Some Problems on the Arithmetic of Elliptic Curves

J. Jiménez Urroz, UPC

Kolkata, February, 2017

1800 BCE

The first historical find of an arithmetical nature is a fragment of a table: the broken clay tablet Plimpton 322 (Larsa, Mesopotamia, ca. 1800 BCE) contains a list of "Pythagorean triples", i.e., integers a, b, c such that

$$a^2 + b^2 = c^2$$

Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

$$\frac{x}{6}$$

Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

$$\frac{x}{6} + \frac{x}{12}$$

Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7}$$

Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5$$

Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2}$$

Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4$$

Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x$$

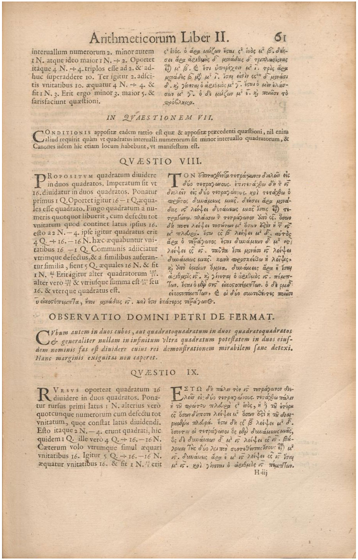
Diophanti Alexandrini, (Third century)

'Here lies Diophantus,' the wonder behold. Through art algebraic, the stone tells how old: 'God gave him his boyhood one-sixth of his life. One twelfth more as youth while whiskers grew rife; And then yet one-seventh ere marriage begun; In five years there came a bouncing new son. Alas, the dear child of master and sage. After attaining half the measure of his father's life chill fate took him. After consoling his fate by the science of numbers for four years, he ended his life.'

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x$$

$x = 84$... can you do it faster?

Arithmeticorum, 1621, 1670, Diophanti Alexandrini



Arithmeticorum Liber II. 61

interuallum numerorum 2. minor autem 1 N. atque ideo maior 1 N. + 2. Oportet itaque 4 N. + 4. triplos esse ad 2. & adhuc superaddere 10. Ter igitur 2. adscitis vnitatibus 10. æquatur 4 N. + 4. & fit 1 N. 3. Erit ergo minor 3. maior 5. & satisfaciunt quæstioni.

IN QVAESTIONEM VII.

CONDITIONIS appositæ eadem ratio est quæ & appositæ præcedenti quæstioni, nil enim aliud requirit quàm vt quadratus interualli numerorum sit minor interuallo quadratorum, & Canones iidem hic etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quod continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{16}{5}$ Erit igitur alter quadratorum $\frac{256}{25}$. alter verò $\frac{144}{25}$ & vtriusque summa est $\frac{400}{25}$ seu 16. & vterque quadratus est.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{16}{5}$ erit

H iij

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum poteſtatem in duos eiuſdem nominis fas eſt diuidere cuius rei demonſtrationem mirabilem ſane detexi. Hanc marginis exiguitas non caperet.

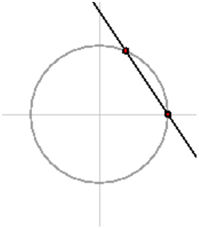
Find the integral solutions of $x^2 + y^2 = z^2$

Find the integral solutions of $x^2 + y^2 = z^2$

Find the rationals solutions of $x^2 + y^2 = 1$

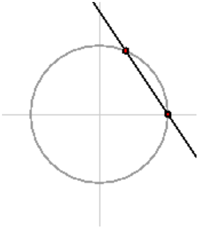
Find the integral solutions of $x^2 + y^2 = z^2$

Find the rationals solutions of $x^2 + y^2 = 1$



Find the integral solutions of $x^2 + y^2 = z^2$

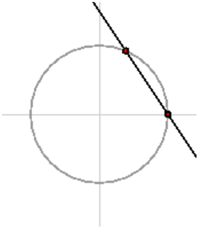
Find the rationals solutions of $x^2 + y^2 = 1$



$$y = t(x - 1)$$

Find the integral solutions of $x^2 + y^2 = z^2$

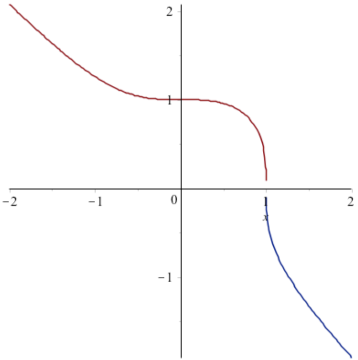
Find the rationals solutions of $x^2 + y^2 = 1$



$y = t(x-1)$, then $x = \frac{t^2-1}{t^2+1}$ $\quad y = \frac{2t}{t^2+1}$

Find the integral solutions to $x^3 + y^3 = z^3$, Find the integral solutions to $x^3 + y^3 = z^3$, is like finding rational solutions of $\quad x^3 + y^3 = 1$

Find the integral solutions to $x^3 + y^3 = z^3$, is like finding rational solutions of $\quad x^3 + y^3 = 1$



We parametrize by $y = t(x-1)$, to get

$$(t^3+1)x^2 + (1-2t^3)x + (1+t^3) = 0$$

Changing variables $x = u + t$, $y = u - t$, we get

$$2u^3 + 6ut^2 = 1$$

Changing variables $x = u + t$, $y = u - t$, we get

$$2u^3 + 6ut^2 = 1$$

Multiplying by $(6/u)^3$, and letting $6/u = X, 36t/u = Y$, we get

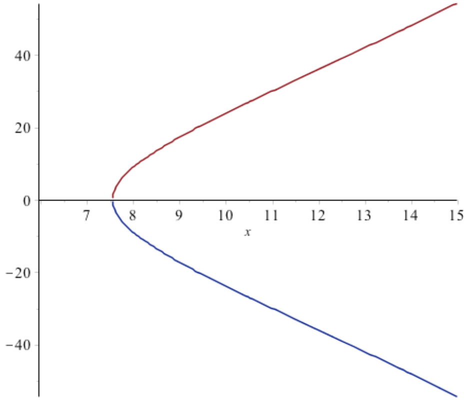
$$Y^2 = X^3 - 432.$$

Changing variables $x = u + t$, $y = u - t$, we get

$$2u^3 + 6ut^2 = 1$$

Multiplying by $(6/u)^3$, and letting $6/u = X, 36t/u = Y$, we get

$$Y^2 = X^3 - 432.$$



Every cubic can be written as $y^2 = x^3 + ax + b$,

Every cubic can be written as $y^2 = x^3 + ax + b$,

Definition

Given a field K. An elliptic curve over K is the set

$$E/K := \left\{(x, y) \in K \times K \;:\; y^2 = x^3 + ax + b, a, b \in K\right\} \cup \{O\}$$

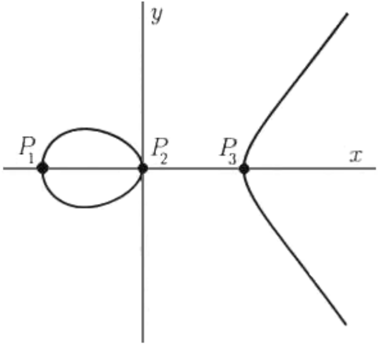
$4a^3 + 27b^2 \neq 0$.

Every cubic can be written as $y^2 = x^3 + ax + b$,

Definition

Given a field K. An elliptic curve over K is the set

$$E/K := \left\{(x, y) \in K \times K \,:\, y^2 = x^3 + ax + b, a, b \in K\right\} \cup \{O\}$$
$$4a^3 + 27b^2 \neq 0.$$



Key point on the theory of elliptic curves:

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

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

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q})$$

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

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

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q})$$

Group law:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \left(\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}\right)$$

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

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

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q})$$

Group law:
$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$
$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \left(\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}\right)$$

Theorem

(Mazur, 1978) If C_n denotes the cyclic group of order n, then the groups that appear as $E_{tors}(\mathbb{Q})$ are C_n with $1 \leq n \leq 10$, C_{12} and $C_2 \times C_2$, $C_2 \times C_4$, $C_2 \times C_6$, and $C_2 \times C_8$.

Key point on the theory of elliptic curves:

$$3 = 2 + 1$$

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

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E_{\text{tors}}(\mathbb{Q})$$

Group law:
$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$
$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \left(\frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}\right)$$

Theorem

(Mazur, 1978) If C_n denotes the cyclic group of order n, then the groups that appear as $E_{tors}(\mathbb{Q})$ are C_n with $1 \leq n \leq 10$, C_{12} and $C_2 \times C_2$, $C_2 \times C_4$, $C_2 \times C_6$, and $C_2 \times C_8$.

The rank, r, is highly unknown.

Very nice. But what do we do now? Can we find points?

Very nice. But what do we do now? Can we find points?

On the elliptic curve $y^2 = x^3 + 877x$, the smallest non trivial point is

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}$$

Very nice. But what do we do now? Can we find points?

On the elliptic curve $y^2 = x^3 + 877x$, the smallest non trivial point is

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}$$

Try to generalize Hasse's principle: Every quadratic form has integer solutions, if and only if has solutions in every completion of $\mathbb{Q}$

Very nice. But what do we do now? Can we find points?

On the elliptic curve $y^2 = x^3 + 877x$, the smallest non trivial point is

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}$$

Try to generalize Hasse's principle: Every quadratic form has integer solutions, if and only if has solutions in every completion of $\mathbb{Q}$

Corollary

$x^2 + 2y^2 = 5z^2$ has no non-trivial integer solutions.

Very nice. But what do we do now? Can we find points?

On the elliptic curve $y^2 = x^3 + 877x$, the smallest non trivial point is

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}$$

Try to generalize Hasse's principle: Every quadratic form has integer solutions, if and only if has solutions in every completion of $\mathbb{Q}$

Corollary

$x^2 + 2y^2 = 5z^2$ has no non-trivial integer solutions.

Unfortunately Hasse's principle does not hold on cubics, as shown by Selmer's example (1957), $3x^3 + 4y^3 + 5z^3 = 0$.

The idea is to wrap all the local information together in one object which contains all the arithmetic information of the elliptic curve.

The idea is to wrap all the local information together in one object which contains all the arithmetic information of the elliptic curve.

$$L(E,s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

where, for p, *prime*, $a_p = p + 1 - |E(\mathbb{F}_p)|$ and for general n we have

The idea is to wrap all the local information together in one object which contains all the arithmetic information of the elliptic curve.

$$L(E,s)=\sum_{n\geq 1}\frac{a_n}{n^s},$$

where, for p, *prime*, $a_p = p+1-|E(\mathbb{F}_p)|$ and for general n we have

$$L(E,s)=\prod_{p|\Delta}\frac{1}{1-a_p p^s}\prod_{p\nmid\Delta,prime}\frac{1}{1-a_p p^s+p^{1-2s}}$$

The idea is to wrap all the local information together in one object which contains all the arithmetic information of the elliptic curve.

$$L(E,s)=\sum_{n\geq 1}\frac{a_n}{n^s},$$

where, for p, *prime*, $a_p = p+1-|E(\mathbb{F}_p)|$ and for general n we have

$$L(E,s)=\prod_{p|\Delta}\frac{1}{1-a_p p^s}\prod_{p\nmid\Delta, prime}\frac{1}{1-a_p p^s+p^{1-2s}}$$

Conjecture:(Birch-Swinnerton Dyer) The order of vanishing at $s=1$ is $r=$rank$(E(\mathbb{Q}))$.

The idea is to wrap all the local information together in one object which contains all the arithmetic information of the elliptic curve.

$$L(E,s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

where, for p, *prime*, $a_p = p + 1 - |E(\mathbb{F}_p)|$ and for general n we have

$$L(E,s) = \prod_{p|\Delta} \frac{1}{1 - a_p p^s} \prod_{p \nmid \Delta, prime} \frac{1}{1 - a_p p^s + p^{1-2s}}$$

Conjecture:(Birch-Swinnerton Dyer) The order of vanishing at $s = 1$ is $r =$rank$(E(\mathbb{Q}))$.

This is like a generalization of the prime number theorem. $\zeta(s) = \sum \frac{1}{n^s} = \prod_p (1 - p^{-s})^{-1}$

Theorem (Hasse, 1930)

$|a_p| \leq 2\sqrt{p}.$

Theorem (Hasse, 1930)

$|a_p| \leq 2\sqrt{p}$.

Example Consider the curve $y^2 = x^3 - 1$ and $q \equiv 2 \pmod 3$. Then, $E(\mathbb{F}_q) = q + 1$.

Theorem (Hasse, 1930)

$|a_p| \leq 2\sqrt{p}$.

Example Consider the curve $y^2 = x^3 - 1$ and $q \equiv 2 \pmod 3$.
Then, $E(\mathbb{F}_q) = q + 1$.
Consider the endomorphism $\sigma : E_p \to E_p$ given by
$\sigma(x, y) = (x^p, y^p)$. Then $|E(\mathbb{F}_p)| = |\ker(1 - \sigma)| = \deg(1 - \sigma)$.

Theorem (Hasse, 1930)

$|a_p| \leq 2\sqrt{p}$.

Example Consider the curve $y^2 = x^3 - 1$ and $q \equiv 2 \pmod 3$. Then, $E(\mathbb{F}_q) = q + 1$.
Consider the endomorphism $\sigma : E_p \to E_p$ given by $\sigma(x, y) = (x^p, y^p)$. Then $|E(\mathbb{F}_p)| = |\ker(1 - \sigma)| = \deg(1 - \sigma)$.

One can prove that $K \subset End(E_p) \otimes \mathbb{Q}$, where $K = \mathbb{Q}(\pi_p)$ is a quadratic imaginary field, and π_p corresponds to the Frobenius element.

Theorem (Hasse, 1930)

$|a_p| \leq 2\sqrt{p}$.

Example Consider the curve $y^2 = x^3 - 1$ and $q \equiv 2 \pmod 3$. Then, $E(\mathbb{F}_q) = q + 1$.
Consider the endomorphism $\sigma : E_p \to E_p$ given by $\sigma(x, y) = (x^p, y^p)$. Then $|E(\mathbb{F}_p)| = |\ker(1 - \sigma)| = \deg(1 - \sigma)$.

One can prove that $K \subset End(E_p) \otimes \mathbb{Q}$, where $K = \mathbb{Q}(\pi_p)$ is a quadratic imaginary field, and π_p corresponds to the Frobenius element. On the other hand, we know that for any $(p \nmid m)$

$$E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

Since any endomorphism is linear, it will preserve the torsion. And we have a map

$$\rho_m : End(E) \to GL_2(\mathbb{Z}/m\mathbb{Z})$$

In this way, there is a matrix g_m corresponding to the Frobenius element so that $\mathrm{Tr}(g_m) = a_p \pmod m$ and $\det(g_m) = p \pmod m$. In particular the characteristic polynomial of g_m is $P(t) = t^2 - a_p t + p$. Since $\mathbb{Q}(\pi_p)$ is imaginary, we get the result. Note that, $N_{K/\mathbb{Q}}(\pi_p - 1) = p + 1 - a_p = |E(\mathbb{F}_p)|$

In this way, there is a matrix g_m corresponding to the Frobenius element so that $\mathrm{Tr}(g_m) = a_p \pmod{m}$ and $\det(g_m) = p \pmod{m}$. In particular the characteristic polynomial of g_m is $P(t) = t^2 - a_p t + p$. Since $\mathbb{Q}(\pi_p)$ is imaginary, we get the result. Note that, $N_{K/\mathbb{Q}}(\pi_p - 1) = p + 1 - a_p = |E(\mathbb{F}_p)|$

Appart from the size of the $\mathbb{F}_p$ rational points, we are interested about the group structure. In this sense, we have

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/e_p\mathbb{Z} \times \mathbb{Z}/d_p\mathbb{Z},$$

for some integers $e_p | d_p$ and the question would be which kind of pairs appear when fixing the elliptic curve and varying the prime.

Maybe the first question could be:

Question: How often is $E(\mathbb{F}_p)$ cyclic?

Maybe the first question could be:

Question: How often is $E(\mathbb{F}_p)$ cyclic?

Theorem (Serre, 1986)

Under GRH, $E(\mathbb{F}_p)$ is cyclic for a positive proportion of primes.

Maybe the first question could be:

Question: How often is $E(\mathbb{F}_p)$ cyclic?

Theorem (Serre, 1986)

Under GRH, $E(\mathbb{F}_p)$ is cyclic for a positive proportion of primes.

This question is still open.

Maybe the first question could be:

Question: How often is $E(\mathbb{F}_p)$ cyclic?

Theorem (Serre, 1986)

Under GRH, $E(\mathbb{F}_p)$ is cyclic for a positive proportion of primes.

This question is still open.

For ordinary primes we have $K = \mathbb{Q}(\pi_p) = End(E_p) \otimes \mathbb{Q}$.

In 1940 Deuring proved that any order $\mathbb{Z}[\pi_p] \subseteq O \subseteq O_K$ is the ring of endomorphisms of some curve over $\mathbb{F}_p$.

Maybe the first question could be:

Question: How often is $E(\mathbb{F}_p)$ cyclic?

Theorem (Serre, 1986)

Under GRH, $E(\mathbb{F}_p)$ is cyclic for a positive proportion of primes.

This question is still open.

For ordinary primes we have $K = \mathbb{Q}(\pi_p) = End(E_p) \otimes \mathbb{Q}$.

In 1940 Deuring proved that any order $\mathbb{Z}[\pi_p] \subseteq O \subseteq O_K$ is the ring of endomorphisms of some curve over $\mathbb{F}_p$.

Question: How often $End(E_p) \simeq \mathbb{Z}[\pi_p]$ or O_K

Maybe the first question could be:

Question: How often is $E(\mathbb{F}_p)$ cyclic?

Theorem (Serre, 1986)

Under GRH, $E(\mathbb{F}_p)$ is cyclic for a positive proportion of primes.

This question is still open.

For ordinary primes we have $K = \mathbb{Q}(\pi_p) = End(E_p) \otimes \mathbb{Q}$.

In 1940 Deuring proved that any order $\mathbb{Z}[\pi_p] \subseteq O \subseteq O_K$ is the ring of endomorphisms of some curve over $\mathbb{F}_p$.

Question: How often $End(E_p) \simeq \mathbb{Z}[\pi_p]$ or O_K

Question: How often $\mathbb{Z}[\pi_p] \simeq O_K$

It is very difficult!

It is very difficult! How often $a_p^2 - 4p$ is squarefree

It is very difficult! How often $a_p^2 - 4p$ is squarefree

One can prove that $a_p^2 - 4p$ squarefree implies cyclicity of $E(\mathbb{F}_p)$.

It is very difficult! How often $a_p^2 - 4p$ is squarefree

One can prove that $a_p^2 - 4p$ squarefree implies cyclicity of $E(\mathbb{F}_p)$. Moreover, let us consider $y^2 = x^3 - x$. One can see that $\mathrm{End}(E_p) \otimes \mathbb{Q} \simeq \mathbb{Q}[i]$ for every prime of ordinary reduction. This means that $a_p^2 - 4p = -4f^2$, for some integer f. So we are asking how many primes p are such that

$$p = (a_p/2)^2 + 1.$$

It is very difficult! How often $a_p^2 - 4p$ is squarefree

One can prove that $a_p^2 - 4p$ squarefree implies cyclicity of $E(\mathbb{F}_p)$. Moreover, let us consider $y^2 = x^3 - x$. One can see that $\mathrm{End}(E_p) \otimes \mathbb{Q} \simeq \mathbb{Q}[i]$ for every prime of ordinary reduction. This means that $a_p^2 - 4p = -4f^2$, for some integer f. So we are asking how many primes p are such that

$$p = (a_p/2)^2 + 1.$$

We don't even know if there are infinitely many primes so that $p = n^2 + 1$!!!

Let $\Pi^{\mathrm{sf}}_{E,r,h}(x) = \#\{2 < p \le x, \text{ prime } : a_p^2 - 4p \in \Delta(r,h)\}$, where r,h are integers and $\Delta(r,h)$ is the set of square-free integers n such that $n \equiv r \bmod h$. Let $E(a,b) := y^2 = x^3 + ax + b$.

Theorem (David-Jimenez, 2010)

For any $\varepsilon > 0$. Let A, B be such that $AB > x\log^8 x$, $A, B > x^{\epsilon}$. Let $E(a,b) \in \mathcal{C}(A,B)$ if $|a| \le A$ and $b \le B$. Then, as $x \to \infty$,

$$\frac{1}{|\mathcal{C}(A,B)|} \sum_{E(a,b)\in\mathcal{C}(A,B)} \Pi^{\mathrm{sf}}_{E(a,b),r,h}(x) = \mathfrak{C}\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

$$\mathfrak{C} = \frac{1}{3h}\prod_{\substack{\ell \| h \\ \ell | r}} \frac{\ell - 1}{\ell} \prod_{\substack{\ell | h \\ \ell \nmid r}} \frac{\ell\left(\ell - 1 - \left(\frac{r}{\ell}\right)\right)}{(\ell - 1)\left(\ell - \left(\frac{r}{\ell}\right)\right)} \prod_{\ell \nmid h} \frac{\ell^4 - 2\ell^2 - \ell + 1}{\ell^2(\ell^2 - 1)}, \quad (1)$$

where all products are taken over odd primes ℓ with the specified conditions.

Question: How often $|E(\mathbb{F}_p)|$ is a prime number?

Question: How often $|E(\mathbb{F}_p)|$ is a prime number? Non torsion on the isogeny class.

Question: How often $|E(\mathbb{F}_p)|$ is a prime number? Non torsion on the isogeny class.

Conjecture (Koblitz,1988)

$$\Pi_E(x) = \{p \leq x \ : \ |E(\mathbb{F}_p)| \textit{ is prime}\} \sim cx/(\log x)^2$$

for some constant $c > 0$.

Question: How often $|E(\mathbb{F}_p)|$ is a prime number? Non torsion on the isogeny class.

Conjecture (Koblitz,1988)

$$\Pi_E(x) = \{p \leq x \ : \ |E(\mathbb{F}_p)| \textit{ is prime}\} \sim cx/(\log x)^2$$

for some constant $c > 0$.

$\mathcal{A}(x) = \{|E(\mathbb{F}_p)|, p \leq x\}$.

- Miri and Murty (2001), Under GRH for non-CM $|\{P_{16} \in \mathcal{A}(x)\}| \gg x/(\log x)^2$.
- Steuding and Weng (2005) Under GRH $|\{P_6 \in \mathcal{A}(x)\}| \gg x/(\log x)^2$ for non-CM curves, $|\{P_4 \in \mathcal{A}(x)\}| \gg x/(\log x)^2$ in the CM case.
- . Cojocaru (2005) Unconditionally for CM elliptic curves $|\{P_5 \in \mathcal{A}(x)\}| \gg x/(\log x)^2$.

Proposition

Let d_E =gcd$(|E(\mathbb{F}_p)|, p$ of ordinary reduction$)$. Then for any E with complex multiplicaiton, $d_E = 1, 2, 3, 4, 8$ or 12.

Theorem (Iwaniec-Jiménez, Jiménez, 2008)

Let E/Q be an elliptic curve with complex multiplication by O_K the ring of integers of the imaginary quadratic field K. For $x \geq 5$ $|\{p \leq x\, ,\, p$ splits in $O_K\, :\, \frac{1}{d_E}|E(\mathbb{F}_p)| = P_2\}| \gg x/(\log x)^2$.

Proposition

Let d_E =gcd($|E(\mathbb{F}_p)|$, p of ordinary reduction). Then for any E with complex multiplicaiton, $d_E = 1, 2, 3, 4, 8$ or 12.

Theorem (Iwaniec-Jiménez, Jiménez, 2008)

Let E/Q be an elliptic curve with complex multiplication by O_K the ring of integers of the imaginary quadratic field K. For $x \geq 5$ $|\{p \leq x\,,\ p$ splits in $O_K\ :\ \frac{1}{d_E}|E(\mathbb{F}_p)| = P_2\}| \gg x/(\log x)^2$.

Sieve methods.

$$W(x) = \sum_{\substack{a \in \mathcal{A}(x) \\ (a, 2P(z)Q(z))=1}} \left\{ 1 - \sum_{\substack{p_0 | a \\ z < p_0 \leq y}} \frac{1}{2} - \sum_{\substack{a = p_1 p_2 p_3 \\ z < p_3 \leq y < p_2 < p_1}} \frac{1}{2} \right\}$$

where

$$z = x^{1/8} \quad \text{and} \quad y = x^{1/3}.$$