Quadratic Points on Modular Curves and Fermat-type Equations

Ekin Özman

Bogazici University

June 8, 2021

Diophantine Equations and the Absolute Galois group

One of the most famous problems in number theory is :
Finding solutions of Diophantine Equations

- $x^n + y^n + z^n = 0 \Rightarrow$ Fermat's Equation
- $Ax^n + By^n + Cz^n = 0 \Rightarrow$ Generalized Fermat's Equation
- $x^m + y^n + z^k = 0 \Rightarrow$ "twisted" Fermat's Equation

Absolute Galois group of $\mathbb{Q}$, $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Understand this!
To understand $G_{\mathbb{Q}}$ we look at its representations:

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

Let $E[p]$ be the p-torsion subgroup in $E(\mathbb{C})$, $G_{\mathbb{Q}}$ acts on $E[p]$.
We obtain a representation

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

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:

- 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)

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

Irreducibility of Galois representations(Mazur)

A key ingredient in 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 :

$$\{\text{Non-cuspidal points on } \mathrm{X}_0(\mathrm{p})\}$$

$$\Updownarrow$$

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

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

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

$$\Updownarrow$$

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

Theorem (Mazur)

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

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

Understanding $X_0(N)(K)$

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

- $\diamond$ $X_1(N)(K) \Leftrightarrow (E, P)$ where $E_{/K}$ and $P \in E[N](K)$.
- $\diamond$ $X_0(N)(K) \Leftrightarrow$ reducible $\rho_{E,p}$ 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 $\mathrm{X_0(N)}(K)$

Definition

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

- **Bars, Harris-Silverman:** If $g(\mathrm{X_0(N)}) \geq 2$ then $\mathrm{X_0(N)}$ has finitely many quadratic points except for 28 values of N.
- **Bruin, Najman:** parametrized all quadratic points on $\mathrm{X_0(N)}$ such that $J_0(N)$ has MW rank 0 and $\mathrm{X_0(N)}$ is hyperelliptic:

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

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

Theorem (O., Siksek)

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

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

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

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

Understanding $X_0(N)(K)$

Recently:

Theorem (Box)

Found and parametrized all quadratic points on $X_0(N)$ such that

- $J_0(N)$ *has positive MW rank,*
- $X_0(N)$ *nonhyperelliptic and*
- $2 \leq g(X_0(N)) \leq 5$*.*

Hence we have a full list of all quadratic points on $X_0(N)(K)$ for $2 \leq g(X_0(N)) \leq 5$

Why is this helpful?

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 $\mathrm{X}_0(34)$

⋄ 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

$$\begin{tikzcd} P_1 \arrow[r, dash, "w_{34}"] \arrow[d, dash, "w_{17}"'] \arrow[dr, dash, "w_2"] & P_2 \arrow[d, dash] \arrow[dl, dash] \\ P_1^\sigma \arrow[r, dash] & P_2^\sigma \end{tikzcd} \qquad \begin{tikzcd} P_5 \arrow[r, dash, "w_{34}"] \arrow[d, dash, "w_2"'] \arrow[dr, dash, "w_{17}"] & P_6 \arrow[d, dash] \arrow[dl, dash] \\ P_5^\sigma \arrow[r, dash] & P_6^\sigma \end{tikzcd} \qquad \begin{tikzcd} P_3 \arrow[r, dash, "w_2"] \arrow[d, Rightarrow, dash, "w_{17},w_{34}"] & P_3 \arrow[d, Rightarrow, dash, "w_{17},w_{34}"] \\ P_3^\sigma \arrow[r, dash, "w_2"] & P_3^\sigma \end{tikzcd} \qquad \begin{tikzcd} P_4 \arrow[r, dash, "w_2"] \arrow[d, Rightarrow, dash, "w_{17},w_{34}"] & P_4 \arrow[d, Rightarrow, dash, "w_{17},w_{34}"] \\ P_4^\sigma \arrow[r, dash, "w_2"] & P_4^\sigma \end{tikzcd}$$

Theoretical Approach

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

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

- ◇ $X^{(2)}$, 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 $P_1, P_2 \in X(K)$ and $P_1 = \bar{P}_2$
- ◇ $D_P = P_1 + P_2$ when $P = \{P_1, P_2\}$.

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 $X^{(2)}(\mathbb{Q})$

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

- any $P = \{P_1, P_2\}$ in $X^{(2)}(\mathbb{Q}) \rightsquigarrow D_P = P_1 + P_2 \sim D' + 2P_0$ for some $[D'] \in J_X(\mathbb{Q}), D' \in Div^0(X)(\mathbb{Q})$
- 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 $\mathrm{J_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{tors}}$
- Even if this is done, $\mathrm{J_0(N)(\mathbb{Q})_{tors}}$ can be huge and Riemann-Roch computations can be complicated

Our Approach:

1. Compute $C_0(N) \leq \mathrm{J_0(N)(\mathbb{Q})}$ where $C_0(N)$ is the rational cuspidal group
2. Bound its index inside $\mathrm{J_0(N)(\mathbb{Q})}$ by I, so $I.\mathrm{J_0(N)(\mathbb{Q})} \subset C$
3. so the effective 2 divs we seek satisfy: $[D - 2P_0] = I[D']$ where $D' \in \mathrm{J_0(N)(\mathbb{Q})}$.
4. Apply a version of MW sieve to eliminate most possibilities for D'.
5. only then use Riemann Roch.

Rational Cuspidal Group, $C_0(N)(\mathbb{Q})$

- $C_0(N) \leq J_0(N)(\overline{\mathbb{Q}})$; generated by classes of differences of cusps; *the cuspidal subgroup.*
- $C_0(N)(\mathbb{Q}) \leq C_0(N)$; grp of points stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; *the rational cuspidal subgroup.*

  ◇ $C_0(N)(\mathbb{Q}) \leq J_0(N)(\mathbb{Q})$

  ◇ Manin-Drinfeld thm: $C_0(N) \subseteq J_0(N)(\overline{\mathbb{Q}})_{\mathrm{tors}}$, and thus $C_0(N)(\mathbb{Q}) \subseteq J_0(N)(\mathbb{Q})_{\mathrm{tors}}$.
- conj. of Ogg, proved by Mazur: $C_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ for N prime.
- generalized Ogg conj.: $C_0(N)(\mathbb{Q}) = J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ for all N.

Theorem (O., Siksek)

The generalized Ogg conjecture holds for $N = 34, 38, 44, 45, 51, 52, 54, 56, 64, 81$.

Rational Cuspidal Group, $C_0(N)(\mathbb{Q})$

Write $X = \mathrm{X}_0(\mathrm{N}), J = J_0(N), C = C_0(N)(\mathbb{Q})$.
Fix a degree 1 cusp place, denoted by $\mathcal{P}_0$ (e.g. ∞ or 0 cusp).
Let $\mathcal{P}_1, \ldots, \mathcal{P}_r$ be the other cusp places.
C is generated by $[\mathcal{P}_i - \deg(\mathcal{P}_i) \cdot \mathcal{P}_0]$ in $\mathrm{Pic}^0(X/\mathbb{Q}) \cong J(\mathbb{Q})$.
To determine the structure of C:

- choose a prime $p \nmid 2N$
- compute using `Magma` $\mathrm{Pic}^0(X/\mathbb{F}_p) \cong J(\mathbb{F}_p)$
- The images of the classes $[\mathcal{P}_i - \deg(\mathcal{P}_i) \cdot \mathcal{P}_0]$ under the composition

$$C(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})_{\mathrm{tors}} \hookrightarrow J(\mathbb{Q}) \hookrightarrow J(\mathbb{F}_p)$$

  generate a subgroup of $J(\mathbb{F}_p)$ that is isomorphic to C.

Details of Computing possibilities $J_0(N)(\mathbb{Q})$

$X = \mathrm{X_0(N)}, J = J_0(N), C = C_0(N)(\mathbb{Q})$
$C \subset J(\mathbb{Q})_{tors} = J(\mathbb{Q}) \hookrightarrow J(\mathbb{F}_p)$ for, $p \nmid 2N$

$\mathcal{A}'_p := \{\iota : C \to A\}$ where

- $A \leq J(\mathbb{F}_p)$
- $\mathrm{red}_p(C) \subset A$ and
- ι is the restriction of the reduction red_p map to C.

For *some* $\iota \in \mathcal{A}'_p$:

$$\begin{tikzcd}
C \arrow[r, hook] \arrow[d, "\iota"'] & J(\mathbb{Q}) \arrow[d, "\text{red}"] \arrow[dl, equal, "\mu"] \\
A \arrow[r, hook] & J(\mathbb{F}_p)
\end{tikzcd}$$

where μ is an isomorphism.

Details of Computing possibilities $J_0(N)(\mathbb{Q})$

$g :=$ genus of X, $m := \#$ of real comps of J. By Gross and Harris:

$$J(\mathbb{Q}) \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}, \qquad d_1 \mid d_2 \mid \cdots \mid d_k$$

where $k \leq g$ or $g + 1 \leq k \leq g + m - 1$ and $d_i \in \{1, 2\}$.
Eliminate from $\mathcal{A}'_p$ all $\iota : C \to A$ where the isom. class of A is incompatible with this. Obtain a subset $\mathcal{A}_p$.
Let $p_1, \ldots, p_s$ be distinct primes $\nmid 2pN$.
$\mathcal{A}_{p;\, p_1,\ldots,p_s}$ set of $\iota : C \to A \in \mathcal{A}_p$ such that :

- For all $p' \in \{p_1, \ldots, p_s\}$ there exists $\iota' : C \to A'$ in $\mathcal{A}_{p'}$ and
- an isomorphism $\psi : A \to A'$
- making the diagram

$$\begin{tikzcd} C \arrow[r, "\iota"] \arrow[dr, "\iota'"'] & A \arrow[d, "\psi"] \\ & A' \end{tikzcd}$$

commute.

A group theory problem

Question

Let C, A, A' be finite abelian groups and suppose $\iota, \iota' : C \to A, A'$ are injective homomorphisms. is there is an isomorphism $\psi : A \to A'$ such that $\psi \circ \iota = \iota'$?

$$\begin{tikzcd} C \arrow[r, "\iota"] \arrow[dr, "\iota'"'] & A \arrow[d, "\psi"] \\ & A' \end{tikzcd}$$

It is possible to give an effective answer to this question.

Details of Computing possibilities $J_0(N)(\mathbb{Q})$

$\mathcal{A}_{p;\, p_1,\ldots,p_s}$ set of $\iota : C \to A \in \mathcal{A}_p$ such that :
For all $p' \in \{p_1, \ldots, p_s\} \exists \iota' : C \to A'$ in $\mathcal{A}_{p'}$ and an isom. $\psi : A \to A'$ making the diagram commute.

$$\begin{tikzcd} C \arrow[r, "\iota"] \arrow[dr, "\iota'"'] & A \arrow[d, "\psi"] \\ & A' \end{tikzcd}$$

$\mathcal{A}_{p;p_1,\ldots,p_s}$ must contain some $\iota_0 : C \to A_0$, where $A_0 = \mathrm{red}_p(C)$

$$\begin{tikzcd} C \arrow[r, hook] \arrow[d, "\iota_0"'] & J(\mathbb{Q}) \arrow[d, "\text{red}"] \arrow[dl, equal, "\mu"] \\ A_0 \arrow[r, hook] & J(\mathbb{F}_p) \end{tikzcd}$$

Aim: to find suitable $p, p_1, \ldots, p_s$ s.t. $\#\mathcal{A}_{p;p_1,\ldots,p_s} = 1$, this is necessarily ι_0, hence $J(\mathbb{Q}) = C$.
We know that $J(\mathbb{Q})/C \cong \mathrm{cokernel}(\iota)$ of some ι in $\mathcal{A}_{p;p_1,\ldots,p_s}$.
Hence we get a positive integer l such that $l \cdot J(\mathbb{Q}) \subseteq C$.

Aim: to find suitable p, $p_1, \ldots, p_s$ s.t. $\#\mathcal{A}_{p;p_1,\ldots,p_s} = 1$.
This is necessarily ι_0, hence $J(\mathbb{Q}) = C$.
Nevertheless;

- We know that $J(\mathbb{Q})/C \cong \mathrm{cokernel}(\iota)$ of some ι in $\mathcal{A}_{p;p_1,\ldots,p_s}$.
- Hence we get a positive integer I such that $I \cdot J(\mathbb{Q}) \subseteq C$.

For each value of N computed $\mathcal{A}_{p;p_1,\ldots,p_s}$ where

- p is the smallest prime not dividing $2N$, and
- $p_1, \ldots, p_s$ are the primes ≤ 17 not dividing $2pN$.

Finding quadratic points

Now we know all the possible G for $G = J(\mathbb{Q})/C$.

- $I := \mathrm{LCM}$ of the exponents of G, thus $I \cdot J(\mathbb{Q}) \subseteq C$.
- $X(\mathbb{Q})$ is known, so $\mathcal{K}_0 := \{P + Q | P, Q \in \mathrm{X_0(N)}(\mathbb{Q})\}$ set of effective degree 2 divisors is known.
- Find a few quadratic pnts P on X and enlarge $\mathcal{K}_0$ be adjoining $P + P^\sigma$ where P^σ is Galois conjugate of P. Obtain $\mathcal{K}$ known set of degree 2 divisors on X.
- apply a special MW sieve for a suitable choice of primes $p_1, \ldots, p_r \geq 3$ of good reduction,
- deduce a subset of $\mathcal{S} \subseteq J(\mathbb{Q})$ that contains the possibilities for $I \cdot [D - 2P_0]$ for $D \in X^{(2)}(\mathbb{Q}) \setminus \mathcal{K}$.
- In almost all cases we found $\mathcal{S} = \emptyset$ and thus $X^{(2)}(\mathbb{Q}) = \mathcal{K}$

Final Word

Theorem (O., Siksek)

For

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

$X_0(N)(\mathbb{Q}(\sqrt{d}))$ *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 $|d| > B, X_0(N)$ doesn't have any non-rational quadratic points for any N? (Say genus of $X_0(N) > 2$)