Modularity, Rational Points and Diophantine Equations

Ekin Özman

Boğaziçi University

March 15, 2021

Diophantine Equations

One of the main problems in number theory is:

Diophantine Equations

One of the main problems in number theory is:

Finding solutions of Diophantine Equations e.g. $x^n + y^n = z^n$

Diophantine Equations

One of the main problems in number theory is:

Finding solutions of Diophantine Equations e.g. $x^n + y^n = z^n$

$$\Downarrow$$

Absolute Galois group of $\mathbb{Q}$, $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Understand this!

Diophantine Equations

One of the main problems in number theory is:

Finding solutions of Diophantine Equations e.g. $x^n + y^n = z^n$

$$\Downarrow$$

Absolute Galois group of $\mathbb{Q}$, $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Understand this!

- $G_{\mathbb{Q}} = \varprojlim \mathrm{Gal}(L/\mathbb{Q})$ where L runs through the finite Galois extensions of $\mathbb{Q}$.

Diophantine Equations

One of the main problems in number theory is:

Finding solutions of Diophantine Equations e.g. $x^n + y^n = z^n$

$$\Downarrow$$

Absolute Galois group of $\mathbb{Q}$, $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Understand this!

- $G_{\mathbb{Q}} = \varprojlim \mathrm{Gal}(L/\mathbb{Q})$ where L runs through the finite Galois extensions of $\mathbb{Q}$.
- To understand $G_{\mathbb{Q}}$ we look at its representations:

Diophantine Equations

One of the main problems in number theory is:

Finding solutions of Diophantine Equations e.g. $x^n + y^n = z^n$

$$\Downarrow$$

Absolute Galois group of $\mathbb{Q}$, $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Understand this!

- $G_{\mathbb{Q}} = \varprojlim \mathrm{Gal}(L/\mathbb{Q})$ where L runs through the finite Galois extensions of $\mathbb{Q}$.
- To understand $G_{\mathbb{Q}}$ we look at its representations:

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$$

Finding $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point $\mathcal{O}$.

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point $\mathcal{O}$.

- $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}$.

Finding $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point $\mathcal{O}$.

- $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}$.
- $E[p]$ is the p-torsion subgroup in $E(\mathbb{C})$, $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$

Finding $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point $\mathcal{O}$.

- $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}$.
- $E[p]$ is the p-torsion subgroup in $E(\mathbb{C})$, $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$
- $E[p] \subset E(\bar{\mathbb{Q}})$ (the torsion points are algebraic).

Finding $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$

Definition

An elliptic curve E is a smooth, projective algebraic curve of genus one, on which there is a specified point $\mathcal{O}$.

- $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax^2 + bx + c\} \cup \{\mathcal{O}\}$.
- $E[p]$ is the p-torsion subgroup in $E(\mathbb{C})$, $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$
- $E[p] \subset E(\bar{\mathbb{Q}})$ (the torsion points are algebraic).
- $G_{\mathbb{Q}}$ acts on $E[p]$. We obtain a representation

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

Strategy of The Proof of FLT

Theorem (Wiles, Taylor-Wiles)

The equation

$$FLT_n : x^n + y^n = z^n$$

has no nonzero integer solutions if $n > 2$.

Strategy of The Proof of FLT

Theorem (Wiles, Taylor-Wiles)

The equation

$$FLT_n : x^n + y^n = z^n$$

has no nonzero integer solutions if $n > 2$.

- To find an elliptic curve corresponding a proposed solution of FLT_p

Strategy of The Proof of FLT

Theorem (Wiles, Taylor-Wiles)

The equation

$$FLT_n : x^n + y^n = z^n$$

has no nonzero integer solutions if $n > 2$.

- To find an elliptic curve corresponding a proposed solution of FLT_p
- To show that this curve has properties conflicting with each other

Strategy of The Proof of FLT

Theorem (Wiles, Taylor-Wiles)

The equation

$$FLT_n : x^n + y^n = z^n$$

has no nonzero integer solutions if $n > 2$.

- To find an elliptic curve corresponding a proposed solution of FLT_p
- To show that this curve has properties conflicting with each other

1. Modularity Theorem (Wiles, Taylor-Wiles)

Strategy of The Proof of FLT

Theorem (Wiles, Taylor-Wiles)

The equation

$$FLT_n : x^n + y^n = z^n$$

has no nonzero integer solutions if $n > 2$.

- To find an elliptic curve corresponding a proposed solution of FLT_p
- To show that this curve has properties conflicting with each other

1. Modularity Theorem (Wiles, Taylor-Wiles)
2. Level Lowering Theorem (Ribet)

Strategy of The Proof of FLT

Theorem (Wiles, Taylor-Wiles)

The equation

$$FLT_n : x^n + y^n = z^n$$

has no nonzero integer solutions if $n > 2$.

- To find an elliptic curve corresponding a proposed solution of FLT_p
- To show that this curve has properties conflicting with each other

1. Modularity Theorem (Wiles, Taylor-Wiles)
2. Level Lowering Theorem (Ribet)
3. Irreducibility of Galois representations(Mazur)

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

Solving $x^n + y^n = z^n$

Three main ingredients:

- Modularity Thm: Every elliptic curve over $\mathbb{Q}$ is associated to a modular form

Three main ingredients:

- Modularity Thm: Every elliptic curve over $\mathbb{Q}$ is associated to a modular form
  There is a modular function $f(z) = \sum_{n=1}^{\infty} a_n q^n$ such that $a_q = a_q(E) = q + 1 - |E(\mathbb{F}_q)|$.

Solving $x^n + y^n = z^n$

Three main ingredients:

- Modularity Thm: Every elliptic curve over $\mathbb{Q}$ is associated to a modular form
  There is a modular function $f(z) = \sum_{n=1}^{\infty} a_n q^n$ such that $a_q = a_q(E) = q + 1 - |E(\mathbb{F}_q)|$.
- Mazur's Thm: If E is an elliptic curve over $\mathbb{Q}$ with full two torsion then $\rho_{E,p}$ is irreducible for $p \geq 5$

Solving $x^n + y^n = z^n$

Three main ingredients:

- Modularity Thm: Every elliptic curve over $\mathbb{Q}$ is associated to a modular form
  There is a modular function $f(z) = \sum_{n=1}^{\infty} a_n q^n$ such that $a_q = a_q(E) = q + 1 - |E(\mathbb{F}_q)|$.
- Mazur's Thm: If E is an elliptic curve over $\mathbb{Q}$ with full two torsion then $\rho_{E,p}$ is irreducible for $p \geq 5$
- Ribet's Thm: is appliciable and E can be 'attached to' a special modular form of lower level.

Solving $x^n + y^n = z^n$

Three main ingredients:

- Modularity Thm: Every elliptic curve over $\mathbb{Q}$ is associated to a modular form
  There is a modular function $f(z) = \sum_{n=1}^{\infty} a_n q^n$ such that $a_q = a_q(E) = q + 1 - |E(\mathbb{F}_q)|$.
- Mazur's Thm: If E is an elliptic curve over $\mathbb{Q}$ with full two torsion then $\rho_{E,p}$ is irreducible for $p \geq 5$
- Ribet's Thm: is appliciable and E can be 'attached to' a special modular form of lower level.
  There is a special modular function $g(z) = \sum_{n=1}^{\infty} a_n q^n$ such that $a_q \equiv a_q(E) \pmod{p}$.

Frey Curve and Irreducibility

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let

$$E : y^2 = x(x - a^p)(x + b^p) \qquad \textbf{Frey Curve}$$

Frey Curve and Irreducibility

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let

$$E : y^2 = x(x - a^p)(x + b^p) \qquad \textbf{Frey Curve}$$

$$\Delta_{min} = \frac{1}{2^8}(abc)^p$$

Let $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Then:

Frey Curve and Irreducibility

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let

$$E : y^2 = x(x - a^p)(x + b^p) \qquad \textbf{Frey Curve}$$

$$\Delta_{min} = \frac{1}{2^8}(abc)^p$$

Let $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Then:

$$\left.\begin{array}{l}\rho_{E,p} \text{ is irreducible by Mazur} \\ E \text{ is modular by Wiles}\end{array}\right\} \Rightarrow$$

Frey Curve and Irreducibility

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let

$$E : y^2 = x(x - a^p)(x + b^p) \qquad \textbf{Frey Curve}$$

$$\Delta_{min} = \frac{1}{2^8}(abc)^p$$

Let $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Then:

$$\left.\begin{array}{l} \rho_{E,p} \text{ is irreducible by Mazur} \\ E \text{ is modular by Wiles} \end{array}\right\} \Rightarrow \quad \begin{array}{l} E \text{ is associated to a newform} \\ \text{of level 2 by Ribet.} \end{array}$$

Frey Curve and Irreducibility

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let

$$E : y^2 = x(x - a^p)(x + b^p) \qquad \textbf{Frey Curve}$$

$$\Delta_{min} = \frac{1}{2^8}(abc)^p$$

Let $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Then:

$$\left.\begin{array}{l} \rho_{E,p} \text{ is irreducible by Mazur} \\ E \text{ is modular by Wiles} \end{array}\right\} \Rightarrow \begin{array}{l} E \text{ is associated to a newform} \\ \text{of level 2 by Ribet.} \end{array}$$

But there is no such newform!

Frey Curve and Irreducibility

Let (a, b, c) be a non-trivial primitive solution to the Fermat equation with exponent $p \geq 5$. Let

$$E : y^2 = x(x - a^p)(x + b^p) \qquad \textbf{Frey Curve}$$

$$\Delta_{min} = \frac{1}{2^8}(abc)^p$$

Let $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. Then:

$$\left.\begin{array}{l}\rho_{E,p} \text{ is irreducible by Mazur} \\ E \text{ is modular by Wiles}\end{array}\right\} \Rightarrow \begin{array}{l}E \text{ is associated to a newform} \\ \text{of level 2 by Ribet.}\end{array}$$

But there is no such newform!

A key ingredient: for big enough p and for any E:

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

is **irreducible** i.e. NOT upper triangular.

Irreducibility of Galois representations(Mazur)

A key ingredient on the proof of FLT_p was that for big enough p and for any E:

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

is **irreducible** i.e. NOT upper triangular.

Irreducibility of Galois representations(Mazur)

A key ingredient on the proof of FLT_p was that for big enough p and for any E:

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

is **irreducible** i.e. NOT upper triangular.

How to parametrize all $\rho_{E,p}$?

Irreducibility of Galois representations(Mazur)

A key ingredient on the proof of FLT_p was that for big enough p and for any E:

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

is **irreducible** i.e. NOT upper triangular.

How to parametrize all $\rho_{E,p}$?

Given p there exists an algebraic curve, $\mathrm{X}_0(\mathrm{p})$ s.t. :

$$\{\text{Points on } \mathrm{X}_0(\mathrm{p})\}$$

$$\Updownarrow$$

$$\{\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p) \text{ such that } \rho_{E,p} \sim \begin{bmatrix} * & * \\ 0 & * \end{bmatrix}\}$$

Understanding $X_0(N)(\mathbb{Q})$

Example (Equation of $X_0(43)$)

$$f(x,y) = x^4 + 2x^3y + 2x^2y^2 + xy^3 - 2x^2y - 2xy^2 - y^3 + 4x^2 +$$

$$+4xy + 2y^2 - 3y + 4 = 0$$

Understanding $X_0(N)(\mathbb{Q})$

Example (Equation of $X_0(43)$)

$$f(x,y) = x^4 + 2x^3y + 2x^2y^2 + xy^3 - 2x^2y - 2xy^2 - y^3 + 4x^2 +$$
$$+ 4xy + 2y^2 - 3y + 4 = 0$$

How to understand the set $X_0(43)(\mathbb{Q}) = \{(x,y) : f(x,y) = 0\}$?

Understanding $\mathrm{X}_0(\mathrm{N})(\mathbb{Q})$

Example (Equation of $X_0(43)$)

$$f(x,y) = x^4 + 2x^3y + 2x^2y^2 + xy^3 - 2x^2y - 2xy^2 - y^3 + 4x^2 +$$

$$+4xy + 2y^2 - 3y + 4 = 0$$

How to understand the set $\mathrm{X}_0(43)(\mathbb{Q}) = \{(x,y) : f(x,y) = 0\}$?

Theorem (Mazur)

If $N > 163$ and prime then $\mathrm{X}_0(\mathrm{N})(\mathbb{Q})$ consists of only cusps.

Understanding $X_0(N)(\mathbb{Q})$

Example (Equation of $X_0(43)$)

$$f(x,y) = x^4 + 2x^3y + 2x^2y^2 + xy^3 - 2x^2y - 2xy^2 - y^3 + 4x^2 +$$

$$+4xy + 2y^2 - 3y + 4 = 0$$

How to understand the set $X_0(43)(\mathbb{Q}) = \{(x,y) : f(x,y) = 0\}$?

Theorem (Mazur)

If $N > 163$ and prime then $X_0(N)(\mathbb{Q})$ consists of only cusps.

Later this has been generalized to composite levels and the situation for small levels is also understood by Kenku, Momose.

What about other Diophantine Equations?

- Can we understand rational solutions $x^p + y^q + z^r = 0$ or $Ax^p + By^p + Cz^p = 0$ or $Ax^p + By^q + Cz^r = 0$ using similar techniques?

What about other Diophantine Equations?

- Can we understand rational solutions $x^p + y^q + z^r = 0$ or $Ax^p + By^p + Cz^p = 0$ or $Ax^p + By^q + Cz^r = 0$ using similar techniques?
- Can we understand solutions of these equations over larger number fields ?

What about other Diophantine Equations?

- Can we understand rational solutions $x^p + y^q + z^r = 0$ or $Ax^p + By^p + Cz^p = 0$ or $Ax^p + By^q + Cz^r = 0$ using similar techniques?
- Can we understand solutions of these equations over larger number fields ?

What is needed?

- Modularity of elliptic curves defined over larger fields than $\mathbb{Q}$ OR
- Modularity of elliptic curves defined over larger fields than $\mathbb{Q}$ but rational up to isogeny.($\mathbb{Q}$-curves)
- Ribet's thm over larger fields

What about other Diophantine Equations?

- Can we understand rational solutions $x^p + y^q + z^r = 0$ or $Ax^p + By^p + Cz^p = 0$ or $Ax^p + By^q + Cz^r = 0$ using similar techniques?
- Can we understand solutions of these equations over larger number fields ?

What is needed?

- Modularity of elliptic curves defined over larger fields than $\mathbb{Q}$ OR
- Modularity of elliptic curves defined over larger fields than $\mathbb{Q}$ but rational up to isogeny.($\mathbb{Q}$-curves)
- Ribet's thm over larger fields
- Mazur's thm defined over larger fields

Understanding $X_0(N)(K)$

- To solve Fermat type equations over higher degree number fields K, we need to understand $X_0(N)(K)$.

Understanding $X_0(N)(K)$

- To solve Fermat type equations over higher degree number fields K, we need to understand $X_0(N)(K)$.

$X_1(N)(K)$ is well understood:

- ◇ $X_1(N)(K) \Leftrightarrow (E, P)$ where $E_{/K}$ and $P \in E[N](K)$.
- ◇ $X_0(N)(K) \Leftrightarrow$ reducible Galois representations OR

Understanding $X_0(N)(K)$

- To solve Fermat type equations over higher degree number fields K, we need to understand $X_0(N)(K)$.

$X_1(N)(K)$ is well understood:

- $X_1(N)(K) \Leftrightarrow (E, P)$ where $E_{/K}$ and $P \in E[N](K)$.
- $X_0(N)(K) \Leftrightarrow$ reducible Galois representations OR
  $(E, \phi : E \to E') = (E, C = \ker \phi \cong \mathbb{Z}/N\mathbb{Z})$

Understanding $X_0(N)(K)$

- To solve Fermat type equations over higher degree number fields K, we need to understand $X_0(N)(K)$.

$X_1(N)(K)$ is well understood:

- ◇ $X_1(N)(K) \Leftrightarrow (E, P)$ where $E_{/K}$ and $P \in E[N](K)$.
- ◇ $X_0(N)(K) \Leftrightarrow$ reducible Galois representations OR

$$(E, \phi : E \to E') = (E, C = \ker \phi \cong \mathbb{Z}/N\mathbb{Z})$$

- By Mazur's work: $X_1(N)(\mathbb{Q}) = \{\text{cusps}\}$ if its genus> 1
- Merel: Say $|K : \mathbb{Q}| \leq d$, then there exists B_d such that $X_1(N)(K) = \{\text{cusps}\}$ if $N > B_d$.
- More precise results by Kamienny, Parent, Derickx, Stein, Stoll...

Unfortunately not much is known for $X_0(N)(K)$ except the following:

Understanding $\mathrm{X}_0(\mathrm{N})(K)$

Definition

A point P is quadratic if $|\mathbb{Q}(P)/\mathbb{Q}| = 2$.

Understanding $X_0(N)(K)$

Definition

A point P is quadratic if $|\mathbb{Q}(P)/\mathbb{Q}| = 2$.

- **Bars, Harris-Silverman:** If $g(X_0(N)) \geq 2$ then $X_0(N)$ has finitely many quadratic points except for 28 values of N.

Understanding $X_0(N)(K)$

Definition

A point P is quadratic if $|\mathbb{Q}(P)/\mathbb{Q}| = 2$.

- **Bars, Harris-Silverman:** If $g(X_0(N)) \geq 2$ then $X_0(N)$ has finitely many quadratic points except for 28 values of N.

- **Bruin, Najman:** parametrized all quadratic points on $X_0(N)$ such that $J_0(N)$ has MW rank 0 and $X_0(N)$ is hyperelliptic:

$$\{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$$

Understanding $X_0(N)(K)$

Theorem (O., Siksek)

Found and parametrized all quadratic points on $\mathrm{X}_0(\mathrm{N})$ such that

- $J_0(N)$ *has MW rank* 0 *and*
- $3 \leq g(\mathrm{X}_0(\mathrm{N})) \leq 5$.

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$$

Understanding $X_0(N)(K)$

Theorem (O., Siksek)

Found and parametrized all quadratic points on $\mathrm{X}_0(\mathrm{N})$ *such that*

- $J_0(N)$ *has MW rank* 0 *and*
- $3 \le g(\mathrm{X}_0(\mathrm{N})) \le 5$.

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$$

Hence we have a full list of all quadratic points on $\mathrm{X}_0(\mathrm{N})$ for $2 \le g(\mathrm{X}_0(\mathrm{N})) \le 5$ with $J_0(N)$ has MW rank 0.

Understanding $X_0(N)(K)$

Recently:

Theorem (Box)

All quadratic points on all $\mathrm{X}_0(\mathrm{N})$ *of genus* $2, 3, 4, 5$ *whose Mordell–Weil group has positive rank have been determined. The values of* N *are* $37, 43, 53, 61, 57, 65, 67$ *and* 73.

Recently:

Theorem (Box)

All quadratic points on all $\mathrm{X}_0(\mathrm{N})$ *of genus* $2, 3, 4, 5$ *whose Mordell–Weil group has positive rank have been determined. The values of N are* $37, 43, 53, 61, 57, 65, 67$ *and* 73.

Hence we have a full list of all quadratic points on $\mathrm{X}_0(\mathrm{N})$ for $2 \leq g(\mathrm{X}_0(\mathrm{N})) \leq 5$

Understanding $X_0(N)(K)$

Recently:

Theorem (Box)

All quadratic points on all $\mathrm{X}_0(\mathrm{N})$ of genus $2, 3, 4, 5$ whose Mordell–Weil group has positive rank have been determined. The values of N are $37, 43, 53, 61, 57, 65, 67$ and 73.

Hence we have a full list of all quadratic points on $\mathrm{X}_0(\mathrm{N})$ for $2 \leq g(\mathrm{X}_0(\mathrm{N})) \leq 5$

Why is this helpful?

Main Theorem

Theorem

Found and parametrized all quadratic points on $X_0(N)$ *for* $N =$

- *Bruin-Najman:*

$\{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$

- *O.-Siksek:* $\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$
- *Box:* $\{37, 43, 53, 61, 57, 65, 67, 73\}$

Main Theorem

Theorem

Found and parametrized all quadratic points on $X_0(N)$ for $N =$

- *Bruin-Najman:*

$\{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$

- *O.-Siksek:* $\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$
- *Box:* $\{37, 43, 53, 61, 57, 65, 67, 73\}$

Why is this helpful?

Main Theorem

Theorem

Found and parametrized all quadratic points on $X_0(N)$ *for* $N =$

- *Bruin-Najman:*

$\{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$

- *O.-Siksek:* $\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$
- *Box:* $\{37, 43, 53, 61, 57, 65, 67, 73\}$

Why is this helpful?

- Modular approach to solve Diop. Eqns. requires the irreducibility of the mod p representation $\rho_{E,p}$ of a Frey elliptic curve E over K.

Main Theorem

Theorem

Found and parametrized all quadratic points on $X_0(N)$ for N =

- *Bruin-Najman:*

$\{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$

- *O.-Siksek:* $\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$
- *Box:* $\{37, 43, 53, 61, 57, 65, 67, 73\}$

Why is this helpful?

- Modular approach to solve Diop. Eqns. requires the irreducibility of the mod p representation $\rho_{E,p}$ of a Frey elliptic curve E over K.
- This Frey elliptic curve often has extra level structure in the form of a K-rational 2 or 3-isogeny

Main Theorem

Theorem

Found and parametrized all quadratic points on $\mathrm{X}_0(\mathrm{N})$ *for* $N =$

- *Bruin-Najman:*

$\{22, 23, 26, 28, 29, 30, 31, 33, 35, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$

- *O.-Siksek:* $\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$
- *Box:* $\{37, 43, 53, 61, 57, 65, 67, 73\}$

Why is this helpful?

- Modular approach to solve Diop. Eqns. requires the irreducibility of the mod p representation $\rho_{E,p}$ of a Frey elliptic curve E over K.
- This Frey elliptic curve often has extra level structure in the form of a K-rational 2 or 3-isogeny
- If the mod p representation is reducible, then the Frey curve gives rise to a point in $\mathrm{X}_0(2p)(K)$ or $\mathrm{X}_0(3p)(K)$

A genus 3 example $X_0(34)$

◇ If the mod p representation is reducible, then the Frey curve gives rise to a point in $\mathrm{X}_0(2p)(K)$ or $\mathrm{X}_0(3p)(K)$

A genus 3 example $X_0(34)$

$\diamond$ If the mod p representation is reducible, then the Frey curve gives rise to a point in $\mathrm{X}_0(2p)(K)$ or $\mathrm{X}_0(3p)(K)$
$\diamond$ The quadratic points of $\mathrm{X}_0(34)$ is used to study quadratic solutions of $x^p + y^p + z^p = 0$ by Freitas and Siksek.

A genus 3 example $X_0(34)$

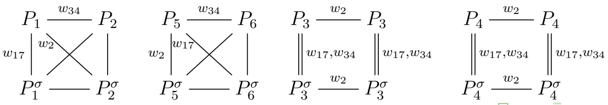
◇ If the mod p representation is reducible, then the Frey curve gives rise to a point in $\mathrm{X}_0(2p)(K)$ or $\mathrm{X}_0(3p)(K)$
◇ The quadratic points of $\mathrm{X}_0(34)$ is used to study quadratic solutions of $x^p + y^p + z^p = 0$ by Freitas and Siksek.

Genus: 3

Model: $x^3z - x^2y^2 - 3x^2z^2 + 2xz^3 + 3xy^2z - 3xyz^2 + 4xz^3 - y^4 + 4y^3z - 6x^2z^2 + 4yz^3 - 2z^4$

$J_0(34)(\mathbb{Q}) = C \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

Name	θ^2	Coordinates	j-invariant	CM by	$\mathbb{Q}$-curve
P_1	-1	$(\theta+1,0,1)$	287496	-16	YES
P_2	-1	$(\frac{\theta+1}{2},\frac{\theta+1}{2},1)$	1728	-4	YES
P_3	-1	$(\theta,-\theta,1)$	1728	-4	YES
P_4	-2	$(\frac{\theta}{2},-\frac{\theta}{2},1)$	8000	-8	YES
P_5	-15	$(\frac{\theta+11}{8},\frac{1}{2},1)$	$\frac{20410\theta+11779}{8}$	NO	YES
P_6	-15	$(\frac{\theta+23}{16},\frac{\theta+7}{16},1)$	$\frac{-531847853404790\theta-7319387769191}{34359738368}$	NO	YES



Idea of the Proof-Theoretical Approach

Theorem (O., Siksek)

Found and parametrized all quadratic points on $\mathrm{X}_0(\mathrm{N})$ *such that* $J_0(N)$ *has MW rank* 0*,* $\mathrm{X}_0(\mathrm{N})$ *nonhyperelliptic and* $3 \leq g \leq 5$*.*

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$$

- Say $X/\mathbb{Q}$ is nonhyperelliptic with $g \geq 3$, $J_X(\mathbb{Q})$ is finite and there exists a $P_0 \in X(\mathbb{Q})$.
- Assume one can enumerate all $J_X(\mathbb{Q})$.

Idea of the Proof-Theoretical Approach

Theorem (O., Siksek)

Found and parametrized all quadratic points on $\mathrm{X}_0(\mathrm{N})$ *such that* $J_0(N)$ *has MW rank* 0*,* $\mathrm{X}_0(\mathrm{N})$ *nonhyperelliptic and* $3 \leq g \leq 5$*.*

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$$

- Say $X/\mathbb{Q}$ is nonhyperelliptic with $g \geq 3$, $J_X(\mathbb{Q})$ is finite and there exists a $P_0 \in X(\mathbb{Q})$.
- Assume one can enumerate all $J_X(\mathbb{Q})$.
- ◇ $X^{(2)}$, symmetric product of X

Idea of the Proof-Theoretical Approach

Theorem (O., Siksek)

Found and parametrized all quadratic points on $\mathrm{X}_0(\mathrm{N})$ *such that* $J_0(N)$ *has MW rank* 0, $\mathrm{X}_0(\mathrm{N})$ *nonhyperelliptic and* $3 \leq g \leq 5$.

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$$

- Say $X/\mathbb{Q}$ is nonhyperelliptic with $g \geq 3, J_X(\mathbb{Q})$ is finite and there exists a $P_0 \in X(\mathbb{Q})$.
- Assume one can enumerate all $J_X(\mathbb{Q})$.

◇ $X^{(2)}$, symmetric product of X

◇ $P = \{P_1, P_2\} \in X^{(2)}(\mathbb{Q})$ implies either $P_1, P_2 \in X(\mathbb{Q})$

Idea of the Proof-Theoretical Approach

Theorem (O., Siksek)

Found and parametrized all quadratic points on $X_0(N)$ *such that* $J_0(N)$ *has MW rank* 0, $X_0(N)$ *nonhyperelliptic and* $3 \leq g \leq 5$.

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$$

- Say $X/\mathbb{Q}$ is nonhyperelliptic with $g \geq 3, J_X(\mathbb{Q})$ is finite and there exists a $P_0 \in X(\mathbb{Q})$.
- Assume one can enumerate all $J_X(\mathbb{Q})$.
- ◇ $X^{(2)}$, symmetric product of X
- ◇ $P = \{P_1, P_2\} \in X^{(2)}(\mathbb{Q})$ implies either $P_1, P_2 \in X(\mathbb{Q})$ or $P_1, P_2 \in X(K), K = \mathbb{Q}(\sqrt{d})$ and $P_1 = \sigma(P_2)$

Idea of the Proof-Theoretical Approach

Theorem (O., Siksek)

Found and parametrized all quadratic points on $\mathrm{X}_0(\mathrm{N})$ *such that* $J_0(N)$ *has MW rank* 0, $\mathrm{X}_0(\mathrm{N})$ *nonhyperelliptic and* $3 \leq g \leq 5$.

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$$

- Say $X/\mathbb{Q}$ is nonhyperelliptic with $g \geq 3$, $J_X(\mathbb{Q})$ is finite and there exists a $P_0 \in X(\mathbb{Q})$.
- Assume one can enumerate all $J_X(\mathbb{Q})$.

◇ $X^{(2)}$, symmetric product of X

◇ $P = \{P_1, P_2\} \in X^{(2)}(\mathbb{Q})$ implies either $P_1, P_2 \in X(\mathbb{Q})$ or $P_1, P_2 \in X(K)$, $K = \mathbb{Q}(\sqrt{d})$ and $P_1 = \sigma(P_2)$

◇ Let $D_P = P_1 + P_2$ when $P = \{P_1, P_2\}$ and consider

Idea of the Proof-Theoretical Approach

Theorem (O., Siksek)

Found and parametrized all quadratic points on $\mathrm{X}_0(\mathrm{N})$ *such that* $J_0(N)$ *has MW rank* 0, $\mathrm{X}_0(\mathrm{N})$ *nonhyperelliptic and* $3 \leq g \leq 5$.

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\}$$

- Say $X/\mathbb{Q}$ is nonhyperelliptic with $g \geq 3, J_X(\mathbb{Q})$ is finite and there exists a $P_0 \in X(\mathbb{Q})$.
- Assume one can enumerate all $J_X(\mathbb{Q})$.

◇ $X^{(2)}$, symmetric product of X

◇ $P = \{P_1, P_2\} \in X^{(2)}(\mathbb{Q})$ implies either $P_1, P_2 \in X(\mathbb{Q})$ or $P_1, P_2 \in X(K), K = \mathbb{Q}(\sqrt{d})$ and $P_1 = \sigma(P_2)$

◇ Let $D_P = P_1 + P_2$ when $P = \{P_1, P_2\}$ and consider

$$\iota : X^{(2)}(\mathbb{Q}) \hookrightarrow J_X(\mathbb{Q}), \ P \mapsto [D_P - 2P_0]$$

Idea: By pulling back finitely many points in $J_X(\mathbb{Q})$ it is possible to determine $X^{(2)}(\mathbb{Q})$

Idea of the Proof-Theoretical Approach

Idea: Pulling back finitely many points in $J_X(\mathbb{Q})$ it is possible to determine $X^{(2)}(\mathbb{Q})$

Idea of the Proof-Theoretical Approach

Idea: Pulling back finitely many points in $J_X(\mathbb{Q})$ it is possible to determine $X^{(2)}(\mathbb{Q})$

- any $P = \{P_1, P_2\}$ in $X^{(2)} \to D_P = P_1 + P_2$

Idea of the Proof-Theoretical Approach

Idea: Pulling back finitely many points in $J_X(\mathbb{Q})$ it is possible to determine $X^{(2)}(\mathbb{Q})$

- any $P = \{P_1, P_2\}$ in $X^{(2)} \to D_P = P_1 + P_2 \sim D' + 2P_0$ for some $[D'] \in J_X(\mathbb{Q}), D' \in Div^0(X)$

Idea of the Proof-Theoretical Approach

Idea: Pulling back finitely many points in $J_X(\mathbb{Q})$ it is possible to determine $X^{(2)}(\mathbb{Q})$

- any $P = \{P_1, P_2\}$ in $X^{(2)} \to D_P = P_1 + P_2 \sim D' + 2P_0$ for some $[D'] \in J_X(\mathbb{Q}), D' \in Div^0(X)$
- for each $[D'] \in J_X(\mathbb{Q})$, enumerate effective degree 2 divs linearly equivalent to $D' + 2P_0$
- Compute the RR space $L(D' + 2P_0)$. Either
  - $\dim L(D' + 2P_0) = 0$: no eff. deg. 2 divisor $D \sim D' + 2P_0$

Idea of the Proof-Theoretical Approach

Idea: Pulling back finitely many points in $J_X(\mathbb{Q})$ it is possible to determine $X^{(2)}(\mathbb{Q})$

- any $P = \{P_1, P_2\}$ in $X^{(2)} \to D_P = P_1 + P_2 \sim D' + 2P_0$ for some $[D'] \in J_X(\mathbb{Q}), D' \in Div^0(X)$
- for each $[D'] \in J_X(\mathbb{Q})$, enumerate effective degree 2 divs linearly equivalent to $D' + 2P_0$
- Compute the RR space $L(D' + 2P_0)$. Either
  - $\dim L(D' + 2P_0) = 0$: no eff. deg. 2 divisor $D \sim D' + 2P_0$
  - $\dim L(D' + 2P_0) = 1$: let $0 \neq f \in L(D' + 2P_0)$ then

Idea of the Proof-Theoretical Approach

Idea: Pulling back finitely many points in $J_X(\mathbb{Q})$ it is possible to determine $X^{(2)}(\mathbb{Q})$

- any $P = \{P_1, P_2\}$ in $X^{(2)} \to D_P = P_1 + P_2 \sim D' + 2P_0$ for some $[D'] \in J_X(\mathbb{Q}), D' \in Div^0(X)$
- for each $[D'] \in J_X(\mathbb{Q})$, enumerate effective degree 2 divs linearly equivalent to $D' + 2P_0$
- Compute the RR space $L(D' + 2P_0)$. Either
    - $\dim L(D' + 2P_0) = 0$: no eff. deg. 2 divisor $D \sim D' + 2P_0$
    - $\dim L(D' + 2P_0) = 1$: let $0 \neq f \in L(D' + 2P_0)$ then $D' + 2P_0 + div(f)$ is unique eff. deg. 2 divisor $\sim D' + 2P_0$.

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$.

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$. Even if this is done,
- $J_0(N)(\mathbb{Q})$ can be huge and R.R. comps. can be complicated

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$. Even if this is done,
- $J_0(N)(\mathbb{Q})$ can be huge and R.R. comps. can be complicated

Our Approach:

1. Compute $C \leq J_0(N)(\mathbb{Q})$, C is the rational cuspidal grp

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$. Even if this is done,
- $J_0(N)(\mathbb{Q})$ can be huge and R.R. comps. can be complicated

Our Approach:

1. Compute $C \leq J_0(N)(\mathbb{Q})$, C is the rational cuspidal grp
    - By Manin-Drinfeld Thm: $C \leq J_0(N)(\mathbb{Q})_{\text{tors}}$

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$. Even if this is done,
- $J_0(N)(\mathbb{Q})$ can be huge and R.R. comps. can be complicated

Our Approach:

1. Compute $C \leq J_0(N)(\mathbb{Q})$, C is the rational cuspidal grp
    - By Manin-Drinfeld Thm: $C \leq J_0(N)(\mathbb{Q})_{\mathrm{tors}}$
    - Generalized Ogg Conj: $C = J_0(N)(\mathbb{Q})_{\mathrm{tors}}$.

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$. Even if this is done,
- $J_0(N)(\mathbb{Q})$ can be huge and R.R. comps. can be complicated

Our Approach:

1. Compute $C \leq J_0(N)(\mathbb{Q})$, C is the rational cuspidal grp
   - By Manin-Drinfeld Thm: $C \leq J_0(N)(\mathbb{Q})_{\text{tors}}$
   - Generalized Ogg Conj: $C = J_0(N)(\mathbb{Q})_{\text{tors}}$.
2. Bound the index of C in $J_0(N)$ by I, so $I.J_0(N)(\mathbb{Q}) \subset C$

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$. Even if this is done,
- $J_0(N)(\mathbb{Q})$ can be huge and R.R. comps. can be complicated

Our Approach:

1. Compute $C \leq J_0(N)(\mathbb{Q})$, C is the rational cuspidal grp
    - By Manin-Drinfeld Thm: $C \leq J_0(N)(\mathbb{Q})_{\text{tors}}$
    - Generalized Ogg Conj: $C = J_0(N)(\mathbb{Q})_{\text{tors}}$.
2. Bound the index of C in $J_0(N)$ by I, so $I.J_0(N)(\mathbb{Q}) \subset C$
3. so the effective degree 2 divs we seek satisfy:

$$[D - 2P_0] = I[D'] \text{ where } D' \in J_0(N)(\mathbb{Q}).$$

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$. Even if this is done,
- $J_0(N)(\mathbb{Q})$ can be huge and R.R. comps. can be complicated

Our Approach:

1. Compute $C \leq J_0(N)(\mathbb{Q})$, C is the rational cuspidal grp
   - By Manin-Drinfeld Thm: $C \leq J_0(N)(\mathbb{Q})_{\mathrm{tors}}$
   - Generalized Ogg Conj: $C = J_0(N)(\mathbb{Q})_{\mathrm{tors}}$.
2. Bound the index of C in $J_0(N)$ by I, so $I.J_0(N)(\mathbb{Q}) \subset C$
3. so the effective degree 2 divs we seek satisfy:

$$[D - 2P_0] = I[D'] \text{ where } D' \in J_0(N)(\mathbb{Q}).$$

4. Apply MW sieve to eliminate most possibilities for D'.

Theoretical Approach-Problems

- It is hard to enumerate $J_0(N)(\mathbb{Q})$. Even if this is done,
- $J_0(N)(\mathbb{Q})$ can be huge and R.R. comps. can be complicated

Our Approach:

1. Compute $C \leq J_0(N)(\mathbb{Q})$, C is the rational cuspidal grp
    - By Manin-Drinfeld Thm: $C \leq J_0(N)(\mathbb{Q})_{\mathrm{tors}}$
    - Generalized Ogg Conj: $C = J_0(N)(\mathbb{Q})_{\mathrm{tors}}$.
2. Bound the index of C in $J_0(N)$ by I, so $I.J_0(N)(\mathbb{Q}) \subset C$
3. so the effective degree 2 divs we seek satisfy:

$$[D - 2P_0] = I[D'] \text{ where } D' \in J_0(N)(\mathbb{Q}).$$

4. Apply MW sieve to eliminate most possibilities for D'.
5. only then use Riemann Roch.

Final Word of 1st Motivation

Theorem (O., Siksek)

For

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\},$$

$\mathrm{X}_0(\mathrm{N})(\mathbb{Q}(\sqrt{d}))$ *consists of only cusps if*

$$d \neq -159, -39, -19, -15, -11, -7-3, -2, -1, 5, 13, 17.$$

Final Word of 1st Motivation

Theorem (O., Siksek)

For

$$\{34, 45, 64, 38, 44, 54, 81, 42, 51, 52, 55, 56, 63, 72, 75\},$$

$\mathrm{X}_0(\mathrm{N})(\mathbb{Q}(\sqrt{d}))$ *consists of only cusps if*

$$d \neq -159, -39, -19, -15, -11, -7 - 3, -2, -1, 5, 13, 17.$$

Open Question:

Is there a bound B such that for all $|d| > B, \mathrm{X}_0(\mathrm{N})$ doesn't have any quadratic points for any N? (Say genus of $\mathrm{X}_0(\mathrm{N}) > 2$)

Second Motivation to study $\mathrm{X}_0(\mathrm{N})(K)$

Recall that one of the main things to solve FLT over higher degree number fields is: Modularity Theorem

Second Motivation to study $\mathrm{X}_0(\mathrm{N})(K)$

Recall that one of the main things to solve FLT over higher degree number fields is: Modularity Theorem

Unfortunately no satisfactory theorem except in a few cases:

Second Motivation to study $\mathrm{X}_0(\mathrm{N})(K)$

Recall that one of the main things to solve FLT over higher degree number fields is: Modularity Theorem

Unfortunately no satisfactory theorem except in a few cases:

1. E.C. over real quadratic fields are modular by Freitas, Le Hung and Siksek

Second Motivation to study $X_0(N)(K)$

Recall that one of the main things to solve FLT over higher degree number fields is: Modularity Theorem

Unfortunately no satisfactory theorem except in a few cases:

1. E.C. over real quadratic fields are modular by Freitas, Le Hung and Siksek
2. E.C. over totally real cubic fields are modular by Derickx, Najman and Siksek

Second Motivation to study $X_0(N)(K)$

Recall that one of the main things to solve FLT over higher degree number fields is: Modularity Theorem

Unfortunately no satisfactory theorem except in a few cases:

1. E.C. over real quadratic fields are modular by Freitas, Le Hung and Siksek
2. E.C. over totally real cubic fields are modular by Derickx, Najman and Siksek
3. $\mathbb{Q}$-curves are modular by Khare and Wintenberger

Second Motivation to study $X_0(N)(K)$

Recall that one of the main things to solve FLT over higher degree number fields is: Modularity Theorem

Unfortunately no satisfactory theorem except in a few cases:

1. E.C. over real quadratic fields are modular by Freitas, Le Hung and Siksek
2. E.C. over totally real cubic fields are modular by Derickx, Najman and Siksek
3. $\mathbb{Q}$-curves are modular by Khare and Wintenberger

Definition (Quadratic $\mathbb{Q}$-curve)

A $\mathbb{Q}$-curve is an elliptic curve over a number field K which is isogenous to all of its Galois conjugates.

Second Motivation to study $X_0(N)(K)$

Recall that one of the main things to solve FLT over higher degree number fields is: Modularity Theorem

Unfortunately no satisfactory theorem except in a few cases:

1. E.C. over real quadratic fields are modular by Freitas, Le Hung and Siksek
2. E.C. over totally real cubic fields are modular by Derickx, Najman and Siksek
3. $\mathbb{Q}$-curves are modular by Khare and Wintenberger

Definition (Quadratic $\mathbb{Q}$-curve)

A $\mathbb{Q}$-curve is an elliptic curve over a number field K which is isogenous to all of its Galois conjugates. If K is quadratic we say that E is a quadratic $\mathbb{Q}$-curve.

Application to Diophantine Eqns.

Recall: If (a, b, c) is a solution to FLT_p then:

$y^2 = x(x - a^p)(x + b^p)$ would have very unusual properties.

Application to Diophantine Eqns.

Recall: If (a, b, c) is a solution to FLT_p then:

$y^2 = x(x - a^p)(x + b^p)$ would have very unusual properties.

Similarly: say (A, B, C) is a solution to $A^4 + B^2 = C^p$ then:

the $\mathbb{Q}$-curve $E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$

would have very unusual properties. (Ellenberg-Skinner)

Application to Diophantine Eqns.

Recall: If (a, b, c) is a solution to FLT_p then:

$y^2 = x(x - a^p)(x + b^p)$ would have very unusual properties.

Similarly: say (A, B, C) is a solution to $A^4 + B^2 = C^p$ then:

the $\mathbb{Q}$-curve $E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$

would have very unusual properties. (Ellenberg-Skinner)

Since E is a $\mathbb{Q}$-curve we know it is modular, run the modular approach to get:

Application to Diophantine Eqns.

Recall: If (a, b, c) is a solution to FLT_p then:

$y^2 = x(x - a^p)(x + b^p)$ would have very unusual properties.

Similarly: say (A, B, C) is a solution to $A^4 + B^2 = C^p$ then:

the $\mathbb{Q}$-curve $E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$

would have very unusual properties. (Ellenberg-Skinner)

Since E is a $\mathbb{Q}$-curve we know it is modular, run the modular approach to get:

Theorem (Ellenberg)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

Application to Diophantine Eqns.

Recall: If (a, b, c) is a solution to FLT_p then:

$y^2 = x(x - a^p)(x + b^p)$ would have very unusual properties.

Similarly: say (A, B, C) is a solution to $A^4 + B^2 = C^p$ then:

the $\mathbb{Q}$-curve $E_{A,B,C} : y^2 = x^3 + 2(1 + i)Ax^2 + (B + iA^2)x$

would have very unusual properties. (Ellenberg-Skinner)

Since E is a $\mathbb{Q}$-curve we know it is modular, run the modular approach to get:

Theorem (Ellenberg)

There are no three positive integers A, B, and C which satisfy the equation $A^4 + B^2 = C^p$ for any value of p greater than 211.

How to parametrize $\mathbb{Q}$-curves?

Twists of $X_0(N)$

Recall that:
$X_0(N)$ is moduli space of $(E, \phi : E \to E'), \ker(\phi) \cong \mathbb{Z}/N\mathbb{Z}$

Twists of $X_0(N)$

Recall that:
$X_0(N)$ is moduli space of $(E, \phi : E \to E'), \ker(\phi) \cong \mathbb{Z}/N\mathbb{Z}$
We need a moduli space which parametrizes quadratic $\mathbb{Q}$-curves:

Twists of $X_0(N)$

Recall that:
$X_0(N)$ is moduli space of $(E, \phi : E \to E'), \ker(\phi) \cong \mathbb{Z}/N\mathbb{Z}$
We need a moduli space which parametrizes quadratic $\mathbb{Q}$-curves:
This is twist of $X_0(N)$ by w_N.

Definition

Given a curve X over $\mathbb{Q}$ its *twist* is another curve over $\mathbb{Q}$ that is isomorphic to X over $\bar{\mathbb{Q}}$.

Twists of $X_0(N)$

Recall that:
$X_0(N)$ is moduli space of $(E, \phi : E \to E'), \ker(\phi) \cong \mathbb{Z}/N\mathbb{Z}$
We need a moduli space which parametrizes quadratic $\mathbb{Q}$-curves:
This is twist of $X_0(N)$ by w_N.

Definition

Given a curve X over $\mathbb{Q}$ its *twist* is another curve over $\mathbb{Q}$ that is isomorphic to X over $\bar{\mathbb{Q}}$.

Remark

Geometrically a curve and its twist are the same.
but arithmetically not... action of Gal$(\bar{\mathbb{Q}}/\mathbb{Q})$ differs.

Twists$(X/K) \Leftrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Aut}(X))$

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi : E \to E')$, $\ker \phi \cong \mathbb{Z}/N\mathbb{Z}$

Definition

Involution w_N on $X_0(N)$: $(E, \phi : E \to E') \mapsto (E', \hat{\phi} : E' \to E)$

Given $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$ and $\zeta_d : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(X_0(N))$ be the cocycle that sends τ to w_N.

Twist of $\mathrm{X_0(N)}$

Recall that $P \in \mathrm{X_0(N)} \Leftrightarrow (E, \phi : E \to E')$, $\ker \phi \cong \mathbb{Z}/N\mathbb{Z}$

Definition

Involution w_N on $\mathrm{X_0(N)}$: $(E, \phi : E \to E') \mapsto (E', \hat{\phi} : E' \to E)$

Given $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$ and
$\zeta_d : \mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{X_0(N)})$ be the cocycle that sends τ to w_N.
Redefine the action of τ on $\mathrm{X_0(N)}$ as:

Twist of $\mathrm{X_0(N)}$

Recall that $P \in \mathrm{X_0(N)} \Leftrightarrow (E, \phi : E \to E')$, $\ker \phi \cong \mathbb{Z}/N\mathbb{Z}$

Definition

Involution w_N on $\mathrm{X_0(N)}$: $(E, \phi : E \to E') \mapsto (E', \hat{\phi} : E' \to E)$

Given $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$ and $\zeta_d : \mathrm{Gal(K/\mathbb{Q})} \to \mathrm{Aut(X_0(N))}$ be the cocycle that sends τ to w_N.
Redefine the action of τ on $\mathrm{X_0(N)}$ as: $P^\tau := w_N \circ \tau(P)$.

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi : E \to E')$, $\ker \phi \cong \mathbb{Z}/N\mathbb{Z}$

Definition

Involution w_N on $X_0(N)$: $(E, \phi : E \to E') \mapsto (E', \hat{\phi} : E' \to E)$

Given $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$ and
$\zeta_d : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(X_0(N))$ be the cocycle that sends τ to w_N.
Redefine the action of τ on $X_0(N)$ as: $P^\tau := w_N \circ \tau(P)$.

Definition

The curve $X_0^d(N)$ is the twist of $X_0(N)$ by ζ_d. In particular rational points of $X_0^d(N)$ are K-rational points of $X_0(N)$ fixed by $\tau \circ w_N$.

- $X_0(N)$ and $X_0^d(N)$ are isomorphic over K.

Twist of $X_0(N)$

Recall that $P \in X_0(N) \Leftrightarrow (E, \phi : E \to E')$, $\ker \phi \cong \mathbb{Z}/N\mathbb{Z}$

Definition

Involution w_N on $X_0(N)$: $(E, \phi : E \to E') \mapsto (E', \hat{\phi} : E' \to E)$

Given $K := \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$ and
$\zeta_d : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(X_0(N))$ be the cocycle that sends τ to w_N.
Redefine the action of τ on $X_0(N)$ as: $P^\tau := w_N \circ \tau(P)$.

Definition

The curve $X_0^d(N)$ is the twist of $X_0(N)$ by ζ_d. In particular rational points of $X_0^d(N)$ are K-rational points of $X_0(N)$ fixed by $\tau \circ w_N$.

- $X_0(N)$ and $X_0^d(N)$ are isomorphic over K.
- $X_0^d(N)$ is also a moduli space!

$X_0^d(N)(\mathbb{Q}) \Leftrightarrow$ Quadratic $\mathbb{Q}$-curves of degree N defined over K

Field of Definition

Let E be a quadratic $\mathbb{Q}$-curve of degree N defined over $\mathbb{Q}(\sqrt{d})$ then:

E corresponds to a $P \in \mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q})$.

Field of Definition

Let E be a quadratic $\mathbb{Q}$-curve of degree N defined over $\mathbb{Q}(\sqrt{d})$ then:

E corresponds to a $P \in \mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q})$.

For which (d, N), $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}) \neq \emptyset$?

Field of Definition

Let E be a quadratic $\mathbb{Q}$-curve of degree N defined over $\mathbb{Q}(\sqrt{d})$ then:

E corresponds to a $P \in \mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q})$.

For which (d, N), $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}) \neq \emptyset$?

Quick answer: *Not for all d and N*.

Field of Definition

Let E be a quadratic $\mathbb{Q}$-curve of degree N defined over $\mathbb{Q}(\sqrt{d})$ then:

E corresponds to a $P \in \mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q})$.

For which (d, N), $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}) \neq \emptyset$?

Quick answer: *Not for all d and N*.

Remark: $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}) \subset \mathrm{X}_0(\mathrm{N})(\mathbb{Q}(\sqrt{d}))$.
$\mathbb{Q}$-pnts of $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ are K-rational pnts of $\mathrm{X}_0(\mathrm{N})$ fixed by $\tau \circ w_N$.

Local Points

Checking all the *local points* is the first thing to do.

Local Points

Checking all the *local points* is the first thing to do.

Given a curve C, if $P \in C(\mathbb{Q})$ then $P \in C(\mathbb{Q}_p)$. What about the reverse?

Local Points

Checking all the *local points* is the first thing to do.

Given a curve C, if $P \in C(\mathbb{Q})$ then $P \in C(\mathbb{Q}_p)$. What about the reverse?

Definition

If a curve C has real and $\mathbb{Q}_p$-points for every prime p but no $\mathbb{Q}$-points then we say that C violates **the Hasse Principle.**

A conic never violates the Hasse Principle but for higher genus curves there are many examples of the violation.

Checking all the *local points* is the first thing to do.

Question 1: Given (N, d, p) what can be said about $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$?

Checking all the *local points* is the first thing to do.

Question 1: Given (N, d, p) what can be said about $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$?

- **Theorem**[O.] There are explicit (and easy to check) conditions such that $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$ is non-empty if and only if the conditions hold.

Checking all the *local points* is the first thing to do.

Question 1: Given (N, d, p) what can be said about $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$?

- **Theorem**[O.] There are explicit (and easy to check) conditions such that $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$ is non-empty if and only if the conditions hold.

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle?

Checking all the *local points* is the first thing to do.

Question 1: Given (N, d, p) what can be said about $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$?

- **Theorem**[O.] There are explicit (and easy to check) conditions such that $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$ is non-empty if and only if the conditions hold.

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle?

- **Theorem**[O.] Given N, the number of the twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse Principle is given by an explicit asymptotic. In particular they have positive density.

Checking all the *local points* is the first thing to do.

Question 1: Given (N, d, p) what can be said about $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$?

- **Theorem**[O.] There are explicit (and easy to check) conditions such that $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})(\mathbb{Q}_p)$ is non-empty if and only if the conditions hold.

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle?

- **Theorem**[O.] Given N, the number of the twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse Principle is given by an explicit asymptotic. In particular they have positive density.

Example (Quadratic twists)

Given a prime number $N \equiv 1 \bmod 4$ and a positive integer Z, let A be the set of positive squarefree integers $d \leq Z$ such that the quadratic twist by $\mathrm{K} = \mathbb{Q}(\sqrt{d})$ and w_N violates the Hasse principle. If $N > 131$, the size of A is asymptotically $C_N \frac{Z}{\log^{1-\alpha_N} Z}$.

Hasse Principle Violations $g \geq 2$

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle? YES

Hasse Principle Violations $g \geq 2$

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle? YES

Question 3: What are the reasons of such violations?

Hasse Principle Violations $g \geq 2$

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle? YES

Question 3: What are the reasons of such violations?

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve:

Hasse Principle Violations $g \geq 2$

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle? YES

Question 3: What are the reasons of such violations?

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve:

$$X(\mathbb{Q}) \quad \xrightarrow{P \mapsto [P] - D} \quad \mathrm{Jac}(\mathbb{Q})$$

Hasse Principle Violations $g \geq 2$

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle? YES

Question 3: What are the reasons of such violations?

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve:

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{P \mapsto [P]-D} & \mathrm{Jac}(\mathbb{Q}) \\ \downarrow_{\mathrm{red}} & & \downarrow_{\mathrm{red}} \\ \prod_{p \in S} X(\mathbb{F}_p) & & \end{array}$$

Hasse Principle Violations $g \geq 2$

Question 2: Is there an asymptotic for the number of twists $\mathrm{X}_0^{\mathrm{d}}(\mathrm{N})$ which violate the Hasse principle? YES

Question 3: What are the reasons of such violations?

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve:

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{P \mapsto [P]-D} & \mathrm{Jac}(\mathbb{Q}) \\ \downarrow \mathrm{red} & & \downarrow \mathrm{red} \\ \prod_{p \in S} X(\mathbb{F}_p) & \xrightarrow{\mathrm{inj}} & \prod_{p \in S} \mathrm{Jac}(\mathbb{F}_p) \end{array}$$

- If P in $X(\mathbb{Q})$ then $\mathrm{red}([P]-D)$ is in $\mathrm{inj}(X(\mathbb{F}_p))$ for any p in S.
- If images of red and inj do not intersect then $X(\mathbb{Q}) = \emptyset$.

Hasse Principle Violations $g = 1$

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve.

Hasse Principle Violations $g = 1$

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve.
- When $\mathrm{X}_0(\mathrm{N})$ is an elliptic curve, w_N sends a point x of $\mathrm{X}_0(\mathrm{N})$ to $-x + S$ for a fixed $S \in \mathrm{X}_0(\mathrm{N})(\mathbb{Q})$.

Hasse Principle Violations $g = 1$

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve.
- When $\mathrm{X_0(N)}$ is an elliptic curve, w_N sends a point x of $\mathrm{X_0(N)}$ to $-x + S$ for a fixed $S \in \mathrm{X_0(N)}(\mathbb{Q})$.
- The rational points on the quadratic twist $\mathrm{X_0^d(N)}$ are:

$$\mathrm{X_0^d(N)}(\mathbb{Q}) = \{P \in \mathrm{X_0(N)}(\mathbb{Q}(\sqrt{d}))|\tau(P) = -P + S\}$$

where τ is the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.

Hasse Principle Violations $g = 1$

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve.
- When $\mathrm{X_0(N)}$ is an elliptic curve, w_N sends a point x of $\mathrm{X_0(N)}$ to $-x + S$ for a fixed $S \in \mathrm{X_0(N)}(\mathbb{Q})$.
- The rational points on the quadratic twist $\mathrm{X_0^d(N)}$ are:

$$\mathrm{X_0^d(N)}(\mathbb{Q}) = \{P \in \mathrm{X_0(N)}(\mathbb{Q}(\sqrt{d}))|\tau(P) = -P + S\}$$

  where τ is the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.
- $\mathrm{X_0^d(N)}(\mathbb{Q}) \neq \emptyset \leftrightarrow$

$$S \in \mathrm{im}\,(\mathrm{tr_{K/\mathbb{Q}}} = 1 + \tau) : \mathrm{X_0(N)}(\mathbb{Q}(\sqrt{d})) \to \mathrm{X_0(N)}(\mathbb{Q}).$$

Hasse Principle Violations $g = 1$

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve.
- When $\mathrm{X_0(N)}$ is an elliptic curve, w_N sends a point x of $\mathrm{X_0(N)}$ to $-x + S$ for a fixed $S \in \mathrm{X_0(N)}(\mathbb{Q})$.
- The rational points on the quadratic twist $\mathrm{X_0^d(N)}$ are:

$$\mathrm{X_0^d(N)}(\mathbb{Q}) = \{P \in \mathrm{X_0(N)}(\mathbb{Q}(\sqrt{d}))|\tau(P) = -P + S\}$$

  where τ is the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.
- $\mathrm{X_0^d(N)}(\mathbb{Q}) \neq \emptyset \leftrightarrow$

$$S \in \mathrm{im}\,(\mathrm{tr_{K/\mathbb{Q}}} = 1 + \tau) : \mathrm{X_0(N)}(\mathbb{Q}(\sqrt{d})) \to \mathrm{X_0(N)}(\mathbb{Q}).$$

- Similarly, $\mathrm{X_0^d(N)}(\mathbb{Q}_p)$ is non-empty $\leftrightarrow$ S is in the image of the local trace map.

Hasse Principle Violations $g = 1$

- Typically when X is a curve of genus $g \geq 2$ we use a method called Mordell-Weil Sieve.
- When $\mathrm{X_0(N)}$ is an elliptic curve, w_N sends a point x of $\mathrm{X_0(N)}$ to $-x + S$ for a fixed $S \in \mathrm{X_0(N)}(\mathbb{Q})$.
- The rational points on the quadratic twist $\mathrm{X_0^d(N)}$ are:

$$\mathrm{X_0^d(N)}(\mathbb{Q}) = \{P \in \mathrm{X_0(N)}(\mathbb{Q}(\sqrt{d}))|\tau(P) = -P + S\}$$

  where τ is the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$.
- $\mathrm{X_0^d(N)}(\mathbb{Q}) \neq \emptyset \leftrightarrow$

$$S \in \mathrm{im}\,(\mathrm{tr}_{\mathrm{K}/\mathbb{Q}} = 1 + \tau) : \mathrm{X_0(N)}(\mathbb{Q}(\sqrt{d})) \to \mathrm{X_0(N)}(\mathbb{Q}).$$

- Similarly, $\mathrm{X_0^d(N)}(\mathbb{Q}_p)$ is non-empty $\leftrightarrow$ S is in the image of the local trace map.

$\mathrm{X_0^d(N)}$ violates the Hasse principle if and only if there exists a local-global trace obstruction for S.

Trace Question

Question: Let $S \in \mathrm{E}(\mathbb{Q})$ such that S lies in the image of the local trace maps for every prime p of $\mathbb{Q}$. Is the point S in the image of the global trace map?

Trace Question

Question: Let $S \in \mathrm{E}(\mathbb{Q})$ such that S lies in the image of the local trace maps for every prime p of $\mathbb{Q}$. Is the point S in the image of the global trace map?

Theorem (Çiperiani, O.)

- *Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve with non-trivial rational 2-torsion. Under some technical assumptions, the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})_2$ if and only if $\mathrm{E}(\mathrm{K})_2 \neq \mathrm{E}(\mathbb{Q})_2$ or $2\mathrm{E}^d(\mathbb{Q}) \neq \mathrm{E}^d(\mathbb{Q}) \cap 2\mathrm{E}^d(\mathrm{K})$.*

Trace Question

Question: Let $S \in \mathrm{E}(\mathbb{Q})$ such that S lies in the image of the local trace maps for every prime p of $\mathbb{Q}$. Is the point S in the image of the global trace map?

Theorem (Çiperiani, O.)

- *Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve with non-trivial rational 2-torsion. Under some technical assumptions, the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})_2$ if and only if $\mathrm{E}(\mathrm{K})_2 \neq \mathrm{E}(\mathbb{Q})_2$ or $2\mathrm{E}^d(\mathbb{Q}) \neq \mathrm{E}^d(\mathbb{Q}) \cap 2\mathrm{E}^d(\mathrm{K})$.*
- *If the local-global trace principle holds for $\mathrm{E}(\mathbb{Q})_2$, then a local trace P is a global trace if and only if certain points in the quadratic twist of E are 2-divisible.*

Trace Question for points that are not 2 torsion

Theorem (Çiperiani, O.)

Let $P \in \mathrm{E}(\mathbb{Q})$ be a local trace at all primes. If the local to global trace criterion holds for $\mathrm{E}(\mathbb{Q})_2$ then P is a global trace if and only if $i(P) \in 2\mathrm{E}^d(\mathrm{K}) + \mathrm{E}^d(\mathbb{Q})$ where $i : \mathrm{E} \to \mathrm{E}^d$ is the isomorphism over K.

Trace Question for points that are not 2 torsion

Theorem (Çiperiani, O.)

Let $P \in \mathrm{E}(\mathbb{Q})$ be a local trace at all primes. If the local to global trace criterion holds for $\mathrm{E}(\mathbb{Q})_2$ then P is a global trace if and only if $i(P) \in 2\mathrm{E}^d(\mathrm{K}) + \mathrm{E}^d(\mathbb{Q})$ where $i : \mathrm{E} \to \mathrm{E}^d$ is the isomorphism over K.

- Check if there is trace obstruction for 2-torsion points.

Trace Question for points that are not 2 torsion

Theorem (Çiperiani, O.)

Let $P \in \mathrm{E}(\mathbb{Q})$ be a local trace at all primes. If the local to global trace criterion holds for $\mathrm{E}(\mathbb{Q})_2$ then P is a global trace if and only if $i(P) \in 2\mathrm{E}^d(\mathrm{K}) + \mathrm{E}^d(\mathbb{Q})$ where $i : \mathrm{E} \to \mathrm{E}^d$ is the isomorphism over K.

- Check if there is trace obstruction for 2-torsion points.
- If not, then there is no trace obstruction for a non-torsion point P if and only if $i(P)$ is 2-divisible over K nontrivially.

To Wrap Up

Trying to understand solutions of Fermat type equations may lead you to questions about:

- points of $X_0(N)$ over higher degree number fields

To Wrap Up

Trying to understand solutions of Fermat type equations may lead you to questions about:

- points of $X_0(N)$ over higher degree number fields
- modularity of special elliptic curves ($\mathbb{Q}$-curves)

To Wrap Up

Trying to understand solutions of Fermat type equations may lead you to questions about:

- points of $X_0(N)$ over higher degree number fields
- modularity of special elliptic curves ($\mathbb{Q}$-curves)
- rational points on twists of $X_0(N)$ and Hasse principle violations

To Wrap Up

Trying to understand solutions of Fermat type equations may lead you to questions about:

- points of $X_0(N)$ over higher degree number fields
- modularity of special elliptic curves ($\mathbb{Q}$-curves)
- rational points on twists of $X_0(N)$ and Hasse principle violations
- trace obstruction questions about elliptic curves

To Wrap Up

Trying to understand solutions of Fermat type equations may lead you to questions about:

- points of $X_0(N)$ over higher degree number fields
- modularity of special elliptic curves ($\mathbb{Q}$-curves)
- rational points on twists of $X_0(N)$ and Hasse principle violations
- trace obstruction questions about elliptic curves
  among many others....

To Wrap Up

Trying to understand solutions of Fermat type equations may lead you to questions about:

- points of $X_0(N)$ over higher degree number fields
- modularity of special elliptic curves ($\mathbb{Q}$-curves)
- rational points on twists of $X_0(N)$ and Hasse principle violations
- trace obstruction questions about elliptic curves among many others....

Epilogue From Barry Mazur:

Trying to understand solutions of Fermat type equations may lead you to questions about:

- points of $X_0(N)$ over higher degree number fields
- modularity of special elliptic curves ($\mathbb{Q}$-curves)
- rational points on twists of $X_0(N)$ and Hasse principle violations
- trace obstruction questions about elliptic curves among many others....

Epilogue From Barry Mazur: *'Number theory produces, without effort, innumerable problems which have a sweet, innocent air about them, tempting flowers; and yet ... number theory swarms with bugs, waiting to bite the tempted flower-lovers who, once bitten, are inspired to excess of effort!. '*