An efficient deterministic test for Kloosterman sum zeros

Omran Ahmadi and Robert Granger

Claude Shannon Institute
UCD and DCU
Ireland

UCD Algebra and Communications Seminar, 17th October 2011

Disclaimer

Disclaimer

- I am not an expert on Kloosterman sums

Disclaimer

- I am not an expert on Kloosterman sums
- This talk is actually about elliptic curves

Outline

Kloosterman sums

Let p be prime, let $n \geq 1$ and let $\mathrm{Tr} : \mathbb{F}_{p^n} \to \mathbb{F}_p$, where

$$\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}.$$

For $\zeta = e^{2\pi i/p}$, the Kloosterman sum $\mathcal{K}_{p^n} : \mathbb{F}_{p^n} \to \mathbb{R}$ can be defined by

$$\mathcal{K}_{p^n}(a) = 1 + \sum_{x \in \mathbb{F}_{p^n}^{\times}} \zeta^{\mathrm{Tr}(x^{-1} + ax)}.$$

- Defined by Kloosterman (1926) to study representability of integers by the form $ax^2 + by^2 + cz^2 + dt^2$
- Applications in coding theory and cryptography

Kloosterman zeros

Definition

A Kloosterman zero is simply an element $a \in \mathbb{F}_{p^n}^{\times}$ for which

$$\mathcal{K}_{p^n}(a) = 0.$$

- $p \in \{2, 3\} \implies \mathcal{K}_{p^n}(a) \in \mathbb{Z}$ for all a
- Zeros exist only for $p \in \{2, 3\}$ (Kononen/Rinta-aho/Väänänen '10)
- Kloosterman zeros give rise to binary/ternary bent functions for $p = 2, 3$ respectively (Dillon '74 and Helleseth/Kholosha '06)
- Finding zeros is believed to be hard

Divisibilty/Congruence results

Since finding zeros is believed to be hard, research has focused on finding conditions on $a \in \mathbb{F}_{p^n}^{\times}$ that characterise $\mathcal{K}_{p^n}(a)$ modulo small integers.

- (Helleseth/Zinoviev '99):

$$\mathcal{K}_{2^n}(a) \equiv 4\mathrm{Tr}(a) \pmod 8$$

- (Lisoněk '08): $16 \mid \mathcal{K}_{2^n}(a) \iff$

$$\mathrm{Tr}(a) = 0 \text{ and } \mathrm{Tr}(y) = 0 \text{ where } y^2 + ay + a^3 = 0$$

- (van der Geer/Vlugt '91, Göloğlu/McGuire/Moloney '10):

$$\mathcal{K}_{3^n}(a) \equiv 3\mathrm{Tr}(a) \pmod 9$$

Divisibilty/Congruence results

- (Göloğlu/McGuire/Moloney '10): For $n \geq 3$

$$\begin{aligned}\mathcal{K}_{3^n}(a) &\equiv 21\left(\mathrm{Tr}(a)\right)^3 + 18\left(\sum_{wt_3(j)=2} a^j\right) \\ &+ 18\left(\sum_{j=2\cdot 3^r+3^s} a^j\right) + 9\left(\sum_{j=3^r+3^s+3^t} a^j\right) \pmod{27}\end{aligned}$$

- Others for $\mathcal{K}_{2^n}(a)$ mod 3 (Moisio '09), $\mathcal{K}_{2^n}(a)$ mod 64 (Göloğlu/McGuire/Moloney '10), and $\mathcal{K}_{3^n}(a)$ mod 4 (Göloğlu '11)
- Using the above one can sieve over a to reduce search space for zeros, but one still needs to evaluate $\mathcal{K}_{p^n}(a)$

Kloosterman sum/EC connection

Theorem (Lachaud/Wolfmann '87, Katz/Livné '89)

Let $a \in \mathbb{F}_{2^n}^{\times}$ and define the elliptic curve $E_{2^n}(a)$ over $\mathbb{F}_{2^n}$ by

$$E_{2^n}(a) : y^2 + xy = x^3 + a.$$

Then $\#E_{2^n}(a) = 2^n + \mathcal{K}_{2^n}(a)$.

Theorem (Katz/Livné '89, van der Geer/Vlugt '91, Moisio '07)

Let $a \in \mathbb{F}_{3^n}^{\times}$ and define the elliptic curve $E_{3^n}(a)$ over $\mathbb{F}_{3^n}$ by

$$E_{3^n}(a) : y^2 = x^3 + x^2 - a.$$

Then $\#E_{3^n}(a) = 3^n + \mathcal{K}_{3^n}(a)$.

Corollaries/results

Let $p \in \{2,3\}$, let $a \in \mathbb{F}_{p^n}^{\times}$ and let W_{p^n} be the Weil interval

$$[p^n + 1 - 2p^{n/2}, p^n + 1 + 2p^{n/2}].$$

- $\#E_{p^n}(a) \in W_{p^n}$ and so we have

$$|\mathcal{K}_{p^n}(a) - 1| \leq 2p^{n/2}$$

- $4 \mid \mathcal{K}_{2^n}(a)$ and $\{2^n + \mathcal{K}_{2^n}(a) | a \in \mathbb{F}_{2^n}^{\times}\} = W_{2^n} \cap 4\mathbb{Z}$
- $3 \mid \mathcal{K}_{3^n}(a)$ and $\{3^n + \mathcal{K}_{3^n}(a) | a \in \mathbb{F}_{3^n}^{\times}\} = W_{3^n} \cap 3\mathbb{Z}$

Kloosterman sums via point counting

- p-adic point counting (due to Satoh, with improvements by Fouquet/Gaudry/Harley, Skjernaa, Vercauteren and Harley) can compute $\mathcal{K}_{p^n}(a)$ in $O(n^{2+\epsilon} \log n)$ time and $O(n^2)$ space, for fixed p.
- In practice, can evaluate a Kloosterman sum over $\mathbb{F}_{2^{64}}$ in $0.02s$ and over $\mathbb{F}_{2^{1000}}$ in less than 7 seconds on cplex (MAGMA V2.16)
- Hence to find a zero one can select random $a \in \mathbb{F}_{p^n}^{\times}$ and test whether $\#E_{p^n}(a) \stackrel{?}{=} p^n$.

Lisoněk's observation

Theorem (Lisoněk '08)

Let $p \in \{2, 3\}$, let $a \in \mathbb{F}_{p^n}^\times$, and let $0 \leq k \leq n$. Then $p^k \mid \mathcal{K}_{p^n}(a)$ if and only if there exists a point of order p^k on $E_{p^n}(a)$.

Proof: By previous theorems, $p^k \mid \mathcal{K}_{p^n}(a) \iff p^k \mid \#E_{p^n}(a)$. We also have $E_{p^n}(a) \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$ where $d_1 \mid d_2$ and $d_1 \mid p^n - 1$. Suppose $p^k \mid \#E_{p^n}(a)$. Since $p \nmid d_1$, we have $p^k \mid d_2$ and by Sylow's (second) Theorem, $\exists G \leq E_{p^n}(a)$ with $G \cong \mathbb{Z}_{p^k}$ and a generator of G is a point of order p^k in $E_{p^n}(a)$. Conversely, if $E_{p^n}(a)$ contains a point of order p^k, by Lagrange's Theorem $p^k \mid \#E_{p^n}(a)$ and hence $p^k \mid \mathcal{K}_{p^n}(a)$.

Lisoněk's algorithm

ALGORITHM 1: **TEST IF** $\mathcal{K}_{p^n}(a) = 0$

INPUT: $a \in \mathbb{F}_{p^n}^{\times}$
OUTPUT: NO if $\mathcal{K}_{p^n}(a) \neq 0$, or (YES, P), $\langle P \rangle = E_{p^n}(a)$

1. $P \xleftarrow{r} E_{p^n}(a)$;
2. while $[p^n]P = \mathcal{O}$ do:
3. if $[p]P \neq \mathcal{O}, \ldots, [p^{n-1}]P \neq \mathcal{O}$ then
4. return (YES, P);
5. else $P \xleftarrow{r} E_{p^n}(a)$;
6. return NO;

A critique of Lisoněk's algorithm

- Assumes $\#E_{p^n}(a) = p^n$ and tries to find a point of this order to prove this
- Equivalent to assuming the Sylow p-subgroup $S_p(E_{p^n}(a))$ has order p^n and finds a generator randomly
- Requires computing $[p^n]P$, so at least n point doublings/triplings

A critique of Lisoněk's algorithm

- Assumes $\#E_{p^n}(a) = p^n$ and tries to find a point of this order to prove this
- Equivalent to assuming the Sylow p-subgroup $S_p(E_{p^n}(a))$ has order p^n and finds a generator randomly
- Requires computing $[p^n]P$, so at least n point doublings/triplings

Question: Is there a better way to do this?

Determining the Sylow p-subgroup of $E_{p^n}(a)$

$E_{2^n}(a)$ contains the unique order 2 point $P_2 = (0, a^{1/2})$, while $E_{3^n}(a)$ contains the order 3 points $P_3^{\pm} = (a^{1/3}, \pm a^{1/3})$, so in both cases the p-torsion $E_{p^n}(a)[p]$ is non-trivial.

- For $x \in \mathbb{Z}_{\geq 1}$, let $\mathrm{ord}_p(x) = \max\{k \text{ s.t. } p^k \mid x\}$.
- For $a \in \mathbb{F}_{p^n}^{\times}$, let $k = \mathrm{ord}_p(\#E_{p^n}(a))$, so that the Sylow p-subgroup $S_p(E_{p^n}(a))$ has order p^k
- By Lisoněk's theorem, $S_p(E_{p^n}(a))$ is cyclic of order p^k
- Hence there are $\phi(p^k) = (p-1)p^{k-1}$ generators of $S_p(E_{p^n}(a)) = E_{p^n}(a)[p^k]$

Determining the Sylow p-subgroup of $E_{p^n}(a)$

- Multiplying these generators by p results in $(p-1)p^{k-2}$ generators of $E_{p^n}(a)[p^{k-1}]$
- Continuing this multiplication by p process, after $k-1$ steps one arrives at the p-torsion subgroup, consisting of $p-1$ order p points and $\mathcal{O}$
- Structure of $S_p(E_{p^n}(a))$ may be viewed as a tree with $\mathcal{O}$ as the root, with children the $p-1$ non-trivial elements of $E_{p^n}(a)[p]$
- If $k>1$ then each of $E_{p^n}(a)[p]\setminus\mathcal{O}$ has p children, which are the elements of $E_{p^n}(a)[p^2]\setminus E_{p^n}(a)[p]$
- For $1<i<k$ at the i-th level, each of the $(p-1)p^{i-1}$ nodes have p children.

Determining the Sylow p-subgroup of $E_{p^n}(a)$

Basic insight: above process can be reversed efficiently, using point-halving for binary fields and point-thirding for ternary fields.

- Cyclic structure of $S_p(E_{p^n}(a))$ means that at each level either all nodes are divisible by p, or none are $\Longrightarrow$ can compute height of tree with a depth-first search, without backtracking
- When a point on a given level P can not be halved or thirded, this level is $\log_p |S_p(E_{p^n}(a))|$ and P is a generator of $S_p(E_{p^n}(a))$
- In particular, can compute $|S_p(E_{p^n}(a))|$ without first computing $\#E_{p^n}(a)$

Computing the Sylow p-subgroup

ALGORITHM 2: DETERMINE $S_p(E_{p^n}(a))$

INPUT: $a \in \mathbb{F}_{p^n}^{\times}$, $P \in E_{p^n}(a)[p] \setminus \{\mathcal{O}\}$

OUTPUT: (k, P_k) with $k = \mathrm{ord}_p(\#E_{p^n}(a))$, $\langle P_k \rangle = S_p(E_{p^n}(a))$

1. counter $\leftarrow 1$;
2. while P is p-divisible do:
3. P := P/p;
4. counter++;
5. return (counter, P)

Computing $S_2(E_{2^n}(a))$

Given a point $P = (x, y) \in E_{2^n}(a)$, $2P = (\xi, \eta)$ is given by the formula:

$$\begin{aligned} \lambda &= x + y/x, \\ \xi &= \lambda^2 + \lambda, \\ \eta &= x^2 + \xi(\lambda + 1). \end{aligned}$$

- Point-halving means given $Q = (\xi, \eta)$, find $P = (x, y)$ such that $[2]P = Q$
- First, if possible we solve $\lambda^2 + \lambda = \xi$. This is solvable in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}(\xi) = 0$

Computing $S_2(E_{2^n}(a))$

For odd n a solution to $\lambda^2 + \lambda = \xi$ is given by the *half trace* function

$$H : c \mapsto \sum_{i=0}^{(n-1)/2} c^{2^{2i}}.$$

- One can check that $\lambda = H(\xi)$ is a solution (as is $\lambda + 1$).
- For even n, the half trace will not work. Instead, choose $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}(\delta) = 1$. Then a solution is given by

$$\lambda = \sum_{i=0}^{n-2} \left(\sum_{j=i+1}^{n-1} \delta^{2^j} \right) \xi^{2^i}$$

- Evaluation can be sped up and depends on $\mathrm{ord}_2(n)$

Computing $S_2(E_{2^n}(a))$

ALGORITHM 3: **DETERMINE** $S_2(E_{2^n}(a))$

INPUT: $a \in \mathbb{F}_{2^n}^{\times}$, $x = a^{1/4}, y = a^{1/2}$

OUTPUT: (k, P_k) with $k = \mathrm{ord}_2(\#E_{2^n}(a))$, $\langle P_k \rangle = S_2(E_{2^n}(a))$

1. counter $\leftarrow 2$;
2. while $\mathrm{Tr}(x) = 0$ do:
3. $\quad\lambda \leftarrow H(x)$;
4. $\quad x \leftarrow (y + x(\lambda + 1))^{1/2}$;
5. $\quad y \leftarrow x(x + \lambda)$;
6. $\quad$counter++;
7. return (counter, $P = (x, y)$)

Computing $S_3(E_{3^n}(a))$

Let $Q = (\xi, \eta) \in E_{3^n}(a)$. To find $P = (x, y)$ such that $[3]P = Q$, when possible, we do the following (à la Miret *et al.* '09):

$$x([3]P) = x(P) - \frac{\Psi_2(x,y)\Psi_4(x,y)}{\Psi_3^2(x,y)},$$

$$(x - \xi)\Psi_3^2(x,y) - \Psi_2(x,y)\Psi_4(x,y) = 0.$$

Working modulo the equation of E_{3^n}, this becomes

$$x^9 - \xi x^6 + a(1-\xi)x^3 - a^2(a+\xi) = 0,$$

whereupon substituting $X = x^3$ gives

$$f(X) = X^3 - \xi X^2 + a(1-\xi)X - a^2(a+\xi) = 0.$$

Computing $S_3(E_{3^n}(a))$

We make the transformation

$$g(X) = X^3 f\left(\frac{1}{X} - \frac{a(1-\xi)}{\xi}\right) = \frac{a^2\eta^2}{\xi^3}X^3 - \xi X + 1.$$

Hence we must solve

$$X^3 - \frac{\xi^4}{a^2\eta^2}X + \frac{\xi^3}{a^2\eta^2} = 0.$$

Writing $X = \frac{\xi^2}{a\eta}\bar{X}$ this becomes

$$\bar{X}^3 - \bar{X} + \frac{a\eta}{\xi^3} = 0.$$

Computing $S_3(E_{3^n}(a))$

- Thirding condition is simply $\mathrm{Tr}(a\eta/\xi^3) = 0$, since for every element of $\mathbb{F}_{3^n}$ we have $\mathrm{Tr}(\bar{X}^3 - \bar{X}) = 0$.
- Using a function similar to the half trace: for $n \equiv 2 \pmod 3$ we define

$$H_3 : c \mapsto c + \sum_{i=1}^{(n-2)/3} c^{3^{3i}} - c^{3^{3i-1}}.$$

- Other two solutions are $H_3(c) \pm 1$. For $n \equiv 1 \pmod 3$ one can define a similar function, whereas for $n \equiv 0 \pmod 3$ one can use an analogue of the binary solution.

Computing $S_3(E_{3^n}(a))$

ALGORITHM 4: **DETERMINE** $S_3(E_{3^n}(a))$

INPUT: $a \in \mathbb{F}_{3^n}^{\times}$, $x = a^{1/3}, y = a^{1/3}$

OUTPUT: (k, P_k) with $k = \mathrm{ord}_3(\#E_{3^n}(a))$, $\langle P_k \rangle = S_3(E_{3^n}(a))$

1. counter $\leftarrow 1$;
2. while $\mathrm{Tr}(ay/x^3) = 0$ do:
3. $\quad \lambda \leftarrow H_3(-ay/x^3)$;
4. $\quad x \leftarrow \left(\frac{ay}{x^2\lambda} - \frac{a(1-x)}{x} \right)^{1/3}$;
5. $\quad y \leftarrow (x^3 + x^2 - a)^{1/2}$;
6. $\quad$ counter++;
7. return (counter, $P = (x, y)$)

Heuristic number of iterations

We make the following:

Heuristic Assumption

Over all $a \in \mathbb{F}_{p^n}^{\times}$, at the start of any iteration, regardless of the height of the tree at that point, the argument of the trace function is uniformly distributed in $\mathbb{F}_{p^n}$.

Heuristic number of iterations for $E_{2^n}(a)$

- Each curve $E_{2^n}(a)$ has initial point of order 4
- On 1st iteration, $2^{n-1} - 1$ of the curves $E_{2^n}(a)$ have $\mathrm{Tr}(a) = 0$
- On 2nd iteration, by our assumption, approximately 2^{n-2} curves have order 8 points with trace-0 x-coordinate.
- Summing over all iterations this gives a total of

$$2^{n-1} + 2^{n-2} + \cdots + 2 + 1 \approx 2^n,$$

for the number of iterations that need to be performed for all $a \in \mathbb{F}_{2^n}^{\times}$.
- $\implies$ geometric mean of $|S_2(E_{2^n}(a))|$ as $n \to \infty$ is $2^{2+1} = 8$.

Heuristic number of iterations for $E_{3^n}(a)$

- Each curve $E_{3^n}(a)$ has initial point of order 3
- On 1st iteration, $3^{n-1} - 1$ of the curves $E_{3^n}(a)$ have $\mathrm{Tr}(a \cdot a^{1/3}/a) = 0$
- On 2nd iteration, by our assumption, approximately 3^{n-2} curves have order 9 points with trace-0 argument
- Summing over all iterations this gives a total of

$$3^{n-1} + 3^{n-2} + \cdots + 3 + 1 \approx 3^n/2,$$

  for the number of iterations that need to be performed for all $a \in \mathbb{F}_{3^n}^{\times}$.
- $\implies$ geometric mean of $|S_3(E_{3^n}(a))|$ as $n \to \infty$ is $3\sqrt{3}$.

Distribution data for E_{2^n}

$\#\{E_{2^n}(a)\}_{a\in\mathbb{F}_{2^n}^\times}$ whose group order is divisible by 2^i:

$n\backslash i$	1	2	3	4	5	6	7	8	≥ 9
1	1	1							
2	3	3							
3	7	7	3						
4	15	15	7	5					
5	31	31	15	5	5				
6	63	63	31	15	12	12			
7	127	127	63	35	14	14	14		
8	255	255	127	55	21	16	16	16	
9	511	511	255	135	63	18	18	18	18
10	1023	1023	511	255	125	65	60	60	60
11	2047	2047	1023	495	253	132	55	55	55
12	4095	4095	2047	1055	495	252	84	72	72

Distribution data for E_{3^n}

$\#\{E_{3^n}(a)\}_{a \in \mathbb{F}_{3^n}^{\times}}$ whose group order is divisible by 3^i:

$n \backslash i$	1	2	3	4	5	6	7	8	≥ 9
1	2								
2	8	2							
3	26	8	3						
4	80	26	4	4					
5	242	80	35	15	15				
6	728	242	83	24	24	24			
7	2186	728	266	77	21	21	21		
8	6560	2186	692	252	48	48	48	48	
9	19682	6560	2168	741	270	108	108	108	108
10	59048	19682	6605	2065	575	100	100	100	100
11	177146	59048	19547	6369	2596	924	264	264	264
12	531440	177146	58751	19864	6616	2352	600	600	600

Exact number of iterations using Katz/Livné '89

- Let $p^n + t$ be an integer in W_{p^n}
- Let $N(t)$ be the number of solutions in $\mathbb{F}_{p^n}^{\times}$ to $\mathcal{K}_{p^n}(a) = t$
- (Katz/Livné '89): let $\alpha = (t + \sqrt{t^2 - 4p^n})/2$ for t as above:

$$N(t) = \sum_{\mathbb{Z}[\alpha] \subset \mathcal{O} \subset \mathbb{Q}(\alpha)} h(\mathcal{O})$$

- Total of all exponents of the Sylow p-subgroups is therefore

$$T_{p^n} = \sum_{(p^n+t) \in W_{p^n}} N(t) \cdot \mathrm{ord}_p(p^n + t)$$

- Expected order of $S_p(E_{p^n}(a))$ is thus $p^{T_{p^n}/(p^n-1)}$

Decomposing T_{p^n}

For $1 \leq k \leq n$, we partition T_{p^n} into the counting functions

$$T_{p^n}(k) = \sum_{(p^n+t)\in W_{p^n}, p^k|(p^n+t)} N(t),$$

so that

$$T_{p^n} = \sum_{k=1}^{n} T_{p^n}(k).$$

- $T_{2^n}(1) = T_{2^n}(2) = 2^n - 1$ and $T_{2^n}(3) = 2^{n-1} - 1$
- $T_{3^n}(1) = 3^n - 1$ and $T_{3^n}(2) = 3^{n-1} - 1$

Estimating $T_{p^n}(k)$

- Note that $j(E_{2^n}(a)) = j(E_{3^n}(a)) = 1/a$
- Hence all the $\overline{\mathbb{F}}_{2^n}$- and $\overline{\mathbb{F}}_{3^n}$-isomorphism classes of elliptic curves respectively, except for $j = 0$.
- Hints at the use of modular curves, which parameterise $\mathbb{F}_{p^n}$-isomorphism classes of elliptic curves with a divisibility property:

Estimating $T_{p^n}(k)$

- Note that $j(E_{2^n}(a)) = j(E_{3^n}(a)) = 1/a$
- Hence all the $\overline{\mathbb{F}}_{2^n}$- and $\overline{\mathbb{F}}_{3^n}$-isomorphism classes of elliptic curves respectively, except for $j = 0$.
- Hints at the use of modular curves, which parameterise $\mathbb{F}_{p^n}$-isomorphism classes of elliptic curves with a divisibility property:

Definition

For $k \geq 2$, let $\mathcal{T}_{2^n}(k)$ be the set of $\mathbb{F}_{2^n}$-isomorphism classes of elliptic curves $E/\mathbb{F}_{2^n}$ such that $\#E(\mathbb{F}_{2^n}) \equiv 0 \pmod{2^k}$.

Estimating $T_{p^n}(k)$

- Note that $j(E_{2^n}(a)) = j(E_{3^n}(a)) = 1/a$
- Hence all the $\overline{\mathbb{F}}_{2^n}$- and $\overline{\mathbb{F}}_{3^n}$-isomorphism classes of elliptic curves respectively, except for $j = 0$.
- Hints at the use of modular curves, which parameterise $\mathbb{F}_{p^n}$-isomorphism classes of elliptic curves with a divisibility property:

Definition

For $k \geq 2$, let $\mathcal{T}_{2^n}(k)$ be the set of $\mathbb{F}_{2^n}$-isomorphism classes of elliptic curves $E/\mathbb{F}_{2^n}$ such that $\#E(\mathbb{F}_{2^n}) \equiv 0 \pmod{2^k}$.

Definition

For $k \geq 1$, let $\mathcal{T}_{3^n}(k)$ be the set of $\mathbb{F}_{3^n}$-isomorphism classes of elliptic curves $E/\mathbb{F}_{3^n}$ such that $\#E(\mathbb{F}_{3^n}) \equiv 0 \pmod{3^k}$.

Estimating $T_{p^n}(k)$

Lemma

For $2 \leq k \leq n$, we have

$$|\mathcal{T}_{2^n}(k)| = T_{2^n}(k).$$

Similarly, for $1 \leq k \leq n$, we have

$$|\mathcal{T}_{3^n}(k)| = T_{3^n}(k).$$

- Considering the number of $\mathbb{F}_{p^n}$-rational points on the Igusa curve of level p^k allows one to prove our main theorem
- For simplicity (and generality) we use a result due to Howe on the group orders of elliptic curves over finite fields

Estimating $T_{p^n}(k)$

- Consider the set of equivalence classes of $\mathbb{F}_q$-isomorphic curves whose group orders are divisible by N:

$$V(\mathbb{F}_q; N) = \{E/\mathbb{F}_q : N \mid \#E(\mathbb{F}_q)\}/ \cong_{\mathbb{F}_q}$$

- For a set S of $\mathbb{F}_q$-isomorphism classes of elliptic curves over $\mathbb{F}_q$, the *weighted cardinality* is defined to be:

$$\#'S = \sum_{[E] \in S} \frac{1}{\#\mathrm{Aut}_{\mathbb{F}_q}(E)}.$$

- $\#\mathrm{Aut}_{\mathbb{F}_q}(E) = 2$ and so for $p = 2, k \geq 2$ and $p = 3, k \geq 1$:

$$|\mathcal{T}_{p^n}(k)| = 2 \cdot \#' V(\mathbb{F}_{p^n}; p^k).$$

Estimating $T_{p^n}(k)$

Theorem (Howe '93)

There is a constant $C \leq 1.262$ such that given a prime power q, let r be the multiplicative arithmetic function such that for all primes l and positive integers a

$$r(l^a) = \begin{cases} \dfrac{1}{l^{a-1}(l-1)}, & \text{if } q \not\equiv 1 \pmod{l^c}; \\[2ex] \dfrac{l^{b+1}+l^b-1}{l^{a+b-1}(l^2-1)}, & \text{if } q \equiv 1 \pmod{l^c}, \end{cases}$$

where $b = \lfloor a/2 \rfloor$ and $c = \lceil a/2 \rceil$. Then for all positive integers N one has

$$\left| \frac{\#' V(\mathbb{F}_q; N)}{q} - r(N) \right| \leq \frac{CN\rho(N)2^{\nu(N)}}{\sqrt{q}},$$

where $\rho(N) = \prod_{p|N}((p+1)/(p-1))$ and $\nu(N)$ denotes the number of prime divisors of N.

Main theorem

Theorem

(i) *For* $3 \leq k < n/4$ *we have* $T_{2^n}(k) = 2^{n-k+2} + O(2^{k+n/2})$,

(ii) *For* $2 \leq k < n/4$ *we have* $T_{3^n}(k) = 3^{n-k+1} + O(3^{k+n/2})$,

(iii) $T_{2^n} = 3 \cdot 2^n + O(n \cdot 2^{3n/4})$,

(iv) $T_{3^n} = 3^{n+1}/2 + O(n \cdot 3^{3n/4})$,

(v) $\lim_{n\to\infty} T_{p^n}/(p^n - 1) = \begin{cases} 3 & \text{if } p = 2, \\ 3/2 & \text{if } p = 3. \end{cases}$

Furthermore, in $(i) - (iv)$ *the implied constants in the* O*-notation are absolute and effectively computable.*

Proof of main theorem

Using Howe's theorem and our lemma, for $3 \leq k \leq n$ we have

$$\left| \frac{T_{2^n}(k)}{2^{n+1}} - \frac{1}{2^{k-1}} \right| \leq \frac{C \cdot 2^k \cdot 3 \cdot 2}{2^{n/2}},$$

from which part (i) follows immediately. Similarly for $2 \leq k \leq n$ we have

$$\left| \frac{T_{3^n}(k)}{2 \cdot 3^n} - \frac{1}{3^{k-1} \cdot 2} \right| \leq \frac{C \cdot 3^k \cdot (4/2) \cdot 2}{3^{n/2}},$$

from which part (ii) follows.

Proof of main theorem

For part (*iii*) we have:

$$T_{2^n} = \sum_{k=1}^{n} T_{2^n}(k) = \sum_{k=1}^{\lfloor n/4 \rfloor - 1} T_{2^n}(k) + \sum_{k=\lfloor n/4 \rfloor}^{n} T_{2^n}(k).$$

Considering these two sums in turn, using part (*i*), for the first term we have

$$\begin{aligned} 2^n &+ (2^n + 2^{n-1} + \cdots + 2^{n-\lfloor n/4 \rfloor + 2}) \\ &+ O(2^{n/2+2} + 2^{n/2+3} + \cdots + 2^{n/2+\lfloor n/4 \rfloor}) \\ &= 2^n + \left(\frac{2^{n+1} - 1}{2-1} - \frac{2^{n-\lfloor n/4 \rfloor + 2} - 1}{2-1} \right) + O(2^{n/2+\lfloor n/4 \rfloor + 1}) \\ &= 2^n + \frac{2^{n+1} - 1}{2-1} + O(2^{3n/4}). \end{aligned}$$

Proof of main theorem

Observe that $p^{k+1} \mid t \implies p^k \mid t$ and so $T_{2^n}(k+1) \leq T_{2^n}(k)$, which for the second term gives

$$\sum_{k=\lfloor n/4 \rfloor}^{n} T_{2^n}(k) \leq (3n/4 + 2) \cdot T_{2^n}(\lfloor n/4 \rfloor) = O(n \cdot 2^{3n/4}).$$

Combining these one obtains

$$T_{2^n} = 2^n + \frac{2^{n+1} - 1}{2 - 1} + O(n \cdot 2^{3n/4}),$$

which proves (*iii*). Part (*iv*) follows with the same argument, but without the first term. Part (*v*) now follows immediately from parts (*iii*) and (*iv*).

Summary and related/further work

- $\lim_{n\to\infty}\left(\prod_{a\in\mathbb{F}_{2^n}^\times}|S_2(E_{2^n}(a))|\right)^{\frac{1}{2^n}} = 8$
- $\lim_{n\to\infty}\left(\prod_{a\in\mathbb{F}_{3^n}^\times}|S_3(E_{3^n}(a))|\right)^{\frac{1}{3^n}} = 3\sqrt{3}$

Summary and related/further work

- $\lim_{n\to\infty}\left(\prod_{a\in\mathbb{F}_{2^n}^{\times}} |S_2(E_{2^n}(a))|\right)^{\frac{1}{2^n}} = 8$
- $\lim_{n\to\infty}\left(\prod_{a\in\mathbb{F}_{3^n}^{\times}} |S_3(E_{3^n}(a))|\right)^{\frac{1}{3^n}} = 3\sqrt{3}$
- Zinoviev independently came up with essentially the same point halving method using division polynomials (WCC 2011), but did not analyse its complexity

Summary and related/further work

- $\lim_{n\to\infty}\left(\prod_{a\in\mathbb{F}_{2^n}^{\times}} |S_2(E_{2^n}(a))|\right)^{\frac{1}{2^n}} = 8$
- $\lim_{n\to\infty}\left(\prod_{a\in\mathbb{F}_{3^n}^{\times}} |S_3(E_{3^n}(a))|\right)^{\frac{1}{3^n}} = 3\sqrt{3}$
- Zinoviev independently came up with essentially the same point halving method using division polynomials (WCC 2011), but did not analyse its complexity
- By traversing isogeny graphs, can find all Kloosterman zeros in essentially linear time, assuming there are $\tilde{O}(\sqrt{p^n})$ zeros (not explicitly proven)