CYCLIC ISOGENIES OF ELLIPTIC CURVES OVER FIXED QUADRATIC FIELDS

BARINDER S. BANWAIT, FILIP NAJMAN, AND OANA PADURARIU

Abstract. Building on Mazur's 1978 work on prime degree isogenies, Kenku determined in 1981 all possible cyclic isogenies of elliptic curves over $\mathbb{Q}$. Although more than 40 years have passed, the determination of cyclic isogenies of elliptic curves over a single other number field has hitherto not been realised.

In this paper we develop a procedure to assist in establishing such a determination for a given quadratic field. Executing this procedure on all quadratic fields $\mathbb{Q}(\sqrt{d})$ with $|d| < 10^4$ we obtain, conditional on the Generalised Riemann Hypothesis, the determination of cyclic isogenies of elliptic curves over 19 quadratic fields, including $\mathbb{Q}(\sqrt{213})$ and $\mathbb{Q}(\sqrt{-2289})$. To make this procedure work, we determine all of the finitely many quadratic points on the modular curves $X_0(125)$ and $X_0(169)$, which may be of independent interest.

1. Introduction

An important problem in the theory of elliptic curves over number fields is to understand their possible torsion groups, parametrised by noncuspidal points on the modular curves $X_1(m,n)$, and possible isogenies, parametrised by noncuspidal points on $X_0(N)$. Mazur [Maz77] determined the possible torsion groups over $\mathbb{Q}$ and Kamienny, Kenku and Momose [Kam92, KM88] determined the possible torsion groups over quadratic fields. More recently, Derickx, Etropolski, van Hoeij, Morrow and Zureick-Brown [DEv$^+$21] determined the possible torsion groups over cubic fields and Derickx, Kamienny, Stein and Stoll [DKSS] determined all the primes dividing the order of some torsion group over number fields of degree $4 \leq d \leq 7$. Merel proved that the set of all possible torsion groups over all number fields of degree d is finite, for any positive integer d [Mer96]. All the possible torsion groups over a fixed number field K, for many fixed number fields of degree 2, 3 and 4 have been determined, see [Naj10, BN16, Trb20], but all the possible isogenies have not been determined over a single number field other than $\mathbb{Q}$.

Unfortunately, much less is known about possible isogeny degrees - for any $d > 1$ it is not known what the possible cyclic isogeny degrees of all elliptic curves over all number fields of degree d are. However, the second author [Naj18] determined all the prime degree isogenies of non-CM elliptic curves E with $j(E) \in \mathbb{Q}$ for number fields $d \leq 7$ (and conditionally on Serre's uniformity conjecture for all d). This has been extended to all $d > 1.4 \times 10^7$ unconditionally by Le Fourn and Lemos [LL21, Theorem 1.3].

Mazur [Maz78] determined all the possible primes which arise as degrees of rational isogenies over $\mathbb{Q}$, and explained in the introduction of his paper that to determine all the possible cyclic isogeny degrees, it suffices to determine the $\mathbb{Q}$-rational points on $X_0(N)$ for a small list $S(\mathbb{Q})$ of composite integers N. We will

2010 *Mathematics Subject Classification.* 11G05 (primary), 11Y60, 11G15. (secondary).

recall this method allowing one to go from prime degree isogenies to composite degree isogenies in Section 2, and will henceforth refer to it as *Mazur's strategy*. Results known at the time allowed Mazur to deal with all but five of these values, viz. $N = 39, 65, 91, 125, 169$. These five cases were subsequently dealt with by Kenku [Ken79, Ken80a, Ken80b, Ken81], who showed for these five values that $X_0(N)(\mathbb{Q})$ consists only of the cusps, yielding the explicit determination of the cyclic isogeny degrees over the rationals. The results are summarized in Table 1.1 below, in which g denotes the genus of $X_0(N)$ and ν is the number of noncuspidal $\mathbb{Q}$-rational points on $X_0(N)$.

N	g	ν	N	g	ν	N	g	ν
≤ 10	0	∞	11	1	3	37	2	2
12	0	∞	14	1	2	43	3	1
13	0	∞	15	1	4	67	5	1
16	0	∞	17	1	2	163	13	1
18	0	∞	19	1	1			
25	0	∞	21	1	4			
			27	1	1			

TABLE 1.1. Cyclic isogenies over $\mathbb{Q}$.

Theorem 1.1 (Mazur, Kenku)**.** *Table 1.1 is a complete classification of all rational cyclic isogenies of elliptic curves over* $\mathbb{Q}$*.*

Since the appearance of Kenku's final paper in 1981, such an explicit determination has not been exhibited for *any other number field*. This is the primary motivation for the present work. An important ingredient in our work will be the algorithm to determine isogenies of prime degree for fixed quadratic fields K recently developed by the first author [Ban22] assuming the Generalised Riemann Hypothesis (GRH). Computing the resulting composite integers $S(K)$ to be treated in Mazur's strategy yields a list typically larger than $S(\mathbb{Q})$. Although the subject of higher degree points on modular curves has seen much recent development (see e.g. [Box21, AAB$^+$21, NV, BGG21]), some of the values $N \in S(K)$ are such that $X_0(N)$ has large genus, and therefore the determination of the K-rational points on $X_0(N)$ is beyond current methods. For this reason, we search for 'convenient' quadratic fields K for which (among other conditions) the largest value in $S(K)$ is 169. This limits the genus of $X_0(N)$ and thereby allows many of the recently developed computational methods to succeed. Our search strategy will be explained in Section 3.

Among the quadratic fields $\mathbb{Q}(\sqrt{d})$ with $|d| < 10^4$, we find 133 which satisfy our definition of convenient, and therefore, for these quadratic fields, we have some positive hope that we may be able to completely determine the $\mathbb{Q}(\sqrt{d})$-rational points on $X_0(N)$ for $N \in S(\mathbb{Q}(\sqrt{d}))$. Carrying out this program - that is, applying the various known methods (summarised in Section 4) for determining whether or not $X_0(N)$ has noncuspidal quadratic points over a fixed quadratic field - is the main technical heart of the paper, and yields our main result.

Theorem 1.2. *Let d be one of the following* 19 *values:*

$$\begin{gathered} -6846,\ -2289,\ 213,\ 834,\ 1545,\ 1885,\ 1923, \\ 2517,\ 2847,\ 4569,\ 6537,\ 7131,\ 7302, \\ 7319,\ 7635,\ 7890,\ 8383,\ 9563,\ 9903. \end{gathered} \tag{1.1}$$

Then, assuming GRH, Table 7.1 lists all cyclic isogenies of elliptic curves defined over $\mathbb{Q}(\sqrt{d})$ that are not contained in Table 1.1.

For the convenience of the reader, we provide here the analogous table to Table 1.1 for the smallest absolute value in the list (1.1).

N	g	ν	N	g	ν	N	g	ν
≤ 10	0	∞	14	1	2	27	1	∞
12	0	∞	15	1	∞	32	1	∞
13	0	∞	17	1	2	36	1	∞
16	0	∞	19	1	1	37	2	2
18	0	∞	20	1	∞	43	3	1
25	0	∞	21	1	4	67	5	1
11	1	3	24	1	∞	163	13	1

TABLE 1.2. Cyclic isogenies over $\mathbb{Q}(\sqrt{213})$, assuming GRH.

Comparing this with the situation of isogenies over $\mathbb{Q}$, we observe several more values of N for which there are infinitely many elliptic curves with a cyclic isogeny of degree N over our quadratic field. These are all explained by the genus 1 modular curves which attain positive rank over $\mathbb{Q}(\sqrt{d})$. We do not obtain values of N larger than those over $\mathbb{Q}$ due to our searching for 'convenient' quadratic fields to consider.

Obtaining such results for a general number field K (not just quadratic) will require enumeration of the K-rational points on some of the same modular curves each time. Indeed, as shown in Lemma 2.2, the values $N = 91, 125, 163, 169$ are guaranteed to arise whenever one attempts to enumerate the cyclic isogenies over any given number field. Since, for these values of N, the modular curve $X_0(N)$ admits only finitely many quadratic points, it would be valuable to have an explicit answer to the following.

Question 1.3. For $N = 91, 125, 163, 169$, can one determine all of the finitely many quadratic points on $X_0(N)$?

Determining the quadratic points on $X_0(91)$ has recently been done by Vukorepa [Vuk]. In this paper we deal with 125 and 169, yielding the following result.

Theorem 1.4. *All finitely many quadratic points on $X_0(125)$ and $X_0(169)$ are as described in Table 6.1 and Table 6.2 in Section 6.*

Of particular note here is the existence of a point on $X_0(125)$ defined over the quadratic field $\mathbb{Q}(\sqrt{509})$ which is not CM and which appears not to have been previously known. Evaluating the j-map at this point yields the following j-invariant of an elliptic curve over $\mathbb{Q}(\sqrt{509})$ which admits a cyclic 125-isogeny:

$$j_{509} = \frac{2140988208276499951039156514868631437312 \pm 948976338978410928412003346760125644 80\sqrt{509}}{161051}.$$

This is perhaps surprising because, as N gets larger, the non-CM quadratic points on $X_0(N)$ become rarer; for example we note that, of the curves $X_0(N)$ appearing in [NV] which have finitely many quadratic points, all of them have either no noncuspidal points or only CM points.

As in Kenku's work, most of the effort for the determination of cyclic isogenies lies in showing that $X_0(N)$ consists only of the cusps. The methods that we use for this have been implemented in Sage [The20]. Moreover, obtaining Theorem 1.4 was achieved with the aid of Magma [BCP97], and certain parts of the computation were verified in PARI/GP [The21]. All of the the code used in our work may be found at the following GitHub repository:

`https://github.com/barinderbanwait/quadratic_kenku_solver`

Paths to filenames given throughout the paper are relative to the top directory in this repository. In particular, we note that this repository has developed a command line tool (in `sage_code/quadratic_kenku_solver.py`) which automates many of the necessary steps to assist in the determination of cyclic isogenies over a given quadratic field (more details at the end of Section 7).

The outline of the paper is as follows. Section 2 explains the strategy of Mazur to reduce the problem to determining all K-rational points on a finite and computable list of modular curves. Section 3 describes the searching method to identify the 133 convenient quadratic fields, and Section 4 gives an overview of the methods we used to determine K-rational points on modular curves for fixed quadratic fields K. While the 19 values in 1.1 were found from running our implementation, it would be illuminating for the reader to have one case worked out in detail; this is done in Section 5 for the quadratic field $\mathbb{Q}(\sqrt{213})$. Theorem 1.4 is proved in Section 6, and Section 7 carries out the computation of the "graph of rational isogenies", which is Part 2 of Mazur's strategy. Finally in Section 8 we outline avenues for further work into this problem.

Acknowledgements. It is a pleasure to thank Jennifer Balakrishnan, Francesca Bianchi, Xavier Guitart, Barry Mazur, Philippe Michaud-Jacobs, Steffen Müller, Jeroen Sijsling, Samir Siksek, Michael Stoll and Borna Vukorepa for helpful comments, discussions and correspondence. We thank John Cremona for suggesting improvements to the Sage implementation of some of our algorithms, and Andrew Sutherland for encouraging us to extend the range of quadratic fields to consider. We are grateful to the organisers of the 'Modern Breakthroughs in Diophantine Problems' workshop, held in June 2022 at the Banff International Research Station in Banff, Canada, which provided the venue for all authors to meet together physically for the first time and to improve the results of the paper.

The first author is grateful to the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation for being granted access to computational resources required for this project. The second author was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313. The third author is supported by NSF grant DMS-1945452 and Simons Foundation grant #550023.

2. Mazur's strategy

Throughout this section K will denote a number field that does not contain the Hilbert class field of an imaginary quadratic field, unless otherwise specified.

Mazur's approach to settling the question of rational isogenies for all N was based on the following notion: an integer N is said to be **minimal of positive genus** if the genus of $X_0(N)$ is positive, but the genus of $X_0(d)$ is zero for all proper divisors d of N. Note that if $N \geq 17$ is prime, then N is minimal of positive genus.

The strategy then is to carry out the following two computational steps:

(a) one determines $X_0(N)(\mathbb{Q})$ for all N which are minimal of positive genus, and
(b) for every elliptic curve $E/\mathbb{Q}$ possessing a rational N-isogeny, with N minimal of positive genus, one determines the "graph of rational isogenies" of E.

Here, by "graph of rational isogenies of E", one means to construct the finitely many elliptic curves which are isogenous to E via a rational isogeny, as well as determine the isogenies of minimal degree between the curves in this isogeny class. See [Cre97, Section 3.8] for more on the computations for this over $\mathbb{Q}$.

The fact that step (a) is a finite computation rests both on Mazur's main theorem in [Maz78] that $X_0(p)(\mathbb{Q})$ consists only of the cusps for primes $p > 163$, as well as on the fact that whenever $X_0(N)$ is an elliptic curve, $X_0(N)$ has rank zero over $\mathbb{Q}$. However, neither of these statements is necessarily true over other number fields. We therefore introduce a new notion.

Definition 2.1. Let K be a number field that does not contain the Hilbert class field of an imaginary quadratic field. An integer N is said to be **minimally finite for** K if the following conditions are satisfied:

(1) $X_0(N)(K)$ is finite;
(2) $X_0(d)(K)$ is infinite for all proper divisors d of N;
(3) N is supported only at primes p for which there exists an elliptic curve over K admitting a K-rational p-isogeny.

The set of such integers is denoted $\mathsf{MF}(K)$.

The restriction on K and condition 3 have been included to ensure that $\mathsf{MF}(K)$ is a finite set; for otherwise it will trivially contain every prime $p \geq 23$. (This diverges slightly from Mazur's framing of the notion of minimal of positive genus, since again, every prime $p \geq 23$ is trivially minimal of positive genus; however, apart from 37, 43, 67 and 163, $X_0(p)(\mathbb{Q})$ consists only of the cusps, so can be ignored in the subsequent step (b).)

Mazur's strategy for general K then proceeds with this new notion as follows:

(a) one determines $X_0(N)(K)$ for all N which are minimally finite for K, and
(b) for every elliptic curve E/K possessing a rational N-isogeny, with N minimally finite for K, one determines the "graph of rational isogenies" of E.

Step (b) is a trivial matter to deal with; indeed, all of Sage [The20], PARI/GP [The21] and Magma [BCP97] have fast implementations for computing the isogeny graph of a given elliptic curve; see Section 7 for details on this.

In this section we first identify the set of levels N that necessarily arise in step (a) for any number field K. We refer to these levels N as *always minimally finite*, and denote this set by AMF.

Lemma 2.2. *We have*

$$\mathsf{AMF} = \{26, 35, 37, 39, 43, 50, 65, 67, 91, 125, 163, 169\}.$$

Proof. The set of integers N which are minimally finite for *every* number field must have the property that $X_0(N)(K)$ is finite for every number field K, but for every proper divisor $d \mid N$, $X_0(d)(K)$ is infinite. If N is prime, then this latter condition is empty, and we find that the genus of $X_0(N)$ must be greater than 1. Condition 3 then implies that N must be one of 37, 43, 67 and 163. For composite N, by considering the genera of $X_0(N)$ and $X_0(d)$, one sees that the set of such levels N is precisely the subset of the composite integers identified by Mazur as being minimal of positive genus, with the further restriction that $X_0(N)$ does not have genus 1. Mazur's list is given as

$$14, 15, 20, 21, 24, 26, 27, 32, 35, 36, 39, 49, 50, 65, 91, 125, 169$$

from which one obtains AMF as in the statement above. □

Next, we describe a procedure which allows one to determine the $\mathsf{MF}(K)$ for a given number field K. This procedure is an algorithm if one assumes the Birch-Swinnerton–Dyer conjecture, as the only issue that stops it from being an algorithm unconditionally is the computation of the rank of elliptic curves over $\mathbb{Q}$ in step 1 below. This procedure works very quickly in practice and in the vast majority of cases gives an unconditionally true result, hence we will refer to it as an algorithm.

Algorithm 2.3. *Given a number field K not containing the Hilbert class field of an imaginary quadratic field, compute $\mathsf{MF}(K)$ as follows.*

(1) (Genus 1) Compute the set of N for which $X_0(N)$ is an elliptic curve with rank 0 over K; call this set $S_1(K)$; denote by $B(K)$ the complementary set of N for which $X_0(N)$ is an elliptic curve with positive rank over K;
(2) (Genus ≥ 2; prime level) Compute the set of primes p for which $X_0(p)(K)$ admits noncuspidal points and has genus ≥ 2; call this set $S_2(K)$;
(3) (Genus ≥ 2; composite level) Compute the set of products pb for

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19\}$$

and $b \in B(K)$; call this set $S_3(K)$;
(4) Set $\mathsf{Output} := S_1(K) \cup S_2(K) \cup S_3(K) \cup \mathsf{AMF}$;
(5) (Remove multiples) Remove multiples from Output (that is, values y in Output for which there exists an x in Output such that x divides y);
(6) Return Output.

Proof. We need to prove that the output of the algorithm is indeed $\mathsf{MF}(K)$ as claimed.

We first consider minimally finite N for which $X_0(N)$ has genus 1. This means that $X_0(N)$ is an elliptic curve with rank 0 over K. There are only twelve levels N for which $X_0(N)$ is an elliptic curve, viz.

$$11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49, \tag{2.1}$$

and it is readily observed that for each integer N in this list, any proper divisor d of N is such that $X_0(d)$ has genus 0, so in particular admits infinitely many K-rational points. Thus the levels N in this list for which $X_0(N)$ has rank 0 over K are indeed minimally finite for K; this accounts for the set $S_1(K)$ in step 1.

We next consider minimally finite N for which $X_0(N)$ has genus > 1. For the prime values of N, this is covered by the set $S_2(K)$ in step 2 , so for the rest of the proof we consider the case of composite N. We observe that the only primes which may divide N are the primes ≤ 19, since primes $p \geq 23$ are such that the genus of $X_0(p)$ is at least 2 (and hence admit only finitely many K-rational points).

By definition of N being minimally finite, we have that $X_0(d)(K)$ is infinite for all proper divisors d of N. There are two ways this could happen: either all of the $X_0(d)$ have genus 0; or at least one of them has genus 1 and has positive rank over K. The first case yields integers which must be contained in AMF, so we are further reduced to considering the levels N which are multiples of the integers in $B(K)$ computed in step 1. Moreover, since any multiple of the integers in 2.1 yields an N for which $X_0(N)$ has genus at least 2, we may restrict to considering only multiples of the integers in $B(K)$ by prime values which, as we observed earlier, are bounded by 19. This explains the computation happening in step 3.

Step 5 is required since the set Output computed in step 4 may contain multiples within it (that is, one member is a proper multiple of another). These proper multiples are clearly not minimal of positive genus, so are removed before being returned. □

Remark 2.4. With the exception of the set $S_2(K)$, the above algorithm is implemented as `minimally_finite(d)` in `sage_code/utils.py`. For $S_2(K)$, one may use the program *Isogeny Primes* explained in [BD22], building on work of the first author [Ban22].

Example 2.5. Running the program *Isogeny Primes* for the two quadratic fields $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{5})$ yields that the sets S_2 in each case are $\{23\}$ and $\{23, 47\}$ respectively. Therefore, running `minimally_finite(d)` for $d = -5$ and 5 we obtain the following.

$$\begin{aligned} \mathsf{MF}(\mathbb{Q}(\sqrt{-5})) &= \mathsf{AMF} \cup \{23, 11, 15, 17, 19, 20, 28, 36, 42, 48, \\ &\qquad 54, 63, 64, 81, 98, 147, 343\}. \\ \mathsf{MF}(\mathbb{Q}(\sqrt{5})) &= \mathsf{AMF} \cup \{23, 47, 11, 14, 15, 19, 20, 21, 24, 34, \\ &\qquad 36, 49, 51, 54, 64, 81, 85, 119, 221, 289\}. \end{aligned} \tag{2.2}$$

3. Searching for convenient quadratic fields

Equation (2.2) shows that, to carry out Mazur's strategy for the two quadratic fields $K = \mathbb{Q}(\sqrt{5})$ and $K = \mathbb{Q}(\sqrt{-5})$, it is necessary to determine the K-rational points on large genus modular curves such as $X_0(289)$ and $X_0(343)$. Unfortunately, the large genera of these curves is a significant obstacle to employing several of the known methods for determining quadratic points on modular curves.

For this reason we searched through all squarefree integers $-10{,}000 < d < 10{,}000$ and returned d if the following conditions were satisfied:

(1) $\mathbb{Q}(\sqrt{d})$ is not an imaginary quadratic field of class number one (which ensures that the set of cyclic isogeny degrees is finite);
(2) the values in $\mathsf{MF}(\mathbb{Q}(\sqrt{d}))$ larger than 100 are only either the unavoidable 125, 163 and 169, or are values N for which all of the quadratic points on $X_0(N)$ have been determined;

(3) the Mordell-Weil group of the Jacobian of the modular curve $X_0^+(163)$ does not grow when base-extended from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{d})$.

The third filter here has been employed to enable the 'No growth in plus-part' method explained in Section 4 to successfully deal with the case of 163, which is otherwise a difficult case to surmount. Values d surviving these filters are the 'convenient' values mentioned in the Introduction, since the subsequent task of determining all $\mathbb{Q}(\sqrt{d})$-rational points on the finitely many resulting modular curves is made somewhat easier to carry out.

The search algorithm is implemented as `search_convenient_d` in `sage_code/utils.py`; running it for the range described above yields 133 convenient values of d, the smallest of which is -9946, the largest is 9995, and only 26 of which are negative.

4. Overview of the methods used

This section gives an overview of the methods we employ to determine the K-rational points on modular curves (for K a quadratic field). The following notation will be used:

$$\begin{aligned}
K &= \text{a quadratic field;}\\
J_0(N) &= \text{Jacobian variety of } X_0(N);\\
w_N &= \text{Atkin-Lehner involution on } X_0(N);\\
X_0^+(N) &= X_0(N)/\langle w_N\rangle;\\
J_0(N)_+ &= \text{the sub-abelian variety } (1+w_N)J_0(N);\\
J_0(N)_- &= \text{the sub-abelian variety } (1-w_N)J_0(N);\\
J_0^+(N) &= \text{the quotient abelian variety } J_0(N)/J_0(N)_-;\\
J_0^-(N) &= \text{the quotient abelian variety } J_0(N)/J_0(N)_+.
\end{aligned}$$

Thus $J_0^+(N)$ (respectively $J_0^-(N)$) are quotients of $J_0(N)$ on which w_N acts as $+1$ (respectively -1). Moreover, from [Maz77, Chapter II Section 10], we have that $J_0^+(N)$ and $J_0(N)_+$ are isomorphic as abelian varieties over $\mathbb{Q}$.

4.1. **Quotient Method.** Given an explicit map between curves $\varphi : C \to D$, whenever we are able to determine the K-rational points on D, we can compute their preimages and so determine $C(K)$. A particularly convenient case is when D is an elliptic curve of rank 0 over K. This is used to deal with $N = 37$ in Section 5.2.

4.2. **Catalogues of quadratic points.** We use existing classifications of quadratic points on low-genus modular curves, due to several independent works in recent years; in order of appearance, these are: Bruin-Najman [BN16], Özman-Siksek [ÖS19], Box [Box21], Najman-Vukorepa [NV], and Vukorepa [Vuk]. In short, quadratic points on $X_0(N)$ are classified **non-exceptional** or **exceptional** according to whether or not they arise as pullbacks of $\mathbb{Q}$-rational points on a quotient $X_0(N)/\langle w_d\rangle$ (d is usually chosen such that the quotient is of minimal genus). Apart from $N = 37$ which is known to be a special case and is treated separately in Box's paper, there are only finitely many exceptional quadratic points, and the aforementioned works determine all such. In some cases, there are only finitely many quadratic points at all, and these are completely determined in those cases.

4.3. **Özman sieve.** Even when there are infinitely many non-exceptional quadratic points on $X_0(N)$, it is sometimes possible to rule out the existence of such points over fixed quadratic fields. One method for this is based on a result of Özman [Özm12], and is explained in greater detail as Proposition 7.3 in [Ban22]. This is used for $N = 65$ in Section 5.3. The package *Isogeny Primes* mentioned in Remark 2.4 contains an implementation of the Özman sieve.

4.4. **Trbović filter.** Another method to rule out possible non-exceptional quadratic points on $X_0(N)$ is based on work of the second author with Trbović [NT22, Theorem 2.13], and applies in the case that $X_0(N)$ is hyperelliptic of genus ≥ 2. The aforementioned result lists the primes less than 100 which must be unramified in any quadratic field K such that $X_0(N)$ admits a K-rational point which is not a $\mathbb{Q}$-rational point. These unramified primes have been encoded into `sage_code/quadratic_points_catalogue.json`. We refer to this method as the **Trbović filter**, and is used to deal with all hyperelliptic values we need to consider apart from $N = 37$.

4.5. **The 'No growth in plus-part' method.** This is analogous to the 'No growth in minus-part' method of [Ban22, Lemma A.2], and may be summarised as follows.

Proposition 4.1. *Let K be a quadratic field, and N an integer such that:*
(1) $X_0^+(N)$ has positive genus;
(2) $J_0^+(N)(K)$ has trivial torsion;
(3) $\mathrm{rk}(J_0^+(N)(K)) = \mathrm{rk}(J_0^+(N)(\mathbb{Q}))$;
Then any K-rational point on $X_0(N)$ arises as the pull-back of a $\mathbb{Q}$-rational point on $X_0^+(N)$.

Proof. For ease of notation in this proof, we write $J = J_0^+(N)$, which by condition 1 is non-trivial. Conditions 2 and 3 tell us that $J(K)$ and $J(\mathbb{Q})$ are isomorphic as abstract groups. We begin by showing that, in fact, they are equal as sets.

Let $r = \mathrm{rk}J(\mathbb{Q}) = \mathrm{rk}J(K)$, let $V = [v_1, \ldots, v_r]$ be the vector of generators of $J(\mathbb{Q})$, and let $W = [w_1, \ldots, w_r]$ be the vector of generators for $J(K)$. Then there exists an $r \times r$ matrix M with coefficients in $\mathbb{Z}$ such that $MW = V$. The matrix M^{-1} may not have coefficients in $\mathbb{Z}$, but there exists an integer d such that dM^{-1} has integer coefficients. Then

$$dW = (dM^{-1})V,$$

so $dw_i = d\overline{w_i} \in J(\mathbb{Q})$. Then $d(w_i - \overline{w_i}) = 0$, which implies that either $w_i = \overline{w_i}$ or we have a torsion point. Since the torsion of $J(K)$ is trivial, we conclude that $J(K) = J(\mathbb{Q})$ as sets.

Writing C for $X_0^+(N)$, this implies that $C(K) = C(\mathbb{Q})$. Indeed, fixing a $\mathbb{Q}$-rational point P of C (e.g. the image of any of the $\mathbb{Q}$-rational cusps of $X_0(N)$) and considering the Abel-Jacobi map

$$\iota_P : C \to J, \quad Q \mapsto [Q - P],$$

we see that, if $Q \in C(K)$, then $\iota_P(Q) = [Q - P] \in J(K) = J(\mathbb{Q})$, and hence $Q \in C(\mathbb{Q})$. Therefore, we find that any K-rational point on $X_0(N)$ in fact arises as the pullback of a $\mathbb{Q}$-rational point on $X_0^+(N)$ under the natural map $X_0(N) \to X_0^+(N)$. □

This is used to deal with $N = 37$ in Section 5.2, and $N = 43$ and 163 in Section 5.3. The reason we call this the 'no growth in plus-part' method is because condition 2 is equivalent to $J_0^+(N)$ gaining no new torsion when base-changed from $\mathbb{Q}$ to K; indeed, that $J_0^+(N)$ has only trivial $\mathbb{Q}$-torsion is a theorem of Mazur [Maz77, Theorem 3].

4.6. **Symmetric Chabauty with Mordell-Weil sieve.** The determination of all quadratic points on $X_0(N)$ for $N = 125$ and $N = 169$ is approached using the Box-Siksek method as developed in [Box21], and using the improvements developed in [NV]. The Box-Siksek method is based on a combination of Siksek's relative Symmetric Chabauty method as developed in [Sik09] together with a Mordell-Weil sieve. We will give more details of this in Section 6 for our particular setup.

5. An example - Cyclic isogenies over $\mathbb{Q}(\sqrt{213})$

To illustrate how the methods in the previous section may be used to carry out step (a) of Mazur's strategy, we provide an extended example with the smallest absolute value of d for which we were able to successfully determine all cyclic isogenies over $\mathbb{Q}(\sqrt{d})$, namely, $d = 213$. The set of minimally finite values to be considered here is as follows.

$$\begin{aligned}\mathsf{MF}(\mathbb{Q}(\sqrt{213})) = \mathsf{AMF} \cup \{&11, 14, 17, 19, 21, 30, 40, 45, 48,\\ &49, 54, 64, 72, 75, 81\}.\end{aligned} \tag{5.1}$$

Since the determination of rational points on $X_0(N)$ depends in large part on the geometry of the modular curve, we have split the values of N to be considered according to whether the curve is elliptic, hyperelliptic, or non-hyperelliptic. Throughout this section we set $K = \mathbb{Q}(\sqrt{213})$.

5.1. **The elliptic cases.** Here we deal with the values of N in $\mathsf{MF}(K)$ for which $X_0(N)$ is an elliptic curve.

Lemma 5.1. *Let $K = \mathbb{Q}(\sqrt{213})$, and let N be an integer such that $X_0(N)$ has genus 1, viz.*

$$11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49.$$

Then $X_0(N)(K)_{tors} = X_0(N)(\mathbb{Q})_{tors}$. In particular, for the genus one values N in $\mathsf{MF}(K)$ in Equation (5.1), the j-invariants of K-rational points on $X_0(N)$ are the same as over $\mathbb{Q}$, which are given in Table 5.1.

Proof. The claims here are all readily achieved via Magma computation; for verifying no growth in torsion see the procedure `CheckTorsionGrowth`, and for the computation of j-invariants see `EllipticJInvs`, both in `magma_code/utils.m` □

5.2. **The hyperelliptic cases.** In this section we deal with the minimally finite N for which $X_0(N)$ is hyperelliptic of genus at least 2, which are as follows:

$$26, 30, 35, 37, 39, 40, 48, 50. \tag{5.2}$$

Proposition 5.2. *For N as in 5.2, we have $X_0(N)(K) = X_0(N)(\mathbb{Q})$. In particular, for $N \neq 37$, $X_0(N)(K)$ consists only of the cuspidal points, and $X_0(37)(K)$ admits two noncuspidal points defined over $\mathbb{Q}$, with corresponding j-invariants:*

$$-9317 \textit{ and } -162677523113838677.$$

N	$j(X_0(N)(\mathbb{Q}))$
11	$-32768, -24729001, -121$
14	$-3375, 16581375$
17	$\frac{-882216989}{131072}, \frac{-297756989}{2}$
19	-884736
20	✗
21	$\frac{-189613868625}{128}, \frac{3375}{2}, \frac{-140625}{8}, \frac{-1159088625}{2097152}$
36	✗
49	✗

Table 5.1. The finitely many j-invariants of elliptic curves corresponding to $\mathbb{Q}$-rational points on genus one modular curves $X_0(N)$. The symbol ✗ means that $X_0(N)(\mathbb{Q})$ consists only of cusps.

Proof. The Trbović filter (Section 4.4) applies to all of the values we need to consider apart from $N = 37$, and shows, for each such N and K, that $X_0(N)(K) = X_0(N)(\mathbb{Q})$. The verification of this may be found in `sage_code/hyperelliptic_verifs.py`. That the $\mathbb{Q}$-rational points on these modular curves consists only of the cusps was already known to Mazur prior to the appearance of [Maz78].

For $N = 37$ we take the following model for the genus 2 curve $X_0(37)$:

$$X_0(37) : y^2 = -x^6 - 9x^4 - 11x^2 + 37.$$

Taking the quotient of $X_0(37)$ by the isomorphism $(x, y) \mapsto (-x, -y)$ we obtain an elliptic curve $E/\mathbb{Q}$ of rank 0 over K. (The elliptic curve E is $J_0(37)^-$, with Cremona label 37b1.) By looking at the preimages of the finitely many points in $E(K)$ we may conclude that $X_0(37)(K) = X_0(37)(\mathbb{Q})$ (see the function `ComputePreimages` in `magma_code/X037.m`) for this verification). That this latter set admits only two noncuspidal points is a classical result of Mazur and Swinnerton-Dyer [MSD74, Proposition 2]. □

5.3. **The non-hyperelliptic cases.** In this section we deal with the non-hyperelliptic minimally finite N, which are as follows:

$$43, 45, 54, 64, 65, 67, 72, 75, 81, 91, 125, 163, 169. \tag{5.3}$$

Proposition 5.3. *For N as in 5.3, we have $X_0(N)(K) = X_0(N)(\mathbb{Q})$. In particular, for $N \notin \{43, 67, 163\}$, $X_0(N)(K)$ consists only of the cuspidal points, and for $N \in \{43, 67, 163\}$, $X_0(N)$ admits precisely one noncuspidal point, whose corresponding j-invariants are given in Table 5.2.*

N	g	ν	$j(X_0(N)(K))$
43	3	1	-884736000
67	5	1	-147197952000
163	13	1	-262537412640768000

Table 5.2. The j-invariants of the noncuspidal rational points on $X_0(43)$, $X_0(67)$, and $X_0(163)$.

The proof will occupy the rest of the section. A number of claims are established via Sage or Magma computation; these can respectively be found in `sage_code/non_hyperelliptic_verifs.py` or `magma_code/non_hyperelliptic_verifs.m`.

5.3.1. *$N = 43$.* We apply [Ban22, Lemma A.2], where we use steps 5–7 of [BD22, Algorithm 7.9] to show that $J_0(43)_-(K) = J_0(43)_-(\mathbb{Q})$. This shows that the only source of K-rational points on $X_0(43)$ beyond the $\mathbb{Q}$-rational points must correspond to elliptic curves with CM by an order in $\mathbb{Q}(\sqrt{-43})$. The inbuilt Sage function `cm_j_invariants` shows that the j-invariant of any such elliptic curve must be defined over $\mathbb{Q}$, whence we find that the only K-rational point on $X_0(43)$ corresponds to the $\mathbb{Q}$-rational point, which is a CM-point with discriminant -43, whose j-invariant is -884736000.

The code to verify the computational claims made here may be found in `sage_code/non_hyperelliptic_verifs.py`.

5.3.2. *$N = 45, 54, 63, 64, 72, 75, 81$.* This follows directly from [ÖS19, Tables].

5.3.3. *$N = 65$.* [Box21, Section 4.5] shows that $X_0(65)$ admits no exceptional quadratic points, and the Özman sieve shows that it admits no non-exceptional K-rational points.

5.3.4. *$N = 67$.* [Box21, Section 4.6] determined all quadratic points on $X_0(67)$. From this we obtain that the only K-rational point on $X_0(67)$ is the one CM point defined over $\mathbb{Q}$, with j-invariant -147197952000.

5.3.5. *$N = 91$.* This is dealt by Vukorepa [Vuk] where all the quadratic points on $X_0(91)$ are determined, and none are rational over K.

5.3.6. *$N = 163$.* We apply Proposition 4.1 to show that any K-rational points on $X_0(163)$ must arise as pullbacks of $\mathbb{Q}$-rational points on $X_0^+(163)$. Conditions 2 and 3 are checked in `magma_code/NonHyperellipticVerifs.m`. [AAB+21, Section 5.3] shows that $X_0^+(163)(\mathbb{Q})$ consists only of one cusp, together with CM-points. Therefore, any pullback of these points under the hyperelliptic involution must themselves be either cuspidal or CM points. As in Section 5.3.1, a quick Sage computation reveals that we have only the one $\mathbb{Q}$-rational CM-point known to Mazur.

5.3.7. *$N = 125, 169$.* These are dealt with in Section 6.

This concludes step (a) of Mazur's strategy for $\mathbb{Q}(\sqrt{213})$. Step (b) will be carried out in Section 7.

6. Quadratic points on $X_0(125)$ and $X_0(169)$

In this section we compute all the quadratic points on $X_0(125)$ and $X_0(169)$. To do this, we apply the approach developed by the second author with Vukorepa [NV], which in turn builds on the results of Box [Box21] and Siksek [Sik09].

In particular, we use the same approach which had been used in [NV, Section 7.5.] to determine the quadratic points on $X_0(131)$. Let $N = 125$ or 169, let $D_\infty := 0 + \infty$ the sum of the two rational cusps of $X_0(N)$. Using the sieve from [NV] using the operator $I := 1 - w_N$, we obtain that for any unknown effective rational divisor of degree 2 in $X_0(N)^{(2)}$, it holds that $(1 - w_N)[Q - D_\infty] = 0$. It follows that $[Q - D_\infty] = w_N([Q - D_\infty])$ and hence, since w_N acts trivially on D_∞,

Name	d	Coordinates	j-invariant	CM
P_1	-1	$(-2w : 1/2w : w : w : 1/2w : 1/2w : 1 : 1)$	287496	-16
P_2	509	$(-38/509w : 21/509w : -12/509w : 5/509w : 1/509w : -1/509w : -1 : 1)$	j_{509}	NO
P_3	-11	$(-4/11w : 1/11w : 2/11w : 1/11w : 1/11w : 1/11w : 1 : 1)$	-32768	-11
P_4	-1	$(1/2w : 1/4w : -1/2w : 0 : 1/4w : -1/4w : -1 : 1)$	1728	-4
P_5	-19	$(0 : -1/19w : 0 : 0 : -1/19w : 0 : 1 : 0)$	-884736	-19

TABLE 6.1. The finitely many quadratic points on $X_0(125)$. See the Introduction for the expression for j_{509}.

$[Q - w_N(Q)] = 0$. Since $X_0(N)$ is not hyperelliptic, it follows that $Q = w_N(Q)$ (as divisors). Hence, Q is a pullback of a point in $X_0^+(N)(\mathbb{Q})$ with respect to the quotient map $X_0(N) \to X_0^+(N)$.

The curve $X_0^+(169)$ is isomorphic to $X_s(13)$, which is known to have 7 rational points by [BDM+19, Theorem 1.1] and the curve $X_0^+(125)$ is known to have 6 rational points [AM, Section 4].

Hence, after computing the pullbacks of the rational points on $X_0^+(N)$, we have all the quadratic points on $X_0(N)$. Using data provided to us by the authors of [CGPS22] and which can be obtained using [CGPS22, Theorem 3.7], we can conclude over which quadratic fields there exist CM points and how many there are. This allows us to conclude that the only non-CM points are the points on $X_0(125)$ defined over $\mathbb{Q}(\sqrt{509})$. Their j-invariants are as given in the Introduction.

Our results are below. We list all the quadratic points, where w denotes $\sqrt{d}$.

6.1. $X_0(125)$. Model for $X_0(125)$:

$$x_1^2 - 10x_2x_3 + 10x_3x_4 - 9x_4^2 - 28x_4x_5 + 70x_4x_6 - 19x_5^2 - 85x_6^2 - x_7^2 - 4x_8^2 = 0,$$
$$x_1x_2 - 5x_2x_3 + 4x_3x_4 - x_4^2 - 14x_4x_5 + 23x_4x_6 - 6x_5x_6 - 18x_6^2 - x_7x_8 - x_8^2 = 0,$$
$$x_1x_3 - 2x_2x_3 - x_3^2 + 2x_3x_4 + 5x_3x_5 - x_4^2 - 7x_4x_5 + 13x_4x_6 - 6x_5x_6 - 8x_6^2 - x_8^2 = 0,$$
$$x_1x_4 - x_2x_3 + 3x_3x_5 - x_4x_5 + 5x_4x_6 - 4x_5x_6 = 0,$$
$$x_1x_5 - x_3x_4 + 2x_3x_5 + x_4x_5 + x_4x_6 - x_5x_6 + x_6^2 = 0,$$
$$x_1x_6 + x_3x_5 - x_4^2 + x_4x_5 + 2x_4x_6 - 2x_5x_6 + 2x_6^2 = 0,$$
$$x_1x_8 - x_2x_7 + x_3x_7 - x_4x_7 + x_4x_8 + x_5x_7 - x_6x_7 + 3x_6x_8 = 0,$$
$$x_2^2 - 2x_2x_3 - x_3^2 + 2x_3x_4 + 2x_3x_5 - x_4^2 - 8x_4x_5 + 14x_4x_6 - x_5^2 - 2x_5x_6 - 14x_6^2 - x_8^2 = 0,$$
$$x_2x_4 - x_3^2 + 3x_4x_5 - 4x_4x_6 + 4x_6^2 = 0,$$
$$x_2x_5 - x_4^2 + 2x_4x_5 + x_4x_6 - x_5^2 - x_5x_6 - x_6^2 = 0,$$
$$x_2x_6 - x_3x_5 + x_4x_5 - x_4x_6 + x_5x_6 = 0,$$
$$x_2x_8 - x_3x_7 + x_4x_7 - x_4x_8 + x_6x_7 = 0,$$
$$x_3x_6 - x_4x_5 + x_4x_6 - 2x_6^2 = 0,$$
$$x_3x_8 - x_4x_7 + x_4x_8 - 2x_6x_8 = 0,$$
$$x_5x_8 - x_6x_7 = 0.$$

Genus of $X_0(125)$: 8.
Genus of $X_0^+(125)$: 2.
Rational cusps: $P_1 := (1 : 0 : 0 : 0 : 0 : 0 : 1 : 0), P_2 := (-1 : 0 : 0 : 0 : 0 : 0 : 1 : 0)$.
Torsion group of $J_0(125)(\mathbb{Q})$: $\mathbb{Z}/25\mathbb{Z} \cdot [P_1 - P_2]$.
Quadratic points (up to conjugation): See Table 6.1.

Primes used in sieve: $3, 7$.

Name	d	Coordinates	j-invariant	CM
P_1	-1	$(w : 0 : 0 : -1/2w : -1/2w : 1 : 1 : 1)$	287496	-16
P_2	-1	$(0 : -1/2w : 0 : 1/4w : 3/4w : 1 : -1 : 1)$	1728	-4
P_3	-3	$(-1/3w : 1/3w : 1/3w : -1/3w : 0 : 1 : 1 : 0)$	54000	-12
P_4	-3	$(-5/18w : 1/6w : 1/6w : 1/2w : 1/9w : 5/2 : 3/2 : 1)$	0	-3
P_5	-3	$(1/3w : 0 : 0 : 0 : -1/3w : 1 : 0 : 1)$	-12288000	-27
P_6	-43	$(2/43w : -1/43w : -2/43w : 2/43w : 2/43w : 0 : 1 : 0)$	-884736000	-43

TABLE 6.2. The finitely many quadratic points on $X_0(169)$.

6.2. $X_0(169)$. Model for $X_0(169)$:

$$x_1^2 - 12x_3^2 - 4x_3x_4 + 12x_3x_5 - 8x_4^2 - 12x_4x_5 - 4x_5^2 - x_6^2 + 4x_6x_8 - 4x_7^2 - 4x_8^2 = 0,$$
$$x_1x_2 - 7x_3^2 - 2x_3x_4 + 8x_3x_5 - 3x_4^2 - 8x_4x_5 + 3x_5^2 - x_6x_7 + 2x_6x_8 - 2x_7^2 - x_8^2 = 0,$$
$$x_1x_3 - 21/8x_3^2 - 9/4x_3x_4 + 13/4x_3x_5 - 25/8x_4^2 - 11/4x_4x_5 - 45/8x_5^2 + 1/2x_6x_8 - 3/2x_7^2 + 1/2x_7x_8 - 19/8x_8^2 = 0,$$
$$x_1x_4 - 15/8x_3^2 + 1/4x_3x_4 + 15/4x_3x_5 - 3/8x_4^2 - 5/4x_4x_5 + 9/8x_5^2 + 1/2x_6x_8 - 1/2x_7^2 - 1/2x_7x_8 - 1/8x_8^2 = 0,$$
$$x_1x_5 - x_3x_4 - x_4^2 + x_4x_5 - 2x_5^2 - x_8^2 = 0,$$
$$x_1x_7 - x_2x_6 + 2x_4x_6 - 4x_4x_7 + x_4x_8 + 2x_5x_6 + 3x_5x_7 - 2x_5x_8 = 0,$$
$$x_1x_8 - x_3x_6 + x_4x_6 - 2x_4x_7 + 3x_5x_6 + 2x_5x_7 - 2x_5x_8 = 0,$$
$$x_2^2 - 3x_3^2 - 2x_3x_4 + 2x_3x_5 - 3x_4^2 - 2x_4x_5 - 3x_5^2 - x_7^2 - x_8^2 = 0,$$
$$x_2x_3 - 19/8x_3^2 + 1/4x_3x_4 + 11/4x_3x_5 + 1/8x_4^2 - 13/4x_4x_5 + 21/8x_5^2 + 1/2x_6x_8 - 1/2x_7^2 - 1/2x_7x_8 + 3/8x_8^2 = 0,$$
$$x_2x_4 - 3/8x_3^2 - 3/4x_3x_4 + 3/4x_3x_5 - 7/8x_4^2 - 1/4x_4x_5 - 27/8x_5^2 + 1/2x_6x_8 - 1/2x_7^2 + 1/2x_7x_8 - 13/8x_8^2 = 0,$$
$$x_2x_5 - 1/2x_3^2 + x_3x_5 + 1/2x_4^2 + 3/2x_5^2 + 1/2x_8^2 = 0,$$
$$x_2x_7 - x_3x_6 - 1/2x_4x_8 + 2x_5x_6 + 1/2x_5x_7 - 2x_5x_8 = 0,$$
$$x_2x_8 - x_4x_6 + x_4x_7 + x_4x_8 - x_5x_7 = 0,$$
$$x_3x_7 - x_4x_6 + 2x_4x_7 - 2x_5x_6 - x_5x_7 + 2x_5x_8 = 0,$$
$$x_3x_8 - x_5x_6 + x_5x_8 = 0.$$

Genus of $X_0(169)$: 8.
Genus of $X_0^+(169)$: 3.
Rational cusps: $P_1 := (1:0:0:0:0:1:0:0), P_2 := (-1:0:0:0:0:1:0:0)$.
Torsion group of $J_0(169)(\mathbb{Q})$: $\mathbb{Z}/7\mathbb{Z} \cdot [P_1 - P_2]$.
Quadratic points (up to conjugation): See Table 6.2.

Primes used in sieve: $3, 5$.

7. Computing isogeny graphs

For a general number field K, step (b) of Mazur's approach is to construct, for the j-invariants of each of the noncuspidal K-rational points on $X_0(N)$ (for $N \in \mathsf{MF}(K)$) found in step (a), the K-rational isogeny graph, and extract any "unrecorded" isogenies; that is, isogenies whose degree is a multiple of N. (We need only consider j-invariants, since whether or not an elliptic curve admits a K-rational N-isogeny depends only on its j-invariant.) As Mazur observed in [Maz78], this is an easy matter to determine (by "pure thought"), and is made even easier thanks to the Sage implementation of isogeny graphs due to David Roe (for elliptic curves over $\mathbb{Q}$) and John Cremona (for elliptic curves over number fields). The code that carries this out may be found in `sage_code/isogeny_graphs.py`. The results have also been verified in the PARI/GP program, via the optimised `ellisomat` implementation based on Billerey's algorithm in [Bil11].

Example 7.1. We continue with the example of Section 5. To summarise the results of that section, we have that, for the Ns in the following list:

$$\mathcal{S}_1 = \{N \leq 10\} \cup \{12, 13, 15, 16, 18, 20, 24, 25, 27, 32, 36\}$$

there are infinitely many elliptic curves over $K = \mathbb{Q}(\sqrt{213})$ supporting a K-rational N-isogeny, and for N in the following list:

$$\mathcal{S}_2 = \{11, 14, 17, 19, 21, 37, 43, 49, 67, 163\}$$

there are only finitely many such elliptic curves; moreover, the j-invariants of these curves are given in Lemma 5.1 and propositions 5.2 and 5.3. For all other integers N, there are no elliptic curves supporting K-rational N-isogenies. Running `unrecorded_isogenies` in `sage_code/isogeny_graphs.py`, we find, just as for Mazur, no "unrecorded" isogenies, and may conclude that Table 1.2 is complete. We note that, by definition of N being minimally finite for K, any proper divisor d of N is such that $X_0(d)$ admits infinitely many K-rational points; this explains the values of N in Table 1.2 for which $\nu = \infty$.

Carrying out this computation for the other 18 values listed in Theorem 1.2, we obtain tables similar to Table 1.2. In the interest of concision we have chosen to present the tables of isogenies in a more condensed format, which may be found in Table 7.1. We only show isogenies (degrees as well as how many up to twist) which are not observed for elliptic curves over $\mathbb{Q}$. For these 19 values, the additional degrees all correspond to values N for which $X_0(N)$ is an elliptic curve of positive rank, and hence admit finitely many isogenies (up to twist). The computation of all necessary isogeny graphs, as well as the entries of Table 7.1, have been automated by the function `quadratic_kenku_solver` in `sage_code/quadratic_kenku_solver.py`, and the 19 values may be verified by the function `very_convenient_vals` in `sage_code/utils.py`.

8. Further work

We remark in closing that, out of the 133 values that were identified to be convenient, we were only able to successfully execute Mazur's strategy on 19 of them. This was due to values of N less than 100 whose $K = \mathbb{Q}(\sqrt{d})$-rational points we were unable to determine. In particular, the value $N = 43$ posed an obstacle for many values of d, particularly when the twisted modular curve $X^d(43)$ was everywhere locally soluble. It is possible that these (and other) values may be treated with an application of the Mordell-Weil sieve, as is done (under additional assumptions which we do not have in our setup) in Section 4.4 of [MJ22].

Finally, in the spirit of Question 1.3, obtaining all finitely many quadratic points on $X_0(163)$ would be of great benefit to obtaining similar determinations over other quadratic fields.

References

[AAB+21] Nikola Adžaga, Vishal Arul, Lea Beneish, Mingjie Chen, Shiva Chidambaram, Timo Keller, and Boya Wen. Quadratic Chabauty for Atkin-Lehner quotients of modular curves of prime level and genus 4, 5, 6. *arXiv preprint arXiv:2105.04811*, 2021.

[AM] Vishal Arul and J. Steffen Müller. Rational points on $X_0^+(125)$. preprint, available at `https://arxiv.org/abs/2205.14744`.

d	$N : \nu_N = \infty$
−6846	15, 27, 32, 36
−2289	15, 21, 24, 36
213	15, 20, 24, 27, 32, 36
834	20, 21, 24, 27
1545	14, 15, 21, 24, 27, 36
1885	14, 15, 20, 21, 24, 32, 36
1923	14, 15, 20, 27
2517	14, 15, 20, 21, 24, 27, 32, 36
2847	14, 15, 21, 32
4569	14, 27, 36
6537	14, 15, 20, 36
7131	14, 20
7302	14, 15, 21, 24, 32
7319	15, 20, 21, 24, 27, 32, 36
7635	14, 15, 20
7890	15, 20, 21, 24, 27, 36
8383	15, 32, 36
9563	21, 24, 27, 36
9903	14, 15, 20, 32

TABLE 7.1. Cyclic isogeny degrees for elliptic curves over $\mathbb{Q}(\sqrt{d})$. Here, for concision, we have only shown the isogenies which are not observed for elliptic curves over $\mathbb{Q}$. All of these values arise from genus 1 modular curves which attain positive rank over $\mathbb{Q}(\sqrt{d})$.

[Ban22] Barinder S. Banwait. Explicit isogenies of prime degree over quadratic fields. *International Mathematics Research Notices*, 2022. to appear, with an appendix by Barinder S. Banwait and Maarten Derickx.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BD22] Barinder S. Banwait and Maarten Derickx. Explicit isogenies of prime degree over number fields. preprint, available at `https://arxiv.org/abs/2203.06009`, 2022.

[BDM+19] Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Annals of mathematics*, 189(3):885–944, 2019.

[BGG21] Josha Box, Stevan Gajović, and Pip Goodman. Cubic and quartic points on modular curves using generalised symmetric Chabauty. *International Mathematics Research Notices*, 2021. To appear, preprint available online at `https://arxiv.org/abs/2102.08236`.

[Bil11] Nicolas Billerey. Critères d'irréductibilité pour les représentations des courbes elliptiques. *International Journal of Number Theory*, 7(04):1001–1032, 2011.

[BN16] Peter Bruin and Filip Najman. A criterion to rule out torsion groups for elliptic curves over number fields. *Research in Number Theory*, 2:13, 2016. Id/No 3.

[Box21] Josha Box. Quadratic points on modular curves with infinite Mordell–Weil group. *Mathematics of Computation*, 90:321–343, 2021.

[CGPS22] Pete L. Clark, Tyler Genao, Paul Pollack, and Frederick Saia. The least degree of a CM point on a modular curve. *Journal of the London Mathematical Socoety*, 105(2):825–883, 2022.

[Cre97] John E. Cremona. *Algorithms for Modular Elliptic Curves*. Cambridge University Press, 1997.

[DEv+21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra & Number Theory*, 15(7):1837–1864, 2021.

[DKSS] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll. Torsion points on elliptic curves over number fields of small degree. Algebra & Number Theory, to appear (https://arxiv.org/abs/1707.00364).

[Kam92] Sheldon Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Inventiones Mathematicae*, 109(2):221–229, 1992.

[Ken79] Monsur A. Kenku. The modular curve $X_0(39)$ and rational isogeny. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 85, pages 21–23. Cambridge University Press, 1979.

[Ken80a] Monsur A. Kenku. The modular curve $X_0(169)$ and rational isogeny. *Journal of the London Mathematical Society*, 2(2):239–244, 1980.

[Ken80b] Monsur A. Kenku. The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 87, pages 15–20. Cambridge University Press, 1980.

[Ken81] Monsur A. Kenku. On the modular curves $X_0(125)$, $X_1(25)$, and $X_1(49)$. *Journal of the London Mathematical Society*, 2(3):415–427, 1981.

[KM88] Monsur A. Kenku and Fumiyuki Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125–149, 1988.

[LL21] Samuel Le Fourn and Pedro Lemos. Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan. *Algebra & Number Theory*, 15(3):747–771, 2021.

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977. With an appendix by Barry Mazur and Michael Rapoport.

[Maz78] Barry Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978. With an appendix by Dorian Goldfeld.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones Mathematicae*, 124(1-3):437–449, 1996.

[MJ22] Philippe Michaud-Jacobs. Fermat's Last Theorem and modular curves over real quadratic fields. *Acta Arithmetica*, 203:319–351, 2022.

[MSD74] Barry Mazur and Peter Swinnerton-Dyer. Arithmetic of Weil curves. *Inventiones mathematicae*, 25(1):1–61, 1974.

[Naj10] Filip Najman. Complete classification of torsion of elliptic curves over quadratic cyclotomic fields. *Journal of Number Theory*, 130(9):1964–1968, 2010.

[Naj18] Filip Najman. Isogenies of non-CM elliptic curves with rational j-invariants over number fields. *Mathematical Proceedings of the Cambridge Philosophical Society*, 164(1):179–184, 2018.

[NT22] Filip Najman and Antonela Trbović. Splitting of primes in number fields generated by points on some modular curves. *Research in Number Theory*, 8(2):18, 2022. Id/No 28.

[NV] Filip Najman and Borna Vukorepa. Quadratic points on bielliptic modular curves. preprint, available at `arXiv:2112.03226`.

[ÖS19] Ekin Özman and Samir Siksek. Quadratic points on modular curves. *Mathematics of Computation*, 88(319):2461–2484, 2019.

[Özm12] Ekin Özman. Points on quadratic twists of $X_0(N)$. *Acta Arithmetica*, 152:323–348, 2012.

[Sik09] Samir Siksek. Chabauty for symmetric powers of curves. 3(2):209–236, 2009.

[The20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020. `https://www.sagemath.org`.

[The21] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.14.0*, 2021. available from `http://pari.math.u-bordeaux.fr/`.

[Trb20] Antonela Trbović. Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d}), 0 < d < 100$. *Acta Arithmetica*, 192(2):141–153, 2020.

[Vuk] Borna Vukorepa. Isogenies over quadratic fields of elliptic curves with rational j-invariant. preprint, available at `arXiv:2203.10672`.

Barinder S. Banwait, Dept. of Mathematics & Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA
Email address: `barinder.s.banwait@gmail.com`
URL: `https://members.vistaserv.net/barinder`

Filip Najman, University of Zagreb, Bijenička Cesta 30, 10000 Zagreb, Croatia
Email address: `fnajman@math.hr`
URL: `http://web.math.pmf.unizg.hr/~fnajman`

Oana Padurariu, Dept. of Mathematics & Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA
Email address: `oana@bu.edu`
URL: `https://sites.google.com/view/oana-padurariu/home`