Density Questions on Elliptic Curves

Mohammad Sadek

Sabanci University, Istanbul

Koç University Mathematics Seminar

March 19, 2024

Goal: Describe the frequency of occurrence of number theoretic objects with certain properties.

Goal: Describe the frequency of occurrence of number theoretic objects with certain properties.

Example:

Arithmetic Statistics

Goal: Describe the frequency of occurrence of number theoretic objects with certain properties.
Example:

$$\pi(X) := \text{the number of prime numbers less than } X$$

Arithmetic Statistics

Goal: Describe the frequency of occurrence of number theoretic objects with certain properties.

Example:

$$\pi(X) := \text{the number of prime numbers less than } X$$

($\sim$1792) Gauss computed tables of $\pi(X)$ by hand for X up to the millions.

Goal: Describe the frequency of occurrence of number theoretic objects with certain properties.
Example:

$$\pi(X) := \text{the number of prime numbers less than } X$$

($\sim$1792) Gauss computed tables of $\pi(X)$ by hand for X up to the millions. Gauss claimed

$$\frac{\pi(X)}{X} \sim \frac{1}{\log X}.$$

Goal: Describe the frequency of occurrence of number theoretic objects with certain properties.

Example:

$$\pi(X) := \text{the number of prime numbers less than } X$$

($\sim$1792) Gauss computed tables of $\pi(X)$ by hand for X up to the millions. Gauss claimed

$$\frac{\pi(X)}{X} \sim \frac{1}{\log X}.$$

($\sim$1896) Hadamard, and de la Vallée-Poussin proved the Prime Number Theorem

$$\lim_{X\to\infty} \frac{\pi(X)/X}{1/\log X} = 1.$$

"It is curious how aggregates rather than single instances creep into our subject even when we aren't looking for statistical trouble."

-Barry Mazur

"It is curious how aggregates rather than single instances creep into our subject even when we aren't looking for statistical trouble."

-Barry Mazur

Question:

"It is curious how aggregates rather than single instances creep into our subject even when we aren't looking for statistical trouble."

-Barry Mazur

Question: ($5 prize)

"It is curious how aggregates rather than single instances creep into our subject even when we aren't looking for statistical trouble."

-Barry Mazur

Question: ($5 prize)

- prove that $aX + b$ with a, b relatively prime integers represent at least one prime number; and yet

"It is curious how aggregates rather than single instances creep into our subject even when we aren't looking for statistical trouble."

-Barry Mazur

Question: (\$5 prize)

- prove that $aX + b$ with a, b relatively prime integers represent at least one prime number; and yet
- the proof doesn't actually show that it represents infinitely many primes.

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,...

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,...
- What is the proportion of primes of the form $4n+1$ among all primes?

Arithmetic Statistics

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,...
- What is the proportion of primes of the form $4n+1$ among all primes?
- For relatively prime integers a and b, define

$$\lim_{X\to\infty} \frac{\#\{p: \ p \text{ is prime of the form } an+b \leq X\}}{\pi(X)}$$

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,...
- What is the proportion of primes of the form $4n+1$ among all primes?
- For relatively prime integers a and b, define

$$\lim_{X\to\infty} \frac{\#\{p:\ p \text{ is prime of the form } an+b \le X\}}{\pi(X)}$$

- Dirichlet proved that the limit above exits;

- 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53,...
- What is the proportion of primes of the form $4n+1$ among all primes?
- For relatively prime integers a and b, define

$$\lim_{X\to\infty} \frac{\#\{p : \ p \text{ is prime of the form } an+b \leq X\}}{\pi(X)}$$

- Dirichlet proved that the limit above exits; and is equal to $1/\phi(a)$, where ϕ is the Euler's totient function.

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

Diophantine Equations

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

(II) If YES, then

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

(II) If YES, then

- can such a solution be found?

Diophantine Equations

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

(II) If YES, then

- can such a solution be found?
- can we describe all such solutions?

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

(II) If YES, then
- can such a solution be found?
- can we describe all such solutions?

(III) Is there a set of instructions to be followed to give answers to questions (I) and (II)?

Diophantine Equations

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

(II) If YES, then
- can such a solution be found?
- can we describe all such solutions?

(III) Is there a set of instructions to be followed to give answers to questions (I) and (II)?

If $\deg f$ is either 1 or 2, then we can answer (I),

Diophantine Equations

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

(II) If YES, then
- can such a solution be found?
- can we describe all such solutions?

(III) Is there a set of instructions to be followed to give answers to questions (I) and (II)?

If $\deg f$ is either 1 or 2, then we can answer (I), and both questions (II) and (III) have affirmative answers.

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

(II) If YES, then
- can such a solution be found?
- can we describe all such solutions?

(III) Is there a set of instructions to be followed to give answers to questions (I) and (II)?

If $\deg f$ is either 1 or 2, then we can answer (I), and both questions (II) and (III) have affirmative answers. What if $\deg f \geq 3$?

Let $f(x_1, \cdots, x_n) = 0$ be a homogeneous polynomial equation with integer coefficients.

(I) Are there nontrivial solutions $(x_1, \cdots, x_n)$ with integer coordiantes?

(II) If YES, then
- can such a solution be found?
- can we describe all such solutions?

(III) Is there a set of instructions to be followed to give answers to questions (I) and (II)?

If $\deg f$ is either 1 or 2, then we can answer (I), and both questions (II) and (III) have affirmative answers. What if $\deg f \geq 3$?

(I') What is the proportion of homogeneous polynomials of degree d in n variables having non-trivial integral zeros?

Our set-up is

$$f(x_1, x_2, x_3) = 0,$$

where the degree of each term of f is exactly 3 (f is homogeneous of degree 3 in 3 variables.)

Our set-up is

$$f(x_1, x_2, x_3) = 0,$$

where the degree of each term of f is exactly 3 (f is homogeneous of degree 3 in 3 variables.)
If $f(x_1, x_2, x_3) = 0$

- describes a smooth curve E, and

Our set-up is

$$f(x_1, x_2, x_3) = 0,$$

where the degree of each term of f is exactly 3 (f is homogeneous of degree 3 in 3 variables.)

If $f(x_1, x_2, x_3) = 0$

- describes a smooth curve E, and
- has at least one nontrivial solution (x_1, x_2, x_3) with integer coordiantes, then

Our set-up is

$$f(x_1, x_2, x_3) = 0,$$

where the degree of each term of f is exactly 3 (f is homogeneous of degree 3 in 3 variables.)
If $f(x_1, x_2, x_3) = 0$

- describes a smooth curve E, and
- has at least one nontrivial solution (x_1, x_2, x_3) with integer coordiantes, then

E is an *elliptic curve*.

"Elliptic curves have been at the heart of many exciting things. They are complicated enough to carry a lot of juicy information, but simple enough to be able to study in depth."

-Peter Sarnak

If E is an elliptic curve over $\mathbb{Q}$, then it can always be described by an affine equation of the form

$$y^2 = x^3 + ax + b,$$

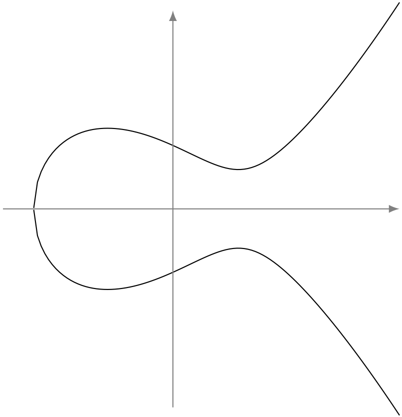
where a and b are integers, and $\Delta = -4a^3 - 27b^2 \neq 0$.

If E is an elliptic curve over $\mathbb{Q}$, then it can always be described by an affine equation of the form

$$y^2 = x^3 + ax + b,$$

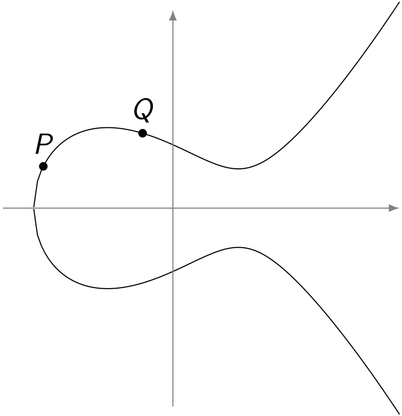
where a and b are integers, and $\Delta = -4a^3 - 27b^2 \neq 0$.

- A group structure!



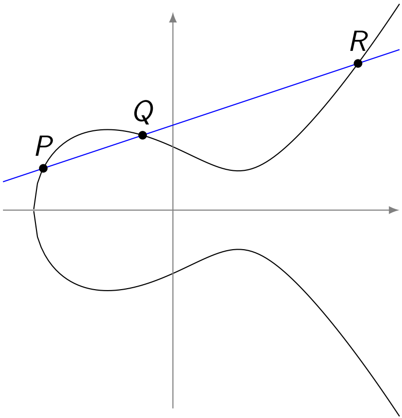
$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Elliptic curves

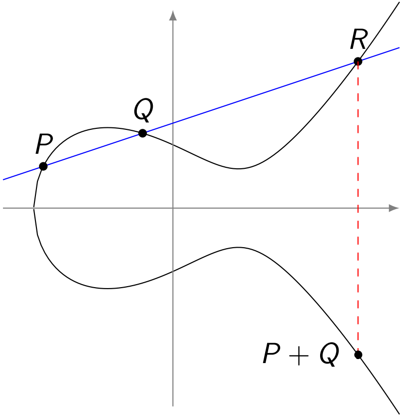


$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Elliptic curves



$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$



$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Let E be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$. Set

$$E(\mathbb{Q}) = \{(x, y) : x, y \in \mathbb{Q}, y^2 = x^3 + ax + b\}.$$

Elliptic curves

Let E be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$. Set

$$E(\mathbb{Q}) = \{(x, y) : x, y \in \mathbb{Q}, y^2 = x^3 + ax + b\}.$$

$E(\mathbb{Q})$ is a subgroup of E.

Elliptic curves

Let E be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$. Set

$$E(\mathbb{Q}) = \{(x, y) : x, y \in \mathbb{Q}, y^2 = x^3 + ax + b\}.$$

$E(\mathbb{Q})$ is a subgroup of E.

"Rational points on elliptic curves are the gems of arithmetic: they are, to diophantine geometry, what units in rings of integers are to algebraic number theory, what algebraic cycles are to algebraic geometry. Despite all that we know about these objects, the initial mystery and excitement that drew mathematicians to this arena in the first place remains in full force today."

Elliptic curves

Let E be an elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$. Set

$$E(\mathbb{Q}) = \{(x, y) : x, y \in \mathbb{Q}, y^2 = x^3 + ax + b\}.$$

$E(\mathbb{Q})$ is a subgroup of E.

"Rational points on elliptic curves are the gems of arithmetic: they are, to diophantine geometry, what units in rings of integers are to algebraic number theory, what algebraic cycles are to algebraic geometry. Despite all that we know about these objects, the initial mystery and excitement that drew mathematicians to this arena in the first place remains in full force today."

-B. Bektemirov, B. Mazur, W. Stein, M. Watkins, *Average ranks of elliptic curves: Tension between data and conjecture*, Bulletin of the American Mathematical Society, **44** (2007), 233-254.

Theorem (Mordell, 1922)

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

Elliptic curves

Theorem (Mordell, 1922)

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

Corollary

There exists a nonnegative integer r such that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}, \qquad |\mathbb{T}| < \infty.$$

Elliptic curves

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Elliptic curves

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

- r is the rank of E.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

- r is the rank of E.
- $\mathbb{T}$ is the torsion part of E.

Theorem (Mazur, 1978)

$\mathbb{T}$ is one of the following fifteen groups in the following list Φ:

$$\mathbb{Z}/n\mathbb{Z},\ 1 \le n \le 12,\ n \ne 11;$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ 1 \le n \le 4.$$

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

- r is the rank of E.
- $\mathbb{T}$ is the torsion part of E.

Theorem (Mazur, 1978)

$\mathbb{T}$ is one of the following fifteen groups in the following list Φ:

$$\mathbb{Z}/n\mathbb{Z},\ 1 \le n \le 12,\ n \ne 11;$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ 1 \le n \le 4.$$

In particular, $|\mathbb{T}| \le 16$.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Question. Given $\mathbb{T} \in \Phi$, what is the proportion of all elliptic curves whose torsion subgroup is $\mathbb{T}$ among all elliptic curves over $\mathbb{Q}$?

Recall:

- For relatively prime integers a and b, what is the proportion of primes of the form $an + b$ among all primes?

Recall:

- For relatively prime integers a and b, what is the proportion of primes of the form $an+b$ among all primes?

$$\lim_{X\to\infty}\frac{\#\{p:\ p \text{ is prime of the form } an+b\le X\}}{\pi(X)}=\frac{1}{\phi(a)}.$$

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Question. Given $\mathbb{T} \in \Phi$, what is the proportion of all elliptic curves whose torsion subgroup is $\mathbb{T}$ among all elliptic curves over $\mathbb{Q}$?

- Do such elliptic curves exist?

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Question. Given $\mathbb{T} \in \Phi$, what is the proportion of all elliptic curves whose torsion subgroup is $\mathbb{T}$ among all elliptic curves over $\mathbb{Q}$?

- Do such elliptic curves exist?
- Are there infinitely many such curves?

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Question. Given $\mathbb{T} \in \Phi$, what is the proportion of all elliptic curves whose torsion subgroup is $\mathbb{T}$ among all elliptic curves over $\mathbb{Q}$?

- Do such elliptic curves exist?
- Are there infinitely many such curves?
- Do we have explicit/parametrized description of these curves?

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Question. Given $\mathbb{T} \in \Phi$, what is the proportion of all elliptic curves whose torsion subgroup is $\mathbb{T}$ among all elliptic curves over $\mathbb{Q}$?

- Do such elliptic curves exist?
- Are there infinitely many such curves?
- Do we have explicit/parametrized description of these curves?
- **How can we define the "size" of an elliptic curve**?

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Question. Given $\mathbb{T} \in \Phi$, what is the proportion of all elliptic curves whose torsion subgroup is $\mathbb{T}$ among all elliptic curves over $\mathbb{Q}$?

- Do such elliptic curves exist?
- Are there infinitely many such curves?
- Do we have explicit/parametrized description of these curves?
- **How can we define the "size" of an elliptic curve**?
- How many curves are there up to a given "size"?

Elliptic curves

- Do such elliptic curves exist?
- Are there infinitely many such curves?
- Do we have explicit/parametrized description of these curves?

- Do such elliptic curves exist?
- Are there infinitely many such curves?
- Do we have explicit/parametrized description of these curves?

Yes,

Elliptic curves

- Do such elliptic curves exist?
- Are there infinitely many such curves?
- Do we have explicit/parametrized description of these curves?

  Yes, Yes,

- Do such elliptic curves exist?
- Are there infinitely many such curves?
- Do we have explicit/parametrized description of these curves?

Yes, Yes, and Yes.

- Do such elliptic curves exist?
- Are there infinitely many such curves?
- Do we have explicit/parametrized description of these curves?

  Yes, Yes, and Yes.

  For example, when $\mathbb{T} \cong \mathbb{Z}/7\mathbb{Z}$, then any elliptic curve with torsion $\mathbb{T}$ over $\mathbb{Q}$ lies in the family

$$\mathcal{E}_7 : y^2+(1-t(t-1))xy-t^2(t-1)y = x^3-t^2(t-1)x^2, \qquad t \in \mathbb{Q}.$$

- **How can we define the "size" of an elliptic curve**?

Elliptic Curves

- **How can we define the "size" of an elliptic curve**?
- Let $\mathcal{E}$ be the set

$$\{y^2 = x^3 + ax + b : \ a, b \in \mathbb{Z}, \, 4a^3 + 27b^2 \neq 0, \ d^4 \mid a, d^6 \mid b \implies d = \pm 1\}.$$

- **How can we define the "size" of an elliptic curve**?
- Let $\mathcal{E}$ be the set

$$\{y^2 = x^3 + ax + b : \; a, b \in \mathbb{Z}, \; 4a^3 + 27b^2 \neq 0, \; d^4 \mid a, d^6 \mid b \implies d = \pm 1\}.$$

- For any E in $\mathcal{E}$, we define the *h*eight of E to be

$$\mathrm{ht}(E) = \max\{4|a|^3, 27b^2\}.$$

Question. **Given $\mathbb{T} \in \Phi$, what is the proportion of all elliptic curves whose torsion subgroup is $\mathbb{T}$ among all elliptic curves over $\mathbb{Q}$?**

Question. Given $\mathbb{T} \in \Phi$, what is the proportion of all elliptic curves whose torsion subgroup is $\mathbb{T}$ among all elliptic curves over $\mathbb{Q}$?

Theorem (Harron-Snowden, 2017)

Let $\mathbb{T} \in \Phi$. Set $N_{\mathbb{T}}(X)$ to be the number of (isomorphism classes of) elliptic curves E over $\mathbb{Q}$ of height at most X for which $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{T}$. Then, there is an explicit constant $d(\mathbb{T})$ such that

$$\lim_{X\to\infty} \frac{\log N_{\mathbb{T}}(X)}{\log X} = \frac{1}{d(\mathbb{T})}.$$

$d(0) = 6/5$, $d(\mathbb{Z}/2\mathbb{Z}) = 2$, $d(\mathbb{Z}/3\mathbb{Z}) = 3$, $d(\mathbb{Z}/5\mathbb{Z}) = 6$, and $d(\mathbb{Z}/7\mathbb{Z}) = 12$.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

- What do we know about the rank r?

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

- What do we know about the rank r?
- r tells how big $E(\mathbb{Q})$ is.

Elliptic curves

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

- What do we know about the rank r?
- r tells how big $E(\mathbb{Q})$ is.
- But how big r can be?

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

- What do we know about the rank r?
- r tells how big $E(\mathbb{Q})$ is.
- But how big r can be?

Conjecture

r can be aribtrarily large

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

- What do we know about the rank r?
- r tells how big $E(\mathbb{Q})$ is.
- But how big r can be?

Conjecture

r can be aribtrarily large; or not.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Recall that

$$\mathcal{E} := \{y^2 = x^3 + ax + b : \ a, b \in \mathbb{Z},\ 4a^3 + 27b^2 \neq 0,\ d^4 \mid a, d^6 \mid b \implies d = \pm 1\}.$$

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Recall that

$$\mathcal{E} := \{y^2 = x^3 + ax + b : \ a, b \in \mathbb{Z},\ 4a^3 + 27b^2 \neq 0,\ d^4 \mid a, d^6 \mid b \implies d = \pm 1\}.$$

Set

$$\mathcal{E}(X) := \{E \in \mathcal{E} : \mathrm{ht}(E) \leq X\},$$

Conjecture (Minimalist Conjecture)

$$\lim_{X\to\infty} \frac{\# \sum_{E\in\mathcal{E}(X)} \mathrm{rank}(E(\mathbb{Q}))}{\#\mathcal{E}(X)} = \frac{1}{2}.$$

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}$$

Recall that

$$\mathcal{E} := \{y^2 = x^3 + ax + b : \ a, b \in \mathbb{Z},\ 4a^3 + 27b^2 \neq 0,\ d^4 \mid a, d^6 \mid b \implies d = \pm 1\}.$$

Set

$$\mathcal{E}(X) := \{E \in \mathcal{E} : \mathrm{ht}(E) \leq X\},$$

Theorem (Bhargava-Shankar, Skinner)

$$0.216 \leq \lim_{X\to\infty} \frac{\# \sum_{E\in\mathcal{E}(X)} \mathrm{rank}(\mathrm{E}(\mathbb{Q}))}{\#\mathcal{E}(X)} \leq 0.885.$$

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

Reduction of Elliptic curves

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

- The above Weierstrass equation is called p-minimal if $\nu_p(\Delta)$ is the smallest among all elliptic curves isomorphic to E.

Reduction of Elliptic curves

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

- The above Weierstrass equation is called p-minimal if $\nu_p(\Delta)$ is the smallest among all elliptic curves isomorphic to E.
- Every elliptic curve over $\mathbb{Q}$ has a globally minimal Weierstrass equation (p-minimal at every prime p).

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

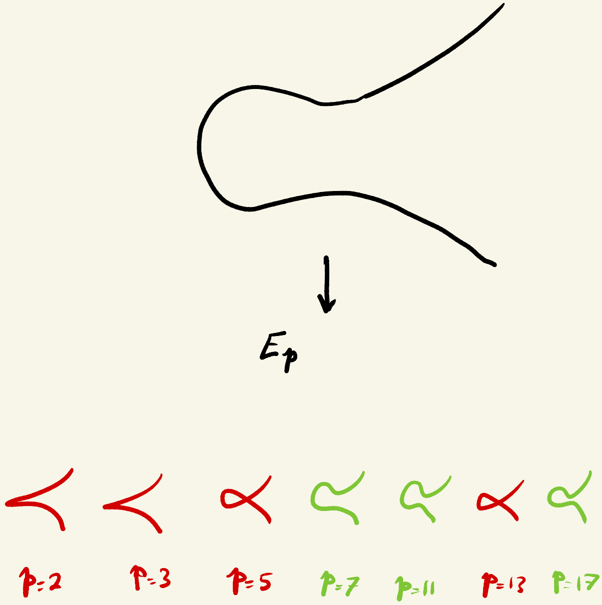
- The above Weierstrass equation is called p-minimal if $\nu_p(\Delta)$ is the smallest among all elliptic curves isomorphic to E.
- Every elliptic curve over $\mathbb{Q}$ has a globally minimal Weierstrass equation (p-minimal at every prime p).
- We set $E_p : y^2 = x^3 + a_p x + b_p$ where $a_p \equiv a \mod p$, $b_p \equiv b \mod p$.

Reduction of Elliptic curves

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

- The above Weierstrass equation is called p-minimal if $\nu_p(\Delta)$ is the smallest among all elliptic curves isomorphic to E.
- Every elliptic curve over $\mathbb{Q}$ has a globally minimal Weierstrass equation (p-minimal at every prime p).
- We set $E_p : y^2 = x^3 + a_p x + b_p$ where $a_p \equiv a \mod p$, $b_p \equiv b \mod p$.
- Is E_p still an elliptic curve over $\mathbb{F}_p$?

$$E: y^2 = x^3 + 432x + 21492$$



Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

- Is $E_p : y^2 = x^3 + a_p x + b_p$ still an elliptic curve over $\mathbb{F}_p$?

Reduction of Elliptic curves

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

- Is $E_p : y^2 = x^3 + a_p x + b_p$ still an elliptic curve over $\mathbb{F}_p$?
- E_p is an elliptic curve over $\mathbb{F}_p$ if $\nu_p(\Delta) = 0$, and E is said to have **good reduction** at p.

Reduction of Elliptic curves

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

- Is $E_p : y^2 = x^3 + a_p x + b_p$ still an elliptic curve over $\mathbb{F}_p$?
- E_p is an elliptic curve over $\mathbb{F}_p$ if $\nu_p(\Delta) = 0$, and E is said to have **good reduction** at p.
- E_p is a singular curve $\mathbb{F}_p$ if $\nu_p(\Delta) > 0$, and E is said to have **bad reduction** at p.

Reduction of Elliptic curves

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

- Is $E_p : y^2 = x^3 + a_p x + b_p$ still an elliptic curve over $\mathbb{F}_p$?
- E_p is an elliptic curve over $\mathbb{F}_p$ if $\nu_p(\Delta) = 0$, and E is said to have **good reduction** at p.
- E_p is a singular curve $\mathbb{F}_p$ if $\nu_p(\Delta) > 0$, and E is said to have **bad reduction** at p. If, moreover, $\nu_p(a) = 0$, then E is said to have **multiplicative reduction** at p

Reduction of Elliptic curves

Let $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, and $p \geq 5$ a prime.

- Is $E_p : y^2 = x^3 + a_p x + b_p$ still an elliptic curve over $\mathbb{F}_p$?
- E_p is an elliptic curve over $\mathbb{F}_p$ if $\nu_p(\Delta) = 0$, and E is said to have **good reduction** at p.
- E_p is a singular curve $\mathbb{F}_p$ if $\nu_p(\Delta) > 0$, and E is said to have **bad reduction** at p. If, moreover, $\nu_p(a) = 0$, then E is said to have **multiplicative reduction** at p; otherwise, E has **additive reduction** at p.

Elliptic Curves with a Prescribed Discriminant

- The minimal discriminant Δ_E of E carries information about the elliptic curve E, e.g., how many primes p are there such that E_p is not an elliptic curve over $\mathbb{F}_p$? how hard it is to get rid of the singularity of E_p?

Elliptic Curves with a Prescribed Discriminant

- The minimal discriminant Δ_E of E carries information about the elliptic curve E, e.g., how many primes p are there such that E_p is not an elliptic curve over $\mathbb{F}_p$? how hard it is to get rid of the singularity of E_p?
- **Question.** Given a nonzero integer D, how many elliptic curves E are there such that $\Delta_E = D$?

- The minimal discriminant Δ_E of E carries information about the elliptic curve E, e.g., how many primes p are there such that E_p is not an elliptic curve over $\mathbb{F}_p$? how hard it is to get rid of the singularity of E_p?
- **Question.** Given a nonzero integer D, how many elliptic curves E are there such that $\Delta_E = D$?
- There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is ± 1.

Elliptic Curves with a Prescribed Discriminant

- The minimal discriminant Δ_E of E carries information about the elliptic curve E, e.g., how many primes p are there such that E_p is not an elliptic curve over $\mathbb{F}_p$? how hard it is to get rid of the singularity of E_p?
- **Question.** Given a nonzero integer D, how many elliptic curves E are there such that $\Delta_E = D$?
- There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is ± 1.
- **Shafarevich's Theorem.** Up to isomorphisms over $\mathbb{Q}$, there are only finitely many elliptic curves E over $\mathbb{Q}$ such that $\Delta_E = D$.

Elliptic Curves with a Prescribed Discriminant

- The minimal discriminant Δ_E of E carries information about the elliptic curve E, e.g., how many primes p are there such that E_p is not an elliptic curve over $\mathbb{F}_p$? how hard it is to get rid of the singularity of E_p?
- **Question.** Given a nonzero integer D, how many elliptic curves E are there such that $\Delta_E = D$?
- There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is ± 1.
- **Shafarevich's Theorem.** Up to isomorphisms over $\mathbb{Q}$, there are only finitely many elliptic curves E over $\mathbb{Q}$ such that $\Delta_E = D$.
- How finite?

Elliptic Curves with a Prescribed Discriminant

- The minimal discriminant Δ_E of E carries information about the elliptic curve E, e.g., how many primes p are there such that E_p is not an elliptic curve over $\mathbb{F}_p$? how hard it is to get rid of the singularity of E_p?
- **Question.** Given a nonzero integer D, how many elliptic curves E are there such that $\Delta_E = D$?
- There is no elliptic curve over $\mathbb{Q}$ whose minimal discriminant is ± 1.
- **Shafarevich's Theorem.** Up to isomorphisms over $\mathbb{Q}$, there are only finitely many elliptic curves E over $\mathbb{Q}$ such that $\Delta_E = D$.
- How finite? Is there a way we can list all such isomorphism classes of elliptic curves?

Given a specified number field K and a finite set of primes S, there is an algorithm that gives a complete set of elliptic curves over K with good reduction outside S, Cremona-Lingham.

Given a specified number field K and a finite set of primes S, there is an algorithm that gives a complete set of elliptic curves over K with good reduction outside S, Cremona-Lingham.

Example. If $K = \mathbb{Q}$ and $S = \{2, 3\}$, then there are 6120 elliptic curves over $\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, with discriminant $2^a \times 3^b$ ($a \leq 8, b \leq 5$.)

Given a specified number field K and a finite set of primes S, there is an algorithm that gives a complete set of elliptic curves over K with good reduction outside S, Cremona-Lingham.

Example. If $K = \mathbb{Q}$ and $S = \{2, 3\}$, then there are 6120 elliptic curves over $\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, with discriminant $2^a \times 3^b$ ($a \leq 8, b \leq 5$.) This list was given earlier by Ogg and Hadano.

Elliptic Curves with a Prescribed Discriminant

- **Question.** Can we list all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a prime power, p^α, $\alpha \geq 1$?

- **Question.** Can we list all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a prime power, p^α, $\alpha \geq 1$?
- **Answer.** Either $|\Delta_E| = p$ or p^2,or else $p = 11$ and $\Delta_E = 11^5$, or $p = 17$ and $\Delta_E = 17^4$, or $p = 19$ and $\Delta_E = 19^3$, or $p = 37$ and $\Delta_E = 37^3$ (Serre, Mestre, Frey, Mazur, Oesterlé, Edixhoven, De Groot, J. Top).

Elliptic Curves with a Prescribed Discriminant

- **Question.** Can we list all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a prime power, p^α, $\alpha \geq 1$?
- **Answer.** Either $|\Delta_E| = p$ or p^2,or else $p = 11$ and $\Delta_E = 11^5$, or $p = 17$ and $\Delta_E = 17^4$, or $p = 19$ and $\Delta_E = 19^3$, or $p = 37$ and $\Delta_E = 37^3$ (Serre, Mestre, Frey, Mazur, Oesterlé, Edixhoven, De Groot, J. Top).

  It is conjectured that there are infinitely many elliptic curves with prime discriminant!

Elliptic Curves with a Prescribed Discriminant

- **Question.** Can we list all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a prime power, p^α, $\alpha \geq 1$?
- **Answer.** Either $|\Delta_E| = p$ or p^2,or else $p = 11$ and $\Delta_E = 11^5$, or $p = 17$ and $\Delta_E = 17^4$, or $p = 19$ and $\Delta_E = 19^3$, or $p = 37$ and $\Delta_E = 37^3$ (Serre, Mestre, Frey, Mazur, Oesterlé, Edixhoven, De Groot, J. Top).

  It is conjectured that there are infinitely many elliptic curves with prime discriminant!
- Can we classify all elliptic curves over $\mathbb{Q}$ whose minimal discriminant is a product of two prime powers?

History:

- The list of all elliptic curves with 2-torsion and with minimal discriminant $2^k p^m$ was given by Ogg, Hadano, and Ivorra.

History:

- The list of all elliptic curves with 2-torsion and with minimal discriminant $2^k p^m$ was given by Ogg, Hadano, and Ivorra.
- The list of elliptic curves with n-torsion, $n \geq 4$, and with minimal discriminant $p^m q^n$, where p and q are distinct primes was given by Bennett-Vatsal-Yazdani, Sadek, Dąbrowski-Jędrzejak.

History:

- The list of all elliptic curves with 2-torsion and with minimal discriminant $2^k p^m$ was given by Ogg, Hadano, and Ivorra.
- The list of elliptic curves with n-torsion, $n \geq 4$, and with minimal discriminant $p^m q^n$, where p and q are distinct primes was given by Bennett-Vatsal-Yazdani, Sadek, Dąbrowski-Jędrzejak.
- **Open Question:** Classify elliptic curves over $\mathbb{Q}$ with trivial rational torsion and good reduction outside the set $\{p, q\}$, with p and q different primes.

Why is the question hard?

Why is the question hard?

- Let E be an elliptic curve over $\mathbb{Q}$. A globally minimal Weierstrass equation describing E is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Z}.$$

Define

Why is the question hard?

- Let E be an elliptic curve over $\mathbb{Q}$. A globally minimal Weierstrass equation describing E is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Z}.$$

Define

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
\Delta_E &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.
\end{aligned}$$

Why is the question hard?

- Let E be an elliptic curve over $\mathbb{Q}$. A globally minimal Weierstrass equation describing E is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Z}.$$

Define

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ \Delta_E &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

- **The Question:** Solve the Diophantine equation

$$-b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = p^\alpha q^\beta$$

in $a_1, a_2, a_3, a_4, a_6, p, q, \alpha, \beta$.

Elliptic Curves with a Prescribed Discriminant

Question. Classify elliptic curves over $\mathbb{Q}$ with a torsion point of order $m \geq 4$ and good reduction outside the set $\{p, q\}$, with p and q different primes.

Theorem (Sadek, 2014)

Let E be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})[6] \neq 0$ and $\Delta_E = \pm p^{\alpha} q^{\beta}$ for distinct prime p and q. It follows that Δ_E is given as follows:

2×7^2, $-2^2 \times 7$, $2^3 \times 7^6$, $2^4 \times 5$, $-2^4 \times 3^3$, $2^6 \times 17$, $-2^6 \times 7^3$, $2^8 \times 3^3$, $-2^8 \times 5^2$.

Question. Classify elliptic curves over $\mathbb{Q}$ with a torsion point of order $m \geq 4$ and good reduction outside the set $\{p, q\}$, with p and q different primes.

Theorem (Sadek, 2014)

Let E be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})[6] \neq 0$ and $\Delta_E = \pm p^\alpha q^\beta$ for distinct prime p and q. It follows that Δ_E is given as follows:

2×7^2, $-2^2\times 7$, $2^3\times 7^6$, $2^4\times 5$, $-2^4\times 3^3$, $2^6\times 17$, $-2^6\times 7^3$, $2^8\times 3^3$, $-2^8\times 5^2$.

- Similar lists when $E(\mathbb{Q})[m] \neq \{0\}$, $m \geq 4$.

Elliptic Curves with a Prescribed Discriminant

Question. Classify elliptic curves over $\mathbb{Q}$ with a torsion point of order $m \geq 4$ and good reduction outside the set $\{p, q\}$, with p and q different primes.

Theorem (Sadek, 2014)

Let E be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})[6] \neq 0$ and $\Delta_E = \pm p^\alpha q^\beta$ for distinct prime p and q. It follows that Δ_E is given as follows:

2×7^2, $-2^2 \times 7$, $2^3 \times 7^6$, $2^4 \times 5$, $-2^4 \times 3^3$, $2^6 \times 17$, $-2^6 \times 7^3$, $2^8 \times 3^3$, $-2^8 \times 5^2$.

- Similar lists when $E(\mathbb{Q})[m] \neq \{0\}$, $m \geq 4$.
- For example: There exists no elliptic curve E over $\mathbb{Q}$ with $E(\mathbb{Q})[10] \neq \{0\}$ and $|\Delta_E| = p^\alpha q^\beta$, where $p \neq q$ are primes, and $\alpha, \beta > 0$.

Elliptic Curves with a Prescribed Discriminant

What is the proportion of elliptic curves whose discriminant/conductor is ...?

What is the proportion of elliptic curves whose discriminant/conductor is ...?

Theorem (Cremona-Sadek, 2023)

- *The density of semistable elliptic curves over $\mathbb{Q}$ is*

$$\zeta(10)/\zeta(2) \approx 60.85\%.$$

What is the proportion of elliptic curves whose discriminant/conductor is ...?

Theorem (Cremona-Sadek, 2023)

- *The density of semistable elliptic curves over* $\mathbb{Q}$ *is*

$$\zeta(10)/\zeta(2) \approx 60.85\%.$$

- *The density of elliptic curves over* $\mathbb{Q}$ *whose minimal discriminant is square-free is*

$$\zeta(10)\prod_{p}\left(1-\frac{2}{p^2}+\frac{1}{p^3}\right) \approx 42.93\%.$$

Order of Reductions of Elliptic Curves

Recall that $E : y^2 = x^3 + ax^2 + b$, $a, b \in \mathbb{Z}$,
$\Delta_E := -4a^3 - 27b^2 \neq 0$.

Order of Reductions of Elliptic Curves

Recall that $E : y^2 = x^3 + ax^2 + b$, $a, b \in \mathbb{Z}$, $\Delta_E := -4a^3 - 27b^2 \neq 0$. Also recall that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}.$$

Recall that $E : y^2 = x^3 + ax^2 + b$, $a, b \in \mathbb{Z}$, $\Delta_E := -4a^3 - 27b^2 \neq 0$. Also recall that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}.$$

We defined $E_p : y^2 = x^3 + a_p x + b_p$ where $a_p \equiv a \mod p$, $b_p \equiv b \mod p$.

Facts:

Recall that $E: y^2 = x^3 + ax^2 + b$, $a, b \in \mathbb{Z}$, $\Delta_E := -4a^3 - 27b^2 \neq 0$. Also recall that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}.$$

We defined $E_p : y^2 = x^3 + a_p x + b_p$ where $a_p \equiv a \bmod p$, $b_p \equiv b \bmod p$.

Facts:

- $\mathbb{T} \hookrightarrow E_p(\mathbb{F}_p)$ for every $p \nmid \Delta_E$

Order of Reductions of Elliptic Curves

Recall that $E : y^2 = x^3 + ax^2 + b$, $a, b \in \mathbb{Z}$, $\Delta_E := -4a^3 - 27b^2 \neq 0$. Also recall that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}.$$

We defined $E_p : y^2 = x^3 + a_p x + b_p$ where $a_p \equiv a \bmod p$, $b_p \equiv b \bmod p$.

Facts:

- $\mathbb{T} \hookrightarrow E_p(\mathbb{F}_p)$ for every $p \nmid \Delta_E$
- $\#\mathbb{T} \mid \#E_p(\mathbb{F}_p)$ for every $p \nmid \Delta_E$

Order of Reductions of Elliptic Curves

Recall that $E: y^2 = x^3 + ax^2 + b$, $a, b \in \mathbb{Z}$, $\Delta_E := -4a^3 - 27b^2 \neq 0$. Also recall that

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times \mathbb{T}.$$

We defined $E_p : y^2 = x^3 + a_p x + b_p$ where $a_p \equiv a \bmod p$, $b_p \equiv b \bmod p$.

Facts:

- $\mathbb{T} \hookrightarrow E_p(\mathbb{F}_p)$ for every $p \nmid \Delta_E$
- $\#\mathbb{T} \mid \#E_p(\mathbb{F}_p)$ for every $p \nmid \Delta_E$
- Mazur: $\#\mathbb{T} \in \{1, 2, \cdots, 10, 12, 16\}$

Order of Reductions of Elliptic Curves

Theorem (Serre-Katz)

Let $m \geq 2$ be an integer. Let E be an elliptic curve defined over K. The following statements are equivalent:

a) $\#E_p(\mathbb{F}_p) \equiv 0 \mod m$ *for a set of primes p of density 1 in $\mathbb{Q}$.*

b) *There exists an elliptic curve E' over $\mathbb{Q}$ such that:*

   i) *E is $\mathbb{Q}$-isogenous to E'; and*

   ii) $\#\mathbb{T}_{E'} \equiv 0 \mod m$.

Order of Reductions of Elliptic Curves

Theorem (Serre-Katz)

Let $m \geq 2$ be an integer. Let E be an elliptic curve defined over K. The following statements are equivalent:

a) $\#E_p(\mathbb{F}_p) \equiv 0 \mod m$ *for a set of primes p of density 1 in $\mathbb{Q}$.*

b) *There exists an elliptic curve E' over $\mathbb{Q}$ such that:*
   i) *E is $\mathbb{Q}$-isogenous to E'; and*
   ii) $\#\mathbb{T}_{E'} \equiv 0 \mod m$.

In particular, $m \in \{1, 2, \cdots, 10, 12, 16\}$.

Recall.

Recall.

- What is the density of primes of the form $p \equiv \alpha \mod m$, $\gcd(m, \alpha) = 1$, among all primes?

Recall.

- What is the density of primes of the form $p \equiv \alpha \mod m$, $\gcd(m, \alpha) = 1$, among all primes?
- Dirichlet proved that the density is $1/\phi(m)$, where ϕ is the Euler's totient function.

Let E be an elliptic curve defined over $\mathbb{Q}$; and $m \geq 2$ be such that $m \nmid \#\mathbb{T}_{E'}$ for any $E' \sim_{\mathbb{Q}} E$.

Order of Reductions of Elliptic Curves

Let E be an elliptic curve defined over $\mathbb{Q}$; and $m \geq 2$ be such that $m \nmid \#\mathbb{T}_{E'}$ for any $E' \sim_{\mathbb{Q}} E$.

Question: For each α mod m, what is the density of primes p such that $\#E_p(\mathbb{F}_p) \equiv \alpha$ mod m?

Example. (Pajaziti-Sadek, 2022)

Example. (Pajaziti-Sadek, 2022)

$$E_t : y^2 = g_t(x) := x^3 - 7t\ x^2 + 96t^2\ x + 256\ t^3.$$

Example. (Pajaziti-Sadek, 2022)

$$E_t : y^2 = g_t(x) := x^3 - 7t\ x^2 + 96t^2\ x + 256\ t^3.$$

- For any $t \in \mathbb{Z} \setminus \mathbb{Z}^2$ and any prime $p \nmid \Delta_{E_t}$, if $\left(\frac{t}{p}\right) = 1$, then $\#E_{t,p}(\mathbb{F}_p) \equiv 0 \mod 5$;

Example. (Pajaziti-Sadek, 2022)

$$E_t : y^2 = g_t(x) := x^3 - 7t\ x^2 + 96t^2\ x + 256\ t^3.$$

- For any $t \in \mathbb{Z} \setminus \mathbb{Z}^2$ and any prime $p \nmid \Delta_{E_t}$, if $\left(\frac{t}{p}\right) = 1$, then $\#E_{t,p}(\mathbb{F}_p) \equiv 0 \mod 5$;
- there are infinitely many rational values of t such that $\#E_{t,p}(\mathbb{F}_p) \equiv 0 \mod 10$ for a set S of primes p of density at least $1/6$; and

Example. (Pajaziti-Sadek, 2022)

$$E_t : y^2 = g_t(x) := x^3 - 7t\ x^2 + 96t^2\ x + 256\ t^3.$$

- For any $t \in \mathbb{Z} \setminus \mathbb{Z}^2$ and any prime $p \nmid \Delta_{E_t}$, if $\left(\frac{t}{p}\right) = 1$, then $\#E_{t,p}(\mathbb{F}_p) \equiv 0 \mod 5$;
- there are infinitely many rational values of t such that $\#E_{t,p}(\mathbb{F}_p) \equiv 0 \mod 10$ for a set S of primes p of density at least $1/6$; and $\#E_{t,p}(\mathbb{F}_p) \equiv 0 \mod 20$ for a positive proportion of the primes in S.

Order of Reductions of Elliptic Curves

Theorem (Sun, 2006, Kim-Koo-Park, 2008)

Let $E : y^2 = x^3 - 12x - 11$ *be an elliptic curve defined over* $\mathbb{Q}$*. Then*

$$\#E_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \text{if } p \equiv 1, 9, 11, 13, 17, 19 \mod 20 \\ 6 \mod 12 & \text{if } p \equiv 3, 7 \mod 20. \end{cases}$$

In particular, $\#E_p(\mathbb{F}_p) \equiv 0 \mod 12$ *for primes of density* $3/4$*, whereas* $\#E_p(\mathbb{F}_p) \equiv 6 \mod 12$ *for primes of density* $1/4$*.*

Order of Reductions of Elliptic Curves

Theorem (Sun, 2006, Kim-Koo-Park, 2008)

Let $E : y^2 = x^3 - 12x - 11$ *be an elliptic curve defined over* $\mathbb{Q}$*. Then*

$$\#E_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \text{if } p \equiv 1, 9, 11, 13, 17, 19 \mod 20 \\ 6 \mod 12 & \text{if } p \equiv 3, 7 \mod 20. \end{cases}$$

In particular, $\#E_p(\mathbb{F}_p) \equiv 0 \mod 12$ *for primes of density* $3/4$*, whereas* $\#E_p(\mathbb{F}_p) \equiv 6 \mod 12$ *for primes of density* $1/4$*.*

Remark. E is $\mathbb{Q}$-isogenous to $E' : y^2 = x^3 - 372x + 2761$ where $E'(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$.

Order of Reductions of Elliptic Curves

Theorem (Sun, 2006, Kim-Koo-Park, 2008)

Let $E : y^2 = x^3 - 12x - 11$ be an elliptic curve defined over $\mathbb{Q}$. Then

$$\#E_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \textit{if } p \equiv 1, 9, 11, 13, 17, 19 \mod 20 \\ 6 \mod 12 & \textit{if } p \equiv 3, 7 \mod 20. \end{cases}$$

In particular, $\#E_p(\mathbb{F}_p) \equiv 0 \mod 12$ for primes of density $3/4$, whereas $\#E_p(\mathbb{F}_p) \equiv 6 \mod 12$ for primes of density $1/4$.

Remark. E is $\mathbb{Q}$-isogenous to $E' : y^2 = x^3 - 372x + 2761$ where $E'(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$.
Another Remark. $E'(\mathbb{Q}(\sqrt{5})) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$.

Order of Reductions of Elliptic Curves

Theorem (Pajaziti-Sadek, 2022)

Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square free integer. Let E be an elliptic curve defined over $\mathbb{Q}$ such that E is $\mathbb{Q}$-isogenous to an elliptic curve E' with $E'(\mathbb{Q})_{\text{tors}} \subsetneq E'(K)_{\text{tors}}$. Assume moreover that ℓ is an odd integer such that $\#E'(K)_{\text{tors}} \equiv 0 \mod \ell$ and $\gcd(\#E''(\mathbb{Q})_{\text{tors}}, \ell) = 1$ for any $\mathbb{Q}$-isogenous elliptic curve E'' to E. If $p \nmid 2d\#E'(K)_{\text{tors}}$ is a prime of good reduction of E, then

$$\#E_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod \ell & \text{if } \left(\frac{d}{p}\right) = 1 \\ 2p+2 \mod \ell & \text{if } \left(\frac{d}{p}\right) = -1. \end{cases}$$

In particular, the density of primes p such that $\#E_p(\mathbb{F}_p) \equiv 0 \mod \ell$ is at least $1/2$.

- $E : y^2 + xy + y = x^3 - x^2 + 47245x - 2990253$ over $\mathbb{Q}$

Order of Reductions of Elliptic Curves

- $E : y^2 + xy + y = x^3 - x^2 + 47245x - 2990253$ over $\mathbb{Q}$
- $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$

Order of Reductions of Elliptic Curves

- $E : y^2 + xy + y = x^3 - x^2 + 47245x - 2990253$ over $\mathbb{Q}$
- $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$
- $E(\mathbb{Q}(\sqrt{-15}))_{\text{tors}} \simeq \mathbb{Z}/16\mathbb{Z}$

Order of Reductions of Elliptic Curves

- $E : y^2 + xy + y = x^3 - x^2 + 47245x - 2990253$ over $\mathbb{Q}$
- $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$
- $E(\mathbb{Q}(\sqrt{-15}))_{\text{tors}} \simeq \mathbb{Z}/16\mathbb{Z}$
- if $p \equiv 7, 11, 13, 14 \mod 15$, or equivalently $\left(\frac{-15}{p}\right) = -1$, then $\#E_p(\mathbb{F}_p) \equiv 0, 2, 4, 6 \mod 8$

Order of Reductions of Elliptic Curves

- $E : y^2 + xy + y = x^3 - x^2 + 47245x - 2990253$ over $\mathbb{Q}$
- $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$
- $E(\mathbb{Q}(\sqrt{-15}))_{\text{tors}} \simeq \mathbb{Z}/16\mathbb{Z}$
- if $p \equiv 7, 11, 13, 14 \mod 15$, or equivalently $\left(\frac{-15}{p}\right) = -1$, then $\#E_p(\mathbb{F}_p) \equiv 0, 2, 4, 6 \mod 8$
- however, E is $\mathbb{Q}$-isogenous to $y^2 + xy + y = x^3 - x^2 - 240755x - 26606253$ whose torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$,

Order of Reductions of Elliptic Curves

- $E : y^2 + xy + y = x^3 - x^2 + 47245x - 2990253$ over $\mathbb{Q}$
- $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$
- $E(\mathbb{Q}(\sqrt{-15}))_{\text{tors}} \simeq \mathbb{Z}/16\mathbb{Z}$
- if $p \equiv 7, 11, 13, 14 \mod 15$, or equivalently $\left(\frac{-15}{p}\right) = -1$, then $\#E_p(\mathbb{F}_p) \equiv 0, 2, 4, 6 \mod 8$
- however, E is $\mathbb{Q}$-isogenous to $y^2 + xy + y = x^3 - x^2 - 240755x - 26606253$ whose torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so $\#E_p(\mathbb{F}_p) \equiv 0 \mod 4$ for any prime p of good reduction of E

Order of Reductions of Elliptic Curves

- $E : y^2 + xy + y = x^3 - x^2 + 47245x - 2990253$ over $\mathbb{Q}$
- $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$
- $E(\mathbb{Q}(\sqrt{-15}))_{\text{tors}} \simeq \mathbb{Z}/16\mathbb{Z}$
- if $p \equiv 7, 11, 13, 14 \mod 15$, or equivalently $\left(\frac{-15}{p}\right) = -1$, then $\#E_p(\mathbb{F}_p) \equiv 0, 2, 4, 6 \mod 8$
- however, E is $\mathbb{Q}$-isogenous to $y^2 + xy + y = x^3 - x^2 - 240755x - 26606253$ whose torsion subgroup is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so $\#E_p(\mathbb{F}_p) \equiv 0 \mod 4$ for any prime p of good reduction of E

$$\#E_p(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 16 & \text{if } p \equiv 1, 2, 4, 8 \mod 15 \\ 0, 4, 8, 12 \mod 16 & \text{if } p \equiv 7, 11, 13, 14 \mod 15. \end{cases}$$

Bibliography

- J. Cremona and M. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Exp. Math. **16** (2007), 303–312.
- J. Cremona and M. Sadek, *Local and Global Densities for Weierstrass Models of Elliptic Curves*, Mathematical Research Letters, **30** (2023), 413–461.
- T. Ekedahl, *An Infinite Version of the Chinese Remainder Theorem*, Comment. Math. Univ. St. Paul. **40** (1991), no. 1, 53–59.
- A. Pajaziti and M. Sadek, *On congruence classes of orders of reductions of elliptic curves*, preprint.
- B. Poonen and M. Stoll, *A local-global principle for densities*, Topics in number theory (University Park, PA, 1997), Math. Appl., vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 241–244.
- M. Sadek, *On elliptic curves whose conductor is a product of two prime powers*, Math. Comput. **83** (2014), 447–460.

Thank you!