Quadratic points on bielliptic modular curves $X_0(n)$

Filip Najman

University of Zagreb

joint work with Borna Vukorepa

Rational points 2022,
March 31st 2022.

Motivating question: What are the possible degrees of isogenies of non-CM elliptic curves over quadratic fields?

To determine all the possible isogenies over a field K of characteritic 0 it is enough to understand the isogenies with cyclic kernel, which is equivalent to determining the cylcic subgroups of E, which is in turn equivalent to finding all the non-cuspidal K-rational points on $X_0(n)$, for all n.

Rational points on $X_0(n)$

Mazur (1978): Let p be a prime. The modular curve $X_0(p)$ has non-cuspidal rational points if and only if

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

Kenku (1984): The modular curve $X_0(n)$ has non-cuspidal rational points if and only if

$$n \in \{1, \dots, 19, 21, 27, 37, 43, 67, 163\}.$$

Quadratic points on $X_0(n)$

The degree d points on $X_0(n)$, for all n, are not known for any $d > 1$. So the current goal is to try to obtain results towards solving the case for $d = 2$.

Unlike in the case of $X_1(p)$, there are noncuspidal quadratic points on $X_0(p)$ for infinitely many p; they come from *CM* elliptic curves.

It is however expected that there are finitely many p with $X_0(p)$ having non-cupsidal non-CM quadratic points.

Even the problem of finding all n such that $X_0^+(n)(\mathbb{Q})$ contains points that are neither CM nor cusps, which can be considered a sub-problem of our problem, is still open.

The set of such n has been conjectured by Elkies to be finite.

Quadratic points on $X_0(n)$

The quadratic CM points on $X_0(n)$ are known for all n.

To find the (non-CM) quadratic points on $X_0(n)$ for all n, one has to:

1. Find an upper bound m such that for $n \geq m$, $X_0(n)$ has only cusps and CM points over all quadratic fields. This is currently not known.
2. Determine the quadratic points on $X_0(n)$ for small n, up to this bound m.

We work towards 2).

Hyperelliptic curves

Let $X : y^2 = f(x)$ be a hyperelliptic curve.

It has an obvious degree 2 map to $\mathbb{P}^1$, sending (x, y) to x.

It has infinitely many quadratic points of the form $(x, \sqrt{f(x)})$ for $x \in \mathbb{Q}$. These are called *non-exceptional* or *obvious* points, while the remaining quadratic points are called *exceptional*.

For almost all hyperelliptic $X_0(n)$, the hyperelliptic involution ι is w_d, for some $d \mid n$, which sends E to a d-isogenous curve.

The non-rational obvious points satisfy $\iota(P) = \sigma(P)$, so it follows that E is d-isognous to E^σ.

A $\mathbb{Q}$-curve is an elliptic curve isogenous to all of its Galois conjugates. So all obvious points correspond to $\mathbb{Q}$-curves.

So for hyperelliptic $X_0(n)$ it remains to find the exceptional points.

Results over quadratic fields

Bruin, N. (2015): determined the quadratic points on all hyperelliptic $X_0(n)$ such that $J_0(n) := J(X_0(n))$ has rank 0 over $\mathbb{Q}$. This is satisfied if and only if

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

In all these cases we have $2 \leq g(X_0(n)) \leq 5$.

Ozman, Siksek (2019): determined the quadratic points on all non-hyperelliptic $X_0(n)$ such that $J_0(n)$ has rank 0 over $\mathbb{Q}$ and such that $2 \leq g(X_0(n)) \leq 5$. This is satisfied if and only if

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

Box (2021): determined the quadratic points on remaining $X_0(n)$ such that $2 \leq g(X_0(n)) \leq 5$, or

$$n \in \{37, 43, 53, 61, 57, 65, 67, 73\}.$$

Bielliptic curves

A curve X obviously has infinitely many quadratic points if there exists a map $X \to C$ of degree 2, where $C(\mathbb{Q})$ has infinintely many points.

This is possible only if $C \simeq \mathbb{P}^1$ (X is hyperelliptic) or C is an elliptic curve (then X is called *bielliptic*) which has positive rank over $\mathbb{Q}$.

Harris and Silverman (1991) showed that the converse is also true: these are the only possible cases when X with $g(X) \geq 2$ can have infinitely many quadratic points.

Bars (1999): determined all the values of n for which $X_0(n)$ is bielliptic.

Question (Mazur, 2021): Can we describe all the quadratic points on all the remaining bielliptic curves?

The remaining values of n:

n	$g(X_0(n))$	$\mathrm{rk}(J_0(n)(\mathbb{Q}))$	n	$g(X_0(n))$	$\mathrm{rk}(J_0(n)(\mathbb{Q}))$
60	7	0	62	7	0
69	7	0	79	6	1
83	7	1	89	7	1
92	10	1	94	11	0
95	9	0	101	8	1
119	11	0	131	11	1

N., Vukorepa (202?): We solve all these cases. We get that in all the cases the exceptional points have CM.

We do this by using 2 approaches:

1. Looking at the moduli interpretation and reducing the problem to rational points on several modular curves.
2. The Box-Siksek method, a combinantion of the *Mordell-Weil sieve* and *relative symmetric Chabauty*, with modifications

Model for $X_0(95)$:

$$x_0^2 + 4x_2x_3 + 4x_2x_5 - 3x_3^2 + 2x_3x_4 + 4x_3x_5 + 19x_4^2 - 32x_4x_5 + 10x_5^2 - x_6^2 + 2x_7x_8 + 4x_8^2 = 0,$$
$$x_0x_1 + 2x_1x_5 + 3x_2x_3 - 3x_2x_5 - 5x_3^2 - 2x_3x_4 + 6x_3x_5 + 14x_4^2 - 26x_4x_5 + 13x_5^2 - x_6x_7 + x_8^2 = 0,$$
$$x_0x_2 - 2x_2x_5 - 2x_3^2 - x_3x_4 + x_3x_5 - 2x_4^2 + x_4x_5 + x_5^2 - x_7^2 = 0,$$
$$x_0x_3 - 2x_2x_3 + 3x_3^2 - 2x_3x_5 - 9x_4^2 + 16x_4x_5 - 7x_5^2 - x_7x_8 - x_8^2 = 0,$$
$$x_0x_4 - 2x_2x_3 + x_3^2 + 2x_3x_4 - 2x_3x_5 - 6x_4^2 + 10x_4x_5 - 4x_5^2 - x_8^2 = 0,$$
$$x_0x_5 - x_2x_3 - x_2x_5 - x_3^2 + x_3x_4 + x_3x_5 - x_4^2 - x_4x_5 + 2x_5^2 = 0,$$
$$x_0x_7 - x_1x_6 + x_4x_6 + 2x_4x_7 - x_4x_8 - x_5x_6 + x_5x_8 = 0,$$
$$x_0x_8 - x_2x_6 + x_3x_6 - x_4x_7 + 3x_4x_8 + x_5x_6 + x_5x_7 - x_5x_8 = 0,$$
$$x_1^2 - 4x_4^2 + 8x_4x_5 - 4x_5^2 - x_7^2 = 0,$$
$$x_1x_2 - 2x_1x_5 - 2x_2x_3 + 2x_2x_5 + 4x_3^2 - 2x_3x_4 - 2x_3x_5 - 8x_4^2 + 18x_4x_5 - 10x_5^2 - x_7x_8 - x_8^2 = 0,$$
$$x_1x_3 - x_1x_5 - 2x_2x_3 + 2x_2x_5 + 2x_3^2 + 2x_3x_4 - 2x_3x_5 - 8x_4^2 + 14x_4x_5 - 8x_5^2 - x_8^2 = 0,$$
$$x_1x_4 - x_1x_5 - x_2x_3 + x_2x_5 + x_3^2 - 2x_4^2 + 4x_4x_5 - 3x_5^2 = 0,$$
$$x_1x_7 - x_2x_6 - x_4x_7 + 2x_5x_6 + x_5x_7 = 0,$$
$$x_1x_8 - x_3x_6 + x_4x_6 - x_4x_8 + x_5x_8 = 0,$$
$$x_2^2 - 2x_2x_3 - 2x_2x_5 + x_3^2 + 4x_3x_4 - 2x_3x_5 - 8x_4^2 + 12x_4x_5 - 3x_5^2 - x_8^2 = 0,$$
$$x_2x_4 - x_2x_5 - x_3^2 + x_3x_4 + x_3x_5 - 3x_4x_5 + 2x_5^2 = 0,$$
$$x_2x_7 - x_3x_6 - x_4x_7 + x_5x_6 - x_5x_7 = 0,$$
$$x_2x_8 - x_4x_6 - x_4x_8 + x_5x_6 - x_5x_8 = 0,$$
$$x_3x_7 - x_4x_6 - x_4x_7 - x_4x_8 + x_5x_6 + x_5x_8 = 0,$$
$$x_3x_8 - x_4x_7 + x_5x_7 - x_5x_8 = 0, \quad x_6x_8 - x_7^2 + x_7x_8 + x_8^2 = 0.$$

Rational points on quotients

Looking at the moduli interpretation of the quotients allows us to solve the cases $n \in \{62, 69, 92, 94\}$.

Take $n = 94$. Bruin and N. showed that all the quadratic points on $X_0(47)$ are non-exceptional and correspond to $\mathbb{Q}$-curves of degree 47.

As any elliptic curve with a subgroup of order 94 has a subgroup of order 47, it follows that all quadratic points on $X_0(94)$ also correspond to $\mathbb{Q}$-curves of degree 47.

We want to take advantage of this fact, and ask to which modular curves do $\mathbb{Q}$-curves of degree 47 with a subgroup of order 2 correspond?

Moduli interpretation of quotients

Proposition (N., Vukorepa)

Let E be a non-CM $\mathbb{Q}$-curve of degree d defined over a quadratic field K having in addition an m-isogeny defined over K with $(m, d) = 1$ and m prime. Then either E corresponds to either a rational point on $X_0(dm)/w_d$ or is isogenous to an elliptic curve which corresponds to a rational point on $X_0^+(dm^2)$.

So for $X_0(94)$, we need to find the rational points on $X_0(94)/w_{47}$, which is an elliptic curve with 2 rational points, and $X_0^+(188)$, which is dealt with by Theorem of Momose.

The Box-Siksek method

- We have a degree 2 map $f : X \to X'$, p a prime good reduction, $J := J(X)$, $D_{pull} = f^*(B)$ for some $B \in X'(\mathbb{Q})$ and $G \leq J(\mathbb{Q})$ such that $I \cdot J(\mathbb{Q}) \leq G$,
- $\iota : X^{(2)}(\mathbb{Q}) \to J(\mathbb{Q})$, $\iota(P) = [P - D_{pull}]$;
- $\phi : X^{(2)}(\mathbb{Q}) \to G$, $\phi(P) = I \cdot [P - D_{pull}]$;
- $m : J(\mathbb{Q}) \to G$, $m(D) = I \cdot D$;
- $red_p : J(\mathbb{Q}) \to J(\mathbb{F}_p)$, $red_p(D) = \widetilde{D}$;
- $h_p : G \to J(\mathbb{F}_p)$, $h_p(D) = red_p(D) = \widetilde{D}$;
- $m_p : J(\mathbb{F}_p) \to J(\mathbb{F}_p)$, $m_p(\widetilde{D}) = I \cdot \widetilde{D}$;

$$\begin{tikzcd}
X^{(2)}(\mathbb{Q}) \arrow[d, "\iota"] \arrow[dr, "\phi"] & \\
J(\mathbb{Q}) \arrow[r, "m"] \arrow[d, "red_p"] & G \arrow[d, "h_p"] \\
J(\mathbb{F}_p) \arrow[r, "m_p"] & J(\mathbb{F}_p).
\end{tikzcd}$$

The Box-Siksek method

We suppose we have a set of known points S_{known} on $X^{(2)}(\mathbb{Q})$, which are not pullbacks from a quotient X' of X.

We star with $B_0 := G$. In each step i, we choose a prime p_i and define $B_i = \ker h_{p_i} \cap B_{i-1}$, so we divide B_{i-1} into B_i-cosets, e.g. subsets of the form $w + B_i$.

These cosets have the property that h_{p_i} is constant on each of the cosets.

There's a relative Chabauty criterion of Box and Siksek which can, for a point $P \in J(\mathbb{F}_{p_i})$ check that $\iota^{-1}(red_{p_i}^{-1}(P))$ contains only one element, up to pullbacks of rational points from X'.

Let $Q \in X^{(2)}(\mathbb{Q})$ be a unknown point which is not a pullback.

If we have $\iota((red_p)(P)) = A$ for some $P \in S_{known}$ for every $A \in m_{p_i}^{-1}(B)$, then obviously $h_{p_i}(\phi(Q))$ cannot be B if the Box-Siksek criterion is satisfied for all $A \in m_{p_i}^{-1}(B)$.

The Box-Siksek method

If this happens, we can remove the B_i-coset in G in which $\phi(P)$ lives.

Furthermore if $h_{p_i}(\phi(P)) \notin m_{p_i}(J(\mathbb{F}_{p_i}))$ for some $P \in G$, then we can again remove the B_i-coset to which P belongs.

Repeating this procedure for various primes we hope to remove all of G.

If we succeed in doing this, we have proved that there are no unknown points on X that are not pullbacks of rational points on X'.

This succeeds for $X_0(n)$ for $n \in \{60, 95, 119\}$, but not for $\{79, 83, 89, 101, 131\}$.

However, even when this does not succeed in finding all the points it can give us information about what $\phi(Q)$ should look like for some unknown point that is not a pullback.

The curve $X_0(p)$

Suppose now from on $p \in \{79, 83, 89, 101, 131\}$, let w_p be the Atkin-Lehner involution.

$$\begin{tikzcd}
X_0(p) \arrow[r, "\iota_1"] \arrow[d, "\rho_p"] & J_0(p) \arrow[d, "(\rho_p)_*"] \\
X_0^+(p) \arrow[r, "\iota_2"] & J_0(p)^+.
\end{tikzcd}$$

By a theorem of Mazur we know that the torsion of $J_0(p)$ is of order equal to the numerator of $\frac{p-1}{12}$ and generated by $T_p = [\infty - 0]$.

In all these cases we have that $X_0^+(p)$ is an elliptic curve and $r(J_0(p)(\mathbb{Q})) = r(J_0(p)^+(\mathbb{Q})) = 1$.

Let D be the generator of the free part of $J_0(p)^+(\mathbb{Q})$ and $D_p = ((\rho_p)_*)^*(D)$.

We have $D_p \in 2J_0(p)(\mathbb{Q})$. In particular if D is a generator of the free part of $J_0(p)(\mathbb{Q})$, then $2D \in \langle D_p, T_p \rangle$.

The cases $p \in \{73, 83, 101\}$

In these cases we take $l = 2$ and using the Box-Siksek method we get that for a hypothetical point Q, which is not a pullback of a rational point on $X_0^+(p)$, we obtain $\phi(Q) = 2[Q - D_{pull}] = kD_p$.

So we have $w_p(2[Q - D_{pull}]) = 2[Q - D_{pull}]$, so $w_p([Q - D_{pull}]) - [Q - D_{pull}]$ is of order dividing 2.

But $J_0(p)(\mathbb{Q})$ has no points of order 2, so it follows that $w_p([Q - D_{pull}]) = [Q - D_{pull}]$.

Since D_{pull} is a pullback of a point on $X_0^+(p)$, it follows $w_p(D_{pull}) = D_{pull}$, so we have $[w_p(Q) - Q] = 0$, and since $X_0(p)$ is not hyperelliptic, $w_p(Q) = Q$.

Writing $Q = Q_1 + Q_1^\sigma$ for some points $Q_1 \in X_0(p)$, it follows that w_p either swaps Q_1 and Q_1^σ, in which case Q is a pullback from $X_0^+(p)$, or Q_1 is a fixed point of w_p and hence corresponds to a CM elliptic curve, which is easy to check.

$p \in \{89, 131\}$

The case $p = 89$ is eliminated in a similar way, with some additional considerations since it has a 2-torison point.

For the case we $p = 131$ we take $G = J_0(p)(\mathbb{Q})_{tors}$ and $I = 1 - w_p$.

Applying the Box-Siksek method and using the fact that $(1 - w_p)J_0(p)(\mathbb{Q}) \subseteq J_0(p)(\mathbb{Q})_{tors}$ we get $\phi(Q) = (1 - w_p)[Q - D_{pull}] = 0$, so $w_p([Q - D_{pull}]) = [Q - D_{pull}]$, and we proceed as before.

Thank you for your attention!