The frequency of elliptic curve groups over prime finite fields

Dimitris Koukoulopoulos

Joint work with V. Chandee, C. David and E. Smith

Université de Montréal

CNTA XIII, Carleton University, Ottawa
June 20, 2014

Elliptic curve groups over $\mathbb{F}_p$

If E is an elliptic curve over $\mathbb{F}_p$, then

$$E(\mathbb{F}_p) := \text{set of } \mathbb{F}_p \text{ points on } E \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}.$$

for a unique pair of integers (m, k).

Question (Banks, Pappalardi, Shparlinski)

$\mathcal{S} := \{(m, k) : \exists\, p \textit{ and } E/\mathbb{F}_p \textit{ such that } E(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}\,\} = ?$

- If $N = m^2k$, Hasse's bound implies that

$$|p + 1 - N| \leq 2\sqrt{p} \quad \Leftrightarrow \quad |p - 1 - N| < 2\sqrt{N}$$

- $E(\overline{\mathbb{F}_p})[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \subset E(\mathbb{F}_p) \xrightarrow{\text{Weil pairing}} p \equiv 1 \pmod{m}$.

Theorem (Rück)

$(m, k) \in \mathcal{S}$ *if-f there is* $p \equiv 1 \pmod{m}$ *with* $|p - N - 1| < 2\sqrt{N}$.

Counting the possible group structures

Theorem (Rück)

$(m, k) \in \mathcal{S}$ *if-f there is* $p \equiv 1 \pmod{m}$ *with* $|p - N - 1| < 2\sqrt{N}$.

$$S(M, K) := \#\{(m, k) \in \mathcal{S} : m \leq M,\ k \leq K\}.$$

Theorem

(a) *(CDKS, 2013) If* $M \leq K^{1/4-\epsilon}$*, then* $S(M, K) \sim MK$.

(b) *(K., 2014) If* $M \leq K^{13/34-\epsilon}$*, then* $S(M, K) \sim MK$.

(c) *(CDKS, 2013) If* $M \geq e^{(\log K)^{2+\epsilon}} \Leftrightarrow K \leq (\log M)^{2-\epsilon'}$*, then* $S(M, K) = o(MK)$.

Counting the frequency of a given group structure

$$M_p(G) := \sum_{\substack{E/\mathbb{F}_p \\ E(\mathbb{F}_p) \cong G}} \frac{1}{|\operatorname{Aut}_p(E)|},$$

with the sum running over isomorphism classes of e.c. over $\mathbb{F}_p$.

Remark

$|\operatorname{Aut}_p(E)| = 2$ *for all but* $O(1)$ *elliptic curves over* $\mathbb{F}_p$*, so*

$$M_p(G) = \frac{1}{2}\#\{E/\mathbb{F}_p : E(\mathbb{F}_p) \cong G\} + O(1).$$

$$M(G) := \sum_p M_p(G).$$

If $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ and $N = |G| = m^2k$, then

$$M(G) = \sum_{\substack{|p-N-1|<2\sqrt{N} \\ p \equiv 1 \pmod{m}}} M_p(G).$$

Remark

For an elliptic curve $E/\mathbb{Q}$, we set

$$M(G; E) = \#\{p : E_p(\mathbb{F}_p) \cong G\}.$$

If $E_{a,b}$ denotes the elliptic curve with equation $y^2 = x^3 + ax + b$ and $\mathcal{C}(A, B) = \{(a, b) : |a| \leq A,\ |b| \leq B,\ 4a^3 + 27b^2 \neq 0\}$, then

$$\lim_{A,B\to\infty} \frac{1}{|\mathcal{C}(A, B)|} \sum_{(a,b)\in\mathcal{C}(A,B)} M(G; E_{a,b}) = M(G).$$

David, Smith : it suffices to take $A, B > N^{1/2+\epsilon}$ with $AB > N^{3/2+\epsilon}$, where $N = |G|$.

Known results on $M(G)$

$$M(G) = \sum_{p} \sum_{\substack{E/\mathbb{F}_p \\ E(\mathbb{F}_p)\cong G}} \frac{1}{|\operatorname{Aut}_p(E)|};$$

if $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$, then $N = m^2 k$ and

$$K(G) := \prod_{\ell \nmid N} \left(1 - \frac{\left(\frac{N-1}{\ell}\right)^2 \ell + 1}{(\ell-1)^2(\ell+1)}\right) \prod_{\ell \mid m} \left(1 - \frac{1}{\ell^2}\right) \prod_{\substack{\ell \mid k \\ \ell \nmid m}} \left(1 - \frac{1}{\ell(\ell-1)}\right).$$

Theorem (David, Smith (2013))

Assuming appropriate conjectures about primes in short intervals, and if $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ with $m \leq (\log k)^A$ and $2 \nmid mk$, then

$$M(G) \sim K(G) \cdot \frac{|G|^2}{|\operatorname{Aut}(G)|} \cdot \frac{1}{\log |G|} \asymp \frac{k}{\log N} \frac{mk}{\phi(m)\phi(k)} \quad (|G| \to \infty).$$

New results on $M(G)$

$$\text{We expect that} \quad M(G) \sim K(G) \cdot \frac{|G|^2}{|\operatorname{Aut}(G)|} \cdot \frac{1}{\log |G|}$$

when $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ with $m \leq k^A$. (Recall that $K(G) \asymp 1$.)

Theorem (Chandee, David, K., Smith (2014))

Let $m \leq k^A$ with $N = m^2 k > 1$ and set

$$\delta = \frac{1}{4\sqrt{N}/(\phi(m)\log N)} \sum_{\substack{|p-N-1|<2\sqrt{N} \\ p\equiv 1 \pmod{m}}} \sqrt{1 - \left(\frac{p-N-1}{2\sqrt{N}}\right)^2} \ll 1,$$

If $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$, then for any fixed $\lambda > 1$,

$$\delta^{\lambda} \cdot \frac{|G|^2}{|\operatorname{Aut}(G)| \log |G|} \ll_{\lambda,A} M(G) \ll_{\lambda,A} \delta^{1/\lambda} \cdot \frac{|G|^2}{|\operatorname{Aut}(G)| \log |G|}.$$

New results on $M(G)$, II

Theorem (Chandee, David, K., Smith (2014))

Fix $\epsilon > 0$ and $A \geq 1$. For $2 \leq x \leq y^{1/4-\epsilon}$ we have that

$$\frac{1}{xy} \sum_{\substack{m \leq x,\, k \leq y \\ mk > 1}} \left| M(G_{m,k}) - \frac{K(G_{m,k})|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})| \log |G_{m,k}|} \right| \ll \frac{y}{(\log y)^A},$$

where $G_{m,k} := \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$.

Theorem (Chandee, David, K., Smith (2014))

Consider numbers x and y with $1 \leq x \leq \sqrt{y}$. Then there are absolute positive constants c_1 and c_2 such that

$$M(G_{m,k}) \geq c_1 \cdot \frac{|G_{m,k}|^2}{|\operatorname{Aut}(G_{m,k})| \log(2|G_{m,k}|)}$$

for at least $c_2 xy$ pairs (m, k) with $m \leq x$ and $k \leq y$.

The Lang-Trotter conjecture and Deuring's theorem

Consider the related question of how big is

$$M^{\#}(N) = \sum_{p} M_p^{\#}(N), \quad \text{where} \quad M_p^{\#}(N) = \sum_{\substack{E/\mathbb{F}_p \\ |E(\mathbb{F}_p)|=N}} \frac{1}{|\operatorname{Aut}_p(E)|}.$$

This is related to the Lang-Trotter conjecture: given a **fixed** elliptic curve $E/\mathbb{Q}$ and some $t \in \mathbb{Z}$, then how big is

$$\#\{p \leq x : p + 1 - |E_p(\mathbb{F}_p)| = t\}?$$

In $M^{\#}(N)$ we are averaging over E. We use Deuring's theorem, a.k.a. vertical Sato-Tate: if $|p - N - 1| < 2\sqrt{N}$ and $D = (p - N - 1)^2 - 4N$, then

$$M_p^{\#}(N) = H(D) := \sum_{\substack{f^2 | D \\ D/f^2 \equiv 0,1 \pmod 4}} \frac{h(D/f^2)}{w(D/f^2)}.$$

If $|p-1-N| < 2\sqrt{N}$ and $n^2|N$, then

$$M_p^{\#}(N;n) := \sum_{\substack{E/\mathbb{F}_p,\, |E(\mathbb{F}_p)|=N \\ E(\mathbb{F}_p)[n]\cong\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}}} \frac{1}{|\operatorname{Aut}_p(E)|} \overset{\text{Schoof}}{=} H(D_p/n^2)\cdot \mathbf{1}_{p\equiv 1 \pmod{n}},$$

where $D_p = (p-N-1)^2 - 4N$.

If $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ and $N = |G|$, then

$$M_p(G) \overset{\text{incl-excl}}{=} \sum_{r^2|k} \mu(r) M_p^{\#}(N;rm) = \widetilde{H}(d_p) := \sum_{\substack{f^2|d_p,\, (f,k)=1 \\ \frac{d_p}{f^2}\equiv 0,1 \pmod{4}}} \frac{h(d_p/f^2)}{w(d_p/f^2)},$$

where $d_p = D_p/m^2 = (j-mk)^2 - 4k$ if $p = 1 + jm$.

Lemma

$$M(G) = \sum_{\substack{|p-N-1|<2\sqrt{N} \\ p\equiv 1 \pmod{m}}} \sum_{\substack{f^2|d_p,\, (f,k)=1 \\ d_p/f^2\equiv 0,1 \pmod{4}}} \frac{\sqrt{|d_p|}}{2\pi f} L\left(1, \left(\frac{d_p/f^2}{\cdot}\right)\right).$$

Bounds for $M(G)$, $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$

Corollary

Let $N = m^2 k$, $d_{1+jm} = (j - mk)^2 - 4k$ *and* $\mathcal{L}(d) = L(1, (\frac{d}{\cdot}))$. *Then*

$$\sum_{\substack{|p-N-1|<2\sqrt{N} \\ p\equiv 1 \pmod{m}}} \sqrt{|d_p|}\mathcal{L}(d_p) \ll M(G) \ll \sum_{\substack{|p-N-1|<2\sqrt{N} \\ p\equiv 1 \pmod{m}}} \frac{|d_p|^{3/2}}{\phi(|d_p|)}\mathcal{L}(d_p).$$

$$\text{Recall} \quad \delta = \frac{1}{4\sqrt{N}/(\phi(m)\log N)} \sum_{\substack{|p-N-1|<2\sqrt{N} \\ p\equiv 1 \pmod{m}}} \sqrt{\frac{|d_p|}{4k}}.$$

$$\frac{1}{\lambda}+\frac{1}{\mu} = 1 : \quad \left(\frac{\delta}{S(-\mu,0)^{1/\mu}}\right)^{\lambda} \ll \frac{M(G)}{\sqrt{kN}/(\phi(m)\log N)} \ll \delta^{1/\lambda} S(\mu,\mu)^{1/\mu},$$

$$\text{where} \quad S(a,b) := \frac{\phi(m)\log N}{4\sqrt{N}} \sum_{\substack{|p-N-1|<2\sqrt{N} \\ p\equiv 1 \pmod{m}}} \sqrt{\frac{|d_p|}{4k}} \left(\frac{|d_p|}{\phi(d_p)}\right)^{b} \mathcal{L}(d_p)^{a}.$$

$$S(a,b)=\frac{\phi(m)\log N}{4\sqrt{N}}\sum_{\substack{|p-N-1|<2\sqrt{N}\\ p\equiv 1\ (\mathrm{mod}\ m)}}\sqrt{\frac{|d_p|}{4k}}\frac{|d_p|^b}{\phi(d_p)^b}\mathcal{L}(d_p)^a \ll \left(\frac{k}{\phi(k)}\right)^a.$$

Reason: if $p=1+jm$, then $d_p=(j-mk)^2-4k$. So $d_p\equiv\square \pmod{k}$.

Three main technical tools in bounding $S(a,b)$:

- Replace $\mathcal{L}(d)$ by $\mathcal{L}(d;y):=\prod_{\ell\le y}(1-\left(\frac{d}{\ell}\right)/\ell)^{-1}$ using zero-density estimates (can take $y=(\log|d_p|)^A$ for most d's).
- Use positivity to majorize $\mathbf{1}_{\text{prime}}$ by a convolution $\lambda * 1$. Here λ is constructed using the beta sieve and has the following properties:
    - $\mathbf{1}_{p|n\ \Rightarrow p>\sqrt{k}}\le 1*\lambda$;
    - $\mathrm{supp}(\lambda)\subset\{n\in\mathbb{N}:\mu^2(n)=1,\ n\le k^{1/10},\ p|n\ \Rightarrow\ p\le\sqrt{k}\}$;
    - If $f:\mathbb{N}\to[-1,1]$ is multiplicative, then

$$\sum_d\frac{\lambda(d)f(d)}{d}\asymp\sum_{p|d\ \Rightarrow p\le\sqrt{k}}\frac{\mu(d)f(d)}{d}=\prod_{\ell\le\sqrt{k}}\left(1-\frac{f(\ell)}{\ell}\right).$$

- Chinese Remainder Theorem

Asymptotic estimates for $M(G)$

$$\text{Recall}: \quad M(G) = \sum_{\substack{|p-N-1|<2\sqrt{N} \\ p\equiv 1 \pmod{m}}} \sum_{\substack{f^2|d_p,\,(f,k)=1 \\ d_p/f^2\equiv 0,1 \pmod{4}}} \frac{\sqrt{|d_p|}\mathcal{L}(d_p/f^2)}{2\pi f}.$$

This eventually leads to:

Theorem (Chandee, David, K., Smith (2014))

If $G = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ *with* $1 \le m \le \sqrt{k}$, *and* $h \in \left[mk^{\epsilon}, \frac{m\sqrt{k}}{(\log k)^{A+3}}\right]$, *then*

$$M(G) = \frac{K(G)|G|^2}{|\operatorname{Aut}(G)|\log|G|} + O_{\epsilon,A}\left(\frac{k}{(\log k)^A} + E\right),$$

where

$$E = \sqrt{k}\sum_{q\le k^{\epsilon}} d_3(q) \sum_{|j-(N+1)/h|<2\sqrt{N}/h} \max_{(a,qm)=1} \left| \sum_{\substack{jh<p\le jh+h \\ p\equiv a \pmod{qm}}} \log p - \frac{h}{\phi(qm)} \right|.$$

Primes in short arithmetic progressions

Theorem (K. (2014))

Let $H = X^{\theta}$ *with* $1/6 + 2\epsilon \leq \theta \leq 1$ *and* $Q^2 \leq H/X^{\alpha+\epsilon}$, *where*

$$\alpha = \begin{cases} (1-\theta)/3 & \text{if } 5/8 \leq \theta \leq 1, \\ 1/8 & \text{if } 13/24 \leq \theta \leq 5/8, \\ 2/3 - \theta & \text{if } 1/2 \leq \theta \leq 13/24, \\ 1/6 & \text{if } 1/6 + 2\epsilon \leq \theta \leq 1/2. \end{cases}$$

$$\Rightarrow \quad \int_X^{2X} \sum_{q \leq Q} \max_{(a,q)=1} \left| \sum_{t<p\leq t+H,\, p\equiv a \,(\mathrm{mod}\, q)} \log p - \frac{H}{\phi(q)} \right| dt \ll_{\epsilon,A} \frac{HX}{(\log X)^A}.$$

- Heath-Brown's identity to decompose the von Mangoldt function
- Approximate functional equation to shorten some sums
- Results of Huxley and of Gallagher-Montgomery on the frequency of large values of Dirichlet polynomials

In our application, $X = x^2y$, $\theta = 1/2 + o(1)$ and $Q \approx x$. So $\alpha = 1/6$ and we need $x^2 \leq (x^2y)^{1/2-1/6-\epsilon} \Leftrightarrow x \leq y^{1/4-\epsilon'}$.

A probabilistic interpretation of the main term

We expect that $$M^{\#}(N) = \sum_{p} \sum_{\substack{E/\mathbb{F}_p \\ |E(\mathbb{F}_p)|=N}} \frac{1}{|\operatorname{Aut}_p(E)|} \sim \frac{K^{\#}(N)N^2}{\phi(N)\log N},$$

where $$K^{\#}(N) = \prod_{\ell \nmid N} \left(1 - \frac{\left(\frac{N-1}{\ell}\right)^2 \ell + 1}{(\ell-1)^2(\ell+1)}\right) \prod_{\ell | N} \left(1 - \frac{1}{\ell^{\nu_\ell(N)}(\ell-1)}\right).$$

David, Martin and Smith : $$\frac{K^{\#}(N)N}{\phi(N)} = \prod_{\ell} \left(\lim_{e\to\infty} \frac{P(\ell^e)}{1/\ell^e} \right)$$

with $P(\ell^e) = \textbf{Prob}\,(\sigma \in GL_2(\mathbb{Z}/\ell^e\mathbb{Z}) : \det(\sigma) + 1 - \operatorname{tr}(\sigma) \equiv N \pmod{\ell^e})$.

Analogy: $\det(\sigma) \leftrightarrow p$, $\operatorname{tr}(\sigma) \leftrightarrow a_p(E)$, $\det(\sigma) + 1 - \operatorname{tr}(\sigma) \leftrightarrow |E(\mathbb{F}_p)|$.

Gekeler : $$\sum_{\substack{E/\mathbb{F}_p \\ |E(\mathbb{F}_p)|=p+1-t}} \frac{1}{|\operatorname{Aut}_p(E)|} = \frac{1}{\pi\sqrt{p}}\left(1-\frac{t^2}{4p}\right)^{1/2}\prod_{\ell} v_\ell(t,p),$$

where for $\ell \nmid p$

$$v_\ell(t,p) = \lim_{e\to\infty} \frac{\textbf{Prob}\left(\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z}) : \begin{array}{l} \mathrm{tr}(\sigma) \equiv t \,(\mathrm{mod}\, \ell^e), \\ \det(\sigma) \equiv p \,(\mathrm{mod}\, \ell^e) \end{array}\right)}{1/(\ell^e\phi(\ell^e))}.$$

$$\mathbb{E}_{p\le x}[v_\ell(t,p)] \sim \lim_{e\to\infty} \frac{\textbf{Prob}\left(\sigma \in \mathrm{GL}_2(\mathbb{Z}/\ell^e\mathbb{Z}) : \mathrm{tr}(\sigma) \equiv t \,(\mathrm{mod}\, \ell^e)\right)}{1/\ell^e}.$$

$$\mathbb{E}_{p\le x}\left[\prod_\ell v_\ell(t,p)\right] \overset{?}{\sim} \prod_\ell \mathbb{E}_{p\le x}[v_\ell(t,p)]$$

Yes (ongoing work with C. David and E. Smith) $\Rightarrow$ new proofs of Lang-Trotter and of Koblitz on average, of asymptotics for $M^{\#}(N)$ and $M(G)$, ...

Thank you!