A question about quadratic points on $X_0(N)$

Barry Mazur

Notes for my "five minute" question

Contents

1. Introduction

I want to thank Jennifer Balakrishnan, Netan Dogra, Brian Lawrence, and Carl Wang-Erickson for organizing the *Rational Points and Galois Representations* workshop, and David Zureick-Brown for organizing this problem session. My "five minute" question is about quadratic points. I also want to thank Abbey Bourdon, Maarten Derickx, Jackson Morrow and Filip Najman for important clarifications, corrections, and additions they gave me, as I revised and extended my draft. There is nothing particularly original here: even my "five minute" question has essentially been asked in the literature. I've compiled these notes as a guide to myself (and perhaps it might also be useful to others) for reading some of the recent articles about this subject.

It has long been known, thanks to a tradition of work culminating in an important sequence of papers of M.A. Kenku[1] that the $\mathbb{Q}$-rational cyclic isogenies of degree N of elliptic curves defined over $\mathbb{Q}$ only occur—and do occur—if $1 \leq N \leq 19$

[1] —by the way, see: http://worldwriterswall.blogspot.com/2013/01/professor-ma-kenku-70-worthy-model-for.html

or if $N = 21, 25, 27, 37, 43, 67$, or 163. All of these N-isogenies can be given 'geometric reasons' for existing; e.g., the 37-isogenies 'come by' applying the hyperelliptic involution (it is non-modular) to the cusps of $X_0(37)$.

A general theorem of Faltings has as a particular consequence that, fixing any positive integer N and ranging over all elliptic curves defined over $\mathbb{Q}$ there are only finitely many such curves that have a **sporadic** cyclic N-isogeny rational over some quadratic field. I want to take "sporadic" to mean that the N-isogeny is non-CM, in the sense to be defined below, and is *not* a member of a family of such "quadratic" cyclic N-isogenies that can be parametrized either by

- rational points on a curve of genus 0 or 1, the parametrization given by a degree two correspondence between the curve and $X_0(N)$;
- or in the case where $X_0(N)$ is of genus two, by a degree two correspondence between an abelian surface and $X_0(N)$.

My "five-minute question" then is:

Question 1.

(i) *Are there only finitely many sporadic cyclic N-isogenies as we range over all N and all quadratic fields? Equivalently, are there none at all over any quadratic field when $N \gg 0$?*

(ii) *Is the same true taking any fixed number field K as base and asking for sporadic cyclic isogenies over fields of degree two over K?*

(iii) *Can one "explain" at least some sporadic cyclic isogenies over quadratic number fields as arising as a consequence of some structural geometric feature of the relevant modular curve? (E.g., as the existence of the $\mathbb{Q}$-rational 37-isogenies are "explained"—or perhaps by some more intricate variant of geometric structure.)*

(iv) *What about resolving this, case by case, (over $\mathbb{Q}$) for all values of N for which $X_0(N)$ is biellptic and for which it has not currently been resolved; see the eight 'boxed values' of N in Proposition 18 below* [2]

Remarks 2. A statement formulated as a hypothesis by Pete Clark and Paul Pollack in the article [13] raises an even broader uniformity question regarding the existence of ℓ-isogenies (over fields of fixed degree over the base field). Specifically, their hypothesis, labeled $SI(d)$ is:

Hypothesis $SI(K, d)$ (Clark-Pollack): For any $d > 0$ there is prime $\ell(K; d)$ such that for all primes $\ell > \ell(K; d)$, the modular curve $X_0(\ell)$ has no noncuspidal non-CM points rational over fields of degree d over K.

Proposition 3. *These are equivalent:*

(i) *An affirmation of Clark-Pollack's Hypothesis $SI(K; 2)$.*

(ii) *An affirmative response to Question 1(ii) above for the base number field K.*

[2] It is already resolved when $X_0(N)$ hyperelliptic.

Proof. Visibly (ii) implies (i). Now assume (i). A counterexample to (ii) would necessarily involve an infinite sequence of values

$$N_1, N_2, \ldots \tag{4}$$

of N for which there are sporadic cyclic N-isogenies over fields that are quadratic extensions of K; these values of N having all their prime divisors among the finite set of primes $\leq \ell(K;2)$. It follows that there is at least one prime $\ell(\leq \ell(K;2))$ such that for every $r > 0$ there is an N_i —call it $N^{\{r\}}$—such that $N^{\{r\}}$ is divisible by ℓ^r. In particular, given the projection $X_0(N^{\{r\}}) \to X_0(\ell^r)$ the existence of sporadic points of $X_0(N^{\{r\}})$ rational over a quadratic extension of K implies the same for $X_0(\ell^r)$. So, assuming the existence of a counter-example to (ii), we would have that

(*) $X_0(\ell^r)$ has sporadic points rational over quadratic extensions of K for every $r > 0$.

But note that Proposition 18 below gives us that if $N > 131$ then $X_0(N)$ is neither hyperelliptic nor bielliptic so by Faltings' Theorem, $X_0(N)$ has only finitely many quadratic points over K. Let, then, r_1 be such that $\ell^{r_1} > 131$ so that $X_0(\ell^{r_1})$ has only finitely many points rational over quadratic extensions of K and let $\{x_j\}_{j \in J}$ be the finite set of those points. If any one of these points (say $x_1 \in X_0(\ell(r_1)(K_1)$ (where K_1/K is a quadratic extension) persists as the image of a point in $X_0(\ell^r)$ defined over quadratic extensions of K for all $r \geq r_1$ it is necessarily either a cusp or CM. So the sporadic points don't 'persist' contradicting **(*)**. □

Part 1. The format of general quadratic point questions

2. Quadratic points

Let V be a variety over a field K of characteristic different from 2, and denote by $S(V)$ the symmetric square of V; that is, the quotient of $V \times V$ by the involution that swaps factors. The K-valued points of $S(V)$ consist of either conjugate pairs of points of V rational over some quadratic extension of K, or unordered pairs of K-rational points of V. Refer, colloquially then, to any K-rational point of $S(V)$ as a K-quadratic point of V.

To focus more specifically to the situation I'm interested in, let K be a number field and X a smooth projective curve, geometrically irreducible, defined over K and processing at least one K-rational point. Consider, then (X, x_o) the pointed curve over K by fixing on some x_o, a choice of K-rational point. What is the structure of (and in particular instances, *what are*) the K-quadratic points of (X, x_o)?

Denoting by $J(X)$ the Jacobian of X, consider the natural map

$$S(X) \xrightarrow{\delta} J(X) := Pic^0(X) \subset Pic(X)$$

by sending an unordered pair $\{x, y\}$ of points on X to the divisor of degree 0 $D = x + y - 2x_o$.

3. Small genus

A. Genus 0. In this instance, the curve X is isomorphic to $\mathbb{P}^1$ over K. We would naturally take such an isomorphism sending our chosen K-rational point x_o to ∞, but we would still have to choose such an isomorphism to get a canonical isomorphism $S(X) \simeq \mathbb{P}^2$. So, the answer here is entirely explicit, given explicit equations for an isomorphism $X \simeq \mathbb{P}^1$, and, one might record this by saying: *X has a single family of quadratic points parameterized by $\mathbb{P}^2$.*

B. Genus 1. Here we may let $E = X$ be the elliptic curve where the K-rational point x_o is taken to be the origin. We have, by Riemann-Roch, that $S(X)$ is then a "$\mathbb{P}^1$"-bundle over E, where the quotation-marks around the "$\mathbb{P}^1$" is to indicate that the fiber over a point $e \in E$ of this bundle is only isomorphic to $\mathbb{P}^1$, and is more explicitly described as the quotient by the unique involution σ_e of E that has e as one of its fixed points. The structure of the set of K-quadratic points of X then depends on the Mordell-Weil group of E, in that for each point e of this Mordell-Weil group there is a linear system of K-quadratic points of X parametrized by the K-rational points of the genus zero curve: $X/\{\text{action of } \sigma_e\} = E/\{\text{action of } \sigma_e\}$.

4. Genus ≥ 2

Let the genus of X be ≥ 2. There are two possibilities:

- X is *not hyperelliptic.* In this case δ maps $S(X)$ isomorphically onto a closed (2-dimensional) subscheme, denoted $\tilde{S}(X)$, in the Jacobian, $J(X)$:

$$\delta : S(X) \overset{\simeq}{\to} \tilde{S}(X) \subset J(X).$$

- X is *hyperelliptic.* Let
  (i) $\sigma : X \to X$ be the (unique) hyperelliptic involution;
  (ii) define the class $e := [x + \sigma(x) - 2x_o] \in J(X)$ (which is independent of the choice of x); and consider
  (iii) $X \overset{h}{\to} X/\{\text{action of } \sigma\} =: \mathcal{P}$ the degree two mapping (to $\mathcal{P}$, the genus zero quotient). The involution σ is call **the** *hyperelliptic involution* of X.

  Form the sequence of mappings

$$X \xrightarrow{g} X \times X \to S(X) \xrightarrow{\delta} J(X)$$

  defined by $g : x \mapsto (x, \sigma(x))$ and where the middle morphism is the natural one: passage to the quotient by the involution of $X \times X$ that switches factors. We have a commutative diagram:

$$\begin{tikzcd}
& X \arrow[r] \arrow[d, "g"] \arrow[dr] & X/\{\text{action of } \sigma\} = \mathcal{P} \arrow[r] \arrow[d, "\subset"] & e \arrow[d, "\epsilon"] \\
\text{Weierstrass pts} \arrow[ur] \arrow[dr] & X \times X \arrow[r] & S(X) \arrow[r, "\delta"] & J(X) \\
& X \arrow[u, "\text{diag}"] \arrow[ur] & &
\end{tikzcd}$$

Here the "Weierstrass points" comprise the intersection of the two copies of X in $X \times X$ as in the diagram.

Proposition 5. *We have a diagram:*

$$\begin{tikzcd}
\mathcal{P} \arrow[r] \arrow[d, "\subset"] & e \arrow[r, "\epsilon"] \arrow[d, "\epsilon"] & J(X) \arrow[d, "="] \\
S(X) \arrow[r] & \tilde{S}(X) \arrow[r, "\subset"] & J(X) \\
S(X) \setminus \mathcal{P} \arrow[r, "="] \arrow[u, "="] & \tilde{S}(X) \setminus \{e\} \arrow[r, "\subset"] \arrow[u, "="] & J(X) \arrow[u, "="]
\end{tikzcd}$$

Here, $\tilde{S}(X)$ is a closed (2-dimensional) subscheme of $J(X)$ and $S(X)$ may be described as a blow-up of $\tilde{S}(X)$ at the point $e \in \tilde{S}(X)$. (So, if the genus g is equal to 2 then $\tilde{S}(X) = J(X)$.)

Recalling Faltings Theorem, we have that the Zariski closure of the set of K-rational points of $\tilde{S}$ (in either case described above) is a finite union of translates of abelian subvarieties $\cup_i A_i$ and a finite set of isolated points. Given that $\tilde{S}$ is just an abelian surface, there are only two possibilities: the abelian varieties might be elliptic curves—and this can happen only if the curve X can be covered by a bielliptic curve—or this “finite union of abelian varieties” is the single, entire abelian surface $J(X)$, and this can happens only if the genus of X is 2.

5. Hyperelliptic and bielliptic covers of curves of genus > 1

Except for the case of curves of genus $g = 2$ (which we will discuss separately below) by ‘family’ of quadratic points (over K) we will mean a‘ family of points of X, defined over quadratic extensions of K, the family being parameterized by the K-rational points of a (‘parameter’) curve of genus 0 or 1 via a degree two correspondence (defined over K) of this parameter curve covering X. That is, such a family $\mathcal{F}$ comes from a nonconstant mapping $f : Y \to X$ (over K) where Y is a curve that is a degree two cover of B, a curve of genus ≤ 1—and, in particular, Y is either hyperelliptic or bielliptic (or both). For simplicity of terminology we will call a curve over K bielliptic if it admits a mapping *defined over* K to a curve of genus 1. The family $\mathcal{F}$ is the image under f of $\mathcal{F}_{Y/B} :=$ the pullback to Y of $B(K)$, the set of K-rational points of B as illustrated in the diagram:

(6)
$$\begin{tikzcd}
 & \mathcal{F}_{Y/B} \arrow[r, "f"] \arrow[dl, "="] \arrow[d, "\subset"] & \mathcal{F} \arrow[d, "\subset"] \\
\mathcal{F}_{Y/B} \arrow[r, "\subset"] \arrow[d, "\text{onto}"] & Y \arrow[r, "f"] \arrow[d, "\text{degree 2}"] & X \\
B(K) \arrow[r, "\subset"] & B. &
\end{tikzcd}$$

Note that if B is of genus 1 and has a finite (nonempty) set of K-rational points, it may be a stretch to call $\mathcal{F}$ (parametrized by the finitely many elements of $B(K)$) a *family* but we'll do that, just to keep from having to distinguish whether $B(K)$ is finite or infinite; i.e., to keep the discussion as brief as possible.

Proposition 7. *Let X be a curve of genus > 1 defined over a number field K. Let $Y \xrightarrow{f} X$ be a (nonconstant) mapping defined over K.*

- *If Y is hyperelliptic then so is X, and the mapping f is equivariant with respect to the hyperelliptic involutions of X and Y.*
- *If Y is bielliptic over K —i.e., if there is a degree two mapping $Y \to E$ where E is an elliptic curve defined over K—then X is bielliptic or hyperelliptic.*

Proof. As Joe Harris and Filip Najman explained to me, the first item—at least without the equivariance statement—is classical. Namely, assume that we have a hyperelliptic cover, $Y \xrightarrow{f} X$, of a curve X of genus > 1. Let $K(Y)/K(X)$ be the field extension of the fields of rational functions on Y and on X respectively—the injection of $K(X)$ into $K(Y)$given by the mapping f (the base field is our number field K). Let $h \in K(Y)$ be a rational function that parametrizes a degree two map of Y onto a curve of genus 0. Since Y is hyperelliptic, such a rational function exists. Then elementary considerations shows that the norm $g := N_{K(Y)/K(X)}(h) \in K(X)$ parametrizes, similarly, a degree two mapping from X to a curve whose rational function field is $K(g)$, i.e., a curve of genus zero as well. So $Y \xrightarrow{f} X$ is a mapping of hyperelliptic curves.

To check equivariance of f relative to the hyperelliptic involutions, it suffices to extend the basefield K (to anything, e.g, $\mathbb{C}$). We may embed Y in its jacobian J_Y sending a Weierstrass point $w \in Y$ to the origin, so that the hyperelliptic involution of Y is induced by the("inversion") mapping $z \mapsto -z$ on J_Y. Now letting $u := f(w) \in X$ and embedding X into its jacobian J_X by sending u to the origin we get a commutative diagram

$$\begin{tikzcd}
Y \arrow[r, "\subset"] \arrow[d, "f"] & J_Y \arrow[d, "f"] \\
X \arrow[r, "\subset"] & J_X
\end{tikzcd}$$

noting that the mapping $J_Y \xrightarrow{f} J_X$ is (a homomorphism of groups, and hence) is equivariant relative to inversion mappings. Since Y is stabilized by inversion and X is its image, X is also stabilized by inversion. Since the quotient of Y by inversion is a curve $\mathcal{P}_Y$ of genus zero, and since the quotient of X by inversion, $\mathcal{P}_X$, is mapped onto by $\mathcal{P}_Y$, it follows that $\mathcal{P}_X$ is also of genus zero, and consequently the inversion mapping of J_X restricted to X is the hyperelliptic involution of X. Consequently the mapping f is equivariant with respect to hyperelliptic involutions.

The second item is Proposition 1 of [20]. More specifically, consider a bielliptic curve $\pi : Y \to B$ admitting a mapping to X as in Diagram 6. The induced (two-valued) mapping of B to X yields a single-valued mapping $B \to S(X) \to$

$\tilde{S}(X)$. If the composite morphism $B \to \tilde{S}$ is trivial—which can only happen if X is hyperelliptic—the family of K-quadratic points parameterized by $Y \to B$ would then be 'majorized' by the family of K-quadratic points parameterized by the hyperelliptic structure of X. If it is not trivial, then letting E denote the image of B in $\tilde{S}$, we have that $E \subset \tilde{S} \subset J(X)$ is a curve of genus 1. Denote by $Y_o \subset X \times X$ the 'pullback' of E to $X \times X$ under the mapping

$$X \times X \to S(X) \to \tilde{S}(X)$$

where the scare-quotes indicate that—in the case where X is also hyperelliptic—if the pullback also contains the exceptional locus of $S(X) \to \tilde{S}(X)$, we discard that exceptional locus. We have a commutative diagram:

$$\begin{tikzcd}
Y \arrow[r] \arrow[d, "\pi"] & Y_o \arrow[r] \arrow[d, "\pi_o"] & X \\
B \arrow[r] & E. &
\end{tikzcd}$$

□

6. The method of 'quadratic' Chabauty

The adjective "quadratic" will occur in two quite different senses in the discussion below. It is used on the one hand, in the phrase "quadratic points," as we have been discussing. But it is also used in the phrase "quadratic Chabauty" and there it is referring to a specific framework within the method of Chabauty-Coleman-Kim—a format that has been recently extremely successful to compute the full set of rational points for many curves of genus > 1. For this see the articles of Jennifer S. Balakrishnan, joint with Amnon Besser, Francesca Bianchi, Netan Dogra, Jan Steffen Müller, Jan Tuitman and Jan Vonk listed as [2] [3] and [4] in the bibliography below.

I want to thank Jackson Morrow for his comments about quadratic Chabauty specifically related to symmetric powers, and for suggesting the following references:

(i) Samir Siksek (cf. [32]) has adapted the Chabauty-Coleman-Kim method to symmetric powers of curves—particularly relevant for us being the symmetric square of curves; see for example the two examples he works out in loc. cit. for curves X of genus 3 whose jacobians have Mordell-Weil rank 1.

(ii) See also Jennifer Park's [29] Effective Chabauty for symmetric powers of curves, in which tropical geometry is used with symmetric power Chabauty.

(iii) In the article [19] of Joseph Gunther and Jackson Morrow the focus is on the "unexpected points" of hyperelliptic curves (e.g., $X_0(29)$ is an example chosen). In that article the work of Bhargava and Gross on average ranks of Jacobians of hyperelliptic curves together with the work of Park (loc. cit.) is used to get statistical density bounds on unexpected points (conditional on a certain hypothesis being met).

(iv) Let K be a number field and $\mathcal{O}_K$ its ring of integers. If $X \hookrightarrow J(X)$ is a choice of embedding over K of a curve X of genus > 1 to its jacobian $J(X)$, denote by $\mathcal{X} \subset \mathcal{J}$ the natural extension of this over $\mathcal{O}_K$, where $\mathcal{J}$ is the Néron model of $J(X)$ and $\mathcal{X}$ is the corresponding model of X over

$\mathcal{O}_K$. If there is a projection (defined over $\mathcal{O}_K$) $\mathcal{J} \to \mathcal{A}$ where $\mathcal{A}$ is an abelian scheme whose generic fiber over K has finite Mordell-Weil group, and such that the composite morphism $\mathcal{X} \to \mathcal{A}$ satisfies a certain "formal immersion" condition, one is in a convenient setting to (at times) be able to compute quadratic (and higher— but reasonably low—degree) rational points on X. This is addressed, for example, in section 3 (see, in particular Theorem 3.2) of the paper of Maarten Derickx, Sheldon Kamienny, William Stein and Michael Stoll [14][3]

(v) The method of symmetric square Chabauty-Coleman was also employed in work of Ozman-Siksek and Box, which will be referred to in Section 11 below. See also [34].

7. Summary

Recalling that (X, x_o) is a pointed curve of genus > 1, the K-rational quadratic points of X are of these possible types:

- If X is hyperelliptic where the quotient by the hyperelliptic involution is isomorphic over K to $\mathbb{P}^1$ and the point is a member of the family of K-quadratic points of X parametrized by the K-rational points of $\mathbb{P}^1$.
- If X can be covered by a bielliptic curve—or equivalently if there is an elliptic curve E contained in $S(X)$—and the point is a member of the family of K-quadratic points of X parametrized by the K-rational points of E.
- If the genus of X is 2 and the point is a member of the family of K-quadratic points of X parametrized by the K-rational points of $J(X)$ and finally:
- the (finitely many) K-quadratic points of X that don't fit into any of the frameworks listed above.

Definition 8. Call this finite set of points $Isol(X; K)$, the set of **isolated quadratic points**[4] of X.

Following [11] and [12] one might ask:

Question 9. *For any genus $g \geq 3$ is there a finite upper bound $U(g)$ such that for any number field K there are only finitely many different K-isomorphism classes of curves over K of genus g such that $|Isol(X; K)| > U(g)$?*

[3] The method involving the "formal immersion" condition is also used in the preprint ([15] Sporadic Cubic Points) of Maarten Derickx, van Hoeij Etropolski, Jackson Morrow, and Zureick-Brown to complete the classification of torsion subgroups appearing for elliptic curves over cubic number fields. They use the formal immersion criterion specifically to determine the rational points of $X_1(65)$ and $X_1(121)$.

[4] I'm calling these "isolated" because I've already use the adjective "sporadic" to mean something a bit different in the question framed in the introduction above.

Part 2. Modular Curves

8. CM N-isogenies

Definition 10. A **CM N-isogeny** defined over a field K is an endomorphism (defined over K) of an elliptic curve with kernel equal to a cyclic group of order N.

Remarks 11. (a) Any elliptic curve admitting a CM N-isogeny (for $N > 1$) is a CM elliptic curve.

(b) Let E be a CM elliptic curve with ring of endomorphisms (over K) equal to $\mathcal{O} \subset F$, where F is a quadratic imaginary field, and $\mathcal{O}$ is an order in F. For any prime p for which there exists an element $\pi \in \mathcal{O}$ such that $N_{F/\mathbb{Q}}(\pi) = p$, and for any positive number r, multiplication by π^r gives us a mapping $E \xrightarrow{\pi^r} E$ that is a cyclic (CM) isogeny of degree p^r rational over K. So, any such CM-elliptic curve admits an infinite chain of cyclic isogenies each of degree p (for $r = 1, 2, 3, \dots$):

$$\dots E \xrightarrow{\pi} E \xrightarrow{\pi} \dots E \xrightarrow{\pi} E, \tag{12}$$

and combining to produce cyclic (CM) isogenies (from E to E) of degree p^r rational over K for any $r > 0$.

(c) There's a sort of converse to the previous item:

Proposition 13. *Let E be an elliptic curve over a number field K. If p is a prime number for which E has cyclic isogenies of degree p^r defined over K for all $r > 0$ then E is a CM elliptic curve and the isogenies are of the form displayed in Equation 12 above.*

Proof. This follows from Serre's open image theorem ([31]). □

For recent results—with base equal to $K = \mathbb{Q}$ but regarding the general problem of classifying the (isomorphism classes of) subgroups in $\mathrm{GL}_2(\mathbb{Q}_\ell)$ arising as the image of the Galois representation given by Galois action on ℓ-power torsion of elliptic curves over $\mathbb{Q}$—see the work of Rouse, Sutherland, Zureick-Brown and Voight in [30] (and see the bibliography there).

(d) An equivalent formulation of Proposition 13 is:

Corollary 14. *For every number field K and prime number p there exists a positive number $r(K;p)$ such that if $r > r(K;p)$ the K-rational points of the modular curve $X_0(p^r)$ are either cusps or CM-points associated to cyclic isogenies of degree p^r of the form displayed in Equation 12 above.*

Proof. If r is sufficiently large $X_0(p^r)$ is of genus > 1 so it has only finitely many K-rational points. Consider mappings $X_0(p^{r+1}) \xrightarrow{\phi} X_0(p^r)$ given by the natural 'forgetful mapping' $\phi : (E, C_{p^{r+1}}) \mapsto (E, C_{p^r})$ where C_{p^r} is a cyclic subgroup of the p^r-torsion points of E, and the comparisons between the r-th level and the next level is as follows.

$$\begin{tikzcd}
C_{p^{r+1}} \arrow[r, "\subset"] & E[p^{r+1}] \\
C_{p^r} \arrow[r, "\subset"] \arrow[u, "\subset"] & E[p^r]. \arrow[u, "\subset"]
\end{tikzcd}$$

We get the chain of mappings of sets (*finite sets*, once r is sufficiently large)

$$\ldots X_0(p^{r+1})(K)^* \xrightarrow{\phi} X_0(p^r)(K)^* \xrightarrow{\phi} \ldots \tag{15}$$

where the superscript $*$ means that we are forming the complement of the subset consisting of CM-points and cusps. It follows that either $X_0(p^r)(K)^*$ is empty for $r \gg 0$ or else there is an elliptic curve E possessing cyclic p^r-isogenies defined over K for all r—and this would contradict Proposition 13. □

9. The Families

- Quadratic points of the family $X_1(N)$ for $(N \geq 1)$ have been largely classified and understood (see [25] and the results of Sheldon Kamienny: [7], [9], [10]. For an extensive discussion of the results regarding the finite number of conductors N for which $X_1(N)$ has a quadratic (or rational) point that is not a cusp (explicitly: $1 \leq N \leq 18$; $N \neq 17$) see [30]; see that article as well for its very useful bibliography. See also [21]).

- **Q**-rational points the family $X_0(p^+)$. This is a case where the MW-rank of the Jacobean is a positive multiple of the genus, and often the MW-rank is *equal to the genus* and therefore presents a natural example to study using quadratic Chabauty. See [2], [3]; also [4]. For recent results about quadratic points on 'nonsplit Cartan' modular curves, see [26].

10. Sporadic (quadratic) points coming from rational points on quotients of $X_0(N)$ by involutions

Specifically, see the papers[5] of Noam Elkies [16] and Stephen Galbraith—[17] and [18] $\sim$ (2000)— on rational points on $X_0(N)^+$; also [8].

Denote by $\nu(N) = \nu$ the number of distinct prime factors of N, and let $W(N)$ be the subgroup of automorphisms of the curve $X_0(N)$ generated by its r Atkin-Lehner involutions. Elkies, in [16] defines $X^*(N)$ to be the quotient of $X_0(N)$ by $W(N) \simeq \mathbb{Z}/2\mathbb{Z})^r$. We have

$$X_0(N) \quad \longrightarrow \quad X_0^+(N) = X_0(N)/\{\sim w_N\}) \quad \longrightarrow \quad X^*(N)$$

Here w_N is the fundamental Atkin-Lehner involution and any rational point on $X_0^+(N)$ gives us a quadratic point on $X_0(N)$.

[5] I want to thank Abbey Bourdon for suggesting them.

Elkies ([16]) point out that when the curve $X^*(N)$ is hyperelliptic (for example, when it is of genus 2) then its hyperelliptic involution may take a cusp or CM point to an unexpected rational point on $X^*(N)$ and this happens for $N = 191$, the largest prime for which $X^*(N)$ has genus 2.

Elkies goes on to say:

> I made the rash conjecture... that this might be the only source of rational points on $X^*(N)$ other than cusps and CM points, once the genus of $X^*(N)$ exceeds 1. But this guess was disproved by S. Galbraith [17], [18] who computed explicit models for many curves $X^*(N)$ and found rational non-CM points and noncuspidal points on the curves $X^*(N)$ for $N = 137$ and $N = 311$ (with $X^*(N)$ of genus 4 in both cases)...

In communication with Maarten Derickx, I learned that he and Michael Stoll are preparing an article that prove that for primes in a large range, i.e. for a certain number $n \ll 1,000,000$ (that they are at present trying to optimize) and for primes p such that $n < p < 1,000,000$ all quadratic points on $X_0(p)$ actually come from $X_0(p)^+$. They also conjecture (in a slightly weaker format) that the question posed at the beginning has a positive answer. Namely, they conjecture that for integers $N \gg 0$ all quadratic points on $X_0(N)$ come from rational points on $X_0(N)^+$.

11. References to some of the literature about quadratic points on $X_0(N)$ over $\mathbb{Q}$.

Given that so much interesting work is currently going on in the actual computation of quadratic points on 'interesting' curves, I found it helpful to do some personal bookkeeping and collect what's known today—so that one can add to it as further things become known. I'm not at all sure that I have a complete current record even for the families of curves I want to think about—how could I?—things are moving; but here's an attempt, as well as some questions. First:

There are the two parameters over which one might quantify such questions:

(i) We might fix the quadratic field K and vary N; or
(ii) fix N and vary the quadratic field K.

A. Fixing the quadratic field K. Here there is significant recent progress; specifically focusing on isogenies of prime degree:

Definition 16. The set *Isog.Prime.Deg*(K) is the set of prime numbers p for which there exists an elliptic curve E defined over a number field K possessing a K-rational p-isogeny.

See the detailed the discussion in [6] describing the recent work of David, Larson-Vaintrob, Momose, Bruin-Najman, Ozman-Siksek, and Box regarding this question; see also his intriguing Theorem 1.10:

Theorem 17. (Bar) *Assuming GRH, we have the following.*

$$Isog.Prime.Deg(\mathbf{Q}(\sqrt{7})) = Isog.Prime.Deg(\mathbf{Q}(\sqrt{-}10))) = Isog.Prime.Deg(\mathbf{Q}),$$

$$\textit{and}$$
$$\mathit{Isog.Prime.Deg}(\mathbf{Q}(\sqrt{-}5)) = \mathit{Isog.Prime.Deg}(\mathbf{Q}) \sqcup \{23\}.$$

B. Some literature about quadratic points in $X_0(N)$ in the cases where $X_0(N)$ is hyperelliptic, bielliptic, or both.

A classical theorem of Ogg [27] gives the nineteen values of N for which $X_0(N)$ is hyperelliptic (we take hyperelliptic to require that the genus is > 1):

N :	22	23	**26**	28	29	**30**	31	33	**35**	**37**
genus :	2	2	2	2	2	3	2	3	3	2

N :	**39**	**40**	41	46	47	**48**	**50**	59	71
genus :	3	3	3	5	4	3	2	5	6

The levels N that appear in boldface above are those values of N such that $X_0(N)$ is bielliptic as well as hyperelliptic. All sporadic quadratic points for any of those modular curves $X_0(N)$ (except for $X_0(37)$) have been computed by Peter Bruin and Filip Najman in their article [10] (which has other interesting results as well). The case of $X_0(37)$ is taken care of in Josha Box's paper [9], in which all sporadic quadratic points have also been computed for the curves $X_0(N)$ with $N = 43, 53, 61, 65$, these being bielliptic curves covering elliptic curves of positive Mordell-Weil rank.

Proposition 18. *These are the values of N for which $X_0(N)$ is of genus > 1 and bielliptic (over $\mathbb{Q}$):*

26	30	34	35	37	38	39	40	43	44	45	48	50	51	53
54	55	56	61	62	64	65	$\boxed{\textit{69}}$	$\boxed{\textit{79}}$	$\boxed{\textit{83}}$	$\boxed{\textit{89}}$	$\boxed{\textit{92}}$	$\boxed{\textit{94}}$	$\boxed{\textit{101}}$	$\boxed{\textit{131}}$

Proof. If $X_0(N)$ (of genus > 1) is bielliptic —i.e., if there is an involution

$$\sigma : X_0(N) \to X_0(N)$$

defined over $\mathbb{Q}$ with quotient of genus 1, denoting

$$E := X_0(N)/\{\text{action of } \sigma\} \tag{19}$$

we have that E is an elliptic curve of conductor N and of modular degree 2, and the induced mapping $X_0(N) \to E$ exhibits $X_0(N)$ as bielliptic over $\mathbb{Q}$.

Conversely, given an elliptic curve E of conductor N of modular degree 2 we get that $X_0(N)$ is bielliptic with the natural modular uniformization $X_0(N) \to E$ expressing $X_0(N)$ as bielliptic over $\mathbb{Q}$.

So the modular curve $X_0(N)$ is bielliptic if and only if there is an elliptic curve of conductor N with modular degree equal to 2. By a theorem of Harris and Silverman [20] we have that if $N > 344$ the modular curve $X_0(N)$ is not (hyperelliptic or) bielliptic.

I thank John Cremona and William Stein for pointing to databases of elliptic curves going their modular degrees[6]. The list in Proposition 18 is precisely the list

[6] John Cremona wrote:

of values of $N < 345$ that are levels of elliptic curves with modular degree 2. So, by [20] these are all values of N with modular degree 2. □

Remarks 20.

(i) For all but five values of N in this list ($N = 26, 38, 37, 50, 54$) the modular curve $X_0(N)$ has a unique elliptic curve quotient with modular degree 2 and this elliptic curve is listed as Na1 in the Cremona or LMFDB database.

(ii) For $N = 26, 37, 50$ the modular curve $X_0(N)$ has *two* elliptic curve quotients with modular degree 2, these being listed as Na1 and Nb1 in the Cremona or LMFDB database.

(iii) $X_0(38)$ and $X_0(54)$ each have unique elliptic curve quotients with modular degree 2 and these are listed as Nb1 in the Cremona or LMFDB database.

(iv) Ekin Ozman and Samir Siksek [28] have computed the sporadic quadratic points in $X_0(N)$ for quite a number of values of N including

$$N = 34, 38, 42, \mathbf{44}, \mathbf{45}, \mathbf{51}, 52, \mathbf{54}, \mathbf{55}, \mathbf{56}, 63, \mathbf{64}, 72, 75, 81, \tag{21}$$

the ones in boldface being values for which $X_0(N)$ is bielliptic[7].

(v) The boxed values of N in the above display correspond to all values of N for which $X_0(N)$ is of genus > 1 and either hyperelliptic or bielliptic and (to my knowledge) no full account of their sporadic quadratic points occurs in the literature.

(vi) If N does not occur in either of the two lists of values of N displayed above, then by Faltings' Theorem $X_0(N)$ has only finitely many quadratic points.

References

[1] D. Abramovich and J. Harris, Abelian varieties and curves in $W_d(C)$, Compositio Math. **78** 227-238 (1991)

[2] J. Balakrishnan, N. Dogra, J. Müller, J. Tuitman, J. Vonk, Quadratic Chabauty for modular curves: Algorithms and examples, `https://arxiv.org/abs/2101.01862`

[3] J. Balakrishnan, A.Besser, F. Bianchi, J. Müller, Explicit quadratic Chabauty over number fields, `arXiv:1910.04653`

[4] J. Balakrishnan, N. Dogra, Quadratic Chabauty and rational points I: p-adic heights, `arXiv.org>math>arXiv:1601.00388`

[5] J. Balakrishnan, N. Dogra, Quadratic imaginary points on Bring's curve, (recent unpublished).

[6] Barinder S. Banwait, Explicit isogenies of prime degree over quadratic fields `https://arxiv.org/abs/2101.02673`

[7] Francesc Bars, Bielliptic Modular Curves Journal of Number Theory **76**, 154-165 (1999)

The second (1997) edition of my book also has all the modular degrees for conductors up to 1000, which you can get online at `https://johncremona.github.io/book/fulltext/table5.pdf.`

and

William Stein pointed me to:

`https://share.cocalc.com/share/9ff7a4234200484b58f78217f35e4284d4d657ff/computations/2021-07-03-modular-degrees/2021-07-03.ipynb?viewer=share`

[7] The list 21 consists of all the levels N which $X_0(N)$ is non-hyperelliptic, of genus g with $2 < g \leq 5$ and for which the jacobian of $X_0(N)$ has Mordell Weil rank zero (cf [28]).

[8] Y. Bilu, P. Parent, M. Rebolledo, Rational points on $X_0^+(p^r)$) [Points rationnels de $X_0^+(p^r)$] Annales de l'Institut Fourier, **63** (2013) no. 3, 957-984.

[9] Josha Box, Quadratic points on modular curves with infinite Mordell-Weil group, `arXiv:1906.05206v3`

[10] P. Bruin, F. Najman, Hyperelliptic modular curves and isogenies of elliptic curves over quadratic fields, LMS Journal of Computation and Mathematics (2015)

[11] L. Caporaso, J. Harris, B. Mazur, Corrections to *Uniformity of rational points* and further comments, `https://arxiv.org/abs/2012.14461`

[12]] L. Caporaso, J. Harris, and B. Mazur, Uniformity of rational points. J. Amer. Math. Soc., **10** 1-5 (1997)

[13] P. Clark, P. Pollack Pursuing polynomial bounds on torsion arXiv:1705.10401 (2017)

[14] M. Derickx, S. Kamienny, W. Stein, M. Stoll, Torsion points on elliptic curves over number fields of small degree, `arXiv:1707.00364`

[15] M. Derickx, van H. Etropolski, J. Morrow, D. Zureick-Brown, Sporadic cubic torsion, `https://arxiv.org/pdf/2007.13929.pdf`

[16] Noam Elkies, On Elliptic K -curves, Progress in Mathematics, **224**, 81-91 (2004) Birkhauser Verlag, Basel/Switzerland

[17] S. Galbraith, Rational points on $X_0^+(N)$. (English summary) Experiment. Math. **8** (1999), no. 4, 311-318

[18] S. Galbraith, Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}-$curves, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 205-219.

[19] J. Gunther, J. S. Morrow Irrational points on hyperelliptic curves, `arXiv:1709.02041`

[20] J. Harris, J. Silverman, Bielliptic curves and symmetric products, Proceeding of the A.M.S., **112** No. 2, (1991) 347-356

[21] Sheldon Kamienny, Torsion points on elliptic curves over all quadratic fields, Duke Mathematical Journal, **53** 157-162 (1986)

[22] Sheldon Kamienny, Torsion points on Elliptic Curves over all quadratic fields II, Bull. Soc. Math. de France. bf 114 (1986) 119-122

[23] Sheldon Kamienny, Torsion points on elliptic curves. Proceedings of the Conference on Number Theory, (1991) 12-15, GH Essen Preprint Series (G. Frey, ed.) (1991).

[24] S. Kamienny, B.Mazur, Rational torsion of prime order in elliptic curves over number fields Astérisque, **228** (1995) 81-98 `http://www.numdam.org/item?id=AST_1995__228__81_0`

[25] M. A. Kenku, F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. **109** (1988) 125-149

[26] Philippe Michaud-Rodgers, Quadratic points on non-split Cartan modular curves, `https://arxiv.org/pdf/2011.00590`

[27] Andrew Ogg, Hyperelliptic modular curves Bulletin de la S. M. F., **102** 449-462 (1974)

[28] E. Ozman, S. Siksek, Quadratic Points on Modular Curves, `arXiv.org>math>arXiv:1806.08192` (2018)

[29] Jennifer Park, Effective Chabauty for symmetric powers of curves Ph.D. thesis, Massachusetts Institute of Technology, (2016) `http://hdl.handle.net/1721.1/90189`

[30] J. Rouse, A.V. Sutherland, D. Zureick-Brown (with an appendix by J. Voight) ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$, `https://arxiv.org/abs/2106.11141`

[31] J.-P. Serre, Proprétés galoisiennes des points elliptiques. Invent. Math. **15** (1972), no. 4, 259-331.

[32] Samir Siksek, Chabauty for symmetric powers of curves `https://homepages.warwick.ac.uk/staff/S.Siksek/papers/symmetric7.pdf`

[33] Andrew V. Sutherland, Torsion subgroups of elliptic curves over number fields, `https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf`

[34] S. Vemullapalli, D. Wang, Uniform bounds for the number of rational points on symmetric squares of curves with low Mordell-Weil rank `arXiv:1708.07057`