Sieving for quadratic points on bielliptic curves

Philippe Michaud-Jacobs

University of Warwick

Representation Theory XVIII
Dubrovnik
19th June 2023

"There has been much recent interest in computing quadratic points on the curves $X_0(N)$" — me.

Is this true? **Yes!**

- Ozman and Siksek. Quadratic Points on Modular Curves, 2018.
- Box. Quadratic points on modular curves with infinite Mordell–Weil group, 2019.
- Najman and Trbović. Splitting of primes in number fields generated by points on some modular curves, 2020.
- Banwait. Explicit isogenies of prime degree over quadratic fields, 2021.
- M. Fermat's Last Theorem and modular curves over real quadratic fields, 2021.
- Najman and Vukorepa. Quadratic points on bielliptic modular curves, 2021.
- M. On elliptic curves with p-isogenies over quadratic fields, 2022.
- Banwait and Derickx. Explicit isogenies of prime degree over number fields, 2022.
- Vukorepa. Isogenies over quadratic fields of elliptic curves with rational j-invariant, 2022.
- Banwait, Najman, Padurariu. Cyclic isogenies of elliptic curves over fixed quadratic fields, 2022.
- Adžaga, Keller, Najman, M., Ozman, and Vukorepa. Computing quadratic points on modular curves $X_0(N)$, 2023.

Why?

- Mazur and Kenku looked after the case of rational points on $X_0(N)$ a long time ago and quadratic points are the next best thing. ☹
- Studying quadratic points on $X_0(N)$ is hard enough to be interesting, but not too hard.

- Deepen our understanding of modular curves.
- Develop techniques for studying low-degree points on curves.
- Deepen our understanding of the arithmetic of elliptic curves and their Galois representations.
- Concrete applications to the modular method for solving Diophantine equations.

Computing quadratic points

A quadratic point on a curve $X/\mathbb{Q}$ is a point

$$P \in X(\mathbb{Q}(\sqrt{d}))\backslash X(\mathbb{Q}).$$

We think of P with its Galois conjugate, P^σ.

What does **"computing the quadratic points on $X_0(N)$"** actually mean?

1. If $X_0(N)$ has **finitely** many quadratic points (as we range over all quadratic fields) then this means **writing them all down on an explicit model**.
2. If $X_0(N)$ has **infinitely** many quadratic points as we range over all quadratic fields then this means **writing down all the points that do not come from a 'geometric family'**.

Quadratic points have been computed on all $X_0(N)$ with $2 \leq g(X_0(N)) \leq 8$.

Bielliptic curves $X_0(N)$

Let $N \in \mathcal{N} = \{53, 61, 79, 83, 89, 101, 131\}$.

- $X_0(N)$ is bielliptic, with a degree 2 map defined over $\mathbb{Q}$:

$$\psi : X_0(N) \longrightarrow X_0^+(N) = X_0(N)/w_N.$$

- $X_0^+(N)$ is an elliptic curve over $\mathbb{Q}$ with

$$X_0^+(N)(\mathbb{Q}) = \langle R \rangle \cong \mathbb{Z}.$$

- Pulling back these points via ψ gives rise to infinitely many quadratic points on $X_0(N)$ as we range over all quadratic fields.

Theorem (Box, Najman–Vukorepa, 2021)

Let $N \in \mathcal{N}$ and let P be a quadratic point on $X_0(N)$. Then $\psi(P) = \psi(P^\sigma) \in X_0^+(N)(\mathbb{Q})$.

This result is **great**, but it does not determine $X_0(N)(\mathbb{Q}(\sqrt{d}))$ for a fixed quadratic field $\mathbb{Q}(\sqrt{d})$.

Theorem (M., 2023)

Let $N \in \mathcal{N} = \{53, 61, 79, 83, 89, 101, 131\}$. *Let* $d \in \mathbb{Z}$ *such that* $|d| < 100$. *Then*

$$\exists P \in X_0(N)(\mathbb{Q}(\sqrt{d})) \backslash X_0(N)(\mathbb{Q}) \iff d \in \mathcal{D}_N,$$

where

$$\mathcal{D}_{53} = \{-43, -11, -7, -1\}, \qquad \mathcal{D}_{61} = \{-19, -3, -1, 61\},$$
$$\mathcal{D}_{79} = \{-43, -7, -3\}, \qquad \mathcal{D}_{83} = \{-67, -43, -19, -2\},$$
$$\mathcal{D}_{89} = \{-67, -11, -2, -1, 89\}, \qquad \mathcal{D}_{101} = \{-43, -19, -1\},$$
$$\mathcal{D}_{131} = \{-67, -19, -2\}.$$

Write $X = X_0(N)$, $E = X_0^+(N)$, and $E(\mathbb{Q}) = \langle R \rangle$.

- **Know:** $P \in X(\mathbb{Q}(\sqrt{d}))$ and $\psi(P) = \psi(P^\sigma) = m \cdot R$.
- **Want:** information about m by investigating matters mod ℓ.

$$\begin{array}{ccc} X & \xrightarrow{\ \psi\ } & E \\ \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} \\ \widetilde{X} & \xrightarrow{\ \widetilde{\psi}\ } & \widetilde{E} \end{array} \qquad \begin{array}{ccc} P & \overset{\psi}{\longmapsto} & m \cdot R \\ \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} \\ \widetilde{P} & \overset{\widetilde{\psi}}{\longmapsto} & m \cdot \widetilde{R} \end{array}$$

- $\widetilde{\psi}(\widetilde{P}) = \widetilde{\psi}(\widetilde{P^\sigma}) = m \cdot \widetilde{R}$.
- Write G_ℓ for the order of $\widetilde{R}$ in $E(\mathbb{F}_\ell)$.
- $m \equiv m_0 \pmod{G_\ell}$ for some $m_0 \in \{0, 1, 2, \ldots, G_\ell - 1\}$.

Fix an $m_0 \in \{0, 1, 2, \ldots, G_\ell - 1\}$ and suppose $m \equiv m_0 \pmod{G_\ell}$.

$$\begin{array}{ccc} X & \xrightarrow{\psi} & E \\ \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} \\ \widetilde{X} & \xrightarrow{\widetilde{\psi}} & \widetilde{E} \end{array} \qquad \begin{array}{ccc} P & \overset{\psi}{\longmapsto} & m \cdot R \\ \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} \\ \widetilde{P} & \overset{\widetilde{\psi}}{\longmapsto} & m \cdot \widetilde{R} \end{array}$$

- Then $\widetilde{\psi}(\widetilde{P}) = \widetilde{\psi}(\widetilde{P^\sigma}) = m_0 \cdot \widetilde{R}$.
- So $\{\widetilde{P}, \widetilde{P^\sigma}\} = \widetilde{\psi}^{-1}(m_0 \cdot \widetilde{R}) \subset \widetilde{X}(\mathbb{F}_{\ell^2})$, a set which we can compute explicitly.
- $\widetilde{\psi}^{-1}(m_0 \cdot \widetilde{R})$ will either be:
    1. A pair of (distinct) points in $\widetilde{X}(\mathbb{F}_\ell)$.
    2. A pair of (distinct) points in $\widetilde{X}(\mathbb{F}_{\ell^2})$ (not in $\widetilde{X}(\mathbb{F}_\ell)$).
    3. A single point in $\widetilde{X}(\mathbb{F}_\ell)$.

- We are supposing $\{\widetilde{P}, \widetilde{P^\sigma}\} = \widetilde{\psi}^{-1}(m_0 \cdot \widetilde{R})$. Is this possible?

Using a nice explicit (diagonalised) model:

1. Suppose $\widetilde{\psi}^{-1}(m_0 \cdot \widetilde{R})$ is a pair of points in $\widetilde{X}(\mathbb{F}_\ell)$.
   If ℓ ramifies or is inert in $\mathbb{Q}(\sqrt{d})$ then $\{\widetilde{P}, \widetilde{P^\sigma}\}$ is a single $\mathbb{F}_\ell$-point or a pair of $\mathbb{F}_{\ell^2}$-points. Contradiction.
2. Suppose $\widetilde{\psi}^{-1}(m_0 \cdot \widetilde{R})$ is a pair of points in $\widetilde{X}(\mathbb{F}_{\ell^2})$.
   If ℓ ramifies or is split in $\mathbb{Q}(\sqrt{d})$ then $\{\widetilde{P}, \widetilde{P^\sigma}\}$ is a single $\mathbb{F}_\ell$-point or a pair of $\mathbb{F}_\ell$-points. Contradiction.
3. Suppose $\widetilde{\psi}^{-1}(m_0 \cdot \widetilde{R})$ is a single point in $\widetilde{X}(\mathbb{F}_\ell)$.
   We can't rule anything out here.

We try and rule out each $m_0 \in \{0, 1, 2, \ldots, G_\ell - 1\}$ to come up with a list of possibilities for $m \pmod{G_\ell}$.

So far: list of possibilities for $m \pmod{G_\ell}$.

- Repeat with several primes $\ell_1, \ell_2, \ldots, \ell_s$.
- No solution to systems of congruences $\Rightarrow$ **Contradiction**.

Let $X = X_0(53)$ and suppose $P \in X(\mathbb{Q}(\sqrt{-47}))\backslash X(\mathbb{Q})$.

- $\ell_1 = 5$ is inert in $\mathbb{Q}(\sqrt{-47})$ and $G_5 = 6$.
- So $\{\widetilde{P}, \widetilde{P^\sigma}\}$ is either a single $\mathbb{F}_5$-point, or a pair of $\mathbb{F}_{5^2}$-points.
- But when $m_0 \in \{0, 1, 2, 4\}$, the set $\widetilde{\psi}^{-1}(m_0 \cdot \widetilde{R})$ is a pair of $\mathbb{F}_5$-points.
- Conclusion: $m \equiv 3 \text{ or } 5 \pmod 6$.

- $\ell_2 = 7$ splits in $\mathbb{Q}(\sqrt{-47})$, $G_7 = 12$, and we find that $m \equiv 0, 3, 4, 7, \text{ or } 11 \pmod{12}$.

- $\ell_3 = 11$ is inert in $\mathbb{Q}(\sqrt{-47})$, $G_7 = 12$, and we find that $m \equiv 1, 2, 5, 7, \text{ or } 10 \pmod{12}$. **Contradiction.**

Conclusion: $X_0(53)(\mathbb{Q}(\sqrt{-47})) = X_0(53)(\mathbb{Q})$.

In fact, $X_0(53)(\mathbb{Q}(\sqrt{d})) = X_0(53)(\mathbb{Q})$ for any quadratic field $\mathbb{Q}(\sqrt{d})$ in which 5 and 11 are inert, and 7 splits.

Does the sieve do what we expect?

Let $X = X_0(53)$ and suppose $P \in X(\mathbb{Q}(\sqrt{-11}))\backslash X(\mathbb{Q})$.

- Apply the sieve using primes $\ell < 1000$:

$$m \equiv 1, 1905121, 2993761, 3175201, 5533921, 5715361, 6804001, 8255521, 8709121, 12065761, 13154401, 14605921, 15694561, 15876001, 17781121, 18234721, 18869761, 21409921, 22226401, 24585121, 24766561, 25855201, 27306721, 27941761, 28395361, 29030401, 30481921, 30935521, 31570561, 33657121, 34110721, 34745761, 34927201, 37285921, 37467361, 38102401, 38556001, 40007521, 40642561, 41731201, 43182721, 43817761, 44271361, 44906401, 46357921, 46811521, 47446561, 47628001, 49986721, 50803201, 53343361, 53978401, 54432001, 55883521, 56337121, 56518561, 57607201, 59058721, 60147361, 62687521 \mod 63504000.$$

- We see that 1 ‘survived’ the sieve.
- Expected, since $\psi^{-1}(1 \cdot R) \subset X(\mathbb{Q}(\sqrt{-11}))\backslash X(\mathbb{Q})$.

Violating the Hasse principle

Since $X_0(53)(\mathbb{Q}(\sqrt{-47})) = X_0(53)(\mathbb{Q})$, we have that

$$X_0^{(-47)}(53)(\mathbb{Q}) = \varnothing.$$

- The curve $X_0^{(d)}(N)$ is the curve $X_0(N)$ twisted by the quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ and the action of the Atkin–Lehner involution w_N.

Applying a result of Ozman, $X_0^{(-47)}(53)$ has points everywhere locally, so this curve violates the Hasse principle.

Thank you!