Group structures of elliptic curves over finite fields

Dimitris Koukoulopoulos
Joint work with Vorrapan Chandee, Chantal David and Ethan Smith

Université de Montréal

2012 CMS Winter Meeting, Montréal
December 8, 2012

Warm-up

$$E: y^2 = x^3 + ax + b, \qquad (*)$$

where a and b are some fixed integers with $4a^3 + 27b^2 \neq 0$.

The set

$$E(\mathbb{Q}) = \{\text{set of solutions to } (*) \text{ over } \mathbb{Q}\} \cup \{\infty\}$$

is a finitely generated abelian group.

Consider the reduction of E over $\mathbb{F}_p$, $p \nmid 4a^3 + 27b^2$:

$$E_p : y^2 = x^3 + a_p x + b_p \quad (a_p = a \,(\mathrm{mod}\, p), b_p = b \,(\mathrm{mod}\, p)), \qquad (*_p)$$

The set

$$E_p(\mathbb{F}_p) = \{\text{set of solutions to } (*_p) \text{ over } \mathbb{F}_p\} \cup \{\infty\}$$

is a finite abelian group of rank at most 2, i.e. $\exists$ unique $m, k \in \mathbb{N}$ such that

$$E_p(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}.$$

Possible group structures

Question

What are the possibilities for $E_p(\mathbb{F}_p)$ as a group, as p runs over all primes and E over all elliptic curves?

$$\mathscr{S} = \{(m,k) : \exists\, p \text{ and } E/\mathbb{F}_p \text{ such that } E(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}\,\}.$$

- If $(m,k) \in \mathscr{S}$ and $N = m^2k$, Hasse's bound implies that

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

- If $(m,k) \in \mathscr{S}$, then $\exists p,\ E/\mathbb{F}_p$ with $E(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$. So

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

Lemma 1

$(m,k) \in \mathscr{S}$ if and only if there is some $p \equiv 1 \pmod{m}$ in $(N - 2\sqrt{N} + 1, N + 2\sqrt{N} + 1) = (m^2k - 2m\sqrt{k} + 1, m^2k + 2m\sqrt{k} + 1)$.

Characterization of admissible groups points

$\mathscr{S} = \{(m,k) : \exists\, p \text{ and } E/\mathbb{F}_p \text{ such that } E(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}\}$.

Lemma 1

$(m,k) \in \mathscr{S}$ if and only if there is some $p \equiv 1 \pmod m$ in $(N - 2\sqrt{N} + 1, N + 2\sqrt{N} + 1) = (m^2k - 2m\sqrt{k} + 1, m^2k + 2m\sqrt{k} + 1)$.

Lemma 2 (Rück)

$N = m^2k = \prod_\ell \ell^{h_\ell}$, $|p - N - 1| < 2\sqrt{N}$. Then $(m,k) \in \mathscr{S}$ if-f

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z} \simeq \mathbb{Z}/p^{h_p}\mathbb{Z} \times \prod_{\ell \neq p} \left(\mathbb{Z}/\ell^{b_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{h_\ell - b_\ell}\mathbb{Z}\right)$$

with $0 \leq b_\ell \leq \min\{v_\ell(p-1), h_\ell/2\}$.

Let $p \equiv 1 \pmod m$ in $(m^2k - 2m\sqrt{k} + 1, m^2k + 2m\sqrt{k} + 1)$, $N = km^2$.

$$v_\ell(m) \leq \lfloor h_\ell/2 \rfloor \quad \text{and} \quad v_\ell(p-1) \geq v_\ell(m), \ \forall \ell \mid m.$$

Take $b_\ell = v_\ell(m)$ in Lemma 2 to deduce Lemma 1.

An average question

Lemma 1

$(m,k) \in \mathscr{S}$ if and only if there is some $p \equiv 1 \pmod{m}$ in $(N - 2\sqrt{N} + 1, N + 2\sqrt{N} + 1) = (m^2k - 2m\sqrt{k} + 1, m^2k + 2m\sqrt{k} + 1)$.

- If k is small, the group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$ might not occur. e.g. if $m = 11, k = 1$, there are no primes $\equiv 1 \pmod{11}$ in $(100, 144)$, so the group $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ is not realized as $E(\mathbb{F}_p)$.
- When $m = 1$, we ask for primes in $(k - 2\sqrt{k} + 1, k + 2\sqrt{k} + 1)$, which should always contain a prime. So all finite cyclic groups should be realized as $E(\mathbb{F}_p)$. Proving this is beyond RH.

Banks-Pappalardi-Shparlinski study

$$\begin{aligned} S(M,K) &= \#\{m \le M, k \le K : (m,k) \in \mathscr{S}\} \\ &= \#\{m \le M, k \le K : \exists p \equiv 1 \pmod{m} \text{ such that} \\ &\qquad\qquad m^2k - 2m\sqrt{k} + 1 < p < m^2k + 2m\sqrt{k} + 1\} \\ &= \#\{m \le M, k \le K : \exists j,\ |j| < 2\sqrt{k},\ \text{with } m^2k + jm + 1 \text{ prime}\}. \end{aligned}$$

Conjectures and heuristics

$$S(M,K) = \#\{m \le M, k \le K : \exists j,\ |j| < 2\sqrt{k},\ \text{with } m^2k + jm + 1 \text{ prime}\}.$$

Conjecture (Banks-Shparlinski-Pappalardi)

$$S(M,K) = \begin{cases} o(MK) & \text{if } K \le (\log M)^{2-\epsilon},\ K \to \infty \\ (1+o(1))MK & \text{if } K \ge (\log M)^{2+\epsilon},\ M \to \infty. \end{cases}$$

$\#\{p \le x\} \sim \int_2^x \frac{dt}{\log t}$. So n is prime with probability $1/\log n$.

$$\textbf{Prob}\left(\{m^2k + jm + 1 \text{ is not prime } \forall j \in [-2\sqrt{k}, 2\sqrt{k}]\}\right)$$

$$\approx \prod_{|j| \le 2\sqrt{k}} \left(1 - \frac{1}{\log(m^2k + jm + 1)}\right)$$

$$\approx \left(1 - \frac{1}{m^2k}\right)^{4\sqrt{k}} \to \begin{cases} 0 & \text{if } \sqrt{k}/\log m \to \infty, \\ 1 & \text{if } \sqrt{k}/\log m \to 0. \end{cases}$$

Results on $S(M, K)$

$S(M,K) = \#\{m \le M, k \le K : \exists j,\ |j| < 2\sqrt{k},\ \text{with } m^2k + jm + 1 \text{ prime}\}.$

Theorem (Banks-Pappalardi-Shparlinski)

$$\begin{cases} S(M,K) \ll_K M/\log M & \textit{for all } M, K \ge 2, \\ S(M,K) \gg_\epsilon MK/\log K & \textit{if } M \le K^{43/94-\epsilon}, \\ S(M,K) \gg_\epsilon MK/(\log K)^2 & \textit{if } M \le K^{1/2-\epsilon}. \end{cases}$$

First part implies BPS conjecture when $K \ll 1$.

Theorem (Chandee-David-K-Smith)

$$\begin{cases} S(M,K) \ll MK^{3/2}/\log M & \textit{for all } M, K \ge 2, \\ S(M,K) = (1 + o_\epsilon(1))MK & \textit{if } M \le K^{1/4-\epsilon}, \\ S(M,K) \gg MK & \textit{if } M \le K^{1/2}. \end{cases}$$

First part implies the full first part of the BPS conjecture, i.e. $S(M,K) = o(MK)$ when $K \le (\log M)^{2-\epsilon}$. Second part implies the second part of the BPS conjecture when $M \le K^{1/4-\epsilon}$.

Proof of $S(M,K) \ll MK^{3/2}/\log M$

$$S(M,K) = \#\{m \le M, k \le K : \exists j,\ |j| < 2\sqrt{k},\ \text{with } m^2k + jm + 1 \text{ prime}\}$$

$$\le \sum_{m \le M} \sum_{k \le K} \sum_{\substack{|j| \le 2\sqrt{k} \\ m^2k+jm+1 \text{ is prime}}} 1 = \sum_{k \le K} \sum_{|j|<2\sqrt{k}} \sum_{\substack{m \le M \\ m^2k+jm+1 \text{ is prime}}} 1$$

$$\ll \sum_{k \le K} \sum_{|j|<2\sqrt{k}} \frac{M}{\log M} \frac{k}{\phi(k)} \prod_{p \le M} \left(1 - \frac{\left(\frac{j^2-4k}{p}\right)}{p}\right).$$

Elliott: Zero-density estimates imply that ...

$$S(M,K) \ll \frac{M}{\log M} \sum_{k \le K} \frac{k}{\phi(k)} \sum_{|j|<2\sqrt{k}} \prod_{p \le (\log M)^{100}} \left(1 - \frac{\left(\frac{j^2-4k}{p}\right)}{p}\right)$$

$$\asymp \frac{M}{\log M} \cdot K \cdot K^{1/2} = \frac{MK^{3/2}}{\log M}.$$

$S(M,K) \sim MK$ when $M \leq K^{1/4-\epsilon}$

$$S(M,K) = \#\{m \leq M, k \leq K : \exists p \equiv 1 \pmod{m} \text{ such that } m^2k - 2m\sqrt{k} + 1 < p < m^2k + 2m\sqrt{k} + 1\}.$$

Theorem (K)

Let $1 \leq h \leq x$ and $1 \leq Q^2 \leq h/x^{1/6+\epsilon}$. For every $A > 0$

$$\frac{1}{x}\int_x^{2x} \sum_{q \leq Q} \max_{(a,q)=1} \left| \sum_{\substack{y<p\leq y+h \\ p\equiv a \,(\mathrm{mod}\, q)}} \log p - \frac{h}{\phi(q)} \right| dy \ll_A \frac{h}{(\log x)^A}.$$

This is proven using zero-density estimates. Most likely it is possible to improve the range $M \leq K^{1/4-\epsilon}$ using sieve-theoretic ideas.

To control $S(M,K)$, we apply the theorem with $x = M^2K$, $h = M\sqrt{K}$, $Q = M$. We need $M^2 \leq M\sqrt{K}/(M^2K)^{1/6+\epsilon}$.

$S(M,K) \gg MK$ when $M \le \sqrt{K}$

$$S(M,K) = \#\{m \le M, k \le K : \exists p \equiv 1 \pmod{m} \text{ such that } p \in I_{m^2k} = (m^2k - 2m\sqrt{k} + 1, m^2k + 2m\sqrt{k} + 1)\}.$$

The Brun-Titchmarsch inequality implies that

$$\#\{p \in I_{m^2k} : p \equiv 1 \pmod{m}\} \ll \frac{m\sqrt{k}}{\phi(m)\log(2k)}.$$

So

$$\begin{aligned} S(M,K) &\gg \sum_{m \le M} \sum_{k \le K} \frac{\#\{p \in I_{m^2k} : p \equiv 1 \pmod{m}\}}{\frac{m^2k}{\phi(m)\log(2k)}} \\ &\gg \frac{\log K}{\sqrt{K}} \sum_{\substack{m \asymp M \\ k \asymp K}} \frac{\phi(m)}{m} \sum_{\substack{p \in I_{m^2k} \\ p \equiv 1 \pmod{m}}} 1 \\ &= \frac{\log K}{\sqrt{K}} \sum_{m \asymp M} \frac{\phi(m)}{m} \sum_{\substack{p \asymp M^2K \\ p \equiv 1 \pmod{m}}} \sum_{\substack{k \asymp K \\ |k-p-1| < 2\sqrt{p}/m^2}} 1 \end{aligned}$$

Thank you!