxed{\deg(y^*) < \frac{d}{2}}$. Moreover, we have

$$\deg(y^*) = -v(y^*) = -v((y^*)') + 1 = -(-d + 1 - 3z) + 1 = d + 3z \equiv d \bmod 3. \tag{3.4.31}$$

  In that case, observe that we have

$$v(y) = 3z = \deg(y^*) - d. \tag{3.4.32}$$

  Finally, it suffices to combine the various items to conclude the proof. ∎

We deduce the following consequence from theorem 3.4.14 and its proof.

Corollary 3.4.21. *Let $E : y^2 = x^3 + bx + A_6$ be an elliptic curve over $K := k(t)$ where k is a finite field of characteristic 3. Assume that $|k| > 3$, that $-b = \beta^2 \in k^\times$ is a square in $k^\times$ and that $A_6 \in k[t]$ is a polynomial of degree d coprime to 3.*

Then the Selmer group $\mathrm{Sel}_\phi(E/K)$ is contained in the image in K/K^3 of the set $S(d)$ of polynomials $y \in k[t]$ of degree $D \leqslant d/2$ such that:

- *For every index j such that $3 \mid j$, the coefficient y_j of t^j in y vanishes, that is, $y_j = 0$.*
- *If $D < d/2$ then $D \equiv d \bmod 3$.*

- *If $D = d/2$ then $y^2 \cdot A_6^{-1} \equiv 1 \pmod{t^{-1}}$.*

More precisely, the reduction map $S(d) \to K/K^3$ is injective and its image contains *$S_\phi(E/K) \cong \mathrm{Sel}_\phi(E/K)$, which means that $|\mathrm{Sel}_\phi(E/K)| \leqslant |S(d)|$.* ⌟

Remark 3.4.22. If we take some element $[z] \in S_\phi(E/K) \hookrightarrow K/K^3$ where $z \in S(d)$ then $[z] \in S_\phi(E/K_{v_\infty}) \hookrightarrow K_{v_\infty}/K_{v_\infty}^3$ is equal to $\epsilon'_{v_\infty}(P) = [y]$ for some $P = (x, y) \in E(K_{v_\infty})$. Let us write $y = \sum_{j \leqslant d} y_j t^j \in K_{v_\infty} = k\big(\!\big(t^{-1}\big)\!\big)$ and $z = \sum_{r=0}^{D} z_r t^r \in k[t]$.

We have $y = z + s^3$ for some $s \in K_{v_\infty}$ so that taking derivatives yields $y' = z'$ and so we conclude that $y_j = z_j$ for all indices j coprime to 3. ⌟

3.4.4 Conclusion on Tate–Shafarevich groups

We finally prove theorem 3.4.1.

Proof of theorem 3.4.1. — First of all, recall from equation (3.4.13) that the Tate–Shafarevich group of E over K is trivial if and only if $|E(K)/\phi(E(K))| = |\mathrm{Sel}_\phi(E/K)|$. Thanks to proposition 3.4.3.2 and since the Selmer group is a finite-dimensional $\mathbb{F}_3$-vector space (seen as a subgroup of K/K^3), we deduce that

$$Ш(E/K) = \{0\} \iff \dim_{\mathbb{F}_3} \mathrm{Sel}_\phi(E/K) = \frac{\mathrm{rk}(E(K))}{2}. \tag{3.4.33}$$

Under the hypothesis on b, we know that $\mathrm{rk}(E(K)) = 2 \cdot 3^n$ by corollary 3.1.22. Also, note that in each case the field of constants $k = \mathbb{F}_{3^{2n}}$ has size > 3 so that the hypothesis from theorem 3.4.14 is fulfilled.

1. Let $n = 1$. In that case, the statement was already proved (in two ways: using the E_6-lattice, or using the fact that $|Ш|$ is always a square of an integer; see remark 3.4.2 and the discussion preceding it). We now give a third proof: first, $d = 3^n + 1 = 4$ and $k = \mathbb{F}_{3^{2n}}$ so $S(d) = \{\, a_1 t + a_2 t^2 \;:\; a_i \in k, a_2^3 = a_2 \,\}$ has size $|k| \cdot 3 = 3^{2n+1}$. Thus from theorem 3.4.14 and remark 3.4.5 we get

$$\mathrm{rk}(E(K))/2 = 3^n = 3 \leqslant \dim_{\mathbb{F}_3} \mathrm{Sel}_\phi(E/K) \leqslant \dim_{\mathbb{F}_3}(S(d)) = 2n + 1 = 3,$$

   thus equality holds and consequently, we find that $Ш(E/K) = \{0\}$ is trivial as claimed, thanks to the equivalence (3.4.33).

2. Let $n = 2$. Then $d = 3^n + 1 = 10$ so that $S(d) = \{\, a_1 t + a_2 t^2 + a_4 t^4 + a_5 t^5 \;:\; a_i \in k, a_5^3 = a_5 \,\}$ has size $|k|^3 \cdot 3 = 3^{3 \cdot 2n+1} = 3^{13}$. We get

$$\mathrm{rk}(E(K))/2 = 3^n = 9 \;\leqslant\; \dim_{\mathbb{F}_3} \mathrm{Sel}_\phi(E/K) \;\leqslant\; \dim_{\mathbb{F}_3}(S(d)) = 13,$$

   which is not sharp, so we need further conditions on the elements of $\mathrm{Sel}_\phi(E/K)$ to conclude. For instance we cannot have $a_5 = a_4 = 0 \neq a_2$ since the degree (if $< d/2 = 5$) must be $\equiv d = 1 \pmod 3$ by corollary 3.4.21.

   By using the points $(0, \pm t^5) \in E(K)$ (which get mapped to $\pm t^5$ via $\epsilon' = -a_4^3 \epsilon : E(K) \to K/K^3, (x, y) \mapsto [y]$), we know that if $[a_1 t + a_2 t^2 + a_4 t^4 + a_5 t^5] \in S_\phi(E/K)$ then $[a_1 t + a_2 t^2 + a_4 t^4] \in S_\phi(E/K)$ because $a_5 \in \{\pm 1, 0\}$ by the condition $a_5^3 = a_5$.

Let us take $y^* := a_1 t + a_2 t^2 + a_4 t^4 \in S(d) \subset k[t]$ such that $[y^*] \in S_\phi(E/K) \subset K/K^3$. Note that corollary 3.4.21 ensures that $\deg(y^*) \equiv d \equiv 1 \pmod 3$. We use remark 3.4.22 to get conditions on the coefficients a_j, by distinguishing 2 cases:

- Assume that $\deg(y^*) = 4$. We have $[y^*] = [y] \in K_{v_\infty}/K_{v_\infty}^3$ for some $P = (x, y) \in E(K_{v_\infty})$. Moreover, equation (3.4.32) ensures that $\deg(y) = 6$. Let us write $y = \sum_{j=-\infty}^{6} y_j t^j$ with $y_6 \neq 0$. From remark 3.4.22, we know that $y_j = 0$ whenever $j < 0$ is not divisible by 3.

  Using lemma 3.3.2 applied to $z := y^2 - t^{10} \in K_{v_\infty} = k\big(\!\big(t^{-1}\big)\!\big)$, we know that if $j > d/p = 12/3 = 4$ is coprime to 3, then $f_j = 0$ (using the notation from this lemma). This gives[29] $y_5 = 0$, $y_4 y_6 = -1$, $y_2 y_6 = y_4^2$, which yields $y_2 = y_6^{-3} = -y_4^3$. Using remark 3.4.22, we deduce the relation $a_2 = -a_4^3$.

- Assume that $\deg(y^*) = 1$. We have $[y^*] = [y] \in K_{v_\infty}/K_{v_\infty}^3$ for some $P = (x, y) \in E(K_{v_\infty})$. Moreover, by equation (3.4.32) we have $\deg(y) = -v(y) = d - \deg(y^*) = 9$. Let us write $y = \sum_{j \leqslant 9} y_j t^j$ with $y_9 \neq 0$.

  Using lemma 3.3.2 applied to $z := y^2 - t^{10}$, we know that if $j > d/p = 12/3 = 4$ is coprime to 3, then $f_j = 0$ (using the notation from this lemma). This gives $y_8 = y_7 = y_5 = y_4 = y_2 = 0$, so in particular $y_2 = -y_4^3$ is also satisfied in this case.

All in all, we see that the Selmer group $\mathrm{Sel}_\phi(E/K)$ injects in

$$S' := \{\, a_1 t + a_2 t^2 + a_4 t^4 + a_5 t^5 \;:\; a_i \in k,\ a_5^3 = a_5,\ a_2 = -a_4^3 \,\}$$

which is a space of cardinality $|S'| = 3 \cdot |k|^2 = 3^{1+2\cdot 2n} = 3^9$, so we find $\dim_{\mathbb{F}_3} \mathrm{Sel}_\phi(E/K) \leqslant \dim_{\mathbb{F}_3}(S') = 9$ and we can therefore conclude that $Ш(E/K)$ is trivial by (3.4.33).

3. Let $n = 3$. Then $d = 3^n + 1 = 28$ so that

$$\mathrm{Sel}_\phi(E/K) \hookrightarrow S(d) = \{a_1 t + a_2 t^2 + a_4 t^4 + a_5 t^5 + a_7 t^7 + a_8 t^8 + \\ + a_{10} t^{10} + a_{11} t^{11} + a_{13} t^{13} + a_{14} t^{14} \;\;;\;\; a_i \in k,\ a_{14}^3 = a_{14}\}.$$

Let us find extra constraints on the coefficients a_j of a polynomial $y^* := a_1 t + a_2 t^2 + a_4 t^4 + a_5 t^5 + a_7 t^7 + a_8 t^8 + a_{10} t^{10} + a_{11} t^{11} + a_{13} t^{13} + a_{14} t^{14} \in S(d) \subset K$ whose class modulo $(K^3, +)$ is in the Selmer group. Some steps are performed with SAGE [The21]; see the files in the folder `SAGE-Tate-Shafarevich-groups-in-characteristic-3` available at https://gitlab.com/gauthierleterrier/maths.

As before, using the rational points $(0, \pm t^{14}) \in E(K)$, we may assume that $a_{14} = 0$. Note that by corollary 3.4.21 we must have $\deg(y^*) \equiv d = 1 \pmod 3$ (since we assumed $a_{14} = 0$ so that $\deg(y^*) < d/2$), which implies that $\deg(y^*) \in \{1, 4, 7, 10, 13\}$. In any case, there is $(x, y) \in E(K_{v_\infty})$ such that $[y^*] = [y] \in K/K^3$. By equation (3.4.32), we have $v_\infty(y) = -\deg(y) = \deg(y^*) - 28$. We distinguish several cases.

- When $\deg(y^*) = 13$, then $\deg(y) = 15$. We get, from equation (3.3.6), $y_{11} = -y_{13}^3, y_8 = 0, y_5 = -y_{13}^9, y_2 = -y_{10}^3$. Note also that $y_j = 0$ for all $j < 0$ which are coprime to 3, and $y_{14} = 0$. Further we get the following relations, using the fact that the element

[29] See the files in `SAGE-Tate-Shafarevich-groups-in-characteristic-3` available at https://gitlab.com/gauthierleterrier/maths.

$z := y^2 - t^{28} \in K_{v_\infty}$ satisfies $z_j = 0$ for all $j > d/p = 10$ coprime to 3, thanks to lemma 3.3.2:

$$\begin{aligned}
y_{15} &= -y_{13}^{-1} \neq 0 \\
y_{12} &= y_{10}y_{13}^{-2} \\
y_9 &= (y_{13}^8 - y_{10}^2 + y_7y_{13}) \cdot y_{13}^{-3} \\
y_6 &= (-y_{10}y_{13}^8 + y_{10}^3 + y_7y_{10}y_{13} + y_4y_{13}^2) \cdot y_{13}^{-4} \\
y_3 &= (-y_{13}^{16} + y_{10}^2y_{13}^8 - y_7y_{13}^9 - y_{10}^4 - y_7^2y_{13}^2 + y_4y_{10}y_{13}^2 + y_1y_{13}^3) \cdot y_{13}^{-5} \\
y_0 &= (y_{10}y_{13}^{16} + y_{10}^3y_{13}^8 - y_7y_{10}y_{13}^9 - y_4y_{13}^{10} + y_{10}^5 - y_7y_{10}^3y_{13} + y_4y_7y_{13}^3 + y_1y_{10}y_{13}^3) \cdot y_{13}^{-6}.
\end{aligned}$$

We also have equations $f_j = 0$ for $j \in \{1, 2, 4, 5, 7, 8, 10\}$ using lemma 3.3.2. Let us denote by $\tilde{f}_j$ the numerator of f_j in $k[y_1, ..., y_{13}]$ (i.e., we get rid of the possible powers of y_{13} in the denominator). Using the above formulas for the y_i's when $3 \mid i$, we get a miraculously simple formula:

$$(-\tilde{f}_5 - \tilde{f}_7 \cdot y_{13}^3) + \tilde{f}_{10} \cdot y_{10}^3 \quad = \quad y_{10}^3 \cdot y_{13}^9 \cdot (-y_7^9 + b^3y_7) \quad = \quad 0$$

from which it follows that either $y_{10} = 0$ or $y_7^9 = b^3y_7$. Using remark 3.4.22, we deduce that the coefficients of y^* also satisfy $a_{10} \cdot (a_7^9 - b^3a_7) = 0$.

- When $\deg(y^*) = 10$, then $\deg(y) = 18$. Applying lemma 3.3.2 to $z := y^2 - t^{28} \in k\left(\left(t^{-1}\right)\right)$ yields equations, from which we find $y_5 = y_8 = y_{11} = y_{13} = y_{14} = y_{16} = y_{17} = 0$ together with $y_{10} = -y_{18}^{-1}, y_2 = y_{18}^{-3} = -y_{10}^3$ and

$$\begin{aligned}
y_{15} &= y_7y_{18}^2 \\
y_{12} &= y_7^2y_{18}^3 + y_4y_{18}^2 \\
y_9 &= y_7^3y_{18}^4 - y_4y_7y_{18}^3 + y_1y_{18}^2 \\
y_6 &= y_7^4y_{18}^5 + y_4^2y_{18}^3 - y_1y_7y_{18}^3 \\
y_3 &= y_7^5y_{18}^6 + y_4y_7^3y_{18}^5 - y_1y_4y_{18}^3.
\end{aligned}$$

Then the equation $f_{11} = 0$ from lemma 3.3.2 becomes $y_7^9y_{18}^3 - y_7y_{18}^3b^3 = 0$ so we get again the relation $y_7^9 = b^3y_7$. Using remark 3.4.22, we deduce that the coefficients of y^* also satisfy $a_7^9 = b^3a_7$.

- When $\deg(y^*) = 7$, then $\deg(y) = 21$. We know (since $(y^*)' = y'$ are equal derivatives, or by remark 3.4.22) that $y_j = 0$ for all $j > 7$ coprime to 3, and that $y_7 = a_7 \neq 0$. Moreover, using the equations from lemma 3.3.2 applied to $z = y^2 - t^{28}$, we get $y_2 = y_5 = 0$. Moreover we find:

$$\begin{aligned}
y_{21} &= -y_7^{-1} \\
y_{18} &= y_4y_7^{-2} \\
y_{15} &= (-y_4^2 + y_1y_7) \cdot y_7^{-3} \\
y_{12} &= (y_4^3 + y_1y_4y_7) \cdot y_7^{-4} \\
y_9 &= (-y_4^4 - y_1^2y_7^2) \cdot y_7^{-5}
\end{aligned}$$

from which $f_{14} = 0$ becomes $-y_7^8 + b^3 = 0$ so again we get the relation (using remark 3.4.22) $a_7^9 = b^3a_7$.

- When $\deg(y^*) = 4$, then $\deg(y) = 24$. Here we get $y_j = 0$ for any $j > 4$ coprime to 3, so in particular $y_8 = 0, y_{11} = 0 = y_{13}, y_2 = 0 = y_{10}$ and $y_7 = 0$ (which implies $y_7^9 = b^3 y_7$).
- When $\deg(y^*) = 1$, then $\deg(y) = 27$. Here we get $y_j = 0$ for any $j > 1$ coprime to 3, so the same equations as in the above item are still true.

All in all, we get an embedding of the Selmer group into a smaller *subset*[30] S' of polynomials:

$$\mathrm{Sel}_\phi(E/K) \hookrightarrow S' := \left\{ \sum_{j=1}^{14} a_j t^j \ : \ a_j \in k, \ \ a_{14}^3 = a_{14}, \ \ a_j = 0 \text{ if } 3 \mid j \quad ; \quad \begin{array}{c} a_{11} = -a_{13}^3, \ \ a_8 = 0, \\ a_5 = -a_{13}^9, \ \ a_2 = -a_{10}^3, \\ a_{10} \cdot (a_7^9 - b^3 a_7) = 0 \end{array} \right\}.$$

There are 9 possibilities[31] for a_7, 3 choices for a_{14}, and all the other coefficients are determined by $a_1, a_4, a_{10}, a_{13} \in k$. Thus $|S'| = 3|k|^2 \cdot (\underbrace{|k|}_{\substack{a_{10}=0 \\ a_7 \text{ arbitrary}}} + (|k| - 1) \cdot 9)$.

Henceforth, we obtain

$$\mathrm{rk}(E)/2 = 3^n = 27 \leqslant \dim_{\mathbb{F}_3} \mathrm{Sel}_\phi(E/K) \leqslant \log_3 |S'| < 27.0948$$

which means $\dim_{\mathbb{F}_3} \mathrm{Sel}_\phi(E/K) = 27 = \mathrm{rk}(E)/2$. Thanks to (3.4.33), we conclude that the Tate–Shafarevich group $Ш(E/K)$ is trivial in that case as well! ■

[30] Ideally, it should embed into a *subspace*, but we are not sure whether the condition $a_7^9 = b^3 a_7$ always holds in the case where $\deg(y) = 15$ (especially if $a_{10} = 0$).

[31] In general, if an element $b \in \mathbb{F}_{p^n}^\times$ (for some odd prime p and some $n \geqslant 1$) satisfies $\mathrm{N}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(b) = (-1)^{n+1}$ then $\#\{ a \in \mathbb{F}_{p^{2n}} \ : \ a^{p^2} = b^p \cdot a \} = p^2$. Indeed, it suffices to show that any root $a \in \overline{\mathbb{F}_p}$ of the separable polynomial $X^{p^2} - b^p X$ belongs to $\mathbb{F}_{p^{2n}}$, which can done following the proof of lemma 3.1.27.

Chapter 4

The family $y^2 = x^3 + b + b't^m$

In this chapter, we study how the rank of the elliptic curves $y^2 = x^3 + b + b't^m$ over $\mathbb{F}_q(t)$ behaves as we vary $m \geqslant 1$ and fix $b, b' \in \mathbb{F}_q^\times$, where q is a power of a prime $p \geqslant 5$. Interesting sphere packings associated to the narrow Mordell–Weil lattice of these curves were obtained in [Shi91], when the characteristic is $p \equiv -1 \bmod 6$. After computing the L-function of these curves (theorem 4.1.2 from section 4.1) in terms of triple Jacobi sums, we can actually recover the results from [Shi91] (see remark 4.1.11).

However, the case of characteristic $p \equiv 1 \bmod 6$ was not discussed in the cited paper. We show in section 4.2 (especially theorem 4.2.1) that under such a congruence condition on p, the rank of the curves $y^2 = x^3 + b + b't^m$ over $\mathbb{F}_q(t)$ is uniformly bounded (by 68), and we give more precise upper bounds in corollary 4.2.23. This is done by analyzing which Jacobi sums (appearing in the L-function of these curves) are *pure*, i.e., some non-zero power is an integer (see definition 4.2.5), using Stickelberger's theorem 1.4.22. This gives us more information about the geometric rank of these curves, which happens to be equal to the rank of the curve over $\mathbb{F}_{p^{2160}}(t)$ (see theorem 4.2.1).

Let k be a finite field of characteristic $p \geqslant 5$, let $b, b' \in k^\times$ and $m \geqslant 1$ be an integer. Let $E'_{m,b,b'}$ be the elliptic curve over $k(t)$ given by the short (affine) Weierstrass equation

$$E'_{m,b,b'} : y^2 = x^3 + b + b't^m \tag{4.0.1}$$

It is a Delsarte elliptic curve in the sense of definition 1.3.36, when m is coprime to $\mathrm{char}(k)$.

When $k \cong \mathbb{F}_q$ has q elements, we consider the narrow Mordell–Weil lattice $L'_{m,b,b',q} := E'_{m,b,b'}(\mathbb{F}_q(t))^0$. These lattices were considered for $b = b' = 1$ and some values of m, q in [Shi91].

The j-invariant of $E'_{m,b,b'}$ is 0. In particular, $E'_{m,b,b'}$ is isotrivial (but it is not trivial over $k(t)$, see remark 4.2.2). Moreover, the Birch–Swinnerton-Dyer conjecture 1.3.34 holds for $E'_{m,b,b'}$ over $k(t)$, either by theorem 1.3.35 (or by theorem 1.3.40 when m is coprime to $\mathrm{char}(k)$).

We remind the reader that a list of symbols can be found at the end of this work, on page 239. In particular, we will use the notations from definitions 1.4.1, 1.4.5 and 1.4.15; for instance k_j denotes the extension of degree $j \geqslant 1$ of a finite field k.

4.1 · L-function of $E'_{m,b,b'}$

We use the notation from section 1.4, especially definitions 1.4.1 and 1.4.12.

In order to state the main result about the L-function of $E'_{m,b,b'}$, we introduce the following notation.

Definition 4.1.1. 1. When $3 \mid \#k_s^\times$, we let $\psi_{k_s} \in \widehat{k_s^\times}[3]$ be the restriction of $\Theta^{\frac{\#k_s^\times}{3}}$ to $k_s^\times$, where Θ denotes the Teichmüller character. In other words, ψ_{k_s} has order exactly 3. (We have $\psi_{k_s} = \theta_{k_s,3,1}$, see also remark 1.4.19).

2. Assume that $|k| \equiv 1 \bmod 3$, so that ψ_{k_s} exists for every $s \geqslant 1$. Given $\epsilon \in \{\pm 1\}$, we define maps

$$\begin{aligned} \alpha'_{b,b',\epsilon} : \bigsqcup_{s\geqslant 1} \widehat{k_s^\times} &\longrightarrow \mathbb{C}^\times \\ \chi \in \widehat{k_s^\times} &\longmapsto \lambda_{k_s}(b)\chi(-bb'^{-1})\psi_{k_s}^\epsilon(-b)J(\psi_{k_s}^\epsilon, \chi, \lambda_{k_s}). \end{aligned} \tag{4.1.1}$$

3. For $\epsilon \in \{\pm 1\}$, define

$$X(m,\epsilon) := \begin{cases} \mathbb{Z}/m\mathbb{Z} \smallsetminus \{0\} & \text{if } 6 \nmid m \\ \mathbb{Z}/m\mathbb{Z} \smallsetminus \left\{0, \epsilon\frac{m}{6}\right\} & \text{if } 6 \mid m. \end{cases}$$

⌟

An explicit expression of the L-function is now given in the following result, which will be proved in subsection 4.1.2 in the case where $|k| \equiv 1 \bmod 3$ and subsection 4.1.3 in the case where $|k| \equiv -1 \bmod 3$.

Theorem 4.1.2 (theorem F). *Let k be a finite field of characteristic $\geqslant 5$, let $b, b' \in k^\times$ and $m \geqslant 1$ be an integer coprime to $|k|$. Let $E'_{m,b,b'}$ be the elliptic curve over $k(t)$ as in equation (4.0.1).*

1. If $|k| \equiv 1 \bmod 3$, then we have

$$L(E'_{m,b,b'}/k(t), T) = \prod_{\epsilon\in\{\pm1\}} \prod_{[r]\in X(m,\epsilon)/\langle|k|\rangle^\times} (1 - \alpha'_{b,b',\epsilon}(\theta_{k_{u(r)},m,r})T^{u(r)})$$

where $u(r) := u_{|k|,m}(r)$ (see section 1.4), $X(m,\epsilon)$, $\alpha'_{b,b',\epsilon}$ are as in the above definition 4.1.1 and where $[r]$ denotes the orbit of $r \in \mathbb{Z}/m\mathbb{Z}$ under the action of the multiplication of the powers of $|k|$ on $\mathbb{Z}/m\mathbb{Z}$.

2. If $|k| \equiv -1 \bmod 3$, then we have[1]

$$L(E'_{m,b,b'}/k(t), T) = \prod_{[r]\in X(m,1)/\langle|k_2|\rangle^\times} (1 - \alpha'_{b,b',1}(\theta_{k_{2u(r)},m,r})T^{2u(r)})$$

where[2] $u(r) := u_{|k_2|,m}(r)$. ⌟

[1] Notice that we have $|k_{2u(r)}| \equiv 1 \bmod 3$ for all r, so that $\alpha'_{b,b',1}(\theta_{k_{2u(r)},m,r})$ is well-defined (namely, the character $\psi_{k_{2u(r)}}$ of order 3 on $k_{2u(r)} = k'_{u(r)}$ does exist, where $k' := k_2$).

[2] Note the difference with the case $|k| \equiv 1 \bmod 3$ where we had set $u(r) := u_{|k|,m}(r)$ (and not $u(r) := u_{|k_2|,m}(r)$).

Remark 4.1.3. 1. When m is not coprime to $p := \mathrm{char}(k)$, one may use the (proof of the) second item of proposition 1.3.46 to determine the L-function of $E'_{m,b,b'}$ over $k(t)$. More precisely, let $v_p(m)$ be the p-adic valuation of m and set $m_1 := m/p^{v_p(m)}$. Let $b_1, b'_1 \in k^\times$ be the unique elements such that $b_1^{p^{v_p(m)}} = b$ and $b_1'^{\,p^{v_p(m)}} = b'$ (recall that the p-th power Frobenius map is a bijection on k; when $b, b' \in \mathbb{F}_p^\times$ we may take $b_1 = b$ and $b'_1 = b'$). Then the Frobenius morphism $\mathrm{Fr}_p^{v_p(m)} : E'_{m_1,b_1,b'_1} \longrightarrow E'_{m,b,b'}$ is an isogeny over $k(t)$, so the curves have the same L-function. In particular (by proposition 1.3.41 or because $E'_{m,b,b'}$ satisfies BSD conjecture 1.3.34), they also have the same algebraic rank.

2. When $|k| \equiv 1 \bmod 3$, the (analytic) rank of $E'_{m,b,b'}$ over $k(t)$ is always even. (This is not true if $|k| \equiv -1 \bmod 3$: when $k = \mathbb{F}_5, m = 2, b = b' = 1$, the rank is 1).

   Indeed, observe that for every multiplicative character χ, we have $\alpha'_{b,b',-1}(\chi) = \overline{\alpha'_{b,b',1}(\overline{\chi})}$, where $\bar{\cdot}$ denotes the complex conjugation. Moreover, we have $\overline{\theta_{k_{u(r)},m,r}} = \theta_{k_{u(r)},m,-r}$ (and $u(r) = u(-r)$) and $r \in X(m,-1) \iff -r \in X(m,1)$. Thus, we have $\alpha'_{b,b',-1}(\theta_{k_{u(r)},m,r}) = |k|^{u(r)}$ (i.e., this index $r \in X(m,-1)$ has a contribution of $+1$ to the analytic rank) if and only if $\alpha'_{b,b',1}(\theta_{k_{u(r)},m,-r}) = |k|^{u(r)}$.

3. As we have explained at the beginning of the proof of proposition 1.4.26, the coefficient $\alpha'_{b,b',\epsilon}(\theta_{k_{u(r)},m,r})$ appearing in theorem 4.1.2 does not depend on the choice of a representative r of the orbit $[r] \in X(m,\epsilon)/\langle |k| \rangle^\times$. ⌟

4.1.1 Reduction types and local term at the infinite place

The places of bad reduction of $E'_{m,b,b'}$ are easily analyzed using Tate's algorithm; the results are actually already given in [Shi91, lemma 3.1].

Proposition 4.1.4. *Consider the elliptic curve $E'_{m,b,b'}$ over $k(t)$ as in equation (4.0.1). Assume that m is coprime to $\mathrm{char}(k)$. Then the discriminant of the given Weierstrass equation is $-16 \cdot 27(b't^m + b)^2$, and the bad places are given as follows.*

- *At places $v \mid (b't^m + b)$, the reduction type of $E'_{m,b,b'}$ is* II, *so that $c_v = 1, v(\Delta_v) = 2, f_v = 2$. Moreover equation (4.0.1) is a minimal integral Weierstrass model of $E'_{m,b,b'}$ at v.*
- *At $v = \infty$, let $\pi := t^{-1}$ and $a := \lceil m/6 \rceil$. Then the change of variables $(x, y) \mapsto (\tilde{x}, \tilde{y}) = (\pi^{2a}x, \pi^{3a}y)$ gives a minimal integral Weierstrass model $\tilde{y}^2 = \tilde{x}^3 + b\pi^{6a} + b'\pi^{6a-m}$ at v. Morever the reduction of $E'_{m,b,b'}$ is:*
  - *good if $m \equiv 0 \pmod 6$.*
  - *type* II^* *if $m \equiv 1 \pmod 6$, so $c_v = 1, v(\Delta_v) = 10, f_v = 2$.*
  - *type* IV^* *if $m \equiv 2 \pmod 6$, so $v(\Delta_v) = 8, f_v = 2$ and $c_v = 3$ if b' is a square in k.*
  - *type* I_0^* *if $m \equiv 3 \pmod 6$, so $v(\Delta_v) = 6, f_v = 2$ and $c_v = 4$ if $-b'$ has 3 cube roots in k.*
  - *type* IV *if $m \equiv 4 \pmod 6$, so $v(\Delta_v) = 4, f_v = 2$ and $c_v = 3$ if b' is a square in k.*
  - *type* II *if $m \equiv 5 \pmod 6$, so $c_v = 1, v(\Delta_v) = 2, f_v = 2$.*
- *All other places v are of good reduction, so that $c_v = 1$ and $f_v = v(\Delta_v) = 0$.*

In particular, the degree of the minimal discriminant is $\deg\left(\Delta_{\min}(E'_{m,b,b'}/k(t))\right) = 2m + 2\epsilon = 12\lceil m/6\rceil$ *and* $f(E'_{m,b,b'}/k(t)) = 2m + 2\delta$*, where* $\epsilon \in \{0, ..., 5\}$ *is such that* $\epsilon \equiv 6 - m \pmod 6$*, and* $\delta = 0$ *if* $6 \mid m$ *and* $\delta = 1$ *otherwise.* ⌟

We state some more properties of $E'_{m,b,b'}$ as given in Shioda's paper [Shi91].

Proposition 4.1.5. *Let* $E'_{m,b,b'}$ *and* k *be as in proposition 4.1.4 (in particular, we assume that* $\gcd(m, \mathrm{char}(k)) = 1$*).*

1. *The curve* $E'_{m,b,b'}$ *is isotrivial; in fact it has a constant sextic twist.*
2. *The torsion subgroup of* $E'_{m,b,b'}(k(t))$ *is trivial.*
3. *The index of the narrow Mordell–Weil lattice* $E'_{m,b,b'}(k(t))^0$ *in* $E'_{m,b,b'}(k(t))$ *is equal to* $c_\infty(E'_{m,b,b'}/k(t))$. ⌟

Proof. — 1. We have already seen that $E'_{m,b,b'}$ is isotrivial since its j-invariant is 0. If we let $u \in \overline{k(t)}$ be such that $u^6 = b't^m + b$ then the change of variables $(x, y) \mapsto (x' = xu^{-2}, y' = yu^{-3})$ shows that $E'_{m,b,b'}$ is a sextic twist of the constant curve $w^2 = z^3 + 1$.

2. This is [Shi91, proposition 3.7].

3. This is [Shi91, corollary 4.7 and equation (3.5)]. ■

Consider the local term at $v = \infty$ given by equation (1.3.9) (for any $s \geqslant 1$):

$$A_{E'_{m,b,b'}}(\infty, k_s) := |k_s| + 1 - |\overline{(E'_{m,b,b'})_\infty}(k_s)|.$$

When $6 \mid m$, it can be expressed via Jacobi sums (introduced in definition 1.4.5).

Proposition 4.1.6. *Let* $m \geqslant 1$ *be coprime to* $\mathrm{char}(k)$*. Then for every* $s \geqslant 1$*, we have* $A_{E'_{m,b,b'}}(\infty, k_s) = 0$ *if* $6 \nmid m$*, and if* $6 \mid m$ *we have*

$$A_{E'_{m,b,b'}}(\infty, k_s) = -\lambda_{k_s}(b') \sum_{\psi \in \widehat{k_s^\times}[3] \smallsetminus \{\mathbb{1}\}} \psi(-b') J(\lambda_{k_s}, \psi).$$ ⌟

Proof. — First, we note that the minimal integral Weierstrass model of $E := E'_{m,b,b'}$ at ∞ is $y^2 = x^3 + b\pi^{6\alpha} + b'\pi^{6\alpha - m}$, where $\pi := t^{-1}, \alpha := \lceil m/6\rceil$. By proposition 4.1.4, we know that E has additive reduction at ∞ if $6 \nmid m$, and good reduction otherwise. In particular, if $6 \nmid m$ then we get $A(\infty, k_s) = 0$ for every $s \geqslant 1$.

When $6 \mid m$, then the reduction $\overline{E'_\infty}$ is $y^2 = x^3 + b'$, which implies that

$$\begin{aligned} A_{E'_{m,b,b'}}(\infty, k_s) &= -\sum_{x \in k_s} \lambda_{k_s}(x^3 + b') \\ &= -\sum_{x' \in k_s} \sum_{\psi \in \widehat{k_s^\times}[3]} \lambda(x' + b')\psi(x') \\ &= -\lambda_{k_s}(b') \sum_{\psi \in \widehat{k_s^\times}[3]} \psi(-b') J(\lambda, \psi). \end{aligned}$$

Finally, we may run the sum over those characters ψ that are *non-trivial*, since a Jacobi sum involving exactly one trivial character is 0 by proposition 1.4.6. ■

Let us assume that m is coprime to $\mathrm{char}(k)$. From proposition 4.1.4, we know that equation (4.0.1) is a minimal integral model of $E'_{m,b,b'}$ at every place $v \neq \infty$. Therefore, proposition 1.3.29 yields

$$\log L(E'_{m,b,b'}/k(t), T) = \sum_{s \geqslant 1} c_{m,b,b'}(s) \frac{T^s}{s} \tag{4.1.2}$$

$$\text{where } c_{m,b,b'}(s) := A_{E'_{m,b,b'}}(\infty, k_s) - \sum_{x,t \in k_s} \lambda_{k_s}(x^3 + b + b't^m). \tag{4.1.3}$$

We can express these coefficients $c_{m,b,b'}(s)$ in terms of Jacobi sums.

Proposition 4.1.7. *Let k be a finite field of characteristic $p \geqslant 5$, fix $b, b' \in k^\times$ and let $m \geqslant 1$ be coprime to p. Then for all integers $s \geqslant 1$ one has:*

$$c_{m,b,b'}(s) = -\lambda_{k_s}(b) \sum_{\substack{\chi^m = \mathbb{1} = \psi^3 \\ \psi, \chi, \chi\psi\lambda \neq \mathbb{1}}} \chi(-bb'^{-1})\psi(-b) J(\chi, \psi, \lambda_{k_s}). \qquad \lrcorner$$

Proof. — We first study the following sum (using proposition 1.4.3):

$$\begin{aligned}
\sum_{x,t \in k_s} \lambda_{k_s}(x^3 + b + b't^m) &= \sum_{\substack{\chi \in \widehat{k_s^\times}[m] \\ \psi \in \widehat{k_s^\times}[3]}} \sum_{x', z' \in k_s} \lambda(x' + b + b'z')\chi(z')\psi(x') \\
\boxed{x' = -bx'', z' = -bz''} \to &= \sum_{\substack{\chi \in \widehat{k_s^\times}[m] \\ \psi \in \widehat{k_s^\times}[3]}} \sum_{x'', z' \in k_s} \lambda(-bx'' + b - bb'z'')\chi(-bz'')\psi(-bx'') \\
\boxed{x = x'', z = b'z''} \to &= \lambda_{k_s}(b) \sum_{\substack{\chi \in \widehat{k_s^\times}[m] \\ \psi \in \widehat{k_s^\times}[3]}} \chi(-bb'^{-1})\psi(-b) \sum_{x,z \in k_s} \lambda(-x + 1 - z)\chi(z)\psi(x) \\
&= \lambda_{k_s}(b) \sum_{\substack{\chi \in \widehat{k_s^\times}[m] \\ \psi \in \widehat{k_s^\times}[3]}} \chi(-bb'^{-1})\psi(-b) J(\chi, \psi, \lambda_{k_s}).
\end{aligned}$$

Note that this sum is 0 if $3 \nmid \#k_s^\times$, because in that case ψ has to be the trivial character and the corresponding Jacobi sum vanishes. Moreover, we may run the sum over those characters χ, ψ that are *non-trivial*, since a Jacobi sum involving a trivial character and the Legendre symbol (which is non-trivial) is 0 by proposition 1.4.6.

We note that when $\chi\psi\lambda = \mathbb{1}$ and $\chi, \psi \neq \mathbb{1}$, then $J(\chi, \psi, \lambda_{k_s}) = -\chi(-1)J(\psi, \lambda_{k_s})$ by proposition 1.4.6. If $\psi \neq \mathbb{1}$, then ψ has order exactly 3, so that $\chi = \psi^{-1}\lambda$ has order exactly $6 = \mathrm{lcm}(3, 2)$ in which case we have $6 \mid m$.

In other words, we have (using the identity $\chi(-bb'^{-1}) = \psi^{-1}\lambda(-bb'^{-1})$ when $\chi\psi\lambda = \mathbb{1}$)

$$\begin{aligned}
&\lambda_{k_s}(b)^{-1} \sum_{x,t \in k_s} \lambda_{k_s}(x^3 + b + b't^m) \\
&= \sum_{\substack{\chi^m = \mathbb{1} = \psi^3 \\ \psi, \chi, \chi\psi\lambda \neq \mathbb{1}}} \lambda_{k_s}(b)^{-1}\lambda_{k_s}(x^3 + b + b't^m) \; + \sum_{\substack{\chi^m = \mathbb{1} = \psi^3 \\ \psi, \chi \neq \mathbb{1}, \chi\psi\lambda = \mathbb{1}}} \lambda_{k_s}(b)^{-1}\lambda_{k_s}(x^3 + b + b't^m)
\end{aligned}$$

$$= \sum_{\substack{\chi^m=\mathbb{1}=\psi^3 \\ \psi,\chi,\chi\psi\lambda\neq\mathbb{1}}} \chi(-bb'^{-1})\psi(-b')J(\chi,\psi,\lambda_{k_s}) - \mathbb{1}_{6|m}\cdot \sum_{\psi^3=\mathbb{1}\neq\psi} \lambda(bb'^{-1})\psi(-b')J(\psi,\lambda_{k_s}).$$

Finally, we get (using the identity $\lambda(b'^{-1}) = \lambda(b')$)

$$\sum_{x,t\in k_s} \lambda_{k_s}(x^3+b+b't^m) = \lambda_{k_s}(b) \sum_{\substack{\chi^m=\mathbb{1}=\psi^3 \\ \psi,\chi,\chi\psi\lambda\neq\mathbb{1}}} \chi(-bb'^{-1})\psi(-b)J(\chi,\psi,\lambda_{k_s}) - \mathbb{1}_{6|m}\cdot \sum_{\psi^3=\mathbb{1}\neq\psi} \lambda(b')\psi(-b')J(\psi,\lambda_{k_s}).$$

Combining this with proposition 4.1.6 finishes the proof. ■

4.1.2 Case $|k| \equiv 1 \pmod 3$

We now assume that $|k| \equiv 1 \pmod 3$. In this case, the character ψ_{k_s} of order 3 (from definition 4.1.1) exists for every $s \geqslant 1$.

For every $s \geqslant 1$, we have from proposition 4.1.7:

$$\begin{aligned} c_{m,b,b'}(s) &= -\lambda_{k_s}(b) \sum_{\epsilon\in\{\pm1\}} \sum_{\substack{\chi^m=\mathbb{1} \\ \chi\neq\mathbb{1},\chi\neq\lambda_{k_s}\psi_{k_s}^{-\epsilon}}} \chi(-bb'^{-1})\psi_{k_s}^{\epsilon}(-b)J(\chi,\psi_{k_s}^{\epsilon},\lambda_{k_s}) \\ &= -\sum_{\epsilon\in\{\pm1\}} \sum_{\substack{\chi\in\widehat{k_s^\times}[m] \\ \chi\neq\mathbb{1},\chi\neq\lambda_{k_s}\psi_{k_s}^{-\epsilon}}} \alpha'_{b,b',\epsilon}(\chi) \end{aligned}$$

using the notations from definition 4.1.1.

Now, the map $\alpha'_{b,b',\epsilon}$ satisfies the two hypothesis from proposition 1.4.26, thanks to theorem 1.4.7 and proposition 1.4.6; this is very similar to the beginning of the proof of theorem 3.1.3 on page 124. To check the first hypothesis, note that $|k|$ is odd so $\lambda_{k_s}^{|k|} = \lambda_{k_s}$ and $|k| \equiv 1 \bmod 3$ implies $(\psi_{k_s}^{\epsilon})^{|k|} = \psi_{k_s}^{\epsilon}$, for all $s \geqslant 1$ and $\epsilon \in \{\pm1\}$.

Using equation (4.1.2), the above expression for $c_{m,b,b'}(s)$ and proposition 1.4.26, we deduce the result from theorem 4.1.2 in the case where $|k| \equiv 1 \bmod 3$. Note that when $6 \mid m$, the character $\chi := \lambda_{k_s}\cdot\psi_{k_s}^{-\epsilon} \in \widehat{k_s^\times}[m]$ is the restriction to $k_s^\times$ of the character

$$\Theta^{|k_s^\times|\cdot\left(\frac{1}{2}-\frac{\epsilon}{3}\right)} = \Theta^{|k_s^\times|\cdot\frac{3-2\epsilon}{6}} = \Theta^{|k_s^\times|\cdot\frac{\epsilon}{6}}$$

where the last equality can be checked for the two cases $\epsilon = +1$ and $\epsilon = -1$ (recalling that $\Theta^{|k_s^\times|}$ is trivial on $k_s^\times$). This is why we removed the element $\epsilon m/6 \in \mathbb{Z}/m\mathbb{Z}$ in the definition of $X(m,\epsilon)$ when $6 \mid m$, since the above expression of $c_{m,b,b'}(s)$ requires $\chi \neq \lambda_{k_s}\psi_{k_s}^{-\epsilon}$.

4.1.3 Case $|k| \equiv -1 \pmod 3$

We now assume that $|k| \equiv -1 \pmod 3$. In this case, we have $c(s) = 0$ for all odd $s \geqslant 1$, by proposition 4.1.7, since there is no character of order exactly 3 on $k_s^\times$ for all odd $s \geqslant 1$. Let $k' = k_2$ be the quadratic extension of k.

Remark 4.1.8. If $|k| \equiv -1 \pmod 3$, then for every $s \geqslant 1$, the characters $\lambda_{k'_s}$ and $\psi_{k'_s}$ are trivial on $k^\times$. Since $b, b' \in k$, we deduce that

$$\alpha'_{b,b',\epsilon}(\chi) = \chi(-bb'^{-1}) J(\psi^\epsilon_{k'_s}, \chi, \lambda_{k'_s}),$$

which implies that the L-function will depend *at most* on bb'^{-1} and not on both b, b'. ⌟

Thus if we set $c'_{m,b,b'}(s') := c_{m,b,b'}(2s')$ for all $s' \geqslant 1$, we have, in view of equation (4.1.2):

$$\log L(E'_{m,b,b'}/k(t), T) = \sum_{s \geqslant 1, s=2s' \text{ even}} c_{m,b,b'}(s)\frac{T^s}{s} = \sum_{s' \geqslant 1} c'_{m,b,b'}(s')\frac{T^{2s'}}{2s'}.$$

For all $s' \geqslant 1$, we have by proposition 4.1.7

$$\begin{aligned} c'_{m,b,b'}(s') = c_{m,b,b'}(2s') &= -\lambda_{k'_{s'}}(b) \sum_{\epsilon \in \{\pm 1\}} \sum_{\substack{\chi^m = \mathbb{1} \\ \chi \neq \mathbb{1}, \lambda_{k'_{s'}} \psi^{-\epsilon}_{k'_{s'}}}} \chi(-bb'^{-1}) \psi^\epsilon_{k'_{s'}}(-b) J(\chi, \psi^\epsilon_{k'_{s'}}, \lambda_{k'_{s'}}) \\ &= -\sum_{\epsilon \in \{\pm 1\}} \sum_{\substack{\chi^m = \mathbb{1} \\ \chi \neq \mathbb{1}, \lambda \psi^{-\epsilon}_{k'_{s'}}}} \alpha'_{b,b',\epsilon}(\chi). \end{aligned}$$

Here we consider the restriction of $\alpha'_{b,b',\epsilon}$ to the characters in $\widehat{k'^\times_s} = \widehat{k^\times_{2s}}$:

$$\alpha'_{b,b',\epsilon} : \bigsqcup_{s \geqslant 1} \widehat{k'^\times_s} \longrightarrow \mathbb{C}^\times.$$

Therefore, if we write $u(r) := u_{|k'|,m}(r)$, we get, following the proof of proposition 1.4.26:

$$\begin{aligned} \log L(E'_{m,b,b'}/k(t), T) = \sum_{s' \geqslant 1} c'(s')\frac{T^{2s'}}{2s'} &= -\sum_{\epsilon \in \{\pm 1\}} \sum_{s' \geqslant 1} \sum_{\substack{\chi^m = \mathbb{1} \\ \chi \neq \mathbb{1}, \lambda \psi^{-\epsilon}_{k'_{s'}}}} \alpha'_{b,b',\epsilon}(\chi)\frac{T^{2s'}}{2s'} \\ &= -\sum_{\epsilon \in \{\pm 1\}} \sum_{r \in X(m,\epsilon)} \sum_{s' \in u(r)\mathbb{Z}_{>0}} \alpha'_{b,b',\epsilon}(\theta_{k'_{s'},m,r})\frac{T^{2s'}}{2s'} \\ &= -\sum_{\epsilon \in \{\pm 1\}} \sum_{r \in X(m,\epsilon)} \sum_{\nu \geqslant 1} \alpha'_{b,b',\epsilon}(\theta_{k'_{u(r)},m,r})^\nu \frac{(T^{2u(r)})^\nu}{2u(r)\nu} \\ &= \frac{1}{2} \sum_{\epsilon \in \{\pm 1\}} \sum_{[r] \in X(m,\epsilon)/\langle |k'| \rangle} \log\left(1 - \alpha'_{b,b',\epsilon}(\theta_{k'_{u(r)},m,r}) T^{2u(r)}\right). \end{aligned}$$

This yields the following intermediate result.

Lemma 4.1.9. *Let k be a finite field of characteristic $\geqslant 5$ such that $|k| \equiv -1 \pmod 3$. Let $b, b' \in k^\times$ and $m \geqslant 1$ be coprime to $\mathrm{char}(k)$. Let $k' = k_2$ be the quadratic extension of k. Then we have*

$$L(E'_{m,b,b'}/k(t), T)^2 = \prod_{\epsilon \in \{\pm 1\}} \prod_{[r] \in X(m,\epsilon)/\langle |k'| \rangle} (1 - \alpha'_{b,b',\epsilon}(\theta_{k'_{u(r)},m,r}) T^{2u(r)}) \tag{4.1.4}$$

where $u(r) = u_{|k'|,m}(r)$. ⌟

We explain how to express the L-function itself and not just its square. Fix $\epsilon \in \{\pm 1\}$.

- First of all, for any finite extension F of $k' = k_2$ and any character $\chi \in \widehat{F^\times}$, we get from proposition 1.4.6

$$J(\chi, \psi_F^\epsilon, \lambda_F) = \frac{G(\psi_F^\epsilon)G(\lambda_F)G(\chi)}{G(\psi_F^\epsilon \lambda_F \chi)} = J(\psi_F^\epsilon, \lambda_F) \cdot J(\psi_F^\epsilon \lambda_F, \chi) \tag{4.1.5}$$

  whenever $\chi \neq \psi_F^{-\epsilon}\lambda_F$ (and we have $\psi_F^\epsilon \lambda_F \neq \mathbb{1}$ anyway).

  Since we assumed that $|k| \equiv -1 \pmod 3$, then we can apply Hasse–Davenport relation and Tate–Shafarevich theorem 1.4.8 to study the Jacobi sum $J(\psi^\epsilon_{k_{2u(r)}}, \lambda_{k_{2u(r)}})$, where $u(r) = u_{|k'|,m}(r)$. Consider the following field extensions:

$$\begin{array}{ccc} k_{u(r)} & \subset & k_{2u(r)} \\ \cup & & \cup \\ k & \subset & k_2 \end{array}$$

  We have

$$\begin{aligned} J(\psi^\epsilon_{k_{2u(r)}}, \lambda_{k_{2u(r)}}) &= J(\psi^\epsilon_{k_2} \circ \mathrm{N}_{k_{2u(r)}/k_2}, \lambda_{k_2} \circ \mathrm{N}_{k_{2u(r)}/k_2}) && \text{proposition 1.4.17} \\ &= -\big(-J(\psi^\epsilon_{k_2}, \lambda_{k_2})\big)^{u(r)} && \text{theorem 1.4.7} \\ &= -(-|k|)^{u(r)} && \text{theorem 1.4.8} \end{aligned}$$

  where the last step uses Tate–Shafarevich lemma and the fact that the restrictions of $\psi^\epsilon_{k_2}, \lambda_{k_2}$ to $k^\times$ are both trivial (the triviality of ψ_{k_2} on $k^\times$ requires[3] the assumption $|k| \equiv -1 \pmod 3$). In particular, $J(\psi^\epsilon_{k_{2u(r)}}, \lambda_{k_{2u(r)}})$ is always an integer when $|k| \equiv -1 \pmod 3$, hence a real number, that is: it is invariant under complex conjugation.

- Secondly, we claim that if $q := |k| \equiv -1 \pmod 3$ then

$$\overline{J(\psi^\epsilon_{k'_s}\lambda_{k'_s}, \chi)} = J(\psi^\epsilon_{k'_s}\lambda_{k'_s}, \chi^g) \tag{4.1.6}$$

  for any character $\chi : {k'_s}^\times \to \mathbb{C}^\times$ of order dividing m (i.e., $\chi \in \widehat{{k'_s}^\times}[m]$), where $g := (-q)^{-1} \bmod m$ (recall that we assume that $\gcd(m, \mathrm{char}(k)) = 1$).

  Indeed, we first note that $\overline{\chi(x)} = \chi^{-1}(x) = \chi^{g\cdot q}(x) = \chi^g(x^q)$ for every $x \in k_s^\times$, since $g \cdot q \equiv -1 \bmod m$. Moreover, we have $\lambda^q = \lambda = \lambda^{-1}$ since q is odd, and $\psi^q = \psi^{-1}$ since $\psi \in \widehat{k_s^\times}$ has order 3 and $q \equiv -1 \bmod 3$. Therefore, $(\psi^\epsilon\lambda)^q = (\psi^\epsilon\lambda)^{-1}$ and hence

$$\begin{aligned} \overline{J(\psi^\epsilon_{k'_s}\lambda_{k'_s}, \chi)} &= \sum_{x \in k'_s} (\psi^\epsilon_{k'_s}\lambda_{k'_s})^{-1}(1-x) \cdot \overline{\chi}(x) \\ &= \sum_{x \in k'_s} (\psi^\epsilon_{k'_s}\lambda_{k'_s})(1-x^q) \cdot \chi^g(x^q) \\ &= \sum_{x' \in k'_s} (\psi^\epsilon_{k'_s}\lambda_{k'_s})(1-x') \cdot \chi^g(x') \\ &= J(\psi^\epsilon_{k'_s}\lambda_{k'_s}, \chi^g). \end{aligned}$$

[3] Indeed, if $|k| \equiv -1 \pmod 3$, then the map $k^\times \to k^\times$ given by $x \mapsto x^3$ is injective and hence surjective, so that all elements of k are cubes, which implies that ψ_{k_2} is trivial on $k^\times$.

Observe that $\psi^{\epsilon}_{k'_s}(-b) = 1$ since $b \in k^\times$ and $\psi_{k'_s}$ is trivial on $k^\times$ whenever $|k| \equiv -1 \pmod 3$. As a result of the above two items, for every $\chi \in \widehat{k'^\times_s}[m]$ we get, using remark 4.1.8:

$$\begin{aligned}
\overline{\alpha'_{b,b',\epsilon}(\chi)} &= \overline{\chi}(-bb'^{-1}) J(\psi^{\epsilon}_{k'_s}, \lambda_{k'_s}) \cdot \overline{J(\psi^{\epsilon}_{k'_s}\lambda_{k'_s}, \chi)} && \text{by equation (4.1.5)} \\
&= \chi^g((-bb'^{-1})^q) J(\psi^{\epsilon}_{k'_s}, \lambda_{k'_s}) \cdot J(\psi^{\epsilon}_{k'_s}\lambda_{k'_s}, \chi^g) && \text{by equation (4.1.6)} \\
&= \alpha'_{b,b',\epsilon}(\chi^g) && \text{(since } b, b' \in k^\times\text{).}
\end{aligned}$$

where $g := (-q)^{-1} \bmod m$ and $q := |k|$. Note also that $\alpha'_{b,b',-1}(\chi) = \overline{\alpha'_{b,b',1}(\overline{\chi})}$, where $\bar{\cdot}$ denotes the complex conjugation. Therefore, we get

$$\begin{aligned}
&\prod_{[r]\in X(m,-1)/\langle |k'|\rangle} (1 - \alpha'_{b,b',-1}(\theta_{k'_{u(r)},m,r}) T^{2u(r)}) \\
&= \prod_{[r]\in X(m,-1)/\langle |k'|\rangle} (1 - \overline{\alpha'_{b,b',1}(\theta^{-1}_{k'_{u(r)},m,r})} T^{2u(r)}) \\
&= \prod_{[r]\in X(m,-1)/\langle |k'|\rangle} (1 - \alpha'_{b,b',1}(\theta^{-g}_{k'_{u(r)},m,r}) T^{2u(r)}) \\
&= \prod_{[r]\in X(m,-1)/\langle |k'|\rangle} \left(1 - \alpha'_{b,b',1}(\theta_{k'_{u(q^{-1}r)},m,q^{-1}r}) T^{2u(q^{-1}r)}\right) \\
&= \prod_{[r']\in X(m,1)/\langle |k'|\rangle} (1 - \alpha'_{b,b',1}(\theta_{k'_{u(r')},m,r'}) T^{2u(r')}),
\end{aligned}$$

where $u(x) = u_{q^2,m}(x)$ and we have set $r' := q^{-1}r \pmod m$ in the last line. Note that $q^{-1} \equiv -1 \pmod 6$ (since $q := |k|$ is odd and $q \equiv -1 \bmod 3$), so we have $q^{-1}X(m,-1) = X(m,1)$.

Henceforth, from equation (4.1.4) we get

$$L(E'_{m,b,b'}/k(t), T)^2 = \prod_{[r]\in X(m,1)/\langle |k'|\rangle} (1 - \alpha'_{b,b',1}(\theta_{k'_{u(r)},m,r}) T^{2u(r)})^2$$

Because the L-function has a constant coefficient equal to 1, we finally conclude

$$L(E'_{m,b,b'}/k(t), T) = \prod_{[r]\in X(m,1)/\langle |k'|\rangle} (1 - \alpha'_{b,b',1}(\theta_{k'_{u(r)},m,r}) T^{2u(r)})$$

which finishes the proof of theorem 4.1.2 in the case $|k| \equiv -1 \bmod 3$.

4.1.4 Some consequences and sphere packings

In characteristic $p \equiv 1 \bmod 3$, we cannot apply Tate–Shafarevich theorem 1.4.8 to get large analytic rank of $E'_{m,b,b'}$ over $\mathbb{F}_p(t)$, since the character $\psi_{k_{u(r)}}$ appearing in the L-function (see theorem 4.1.2) is not trivial on $k = \mathbb{F}_p$. In fact, the rank will actually be *bounded* when $m \geqslant 1$ varies, as we will show in theorem 4.2.1.

However, when k has characteristic $p \equiv -1 \bmod 3$, we can recover Shioda's result from [Shi91, theorem 1.2].

Corollary 4.1.10. *Let $p \geqslant 5$ be a prime and $m \geqslant 1$ be an integer coprime to p. Assume that there is some integer $\nu > 0$ such that $p^\nu \equiv -1 \bmod d(m)$ where $d(m) := \operatorname{lcm}(6, m)$. Let $k = \mathbb{F}_{p^{2\nu}}$ and let $b, b' \in \mathbb{F}^\times_{p^\nu}$.*

Then the (analytic) rank of $E'_{m,b,b'}$ over $k(t)$ equals

$$\rho = \begin{cases} 2m-4 & \text{if } 6 \mid m \\ 2m-2 & \text{if } 6 \nmid m \end{cases}$$

and the L-function is $L(E'_{m,b,b'}/k(t)) = (1-|k|T)^\rho$. In particular, the geometric rank of $E'_{m,b,b'}$ is equal to ρ. ⌟

Proof. — From theorem 4.1.2, using the fact that $|k| = p^{2\nu} \equiv 1 \bmod 3$, we know that the analytic rank is

$$\rho(E'_{m,b,b'}/k(t)) = \sum_{\epsilon\in\{\pm 1\}} \#\Big\{ [r] \in X(m,\epsilon)\Big/\langle |k| \rangle \ : \ \alpha'_{b,b',\epsilon}(\theta_{k_{u(r)},m,r}) = |k|^{u(r)} \Big\}.$$

where $u(r) := u_{|k|,m}(r) = 1$ for all r, since $p^\nu \equiv -1 \bmod m$.

Let $k' := \mathbb{F}_{p^\nu} \subset k$ and fix $r \in X(m,\epsilon)$. The assumption implies that $p^\nu \equiv -1 \bmod 3$ so it forces ν to be odd (and $p \equiv -1 \bmod 6$). By the second item of lemma 1.4.30 (applied to $d = m$ and $c = \nu$), we know that if $r \neq m/2$ when m is even, then $\theta_{k,m,r}$ is trivial on k', so $\theta_{k,m,r}(-bb'^{-1}) = 1$. If m is even and $r = m/2$, then $\theta_{k,m,r} = \lambda_k$ is the Legendre symbol, and $b, b' \in k'$ are necessarily squares in k, so we also have that $\theta_{k,m,r}$ is trivial on k' (so $\theta_{k,m,r}(-bb'^{-1}) = 1$) in that case. Moreover, we always have $\lambda_k(b) = 1$ since $b \in k'$.

Finally, since $p^\nu \equiv -1 \bmod 3$, any element of $\mathbb{F}_{p^\nu}^\times$ is a cube in $\mathbb{F}_{p^\nu}^\times$; in particular $-b$ is a cube in k' and hence in k. Because ψ_k has order 3, it follows that ψ_k is trivial on k'; in particular $\psi_k^\epsilon(-b) = 1$. Therefore we find

$$\alpha'_{b,b',\epsilon}(\theta_{k,m,r}) = J(\psi_k^\epsilon \ ; \ \theta_{k,m,r} \ ; \ \lambda_k) = G(\psi_k^\epsilon)\cdot G(\theta_{k,m,r})\cdot G(\lambda_k)\cdot G(\chi)^{-1}, \tag{4.1.7}$$

where $\chi := \psi_k^\epsilon \cdot \theta_{k,m,r} \cdot \lambda_k$ is non-trivial since $r \neq \epsilon m/6$ if $6 \mid m$ (recall that $r \in X(m,\epsilon)$), so we have been able to apply proposition 1.4.6. From the above discussion, we have seen that the four characters $\psi_k^\epsilon \ ; \ \theta_{k,m,r} \ ; \ \lambda_k$ and χ are trivial on k'. Therefore, Tate–Shafarevich theorem 1.4.8, together with (4.1.7), imply that $\alpha'_{b,b',\epsilon}(\theta_{k,m,r}) = |k|$ for all $r \in X(m,\epsilon)$. Therefore, we find[4]

$$\rho(E'_{m,b,b'}/k(t)) = \sum_{\epsilon\in\{\pm 1\}} \#X(m,\epsilon)$$

since $|k| = p^{2\nu} \equiv 1 \bmod m$ acts trivially (by multiplication) on $\mathbb{Z}/m\mathbb{Z}$. Therefore, we get the claimed formula for the rank (recall also that $E'_{m,b,b'}$ satisfies the Birch–Swinnerton-Dyer conjecture 1.3.34, so analytic and algebraic ranks agree).

The asserted expression of the L-function is also clear from here. Finally, the geometric rank must be equal to r, as it can be seen by repeating the argument with any finite extension k_n of k (the key point is that $|k_n| \equiv 1 \bmod \mathrm{lcm}(3,m)$). Alternatively, one may argue using the bound (1.3.12) from remark 1.3.33: we have $\rho(E'_{m,b,b'}/k(t)) = f(E'_{m,b,b'}) - 4$, using proposition 4.1.4. ■

[4] Similarly, using theorem 4.1.2, we find $\rho(E'_{m,b,b'}/\mathbb{F}_{p^\nu}(t)) = \left| X(m,1)\Big/\langle p^{2\nu}\rangle \right| = |X(m,1)|$.

Remark 4.1.11. We can recover some results from Shioda's work [Shi91], and give more computations for the packing densities of these Mordell–Weil lattices $L'_{m,b,b',p^{2e}}$, where $p^e \equiv -1 \pmod{\operatorname{lcm}(6,m)}$ and $b, b' \in \mathbb{F}_{p^e}^\times$. Note that $p^e \equiv -1 \bmod 3$ ensures that any element in $\mathbb{F}_{p^e}^\times$ (for instance $-b'$) has 3 cube roots, and moreover we know that b, b' are squares in $k := \mathbb{F}_{p^{2e}}$. Thus the Tamagawa number c_∞ of $E'_{m,b,b'}$ at $v = \infty$ is as indicated in proposition 4.1.4. From corollary 4.1.10 we know that $L^*(E'_{m,b,b'}/k(t)) = 1$ and proposition 4.1.5 ensures that $E'_{m,b,b'}(k(t))$ is torsion-free. Thus, by proposition 2.1.1, we get a lower bound on the center packing density of $L'_{m,b,b',p^{2e}}$ given by

$$\delta(L'_{m,b,b',p^{2e}}) \geqslant \frac{(\Delta/24)^{r/2}}{c_\infty^{1/2} \cdot |k|^{\Delta/24-1/2}}$$

where $\Delta := \deg\left(\Delta_{\min}(E'_{m,b,b'}/k(t))\right)$ is given in proposition 4.1.4 and $r := \operatorname{rk}(L'_{m,b,b',p^{2e}})$ is given in corollary 4.1.10. In particular, when $6 \mid m$, we get $\Delta = 2m, r = 2m-4, c_\infty = 1$ so that

$$\delta(L'_{m,b,b',p^{2e}}) \geqslant \frac{(m/12)^{m-2}}{p^{2e(m/12-1/2)}}.$$

When the rank r goes to infinity, the (non-normalized) packing density satisfies an asymptotic lower bound

$$D(L'_{m,b,b',p^{2e}}) \geqslant r^{-\frac{r}{12}(1+o(1))},$$

which is consistent with theorem 2.3.1, since by proposition 4.1.4 the Szpiro ratio of $E'_{m,b,b'}$ tends to 1, and by corollary 4.1.10, Brumer's bound is asymptotically achieved. It can be improved in some cases using better lower bounds on the size of the Tate–Shafarevich group, see remark 2.3.6.

Here are few examples of dense Mordell–Weil lattices $L'_{m,b,b',p^{2e}}$ where $b, b' \in \mathbb{F}_{p^e}^\times$, when p is small and $e = 1$ (see also remark 3.5 in [Shi91]):

m	p	$\operatorname{rk}(L'_{m,b,b',p^2})$	$\delta(L'_{m,b,b',p^{2e}})$
2	5	2	$\frac{1}{2\sqrt{3}} = \delta(A_2)$
3	5	4	$\frac{1}{8} = \delta(D_4)$
4	11	6	$\frac{1}{8\sqrt{3}} = \delta(E_6)$
6	5	8	$\frac{1}{16} = \delta(E_8)$
5	29	8	$\frac{1}{16} = \delta(E_8)$
12	11	20	$\frac{1}{11} < \delta(\Lambda_{20}) = \frac{1}{8}$

When $p = 17, m = 18$, the 32-dimensional narrow Mordell–Weil lattice has center density $\log_2(\delta) = 1.184$, a bit worse than the Quebbemann lattice Q_{32} which has $\log_2(\delta) = 1.359$.

Here is a table giving more examples of dense Mordell–Weil lattices $L'_{m,b,b',p^{2e}}$ where $b, b' \in \mathbb{F}_{p^e}^\times$. In some dimensions, they are the densest sphere packings known so far in their respective dimensions if the rank is $\leqslant 980$ (in particular, they have a greater density than Keith Ball's lower bound from theorem 1.2.16; in dimensions 1004,1016 and 1040 they still achieve a density greater than Minkowski's lower bound from theorem 1.2.15).

m	p	e	rank	$\log_2(\delta) \geqslant$
21	41	1	40	2.9273
24	23	1	44	8.4293
30	29	1	56	17.5821
36	71	1	68	23.14
38	113	1	74	25.1586
42	41	1	80	40.1489
48	47	1	92	53.1179
54	53	1	104	67.0127
57	113	1	112	67.6464
60	59	1	116	81.728
63	5	3	124	81.8269
69	137	1	136	96.6991
72	71	1	140	113.3002
80	239	1	158	118.2773
84	83	1	164	147.3276
87	173	1	172	144.9078
90	89	1	176	165.1461
96	191	1	188	168.3386
99	197	1	196	179.6185
102	101	1	200	202.2149
108	107	1	212	221.4071
114	113	1	224	241.0047
126	5	3	248	281.3317
132	131	1	260	302.0242
138	137	1	272	323.0477
147	293	1	292	334.3288
150	149	1	296	366.0307
168	167	1	332	432.6609
174	173	1	344	455.4031
180	179	1	356	478.3959
192	191	1	380	525.0997
198	197	1	392	548.7956

m	p	e	rank	$\log_2(\delta) \geqslant$
210	419	1	416	562.7234
216	431	1	428	586.0599
222	443	1	440	609.5979
225	449	1	448	624.5446
228	227	1	452	670.4493
234	233	1	464	695.3742
240	239	1	476	720.4851
252	251	1	500	771.2461
258	257	1	512	796.8875
264	263	1	524	822.6976
270	269	1	536	848.6723
282	281	1	560	901.1013
294	293	1	584	954.1469
312	311	1	620	1034.817
318	317	1	632	1061.9892
348	347	1	692	1199.8503
354	353	1	704	1227.8059
360	359	1	716	1255.8843
384	383	1	764	1369.3844
390	389	1	776	1398.0466
402	401	1	800	1455.7034
420	419	1	836	1542.9947
432	431	1	860	1601.7081
444	443	1	884	1660.8235
450	449	1	896	1690.5285
462	461	1	920	1750.2265
468	467	1	932	1780.217
480	479	1	956	1840.475
492	491	1	980	1901.0946
504	503	1	1004	1962.0669
510	509	1	1016	1992.6828
522	521	1	1040	2054.1686

⌟

Remark 4.1.12. The elliptic curves $E : y^2 = x^3 + t^{p^e} - t$ over $\mathbb{F}_{p^{2e}}(t)$ from [GU20] have narrow Mordell–Weil lattices with the same lower bound on the packing density as the lattices $L'_{p^e+1,b,b',p^{2e}}$, when $p^e \equiv -1 \bmod 12$ (and the same rank, namely $2(p^e - 1)$).

Note that they are both sextic twists of the same constant curve (in particular both are isotrivial), but it does not mean that those two curves are sextic twists of one another (they are only twists of each other over a compositum LL' where $[L : K] = [L' : K] = 6$). The two curves E and $E'_{p^e+1,1,1}$ are not isogenous over K since their conductors are different (they do not have the same places of bad reduction, as $v := t = 0$ shows). However the *degree* of the conductor is the same in both cases (namely $2(p^e + 1)$). ⌟

4.2 · Bounded ranks in characteristic $p \equiv 1 \bmod 3$

We have seen in corollary 4.1.10 that in given characteristic $p \equiv -1 \bmod 3$, the rank of $E'_{m,b,b'}$ over[5] $\mathbb{F}_{p^{2e}}(t)$ (hence over $\overline{\mathbb{F}_p}(t)$) can get arbitrarily large as we vary $m \geqslant 1$. The situation is not the same when $p \equiv 1 \bmod 3$. In this section, we are going to prove the following result (see subsection 4.2.3).

Theorem 4.2.1 (theorem G). *For any finite field k of characteristic $p \equiv 1 \pmod 3$, for all $b, b' \in k^\times$ and all integers $m \geqslant 1$ (not necessarily coprime to p), the rank of the elliptic curve $E'_{m,b,b'} : y^2 = x^3 + b + b't^m$ over $k_{2160}(t)$ is equal to its geometric rank and is at most 68 (where $k_n \subset \overline{k}$ denotes the extension of degree n as in definition 1.4.1).*

Moreover, if m is divisible by 360, then the rank of the elliptic curve $E'_{m,b,b'}$ over $k_{2160}(t)$ is equal *to 68.* ⌟

Remark 4.2.2.

- Equivalently, by proposition 1.3.46, this means that the curve $y^2 = x^3 + b + b't^{360}$ has rank 68 in the "Kummer family" of function fields $\mathbb{F}_{p^{2160}}(t^{1/m'})$ for all $m' \geqslant 1$, whenever $p \equiv -1 \bmod 3$.
- The geometric rank does not depend on the coefficients b, b' by remark 1.3.39.
- To our knowledge, this is the first *explicit* example of an (isotrivial) elliptic curve with *constant non-zero* rank on this Kummer family of function fields of positive characteristic. At the end of [Ulm07a, §6.6], it was conjectured that for all primes p there are elliptic curves[6] over $\mathbb{F}_p(t)$ which have bounded Mordell-Weil ranks in the "tower" $\overline{\mathbb{F}_p}(t^{1/d})$. It was proved for $p \in \{2, 3, 5, 7, 11\}$ in [Ulm07a, theorem 6.2] with (non-isotrivial) curves of rank 0. The work [Ber12, theorem 1.2] seems to answer the conjecture from [Ulm07a, §6.6], but here the (non-isotrivial) curves given in that work have rank 0.
- Note that theorem 4.2.1 involves the isotrivial elliptic curve $E'_{m,b,b'}$, which is *not* trivial over $k(t^{1/m})$, for any $m \geqslant 1$ coprime to $\mathrm{char}(k)$. Indeed, it is trivial if and only if there is some $u = \frac{f}{g} \in k(t)$ such that $1 + t^m = u^6$, where $f, g \in k[t]$ are coprime. This yields $g^6 \cdot (1 + t^m) = f^6 \in k[t]$ so that for all non-zero prime ideals $\mathfrak{p} \trianglelefteq k[t]$, the $\mathfrak{p}$-adic valuation of $1 + t^m$ is divisible by 6 and is non-negative. This means that $1 + t^m = u^6$ for a *polynomial* $u(t) \in k[t]$. Then taking derivatives on both sides yields $6u^5u' = mt^{m-1}$ so that the only factors of $u(t)$ are powers of t, i.e. $u(t) = \alpha t^d$ for some $\alpha \in k^\times$ and $d \geqslant 1$. But then the equality $1 + t^m = u(t)^6$ does not hold (as evaluating at $t = 0$ shows). ⌟

Remark 4.2.3. The work [Shi86, theorem 1] provides an algorithm to compute the geometric rank of any Delsarte elliptic curve (see definitions 1.3.11 and 1.3.36), as we will explain later in remark 4.2.33.

In particular, it is proved that $y^2 = x^3 + 1 + t^m$ has rank $\leqslant 68$ over $\mathbb{C}(t)$, and this is an equality if and only if $360 \mid m$; see [SS19, theorem 13.26] and [Hei11, §4.1, p. 26]. This holds also over $\overline{\mathbb{F}_p}(t)$ provided that $p \equiv 1 \bmod \mathrm{lcm}(6, m)$ (see the works [Usu01, p. 65] and

[5] What matters here is the characteristic, not the size of the base field, which is $p^{2e} \equiv +1 \bmod 3$ here!

[6] Non-isotriviality is probably assumed, or at the very least non-triviality over $\overline{\mathbb{F}_p}(t^{1/d})$ for any $d > 0$. If we take $E' : y^2 = x^3 + t$ over $\mathbb{F}_p(t)$, then E' is isotrivial and not trivial, but it becomes trivial over $k(t^{1/6})$, so the rank is obviously bounded in the family of fields $k(t^{1/m})$ (and the rank is 0 whenever $6 \mid m$ by remark 2.4.1).

[Usu00, Usu06, Usu08]; the point is that the sets $B_d^2(p)$ and B_d^2 defined in [Shi86, equations (2.7), (2.8)] are equal when $p \equiv 1 \bmod d$, see also [Shi86, theorem 7]).

But for fixed p, the condition $p \equiv 1 \bmod \mathrm{lcm}(6, m)$ is quite restrictive since this leaves us with finitely many m (while we want $m \geqslant 1$ to vary among all positive integers!). In some sense, we will show that the condition $p \equiv 1 \bmod 3$ suffices. Moreover, our approach allows to study the (analytic) rank of $E'_{m,b,b'}$ over $k(t)$ when k is a *finite* field, see corollary 4.2.23 (as opposed to when k is algebraically closed, which only gives the geometric rank). ⌟

Remark 4.2.4. We point out that the parity condition in from theorem 1.3.48 is not satisfied here, by proposition 4.1.4, which is indeed expected since the rank is *bounded* in the Kummer family $\{ E'_{m,b,b'}/k(t) \ : \ m \geqslant 1 \}$ if $\mathrm{char}(k) \equiv 1 \bmod 3$. ⌟

4.2.1 Pure Jacobi sums and geometric rank of elliptic curves

We start with the notion of *pure* exponential sum. Throughout, we fix a field embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

Definition 4.2.5. 1. Given an integer $n \geqslant 1$, we say that a complex number z is pure of degree n if $z \neq 0$ and $z^n \in \mathbb{R}$ is a real number. We say that z is *pure* if it is pure of degree n for some integer $n \geqslant 1$. (In particular, z^{2n} is equal to the positive real number $|z|^{2n}$).

2. For a field K, we denote by $\mu_\infty(K) \subset K^\times$ the subgroup of all roots of unity and by $\mu_n(K) := K^\times[n] \leqslant K^\times$ the subgroup of n-th roots of unity. When $K = \mathbb{C}$ or $K = \overline{\mathbb{Q}}$ we simply write μ_∞ and μ_n respectively. ⌟

Remark 4.2.6. If $z \in \mathbb{C}$ is pure, then there exists some integer $n \geqslant 1$ such that $\left(\frac{z}{|z|}\right)^n \in S^1 \cap \mathbb{R} = \{\pm 1\}$, where $S^1 \subset \mathbb{C}$ denotes the unit circle. This implies that $z = \zeta|z|$ where ζ is some $(2n)$-th root of unity. In particular, if the modulus $|z|$ is an integer, then $z^{2n} = |z|^{2n}$ is a positive *integer*. ⌟

Lemma 4.2.7. *Let k be a finite field. Let E be a non-constant elliptic curve over $k(t)$ which satisfies the Birch–Swinnerton-Dyer conjecture 1.3.34 over $k_n(t)$ for any $n \geqslant 1$. Let us write its L-function as $L(E/k(t), T) = \prod_{j=1}^{D}(1 - \omega_j T)$ where $\omega_j \in \overline{\mathbb{Q}}$ is a $|k|$-Weil number of weight 1, for each $j \in \{1, ..., D\}$ (as allowed by theorem 1.3.30).*

Define the set

$$P := \{ j \in \{1, ..., D\} \ : \ \omega_j \text{ pure} \}$$

and let $N \geqslant 1$ be an integer[7] *such that $\omega_j^N \in \mathbb{Z}_{>0}$ for each $j \in P$.*

Then the geometric rank of E over $k(t)$ is given by

$$\mathrm{rk}_{\mathbb{Z}}\, E(\overline{k}(t)) = \mathrm{rk}_{\mathbb{Z}}\, E(k_N(t)) = |P|.$$ ⌟

Proof. — Since E is non-constant, the group $E(\overline{k}(t))$ is finitely generated, and so there is some integer $M \geqslant 1$ such that $E(\overline{k}(t)) = E(k_M(t))$. Let $s_0 = \mathrm{lcm}(M, N)/N$ so that $N \cdot s_0$

[7] Such an integer exists since $|\omega_j| = |k| \in \mathbb{Z}_{>0}$ for all j, so that remark 4.2.6 applies.

is a multiple of M; in particular we have $E(\overline{k}(t)) = E(k_{N\cdot s_0}(t))$ and hence $\mathrm{rk}_{\mathbb{Z}}\, E(\overline{k}(t)) = \mathrm{rk}_{\mathbb{Z}}\, E(k_{Ns_0}(t))$.

Let $s \geqslant 1$ be an arbitrary integer. Since the ω_j's are $|k|$-Weil number of weight 1, for each $j \in P$ we must have $\omega_j^{N\cdot s} = |k|^{N\cdot s}$. On the other hand, if $j \notin P$, then $\omega_j^{N\cdot s} \neq |k|^{N\cdot s}$, because ω_j is not pure.

Since $E/k_{N\cdot s}(t)$ satisfies the BSD conjecture, it follows that, using proposition 1.3.43:

$$\mathrm{rk}_{\mathbb{Z}}\, E(k_{N\cdot s}(t)) = \operatorname*{ord}_{T=|k_{Ns}|^{-1}} L(E/k_{Ns}(t), T) = |P|.$$

In particular, applying the above equality to $s = s_0$ and $s = 1$, we get

$$\mathrm{rk}_{\mathbb{Z}}\, E(\overline{k}(t)) = \mathrm{rk}_{\mathbb{Z}}\, E(k_{Ns_0}(t)) = |P| = \mathrm{rk}_{\mathbb{Z}}\, E(k_N(t))$$

as desired. ■

In some cases, we can say a bit better, as the next lemma explains.

Lemma 4.2.8. *Let k be a finite field and E be a non-constant elliptic curve over $k(t)$ which satisfies the Birch–Swinnerton-Dyer conjecture 1.3.34. Assume that the L-function takes the form*

$$L(E/k(t), T) = \prod_{r=1}^{D'} (1 - \alpha(r) T^{u(r)})$$

for some $\alpha(r) \in \overline{\mathbb{Q}}$, some integers $u(r) \geqslant 1$ and some $D' \geqslant 1$, (note that we have $|\alpha(r)| = |k|^{u(r)}$ for all r). Let $P = \{\, r \in \{1, ..., D'\} \;:\; \alpha(r) \text{ is pure} \,\}$ and for all $r \in P$, fix an integer $M(r) \geqslant 1$ such that $\alpha(r)^{M(r)} \in \mathbb{Z}_{>0}$. Let $N \geqslant 1$ is an integer such that

$$\forall r \in P, \qquad M(r) \,\Big|\, \frac{N}{\gcd(N, u(r))}. \tag{4.2.1}$$

Then the rank of E over $k_N(t)$ equals $\sum_{r\in P} \gcd(N, u(r))$. In particular, if $N \geqslant 1$ satisfies

$$\forall r \in P, \qquad M(r) \cdot u(r) \mid N, \tag{4.2.2}$$

then the geometric rank is equal to the rank of E over $k_N(t)$, which is equal to $\sum_{r\in P} u(r)$. ⌟

We first explicitly write the L-function of the base change:

Lemma 4.2.9. *Assume that the L-function of an elliptic curve E over $k(t)$ takes the form*

$$L(E/k(t), T) = \prod_{r=1}^{D'} (1 - \alpha(r) T^{u(r)})$$

for some parameters $\alpha(r) \in \mathbb{C}, u(r) \in \mathbb{Z}_{\geqslant 1}$. Then for all $N \geqslant 1$ we have

$$L(E/k_N(t), T) = \prod_{r=1}^{D'} \left(1 - \alpha(r)^{\frac{N}{\gcd(N,u(r))}} T^{\frac{u(r)}{\gcd(N,u(r))}}\right)^{\gcd(N,u(r))}.$$ ⌟

Proof. — Let us write $\alpha(r) = |\alpha(r)|e^{i\theta(r)}$ for some unique $\theta(r) \in [0, 2\pi[$ so that

$$L(E/k(t), T) = \prod_{r=1}^{D'} \prod_{j=1}^{u(r)} (1 - |\alpha(r)|^{\frac{1}{u(r)}} e^{\frac{i\theta(r)}{u(r)}} \zeta_{u(r)}^j T)$$

where $\zeta_{u(r)} := \exp(2\pi i/u(r))$. Therefore proposition 1.3.43 yields

$$L(E/k_N(t), T) = \prod_{r=1}^{D'} \prod_{j=1}^{u(r)} (1 - |\alpha(r)|^{\frac{N}{u(r)}} e^{\frac{iN\theta(r)}{u(r)}} \zeta_{u(r)}^{N\cdot j} T).$$

Note that $\zeta_{u(r)}^N$ is a primitive root of unity of order $u'(r) := \frac{u(r)}{\gcd(u(r),N)}$, so we get

$$L(E/k_N(t), T) = \prod_{r=1}^{D'} \prod_{j=1}^{\frac{u(r)}{\gcd(u(r),N)}} \left(1 - |\alpha(r)|^{\frac{N}{u(r)}} e^{\frac{iN\theta(r)}{u(r)}} \zeta_{u(r)}^{N\cdot j} T\right)^{\gcd(u(r),N)}.$$

Finally, note that

$$\begin{aligned} |\alpha(r)|^{\frac{N}{u(r)}} e^{\frac{iN\theta(r)}{u(r)}} &= |\alpha(r)|^{\frac{N/\gcd(u(r),N)}{u(r)/\gcd(u(r),N)}} \cdot e^{\frac{iN\theta(r)/\gcd(u(r),N)}{u(r)/\gcd(u(r),N)}} \\ &= |\alpha_N(r)|^{\frac{1}{u(r)/\gcd(u(r),N)}} \cdot e^{\frac{i\theta_N(r)}{u(r)/\gcd(u(r),N)}} \end{aligned}$$

where $\alpha_N(r) := \alpha(r)^{\frac{N}{\gcd(u(r),N)}}$ and $\theta_N(r) := \frac{N}{\gcd(N,u(r))}\theta(r)$. Set $\zeta_{u'(r)} := \zeta_{u(r)}^N = \exp\left(2\pi i \frac{N/\gcd(u(r),N)}{u'(r)}\right)$, which is a primitive $u'(r)$-th root of unity. We finally get

$$\begin{aligned} L(E/k_N(t), T) &= \prod_{r=1}^{D'} \prod_{j=1}^{u'(r)} \left(1 - |\alpha_N(r)|^{\frac{1}{u'(r)}} e^{\frac{i\theta_N(r)}{u'(r)}} \zeta_{u'(r)}^j T\right)^{\gcd(u(r),N)} \\ &= \prod_{r=1}^{D'} \left(1 - \alpha_N(r) T^{u'(r)}\right)^{\gcd(u(r),N)}, \end{aligned}$$

since $\alpha_N(r) = |\alpha_N(r)| \cdot e^{i\cdot\theta_N(r)}$, which gives the claimed identity. ∎

Proof of lemma 4.2.8. — For every integer $H \geqslant 1$, the analytic rank over $k_H(t)$ is given by the order of vanishing of $L(E/k_H(t), T)$ at $T = |k_H|^{-1} = |k|^{-H}$. Moreover, observe that for any integers $q, v \geqslant 1$, the polynomial $1 - (qT)^v$ vanishes with order 1 at $T = q^{-1}$, while $(1 - qT)^v$ vanishes with multiplicity v (just take derivatives with respect to T).

Let $N \geqslant 1$ be such that (4.2.1) holds, and let $H = c \cdot N \geqslant 1$ be a multiple of N. Note that $\frac{H}{(H,u(r))} = \frac{cN}{(cN,u(r))}$ is a multiple of $\frac{cN}{(cN,cu(r))} = \frac{N}{(N,u(r))}$, hence a multiple of $M(r)$, for any $r \in P$. From lemma 4.2.9, we know that the analytic rank of E over $k_H(t)$ is

$$\rho(E/k_H(t)) = \sum_{r=1}^{D'} \gcd(H, u(r)) \cdot \mathbb{1}\left(\alpha(r)^{\frac{H}{(H,u(r))}} = |k_H|^{\frac{u(r)}{(H,u(r))}}\right).$$

We can run the above sum over $r \in P$, because when $r \notin P$, no non-zero power of $\alpha(r)$ can be an integer. Since $\frac{H}{(H,u(r))}$ is a multiple of $M(r)$ for all $r \in P$, and $\alpha(r)^{M(r)} = |k|^{u(r)\cdot M(r)}$, we get

$$\rho(E/k_H(t)) = \sum_{r\in P} \gcd(H, u(r)).$$

In particular, if N is a multiple of $u(r)$ for any $r \in P$ (i.e., it satisfies (4.2.2)), then the rank of E over $k_{c\cdot N}(t)$ equals $\sum_{r\in P} u(r)$ for any $c \geqslant 1$, so it is equal to the geometric rank of E. ■

Remark 4.2.10. In the specific cases of the curves $E_{m,b,b'}$ and $E'_{m,b,b'}$ we consider, one can prove lemma 4.2.9 in a different way, using the Hasse–Davenport relation from theorem 1.4.7 (and without using proposition 1.3.43).

Assume that there is some subset $X(d) \subset \mathbb{Z}/d\mathbb{Z}$ (for some $d \geqslant 1$) such that for *every* finite extension k'/k, the L-function is written as

$$L(E/k'(t), T) = \prod_{[r]\in X(d)/\langle |k'|\rangle^\times} \left(1 - \alpha(\theta_{k'_{u(r)},d,r})T^{u(r)}\right),$$

where $u(r) := u_{|k'|,d}(r)$ and $\alpha : \bigsqcup_{n\geqslant 1} \widehat{k_n^\times} \to \mathbb{C}$ is a map satisfying the 2 conditions from proposition 1.4.26. The above formula applied to $k_N(t)$ yields

$$L(E/k_N(t), T) = \prod_{[r]\in X(d)/\langle |k'|\rangle} \left(1 - \alpha(\theta_{k'_{u'(r)},d,r})T^{u'(r)}\right)$$

where $k' := k_N$ and

$$u'(r) := u_{|k'|,d}(r) = \operatorname{ord}^\times\left(|k'| \bmod \frac{r}{(d,r)}\right) = \frac{u(r)}{(N, u(r))}.$$

Therefore $k'_{u'(r)} = k_{\frac{N\cdot u(r)}{(N,u(r))}}$ is an extension of $k_{u(r)}$ of degree $\frac{N}{(N,u(r))}$. By proposition 1.4.17 and by property 2 of α in proposition 1.4.26, we deduce that

$$\begin{aligned} L(E/k_N(t), T) &= \prod_{[r]\in X(d)/\langle |k'|\rangle} \left(1 - \alpha(\theta_{k_{u(r)},d,r})^{\frac{N}{(N,u(r))}} T^{u'(r)}\right) \\ &= \prod_{[r]\in X(d)/\langle |k'|\rangle} \left(1 - \alpha(\theta_{k_{u(r)},d,r})^{\frac{N}{(N,u(r))}} T^{\frac{u(r)}{(N,u(r))}}\right) \\ &= \prod_{[r]\in X(d)/\langle |k|\rangle} \left(1 - \alpha(\theta_{k_{u(r)},d,r})^{\frac{N}{(N,u(r))}} T^{\frac{u(r)}{(N,u(r))}}\right)^{(N,u(r))} \end{aligned}$$

where the last step follows because, if we let $q = |k|$, then the $\langle q\rangle$-orbit of each $r \in X(d)$ splits into $\gcd(N, u(r))$ $\langle q^N\rangle$-orbits. Indeed,

$$\#\operatorname{orb}_{\langle q^N\rangle}(r) = \#\{r, q^N r, q^{2N} r, \ldots\} = u_{q^N,d}(r) = \frac{u_{q,d}(r)}{(N, u_{q,d}(r))} = \frac{\#\operatorname{orb}_{\langle q\rangle}(r)}{(N, u_{q,d}(r))}.$$ ⌟

In view of lemma 4.2.7 and of the fact that the L-function of $E'_{m,b,b'}$ is expressed in terms of Jacobi sums (by theorem 4.1.2), it makes sense to study when those sums are pure. This is possible thanks to Stickelberger's theorem 1.4.22. We recall from definition 1.4.1 that $\{x\} \in [0, 1[$ denotes the fractional part of a real number x.

A statement for Gauss sums analogous to the next lemma is given in [Aok12, proposition 4.4], [Aok04, 2.3], and in [Aok97, proposition 3.1] for Jacobi sums (but the proof is not self-contained there and not as complete as ours).

Lemma 4.2.11. *Let $k = \mathbb{F}_q$ be a finite field where $q = p^e$ for some prime p and some $e \geqslant 1$. Let $n \geqslant 1, D \geqslant 2$ be integers[8] such that $\gcd(D, p) = 1$ and n is odd. Let $\vec{a} = (a_1, ..., a_n) \in (\mathbb{Z}/D\mathbb{Z} \smallsetminus \{0\})^n$ be such that $a_{n+1} := -\sum_{i=1}^{n} a_i \neq 0$. Consider the character $\omega_{q,D}$ on $k^\times_{\mathrm{ord}(q \bmod D)}$ of order m as in definition 1.4.20 and define the map*

$$\beta' : (\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{Z}, \quad t \mapsto \beta_{q,D}(t \cdot \vec{a})$$

where we use the notations from definition 1.4.20.

Consider the Jacobi sum $J := J(\omega_{q,D}^{a_1}, ..., \omega_{q,D}^{a_n})$ as an algebraic integer in $\mathbb{Z}[\zeta_D]$. Then the following are equivalent:

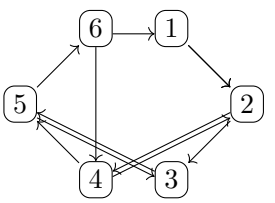
1. *The algebraic number J is pure.*
2. *The ideal $(J) \trianglelefteq \mathbb{Z}[\zeta_D]$ is Galois-invariant (under the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$).*
3. *The ideal $(J) \trianglelefteq \mathbb{Z}[\zeta_D]$ is invariant under complex conjugation.*
4. *The map β' is a constant map.*
5. *We have $\beta'(t) = \beta'(-t)$ for all $t \in (\mathbb{Z}/D\mathbb{Z})^\times$.*
6. *We have $\beta'(t) = \frac{f \cdot (n-1)}{2}$ for all $t \in (\mathbb{Z}/D\mathbb{Z})^\times$, where $f \geqslant 1$ is such that $p^f = q^{\mathrm{ord}^\times(q \bmod D)}$. Equivalently,*

$$\forall t \in (\mathbb{Z}/D\mathbb{Z})^\times, \qquad \beta'(t) + f = \sum_{j=0}^{f-1} \sum_{i=1}^{n+1} \left\{ \frac{-t \cdot a_i \cdot p^j}{D} \right\} = \frac{f \cdot (n+1)}{2}. \tag{4.2.3}$$

⌟

Remark 4.2.12. When $n = 3$, equation (4.2.3) is exactly the condition that defines the set $B_d(p)$ given in [Shi91, equation (2.8)]. See also remark 4.2.33 for more details. ⌟

Proof. — We prove the following implications:



1 $\implies$ 2. Since $\sum_{i=1}^{n} a_i \neq 0 \neq a_i$ for all i, we can apply proposition 1.4.6 to deduce that $|J| = Q^{(n-1)/2}$ where $Q := q^{\mathrm{ord}(q \bmod D)}$. Note that $|J| \in \mathbb{Q}$ since we assumed n to be odd. If J is pure, then $J = \zeta \cdot |J|$ for some root of unity $\zeta = J \cdot |J|^{-1} \in \mathbb{Z}[\zeta_D]^\times$, which means that we have an equality of ideals $(J) = (|J|) \trianglelefteq \mathbb{Z}[\zeta_D]$. Since $|J|$ is rational, it is clear that (J) is Galois-invariant.

2 $\implies$ 3. Immediate.

[8] This integer D has nothing to do with the degrees D or D' of the L-functions considered in lemmas 4.2.7 to 4.2.9.

2 $\iff$ 4. For each $t \in (\mathbb{Z}/D\mathbb{Z})^\times$, we denote by $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ the unique element such that $\sigma_t(\zeta_D) = \zeta_D^t$. From Stickelberger's theorem 1.4.22, we know that we have a prime factorization

$$(J) = \prod_{[t] \in (\mathbb{Z}/D\mathbb{Z})^\times/\langle p \rangle^\times} \sigma_{t^{-1}}(\mathfrak{p})^{\beta'(t)}$$

where $\mathfrak{p} \trianglelefteq \mathbb{Z}[\zeta_D]$ is the prime ideal above p as in definition 1.4.20. For every $s \in (\mathbb{Z}/D\mathbb{Z})^\times$ we have

$$\begin{aligned}\sigma_s((J)) &= \prod_{[t] \in (\mathbb{Z}/D\mathbb{Z})^\times/\langle p \rangle^\times} \sigma_s\sigma_{t^{-1}}(\mathfrak{p})^{\beta'(t)} \\ &= \prod_{[t] \in (\mathbb{Z}/D\mathbb{Z})^\times/\langle p \rangle^\times} \sigma_{st^{-1}}(\mathfrak{p})^{\beta'(t)} = \prod_{[t'] \in (\mathbb{Z}/D\mathbb{Z})^\times/\langle p \rangle^\times} \sigma_{t'^{-1}}(\mathfrak{p})^{\beta'(s^{-1}t')},\end{aligned}$$

where the last equality follows by setting $t' := s^{-1}t$. We know that (J) is Galois-invariant if and only if $\sigma_s((J)) = (J)$ for all $s \in (\mathbb{Z}/D\mathbb{Z})^\times$. The uniqueness of the decomposition into prime ideals forces the equality $\beta'(t) = \beta'(s^{-1}t)$ for every $s, t \in (\mathbb{Z}/D\mathbb{Z})^\times$. It follows β' is a constant map if and only if (J) is Galois-invariant.

3 $\iff$ 5. Invariance under complex conjugation means that we take $s = -1$ in the above computation (since σ_{-1} is the complex conjugation). This exactly means that $\beta'(t) = \beta'(-t)$ for all t.

4 $\implies$ 5. Immediate.

5 $\implies$ 6. Recall from definition 1.4.20 that for all t, we have

$$\beta'(t) = \sum_{j=0}^{f-1} \left(-1 + \sum_{i=1}^{n+1} \left\{\frac{-ta_i \cdot p^j}{D}\right\}\right)$$

where $f := e \cdot \mathrm{ord}^\times(q \bmod D)$. The key fact is that for every $x \in \mathbb{R} \smallsetminus \mathbb{Z}$, we have $\{-x\} = 1 - \{x\}$. Since $(p, D) = 1$, $t \in (\mathbb{Z}/D\mathbb{Z})^\times$ and $a_i \not\equiv 0 \bmod D$ for all i, we know that $\frac{-ta_i \cdot p^j}{D}$ is never an integer. Thus, we find

$$\begin{aligned}\beta'(t) = \sum_{j=0}^{f-1} \left(-1 + \sum_{i=1}^{n+1} \left(1 - \left\{\frac{ta_i \cdot p^j}{D}\right\}\right)\right) &= -f + f \cdot (n+1) - \sum_{j=0}^{f-1}\sum_{i=1}^{n+1} \left\{\frac{ta_i \cdot p^j}{D}\right\} \\ &= f + f \cdot (n-1) - \sum_{j=0}^{f-1}\sum_{i=1}^{n+1} \left\{\frac{ta_i \cdot p^j}{D}\right\} \\ &= f \cdot (n-1) - \beta'(-t).\end{aligned}$$

By assumption, we have $\beta'(-t) = \beta'(t)$, which implies that $\beta'(t) = \frac{f \cdot (n-1)}{2}$.

6 $\implies$ 4. Immediate.

6 $\implies$ 1. We know that $|J| = Q^{(n-1)/2}$ where $Q := q^{\mathrm{ord}(q \bmod D)} = p^f$. Now the ideal generated by $Q^{(n-1)/2}$ in $\mathbb{Z}[\zeta_D]$ is $(p)^{f \cdot (n-1)/2} = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{f \cdot (n-1)/2}$, where $\mathfrak{p}_i$ are the primes above p. The assumption on β' implies that the ideals $(J) = (Q^{(n-1)/2})$ coincide, which means that $J = u \cdot Q^{(n-1)/2}$ for some unit $u \in \mathbb{Z}[\zeta_D]^\times$. Since n is odd, $Q^{(n-1)/2} \in \mathbb{Q}$. Moreover, for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ we have $|\sigma(J)| = Q^{(n-1)/2}$, which means that $|\sigma(u)| = 1$. By Kronecker's theorem (see [Coh07, Proposition 3.3.9]), it follows that u must be a root of unity, which in turn implies that J is pure, as desired. ∎

We will need the following result, which is an analogue of Lemma 6, p. 246 in [Eva81] for Jacobi sums. It tells us which power of a pure Jacobi sum gives a positive integer.

Lemma 4.2.13. *Let $k = \mathbb{F}_{p^e}$ be a finite field where p is some prime and $e \geqslant 1$ is an integer. Let $n \geqslant 1$ be an* odd *integer and $\chi_1, ..., \chi_n : k^\times \to \mathbb{Q}(\zeta_D)^\times$ be non-trivial characters of order dividing some integer $D > 1$. Assume that the product $\chi_1 \cdots \chi_n$ is non-trivial.*

Set $N := \gcd\left(\frac{D}{(D,2)}, p-1\right)$. If the Jacobi sum $J(\chi_1, ..., \chi_n)$ is pure, then

$$J(\chi_1, ..., \chi_n)^{2N} = |k|^{(n-1)N}.$$

Proof. —

- Define $J' := \frac{1}{|k|^{(n-1)/2}} J(\chi_1, ..., \chi_n)$, which is a complex number of modulus 1, since $\chi_1 \cdots \chi_n \neq \mathbb{1}$ (see proposition 1.4.6). If the Jacobi sum $J(\chi_1, ..., \chi_n)$ is pure, then J' is a root of unity by remark 4.2.6. Note that $|k|^{(n-1)/2} \in \mathbb{Z}$ since n is odd. This implies that J' belongs to $\mathbb{Q}(\zeta_D) \cap \mu_\infty$, since all characters χ_i have order dividing D. The only roots of unity in $\mathbb{Q}(\zeta_D)$ are $\mu_{2D/\gcd(2,D)} \subset \mu_{2D}$, by [Coh07, Corollary 3.5.12]. In particular, $J' \in \mu_{2D/\gcd(2,D)}$ which precisely means that

$$J'^{\frac{2D}{\gcd(2,D)}} = 1. \tag{4.2.4}$$

- Finally, we check that $J'^{2(p-1)} = 1$, which is equivalent to $J'^{2p} = J'^2$. Since p and D are necessarily coprime, we consider the field automorphism $\sigma_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ such that $\sigma_p(\zeta) = \zeta^p$ for any D-th root of unity $\zeta \in \mu_D$. In particular, by equation (4.2.4) we can consider $J'^2 \in \mu_D$, which yields

$$\sigma_p(J'^2) = J'^{2p}. \tag{4.2.5}$$

  On the other hand, we compute (similarly to proposition 1.4.6.3)

$$\begin{aligned}
\sigma_p(J(\chi_1, ..., \chi_n)) &= \sum_{\substack{x_1,...,x_n \in k \\ x_1+\cdots+x_n=1}} \sigma_p(\chi_1(x_1) \cdots \chi_n(x_n)) \\
&= \sum_{\substack{x_1,...,x_n \in k \\ x_1+\cdots+x_n=1}} \chi_1(x_1)^p \cdots \chi_n(x_n)^p \\
&= \sum_{\substack{x_1,...,x_n \in k \\ x_1+\cdots+x_n=1}} \chi_1(x_1^p) \cdots \chi_n(x_n^p) = J(\chi_1, ..., \chi_n),
\end{aligned}$$

  where the last equality follows because the Frobenius automorphism induces a bijection of the set $\{(x_1, ..., x_n) \in k^n \ : \ x_1 + \cdots + x_n = 1\}$. This computation shows that $\sigma_p(J'^2) = J'^2$. Together with equation (4.2.5), we get the desired equality $J'^{2p} = J'^2$.

  All in all, we combine the identities $J'^{2(p-1)} = 1$ and $J'^{2D/\gcd(2,D)} = 1$ to deduce $J'^{2\gcd(p-1, D/(2,D))} = 1$, which concludes the proof. ∎

4.2.2 Purity of triple Jacobi sums with a cubic character and the Legendre symbol

Assume that k is a finite field of characteristic $p \equiv 1 \bmod 3$. We are going to determine for which integers m the Jacobi sums of the form[9]

$$J_{k,m,r} := J\big(\theta_{k_{u(r)},m,r}\ ;\ \psi_{k_{u(r)}}\ ;\ \lambda_{k_{u(r)}}\big) \tag{4.2.6}$$

(appearing in theorem 4.1.2) are pure.

Definition 4.2.14. We define a set of 34 rational numbers and a set of 11 integers:

$$\begin{aligned}\mathcal{S} := \big\{&\tfrac{1}{2}, \tfrac{1}{3}, \tfrac{2}{3}, \tfrac{1}{4}, \tfrac{3}{4}, \tfrac{1}{5}, \tfrac{2}{5}, \tfrac{3}{5}, \tfrac{4}{5}, \tfrac{5}{6}, \tfrac{2}{9}, \tfrac{5}{9}, \tfrac{8}{9}, \tfrac{5}{12}, \tfrac{11}{12}, \tfrac{5}{18}, \tfrac{11}{18}, \tfrac{17}{18},\\ &\tfrac{5}{24}, \tfrac{11}{24}, \tfrac{17}{24}, \tfrac{23}{24}, \tfrac{11}{30}, \tfrac{17}{30}, \tfrac{23}{30}, \tfrac{29}{30}, \tfrac{11}{60}, \tfrac{17}{60}, \tfrac{23}{60}, \tfrac{29}{60}, \tfrac{41}{60}, \tfrac{47}{60}, \tfrac{53}{60}, \tfrac{59}{60}\big\}\\ \mathcal{M} := \{&2, 3, 4, 5, 6, 9, 12, 18, 24, 30, 60\}.\end{aligned}$$

We note that the least common multiple of the integers $m \in \mathcal{M}$ is $360 = 2^3 \cdot 3^2 \cdot 5$, and that $\mathcal{M}$ is exactly the set of denominators of the elements in $\mathcal{S}$.

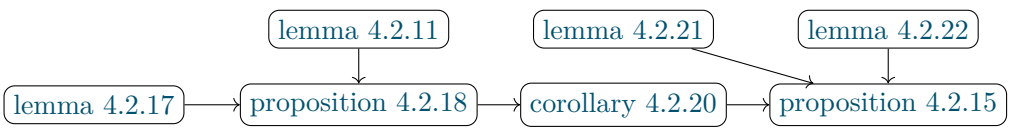
When the characteristic of k is $p \equiv 1 \bmod 3$, we can determine exactly which Jacobi sums $J_{k,m,r}$ (introduced in (4.2.6)) are pure. The goal of this subsection is to show the following assertion.

Proposition 4.2.15. *Let k be a finite field of characteristic $p \equiv 1 \bmod 3$. Let $m \geqslant 1$ be coprime to p and fix $r \in \{1, ..., m-1\}$ such that $r \neq m/6$ if $6 \mid m$. Then:*

$$J_{k,m,r} \text{ is pure} \quad \text{if and only if} \quad r \in m\mathcal{S} := \{\, m \cdot x \ :\ x \in \mathcal{S}\,\}.$$

In particular, if $J_{k,m,r}$ is pure then $m\mathcal{S} \cap \mathbb{Z} \neq \varnothing$, so $m \in \mathcal{M}\mathbb{Z} := \{\, xy \ :\ x \in \mathcal{M}, y \in \mathbb{Z}\,\}$ and the order $\frac{m}{(m,r)}$ of the character $\theta_{k_{u(r)},m,r}$ belongs to $\mathcal{M}$.

The roadmap will be as displayed in the following dependency graph.



We first start with some notations; we recall that $\{x\} \in [0, 1[$ denotes the fractional part of any real number x.

Definition 4.2.16. 1. Define the map $g : \mathbb{R}^3 \to \mathbb{R}$ by

$$g(x_1, x_2, x_3) := \{x_1\} + \{x_2\} + \{x_3\} + \{-x_1 - x_2 - x_3\}.$$

2. Given an integer $d \geqslant 1$, $\epsilon \in \{\pm 1\}$, $a \in \mathbb{Z}/d\mathbb{Z}$ and $x \in \mathbb{Z}$, we set

$$G_{d,\epsilon}(a, x) := g(ax/d, \epsilon x/3, x/2) = \left\{\frac{ax}{d}\right\} + \left\{\frac{\epsilon x}{3}\right\} + \left\{\frac{x}{2}\right\} + \left\{-\frac{x}{d} \cdot \left(a + \frac{\epsilon d}{3} + \frac{d}{2}\right)\right\}.$$

[9] Observe that the assumption $p \equiv 1 \bmod 3$ ensures that 3 divides $|k_{u(r)}^\times|$, so that the character ψ of order 3 on $k_{u(r)}^\times$ indeed exists.

The following easy result is very useful.

Lemma 4.2.17. *1. Given real numbers $0 \leqslant x_1, x_2, x_3 < 1$ such that $x_1x_2x_3 > 0$ we have*

$$g(x_1,x_2,x_3) = \begin{cases} 1 & \text{if } x_2+x_3 \leqslant 1 \text{ and } 0 \leqslant x_1 \leqslant 1-x_2-x_3 \\ 2 & \text{if } x_2+x_3 \leqslant 1 \text{ and } x_1 > 1-x_2-x_3 \\ 2 & \text{if } x_2+x_3 > 1 \text{ and } 0 \leqslant x_1 \leqslant 2-x_2-x_3 \\ 3 & \text{if } x_2+x_3 > 1 \text{ and } x_1 > 2-x_2-x_3. \end{cases}$$

2. If $6 \mid d$ and $x \in \mathbb{Z}$ is coprime to d, then

$$G_{d,\epsilon}(a,x) = \begin{cases} 1 & \text{if } x \equiv \epsilon \bmod 6 \text{ and } \left\{\frac{xa}{d}\right\} \leqslant \frac{1}{6} = 1-\frac{1}{2}-\frac{1}{3} \\ 2 & \text{if } x \equiv \epsilon \bmod 6 \text{ and } \left\{\frac{xa}{d}\right\} > \frac{1}{6} \\ 2 & \text{if } x \equiv -\epsilon \bmod 6 \text{ and } \left\{\frac{xa}{d}\right\} \leqslant \frac{5}{6} = 2-\frac{1}{2}-\frac{2}{3} \\ 3 & \text{if } x \equiv -\epsilon \bmod 6 \text{ and } \left\{\frac{xa}{d}\right\} > \frac{5}{6}. \end{cases} \tag{4.2.7}$$

⌟

Proof. — 1. This is an immediate case-by-case verification.

2. Since x is coprime to d and $6 \mid d$, we may write $x = 6t_1 + t_0$ for some $t_0 \in \{\pm 1\}$ and $t_1 \in \mathbb{Z}$. Then we get

$$\left\{\frac{x}{2}\right\} = \left\{3t_1 + \frac{t_0}{2}\right\} = \left\{\frac{t_0}{2}\right\} = \frac{1}{2}$$
$$\left\{\frac{x}{3}\right\} = \left\{\frac{t_0}{3}\right\} = \begin{cases} \frac{1}{3} & \text{if } x \equiv 1 \bmod 6 \\ \frac{2}{3} & \text{if } x \equiv -1 \bmod 6. \end{cases}$$

So for instance if $x \equiv \epsilon \bmod 6$ and $\left\{\frac{xa}{d}\right\} \leqslant \frac{1}{6} = 1-\frac{1}{2}-\frac{1}{3}$, then

$$G_{d,\epsilon}(a,x) = \left\{\frac{ax}{d}\right\} + \frac{1}{3} + \frac{1}{2} + \left\{-\frac{ax}{d} - \frac{1}{3} - \frac{1}{2}\right\} = g\left(\left\{\frac{ax}{d}\right\}, \frac{1}{3}, \frac{1}{2}\right),$$

so the result follows from the first item. The other cases are analyzed in a similar way. ■

The following result is the place where we use the hypothesis $p \equiv 1 \bmod 3$.

Proposition 4.2.18. *Let q be a power of a prime $p \equiv 1 \bmod 3$ and let $d \geqslant 1$ be an integer coprime to q and suppose that $6 \mid d$. Let $v := \mathrm{ord}^{\times}(q \bmod d)$ and write $q^v = p^f$ for some integer $f \geqslant 1$. Consider the character $\omega := \omega_{q,d} \in \widehat{\mathbb{F}_{q^v}^{\times}}$ of order d as in definition 1.4.20. Let $a \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ and $\epsilon \in \{\pm 1\}$.*

Then the Jacobi sum $J := J(\omega^a, \omega^{\epsilon d/3}, \omega^{d/2})$ is pure if and only if

$$\forall t \in (\mathbb{Z}/d\mathbb{Z})^{\times}, \quad G_{d,\epsilon}(a,t) = 2. \tag{4.2.8}$$

⌟

Proof. — From lemma 4.2.11, we know that J is pure if and only if equation (4.2.3) holds (for any $-t \in (\mathbb{Z}/d\mathbb{Z})^\times$) for the odd integer $n = 3$, which means that for every $t \in (\mathbb{Z}/d\mathbb{Z})^\times$ one has:

$$\sum_{j=0}^{f-1} \left(\left\{ \frac{tap^j}{d} \right\} + \left\{ \frac{t\epsilon dp^j/3}{d} \right\} + \left\{ \frac{tdp^j/2}{d} \right\} + \left\{ -\frac{tap^j}{d} - \frac{t\epsilon p^j}{3} - \frac{tp^j}{2} \right\} \right) =$$
$$= \sum_{j=0}^{f-1} G_{d,\epsilon}(a, tp^j) = \frac{f \cdot (n+1)}{2} = 2f. \tag{4.2.9}$$

It is clear that if (4.2.8) holds true, then (4.2.9) holds as well.

Let us show the converse by the contrapositive. Namely, let us suppose that (4.2.8) is *not* verified, i.e., there is some $t_0 \in (\mathbb{Z}/d\mathbb{Z})^\times$ such that $G_{d,\epsilon}(a, t_0) \neq 2$. We are going to show that (4.2.9) is *not* fulfilled for $t_0 \in (\mathbb{Z}/d\mathbb{Z})^\times$.

Up to replacing t_0 by $-t_0$, we may assume that $G_{d,\epsilon}(a, t_0) = 1$ in view of lemma 4.2.17. Now, the assumption $p \equiv 1 \bmod 6$ (observe that p is necessarily odd) implies that $G_{d,\epsilon}(a, t_0 p^j) \in \{1, 2\}$ for all j (again by lemma 4.2.17), since $t_0 p^j \equiv \epsilon \bmod 6$. But then the equality (4.2.9) cannot be true for t_0 because

$$\sum_{j=0}^{f-1} G_{d,\epsilon}(a, t_0 p^j) = 1 + \sum_{j=1}^{f-1} G_{d,\epsilon}(a, t_0 p^j) \leqslant 1 + 2(f-1) = 2f - 1,$$

which concludes the proof. ∎

Remark 4.2.19. The condition (4.2.8) is exactly the one that defines the set B_d^2 in [Shi86, equation (2.7)]. See remark 4.2.33 for more details. ⌟

We now consider the case $\epsilon = +1$.

Corollary 4.2.20. *Let k be a finite field of characteristic $p \equiv 1 \bmod 3$ and let $m \geqslant 1$ be coprime to p. Let $r \in X(m, 1)$ and set $d = \operatorname{lcm}(6, m)$. Then the Jacobi sum $J_{k,m,r}$ from equation (4.2.6) is pure if and only if*

$$\forall t \in (\mathbb{Z}/d\mathbb{Z})^\times, \quad t \equiv 1 \bmod 6 \implies \left\{ \frac{t \cdot r}{m} \right\} > \frac{1}{6}. \tag{4.2.10}$$

⌟

Proof. — The basic idea in order to apply proposition 4.2.18 is to express the three characters $\theta_{k_{u(r)},m,r}$, ψ and $\lambda \in \widehat{k_{u(r)}^\times}$ as powers of a single character of order $d := \operatorname{lcm}(6, m)$. However, such a character might be defined only over an *extension* of $k_{u(r)}$, but then one can use Hasse–Davenport theorem 1.4.7 to conclude.

Let us first introduce some notations for convenience:

$$q := |k|, \quad v := \operatorname{ord}^\times(q \bmod d), \quad c := \frac{6}{\gcd(m, 6)}.$$

Observe that $d := \operatorname{lcm}(6, m) = \frac{6m}{\gcd(6,m)} = c \cdot m$. Consider the character $\omega := \omega_{q,d} \in \widehat{k_v^\times}$ of order d as in definition 1.4.20.

- We claim that $J_{k,m,r}$ is pure if and only if $J(\omega^{r\cdot c}, \omega^{d/3}, \omega^{d/2})$ is pure. In fact, we shall prove that

$$J(\omega^{r\cdot c}, \omega^{d/3}, \omega^{d/2}) = J_{k,m,r}^{\frac{v}{u(r)}}, \tag{4.2.11}$$

from which the claim immediately follows.

We first check that k_v is an extension of $k_{u(r)}$. By definition we have

$$u(r) = u_{q,m}(r) = \mathrm{ord}^{\times}\left(q \bmod \frac{m}{(m,r)}\right)$$

and we have a group morphism $(\mathbb{Z}/d\mathbb{Z})^{\times} \to \left(\mathbb{Z}/\frac{m}{(m,r)}\mathbb{Z}\right)^{\times}$ which shows that $u(r)$ must divide $v = \mathrm{ord}^{\times}(q \bmod d)$.

By proposition 1.4.17, we have

$$\theta_{k_v,m,r} = \theta_{k_{u(r)},m,r} \circ \mathrm{N}_{k_v/k_{u(r)}}$$

and similarly $\psi_{k_v} = \psi_{k_{u(r)}} \circ \mathrm{N}_{k_v/k_{u(r)}}$ and $\lambda_{k_v} = \lambda_{k_{u(r)}} \circ \mathrm{N}_{k_v/k_{u(r)}}$ (see remark 1.4.19). Hence, Hasse–Davenport lifting relation from theorem 1.4.7 implies that

$$J(\theta_{k_v,m,r};\ \psi_{k_v};\ \lambda_{k_v}) = J_{k,m,r}^{\frac{v}{u(r)}}. \tag{4.2.12}$$

Now, we observe that (see also equation (1.4.11))

$$\theta_{k_v,m,r} = \Theta^{\frac{|k_v^{\times}|\cdot r}{m}} = \Theta^{\frac{|k_v^{\times}|\cdot c\cdot r}{d}} = \omega_{q,d}^{c\cdot r}$$

where Θ denotes the restriction of the Teichmüller character $\overline{\mathbb{F}_p}^{\times} \to \overline{\mathbb{Q}}^{\times}$ to $k_v^{\times}$. It is also clear that $\psi_{k_v} = \omega_{q,d}^{\frac{d}{3}}$ and $\lambda_{k_v} = \omega_{q,d}^{\frac{d}{2}}$ (which is the unique character of order 2). Consequently, we see that equation (4.2.12) is exactly the same as equation (4.2.11).

- By proposition 4.2.18, we know that $J(\omega^{r\cdot c}, \omega^{d/3}, \omega^{d/2})$ is pure if and only if for all $t \in (\mathbb{Z}/d\mathbb{Z})^{\times}$, we have $G_{d,1}(r\cdot c, t) = 2$. By considering $-t$ instead of t, lemma 4.2.17 tells us that this is equivalent to

$$\left\{\tfrac{t\cdot r\cdot c}{d}\right\} = \left\{\tfrac{t\cdot r}{m}\right\} > \frac{1}{6}$$

for all $t \in (\mathbb{Z}/d\mathbb{Z})^{\times}$ such that $t \equiv 1 \bmod 6$. This concludes the proof. ■

We will need the following "technical" lemma.

Lemma 4.2.21. *Let $m \geqslant 1$ be an integer. Let $r \in \mathbb{Z}/m\mathbb{Z}$ and $d := \mathrm{lcm}(6, m)$. Define $r_0 = \frac{r}{(r,m)}, m_0 = \frac{m}{(r,m)}$.*

1. *Assume that $m_0 \geqslant 6$ and [$r_0 \equiv 1 \bmod 3$ or $3 \nmid m_0$]. Then (4.2.10) is* not *satisfied, i.e., there is an integer $t \equiv 1 \bmod 6$, coprime to d such that $\left\{\frac{tr}{m}\right\} \leqslant \frac{1}{6}$.*

2. Assume that $3 \mid m_0$ and $r_0 \equiv -1 \mod 3$. Then we have an equivalence:

$$\begin{aligned} &\exists t \in \mathbb{Z},\ t \equiv 1 \bmod 6, \quad \gcd(t,d) = 1, \quad \left\{\frac{tr}{m}\right\} \leqslant \frac{1}{6} \\ \iff &\exists t' \in \mathbb{Z}, t' \equiv -1 \bmod \gcd(m_0,6), \quad \gcd(t',m_0) = 1, \quad \left\{\frac{t'}{m_0}\right\} \leqslant \frac{1}{6} \end{aligned}$$ ⌟

Proof. — In what follows, we denote by m_1 the product of the primes $p \mid d = \operatorname{lcm}(6,m)$ such that $p \nmid m_0$. Note that $\gcd(m_0,m_1) = 1$.

1. First, we observe that r_0 is coprime to m_0. Using the Chinese remainder theorem, we find some integer t such that

$$\begin{cases} t &\equiv r_0^{-1} \bmod m_0 \\ t &\equiv 1 \quad \bmod m_1. \end{cases}$$

   We have $\left\{\frac{tr}{m}\right\} = \left\{\frac{tr_0}{m_0}\right\} = \frac{1}{m_0} \leqslant \frac{1}{6}$, since $m_0 \geqslant 6$. Moreover, t is coprime to m_0 and m_1 and hence to d as well. Finally, we check that $t \equiv 1 \bmod 6$. To this end, set $g := \gcd(6,m_0) \in \{1,2,3,6\}$. Our assumption implies that either $r_0 \equiv 1 \bmod 3$ or $3 \nmid m_0$ in which case $g \in \{1,2\}$.

   - If $g = 1$, then $6 \mid m_1$ so we simply use the fact that $t \equiv 1 \bmod m_1$.
   - If $g = 2$, then r_0 must be odd (it is coprime to m_0), so that we have $t \equiv 1 \bmod 2$. Furthermore, we have $3 \mid m_1$ which implies that $t \equiv 1 \bmod 3$. Consequently, we have $t \equiv 1 \bmod 6$.
   - If $g = 3$, then $t \equiv r_0^{-1} \equiv 1 \bmod 3$. Moreover, $2 \mid m_1$, which implies that $t \equiv 1 \bmod 2$, so the conclusion holds here as well.
   - If $g = 6$, then $r_0 \equiv 1 \bmod 3$. Since r_0 is coprime to m_0, it must be odd. Thus we must have $t \equiv r_0^{-1} \equiv 1 \bmod 6$ in that case.

2. $\implies$: Suppose that there exists some $t \in \mathbb{Z}$ as in the "left-hand side" of the equivalence. We define $t' := t \cdot r_0$, which clearly satisfies $\left\{\frac{t'}{m_0}\right\} = \left\{\frac{tr}{m}\right\} \leqslant \frac{1}{6}$.

   Note that r_0 and m_0 are coprime. Moreover, by assumption, we know that t is coprime to d hence to m_0. Therefore t' is coprime to m_0.

   Finally, we check that $t' \equiv -1 \bmod \gcd(m_0,6)$. Since $3 \mid m_0$, we know that $g := \gcd(m_0,6) \in \{3,6\}$. If $g = 3$, then we clearly have $t' = tr_0 \equiv -1 \bmod g$ since $r_0 \equiv -1 \bmod 3$ by assumption. If $g = 6$, then m_0 is even and because r_0 is coprime to m_0, this ensures that r_0 is odd, so we must have $r_0 \equiv -1 \bmod 6$. This shows $t' \equiv -1 \bmod g$ in that case as well.

   $\impliedby$: Conversely, let us suppose that there exists some $t' \in \mathbb{Z}$ as in the "right-hand side" of the equivalence. By the Chinese remainder theorem, there is some $t \in \mathbb{Z}$ such that

$$\begin{cases} t &\equiv t' r_0^{-1} \bmod m_0 \\ t &\equiv -1 \quad \bmod m_1, \end{cases}$$

   where we use the notations m_1 from item 1 above.

We clearly have $\left\{\frac{tr}{m}\right\} = \left\{\frac{tr_0}{m_0}\right\} = \left\{\frac{t'}{m_0}\right\} \leqslant \frac{1}{6}$. Moreover, t is coprime to m_0 and to m_1, so it is coprime to d. Let $g := \gcd(m_0, 6) \in \{3, 6\}$. If $g = 3$, then we know that $t \equiv (-1) \cdot (-1) = 1 \bmod 3$. But we must have $2 \mid m_1$, so t must be odd since $t \equiv -1 \bmod m_1$. Henceforth, we get $t \equiv 1 \bmod 6$ in this case. Finally, if $g = 6$ then we directly get $t \equiv 1 \bmod 6$ (since $r_0 \equiv -1 \bmod 6$ because r_0 must be odd in that case). ■

The following result is crucial for the rest; it determines the order m_0 of the characters χ such that the Jacobi sum $J(\chi, \psi, \lambda)$ is pure over fields of characteristic $p \equiv 1 \bmod 6$.

Lemma 4.2.22. *Let $m_0 \geqslant 1$ be an integer. The following statements are equivalent:*

a) *For all integers $t \in \mathbb{Z}$ coprime to m_0 such that $t \equiv -1 \bmod \gcd(m_0, 6)$, we have $\left\{\frac{t}{m_0}\right\} > \frac{1}{6}$.*

b) *$m_0 \in \mathcal{M} = \{2, 3, 4, 5, 6, 9, 12, 18, 24, 30, 60\}$.* ⌟

Proof. — • We prove that a) implies b). There are 3 cases.

– First, if $\gcd(m_0, 6) = 1$ or $\gcd(m_0, 6) = 2$, then we may take $t = 1$ in a), to get $m_0 < 6t = 6$, that is $m_0 \in \{2, 3, 4, 5\}$ (note that $m_0 = 1$ does not work since $\left\{t/m_0\right\} = 0$ in that case).

– If $\gcd(m_0, 6) = 3$ then we may take $t = 2$ in a) to get $m_0 < 6t = 12$, so that $m_0 \in \{3, 9\}$.

– Finally, assume that $\gcd(m_0, 6) = 6$. If $\gcd(m_0, 5) = 1$, then we may take $t = 5 \equiv -1 \bmod 6$ in a) to get $m_0 < 30$ so that $m_0 \in \{6, 12, 18, 24\}$.

Otherwise, $\gcd(m_0, 5) = 5$ which implies that $30 \mid m_0$. Property a) implies that if $p \leqslant \frac{m_0}{6}$ is a prime such that $p \equiv -1 \pmod 6$ then p divides m_0. Let us define the ratio $m' := m_0 / \prod_{i=1}^{R} p_i$ where $p_1 = 5 < p_2 < \ldots < p_R$ are all the prime divisors of m_0 such that $p_i \equiv -1 \pmod 6$ for every i. Note that we must have $6 \mid m'$, $R \geqslant 1$ (and m' may have some prime factors $p \equiv -1 \bmod 6$).

Define $t' := 6 \cdot \prod_{i=1}^{R-1} p_i + p_R > 0$. Note that $t' \equiv p_R \equiv -1 \bmod 6$, so there exists a prime factor $t \mid t'$ such that $t \equiv -1 \bmod 6$. Moreover t is coprime to m_0, otherwise t would have to be equal to p_i for some i (since t would be a prime factor of m_0 such that $t \equiv -1 \bmod 6$), which is impossible: it is quite clear that p_i does not divide t' for any i. Thus assumption a) implies that $t > \frac{m_0}{6}$. Consequently, we get

$$t' = 6 \cdot \prod_{i=1}^{R-1} p_i + p_R \;\geqslant\; t \;>\; \frac{m'}{6} \prod_{i=1}^{R} p_i \;\geqslant\; \prod_{i=1}^{R} p_i. \tag{4.2.13}$$

We now claim that $R = 1$. If we assume that $R \geqslant 2$, then dividing both sides of (4.2.13) by $\prod_{i=1}^{R-1} p_i \geqslant p_1 = 5$ yields

$$p_R \cdot \Big(1 - \frac{1}{5}\Big) \leqslant p_R \cdot \Big(1 - \Big(\prod_{i=1}^{R-1} p_i\Big)^{-1}\Big) < 6.$$

Thus $p_R < \frac{15}{2}$, and because $p_R \equiv -1 \pmod 6$ we find $p_R = 5$ which is a contradiction since $p_R \geqslant p_2 > p_1 = 5$. Therefore we get $R = 1$.

On the other hand, if $m_0 \geqslant 90$ then $p := 11 \leqslant 15 \leqslant \frac{m_0}{6}$ is such that $p \equiv -1 \bmod 6$ and so hypothesis a) would tell us that $p \mid m_0$, which would mean that $R \geqslant 2$ (with $p_2 = 11$). This is impossible by the observation we just made. Therefore, we conclude that $m_0 \in \{30, 60\}$ which finishes the proof of $a) \implies b)$.

- To prove that b) implies a), we simply check that for each $m_0 \in \mathcal{M}$, any integer $1 \leqslant t \leqslant \frac{m_0}{6}$ coprime to m_0 must satisfy $t \not\equiv -1 \bmod \gcd(m_0, 6)$. This is an easy computation.

  If $1 < m_0 < 6$, then there are *no* integer t such that $1 \leqslant t \leqslant \frac{m_0}{6}$, so this is clear. If $m_0 \in \{6, 9, 12, 18, 24, 30\}$, then the only integer $t \in [1, \frac{m_0}{6}]$ coprime to m_0 is $t = 1$ and we indeed have $t \not\equiv -1 \bmod \gcd(m_0, 6)$. Finally, if $m = 60$, the only integers $t \in [1, \frac{m_0}{6}]$ coprime to m_0 are $t = 1$ and $t = 7$, which satisfy $t \not\equiv -1 \bmod 6$. This concludes the proof. ∎

Proof of proposition 4.2.15. — By corollary 4.2.20, we know that the Jacobi sum $J_{k,m,r}$ (from equation (4.2.6)) is pure if and only if (4.2.10) holds. All we have to do is to check that the latter condition is equivalent to $r \in m\mathcal{S}$. Let us define $r_0 = \frac{r}{(m,r)}, m_0 = \frac{m}{(m,r)}$.

- If $m_0 \leqslant 6$, then because we assumed $0 < r < m$, we must have (recalling that r_0 and m_0 are coprime)
$$\frac{r}{m} = \frac{r_0}{m_0} \in \left\{\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{1}{6}, \frac{5}{6}\right\} =: \mathcal{S}_1.$$
  If $\frac{r}{m} \in \mathcal{S}_1 \smallsetminus \{\frac{1}{6}\}$, then for any $t \in \mathbb{Z}$ coprime to m (hence coprime to m_0), we know that $\frac{tr}{m}$ is not an integer so we get $\left\{\frac{tr}{m}\right\} \geqslant \frac{r}{m} > \frac{1}{6}$. In particular, (4.2.10) holds which means that $J_{k,m,r}$ is pure. Conversely, if $J_{k,m,r}$ is pure then in particular by setting $t = 1$ in (4.2.10), we see that $\frac{r}{m} \in \mathcal{S}_1 \smallsetminus \{\frac{1}{6}\}$ whenever $m_0 \leqslant 6$.

  (Notice that removing $1/6$ from $\mathcal{S}_1$ is exactly asking that $r \neq m/6$ when $6 \mid m$, which is ensured by having $r \in X(m, 1)$ as in definition 4.1.1).

- Let us assume now that $m_0 > 6$. If $r_0 \equiv 1 \bmod 3$ or if $3 \nmid m_0$, then $J_{k,m,r}$ is not pure in view of corollary 4.2.20 and lemma 4.2.21.

  Conversely, we show that if $r_0 \not\equiv 1 \bmod 3$ and if $3 \mid m_0$, then $J_{k,m,r}$ is pure if and only if $r \in m\mathcal{S}$. Because $\gcd(r_0, m_0) = 1$, we must have $r_0 \equiv -1 \bmod 3$. Thus by lemma 4.2.21 and lemma 4.2.22, we know that $J_{k,m,r}$ is pure if and only if $m_0 \in \mathcal{M} = \{2, 3, 4, 5, 6, 9, 12, 18, 24, 30, 60\}$. Since $m_0 > 6$ and $r_0 \equiv -1 \bmod 3$ is coprime to m_0, this tells us that $\frac{r}{m} = \frac{r_0}{m_0}$ belongs to
$$\mathcal{S}_2 := \left\{\tfrac{2}{9}, \tfrac{5}{9}, \tfrac{8}{9}, \tfrac{5}{12}, \tfrac{11}{12}, \tfrac{5}{18}, \tfrac{11}{18}, \tfrac{17}{18}, \tfrac{5}{24}, \tfrac{11}{24}, \tfrac{17}{24}, \tfrac{23}{24}, \tfrac{11}{30}, \tfrac{17}{30}, \tfrac{23}{30}, \tfrac{29}{30}, \tfrac{11}{60}, \tfrac{17}{60}, \tfrac{23}{60}, \tfrac{29}{60}, \tfrac{41}{60}, \tfrac{47}{60}, \tfrac{53}{60}, \tfrac{59}{60}\right\}.$$

All in all, we conclude that $J_{k,m,r}$ is pure if and only if $\frac{r}{m} \in \mathcal{S}_1 \cup \mathcal{S}_2 \smallsetminus \{\frac{1}{6}\} = \mathcal{S}$, which exactly means that $r \in m\mathcal{S}$. This finishes the proof. ∎

4.2.3 Rank of the curves $E'_{m,b,b'}$ in characteristic $p \equiv 1 \bmod 3$

In our case, the L-function of $E'_{m,b,b'}$ is expressed in terms of Jacobi sums so we get the following expression for its geometric rank.

Corollary 4.2.23. *Let k be a finite field of characteristic $p \equiv 1 \bmod 3$. Let $b, b' \in k^\times$ and $m \geqslant 1$ be coprime to p. Then:*

1. *We have an upper bound on the rank:*

$$\operatorname{rk} E'_{m,b,b'}(k(t)) \leqslant 2 \cdot \#\Big\{ [r] \in X(m,1)/\langle |k| \rangle^\times \ : \ \Big\{\tfrac{r}{m}\Big\} \in \mathcal{S} \Big\}.$$

2. *The geometric rank $\operatorname{rk} E'_{m,b,b'}(\overline{k}(t))$ is equal to*

$$2 \cdot \#\Big\{ r \in X(m,1) \ : \ \Big\{\tfrac{r}{m}\Big\} \in \mathcal{S} \Big\} \quad = \quad 2 \cdot |\mathbb{Z} \cap m\mathcal{S}|,$$

where $X(m,1) \subset \mathbb{Z}/m\mathbb{Z}$ is as in definition 4.1.1 and $\mathcal{S} \subset \mathbb{Q}$ is a 34-element set defined in definition 4.2.14. In particular, when m is coprime to $30 = 2 \cdot 3 \cdot 5$, the geometric rank of $E'_{m,b,b'}$ is 0. ⌟

Remark 4.2.24. As explained at the beginning of the proof of proposition 1.4.26, the Jacobi sum $J_{k,m,r}$ (from equation (4.2.6)) does not depend on a representative $r \in X(m,1)$ of $[r] \in X(m,1)/\langle |k| \rangle$. One can check also that the condition $\left\{\frac{r}{m}\right\} \in \mathcal{S}$ does not depend on the representative (the point is that when $m/\gcd(r,m) > 6$, the numerator $r/\gcd(r,m)$ is $\equiv -1 \bmod 3$, while we have $|k| \equiv 1 \bmod 3$).

Moreover, if $|k| \equiv 1 \bmod m$, then the upper bound on $\operatorname{rk} E'_{m,b,b'}(k(t))$ from item 1 matches the geometric rank, but it does *not* mean that the geometric rank is achieved over $k(t)$ (i.e., is equal to $\operatorname{rk} E'_{m,b,b'}(k(t))$). ⌟

Proof. — 1. By theorem 4.1.2 and since $|k| \equiv 1 \bmod 3$, we know that the analytic rank is

$$\begin{aligned}\rho(E'_{m,b,b'}/k(t)) &= \sum_{\epsilon \in \{\pm 1\}} \#\Big\{ [r] \in X(m,\epsilon)\Big/\langle |k| \rangle \ : \ \alpha'_{b,b',\epsilon}(\theta_{k_{u(r)},m,r}) = |k|^{u(r)} \Big\} \\ &= 2 \cdot \#\Big\{ [r] \in X(m,1)\Big/\langle |k| \rangle \ : \ \alpha'_{b,b',1}(\theta_{k_{u(r)},m,r}) = |k|^{u(r)} \Big\} \qquad (4.2.14)\end{aligned}$$

where

$$\alpha'_{b,b',1}(\theta_{k_{u(r)},m,r}) = \lambda(b) \cdot \theta_{k_{u(r)},m,r}(-bb'^{-1}) \cdot \psi_{k_{u(r)}}(-b) \cdot J_{k,m,r}$$

and $J_{k,m,r}$ was introduced in equation (4.2.6) (as noted in remark 4.1.3 the rank is always even if $|k| \equiv 1 \bmod 3$). If $\alpha'_{b,b',1}(\theta_{k_{u(r)},m,r})$ is a (positive) integer, then it is clear that $J_{k,m,r}$ is pure (since these two quantities only differ by roots of unity given by the values of some characters), so we have an upper bound

$$\rho(E'_{m,b,b'}/k(t)) \leqslant 2 \cdot \#\Big\{ [r] \in X(m,1)\Big/\langle |k| \rangle \ : \ J_{k,m,r} \text{ is pure} \Big\}.$$

Now the conclusion readily follows from proposition 4.2.15.

2. This follows from the above discussion, together with lemma 4.2.8. Indeed, using proposition 1.4.16, the geometric rank is equal to

$$2 \cdot \sum_{\substack{r \in X(m,1)/\langle |k| \rangle \\ J_{k,m,r} \text{ is pure}}} u_{|k|,m}(r) \quad = \quad 2 \cdot \sum_{\substack{r \in X(m,1) \\ J_{k,m,r} \text{ is pure}}} 1.$$

Finally, when m is coprime to 30, the set $m\mathcal{S} \subset \mathbb{Q}$ does not contain any integer, so the geometric rank is 0. ■

We get an analogue of the result cited in [SS19, theorem 13.26] over $\mathbb{C}(t)$.

Corollary 4.2.25. *Let k be a finite field of characteristic $p \equiv 1 \bmod 3$ and $b, b' \in k^\times$. Then the map*

$$\mathbb{Z}_{>0} \smallsetminus p\mathbb{Z} \longrightarrow \mathbb{Z}_{\geqslant 0}, \qquad m \longmapsto \operatorname{rk} E'_{m,b,b'}(\overline{k}(t))$$

is 360-periodic, and achieves its maximum of 68 exactly at the multiples m of 360.

In particular, for any $b, b' \in k^\times$ and any $m \geqslant 1$ we have $\operatorname{rk} E'_{m,b,b'}(k(t)) \leqslant 68$. ⌟

Proof. — We simply apply the second part of corollary 4.2.23 and the following lemma.

Lemma 4.2.26. *Let $S \subset \mathbb{Q}_{>0}$ be a finite set of positive rational numbers and let N be the least common multiple of the denominators of elements of S. Then the map $f_S : \mathbb{Z}_{>0} \to \mathbb{Z}_{\geqslant 0}, m \mapsto |\mathbb{Z} \cap mS|$ is N-periodic and attains its maximum whenever m is a multiple of N, in which case $f_S(m) = |S|$.* ⌟

The proof of the lemma is immediate, since $NS \subset \mathbb{Z}$. Moreover, note that $f_S(m) = 0$ whenever m is coprime to N.

Applying the lemma to the set $\mathcal{S}$ from definition 4.2.14, we have $N = 360 = 2^3 \cdot 3^2 \cdot 5$, and so the rank of $E'_{m,b,b'}$ over $k(t)$ is at most $2|S| = 68$, and this upper bound is an equality when m is a multiple of 360.

As for the last claim, it is clear that $\{ \operatorname{rk} E'_{m,b,b'}(k(t)) \ : \ m \geqslant 1, \gcd(m,p) = 1 \}$ is bounded (by 68). Moreover, when $p \mid m$, we may apply remark 4.1.3 to the elliptic curve $E'_{m,b,b'}$ over $k(t)$ to conclude that its rank is the same as the rank of E'_{m_1,b_1,b'_1} for some $b_1, b'_1 \in k^\times$, where $m_1 := m/p^{v_p(m)}$. So the rank $E'_{m,b,b'}$ is also bounded by 68. ■

Example 4.2.27. For $p = 7 \equiv 1 \bmod 3$, corollary 4.2.23 tells us that the rank of $E'_{m,b,b'} : y^2 = x^3 + b + b't^m$ over $\mathbb{F}_7(t)$ is at most 28 for all $b, b' \in \mathbb{F}_7^\times$ and all $m \geqslant 1$ (not necessarily coprime to 7, thanks to remark 4.1.3), since the rank is at most $2 \cdot |m\mathcal{S} \cap R|$ where $R \subset \{1, ..., m-1\}$ is a set of representatives of $X(m,1)/\langle |k| \rangle$, and $|m\mathcal{S} \cap R|$ attains its maximum when m is a multiple of 360 (as the lemma 4.2.26 showed).

More precisely, we get the following upper bounds for specific values of m (and any $b, b' \in \mathbb{F}_7^\times$):

m	1	2	3	4	5	6	8	9	10	11	12	60	360
$\operatorname{rk} E'_{m,b,b'}(\mathbb{F}_7(t)) \leqslant$	0	2	4	4	2	8	4	6	4	0	12	20	28

⌟

We now prove the main result of this section.

Proof of theorem 4.2.1. — We are going to use lemmas 4.2.8 and 4.2.13 together with our knowledge of which Jacobi sums (appearing in the L-function of $E'_{m,b,b'}$) are pure, thanks to proposition 4.2.15.

- We first prove the general statement, when m is coprime to p. Define $P_m := \mathbb{Z} \cap m\mathcal{S}$, which is exactly the set of $r \in \{1, ..., m-1\}$ such that $\alpha'_{b,b',1}(\theta_{k_{u(r)},m,r})$ (or equivalently $J_{k,m,r}$) is pure by proposition 4.2.15. For each $r \in P_m$, let $N(r) \geqslant 1$ be an integer such that $J_{k,m,r}^{N(r)}$ is a positive real number, where $J_{k,m,r}$ is the Jacobi sum from equation (4.2.6). By lemma 4.2.13, we may take

$$N(r) := \gcd\Big(\operatorname{lcm}\big(\tfrac{m}{(r,m)}, 6\big)\ ,\ 2(p-1)\Big).$$

  Indeed, the character $\theta_{k_{u(r)},m,r}$ has order $\frac{m}{(m,r)}$ (see proposition 1.4.17), $\psi_{k_{u(r)}}$ has order 3 and the Legendre symbol has order 2, so overall these orders divide $D := \operatorname{lcm}(\frac{m}{(r,m)}, 6)$ (which is an even integer).

  Using again this information about the orders of the characters, we know that

$$\alpha'_{b,b',1}(\theta_{k_{u(r)},m,r})^{M(r)} \in \mathbb{R}_{>0} \quad \text{where} \quad M(r) := \operatorname{lcm}\Big(N(r), 6, \frac{m}{(m,r)}\Big).$$

  From lemma 4.2.8 and theorem 4.1.2, we know that the geometric rank is achieved over $k_H(t)$ as soon as $H \geqslant 1$ satisfies

$$\forall r \in P_m, \qquad M(r) \cdot u_{|k|,m}(r) \mid H. \tag{4.2.15}$$

  We claim that $H := 2160$ always works. First, $N(r)$ certainly divides $\operatorname{lcm}\big(\frac{m}{(r,m)}, 6\big)$ so $M(r)$ divides $\operatorname{lcm}\big(\frac{m}{(r,m)}, 6\big)$ as well. Furthermore, $u(r) = \operatorname{ord}^\times(|k| \bmod \frac{m}{(m,r)})$ divides the value of the Carmichael function[10] $\lambda(\frac{m}{(m,r)})$. Consequently, (4.2.15) follows as soon as we have

$$\forall r \in P_m, \qquad \operatorname{lcm}(m_r, 6) \cdot \lambda(m_r) \mid H \tag{4.2.16}$$

  where $m_r := \frac{m}{\gcd(r,m)}$.

  We know that if $r \in P_m = \mathbb{Z} \cap m\mathcal{S}$ then $\frac{r}{m} = \frac{r/(r,m)}{m_r} \in \mathcal{S}$ so $m_r \in \mathcal{M}$ (we recall that $\mathcal{M} = \{2, 3, 4, 5, 6, 9, 12, 18, 24, 30, 60\}$, as in definition 4.2.14). Thereby, to ensure (4.2.16), it suffices to check that

$$\forall m' \in \mathcal{M}, \qquad \operatorname{lcm}(m', 6) \cdot \lambda(m') \mid H. \tag{4.2.17}$$

  It takes now an easy computation to verify that $H := 2160 = 2^4 \cdot 3^3 \cdot 5$ is the smallest integer satisfying (4.2.17), since it is the least common multiple of $\operatorname{lcm}(m', 6) \cdot \lambda(m')$ as m' varies in $\mathcal{M}$.

- When $m = 360m'$ for some $m' \geqslant 1$ is coprime to p then corollary 4.2.25 asserts that $E'_{360m',b,b'}$ has geometric rank equal to 68.

[10] We use the standard notation λ, even though it conflicts with our notation of the Legendre symbol, since it will cause no harm.

- When $p \mid m$, we may use remark 4.1.3 to conclude that the rank of $E'_{360m,b,b'}$ over $k_{2160}(t)$ is the same as the rank of E'_{360m_1,b_1,b'_1} over $k_{2160}(t)$, for some $b_1, b'_1 \in k^\times$ and where $m_1 := m/p^{v_p(m)}$. Thus the geometric rank $E'_{360m,b,b'}$ is also 68. ■

Remark 4.2.28. The statement of theorem 4.2.1 can be improved (or refined) in several ways.

1. We know that the geometric rank is attained over $k_H(t)$ as soon as H satisfies (4.2.15). For instance, when $p = 7 \equiv 1 \bmod 3$ and $m = 3$, we find that $H = 6$ works, so the geometric rank (which equals 4) of $y^2 = x^3 + b + b't^3$ is attained over $\mathbb{F}_{p^6}(t)$. One can show that this is optimal when $b = 3, b' = 2$ in the sense that the rank over $\mathbb{F}_{7^j}(t)$ is not equal to the geometric rank if $j < 6$ (in which case the rank over $\mathbb{F}_{7^j}(t)$ is actually 0).

2. If b is a 6-th power in $k^\times$ and $b' = -b$ (e.g., $b = 1, b' = -1$) then b is a square, $-b$ is a cube and $-bb'^{-1} = 1$ so that $\alpha'_{b,b',1}(\theta_{k_{u(r)},m,r}) = J_{k,m,r}$ (the latter Jacobi sum being defined in equation (4.2.6)).

   In that case, we may replace $M(r)$ by $N(r)$ in equation (4.2.15), that is, if H is a multiple of $N(r) \cdot u_{|k|,m}(r)$ for all $r \in P_m := \mathbb{Z} \cap m\mathcal{S}$, then the geometric rank of $E'_{m,b,b'}$ is equal to the rank over $k_H(t)$. For instance when $p = 7, m = 360$, the geometric rank of $E'_{m,1,-1}$ is achieved over $\mathbb{F}_{p^{144}}(t)$.

   It can be checked that $H = 720$ always works. In fact, if b is a 6-th power in $k^\times$ and $b' = -b$ (and k has characteristic $\equiv 1 \bmod 3$), then for any $m \geqslant 1$ the geometric rank of $E'_{m,b,b'}$ is equal to the rank over $k_H(t)$ for some divisor H of $720 = 2^4 \cdot 3^2 \cdot 5$. (The point is that one only needs to check primes $p = \mathrm{char}(k)$ modulo 360, since $N(r)$ only depends on the class of p modulo $m/(m, r)$, which divides 360 when $r \in P_m$).

3. On the other hand, if $-bb'^{-1}$ generates $k^\times$, then the factor $\theta_{k_{u(r)},m,r}(-bb'^{-1})$ (appearing in $\alpha'_{b,b',1}(\theta_{k_{u(r)},m,r})$) is a primitive root of unity of order $\frac{m}{(m,r)}$, so it is pure of rather "large" degree. It could happen that the Jacobi sum $J_{k,m,r}$ is pure of large degree as well (this could occur for instance if $\alpha'_{b,b',1}(\theta_{k_{u(r)},m,r})$ is an integer). But in general we could expect the rank of $E'_{m,b,b'}$ over $k(t)$ to be quite small (typically 0), if $-bb'^{-1}$ generates $k^\times$, and we could expect the geometric rank is achieved over $k_N(t)$ with $N \leqslant 2160$ being quite "large".

4. Let us give some examples. When $p = 19$, then $E'_{360,1,-1} : y^2 = x^3 + 1 - t^{360}$ attains its geometric rank over $\mathbb{F}_{p^{36}}(t)$.

   When $p = 1801 \equiv 1 \bmod 360$, then $E'_{360,1,-1}$ achieves its geometric rank over $\mathbb{F}_{p^{60}}(t)$. The geometric rank of $E'_{5,1,-1} : y^2 = x^3 + 1 - t^5$ is 8 and is achieved over $\mathbb{F}_{p^{15}}(t)$. These results can be obtained via explicit computations (using SAGE [The21]) of the Jacobi sums involved in the L-function of $E'_{m,1,-1}$ given in theorem 4.1.2. ⌟

4.2.4 Various comments

Remark 4.2.29. Our upper bounds on the analytic rank of $E'_{m,b,b'}$ only take into account the *purity* of the coefficients $\alpha(r) := \alpha'_{b,b',1}(\theta_{k_{u(r)},m,r})$ that appear in the L-function as in theorem 4.1.2.

A more refined analysis is required to get better control on the (analytic) rank, which is given by equation (4.2.14) in terms of the number of those coefficients $\alpha(r)$ that are equal to a positive integer (which is necessarily $|k|^{u(r)}$ by remark 4.2.6), instead of just having a *power* being equal to a positive integer — which is what purity means.

Let us assume that $b = 1, b' = -1$ as in remark 4.2.28.2, so that $\alpha(r) = J_{k,m,r}$ (see equation (4.2.6)). This assumption simplifies the analysis, since very often the rank depends on b, b' in some rather erratic manner and it seems difficult to get exact formulas for any choice of the parameters.

In general, we have $J_{k,m,r} \in \mathbb{Z}[\zeta_D]$ where $D := \mathrm{lcm}(6, m/\gcd(m, r))$. Given a finite field k of characteristic $p \equiv 1 \bmod 3$ and $m \geqslant 1$ coprime to p, we want to understand for which $r \in \mathbb{Z}/m\mathbb{Z}$ the triple Jacobi sum $J_{k,m,r}$ is a positive integer. There are two directions:

- We can try to study or compute explicitly Jacobi sum of the form $J(\chi_m^r, \chi_3, \chi_2)$ where $\chi_2, \chi_3, \chi_m : k_n^\times \to \mathbb{C}^\times$ are characters of order $2, 3, m$ respectively over some finite extension k_n of k. Up to replacing m by $\frac{m}{\gcd(m,r)}$, we may assume that $m \in \mathcal{M}$ because otherwise this sum is not pure, by proposition 4.2.15 (recall that we work in characteristic $p \equiv 1 \bmod 3$ and that $\mathcal{M}$ was introduced in definition 4.2.14).

  When $m \in \{2, 3, 4, 5, 6, 12, 24\}$, [BEW98, chapter 3] gives explicit computations of some Jacobi sums and there are some indications for the case $m = 18$ (hence we get also the case $m = 9$ by using χ_{18}^2), and $m = 30, m = 60$ in [BEW98, exercise 14, p. 149 and notes on p. 150-151]. However, it seems quite involved and tedious to work with these results. Moreover, these results are stated exclusively over $\mathbb{F}_p$ and not general[11] $\mathbb{F}_q$ (in other words, they assume that $p \equiv 1 \bmod m$). See [BE79] for the exact evaluation and determination of some Jacobi sums over $\mathbb{F}_{p^2}$.

- Another approach is to say that at the very least, $J_{k,m,r}$ must be a rational number (so we "forget" about its sign), which means that it is fixed by the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_D)/\mathbb{Q})$ (in contrast, recall that from lemma 4.2.11 that purity means that the *ideal* generated by $J_{k,m,r}$ is fixed by the Galois group). In general, we may study the abelian extension $\mathbb{Q}(J_{k,m,r})/\mathbb{Q}$ generated by this triple Jacobi sum. Some works in this direction have been published: [Aok96, theorem 0.3, remark 6.6], [Hos22, Mik95]; for Jacobi sums where all the characters are the same (which does not apply to our case), see [OK93, OG93, Ono93]; for double Jacobi sums, see [Yok64, Lemma 2, p. 147] or [Aki96]. ⌟

In view of experimental data gathered and patterns[12] observed for a few primes p and some integers m, we formulate the following open problem, which refines corollary 4.2.25.

Conjecture 4.2.30. For every finite field k of characteristic $p \equiv 1 \bmod 3$ and all $b, b' \in k^\times$, the map

$$\mathbb{Z}_{>0} \smallsetminus p\mathbb{Z} \longrightarrow \mathbb{Z}_{\geqslant 0}, \qquad m \mapsto \mathrm{rk}\, E'_{m,b,b'}(k(t))$$

is periodic, with a period that divides $360 = 2^3 \cdot 3^2 \cdot 5$. In particular, there is a constant $r = r_{k,b,b'} \geqslant 0$ such that the rank of $E'_{360m',b,b'}(k(t))$ is equal to r, for all $m' \geqslant 1$.

[11] If needed we may assume that $p \equiv 1 \pmod{360}$, e.g., $p = 1801$, so that all the characters of order $m \in \mathcal{M} = \{2, 3, 4, 5, 6, 9, 12, 18, 24, 30, 60\}$ can be defined over $\mathbb{F}_p$.

[12] See the file `q = 7 - List or table of analytic ranks (conjecture 4.2.30).pdf` available at https://gitlab.com/gauthierleterrier/maths.

Furthermore, for each such finite field k, there are $b, b' \in k^\times$ such that $r_{k,b,b'} > 0$ is non-zero. ⌟

Notice that theorem 4.2.1 proves the case where $b, b' \in \mathbb{F}_p^\times$ and $k = \mathbb{F}_{p^N}$, where N is any integer multiple of 2160, in which case $r_{k,b,b'} = 68 > 0$.

Remark 4.2.31. Let us introduce the following terminology.

Definition 4.2.32. Let k be a field and E be a non-constant elliptic curve over $k(t)$. A finite extension k'/k is called:

1. a splitting field of $E/k(t)$ if $E(k'(t)) = E(\overline{k}(t))$.
2. a geometric field for $E/k(t)$ if $\mathrm{rk}_{\mathbb{Z}} E(k'(t)) = \mathrm{rk}_{\mathbb{Z}} E(\overline{k}(t))$. (In that case, we also say that the geometric rank is attained or achieved over $k'(t)$).

In other words, the index of $E(k'(t))$ in $E(\overline{k}(t))$ is 1 or finite, respectively. ⌟

It was shown in [Usu01] that for the values of m given in the table below, there is some prime p such that $k = \mathbb{F}_p$ is a splitting field for $E'_{m,-1,1} : y^2 = x^3 - 1 + t^m / \mathbb{F}_p(t)$. In fact, we have $p \equiv 1 \pmod m$ in all the given cases. No such prime is known for $m = 60$, although there is probably one (in characteristic 0, more precisely over $\mathbb{Q}(t)$, see [Shi99b]).

m	9	12	18	24	30
p	433	397	433	1801	25261

⌟

Remark 4.2.33. We briefly explain how to apply [Shi86] to get the geometric rank of $E'_{m,b,b'}$ over $k(t)$ where k is any (algebraically closed) field of characteristic $p \geqslant 0$ with $p \neq 2, 3$; we may assume that $b = b' = 1$ by remark 1.3.39. The algorithm starts with the projective surface[13] $-Y^2 Z^{m-2} + X^3 Z^{m-3} + Z^m + T^m = 0$ over k. This gives us the matrix

$$A = \begin{pmatrix} 0 & 2 & 0 & m-2 \\ 3 & 0 & 0 & m-3 \\ 0 & 0 & 0 & m \\ 0 & 0 & m & 0 \end{pmatrix}$$

as in definition 1.3.36 (see also example 1.3.38). Following the notations from [Shi86] we have: $\delta = \frac{m}{(6,m)}$, $d = \frac{|\det(A)|}{\delta} = \frac{6m^2}{\delta} = \mathrm{lcm}(6, m)$. We define

$$m' = \frac{m}{(6,m)}, \qquad c = \frac{6}{(6,m)},$$

$$L_A = \{\, [a_0, a_1, a_2, -a_0 - a_1 - a_2]B \;:\; a_i \in \mathbb{Z}/d\mathbb{Z} \,\}, \quad B := \begin{pmatrix} 0 & 2m' & c - 2m' & 0 \\ 3m' & 0 & c - 3m' & 0 \\ 0 & 0 & 0 & c \\ 0 & 0 & c & 0 \end{pmatrix}.$$

We easily see that L_A is $\mathbb{Z}/d\mathbb{Z}$-spanned by 3 elements:

$$L_A = \langle e_0 := (0, 2m, -2m', 0), e_1 := (3m', 0, -3m', 0), e_2 := (0, 0, -c, c) \rangle.$$

[13] As noticed in footnote 26 on page 36, this is a *singular* surface.

Note that $e_1 = -e_1$ since $6m' = d \equiv 0 \in \mathbb{Z}/d\mathbb{Z}$. We further introduce (as in [Shi86])

$$A_d := \{\, v \in (\mathbb{Z}/d\mathbb{Z})^4 \;:\; v_i \neq 0, \forall i \,\}$$

$$B_d(p) := \left\{ v \in A_d \;:\; \forall t \in (\mathbb{Z}/d\mathbb{Z})^\times, \sum_{i=0}^{3} \sum_{j=0}^{\mathrm{ord}(p)-1} \left\{ \frac{tp^j v_i}{d} \right\} = 2\,\mathrm{ord}(p) \right\} \quad \text{if } p > 0 \tag{4.2.18}$$

$$B_d(0) := \left\{ v \in A_d \;:\; \forall t \in (\mathbb{Z}/d\mathbb{Z})^\times, \sum_{i=0}^{3} \left\{ \frac{tv_i}{d} \right\} = 2 \right\} \tag{4.2.19}$$

where $\mathrm{ord}(p) = \mathrm{ord}^\times(p \mod d)$ and we assumed that $\gcd(d, p) = 1$. Then Shioda's main result in [Shi86] states that $\mathrm{rk}(E'_{m,b,b'}/\overline{k}(t)) = b_2 - \lambda - t$ where

$$\lambda := |L_A \cap (A_d \smallsetminus B_d(p))| \quad \text{and} \quad \begin{cases} b_2 = 2m - 2, \; t = 2 & \text{if } 6 \mid m \\ b_2 = 12\lceil m/6 \rceil - 2, \; t = 12 - 2(m - 6\lfloor m/6 \rfloor) & \text{if } 6 \nmid m. \end{cases}$$

Simplifying these expressions, we find:

$$\mathrm{rk}(E'_{m,b,b'}/\overline{k}(t)) = \begin{cases} 2m - 4 - \lambda & \text{if } 6 \mid m, \\ 2m - 2 - \lambda & \text{else.} \end{cases}$$

By analyzing the elements in $L_A \cap A_d$, it can be checked that

$$\lambda = 2 \cdot \#\{\, r \in \{1, ..., m-1\} \smallsetminus \{m/6\} \;:\; (3m', 2m', -5m' - rc, rc) \notin B_d(p) \,\}.$$

(when $6 \nmid m$, we necessarily have $r \notin \{m/6\}$ since a is an integer).

It is easily seen that the condition $(3m', 2m', -5m' - rc, rc) \in B_d(p)$ is tantamount to equation (4.2.9) (with $d := \mathrm{lcm}(6, m)$, $q := p$ and $a := r \cdot c$).

If $p \equiv 1 \pmod{d}$, then we have $B_d(p) = B_d(0)$, but proposition 4.2.18 shows that this is actually the case if we simply assume $p \equiv 1 \pmod 6$. Consequently, for any $p \equiv 1 \pmod 6$, we have $\mathrm{rk}(E'_{m,1,1}/\overline{\mathbb{F}_p}(t)) = \mathrm{rk}(E'_{m,1,1}/k(t))$ where k is any algebraically closed field *of characteristic 0*. ⌟

Remark 4.2.34. By proposition 4.1.5, the group $E'_{m,b,b'}(k(t))$ is torsion-free, so it is not clear how to use a descent procedure to get upper bounds on the rank (as in [Sil08a, chapter X], where there is the crucial assumption that $E[M] \subset E(K)$ for some integer $M > 1$). ⌟

Chapter 5

Further directions

I have questions to all your answers.

Woody Allen

We conclude this text by gathering here some questions that arose from this work, which could be of some interest but that we did not have time to investigate. See also conjecture 4.2.30.

1. All the examples of Mordell–Weil lattices we have studied are coming from elliptic curves over $k(t)$, i.e., the function field of $\mathbb{P}^1$. Can we obtain anything interesting by looking at non-constant elliptic curves over $k(C)$, where C has genus > 0?

   The case of *constant* curves E over $k(C)$ was discussed in remark 2.4.1. However the asymptotic behavior on the lower bound on the packing density has not been analyzed: what could be obtained here?

2. In [Oes90, §3.4] and [Tsf91, §9, question 10], it is explicitly asked what packings one can obtain from narrow Mordell–Weil lattices $A(K)^0$ of higher dimensional jacobians or abelian varieties A over global function fields K. We pointed out in remark 2.4.3 that the main obstacle here is to get an (explicit) analogue of Shioda's theorem 1.3.24 on the minimal non-zero height on $A(K)^0$.

3. We mostly looked at *Kummer families* of elliptic curves, as in definition 1.3.45. We mentioned in remark 4.1.12 that the *Artin–Schreier* family $y^2 = x^3 + t^q - t$ gives packings with the same (lower bound on the) sphere packing density as the ones from [Shi91].

   Can we find some other examples of Artin–Schreier families giving interesting sphere packings?

4. For fixed $n > 0$, let $B := \{\, b \in \mathbb{F}_{3^n} \;:\; \mathrm{N}_{\mathbb{F}_{3^n}/\mathbb{F}_3}(b) = (-1)^{n+1} \,\}$. When b varies in B, are the curves $E_{3^n+1,b,1} : y^2 = x^3 + bx + t^{3^n+1}$ isogenous over $\mathbb{F}_{3^{2n}}(t)$ (they have the same L-function by corollary 3.1.22 but see remark 1.3.42)? Are the corresponding narrow Mordell–Weil lattices isometric (= isomorphic)?

   More generally, when do two elliptic curves E, E' over K have isomorphic Mordell–Weil lattices? For instance, when $p^e \equiv -1 \bmod 12$, the narrow Mordell–Weil lattices of the curves $y^2 = x^3 + t^{p^e} - t$ from [GU20] have the same rank and the same (lower bound on the) packing density as Shioda's curves $E'_{p^e+1,1,1}$ in [Shi91] (these curves are not isogenous; see remark 4.1.12). Are these lattices isometric? Or do they have the same theta functions?

   As a related question, one could implement some algorithms to determine whether two elliptic curves over a global function field are isogenous. The work [AW22, Corollary 0.8] seems to be relevant here.

5. Is the lower bound on $\lambda_1(E(K)^0)$ from theorem 1.3.24 attained in the case of Elkies' curves $\Gamma_{4,2^n+1}$ from remark 1.3.47 (when $n > 5$ is odd), or in the case of the curves $E_{3^n+1,b,1}$ when $n > 5$ and $\mathrm{N}_{\mathbb{F}_{3^n}/\mathbb{F}_3}(b) = (-1)^{n+1}$ as discussed in subsection 3.2.2.1 and proposition 3.2.14?

6. Is there a more efficient way to compute the kissing number of the Mordell–Weil lattices $L_{3^n+1,b,1,3^{2n}}$ than the method given in section 3.3 (the same question was asked in [Elk01, §5] for the characteristic 2 family)? For instance, what is the asymptotic behaviour (as $n \to +\infty$) of $\kappa(L_{3^n+1,b,1,3^{2n}})$?

   It is worth investigating this problem because the exponential rate of *lattice* kissing numbers has only been shown quite recently, by Vlăduţ [Vlă19].

   As a related question, we do not know if there is a $\mathbb{Z}$-basis of minimal vectors of the 54-dimensional lattice $L_{3^n+1,b,1,3^{2n}}$ when $n = 3$ and $b = 1$. Computational proposition 3.3.10, together with theorem 3.4.1, tells us that this lattice is generated (over $\mathbb{Z}$) by its minimal vectors, though (there are more than 15 millions of them by computational theorem 3.3.1).

7. Can we compute the Tate–Shafarevich group of some of the curves $E'_{3^n+1,b,1}$ in characteristic 3 when $n > 3$, as done for $n \leqslant 3$ in section 3.4? The technique used there only provides an upper bound on a certain subgroup $Ш[\phi]$ of the Tate–Shafarevich group (and getting better bounds may require the use of a computer as in the proof of theorem 3.4.1 for $n = 3$).

8. One could generalize the construction of the laminated lattices given in propositions 1.2.9 and 3.2.22 to get new sphere packings in dimensions $d + 2, d + 3, \ldots$ (where $d = 2 \cdot 3^n$)

9. Theorem 4.2.1 provides, for each prime $p \equiv 1 \bmod 3$, an isotrivial elliptic curve with bounded non-zero ranks in the family of fields $\mathbb{F}_p(t^{1/m})$, $m \geqslant 1$. Are there such examples in characteristic $p \not\equiv 1 \bmod 3$? Are there examples of *non-isotrivial* elliptic curves with bounded non-zero rank in such a Kummer family of function fields?

   Similarly, in [GU20], there is an example of an Artin–Schreier family with bounded rank, where the rank is actually constantly zero. Is there an example of Artin–Schreier family of elliptic curves over global function fields with bounded but non-zero ranks?

10. One could apply Stickelberger's theorem 1.4.22 to the family $y^2 = x^3 + x + t^m$ when $p \equiv 1 \bmod 4$ to see if indeed Brumer's bound is *not* attained, as mentioned in remark 3.1.21.

11. For any finite field k and any integer $R \geqslant 0$, is there an elliptic curve E over $k(t)$ such that $E(k(t))$ has rank R? Odd ranks were obtained in [Gri20] under some conditions somehow similar to Artin's conjecture on primitive roots, see remark 1.3.49.

12. As mentioned in remark 1.3.49, it was suggested in [PPVW19, §12.5] that elliptic curves $E/k(t)$ *not defined over a proper subfield* have bounded rank. One could try to investigate some examples (beyond the one given in remark 1.3.49).

13. Is there a finite field k and an elliptic curve E over $k(t)$ such that $E(k(t^{1/n}))$ has bounded rank but $E(\bar{k}(t^{1/n}))$ does not, as n ranges over positive integers coprime to the characteristic of k (i.e., we have unbounded geometric rank but bounded algebraic rank)?

14. Here are various questions related to the notions of splitting field introduced in remark 4.2.31.

    (a) Given a finite field k, is it true that

    $$\operatorname{rk} E(k(t)) = \operatorname{rk} E(\overline{k}(t)) \implies E(k(t)) \xhookrightarrow{\cong} E(\overline{k}(t)).$$

    (b) Given a field k and $m > 1$, is it true that

    $$\operatorname{rk} E(k(t)) = \operatorname{rk} E(k(t^{1/m})) \implies E(k(t)) \xhookrightarrow{\cong} E(k(t^{1/m})).$$

    (c) Given two algebraically closed fields $K \subset L$, is it true that

    $$\operatorname{rk} E(K(t)) = \operatorname{rk} E(L(t)) \implies E(K(t)) \xhookrightarrow{\cong} E(L(t)).$$

    We point out that if E is an elliptic curve over K and $K \subset K'$ is a finite extension of global fields such that $E(K)$ and $E(K')$ have the same rank and the same torsion, it does not mean that the inclusion $E(K) \subset E(K')$ is an equality (we just have a subgroup of finite index).

    For instance, consider $K = \mathbb{Q}$, $K' = \mathbb{Q}(i)$ and $E/\mathbb{Q}$ given by the minimal model $y^2 = x^3 + x^2 + 4$ (a short Weierstrass equation is $y^2 = x^3 - 432x + 190080$; this is the curve with labels 112.a2 and 392.1-a1 from the database [LMF22]). The Mordell–Weil groups $E(\mathbb{Q})$ and $E(\mathbb{Q}(i))$ both happen to be isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, but $P := (-2i, 2i + 2) \in E(\mathbb{Q}(i)) \smallsetminus E(\mathbb{Q})$, so we definitely do *not* have an equality $E(\mathbb{Q}) = E(\mathbb{Q}(i))$. In fact, this point P generates the torsion-free part of $E(\mathbb{Q}(i))$, while $Q := (0, 2) = 2P + (-2, 0) \in E(\mathbb{Q})$ generates the torsion-free part of $E(\mathbb{Q})$. Here the torsion of both groups is generated by $(-2, 0)$.

Appendix A

Proof of the upper bound on the Brauer–Siegel ratio

In this appendix, we provide a detailed version (with explicit constants) of the proof of the upper bound on the Brauer–Siegel ratio $\mathrm{BS}(E/K) \leqslant 1 + o(1)$ from [HP16], as stated in theorem 2.2.4. We do not claim originality here; the goal is only to make sure that we can safely remove the dependency on $q := |k|$ (the cardinality of the field of constants).

In what follows, we will use the "complex-analytic" version of the L-function $\mathcal{L}(E/K, s) := L(E/K, T = q^{-s})$ as in remark 1.3.33; in particular we have $\mathcal{L}^*(E/K) = \log(q)^r L^*(E/K)$ where r is the (analytic) rank of E/K. We point out that in [HP16, Remark 2.5], the regulator is defined using the pairing $\log(q) \cdot \langle -, - \rangle_{\mathrm{NT}}$ (see remark 1.3.17), where log denotes the natural logarithm (in base e). In particular, the Brauer–Siegel ratio of E/K as defined in [HP16] is equal to $\mathrm{BS}(E/K) + \frac{r \log\log(q)}{\log H(E/K)}$ (using our notation from definition 2.2.1).

The general idea in [HP16] to get an upper bound on the Brauer–Siegel ratio can be described in five steps (we use the notations from theorem 2.2.4):

1. Get "easy" upper bounds on $|\log(\mathcal{L}(E/K, s))|$, from Euler product and from Weil conjectures, where $\mathrm{Re}(s) = 1 + \rho$ or $\mathrm{Re}(s) = 3/2 + \rho$ with $\rho \in]0, 1/3[$. See proposition A.4.
2. Apply Phragmen–Lindelöf principle on the strip $\{s \in \mathbb{C} \ : \ 1 + \rho \leqslant \mathrm{Re}(s) \leqslant \frac{3}{2} + \rho\}$, where $\rho \in]0, 1/3[$ (proposition A.5). In particular, we get an upper bound on $|\log(\mathcal{L}(E/K, s))|$ for $\mathrm{Re}(s) = 1 + 2\rho$.
3. Use the functional equation of $\mathcal{L}(E/K, s)$ to get an upper bound on $|\log(\mathcal{L}(E/K, s))|$ for $\mathrm{Re}(s) = 1 - 2\rho$. Then apply Phragmen–Lindelöf theorem again, on a strip containing $s = 1$. See proposition A.6.
4. Cauchy integral formula together with Brumer's bound provide an upper bound on $|\mathcal{L}^*(E/K)|$ (proposition A.7).
5. Finally, BSD formula (from conjecture 1.3.34) gives the desired result (theorem 2.2.4).

We start by writing the zeta function of $K = k(C)$ as

$$\zeta_K(s) = \frac{Q_K(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})},$$

where $Q_K(T) = \prod_{j=1}^{2g} (1 - a_j T) \in \mathbb{Z}[T]$ has degree $2g$, and $|a_j| = q^{1/2}$ for every j. We have an easy estimate:

Lemma A.1. *Let $s \in \mathbb{C}$ with $\sigma = \mathrm{Re}(s) \in]1, 2[$. Then*

$$|\zeta_K(s)| \leqslant \frac{3 \cdot 2^{2g}}{\sigma - 1}.$$

We could replace the constant 3 in the numerator by any real number $c > \max\{\zeta_{\mathbb{P}^1_{\mathbb{F}_2}}(2); \frac{2}{\ln(2)}\} = \max\{8/3, 2/\ln(2)\} = 2/\ln(2) \simeq 2.885$.

Proof of lemma A.1. — To begin with, we have

$$|Q_K(q^{-s})| = \prod_{j=1}^{2g} |1 - a_j q^{-s}| \leqslant (1 + q^{1/2-\sigma})^{2g} \leqslant 2^{2g},$$

since $1/2 - \sigma < 1 - \sigma < 0$.

Thus it is sufficient to show that

$$|\zeta_{k(t)}(s)| = |\zeta_{\mathbb{P}^1_k}(s)| = \left| \frac{1}{(1 - q^{-s})(1 - q^{1-s})} \right| \leqslant \frac{3}{\sigma - 1}$$

Recall that $|1 - q^{-s}| \geqslant |1 - |q^{-s}|| = 1 - q^{-\sigma} > 0$, so that

$$|\zeta_{\mathbb{P}^1_k}(s)| \leqslant \frac{1}{(1 - q^{-\sigma})(1 - q^{1-\sigma})}$$

Therefore we want to show $\sigma - 1 \leqslant 3(1 - q^{-\sigma})(1 - q^{1-\sigma})$ for every $\sigma \in]1, 2[$, i.e.

$$3(1 - x)(1 - qx) + \ln(x)/\ln(q) + 1 \geqslant 0$$

for every $x = q^{-\sigma} \in]q^{-2}, q^{-1}[$. Since $\ln(q) > 0$, this is equivalent to show that

$$f_q(x) := 3\ln(q)(1 - x)(1 - qx) + \ln(qx) \geqslant 0$$

is non-negative on $]q^{-2}, q^{-1}[$. This follows from the three easy facts listed below:

- Firstly, $f_q(q^{-1}) = 0$ is clear.
- Secondly, we have $f_q(q^{-2}) > 0$. Indeed, since $q \geqslant 2$, we get

$$\begin{aligned} f_q(q^{-2}) &= \ln(q) \cdot (3(1 - q^{-2})(1 - q^{-1}) - 1) \\ &\geqslant \ln(q) \cdot (3(1 - 2^{-2})(1 - 2^{-1}) - 1) \\ &= \ln(q) \cdot \left(3 \cdot \frac{3}{8} - 1\right) > 0. \end{aligned}$$

- Thirdly, we check that $f'_q(q^{-1}) < 0$. Indeed, we have

$$f'_q(x) = 3\ln(q)(2qx - q - 1) + \frac{1}{x},$$

and using the inequality $q \geqslant 2$ again, we obtain

$$\begin{aligned} f'_q(q^{-1}) &= 3\ln(q)(1 - q) + q = (1 - q)(3\ln(q) - 1) + 1 \\ &\leqslant -(3\ln(q) - 1) + 1 = 2 - 3\ln(q) \leqslant 2 - 3\ln(2) < 0. \end{aligned}$$

Notice that $f'_q(x) = g(x)/x$, where g is a convex quadratic function of x. Let $a, b \in \mathbb{R}$ be the two zeros of f'_q and note that we have $a < q^{-1} < b$ by the third observation $f'_q(q^{-1}) < 0$ above.

— If $f_q'(q^{-2}) \geqslant 0$, then f_q is increasing on $]q^{-2}, a]$ and is decreasing on $[a, q^{-1}[$, so that $f_q(x) \geqslant 0$ holds true for every $x \in [q^{-2}, q^{-1}]$, since $f_q(q^{-2}) > 0 = f_q(q^{-1})$.

— If $f_q'(q^{-2}) < 0$, then f_q is decreasing on $[q^{-2}, q^{-1}]$, so that f_q is non-negative on this interval, because $f_q(q^{-2}) > 0 = f_q(q^{-1})$.

In all cases, we have $f_q \geqslant 0$ over $]q^{-2}, q^{-1}[$, as desired. ■

Moreover, recall that if E/K is non-constant, then by theorem 1.3.30, we can write the L-function as a polynomial

$$\mathcal{L}(E/K, s) = \prod_{j=1}^{D_{E/K}} (1 - \beta_j q^{-s}) \tag{A.1}$$

for every $s \in \mathbb{C}$, where $|\beta_j| = q$ for every j. On the other hand, the Euler product

$$\mathcal{L}(E/K, s) = \prod_{v \in |C|} \prod_{j=1}^{2} (1 - a_{v,j} q_v^{-s})^{-1} \tag{A.2}$$

(valid whenever $\mathrm{Re}(s) > 3/2$), satisfies[1] $|a_{v,j}| \leqslant q_v^{1/2}, q_v = q^{\deg(v)}$.

Equations (A.1) and (A.2) yield the upper bounds given respectively in lemmas A.3 and A.2.

Lemma A.2. *If $\sigma = \mathrm{Re}(s) > 3/2$, then*

$$|\mathcal{L}(E/K, s)| \leqslant \zeta_K(\sigma - 1/2)^{2d} \quad \textit{and} \quad |\log(\mathcal{L}(E/K, s))| \leqslant 2d \, \log(\zeta_K(\sigma - 1/2)). \qquad ⌟$$

Proof. — The first inequality follows from the second one, so it is sufficient to prove the second inequality. From (A.2), we have $\log(\mathcal{L}(E/K, s)) = -\sum_v \sum_j \log(1 - a_{v,j} q_v^{-s})$. Recall that if $|z| < 1$, then

$$|\ln(1 - z)| = \left| -\sum_{n \geqslant 1} \frac{z^n}{n} \right| \leqslant \sum_{n \geqslant 1} \frac{|z|^n}{n} = -\ln(1 - |z|) = |\ln(1 - |z|)|. \tag{A.3}$$

Since $|a_{v,j} q_v^{-s}| \leqslant q_v^{1/2-\sigma} < 1$, we get

$$\begin{aligned} |\log(\mathcal{L}(E/K, s))| &\leqslant \sum_v \sum_j -\log(1 - |a_{v,j}| q_v^{-\sigma}) \\ &\leqslant \sum_v \sum_j -\log(1 - q_v^{1/2-\sigma}) = \sum_v 2d \log((1 - q_v^{1/2-\sigma})^{-1}) \\ &= 2d \log(\zeta_K(\sigma - 1/2)). \end{aligned}$$ ■

Lemma A.3. *Let $s \in \mathbb{C}$ with $\sigma := \mathrm{Re}(s) > 1$. Then*

$$|\log(\mathcal{L}(E/K, s))| \leqslant D_{E/K} |\log(1 - q^{1-\sigma})|. \qquad ⌟$$

[1] For all places v of good reduction for E, we have an equality $|a_{v,j}| = q_v^{1/2}$.

Proof. — By equations (A.1) and (A.3), we have

$$\begin{aligned}|\log \mathcal{L}(E/K,s)| &\leqslant \sum_{j=1}^{D} |\log(1-\beta_j q^{-s})| \\ &\leqslant \sum_{j=1}^{D} |\log(1-q^{1-\sigma})| = D_{E/K}|\log(1-q^{1-\sigma})|.\end{aligned}$$

■

We can now prove lemma 7.2 from [HP16].

Proposition A.4. *Set $\beta := 3\cdot 2^{2g}$. Let $\rho \in]0,1/\beta]$.*

- *If $\sigma := \mathrm{Re}(s) \in [1+\rho, 3/2]$, then*
$$|\log(\mathcal{L}(E/K,s))| \leqslant 2D_{E/K}|\log(\rho)|$$
- *If $\sigma := \mathrm{Re}(s) \in [3/2+\rho, 2[$, then*
$$|\log(\mathcal{L}(E/K,s))| \leqslant 4|\log(\rho)|.$$

⌟

Proof. — The first part readily follows from lemma A.3 and from the inequalities

$$|\log(1-q^{1-\sigma})| \leqslant 2\log\left(\frac{1}{\sigma-1}\right) \leqslant 2\log\left(\frac{1}{\rho}\right) = 2|\log(\rho)|.$$

the first one being valid if $q \geqslant 2$ and $\sigma \in]1, \frac{3}{2}]$.

The second part follows from lemmas A.1 and A.2: if $\sigma \in]3/2+\rho, 2[$ then

$$|\log(\mathcal{L}(E/K,s))| \leqslant 2\,\log(\zeta_K(\sigma-1/2)) \leqslant 2\log\left(\frac{3\cdot 2^{2g}}{\rho}\right) = 2(\log(3\cdot 2^{2g})+|\log(\rho)|) \leqslant 4|\log(\rho)|.$$

■

We now deduce lemma 7.3 from [HP16].

Proposition A.5. *Set $\beta := 3\cdot 2^{2g}$. Assume that $D_{E/K} \geqslant 9$ and that $\rho := \frac{1}{2}\frac{\log\log D_{E/K}}{\log D_{E/K}} \leqslant 1/\beta$. Define $\gamma := 2\rho$.*

Then for every $t \in \mathbb{R}$, we have

$$|\log(\mathcal{L}(E/K, 1+\gamma+it))| \leqslant 12 D_{E/K}\frac{\log\log(D_{E/K})}{\log D_{E/K}}.$$

⌟

Proof. — Consider the strip $S := \{s \in \mathbb{C} \ : \ 1+\rho \leqslant \mathrm{Re}(s) \leqslant \frac{3}{2}+\rho\}$. We apply Phragmen–Lindelöf theorem to[2] $\frac{\log \mathcal{L}(E/K,s)}{D_{E/K}^{1-2(s-1-\rho)}}$ over this strip, where we know the bounds on the boundaries thanks to proposition A.4. Then for every $\rho \in]0,1/\beta], \gamma \in [\rho, \rho+\frac{1}{2}]$ and every $t \in \mathbb{R}$, one has

$$|\log(\mathcal{L}(E/K, 1+\gamma+it))| \leqslant 4 D_{E/K}^{1-2(\gamma-\rho)}|\log(\rho)|. \tag{A.4}$$

[2]Notice that when $s = 1+\gamma+it$ then $|D_{E/K}^{1-2(s-1-\rho)}| = D_{E/K}^{1-2(\gamma-\rho)}$.

Define $\rho := \frac{1}{2}\frac{\log\log D_{E/K}}{\log D_{E/K}} \in]0, 1/2]$, and set $\gamma := 2\rho \in [\rho, \rho + \frac{1}{2}]$. Since we assume that $\rho \leqslant 1/\beta$, the upper bound (A.4) yields

$$\begin{aligned}
|\log(\mathcal{L}(E/K, 1+\gamma+it))| &\leqslant 4D_{E/K}^{1-2\rho}|\log(\rho)| \\
&= 4D_{E/K} \cdot D_{E/K}^{-\frac{\log\log D_{E/K}}{\log D_{E/K}}} \left|\log\left(\frac{\log\log D_{E/K}}{2\log D_{E/K}}\right)\right| \\
&= 4\frac{D_{E/K}}{\log D_{E/K}}|\log\log\log(D_{E/K}) - \log\log(D_{E/K}) - \log(2)| \\
&\leqslant 4\frac{3D_{E/K}}{\log D_{E/K}}\log\log(D_{E/K}),
\end{aligned}$$

where the last inequality holds if $D_{E/K} \geqslant 9$. ■

We now use the functional equation for $\mathcal{L}(E/K, s)$ to get an upper bound on the vertical line $\mathrm{Re}(s) = 1 - \rho$, and then another application of Phragmen–Lindelöf principle will imply the following result.

Proposition A.6. *There exists a constant $D_0 > 0$ (depending on g but not on q) such that whenever $D_{E/K} \geqslant D_0$, we have*

$$|\mathcal{L}(E/K, s)| \leqslant \exp\left(D_{E/K}\frac{\log\log(D_{E/K})}{\log D_{E/K}}(13 + \log(q))\right),$$

for every $s \in S'$ where $S' := \{s \in \mathbb{C} \ : \ 1 - \gamma \leqslant \mathrm{Re}(s) \leqslant 1 + \gamma\}$ and $\gamma := \dfrac{\log\log(D_{E/K})}{\log D_{E/K}}$. ⌟

Proof. — The functional equation of $\mathcal{L}(E/K, s)$ is $\mathcal{L}(E/K, 2-s) = \pm q^{(s-1)D_{E/K}}\mathcal{L}(E/K, s)$ by theorem 1.3.30. In particular,

$$\mathcal{L}(E/K, 1-\gamma-it) = \mathcal{L}(E/K, 2-(1+\gamma+it)) = \pm q^{(\gamma+it)D_{E/K}}\mathcal{L}(E/K, 1+\gamma+it)$$

Using proposition A.5, we deduce that when $D_{E/K}$ is large enough ($D_{E/K} \to \infty$), we have the inequality

$$|\log \mathcal{L}(E/K, 1-\gamma-it)| \leqslant D_{E/K}\frac{\log\log(D_{E/K})}{\log D_{E/K}}(13 + \log(q))$$

for every $t \in \mathbb{R}$, where $\gamma := \dfrac{\log\log(D_{E/K})}{\log D_{E/K}}$.

Combining this upper bound with the one obtained in proposition A.5, we deduce from Phragmen–Lindelöf principle that the above inequality holds true whenever $1 - \gamma - it$ is replaced by $s \in S'$. This terminates the proof. ■

We can now derive an upper bound for the derivatives of $\mathcal{L}(E/K, s)$ at $s = 1$ using Cauchy integral formulas, and Brumer's bound from theorem 2.2.6. This corresponds to theorem 7.5 in [HP16].

Proposition A.7. *There exists a constant $c_1 > 0$ (depending on g and the constant c_0 given in the statement of theorem 2.2.4, but does not depend on q) such that*

$$\log|\mathcal{L}^*(E/K)| \leqslant f_{E/K}\frac{\log\log(f_{E/K})}{\log f_{E/K}}(13 + c_1\log(q)).$$

Proof. — Let C be the circle of center 1 and radius γ as in proposition A.6, and r be the analytic rank of E/K. Then Cauchy integral formula

$$\frac{\mathcal{L}^{(r)}(E/K,1)}{r!} = \frac{1}{2\pi i}\int_C \frac{\mathcal{L}(E/K,z)}{(z-1)^{r+1}}\,\mathrm{d}z$$

yields

$$\begin{aligned}|\mathcal{L}^*(E/K)| = \left|\frac{\mathcal{L}^{(r)}(E/K,1)}{r!}\right| &\leqslant \frac{1}{2\pi}\mathrm{length}(C)\cdot\gamma^{-(r+1)}\cdot\max_{z\in C}|\mathcal{L}(E/K,z)|\\ &= \gamma^{-r}\cdot\max_{z\in C}|\mathcal{L}(E/K,z)|.\end{aligned}$$

By Brumer's theorem 2.2.6 and since we assume that $q \leqslant f_{E/K}^{c_0}$, we have

$$\begin{aligned}r &\leqslant \frac{f_{E/K}+4g_C-4}{2\log(f_{E/K})}\log(q) + \frac{c_0 f_{E/K}\log(q)\log(f_{E/K})}{\log(f_{E/K})^2(1-2^{-1/2})^2} + 1 + 2\beta_K + \frac{c_K c_0\log(f_{E/K})}{2\log(f_{E/K})}.\\ &\leqslant \frac{f_{E/K}+4g_C-4}{2\log(f_{E/K})}\log(q) + \frac{c_0\cdot f_{E/K}\log(q)}{\log(f_{E/K})(1-2^{-1/2})^2} + \mathcal{O}_{c_0,g}(1)\\ &\leqslant c_1'\cdot\frac{f_{E/K}\log(q)}{\log(f_{E/K})}\end{aligned} \tag{A.5}$$

for some $c_1' > 0$ which depends on g, c_0 but not on q.

Since C is contained in the strip S', proposition A.6 implies that if $f_{E/K}$ is large enough, then

$$\begin{aligned}|\mathcal{L}^*(E/K)| &\leqslant \left(\frac{\log(D_{E/K})}{\log\log D_{E/K}}\right)^r \exp\left(D_{E/K}\frac{\log\log(D_{E/K})}{\log D_{E/K}}(13+\log(q))\right)\\ &\leqslant \exp\left(c_1'\cdot\frac{f_{E/K}\log(q)}{\log(f_{E/K})}\log\log D_{E/K} \;+\; D_{E/K}\frac{\log\log(D_{E/K})}{\log D_{E/K}}(13+\log(q))\right).\end{aligned}$$

Thus, since $D_{E/K} \sim f_{E/K}$ (by theorem 1.3.30, as g is fixed), we get

$$\log|\mathcal{L}^*(E/K)| \leqslant f_{E/K}\frac{\log\log(f_{E/K})}{\log f_{E/K}}(13 + c_1\log(q)),$$

where $c_1 := 1 + c_1'$. This concludes the proof. ■

Finally, we are able and ready to prove the upper bound on the Brauer–Siegel ratio, as stated in theorem 2.2.4.

Proof of theorem 2.2.4. — By theorem 1.3.35, all elliptic curves E/K in the statement satisfy the BSD formula.

Fix $\epsilon > 0$. On the one hand, we have $|E(K)_{\mathrm{tors}}|^2 \ll \mathcal{O}(1)$ by proposition 2.1.4, where the implicit constant depends only on g (note that we assumed that $f(E/K)^{c_0} \geqslant q = |k|$, so this forces E/K to be non-constant). On the other hand, $c_v(E/K) \geqslant 1$ for every place v, so BSD formula leads to

$$|Ш(E/K)| \cdot \mathrm{Reg}(E/K) \leqslant L^*(E/K) \cdot q^{g-1} \cdot H(E/K).$$

As mentioned in remark 1.3.33, we have $L^*(E/K) = \log(q)^{-r}\mathcal{L}^*(E/K)$ where r is the rank of E/K. When $q > 2$, we have $L^*(E/K) \leqslant \mathcal{L}^*(E/K)$ since $\log(q) > 1$. When $q = 2$, we have $\log(q)^{-1} > 1$ so equation (A.5) yields

$$(\log(q)^{-1})^r = \exp[r \cdot (-\log\log(q))] \leqslant \exp\left(c_1' \cdot \frac{f_{E/K}\log(2)}{\log(f_{E/K})} \cdot (-\log\log(2))\right)$$

Let us set $c_2' := c_1' \cdot \frac{\log(2)}{-\log\log(2)} > 0$ and $c_2 := \max\{c_2', 1\}$ (which does not depend on q). Thus in all cases we have $(\log(q)^{-1})^r \leqslant \exp\left(c_2 \cdot \frac{f_{E/K}}{\log(f_{E/K})}\right)$.

Since $f_{E/K} \leqslant \deg\left(\Delta_{\min}(E/K)\right)$ by theorem 2.2.2, we get

$$f_{E/K} \cdot \frac{\log\log f_{E/K}}{\log f_{E/K}} \ll_\epsilon \epsilon \cdot \deg\left(\Delta_{\min}(E/K)\right),$$

as $f_{E/K} \to +\infty$. Thereby, proposition A.7 gives, when $f_{E/K} \to \infty$:

$$\begin{aligned}
|Ш(E/K)| \cdot \mathrm{Reg}(E/K) &\ll_g H(E/K) \cdot q^{g-1} \cdot \log(q)^{-r} \cdot \\
&\qquad \cdot \exp\left(f_{E/K}\frac{\log\log(f_{E/K})}{\log f_{E/K}}(13 + c_1\log(q))\right) \\
&\ll_g H(E/K)^{1+\epsilon} \cdot \exp\left(c_2 \cdot \frac{f_{E/K}}{\log(f_{E/K})}\right) \cdot \\
&\qquad \cdot \exp\left(f_{E/K}\frac{\log\log(f_{E/K})}{\log f_{E/K}}(13 + c_1\log(q))\right) \\
&\leqslant H(E/K)^{1+\epsilon} \cdot \exp(c_2 \cdot \epsilon \cdot f_{E/K}) \cdot \\
&\qquad \cdot \exp\left[\epsilon \cdot \deg\left(\Delta_{\min}(E/K)\right)(13 + c_1\log(q))\right] \\
&\leqslant H(E/K)^{1+\epsilon} \cdot H(E/K)^{\frac{12c_2}{\log(q)}\epsilon} \cdot H(E/K)^{\frac{1}{\log(q)}\cdot\epsilon\cdot(13+c_1\log(q))} \\
&\leqslant H(E/K) \cdot H(E/K)^{\epsilon\cdot(1+12c_2\log(2)^{-1}+13\log(2)^{-1}+c_1)}
\end{aligned}$$

The third inequality comes from the fact that $\frac{\log\log(t)}{\log(t)} \to 0$ and $\frac{1}{\log(t)}$ when $t \to +\infty$.

In other words, we proved that for every $\epsilon > 0$, there are some $B_{\epsilon,g,c_0}, B'_{\epsilon,g,c_0} > 0$ such that $f_{E/K} \geqslant B_{\epsilon,g,c_0}$ implies

$$|Ш(E/K)| \cdot \mathrm{Reg}(E/K) \leqslant B'_{\epsilon,g,c_0} \cdot H(E/K)^{1+\epsilon},$$

for every E/K as in the statement of the theorem, which finishes the proof. ■

List of symbols

$(\mathbb{Z}/d\mathbb{Z})/\langle a\rangle^\times$ Set of orbits of the action of the cyclic subgroup $\langle a\rangle \leqslant (\mathbb{Z}/d\mathbb{Z})^\times$ on $\mathbb{Z}/d\mathbb{Z}$, page 61

$Ш(E/K)$ Tate–Shafarevich group of E over K, page 35

$\{x\}$ Fractional part of x, page 61

$\langle -,-\rangle_{\mathrm{NT}}$ Néron–Tate pairing $E(K)\times E(K)\to\mathbb{R}$, page 38

$A_E(v,j)$ For an elliptic curve E, a place v and a multiple j of $\deg(v)$, we set $A_E(v,j) := |k|^j + 1 - \left|\overline{E_v}(k_j)\right|$, page 46

A_n Elliptic curve $y^2+y=x^3+t^{2^n+1}$ over $\mathbb{F}_2(t)$, page 98

$\alpha'_{b,b',\epsilon}$ A certain map $\bigsqcup_{n\geqslant 1}\widehat{k_n^\times}\longrightarrow\mathbb{C}$, page 194

$\alpha_{b,b'}$ A certain map $\bigsqcup_{n\geqslant 1}\widehat{k_n^\times}\longrightarrow\mathbb{C}$, page 114

$a_v(E)$ For an elliptic curve E and a place v, we set $a_v(E) := |\mathbb{F}_v| + 1 - \left|\overline{E_v}(\mathbb{F}_v)\right|$, page 46

$B_p^n(x,r)$ Open L^p-ball centered at x of radius r (p is omitted if $p=2$, (x,r) omitted if $(x,r)=(0,1)$), page 21

$\mathrm{BS}(E/K)$ Brauer–Siegel ratio of E over K, page 83

$\beta(\vec{b})$ Integer appearing as p-adic valuation of some Jacobi sums, page 71

C'_n Hyperelliptic curve with affine model $u^2+u=t^{2^n+1}$ over $\mathbb{F}_2$, page 99

$C_b(\psi,n)$ Character sum $\sum_{x\in k_n}\psi(x^3+bx)$, page 120

$C_{n,b}$ Superelliptic curve with affine model $v^{p^n+1}=u^p+bu$ over $\mathbb{F}_{p^n}$, page 135

$|C|$ Set of closed points of an algebraic curve C, page 32

$c(E/K)$ Global Tamagawa number of E over K, page 35

$c_v(E/K)$ Local Tamagawa number of E over K, page 35

$c_{m,b,b'}$ Coefficients appearing in the series $\log L(E'_{m,b,b'}/k(t),T)$, page 197

$D(E/K)$ Degree of the L-function of E over K (also denoted $D_{E/K}$ in appendix A), page 47

$D(L)$ Sphere packing density of a lattice L (between 0 and 1), page 23

$\Delta_{\min}(E/K)$ Minimal discriminant of E over K, page 34

$\delta(L)$	Center sphere packing density of a lattice L, page 23
$\delta_\ell(C)$	Center (lattice packing) density of a centrally symmetric convex body C, page 24
$\delta_\ell(n)$	Center (lattice packing) density of n-dimensional euclidean balls, page 25
$\mathrm{disc}(L)$	Discriminant of a lattice L, page 17
$E'_{m,b,b'}$	Elliptic curve $y^2 = x^3 + b + b't^m$ over $\mathbb{F}_q(t)$, page 193
$E(K)^0$	Narrow Mordell–Weil lattice of E over K, page 42
$E_{m,b,b'}$	Elliptic curve $y^2 = x^3 + bx + b't^m$ over $\mathbb{F}_q(t)$, page 113
$\mathscr{E}$	Elliptic surface (over C) attached to an elliptic curve E over $k(C)$, page 36
$\epsilon_{m,b,b',k}$	A certain polynomial of degree $\leqslant 2$ over $\mathbb{Z}$, page 114
$\mathcal{E}$	Néron model of an elliptic curve E over $k(C)$, page 36
$e(X)$	Topological Euler number of a proper variety X, page 37
$\mathbb{F}_q$	Finite field with q elements, page 32
$\mathfrak{f}(E/K)$	Conductor of E over $K = k(C)$ (seen as a divisor on C), page 35
$f(E/K)$	Degree of the conductor divisor of E over $K = k(C)$, page 35
$G(\chi)$	Gauss sum, page 63
$G_{d,\epsilon}(a,x)$	A certain sum of fractional parts related to the p-adic valuation of Jacobi sums, page 213
g	Function defined by $g(x_1,x_2,x_3) := \{x_1\} + \{x_2\} + \{x_3\} + \{-x_1 - x_2 - x_3\}$, page 213
$H(E/K)$	Height of an elliptic curve E/K, page 48
$\check{\mathrm{H}}^n(S/R,\mathcal{F})$	Amistur–Čech cohomology group, page 177
$\hat{h}$	Néron–Tate height $\hat{h} : E(K) \to \mathbb{R}_{\geqslant 0}$, page 38
$J(\chi_1,...,\chi_n)$	Jacobi sum, page 63
$J_{k,m,r}$	A certain triple Jacobi sum $J\big(\theta_{k_{u(r)},m,r}\ ;\ \psi_{k_{u(r)}}\ ;\ \lambda_{k_{u(r)}}\big)$ with a cubic character and the Legendre symbol, page 213
$\widehat{k^\times}$	Group of multiplicative characters on k, page 60
$\kappa(L)$	Kissing number a lattice L, page 17
k_n	Extension of degree n of a finite field k, page 61
$L'_{m,b,b',q}$	Narrow Mordell–Weil lattice of $y^2 = x^3 + b + b't^m$ over $\mathbb{F}_q(t)$, page 193
$L'_{n,b}$	Narrow Mordell–Weil lattice of $y^2 = x^3 + bx + t^{3^n+1}$ over $\mathbb{F}_{3^{2n}}(t)$, page 146
$L(E/K)$	L-function of E over K, page 47
$L^*(E/K)$	Special value of the L-function of E/K at $s = 1$, page 48

$L_{m,b,b',q}$ Narrow Mordell–Weil lattice of the elliptic curve $y^2 = x^3 + bx + b't^m$ over $\mathbb{F}_q(t)$, page 114

$\lambda_1(L)$ Minimal norm of a non-zero vector in a lattice L, page 17

λ_k Legendre symbol, page 61

$\mathcal{M}$ The set $\{2, 3, 4, 5, 6, 9, 12, 18, 24, 30, 60\}$ of 11 integers, page 213

$\mathrm{N}_{k'/k}$ Norm map $k'^{\times} \to k^{\times}$, page 61

$\mathrm{ord}^{\times}(a \bmod d)$ Multiplicative order of $a \in (\mathbb{Z}/d\mathbb{Z})^{\times}$, page 61

$\rho(E/K)$ Analytic rank of E over K, page 48

$S(d)$ A certain set of polynomials of degree $\leqslant d/2$, page 187

$S_\phi(E/K)$ Subset of K/K^3 isomorphic to the ϕ-Selmer group of E/K, page 181

$S_{b,b'}(\chi, n)$ Character sum $\sum_{z,x \in k_n} \lambda_{k_n}(x^3 + bx + b'z)\chi(z)$, page 118

$\mathrm{Sel}_\phi(E/K)$ ϕ-Selmer group of E over K, page 181

$\mathcal{S}$ A certain set of 34 rational numbers related to purity of Jacobi sums, page 213

$\sigma(E/K)$ Szpiro ratio of E over K, page 83

$\sigma_b(j, t)$ Sum of $\lambda_{\mathbb{F}_{3^{2nj}}}(x^3 + bx + t)$ over $x \in \mathbb{F}_{3^{2nj}}$, page 135

Θ Teichmüller character $\Theta : \overline{\mathbb{F}_p}^{\times} \to \overline{\mathbb{Q}}^{\times}$, page 66

$\theta_{\mathbb{F}_{q^n},d,r}$ Character on $\mathbb{F}_{q^n}^{\times}$ of order dividing d, page 68

$u_{q,d}(r)$ Cardinality of the orbit of $r \in \mathbb{Z}/d\mathbb{Z}$ under the action of $\langle q \bmod d \rangle \leqslant (\mathbb{Z}/d\mathbb{Z})^{\times}$, page 68

V_K Set of (representatives of) all places of K, page 33

$\omega_{q,D}$ Character of order D on $\mathbb{F}_{q^{\mathrm{ord}(q \bmod D)}}^{\times}$, page 71

$X(m, \epsilon)$ A certain subset of $\mathbb{Z}/m\mathbb{Z}$, page 194

$X_m(n)$ A certain set of multiplicative characters, page 121

X_n Space of unimodular lattices, $\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$, page 17

$\chi(S)$ Euler characteristic of a surface S, page 37

ψ_{k_s} Character of order exactly 3 on $k_s^{\times}$, page 194

$Z(C/k, T)$ Zeta function of a curve C over a finite field k, page 104

$Z(m)$ A certain subset of $\mathbb{Z}/d(m)\mathbb{Z}$ where $d(m) = 4m/\gcd(2, m)$, page 114

Bibliography

[ACH+20] Nima Afkhami-Jeddi, Henry Cohn, Thomas Hartman, David de Laat, and Amirhossein Tajdini. High-dimensional sphere packing and the modular bootstrap. *Journal of High Energy Physics*, (66), 12 2020. (↑ 2, 12, 31)

[AEN] Yoshinori Aono, Thomas Espitau, and Phong Q. Nguyen. Random lattices : theory and practice. Preprint available at `https://espitau.github.io/bin/random_lattice.pdf`. (↑ 19, 27)

[AGTT21] Sarah Arpin, Richard Griffon, Libby Taylor, and Nicholas Triantafillou. On the arithmetic of a family of superelliptic curves. *arXiv preprint arXiv:2105.02812*, 2021. To appear in *Manuscripta Mathematica*. (↑ 59, 95)

[AHP18] Pascal Autissier, Marc Hindry, and Fabien Pazuki. Regulators of Elliptic Curves. *International Mathematics Research Notices*, 2021(7):4976–4993, 12 2018. (↑ 95)

[Aki96] Shigeki Akiyama. On the pure Jacobi sums. *Acta Arithmetica*, 75(2):97–104, 1996. (↑ 224)

[Aok96] Noboru Aoki. Abelian fields generated by a Jacobi sum. *Rikkyo Daigaku sugaku zasshi*, 45(1):1–21, 1996. (↑ 224)

[Aok97] Noboru Aoki. On the purity problem of Gauss sums and Jacobi sums over finite fields. *Rikkyo Daigaku sugaku zasshi*, 46(2):223–233, 1997. (↑ 209)

[Aok04] Noboru Aoki. A finiteness theorem on pure Gauss sums. *Rikkyo Daigaku sugaku zasshi*, 53(2):145–168, 2004. (↑ 209)

[Aok12] Noboru Aoki. On pure Gauss sums. *Rikkyo Daigaku sugaku zasshi*, 61(2):133–165, 2012. (↑ 209)

[AP04] Yves Aubry and Marc Perret. Divisibility of zeta functions of curves in a covering. *Archiv der Mathematik*, 82:205–213, 2004. (↑ 138)

[Aut16] Pascal Autissier. Variétés abéliennes et théorème de Minkowski-Hlawka. *Manuscripta Mathematica*, 149:275–281, 2016. (↑ 28)

[AW22] Cécile Armana and Fu-Tsun Wei. Sturm-type bounds for modular forms over function fields. *Journal of Number Theory*, 237:67–98, 2022. (↑ 227)

[Bal92] Keith Ball. A lower bound for the optimal density of lattice packings. *International Mathematics Research Notices*, 1992(10):217–221, 05 1992. (↑ 2, 8, 12, 28, 143, 144, 147)

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). (↑ 3, 72)

[BDS04] Irene I. Bouw, Claus Diem, and Jasper Scholten. Ordinary elliptic curves of high rank over $\overline{\mathbb{F}_p}(x)$ with constant j-invariant. *Manuscripta Mathematica*, 114(4):487–501, Aug 2004. (↑ 5, 11, 57, 92)

[BE79] Bruce C Berndt and Ronald J Evans. Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer. *Illinois Journal of Mathematics*, 23(3):374–437, 1979. (↑ 224)

[Ber08] Lisa Berger. Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields. *Journal of Number Theory*, 128(12):3013 – 3030, 2008. (↑ 5, 50, 57)

[Ber12] Lisa Berger. Elliptic curves with bounded ranks in function field towers. *Acta Arithmetica*, 156(4):301–323, 2012. (↑ 5, 60, 205)

[BEW98] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams. *Gauss and Jacobi Sums*. Canadian Mathematical Society series of monographs and advanced texts. Wiley, 1998. (↑ 64, 71, 119, 140, 224)

[BG06] Enrico Bombieri and Walter Gubler. *Heights in Diophantine geometry*. Number 4. Cambridge university press, 2006. (↑ 96)

[BHP+20] Lisa Berger, Chris Hall, René Pannekoek, Jennifer Park, Rachel Pries, Shahed Sharif, Alice Silverberg, and Douglas Ulmer. *Explicit arithmetic of Jacobians of generalized Legendre curves over global function fields*, volume 266. American Mathematical Society, 2020. (↑ 59)

[BL95] Wieb Bosma and Hendrik W. Lenstra. Complete systems of two addition laws for elliptic curves. *Journal of Number theory*, 53(2):229–240, 1995. (↑ 175, 180)

[Bli35] Hans Frederick Blichfeldt. The minimum values of positive quadratic forms in six, seven and eight variables. *Mathematische Zeitschrift*, 39:1–15, 1935. (↑ 26)

[BMP06] P. Brass, W.O.J. Moser, and Janos Pach. *Research Problems in Discrete Geometry*. Springer, 2006. (↑ 28)

[Bou04] Nicolas Bourbaki. *Integration II, Chapters 7–9*. Springer, 2004. (↑ 18)

[Bro97] Antonios Broumas. Effective p-descent. *Compositio Mathematica*, 107(2):125–141, 1997. (↑ 173)

[Bru92] Armand Brumer. The average rank of elliptic curves I. *Inventiones mathematicae*, 109(1):445–472, Dec 1992. (↑ 59, 86)

[CdLS22] Henry Cohn, David de Laat, and Andrew Salmon. Three-point bounds for sphere packing. *arXiv preprint arXiv:2206.15373*, 2022. (↑ 31)

[CE03] Henry Cohn and Noam Elkies. New upper bounds on sphere packings. I. . *Ann. Math. (2)*, 157(2):689–714, 2003. (↑ 12, 22, 31)

[Che13] Hao Chen. On a generalization of Craig lattices. *Journal de Théorie des Nombres de Bordeaux*, 25(1):59–70, 2013. Previous version available on ArXiv as "New lattice sphere packings denser than Mordell-Weil lattices". (↑ 30)

[CHU13] Ricardo Conceição, Chris Hall, and Douglas Ulmer. Explicit points on the Legendre curve II. *Mathematical Research Letters*, 21, 07 2013. (↑ 56)

[CK04] Henry Cohn and Abhinav Kumar. The densest lattice in twenty-four dimensions. *Electronic Research Announcements of the American Mathematical Society*, 10(7):58–67, 2004. (↑ 1)

[CK09] Henry Cohn and Abhinav Kumar. Optimality and uniqueness of the Leech lattice among lattices. *Annals of mathematics*, pages 1003–1050, 2009. (↑ 1, 26)

[CKM+17] Henry Cohn, Abhinav Kumar, Stephen D. Miller, Danylo Radchenko, and Maryna Viazovska. The sphere packing problem in dimension 24. *Annals of Mathematics*, 185(3):1017–1033, 2017. (↑ 2, 26, 31)

[Coh07] Henri Cohen. *Number Theory, Volume I: Tools and Diophantine Equations*. Graduate Texts in Mathematics. Springer, 2007. (↑ 64, 67, 71, 211, 212)

[Con06] Brian Conrad. Chow's K/k-image and K/k-trace, and the Lang-Néron theorem. *Enseign. Math*, 52(2):37–108, 2006. (↑ 37)

[CS88] John Horton Conway and Neil Sloane. Low-dimensional lattices. III. Perfect forms. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 418(1854):43–80, 1988. (↑ 26)

[CS89] John Horton Conway and Neil Sloane. Errata: Low-Dimensional Lattices. III. Perfect Forms. *Proceedings of the Royal Society of London Series A*, 426(1871):441, 1989. (↑ 26)

[CS95] John H Conway and Neil JA Sloane. A lattice without a basis of minimal vectors. *Mathematika*, 42(1):175–177, 1995. (↑ 166)

[CS98] John Conway and Neil Sloane. *Sphere Packings, Lattices and Groups*, volume 290. Springer-Verlag, 3rd edition, 1998. (↑ 2, 8, 18, 26, 27, 28, 29, 30, 144, 147, 155, 156, 166)

[DO16] Christopher Davis and Tommy Occhipinti. Explicit points on $y^2 + xy - t^d y = x^3$ and related character sums. *Journal of Number Theory*, 168:13 – 38, 2016. (↑ 5, 58)

[Dok13] Tim Dokchitser. Notes on the parity conjecture. In *Elliptic curves, Hilbert modular forms and Galois deformations*, pages 201–249. Springer, 2013. (↑ 53, 103)

[Dok21] Tim Dokchitser. Models of curves over discrete valuation rings. *Duke Mathematical Journal*, 170(11):2519–2574, 2021. (↑ 95)

[Dol72] Igor Vladimirovich Dolgachev. The Euler characteristic of a family of algebraic varieties. *Matematicheskii Sbornik*, 131(2):297–312, 1972. Translated to English in *Mathematics of the USSR-Sbornik*, 18(2): 303–319, 1972. (↑ 37, 46)

[DS07] Claus Diem and Jasper Scholten. Ordinary elliptic curves of high rank over $\overline{\mathbb{F}_p}(x)$ with constant j-invariant II. *Journal of Number Theory*, 124(1):31 – 41, 2007. (↑ 57)

[DS11] Michele Elia Davide Schipani. Gauss Sums of the Cubic Character over $GF(2^m)$: an Elementary Derivation. *Bulletin of the Polish Academy of Sciences. Mathematics*, 59(1):11–18, 2011. (↑ 111)

[DSvW21] Léo Ducas, Marc Stevens, and Wessel van Woerden. Advanced lattice sieving on GPUs, with tensor cores. In *Advances in Cryptology – EUROCRYPT 2021*, pages 249–279. Springer, 2021. Preprint available at `https://eprint.iacr.org/2021/141.pdf`. (↑ 20)

[Dum95] Neil Dummigan. The Determinants of Certain Mordell-Weil Lattices. *American Journal of Mathematics*, 117(6):1409–1429, 1995. (↑ 94, 170)

[Elk94] Noam D. Elkies. Mordell-Weil lattices in characteristic 2: I. Construction and first properties. *International Math. Research Notices*, 8:343–361, 1994. (↑ 3, 4, 6, 9, 11, 30, 56, 81, 88, 98, 104, 107, 108, 110, 133, 134, 145, 149, 156, 163, 164, 170, 171, 179)

[Elk97] Noam D. Elkies. Mordell–Weil lattices in characteristic 2 II: The Leech lattice as a Mordell–Weil lattice. *Inventiones mathematicae*, 128:1–8, 1997. (↑ 3, 43)

[Elk01] Noam D. Elkies. Mordell–Weil Lattices in Characteristic 2, III: A Mordell–Weil Lattice of Rank 128. *Experimental Mathematics*, 10(3):467–473, 2001. (↑ 3, 30, 228)

[Eva81] Ronald J. Evans. Pure Gauss sums over finite fields. *Mathematika*, 28(2):239–248, 1981. (↑ 212)

[EvdGM] Bas Edixhoven, Gerard van der Geer, and Ben Moonen. *Abelian varieties*. Available at `http://gerard.vdgeer.net/AV.pdf`. (↑ 40, 41, 53, 92, 93, 95, 97, 103, 173)

[FIdD11] André Luiz Flores, J. Carmelo Interlando, Trajano Pires da Nabrega Neto, and José Othon Dantas Lopes. On a refinement of Craig's lattices. *Journal of Pure and Applied Algebra*, 215(6):1440 – 1442, 2011. (↑ 8, 29, 143, 144, 147)

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. Version 2.0 available at `https://www.math.auckland.ac.nz/~sgal018/crypto-book/main.pdf`. (↑ 38, 105, 171)

[Gd21] Richard Griffon and Guus de Wit. Elliptic curves with large Tate-Shafarevich groups over $\mathbb{F}_q(t)$. In *Arithmetic, Geometry, Cryptography and Coding Theory*, volume 770, pages 151–183. AMS, 2021. (↑ 60, 91)

[GM03] Daniel Goldstein and Andrew Mayer. On the equidistribution of Hecke points. *Forum Mathematicum*, 15:165–189, 2003. (↑ 20)

[GNR10] Nicolas Gama, Phong Q. Nguyen, and Oded Regev. Lattice enumeration using extreme pruning. In *Advances in Cryptology – EUROCRYPT 2010*, pages 257–278. Springer, 2010. (↑ 20)

[GPS02] S. D. Galbraith, S. M. Paulus, and N. P. Smart. Arithmetic on superelliptic curves. *Mathematics of Computation*, 71(237):393–405, 2002. (↑ 105, 135)

[Gri16] Richard Griffon. *Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques*. PhD thesis, Université Paris Diderot, France, 2016. (↑ 47, 49, 56, 57, 58, 67, 71, 73, 85, 86, 106, 120, 121)

[Gri17] Richard Griffon. Explicit L-functions and a Brauer-Siegel theorem for Hessian elliptic curves. *Journal de Théorie des Nombres de Bordeaux*, 30, 09 2017. (↑ 85)

[Gri19] Richard Griffon. Bounds on special values of L-functions of elliptic curves in an Artin–Schreier family. *European Journal of Mathematics*, 5(2):476–517, Jun 2019. (↑ 57)

[Gri20] Richard Griffon. A New Family of Elliptic Curves with Unbounded Rank. *Moscow Mathematical Journal*, 20(2):343–374, 2020. (↑ 57, 59, 228)

[Gro68] Alexander Grothendieck. Le groupe de Brauer III. In *Dix exposés sur la cohomologie des schémas*, pages 88–187. 1968. (↑ 173)

[Gro86] Helmut Groemer. Some basic properties of packing and covering constants. *Discrete & computational geometry*, 1(2):183–193, 1986. (↑ 22)

[Gro90] Benedict H. Gross. Group Representations and Lattices. *Journal of the American Mathematical Society*, 3(4):929–960, 1990. (↑ 93, 94)

[Gro11] Benedict H. Gross. Lectures on the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic of L-functions*, chapter 7, pages 169–210. American Mathematical Society, 2011. (↑ 40, 48, 49, 50, 53, 92, 103)

[Gru07] Peter Gruber. *Convex and discrete geometry*, volume 336. Springer, 2007. (↑ 22, 23)

[GS95a] Arnaldo Garcia and Henning Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. *Inventiones mathematicae*, 121(1):211–222, 1995. (↑ 30, 94)

[GS95b] Dorian M. Goldfeld and Lucien Szpiro. Bounds for the order of the Tate-Shafarevich group. *Compositio Mathematica*, 97(1-2):71–87, 1995. (↑ 44, 83, 91, 94)

[GU20] Richard Griffon and Douglas Ulmer. On the arithmetic of a family of twisted constant elliptic curves. *Pacific Journal of Mathematics*, 305(2):597–640, 2020. (↑ 57, 60, 204, 227, 228)

[GW20] Ulrich Görtz and Torsten Wedhorn. *Algebraic Geometry: Part I: Schemes. With Examples and Exercises*. Advanced Lectures in Mathematics. Springer, 2nd edition, 2020. Erratum available at `https://algebraic-geometry.de/errata/`. (↑ 32, 34, 38, 55, 92, 99, 105, 135, 138, 173, 175)

[Hal05] Thomas C. Hales. A proof of the Kepler conjecture. *Annals of mathematics*, 162(3):1065–1185, 2005. (↑ 26)

[Hei11] Bas Leonard Heijne. *Elliptic Delsarte surfaces*. PhD thesis, University of Groningen, 2011. (↑ 51, 58, 205)

[Hei12] Bas Heijne. The maximal rank of elliptic Delsarte surfaces. *Mathematics of Computation*, 81(278):1111–1130, 2012. (↑ 51, 58)

[Her50] Charles Hermite. Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objects de la théorie des nombres. *Journal für die reine und angewandte Mathematik*, 40:261–277, 1850. (↑ 1)

[Hos22] Yuichiro Hoshi. A note on fields generated by jacobi sums. 2022. Preprint available at `https://www.kurims.kyoto-u.ac.jp/~yuichiro/fjs.pdf`. (↑ 224)

[HP16] Marc Hindry and Amilcar Pacheco. Analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic. *Moscow Mathematical Journal*, 16(1):45–93, 2016. `https://doi.org/10.17323/1609-4514-2016-16-1-45-93`. (↑ 6, 12, 44, 49, 81, 83, 85, 90, 91, 94, 96, 97, 231, 234, 235)

[HS88] Marc Hindry and Joseph H. Silverman. The canonical height and integral points on elliptic curves. *Inventiones mathematicae*, 93(2):419–450, 1988. (↑ 44)

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine Geometry: An Introduction*. Graduate Texts in Mathematics. Springer New York, 2000. (↑ 37, 39, 40, 41, 93, 95, 96)

[Ill79] Luc Illusie. Complexe de de Rham-Witt et cohomologie cristalline. *Ann. Sci. École Normale Supérieure*, (4) 12:501–661, 1979. (↑ 50)

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*. Graduate texts in mathematics. Springer, 2nd edition, 1990. (↑ 139)

[Jon02] A. J. Jong. Counting elliptic surfaces over finite fields. *Moscow Mathematical Journal*, 2(2):281–311, 2002. (↑ 59)

[Kah06] Bruno Kahn. Sur le groupe des classes d'un schéma arithmétique. *Bulletin de la Société Mathématique de France*, 134(3):395–415, 2006. (↑ 37)

[Kel14] Timo Keller. *The conjecture of Birch and Swinnerton-Dyer for Jacobians of constant curves over higher dimensional bases over finite fields*. PhD thesis, University of Regensburg, October 2014. (↑ 97)

[KL78] G. A. Kabatiansky and V. I. Levenshtein. Bounds for packings on a sphere and in space. *Problemy Peredachi Informacii*, 14(1):3–25, 1978. English translation in Probl. Inf. Transm. 14 (1978), 1–17. (↑ 2, 31)

[Kob91] Neal Koblitz. Jacobi Sums, Irreducible Zeta-Polynomials, and Cryptography. *Canadian Mathematical Bulletin*, 34(2):229–235, 1991. (↑ 104)

[Kra77] Kenneth Kramer. Two-descent for elliptic curves in characteristic two. *Transactions of the American Mathematical Society*, 232:279–295, 1977. (↑ 173)

[KST17] Max Kronberg, Muhammad Afzal Soomro, and Jaap Top. Twists of elliptic curves. *SIGMA. Symmetry, Integrability and Geometry: Methods and Applications*, 13(083), 2017. (↑ 101)

[KT03] Kazuya Kato and Fabien Trihan. On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$. *Inventiones mathematicae*, 153(3):537–592, Sep 2003. (↑ 50, 94, 95)

[KT08] Boris È Kunyavskii and Michael A. Tsfasman. Brauer–Siegel theorem for elliptic surfaces. *International Mathematics Research Notices*, 2008, 2008. Erratum available at `https://doi.org/10.1093/imrn/rnp234`. (↑ 85)

[Lan83] Serge Lang. Conjectured Diophantine Estimates on Elliptic Curves. In Michael Artin and John Tate, editors, *Arithmetic and Geometry: Papers Dedicated to I.R. Shafarevich on the Occasion of His Sixtieth Birthday Volume I Arithmetic*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983. (↑ 85)

[Lan91] Serge Lang. *Number theory III: Diophantine geometry*, volume 60. Springer, 1991. (↑ 101)

[Let22] Gauthier Leterrier. On the Mordell–Weil lattice of $y^2 = x^3 + bx + t^{3^n+1}$ in characteristic 3. *Research in Number Theory*, 8(2):23, 2022. (↑ i, iii, 8, 134, 146)

[Lev68] Martin Levin. On the group of rational points on elliptic curves over function fields. *American Journal of Mathematics*, 90(2):456–462, 1968. (↑ 83)

[Liu06] Qing Liu. *Algebraic geometry and arithmetic curves*. Oxford University Press, 2006. (↑ 32)

[LLL82] Arjen K. Lenstra, Hendrik W. Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982. (↑ 20)

[LMF22] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2022. Online. (↑ 229)

[Lor96] D. Lorenzini. *An Invitation to Arithmetic Geometry*. Graduate studies in mathematics. American Mathematical Society, 1996. (↑ 47, 92, 106)

[Mar01] Jacques Martinet. Sur l'indice d'un sous-réseau. *Réseaux euclidiens, designs sphériques et formes modulaires, Monogr. Enseign. Math*, 37:163–211, 2001. (↑ 166)

[Mar02] Jacques Martinet. *Perfect Lattices in Euclidean Spaces*. Grundlehren der mathematischen Wissenschaften. Springer, 2002. (↑ 17, 18, 20, 22, 26, 27, 28, 166)

[MB85] Laurent Moret-Bailly. Pinceaux de variétés abéliennes. *Astérisque*, 129, 1985. (↑ 53)

[McD18] Robert J. S. McDonald. Torsion subgroups of elliptic curves over function fields of genus 0. *Journal of Number Theory*, 193:395–423, 2018. (↑ 83)

[McD19] Robert J. S. McDonald. *Torsion Subgroups of Elliptic Curves over Function Fields*. PhD thesis, University of Connecticut, 2019. (↑ 83)

[MH73] John Milnor and Dale Husemoller. *Symmetric bilinear forms*, volume 73. Springer, 1973. (↑ 29)

[Mik95] Hiroo Miki. On Shioda's problem about Jacobi sums II. *Acta Arithmetica*, 73(4):373–377, 1995. (↑ 224)

[Mil68] James S. Milne. The Tate-Šafarevič group of a constant abelian variety. *Inventiones mathematicae*, 6(1):91–105, 1968. (↑ 50, 95, 97)

[Mil75] James Milne. On a conjecture of Artin and Tate. *Ann. of Math.*, 102(2):517–533, 1975. See also `http://www.jmilne.org/math/articles/1975a.html` for $p \neq 2$. (↑ 50)

[Mil80] James Milne. *Etale cohomology*, volume 33. Princeton, 1980. (↑ 173, 174, 177)

[Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006. 2nd edition available at `https://doi.org/10.1142/11870`. (↑ 40)

[Mil17] James S. Milne. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2017. (↑ 176)

[Möh14] Gerriet Möhlmann. *Zur Berechnung von Mordell-Weil Basen elliptischer Kurven über globalen Funktionenkörpern*. PhD thesis, Universität Oldenburg, 2014. PhD thesis. (↑ 173)

[Mor10] Cristinel Mortici. New sharp inequalities for approximating the factorial function and the digamma function. *Miskolc Mathematical Notes*, 11(1):79–86, 2010. (↑ 27)

[Mor15] Dave Witte Morris. *Introduction to arithmetic groups*, volume 2. Deductive Press, 2015. (↑ 18)

[Mou17] Philippe Moustrou. On the density of cyclotomic lattices constructed from codes. *International Journal of Number Theory*, 13(5):1261–1274, 2017. (↑ 28)

[MS12] Jacques Martinet and Achill Schürmann. Bases of minimal vectors in lattices, III. *International Journal of Number Theory*, 8(02):551–567, 2012. (↑ 166)

[Mum12] David Mumford. *Abelian varieties*. Amer. Mathematical Society, 2012. (↑ 40)

[MZ10] Gary McGuire and Alexey Zaytsev. On the zeta functions of an optimal tower of function fields over $\mathbb{F}_4$. In *Finite fields: theory and applications*, volume 518, pages 327–338. American Mathematical Society, 2010. (↑ 94)

[Neb98] Gabriele Nebe. Some Cyclo-Quaternionic Lattices. *Journal of Algebra*, 199:472–498, 1998. (↑ 30, 164)

[Neb12] Gabriele Nebe. An even unimodular 72-dimensional lattice of minimum 8. *Journal für die reine und angewandte Mathematik*, 2012(673):237–247, 2012. (↑ 144)

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999. (↑ 102, 103)

[Ngu00] Khac-Viet Nguen. On certain Mordell-Weil lattices of hyperelliptic type on rational surfaces. *Journal of Mathematical Sciences*, 102(2):3938–3977, 2000. (↑ 96)

[Occ12] Thomas Occhipinti. A family of elliptic curves of large rank. *Journal of Number Theory*, 132(4):657–665, 2012. (↑ 58)

[Oes90] Joseph Oesterlé. Empilements de sphères. In *Séminaire Bourbaki : volume 1989/90, exposés 715-729*, number 189-190 in Astérisque, pages 375–397. Société mathématique de France, 1990. (↑ 3, 22, 40, 48, 59, 85, 90, 92, 94, 227)

[Oes98] Joseph Oesterlé. Densité maximale des empilements de sphères en dimension 3. *Séminaire Bourbaki*, 41:405–413, 1998. (↑ 26)

[Oes19] Joseph Oesterlé. Densité maximale des empilements de sphères en dimensions 8 et 24. *Séminaire Bourbaki*, 2019. (↑ 26)

[OG93] Takashi Ono and Akihiko Gyoja. A note on Jacobi sums, II. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 69(4):91–93, 1993. (↑ 224)

[OK93] Takashi Ono and Masanari Kida. A note on Jacobi sums. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 69(2):32–34, 1993. (↑ 224)

[Ono93] Takashi Ono. A note on Jacobi sums, III. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 69(7):272–274, 1993. (↑ 224)

[PA11] Janos Pach and P.K. Agarwal. *Combinatorial Geometry*. Wiley Series in Discrete Mathematics and Optimization. Wiley, 2011. (↑ 22, 26, 28)

[Paz22] Fabien Pazuki. The regulator dominates the rank. *arXiv preprint arXiv:2201.02383*, 2022. (↑ 86)

[Pazar] Fabien Pazuki. Heights, ranks and regulators of abelian varieties. *Ramanujan Math. Society, Lecture Notes Series*, 26, to appear. arXiv preprint 1506.05165. (↑ 96)

[PBM05] Janos Pach, Peter Brass, and William Moser. *Research Problems in Discrete Geometry*. Springer-Verlag, New York, 2005. (↑ 31)

[Poo17] Bjorn Poonen. *Rational Points on Varieties*. Graduate Studies in Mathematics. American Mathematical Society, 2017. (↑ 32)

[PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. *Journal of the European Mathematical Society*, 21(9):2859–2903, 2019. arXiv version available at `https://arxiv.org/abs/1602.01431`. (↑ 58, 59, 228)

[PS00] Jérôme Pesenti and Lucien Szpiro. Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques. *Compositio Mathematica*, 120(1):83–117, 2000. (↑ 84)

[PU13] Carl Pomerance and Douglas Ulmer. On balanced subgroups of the multiplicative group. In *Number theory and related fields*, pages 253–270. Springer, 2013. (↑ 56)

[PU16] Rachel Pries and Douglas Ulmer. Arithmetic of abelian varieties in Artin-Schreier extensions. *Transactions of the American Mathematical Society*, 368(12):8553–8595, 2016. (↑ 50, 57, 59, 60)

[Rog56] Claude Ambrose Rogers. The number of lattice points in a set. *Proceedings of the London Mathematical Society*, 3(2):305–320, 1956. (↑ 19, 27)

[Rog64] C. A. Rogers. *Packing and Covering*, volume 54. Cambridge Tracts in Mathematics and Mathematical Physics, 1964. (↑ 22, 27)

[RS98] Eric M. Rains and Neil Sloane. The shadow theory of modular and unimodular lattices. *Journal of Number Theory*, 73(2):359–389, 1998. (↑ 29)

[Sch82] Peter Schneider. Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionenkörpern. *Mathematische Annalen*, 260(4):495–510, Sep 1982. (↑ 50, 94)

[Sch05] Andreas Schweizer. On the p^e-torsion of elliptic curves and elliptic surfaces in characteristic p. *Transactions of the American Mathematical Society*, 357(3):1047–1059, 2005. (↑ 83)

[Ser89] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Springer, 1989. (↑ 40, 92, 95)

[Sha64] Stephen S. Shatz. Cohomology of artinian group schemes over local fields. *Annals of Mathematics*, 79(3):411–449, 1964. (↑ 176, 177, 178)

[Sha72] Stephen S. Shatz. *Profinite groups, arithmetic, and geometry*. Number 67. Princeton University Press, 1972. (↑ 176, 177)

[Shi86] Tetsuji Shioda. An Explicit Algorithm for Computing the Picard Number of Certain Algebraic Surfaces. *American Journal of Mathematics*, 108(2):415–432, 1986. (↑ 3, 5, 51, 52, 56, 58, 59, 60, 113, 128, 205, 206, 215, 225, 226)

[Shi90] Tetsuji Shioda. On the Mordell-Weil Lattices. *Commentarii Mathematici Universitatis Sancti Pauli*, 39, 01 1990. (↑ 3)

[Shi91] Tetsuji Shioda. Mordell-Weil Lattices and Sphere Packings. *American Journal of Mathematics*, 113(5):931–948, 1991. (↑ 3, 4, 5, 6, 10, 30, 56, 81, 88, 91, 107, 144, 145, 146, 149, 153, 164, 170, 193, 195, 196, 201, 203, 210, 227)

[Shi92a] Tetsuji Shioda. Mordell-Weil lattices for higher genus fibration. *Proc. Japan Acad. Ser. A Math. Sci.*, 68(9):247–250, 1992. (↑ 59, 96)

[Shi92b] Tetsuji Shioda. Some remarks on elliptic curves over function fields. In Coray D. F. and Pétermann Y.-F. S, editors, *Journées arithmétiques de Genève - 9-13 septembre 1991*, number 209 in Astérisque, pages 99–114. Société mathématique de France, 1992. (↑ 48)

[Shi99a] Tetsuji Shioda. Mordell–Weil lattices for higher genus fibration over a curve. In *New trends in algebraic geometry*, volume 264, pages 359–374. Cambridge University Press, 1999. (↑ 96)

[Shi99b] Tetsuji Shioda. The splitting field of Mordell-Weil lattices. In *Algebraic Geometry: Hirzebruch 70*, volume 241, pages 297–303. American Mathematical Society, 1999. (↑ 225)

[Shi00] Tetsuji Shioda. A note on K_3 surfaces and sphere packings. *Proc. Japan Acad. Ser. A Math. Sci.*, 76(5):68–72, 05 2000. (↑ 3)

[Shi08] Tetsuji Shioda. K3 surfaces and sphere packings. *J. Math. Soc. Japan*, 60(4):1083–1105, 10 2008. (↑ 3)

[Shi15] Tetsuji Shioda. Mordell-Weil lattice of higher genus fibration on a Fermat surface. *J. Math. Sci. Univ. Tokyo*, 22:443–468, 2015. (↑ 96)

[Sie45] Carl Ludwig Siegel. A mean value theorem in geometry of numbers. *Annals of Mathematics*, pages 340–347, 1945. (↑ 19)

[Sie89] Carl Ludwig Siegel. *Lectures on the Geometry of Numbers*. Springer, 1989. (↑ 23, 28)

[Sil93] A. Silverberg. Galois representations attached to points on shimura varieties. *Séminaire de Théorie Des Nombres: Paris 1990-91*, 108:221, 1993. (↑ 53)

[Sil08a] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2nd edition, 2008. (↑ 33, 34, 35, 37, 38, 39, 40, 41, 42, 44, 47, 83, 84, 89, 92, 100, 116, 150, 170, 172, 226)

[Sil08b] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 2nd edition, 2008. (↑ 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 45, 46, 58, 83, 84, 96, 115, 116, 117, 152, 165)

[Slo98] Neil Sloane. The Sphere Packing Problem. *Documenta Mathematica*, 3(13):387–396, 1998. Proceedings ICM Berlin. (↑ 2)

[Spr13] Johannes Sprang. Minimal number of points with bad reduction for elliptic curves over $\mathbb{P}^1$. *The Rocky Mountain Journal of Mathematics*, 43(6):2017–2032, 2013. (↑ 43)

[SS10] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. In *Algebraic Geometry in East Asia, Seoul 2008*, pages 51–160, Tokyo, Japan, 2010. Mathematical Society of Japan. (↑ 36, 83)

[SS19] Matthias Schütt and Tetsuji Shioda. *Mordell–Weil Lattices*. Springer, 1st edition, 2019. (↑ 3, 15, 36, 37, 42, 43, 44, 45, 46, 51, 54, 56, 58, 83, 96, 151, 154, 155, 205, 221)

[Sta23] The Stacks Project Authors. *Stacks Project*. `http://stacks.math.columbia.edu`, 2023. (↑ 175)

[Tat66a] John Tate. Endomorphisms of Abelian Varieties over Finite Fields. *Inventiones mathematicae*, 2:134–144, 1966. (↑ 53, 92, 99)

[Tat66b] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki : années 1964/65 1965/66, exposés 277-312*, number 9 in Séminaire Bourbaki, pages 415–440. Société mathématique de France, 1966. (↑ 50)

[The21] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.3)*, 2021. `https://www.sagemath.org`. (↑ 9, 70, 156, 162, 164, 168, 169, 176, 180, 189, 223)

[TS67] J. T. Tate and I. R. Shafarevich. The rank of elliptic curves. *Dokl. Akad. Nauk SSSR*, 175(4):770–773, 1967. English translation available in *Collected Works of John Tate: Part I (1951–1975)*. (↑ 5, 7, 11, 54, 56, 65, 81, 104)

[Tsf91] Michael A. Tsfasman. Global fields, codes and sphere packings. In Lachaud Gilles, editor, *Journées arithmétiques de Luminy 17-21 Juillet 1989*, number 198-199-200 in Astérisque, pages 373–396. Société mathématique de France, 1991. (↑ 2, 3, 30, 227)

[Tó17] G. Fejes Tóth. Packing and covering. In Csaba D. Tóth, Joseph O'Rourke, and Jacob E. Goodman, editors, *Handbook of discrete and computational geometry*, chapter 2, pages 27–66. CRC press, 2017. (↑ 22)

[Ulm91] Douglas L Ulmer. p-descent in characteristic p. *Duke mathematical journal*, 62(2):237–265, 1991. (↑ 173)

[Ulm02] Douglas Ulmer. Elliptic Curves with Large Rank over Function Fields. *Annals of Mathematics*, 155(1):295–315, 2002. (↑ 5, 36, 54, 65, 90, 128)

[Ulm07a] Douglas Ulmer. Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields. *Mathematical Research Letters*, 14(3):453–467, 2007. Erratum available at `https://www.math.arizona.edu/~ulmer/research/papers/2007c-correction.pdf`. (↑ 5, 60, 72, 205)

[Ulm07b] Douglas Ulmer. L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields. *Inventiones mathematicae*, 167(2):379–408, Feb 2007. (↑ 52, 56, 57, 58, 59, 86, 91, 96, 97, 102)

[Ulm11] Douglas Ulmer. Park City lectures on elliptic curves over function fields. In *Arithmetic of L-functions*, pages 213–280. IAS/Park City Mathematics Series, 2011. arXiv version available at https://arxiv.org/abs/1101.1939. (↑ 36, 48, 50, 51, 52, 56, 57, 58, 83, 92, 148)

[Ulm13] Douglas Ulmer. On Mordell–Weil groups of Jacobians over function fields. *Journal of the Institute of Mathematics of Jussieu*, 12(1):1–29, 2013. (↑ 57, 59)

[Ulm14a] Douglas Ulmer. Curves and Jacobians over function fields. In G. Boeckle et al., editor, *Arithmetic geometry over global function fields*, pages 281–337. Springer, 2014. arXiv version available at https://arxiv.org/abs/1203.5573v2. (↑ 36, 37)

[Ulm14b] Douglas Ulmer. Explicit points on the Legendre curve III. *Algebra Number Theory*, 8(10):2471–2522, 2014. (↑ 56)

[Ulm14c] Douglas Ulmer. Explicit points on the Legendre curve. *Journal of Number Theory*, 136:165 – 194, 2014. (↑ 56)

[Ulm19] Douglas Ulmer. On the Brauer–Siegel ratio for abelian varieties over function fields. *Algebra Number Theory*, 13(5):1069–1120, 2019. (↑ 53, 54, 97)

[Usu00] Hisashi Usui. On the Mordell-Weil Lattice of the Elliptic Curve $y^2 = x^3 + t^m + 1$ (I). *Commentarii mathematici Universitatis Sancti Pauli*, 49:71–78, jun 2000. (↑ 206)

[Usu01] Hisashi Usui. On the Mordell-Weil Lattice of the Elliptic Curve $y^2 = x^3 + t^m + 1$ (II). *Commentarii mathematici Universitatis Sancti Pauli*, 50(1):65–87, 2001. (↑ 205, 225)

[Usu06] Hisashi Usui. On the Mordell-Weil Lattice of the Elliptic Curve $y^2 = x^3 + t^m + 1$ (III). *Commentarii mathematici Universitatis Sancti Pauli*, 55(2):173–194, 2006. (↑ 206)

[Usu08] Hisashi Usui. On the Mordell-Weil Lattice of the Elliptic Curve $y^2 = x^3 + t^m + 1$ (IV). *Commentarii mathematici Universitatis Sancti Pauli*, 57(1):23–63, 2008. (↑ 206)

[UZ10] Douglas Ulmer and Yuri G. Zarhin. Ranks of Jacobians in towers of function fields. *Mathematical Research Letters*, 17(4):637–645, 2010. (↑ 59)

[Van11] Stephanie Vance. Improved sphere packing lower bounds from Hurwitz lattices. *Advances in Mathematics*, 227(5):2144 – 2156, 2011. (↑ 2, 28)

[Ven13] Akshay Venkatesh. A Note on Sphere Packings in High Dimension. *International Mathematics Research Notices*, 2013(7):1628–1642, 2013. (↑ 2, 28, 31)

[Via17] Maryna S. Viazovska. The sphere packing problem in dimension 8. *Annals of Mathematics*, 185(3):991–1015, 2017. (↑ 2, 26, 31)

[Vlă19] Serge Vlăduţ. Lattices with exponentially large kissing numbers. *Moscow Journal of Combinatorics and Number Theory*, 8(2):163–177, 2019. (↑ 31, 228)

[Vol90] José F. Voloch. Explicit p-descent for elliptic curves in characteristic p. *Compositio Mathematica*, 74(3):247–258, 1990. (↑ 173)

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, 2nd edition, 1997. (↑ 66, 67)

[Was08] Lawrence C. Washington. *Elliptic curves, Number Theory and Cryptography*. Chapman & Hall, 2nd edition, 2008. (↑ 47)

[Waw21] Wojciech Wawrów. On torsion of superelliptic Jacobians. *Journal de Théorie des Nombres de Bordeaux*, 33(1):223–235, 2021. (↑ 104)

[Yok64] Akio Yokoyama. On the Gaussian sum and the Jacobi sum with its application. *Tohoku Mathematical Journal, Second Series*, 16(2):142–153, 1964. (↑ 224)

Gauthier Leterrier

Curriculum Vitae

Nationality: French
gauthier.leterrier [at] gmail.com

Education

2019–(2023) PhD student in Mathematics, *École polytechnique fédérale de Lausanne (EPFL)*, Switzerland
Supervisor : Prof. Maryna Viazovska.

2016–2018 M.Sc. in Mathematics, *École polytechnique fédérale de Lausanne (EPFL)*, Switzerland

2013–2016 B.Sc. in Mathematics, *École polytechnique fédérale de Lausanne (EPFL)*, Switzerland

2010–2013 Gymnase de Beaulieu, *Lausanne*

Publications

2022 *On the Mordell–Weil lattice of $y^2 = x^3 + bx + t^{3^n+1}$ in characteristic 3*
Published in *Research in Number Theory*, vol. 8 (2), 2022, `https://doi.org/10.1007/s40993-022-00321-0`.

2021 *Empilons des sphères dans toutes les dimensions*
Popularization article in the French magazine "La Recherche", n. 566 (July-September 2021)

Reviews

Reviews of papers MR4399126, MR4468717, MR4496969 and MR4472439 for MathSciNet.

Teaching experience

2022 Dean's award for Excellence in Teaching, EPFL

Fall 2022 Supervised the semester project of a Master student, *Topic : isogeny-based cryptography*

Fall 2021 Main assistant for "Mathématiques I"

Fall 2020 Assistant for Structures algébriques

Spring 2020, 2021, 2022, 2023 Main assistant for "Number theory in cryptography", *Master course given by Dr. Vlad Serban (2020, 2021) and Dr. Dimitar Jetchev (2022, 2023)*

Fall 2019 Assistant for Analyse I

Talks

16/11/2021 Réseaux de Mordell–Weil en caractéristique 3 et empilements de sphères, invited to the seminar of Number Theory in Clermont–Ferrand (in person)

14/03/2023 Elliptic curves over function fields and sphere packings, Université de Neuchâtel, Swiss Doctoral Day 2023

Conferences and workshops attended

30.05 - 02.06.2023 Summer school *Quadratic forms and applications in algebraic geometry*, Aachen

30.10 - 01.11.2022 Swiss Number Theory Days, EPFL, Lausanne

11-14 July 2022 ICM sectional workshop in Number Theory and Algebraic Geometry, ETH Zürich

24-28 May 2021 Curves over Finite Fields : Past, Present and Future, Online

24-28.08.2020 Online summer school on Optimization, Interpolation and Modular Forms, (EPFL)

25-26.10.2019 Swiss Number Theory Days, ETH Zürich