Elliptic curves with a given number of points over finite fields

Chantal David, Concordia University, Montréal.
Joint work with Ethan Smith, CRM, Montréal

Korea, December 2011

Elliptic curves over $\mathbb{Q}$

Let E be an elliptic curve over $\mathbb{Q}$, i.e.

$$E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{Q}$$

with $\Delta_E = -16(4a^3 + 27b^2) \neq 0$.

Let $E(\mathbb{Q}) = \left\{(X, Y) \in \mathbb{Q}^2 \ : \ Y^2 = X^3 + aX + b\right\}$ be the set of points of E defined over $\mathbb{Q}$.

Theorem (Mordell's Theorem)

$E(\mathbb{Q})$ is a finitely generated generated abelian group.

Elliptic curves over $\mathbb{Q}$

Let E be an elliptic curve over $\mathbb{Q}$, i.e.

$$E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{Q}$$

with $\Delta_E = -16(4a^3 + 27b^2) \neq 0$.

Let $E(\mathbb{Q}) = \left\{(X, Y) \in \mathbb{Q}^2 \ : \ Y^2 = X^3 + aX + b\right\}$ be the set of points of E defined over $\mathbb{Q}$.

Theorem (Mordell's Theorem)

$E(\mathbb{Q})$ is a finitely generated generated abelian group.

For each prime p of good reduction, i.e. $p \nmid \Delta_E$, E reduces to a curve E_p over the finite field $\mathbb{F}_p$ by reducing a and b modulo p.

Elliptic curves over $\mathbb{F}_p$

Let

$$E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{F}_p$$

be an elliptic curve over $\mathbb{F}_p$. Then, $E(\mathbb{F}_p)$ is a abelian group with at most p^2 elements.

Elliptic curves over $\mathbb{F}_p$

Let

$$E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{F}_p$$

be an elliptic curve over $\mathbb{F}_p$. Then, $E(\mathbb{F}_p)$ is a abelian group with at most p^2 elements.

- Each $x_0 \in \mathbb{F}_p$ is the X-coordinate of a point $P = (x_0, y_0) \in E(\mathbb{F}_p)$ if and only if $x_0^3 + ax_0 + b$ is a square modulo p

Elliptic curves over $\mathbb{F}_p$

Let

$$E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{F}_p$$

be an elliptic curve over $\mathbb{F}_p$. Then, $E(\mathbb{F}_p)$ is a abelian group with at most p^2 elements.

- Each $x_0 \in \mathbb{F}_p$ is the X-coordinate of a point $P = (x_0, y_0) \in E(\mathbb{F}_p)$ if and only if $x_0^3 + ax_0 + b$ is a square modulo p
- In that case, there are 2 points $P = (x_0, \pm\sqrt{x_0^3 + ax_0 + b})$ corresponding to such a x_0 with $x_0^3 + ax_0 + b \neq 0$.

Elliptic curves over $\mathbb{F}_p$

Let

$$E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{F}_p$$

be an elliptic curve over $\mathbb{F}_p$. Then, $E(\mathbb{F}_p)$ is a abelian group with at most p^2 elements.

- Each $x_0 \in \mathbb{F}_p$ is the X-coordinate of a point $P = (x_0, y_0) \in E(\mathbb{F}_p)$ if and only if $x_0^3 + ax_0 + b$ is a square modulo p
- In that case, there are 2 points $P = (x_0, \pm\sqrt{x_0^3 + ax_0 + b})$ corresponding to such a x_0 with $x_0^3 + ax_0 + b \neq 0$.

As half of the elements of $\mathbb{F}_p^*$ are squares, and half are non-squares, we can expect that $E(\mathbb{F}_p)$ has about p points.

Order of $E(\mathbb{F}_p)$

Theorem (Hasse bound)

Let E be an elliptic curve defined over $\mathbb{F}_p$. Then,

$$\#E(\mathbb{F}_p) = p + 1 - a_p(E)$$

with

$$|a_p(E)| \leq 2\sqrt{p}.$$

This is a particular case of the Weil's conjectures for the number of points on a curve of genus g over $\mathbb{F}_p$. In that case,

$$|\#C(\mathbb{F}_p) - (p+1)| \leq 2g\sqrt{p}.$$

Order of $E(\mathbb{F}_p)$

The proof uses the Frobenius endomorphism

$$\begin{aligned} \phi_p : E &\rightarrow E \\ (x, y) &\mapsto (x^p, y^p) \end{aligned}$$

which satisfies the quadratic equation

$$T^2 - a_p(E)T + p = (T - \alpha_p(E))(T - \overline{\alpha_p(E)}) = 0$$

with complex conjugate roots.

Endomorphism Ring of E_p over $\mathbb{F}_p$

Let E_p be an elliptic curve over $\mathbb{F}_p$. Let $\mathrm{End}(E_p)$ be the ring of endomorphisms of E_p. Then,

$$\mathbb{Z}[\phi_p] = \mathbb{Z}\left[\sqrt{a_p^2(E) - 4p}\right] \subseteq \mathrm{End}(E_p).$$

If E_p is not supersingular, then

$$\mathrm{End}(E_p) \subseteq \mathbb{Q}\left(\sqrt{a_p(E)^2 - 4p}\right),$$

some quadratic imaginary field.

Group structure of elliptic curves over $\mathbb{F}_p$

Let E be an elliptic curve over $\mathbb{F}_p$

$$E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{F}_p.$$

Then, $E(\mathbb{F}_p)$ is a finite abelian group with $p + 1 - a_p(E)$ elements.

Group structure of elliptic curves over $\mathbb{F}_p$

Let E be an elliptic curve over $\mathbb{F}_p$

$$E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{F}_p.$$

Then, $E(\mathbb{F}_p)$ is a finite abelian group with $p + 1 - a_p(E)$ elements.

Theorem

$E(\mathbb{F}_p)$ is a finite abelian group with rank at most 2, and

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z},$$

for some unique integers N_1, N_2.

Reduction Conjectures

There are many conjectures about properties of the reductions $E_p/\mathbb{F}_p$ at all primes p for a given elliptic curve E over $\mathbb{Q}$. We first review some of the classical ones:

- The Sato-Tate Conjecture
- The Lang-Trotter conjecture for a fixed trace
- The Lang-Trotter conjecture for a fixed endomorphism ring

Complex Multiplication

Let E be an elliptic curve over $\mathbb{Q}$. Since $E(\mathbb{Q})$ is an abelian group, the multiplication-by-m maps

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto [m]P = P \oplus \cdots \oplus P \end{aligned}$$

are endomorphisms of $E(\mathbb{Q})$, and $\mathbb{Z}$ is a subring of $\mathrm{End}(E/\mathbb{Q})$.

Complex Multiplication

Let E be an elliptic curve over $\mathbb{Q}$. Since $E(\mathbb{Q})$ is an abelian group, the multiplication-by-m maps

$$\begin{aligned} [m] : E &\to E \\ P &\mapsto [m]P = P \oplus \cdots \oplus P \end{aligned}$$

are endomorphisms of $E(\mathbb{Q})$, and $\mathbb{Z}$ is a subring of $\mathrm{End}(E/\mathbb{Q})$.

For most curves, $\mathrm{End}(E/\mathbb{Q}) = \mathbb{Z}$. If not, $\mathrm{End}(E/\mathbb{Q})$ is an order in a quadratic imaginary field K and we say that E has complex multiplication (CM).

The Sato-tate Conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$ without CM. For each prime $p \nmid \Delta_E$, E reduces to an elliptic curve over $\mathbb{F}_p$.
We write

$$\frac{a_p(E)}{2\sqrt{p}} = \cos\theta_p, \quad 0 \leq \theta_p \leq \pi.$$

Let $I = (\alpha, \beta) \subseteq (0, \pi)$, for any $0 \leq \alpha < \beta \leq \pi$.

Conjecture (Sato-Tate conjecture)

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Then,

$$\lim_{x\to\infty} \frac{\#\{p \leq x \ : \ \theta_p \in (\alpha, \beta)\}}{\pi(x)} \quad .$$

The Sato-tate Conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$ without CM. For each prime $p \nmid \Delta_E$, E reduces to an elliptic curve over $\mathbb{F}_p$.
We write

$$\frac{a_p(E)}{2\sqrt{p}} = \cos\theta_p, \quad 0 \leq \theta_p \leq \pi.$$

Let $I = (\alpha, \beta) \subseteq (0, \pi)$, for any $0 \leq \alpha < \beta \leq \pi$.

Conjecture (Sato-Tate conjecture)

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication. Then,

$$\lim_{x\to\infty} \frac{\#\{p \leq x \ : \ \theta_p \in (\alpha, \beta)\}}{\pi(x)} = \frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2(\theta)\, d\theta.$$

The Sato-tate Conjecture

The Sato-Tate conjecture was recently proven by Taylor, Harris and Shepherd-Barron. It can be rephrased in the context of Random Matrix Theory as

$$a_p(E) = \alpha_p(E) + \overline{\alpha_p(E)} = \sqrt{p}(e^{i\theta_p} + e^{-i\theta_p}),$$

corresponds to the matrice

$$\begin{pmatrix} e^{i\theta_p} & 0 \\ 0 & e^{-i\theta_p} \end{pmatrix}$$

in USp(2). The measure of the Sato-Tate conjecture is the Haar measure on USp(2).

The Lang-Trotter Conjecture for a fixed trace

Let E be an elliptic curve defined over $\mathbb{Q}$. For each prime $p \nmid \Delta_E$, E reduces to an elliptic curve over $\mathbb{F}_p$.

Conjecture (Lang and Trotter)

Let E be an elliptic curve over $\mathbb{Q}$, and let t be a fixed integer. If E has complex multiplication, then $t \neq 0$. Then

$$\pi_{E,t}(x) \quad = \quad \#\{p \leq x : a_p(E) = t\}$$

The Lang-Trotter Conjecture for a fixed trace

Let E be an elliptic curve defined over $\mathbb{Q}$. For each prime $p \nmid \Delta_E$, E reduces to an elliptic curve over $\mathbb{F}_p$.

Conjecture (Lang and Trotter)

Let E be an elliptic curve over $\mathbb{Q}$, and let t be a fixed integer. If E has complex multiplication, then $t \neq 0$. Then

$$\begin{aligned} \pi_{E,t}(x) &= \#\{p \leq x : a_p(E) = t\} \\ &\sim C(E,t)\frac{\sqrt{x}}{\log x} \end{aligned}$$

where $C(E,t)$ is an explicit constant depending only on E and t.

The Lang-Trotter Conjecture for a fixed trace

- The case $t = 0$ corresponds to the supersingular primes.

The Lang-Trotter Conjecture for a fixed trace

- The case $t = 0$ corresponds to the supersingular primes.
- If E has complex multiplication by a quadratic imaginary field K, then p is supersingular if and only if p splits in K. Then, half of the primes are supersingular in that case.

The Lang-Trotter Conjecture for a fixed trace

- The case $t = 0$ corresponds to the supersingular primes.
- If E has complex multiplication by a quadratic imaginary field K, then p is supersingular if and only if p splits in K. Then, half of the primes are supersingular in that case.
- For E without complex multiplication, Elkies showed that there are infinitely many supersingular primes. If $t \neq 0$, it is not known for any curve E that there are infinitely many primes p such that $a_p(E) = t$.

The Lang-Trotter Conjecture for a fixed trace

- The case $t = 0$ corresponds to the supersingular primes.
- If E has complex multiplication by a quadratic imaginary field K, then p is supersingular if and only if p splits in K. Then, half of the primes are supersingular in that case.
- For E without complex multiplication, Elkies showed that there are infinitely many supersingular primes. If $t \neq 0$, it is not known for any curve E that there are infinitely many primes p such that $a_p(E) = t$.
- If E has complex multiplication by a quadratic field, the conjecture can be rephrased in terms of primes represented by quadratic polynomials. For example, let $E : y^2 = x^3 - x$ with $\mathrm{End}(E/\mathbb{Q}) = \mathbb{Z}[i]$. Then

$$a_p(E) = \pm 1 \iff p = n^2 + 1.$$

The Lang-Trotter Conjecture for the endomorphism rings

Conjecture (Lang and Trotter)

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication, and let K be a fixed quadratic imaginary field. Then

$$\pi_{E,K}(x) \quad = \quad \#\{p \leq x : End(E/\mathbb{Q}) \subset K\}$$

The Lang-Trotter Conjecture for the endomorphism rings

Conjecture (Lang and Trotter)

Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication, and let K be a fixed quadratic imaginary field. Then

$$\begin{aligned} \pi_{E,K}(x) &= \#\{p \leq x : End(E/\mathbb{Q}) \subset K\} \\ &\sim C(E,K)\frac{\sqrt{x}}{\log x}. \end{aligned}$$

Partial results about the Lang-Trotter conjectures

As we mentioned, the only known lower bound for the Lang-Trotter conjectures is the result of Elkies about infinitely many supersingular primes. There are also known upper bounds (with and without the Generalized Riemann Hypothesis).

Partial results about the Lang-Trotter conjectures

As we mentioned, the only known lower bound for the Lang-Trotter conjectures is the result of Elkies about infinitely many supersingular primes. There are also known upper bounds (with and without the Generalized Riemann Hypothesis).

Further evidence for the conjectures can be obtained by showing that the conjectures are true on average, i.e. averaging over all curves $E(a, b)$ in some set. For A, B positive integers, let

$$\mathfrak{C}(A, B) = \left\{ E(a, b) : Y^2 = X^3 + aX + b \ : \ |a| \leq A, |b| \leq B \right\}.$$

Then,

$$\#\mathfrak{C}(A, B) \sim 4AB.$$

We consider the conjectures on average over all curves $E(a, b) \in \mathfrak{C}(A, B)$ when A, B are big.

The Lang-Trotter conjecture on average

Theorem (Fouvry-Murty, David-Pappalardi)

Let $x > 0$, $\varepsilon > 0$, and let A, B be such that $A, B \geq x^{3/4+\varepsilon}$. Then,

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E(a,b)\in\mathfrak{C}(A,B)} \pi_{E(a,b),t}(x)$$

The Lang-Trotter conjecture on average

Theorem (Fouvry-Murty, David-Pappalardi)

Let $x > 0$, $\varepsilon > 0$, and let A, B be such that $A, B \geq x^{3/4+\varepsilon}$. Then,

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E(a,b)\in\mathfrak{C}(A,B)} \pi_{E(a,b),t}(x) \sim \mathfrak{C}\frac{\sqrt{x}}{\log x},$$

as $x \to \infty$, where $\mathfrak{C}$ is an explicit constant which is the average of the conjectural constants $C(E(a,b),t)$ of Lang and Trotter.

The Lang-Trotter conjecture on average

Theorem (Cojocaru-Iwaniec-Jones)

Let $x > 0$, $\varepsilon > 0$, and let A, B be large enough. Then,

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E(a,b)\in\mathfrak{C}(A,B)} \pi_{E(a,b),K}(x) \sim \mathfrak{C}\frac{\sqrt{x}}{\log x},$$

as $x \to \infty$, where $\mathfrak{C}$ is an explicit constant.

Number of reductions with a fixed cardinality N

We are now considering another reduction question, but with a very different flavor as we will see.
Let N be a positive integer. We are interested in

$$M_E(N) := \#\{p : \#E_p(\mathbb{F}_p) = N\}.$$

Number of reductions with a fixed cardinality N

We are now considering another reduction question, but with a very different flavor as we will see.
Let N be a positive integer. We are interested in

$$M_E(N) := \#\{p : \#E_p(\mathbb{F}_p) = N\}.$$

Note that if $\#E_p(\mathbb{F}_p) = N$, then the Hasse bound implies

$$\begin{aligned} & p + 1 - 2\sqrt{p} \; < N < \; p + 1 + 2\sqrt{p} \\ \iff \; & N^- := N + 1 - 2\sqrt{N} \; < p < \; N + 1 + 2\sqrt{N} =: N^+. \end{aligned}$$

Number of reductions with a fixed cardinality N

We are now considering another reduction question, but with a very different flavor as we will see.
Let N be a positive integer. We are interested in

$$M_E(N) := \#\{p : \#E_p(\mathbb{F}_p) = N\}.$$

Note that if $\#E_p(\mathbb{F}_p) = N$, then the Hasse bound implies

$$\begin{aligned} & p + 1 - 2\sqrt{p} \; < N < \; p + 1 + 2\sqrt{p} \\ \iff \; & N^- := N + 1 - 2\sqrt{N} \; < p < \; N + 1 + 2\sqrt{N} =: N^+. \end{aligned}$$

Then, $M_E(N)$ is a finite number, and the Hasse bound implies the bound

$$M_E(N) \ll \frac{\sqrt{N}}{\log(N+1)}.$$

Number of reductions with a fixed cardinality N

Then, $M_E(N)$ is a finite number, and we have the trivial bound

$$M_E(N) \ll \frac{\sqrt{N}}{\log(N+1)}.$$

Number of reductions with a fixed cardinality N

Then, $M_E(N)$ is a finite number, and we have the trivial bound

$$M_E(N) \ll \frac{\sqrt{N}}{\log(N+1)}.$$

It is conjectured that

$$M_E(N) \ll_{E,\varepsilon} N^{\varepsilon},$$

for any $\varepsilon > 0$, but no bound between the trivial bound and the conjecture is known for curves without CM.

Number of reductions with a fixed cardinality N

Then, $M_E(N)$ is a finite number, and we have the trivial bound

$$M_E(N) \ll \frac{\sqrt{N}}{\log(N+1)}.$$

It is conjectured that

$$M_E(N) \ll_{E,\varepsilon} N^{\varepsilon},$$

for any $\varepsilon > 0$, but no bound between the trivial bound and the conjecture is known for curves without CM.

For CM curves, $M_E(N)$ is bounded by the number of ideals of norm N in the field K of complex multiplication, and $M_E(N) \ll_{E,\varepsilon} N^{\varepsilon}$.

Probabilistic Model

If we suppose that the values of $\#E(\mathbb{F}_p)$ are uniformly distributed, i.e., that

$$\text{Prob}\left(\#E(\mathbb{F}_p) = N\right) = \begin{cases} \frac{1}{4\sqrt{p}} & \text{if } N^- < p < N^+, \\ 0 & \text{otherwise,} \end{cases}$$

then we expect that

$$M_E(N) \approx \sum_p \text{Prob}\left(\#E(\mathbb{F}_p) = N\right) = \sum_{N^- < p < N^+} \frac{1}{4\sqrt{p}}$$

$$\sim \frac{1}{4\sqrt{N}} \int_{N^-}^{N^+} \frac{dt}{\log t} \sim \frac{1}{\log N}.$$

Probabilistic Model

If we suppose that the values of $\#E(\mathbb{F}_p)$ are uniformly distributed, i.e., that

$$\text{Prob}\left(\#E(\mathbb{F}_p) = N\right) = \begin{cases} \frac{1}{4\sqrt{p}} & \text{if } N^- < p < N^+, \\ 0 & \text{otherwise,} \end{cases}$$

then we expect that

$$M_E(N) \approx \sum_p \text{Prob}\left(\#E(\mathbb{F}_p) = N\right) = \sum_{N^- < p < N^+} \frac{1}{4\sqrt{p}}$$
$$\sim \frac{1}{4\sqrt{N}} \int_{N^-}^{N^+} \frac{dt}{\log t} \sim \frac{1}{\log N}.$$

This reflects the fact that the primes have density $1/\log N$ in the integers.

Primes in short intervals

To prove the correct order for $M_E(N)$ on average, we have to assume some conjectures about the distribution of primes in short intervals as we have

$$p \in (N^-, N^+) = (N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N}),$$

an interval which is so short that even the Riemann Hypothesis does not guarantee the existence of a prime in this interval.

Primes in short intervals

To prove the correct order for $M_E(N)$ on average, we have to assume some conjectures about the distribution of primes in short intervals as we have

$$p \in (N^-, N^+) = (N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N}),$$

an interval which is so short that even the Riemann Hypothesis does not guarantee the existence of a prime in this interval.

We then work under some conjecture, a generalisation of the Barban-Davenport-Halberstam Theorem for short intervals. Without this conjecture, we cannot get an asymptotic for the average, but upper and lower bounds of the correct order of magnitude using sieve theory.

Average for $M_E(N)$

Theorem

Assume that the BDH Theorem holds for primes in short intervals. Suppose further that $A, B \gg N^{1/2+\varepsilon}$ and that $AB \gg N^{3/2+\epsilon}$. Then as $N \to \infty$, we have

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E \in \mathfrak{C}(A,B)} M_E(N) \sim K(N) \frac{N}{\varphi(N) \log N}$$

where $K(N)$ is uniformly bounded with respect to N.

Average for $M_E(N)$

Theorem

Assume that the BDH Theorem holds for primes in short intervals. Suppose further that $A, B \gg N^{1/2+\varepsilon}$ and that $AB \gg N^{3/2+\epsilon}$. Then as $N \to \infty$, we have

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E \in \mathfrak{C}(A,B)} M_E(N) \sim K(N) \frac{N}{\varphi(N) \log N}$$

where $K(N)$ is uniformly bounded with respect to N.

The "extra factor"

$$\frac{N}{\varphi(N)} = \prod_{p|N} \frac{N}{N-1} \ll \log \log N$$

does not depend on the size of N, but arithmetic properties of N.

The Cohen-Lenstra Heuristics

The general philosophy of Cohen-Lenstra is that random abelian groups occur with probability weigthed by the size of their automorphism group, i.e. the probabilities should be weighted by the factor

$$\frac{\#G}{\#\mathrm{Aut}(G)}.$$

The Cohen-Lenstra Heuristics

The general philosophy of Cohen-Lenstra is that random abelian groups occur with probability weigthed by the size of their automorphism group, i.e. the probabilities should be weighted by the factor

$$\frac{\#G}{\#\mathrm{Aut}(G)}.$$

Cohen and Lenstra looked at class groups of quadratic imaginary fields. For example, they notice that when 9 divides exactly the class number $h(-D)$, then $\mathbb{Z}/9\mathbb{Z}$ occurs about 8 times more often than $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

The Cohen-Lenstra Heuristics

The general philosophy of Cohen-Lenstra is that random abelian groups occur with probability weigthed by the size of their automorphism group, i.e. the probabilities should be weighted by the factor

$$\frac{\#G}{\#\mathrm{Aut}(G)}.$$

Cohen and Lenstra looked at class groups of quadratic imaginary fields. For example, they notice that when 9 divides exactly the class number $h(-D)$, then $\mathbb{Z}/9\mathbb{Z}$ occurs about 8 times more often than $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

In this case

$$\begin{aligned} \#\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) &= \varphi(9) = 6 \\ \#\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) &= 2^2 \times 3 \times 4 = 48. \end{aligned}$$

The Cohen-Lenstra Heuristics

This seem to be the same phenomenon that we notice in our Theorem, where we proved that the average was asymptotic to

$$K(N)\frac{N}{\varphi(N)\log N} = \frac{K(N)}{\log N}\frac{N}{\varphi(N)}.$$

The Cohen-Lenstra Heuristics

This seem to be the same phenomenon that we notice in our Theorem, where we proved that the average was asymptotic to

$$K(N)\frac{N}{\varphi(N)\log N} = \frac{K(N)}{\log N}\frac{N}{\varphi(N)}.$$

For a given group order N, the cyclic groups, which are the most common according to the Cohen-Lenstra philosophy, will dominate, and for $G = \mathbb{Z}/N\mathbb{Z}$,

$$\frac{\#G}{\#\mathrm{Aut}(G)} = \frac{N}{\varphi(N)}.$$

Number of reductions with a fixed group G

To give more evidence for the "Cohen-Lenstra phenomenon" in our Theorem, we fix a group $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$ of cardinality $N = N_1^2N_2$, and we define the following counting function

$$M_E(G) = \{p \ : \ E(\mathbb{F}_p) \simeq G\}$$

Number of reductions with a fixed group G

To give more evidence for the "Cohen-Lenstra phenomenon" in our Theorem, we fix a group $G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$ of cardinality $N = N_1^2N_2$, and we define the following counting function

$$M_E(G) = \{p \ : \ E(\mathbb{F}_p) \simeq G\}$$

Theorem

Assume that the BDH Theorem holds for primes in short intervals. Suppose further that $A, B \gg N^{1/2+\varepsilon}$ and that $AB \gg N^{3/2+\epsilon}$. Then as $N = N_1^2N_2 \to \infty$, with $N_1 \leq (\log N)^\gamma$ and N_2 square-free,

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E \in \mathfrak{C}(A,B)} M_E(G) \sim K(G) \frac{\#G}{\#Aut(G) \log \#G}$$

where $K(G)$ is uniformly bounded with respect to $N = \#G$.

Idea of the proofs

Reversing the order of summation, we have that

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E \in \mathfrak{C}(A,B)} M_E(N)$$

$$= \frac{1}{\#\mathfrak{C}(A,B)} \sum_{N^- < p < N^+} \#\{E \in \mathfrak{C}(A,B) \ : \ \#E(\mathbb{F}_p) = N\}$$

Idea of the proofs

Reversing the order of summation, we have that

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E \in \mathfrak{C}(A,B)} M_E(N)$$
$$= \frac{1}{\#\mathfrak{C}(A,B)} \sum_{N^- < p < N^+} \#\{E \in \mathfrak{C}(A,B) \ : \ \#E(\mathbb{F}_p) = N\}$$

The value of $\#E(a,b)(\mathbb{F}_p)$ depends only on $a \mod p$ and $b \mod p$, and for any $(r,s) \in \mathbb{F}_p^2$,

$$\#\{|a| \leq A, |b| \leq B \ : \ a \equiv r \mod p, \ b \equiv s \mod p\}$$
$$= \left(\frac{2A}{p} + O(1)\right)\left(\frac{2B}{p} + O(1)\right) \sim \frac{4AB}{p^2}.$$

Then,

$$\frac{1}{\#\mathfrak{C}(A,B)} \sum_{E \in \mathfrak{C}(A,B)} M_{E(a,b)}(N)$$

$$= \frac{1}{\#\mathfrak{C}(A,B)} \sum_{N^- < p < N^+} \#\{E \in \mathfrak{C}(A,B) \ : \ \#E(\mathbb{F}_p) = N\}$$

$$\sim \frac{1}{4AB} \sum_{N^- < p < N^+} \frac{4AB}{p^2} \#\{E/\mathbb{F}_p : \ \#E(\mathbb{F}_p) = N\}$$

for A, B big enough with respect to x.

Deuring's Theorem

Theorem

Let t be an integer such that $|t| \leq 2\sqrt{p}$. The number of elliptic curves over $\mathbb{F}_p$ with $a_p(E) = t$ is

$$H(t^2 - 4p)(p-1),$$

where for $D < 0$, the Kronecker class number $H(D)$ is

$$H(D) = \sum_{\substack{f^2 | D \\ \frac{D}{f^2} \equiv 0,1 \bmod 4}} \frac{h(D/f^2)}{w(D/f^2)}$$

defined in terms of the class number $h(D/f^2)$ and the number of units $w(D/f^2)$ of the order of discriminant D in $\mathbb{Q}(\sqrt{D})$.

An average of class numbers

Then, the proof of the average order for $M_E(N)$ is then equivalent to the computation of an average of Kronecker class numbers, since by Deuring's Theorem for

$$N = p + 1 - t \iff t = p + 1 - N,$$

we have

$$\sum_{N^- < p < N^+} \#\{E/\mathbb{F}_p : \#E(\mathbb{F}_p) = N\}$$
$$\sim \sum_{N^- < p < N^+} H((p+1-N)^2 - 4p)\,(p-1).$$

An average of class numbers

Theorem

Assume the BDH conjecture for primes in short intervals. Then, as $N \to \infty$

$$\sum_{N^- < p < N^+} \frac{H((p+1-N)^2 - 4p)}{p} \sim K(N) \frac{N}{\varphi(N) \log N}.$$

An average of class numbers

Theorem

Assume the BDH conjecture for primes in short intervals. Then, as $N \to \infty$

$$\sum_{N^- < p < N^+} \frac{H((p+1-N)^2 - 4p)}{p} \sim K(N) \frac{N}{\varphi(N) \log N}.$$

Evaluating averages of class numbers is a classical subject, going back the conjectures of Gauss for the average class number of real and imaginary quadratic fields.

Number of reductions with a fixed group G

By Deuring's Theorem, for every N such that

$$p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p},$$

there exists E over $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = N$, and there are $H((p+1-N)^2 - 4p)(p-1)$ such curves.

Number of reductions with a fixed group G

By Deuring's Theorem, for every N such that

$$p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p},$$

there exists E over $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = N$, and there are $H((p+1-N)^2 - 4p)(p-1)$ such curves.

The question is more subtle for curves over $\mathbb{F}_p$ with a fixed group structure, and it is not true that for all groups

$$G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$$

of order $N = N_1N_2^2$, where N satisfies the condition above, there are curves over $\mathbb{F}_p$ with $E(\mathbb{F}_p) \simeq G$.

Number of reductions with a fixed group G

By Deuring's Theorem, for every N such that

$$p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p},$$

there exists E over $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p) = N$, and there are $H((p+1-N)^2 - 4p)(p-1)$ such curves.

The question is more subtle for curves over $\mathbb{F}_p$ with a fixed group structure, and it is not true that for all groups

$$G = \mathbb{Z}/N_1\mathbb{Z} \times \mathbb{Z}/N_1N_2\mathbb{Z}$$

of order $N = N_1N_2^2$, where N satisfies the condition above, there are curves over $\mathbb{F}_p$ with $E(\mathbb{F}_p) \simeq G$.

For example, there are no curves over any field $\mathbb{F}_p$ such that

$$G \simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}, \text{ or } G \simeq \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/(11 \cdot 14)\mathbb{Z}, \text{ or}$$
$$G \simeq \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/(13 \cdot 6)\mathbb{Z}, \text{ or } G \simeq \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/(13 \cdot 25)\mathbb{Z}, \text{ etc.}$$

Generalisation of Deuring's Theorem to group structure

Theorem

Let p be a prime, and let N be an odd integer satisfying $p+1-2\sqrt{p} < N < p+1+2\sqrt{p}$. Let $m^2 \mid N$. Then the number of curves over $\mathbb{F}_p$ with exactly N points and full m-torsion over $\mathbb{F}_p$ is

$$\begin{cases} H\left(\frac{(p+1-N)^2-4p}{m^2}\right) & \text{when } p \equiv 1 \mod m \\ 0 & \text{otherwise.} \end{cases}$$

Generalisation of Deuring's Theorem to group structure

Theorem

Let p be a prime, and let N be an odd integer satisfying $p+1-2\sqrt{p} < N < p+1+2\sqrt{p}$. Let $m^2 \mid N$. Then the number of curves over $\mathbb{F}_p$ with exactly N points and full m-torsion over $\mathbb{F}_p$ is

$$\begin{cases} H\left(\frac{(p+1-N)^2-4p}{m^2}\right) & \text{when } p \equiv 1 \mod m \\ 0 & \text{otherwise.} \end{cases}$$

Then, there is a curve over $\mathbb{F}_p$ with $E(\mathbb{F}_p) \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ if and only if there exists a prime $p \equiv 1 \mod N$ such that

$$\begin{aligned} & p+1-2\sqrt{p} < N^2 < p+1+2\sqrt{p} \\ \iff \quad & N^2+1-2N < p < N^2+1+2N. \end{aligned}$$