Possible Group Structures of Elliptic Curves over Finite Fields

Igor Shparlinski (Sydney)

Joint work with:

Bill Banks (Columbia-Missouri)
Francesco Pappalardi (Roma)

Introduction

Two common beliefs

A. Besides torsion groups, we know where little about possible group structures of elliptic curves over $\mathbb{Q}$.

B. We know everything we need about possible group structures of elliptic curves over $\mathbb{F}_q$, *Ruck, Schoof, Voloch, Waterhouse, . . .*

A. is certainly correct. . .

How about **B.**?

What do we know about $E(\mathbb{F}_q)$?

$E(\mathbb{F}_q)$ is of rank two:

$$E(\mathbb{F}_q) \cong \mathbf{Z}_n \times \mathbf{Z}_{nk}$$

E.g., nk is the exponent of $E(\mathbb{F}_q)$.

<u>Question:</u> What pairs (n,k) can be realised by all possible prime powers q and curves $E/\mathbb{F}_q$?

We introduce and study the set

$$\mathcal{S}_{\Pi} = \{(n,k) \in \mathbb{N} \times \mathbb{N} \ : \quad \exists \ \text{prime power } q \text{ and } E/\mathbb{F}_q \text{ with } E(\mathbb{F}_q) \cong \mathbf{Z}_n \times \mathbf{Z}_{nk}\}$$

We are also study the subset $\mathcal{S}_{\pi} \subset \mathcal{S}_{\Pi}$ defined by

$$\mathcal{S}_{\pi} = \{(n,k) \in \mathbb{N} \times \mathbb{N} \ : \quad \exists \ \text{prime } p \text{ and } E/\mathbb{F}_p \text{ with } E(\mathbb{F}_p) \cong \mathbf{Z}_n \times \mathbf{Z}_{nk}\}$$

What do we know about n and k?

Hasse Bound:

$$\#E(\mathbb{F}_q) = n^2k = q + 1 - t \quad \text{where } |t| \le 2q^{1/2}$$

Weil pairing

$$n \mid q - 1$$

Lemma 1 *If q is a prime power, and $E/\mathbb{F}_q$ is such that*

$$E(\mathbb{F}_q) \cong \mathbf{Z}_n \times \mathbf{Z}_{nk},$$

then

$$q = n^2k + n\ell + 1 \quad \textit{where } |\ell| \le 2\sqrt{k}.$$

Warning: These conditions are **almost** “if and only if”, but not quite. . .

Remark: Given an pair (n, k) we can test whether $(n, k) \in \mathcal{S}_\Pi$ or $(n, k) \in \mathcal{S}_\pi$ in finitely many steps.

What do we study?

One expects $\mathcal{S}_\pi$ and $\mathcal{S}_\Pi$ to be reasonably "dense" in $\mathbb{N} \times \mathbb{N}$, the complementary sets appear to be rather large:

List of the pairs $(n,k) \notin \mathcal{S}_\Pi$ with $n,k \le 25$:

$$(11,1),(11,14),(13,6),(19,7),(19,10),(19,14),\\ (19,15),(19,18),(21,18),(23,1),(23,5),(23,8),\\ (23,19),(25,5),(25,14).$$

To investigate the distribution of the elements of $\mathcal{S}_\pi$ and of $\mathcal{S}_\Pi$, we introduce the sets

$$\mathcal{S}_\pi(N,K) = \Big\{(n,k) \in \mathcal{S}_\pi \ : \ n \le N,\ k \le K\Big\},$$
$$\mathcal{S}_\Pi(N,K) = \Big\{(n,k) \in \mathcal{S}_\Pi \ : \ n \le N,\ k \le K\Big\},$$

We obtain estimates for the cardinalities of these sets in various ranges of N and K

We consider the set of primes p such that $\mathbf{Z}_n \times \mathbf{Z}_{nk}$ can be realized as the group of points of an elliptic curve over $\mathbb{F}_p$:

$$\mathcal{J}_\pi(n,k) = \{\text{primes } p \ : \quad \exists \ \ E/\mathbb{F}_p \text{ for which } E(\mathbb{F}_p) \cong \mathbf{Z}_n \times \mathbf{Z}_{nk}\}.$$

We obtain an asymptotic formula in certain ranges of N and K for

$$J_\pi(N,K) = \sum_{n \le N} \sum_{k \le K} \# \mathcal{J}_\pi(n,k),$$

Motivated by Lemma 1, we compare

$$\mathcal{N}_{k,m} = \{n \in \mathbb{N} \ : \quad \exists \ \ p \text{ prime and } E/\mathbb{F}_{p^m} \text{ with } E(\mathbb{F}_{p^m}) \cong \mathbf{Z}_n \times \mathbf{Z}_{kn}\}.$$

and

$$\widetilde{\mathcal{N}}_{k,m} = \{n \in \mathbb{N} \ : \quad \exists \ \ l \in \mathbf{Z}, \ p \text{ prime with } |l| \le 2\sqrt{k} \text{ and } p^m = n^2k + ln + 1\}.$$

Basic Tools

Characterisation of cardinalities

Waterhouse (1969):

Lemma 2 *Let $q = p^m$ be a power of a prime p and let $N = q + 1 - a$. There is an elliptic curve $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$ and a satisfies one of the following:*

(i) $\gcd(a, p) = 1$*;*

(ii) m *even and* $a = \pm 2\sqrt{q}$*;*

(iii) m *is even,* $p \not\equiv 1 \pmod 3$*, and* $a = \pm\sqrt{q}$*;*

(iv) m *is odd,* $p = 2$ *or 3, and* $a = \pm p^{(n+1)/2}$*;*

(v) m *is even,* $p \not\equiv 1 \pmod 4$*, and* $a = 0$*;*

(vi) m *is odd and* $a = 0$*.*

Characterisation of group structures

Rück and Voloch (1987)

Lemma 3 *Let N be an integer that occurs as the order of an elliptic curve over a finite field $\mathbb{F}_q$ where $q = p^m$ is a power of a prime p. Write $N = p^e n_1 n_2$ with $p \nmid n_1 n_2$ and $n_1 \mid n_2$. (possibly $n_1 = 1$). There is an elliptic curve E over $\mathbb{F}_q$ such that*

$$E(\mathbb{F}_q) \cong \mathbf{Z}_{p^e} \times \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2}$$

if and only if

1. *$n_1 = n_2$ in the case (ii) of Lemma 2;*
2. *$n_1 | q - 1$ in all other cases of Lemma 2.*

Prime fields

Combining Lemmas 2 and 3 we get:

Corollary 4 *If*

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

and $N = n_1 n_2$ *with*

$$n_1 \mid n_2 \quad \textit{and} \quad n_1 \mid p-1$$

then there is an elliptic curve $E/\mathbb{F}_p$ *with*

$$E(\mathbb{F}_p) \cong \mathbf{Z}_{n_1} \times \mathbf{Z}_{n_2}.$$

Corollary 5 *We have*

$$p \in \mathcal{J}_\pi(n,k)$$

if and only if

$$p = n^2 k + n\ell + 1 \quad \textit{where } |\ell| \leq 2\sqrt{k}.$$

For prime $q = p$, Lemma 1 is an "if and only if" statement:

Proof.

"If": Taking $N = n^2k$, we have

$$\begin{aligned} |p+1-N|^2 &= (n\ell+2)^2 = n^2\ell^2 + 4n\ell + 4 \\ &\leq 4n^2k + 4n\ell + 4 = 4p, \end{aligned}$$

hence $|p+1-N| \leq 2\sqrt{p}$. Applying Corollary 4 with $n_1 = n$ and $n_2 = nk$, we see that there is an elliptic curve $E/\mathbb{F}_p$ such that $E(\mathbb{F}_p) \cong \mathbf{Z}_n \times \mathbf{Z}_{nk}$, and thus $p \in \mathcal{J}_\pi(n,k)$.

"Only If": Lemma 1. $\square$

Analytic number theory

We put

$$\pi(x;m,a) = \#\Big\{p \le x \ :\ p \equiv a \pmod{m}\Big\},$$
$$\Pi(x;m,a) = \#\Big\{q \le x \ :\ q \equiv a \pmod{m}\Big\}.$$

Lemma 6 *For all* $N, K \in \mathbb{N}$ *we have*

$$J_\pi(N,K) = \sum_{\substack{n \le N \\ |\ell| \le 2\sqrt{K}}} \Big(\pi(n^2K + n\ell + 1; n^2, n\ell + 1) - \pi(\tfrac{1}{4}n^2\ell^2 + n\ell; n^2, n\ell + 1)\Big).$$

What is next?

Good News: $J_\pi(N, K)$ is expressed via classical functions

Bad News: We need to study primes in short arithmetic progressions: modulus $\asymp N^2$, the length $\asymp K$, while unconditional results are very weak.

Good News: We need this "on average" over n: recall Bombieri-Vinogradov

Bad News: The averaging is over square moduli, rather than over all moduli up to a certain limit.

Good News: *Baier & Zhao* (2008) have exactly this version of the Bombieri-Vinogradov theorem!

Bombieri-Vinogradov theorem modulo squares

As usual, we set

$$\psi(x;m,a) = \sum_{\substack{n \le x \\ n \equiv a \pmod m}} \Lambda(n),$$

where $\Lambda(n)$ is the von Mangoldt function.

Baier & Zhao (2008):

Lemma 7 *For fixed $\varepsilon > 0$ and $C > 0$, we have*

$$\sum_{m \le x^{2/9-\varepsilon}} m \max_{\gcd(a,m)=1} \left| \psi(x;m^2,a) - \frac{x}{\varphi(m^2)} \right| \ll \frac{x}{(\log x)^C}.$$

Moduli m^2 run up to almost $x^{4/9}$, only a little bit behind of $x^{1/2}$ as in the Bombieri-Vinogradov theorem.

Are we done?

Not quite . . . . Things still to be taken care of:

- Switch from ψ to π
  - Partial summation!
- The upper limits in $\pi(n^2K + n\ell + 1; n^2, n\ell + 1)$ and $\pi(\frac{1}{4}n^2\ell^2 + n\ell; n^2, n\ell + 1)$ are "moving" with n.
  - Separate the range of summation over n, into $O(\Delta^{-1} \log N)$ intervals $[M, M + \Delta M]$
  - replace n^2 with M^2 (up to the error term of $O(M^2\Delta)$
  - optimise Δ

We can deal with $J_\pi(N, K)$ for $N \le K^{2/5-\varepsilon}$, i.e., for groups generated by E/F_p with a large torsion group over $\mathbb{F}_p$.

Sets $\mathcal{S}_{\prod}(N,K)$ and $\mathcal{S}_{\prod}(N,K)$

Theorem 8 *For any* $\varepsilon > 0$ *and* $N \le K^{2/5-\varepsilon}$,

$$NK \ge \#\mathcal{S}_{\prod}(N,K) \ge \#\mathcal{S}_{\pi}(N,K) \gg \frac{NK}{\log K}.$$

Proof. If $p = 1 + n^2k$ then

$$(n,(q-1)/n^2) \in \mathcal{S}_{\pi}(N,K)$$

$$\Downarrow$$

$$\begin{aligned}
\#\mathcal{S}_{\pi}(N,K) &\ge \sum_{n\le N} \pi(n^2K, n^2, 1)\\
&\ge \sum_{N/2\le n\le N} \pi(n^2K, n^2, 1)\\
&\gg \frac{1}{\log K}\sum_{N/2\le n\le N} \psi(n^2K, n^2, 1)\\
&\gg \frac{1}{\log K}\sum_{N/2\le n\le N} \psi(N^2K/4, n^2, 1).
\end{aligned}$$

The result of *Baier & Zhao* (2008), i.e., Lemma 7, applies if $N \ll (N^2K)^{2/9-\delta}$ for some $\delta > 0$ or $N \ll K^{2/5-\varepsilon}$ for some $\varepsilon > 0$. $\square$

Suppose that K is fixed

We are interested in prime powers:

$$q = n^2 k + n\ell + 1 \quad \text{and} \quad |\ell| \leq 2\sqrt{k}$$

Good News: Sieve methods can be used for upper bounds

Bad News: We need explicit bounds and we have $\sim 4k^{1/2}$ progressions.

Good News: When k is fixed this should work.

Selberg sieve:

Theorem 9 *For any integer $K \geq 1$ there exists a constant $A(K)$ such that*

$$\#\mathcal{S}_{\prod}(N, K) \leq A(K) \frac{N}{\log N}.$$

E.g., there are infinitely many pairs (n, k) which do not lie in $\mathcal{S}_{\prod}$. More precisely:

Corollary 10 *For every k_0, almost all $(n, k_0) \notin \mathcal{S}_{\prod}$.*

E.g. there are infinitely many pairs (n, k) which do not lie in $\mathcal{S}_{\prod}$.

More precisely, for every k_0, almost all $(n, k_0) \notin \mathcal{S}_{\prod}$.

<u>Suppose that N is fixed</u>

It is quite reasonable to believe that $\mathcal{S}_{\Pi}$ contains all pairs $(n, k) \in \mathbb{N} \times \mathbb{N}$ with $n \leq N_0$ except for at most finitely many.

This is a consequence of an analogue of the Cramer's Conjecture for primes in a fixed arithmetic progression (and is out of reach . . .).

<u>Easier (?) Question</u>: Let n_0 be fixed, Is it true that for almost k, $(n_0, k) \in \mathcal{S}_{\Pi}$?

Set $\mathcal{S}_{\prod}(N,K) \setminus \mathcal{S}_{\pi}(N,K)$

Question: Prime powers $q = p^m$ with $m \geq 2$ are very rare. Do they contribute to $\mathcal{S}_{\prod}$?

Yes!

$$\#(\mathcal{S}_{\prod}(N,1) \setminus \mathcal{S}_{\pi}(N,1)) \geq (1+o(1))\frac{N}{12\log N}$$

Open Question: Any contribution to $\mathcal{S}_{\prod} \setminus \mathcal{S}_{\pi}$ from $k \geq 2$?

Sets $\mathcal{N}_{k,m}$ and $\widetilde{\mathcal{N}}_{k,m}$

Recall:

$$\mathcal{N}_{k,m} = \{n \in \mathbb{N} \ : \ \exists \ p \text{ prime and } E/\mathbb{F}_{p^m} \text{ with } E(\mathbb{F}_{p^m}) \cong \mathbf{Z}_n \times \mathbf{Z}_{kn}\}.$$

and

$$\widetilde{\mathcal{N}}_{k,m} = \{n \in \mathbb{N} \ : \ \exists \ l \in \mathbf{Z},\ p \text{ prime with } |l| \le 2\sqrt{k} \text{ and } p^m = n^2k + ln + 1\}.$$

We have

$$\mathcal{N}_{k,m} \subseteq \widetilde{\mathcal{N}}_{k,m}$$

Question Is the inclusion proper?

Theorem 11 *We have,* $\mathcal{N}_{k,1} = \widetilde{\mathcal{N}}_{k,1}$.

Proof. Easy! $\square$

For $m = 2$, the situation is more complicated. We have:

Theorem 12 *We have that*

$$\mathcal{N}_{k,2} = \widetilde{\mathcal{N}}_{k,2}$$

except possibly in the following cases:

(i) $k = p^2 + 1$ *and* $p \equiv 1 \pmod 4$ *when*

(ii) $k = p^2 \pm p + 1$ *and* $p \equiv 1 \pmod 3$*;*

(iii) $k = M^2$*,* $M > 1$*.*

In the cases (i) and (ii), we have $\widetilde{\mathcal{N}}_{k,2} \setminus \mathcal{N}_{k,2} \subseteq \{1\}$ *while in the case (iii) we have*

$$\mathcal{N}_{M^2,2} = \begin{cases} \{1\} & \text{if } M \text{ is prime} \\ \emptyset & \text{otherwise} \end{cases}$$

and

$$\widetilde{\mathcal{N}}_{M^2,2} \setminus \mathcal{N}_{M^2,2} \supset \{(p \pm 1)/M \ : \ p \equiv 1 \pmod M \text{ is prime}\}.$$

Proof. Uses some properties of the Pell equation.

$\square$

Corollary 13 *Suppose that k is not a perfect square. We have the following:*

$$\mathcal{N}_{2,k}(T) \ll_k \log T.$$

Furthermore

$$\begin{aligned} \mathcal{N}_{2,1}(T) &= \pi(T-1) + \pi(T+1) \\ &\quad - \#\{p \leq T+1 \ : \ p, p-2 \text{ are prime}\} \end{aligned}$$

For $m \geq 3$, the situation is more complicated. . .

Even the case $k = 1$ is hard:

Conjecture 1 *Let $m \geq 4$. Then the (positive) integer solutions the three Diophantine equations:*

$$y^m = x^2 + 1, \quad y^m = x^2 + x + 1, \quad y^m = x^2 - x + 1.$$

are respectively

$$\{(0, 1)\}, \quad \{(0, 1)\}, \quad \{(1, 1), (0, 1)\}.$$

Faltings Theorem $\Longleftarrow$ the set of solutions is finite.

Conjecture 2 *The set of finite points with integer coordinates of the elliptic curve:*

$$E: \quad y^3 = x^2 + x + 1$$

is

$$\{(-19, 7), (18, 7), (-1, \pm 1), (0, \pm 1)\}.$$

Conductor 3^5 and it is called 243a1 in Cremona's Table. E is 243a1 in Cremona's Table, it is of conductor 3^5, and its Mordell-Weyl group generated by $(1, 1)$.

Special case of the *Bateman and Horn Conjecture:*

Conjecture 3 *Suppose* $f(X) = X^2 + aX + 1$ *is irreducible over* **Z**. *Then*

$$\#\{n \leq T \ : \ f(n) \text{ is prime}\} = \frac{1 + o(1)}{\gcd(2, a)} \prod_{p>3} \left(1 - \frac{\left(\frac{a^2-4}{p}\right)}{p - 1}\right) \cdot \frac{T}{\log T},$$

where (b/p) *is the Legendre symbol modulo* p.

Theorem 14 *Under the Conjectures 1 and 2, we have the following: if $m = 2r$ is even, then*

$$\#\mathcal{N}_{1,m}(T) = (m + o(1))\,\frac{T^{1/r}}{\log T}.$$

If $m > 3$ is odd, then $\mathcal{N}_{1,m}(T)$ is empty while $\mathcal{N}_{1,3} = \{18, 19\}$. If $m = 1$, then

$$\mathcal{N}_{1,1}(T) \ll \frac{T}{\log T}.$$

Finally, assuming Conjecture 3, there exists a constant $\alpha > 0$ such that

$$\mathcal{N}_{1,1}(T) = (\alpha + o(1))\,\frac{T}{\log T}.$$

Conclusion

$\log\log\log n$ *has been proved to go to infinity with* n*, but it has never been observed doing so . . .*

Carl Pomerance