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

Barry Mazur

Notes for my “five minute” question

CONTENTS

1. Introduction 1

Part 1. The format of this general quadratic point question 2

2. Quadratic Points 2
3. Small genus 3
4. Uniformity Conjecture 5
5. Modular Curves 5
6. Questions about—and references to some of the literature about—quadratic points of the family of modular curves $X_0(N)$ over $\mathbb{Q}$ for $N \geq 1$ 6

Part 2. A beginning attempt to collect literature around the question 9

References 14

1. Introduction

A. The workshop and Questions session. 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 question session.

B. Cyclic $N$-isogenies of elliptic curves over $\mathbb{Q}$. It has long been known, thanks to a tradition of work culminating in a sequence of papers of M.A. Kenku ([16], [17], [18], [19]) that the $\mathbb{Q}$-rational cyclic isogenies of degree $N$ of elliptic curves defined over $\mathbb{Q}$ only occur—and do occur—if $1 \leq N \leq 19$ or if $N = 21, 25, 27, 37, 43, 67, 163$. 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 $X_0(37)$. 

1
C. My question is about quadratic points. A general theorem of Faltings has as a particular consequence that, fixing any positive integer \( N \) and ranging over all non-CM 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 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 \( X_0(N) \).

It is natural to ask

- whether there are only finitely many sporadic cyclic isogenies (for the entire range of non-CM-elliptic curves; equivalently, whether there are none at all when \( N \gg 0 \)).
- related questions about specific examples.

Part 1. The format of this general quadratic point question

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:

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 \((X, x_o)\)?

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 \(\infty\), 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 \(\sigma_e\) 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: \(X/\{\text{action of } \sigma_e\} = E/\{\text{action of } \sigma_e\}\).

C. Genus \(\geq 2\). Denoting by \(J(X)\) the Jacobian of \(X\), consider the natural map

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

by sending an unordered pair \(\{x, y\}\) of points on \(X\) to the divisor of degree 0 \(D = x + y - 2x_o\). There are two possibilities:

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

\[
\delta : S(X) \cong \tilde{S}(X) \subset J(X).
\]

- **\(X\) 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) \( X \xrightarrow{h} X/{\text{action of } \sigma} =: \mathcal{P} \) the degree two mapping (to \( \mathcal{P} \), the genus zero quotient).

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:

\[
\begin{array}{ccc}
X & \xrightarrow{\text{Weierstrass pts}} & X/\{\text{action of } \sigma\} = \mathcal{P} \\
\downarrow{g} & & \downarrow{e} \\
X \times X & \rightarrow & S(X) \\
\downarrow{\text{diag}} & & \downarrow{\delta} \\
X & \rightarrow & J(X)
\end{array}
\]

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

**Proposition 1.** We have a diagram:

\[
\begin{array}{ccc}
\mathcal{P} & \xrightarrow{\epsilon} & J(X) \\
\downarrow{\subset} & & \downarrow{=} \\
S(X) & \xrightarrow{\subset} & \tilde{S}(X) \\
\downarrow{=} & & \downarrow{=} \\
S(X) \setminus \mathcal{P} & \xrightarrow{=} & \tilde{S}(X) \setminus \{e\} \xrightarrow{\subset} J(X)
\end{array}
\]

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 \( \bigcup_i A_i \) 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.
Summary 2. The $K$-rational quadratic points (in $S(X)$) can be of these possible types:
- If $X$ is hyperelliptic: a rationally parametrized family of $K$-rational points in $\mathcal{P} \subset S(X)$; and
- if $X$ can be covered by a bielliptic curve, an infinite family of points parametrized by the $K$-rational points of a translate of an elliptic curve in $S(X)$ and
- if the genus of $X$ is 2 and the Mordell-Weil rank over $K$ of $J(X)$ is $> 0$, the infinite family of points parametrized by the $K$-rational points of $J(X)$ and finally:
- the (finitely many) $K$-rational points that don’t fit into any of the frameworks listed above.

Definition 3. Call this finite set of points $\text{Isol}(X; K)$, the set of isolated quadratic points of $X$.

4. Uniformity Conjecture

Following [10] and [11] one might ask whether for any genus $g \geq 3$ there is 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 $|\text{Isol}(X; K)| > U(g)$.

5. Modular Curves

A. The Families:
- Quadratic points of the family $X_1(N)$ for $(N \geq 1)$ have been largely classified and understood (see [20] and the results of Sheldon Kamienny: [7], [8], [9]. 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 [24]; see that article as well for its very useful bibliography. See also [12]).

- $Q$-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] and also [4]. For recent results about quadratic points on ‘nonsplit Cartan’ modular curves, see [21].

- “Generalized Bring’s curves.” These are interesting curves that Karl Rubin and I are starting to think about. (discussion to be included). The classical Bring’s Curve $B$ is the projective curve
over $\mathbb{Q}$ given by the homogenous equations $\sum_i x_i^j = 0$ with $1 \leq i \leq 5$ and $j = 1, 2, 3$. This curve has the symmetry group $S_5$ as a group of automorphisms. It is a bielliptic curve over $\mathbb{Q}$ (not hyperelliptic) and its jacobian is isogenous to a power of a curve of conductor 50, so has Mordell-Weil rank zero. See the recent note of Jennifer Balakrishnan and Netan Dogra [5] that shows that its quadratic points consist of the $S_5$-translates of $(1, -1, i, -i, 0)$.

The next interesting thing to do with Bring’s curve is to make a (quadratic) twist of the curve $B$ by a nontrivial homomorphism $\chi : Gal(L/K) \to Aut(B) = S_5$ for $L/K$ a quadratic extension (taking the image to be the subgroup of $S_5$ generated by a transposition) and ask the same question, noting that the jacobian is the twist of the Bring’s jacobian by the same character—i.e., somehow built out of the corresponding twist of the elliptic curve of conductor 50. There, one has one’s choice: one can consider the analogous cases where the Mordell-Weil rank is zero, or not. If, for example the MW-rank of the twisted elliptic curve is 1, one is in the MW-rank of the jacobian = the dimension of the jacobian case...that people engaged in Chabauty-Coleman-Kim methods like! A question: suppose you want to perform efficient computations, using Chabauty-Coleman-Kim methods, covering lots of twists at once, are there convenient ways of organizing the procedure to make it nicely efficient?

6. Questions about—and references to some of the literature about—quadratic points of the family of modular curves $X_0(N)$ over $\mathbb{Q}$ for $N \geq 1$

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 $K$.

(i) Regarding the first mode of quantifying the problem; i.e., fixing the quadratic field $K$ there is significant recent progress; and specifically focusing on isogenies of prime degree:
**Definition 4.** The set $\text{Isog.} \text{Prime.} \text{Deg}(K)$ 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 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 5.** (Bar) Assuming GRH, we have the following.

\[
\text{Isog.} \text{Prime.} \text{Deg}(\mathbb{Q}(\sqrt{7})) = \text{Isog.} \text{Prime.} \text{Deg}(\mathbb{Q}(\sqrt{-10})) = \text{Isog.} \text{Prime.} \text{Deg}(\mathbb{Q}),
\]

and

\[
\text{Isog.} \text{Prime.} \text{Deg}(\mathbb{Q}(\sqrt{-5})) = \text{Isog.} \text{Prime.} \text{Deg}(\mathbb{Q}) \sqcup \{23\}.
\]

(ii) Regarding the second mode of quantifying the problem; i.e., fixing $N$ let

\[
\mathcal{K}(N) := \bigcup_{K\text{-quadratic}} X_0(N)(K),
\]

i.e., the union of all quadratic (or $\mathbb{Q}$-rational) points on $X_0(N)$.

Since the curves $X_0(N)$ of genus $\leq 2$ have their own natural ways to organize questions about $\mathcal{K}(N)$ let’s fix attention to the values of $N$ where the genus of $X_0(N)$ is $\geq 3$. To repeat subsection [C], a bit, but to be more specific about the classification given there, here are some subsets of $\mathcal{K}(N)$:

(a) $\mathbb{Q}$-Rational points of $X_0(N)$.
(b) Quadratic cusps on $X_0(N)$; i.e., cusps that are rational over a quadratic field.
(c) Parametrized quadratic points of $X_0(N)$; by this I mean the following:

Suppose given a curve with involution defined over $\mathbb{Q}$: $\sigma : C \to C$ which fits into a diagram (defined over $\mathbb{Q}$):

\[
\begin{array}{ccc}
C & \xrightarrow{\phi} & X_0(N) \\
\downarrow^{\text{degree 2}} & & \\
C/\{\sim \sigma\} & \xrightarrow{\simeq} & B
\end{array}
\]

where we are assuming that $\phi$ is a nontrivial covering of $X_0(N)$ by a curve $C$ and that $B$ is of genus $\leq 1$. 
Definition 6. A parametrized quadratic point $x \in X_0(N)(\mathbb{Q})$ is a quadratic point fitting into the pattern:

\[
\begin{array}{c}
\phi \\
\text{degree 2} \\
\end{array}
\]

\[
\begin{array}{c}
c \\
\rightarrow \\
\phi \\
\text{degree 2} \\
\rightarrow \\
\tilde{c} \\
\rightarrow \\
b \in B(\mathbb{Q})
\end{array}
\]

and such that we have a $\mathbb{Q}$-rational point $b \in B(\mathbb{Q})$ where, lifting it to a (quadratic) point $c \in C$, we have $\phi(c) = x$.

So, $C$ is a double cover of $B$, which is either $\mathbb{P}^1$ or an elliptic curve. Since the problem of finding $\mathbb{Q}$-rational points on curves of genus $\leq 1$ is of as somewhat different nature than the problem of finding quadratic points on curves of genus $\geq 3$, it makes sense to distinguish them. Moreover, the issue of finding coverings of the curve $X_0(N)$ of the sort described in [7] is properly an algebraic geometric question rather than a Diophantine one.

(d) CM quadratic points A CM-point of $X_0(N)$ is a point that classifies an elliptic curve with a cyclic $N$-isogeny (hence: a point on $X_0(N)$) of the following form $E \xrightarrow{\alpha} E$. Necessarily (noting the $N > 1$) such an elliptic curve $E$ must have CM.

Definition 8. A sporadic quadratic point of $X_0(N)$ is an element of $\mathcal{K}(N)$ that is not of any of the above four types.

Faltings’ Theorem implies that any $X_0(N)$ of genus $\geq 3$ has only finitely many sporadic quadratic points.

Conjecture 9. (i) There is a finite upper bound $N_o$ such that if $N \geq N_o$ $X_0(N)$ has no parametrized quadratic points.

(ii) There is a finite upper bound $N_1$ such that if $N \geq N_1$ $X_0(N)$ has no sporadic quadratic points.

To get an overall view of the state of literature regarding quadratic points on $X_0(N)$ over $\mathbb{Q}$ I made the attached scorecard that lists all values of $N$—such that $X_0(N)$ is either hyperelliptic, bielliptic, or both; and for which ones do we currently have actual computations of (all?) quadratic points [in the literature that I found]. The values of $N$ put
in boldface are those where the genus of $X_0(N)$ is $\geq 3$, so offer the interesting problem of determining whether they have any sporadic points. Have I missed much of the literature in my scorecard? Are there people working on various aspects of this? E.g., among the people also working on $X_0(N)^+$?

Part 2. A beginning attempt to collect literature around the question.

Below are tables that list some recent work about quadratic points of the modular curves $X_0(N)$ for various values of $N$.

- The first column below gives a complete list of values $N$ such that $X = X_0(N)/\mathbb{Q}$ is (of genus $> 1$, and) either hyperelliptic or bielliptic or both (plus $N = 52$).

- In the second column “h” means hyperelliptic; “b” means bielliptic and the elliptic curve in question has MW-rank 0; “b*” means bi-elliptic with the elliptic curve in question having MW-rank $> 0$.

- The third column tells who determined the isolated quadratic points for that value of $N$: B-N = [9]; O-S = [23]; Box= [8]; —in the references on page 6. And “?” means that it isn’t yet determined (as far as I know).
<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td></td>
<td></td>
<td>h b</td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td>h</td>
</tr>
<tr>
<td>26</td>
<td></td>
<td>h b</td>
<td>B − N</td>
</tr>
<tr>
<td>28</td>
<td>h b</td>
<td></td>
<td>B − N</td>
</tr>
<tr>
<td>29</td>
<td></td>
<td></td>
<td>h</td>
</tr>
<tr>
<td>30</td>
<td>h b</td>
<td></td>
<td>B − N</td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td>h</td>
</tr>
<tr>
<td>33</td>
<td>h b</td>
<td></td>
<td>B − N</td>
</tr>
<tr>
<td>34</td>
<td></td>
<td></td>
<td>b</td>
</tr>
<tr>
<td>35</td>
<td>h b</td>
<td></td>
<td>B − N</td>
</tr>
<tr>
<td>37</td>
<td>h b</td>
<td></td>
<td>Box</td>
</tr>
<tr>
<td>38</td>
<td>b</td>
<td></td>
<td>O − S</td>
</tr>
<tr>
<td>39</td>
<td>h b</td>
<td></td>
<td>B − N</td>
</tr>
<tr>
<td></td>
<td>h</td>
<td>b</td>
<td>B − N</td>
</tr>
<tr>
<td>---</td>
<td>----</td>
<td>----</td>
<td>-------</td>
</tr>
<tr>
<td>40</td>
<td>h</td>
<td>b</td>
<td>B − N</td>
</tr>
<tr>
<td>41</td>
<td>h</td>
<td></td>
<td>B − N</td>
</tr>
<tr>
<td>42</td>
<td>b</td>
<td></td>
<td>O − S</td>
</tr>
<tr>
<td>43</td>
<td></td>
<td>b*</td>
<td>Box</td>
</tr>
<tr>
<td>44</td>
<td>b</td>
<td></td>
<td>O − S</td>
</tr>
<tr>
<td>45</td>
<td>b</td>
<td></td>
<td>O − S</td>
</tr>
<tr>
<td>46</td>
<td>h</td>
<td></td>
<td>B − N</td>
</tr>
<tr>
<td>47</td>
<td>h</td>
<td></td>
<td>B − N</td>
</tr>
<tr>
<td>48</td>
<td>h</td>
<td>b</td>
<td>B − N</td>
</tr>
<tr>
<td>49</td>
<td>h</td>
<td>b</td>
<td>B − N</td>
</tr>
<tr>
<td>50</td>
<td>b</td>
<td></td>
<td>O − S</td>
</tr>
<tr>
<td>51</td>
<td></td>
<td>b</td>
<td>O − S</td>
</tr>
<tr>
<td>52</td>
<td></td>
<td></td>
<td>O − S</td>
</tr>
<tr>
<td>53</td>
<td></td>
<td>b*</td>
<td>Box</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>54</td>
<td>$b$</td>
<td>$O - S$</td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>$b$</td>
<td>$O - S$</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>$b$</td>
<td>$O - S$</td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>$h$</td>
<td>$B - N$</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>$b$</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>$b^*$</td>
<td>$Box$</td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>$b$</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>$b$</td>
<td>$O - S$</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>$b$</td>
<td>$O - S$</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>$b^*$</td>
<td>$Box$</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>$b$</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>$h$</td>
<td>$B - N$</td>
<td></td>
</tr>
</tbody>
</table>
72  $b$  $O - S$

75  $b$  $O - S$

79  $b^*$  ?

81  $b$  $O - S$

83  $b^*$  ?

89  $b^*$  ?

92  $b$  ?

94  $b$  ?

95  $b$  ?

101  $b^*$  ?

119  $b$  ?

131  $b^*$  ?
References