QUADRATIC ISOGENY PRIMES

BARINDER S. BANWAIT

Abstract. Let K be a quadratic field which is not an imaginary quadratic field of class number one. We describe an algorithm to compute a superset of the **isogeny primes for** K, the primes for which there exists an elliptic curve over K which admits a K-rational isogeny of degree p. This is then used to give the first instances of the determination of isogeny primes for a number field after Mazur's 1978 determination of the isogeny primes for $\mathbb{Q}$. The algorithm is implemented as a software package in Sage and PARI/GP, and has been released under the GPLv3+ license.

This short paper serves as a submission for a Computation presentation at the conference 'Effective Methods in Algebraic Geometry', to be held in Tromsø, Norway, in June 2021. It is based on a recent paper of the author which has been submitted for publication in a mathematics journal.

1. Introduction

A key notion in the study of elliptic curves is that of an **isogeny**, defined as a surjective morphism $\phi : E \to E'$ between elliptic curves which maps the identity element of E to that of E'; or equivalently, precisely those surjective morphisms of curves which induce a group homomorphism between the underlying group of geometric points on E and E'. The **degree of** ϕ is defined as its degree when viewed as a morphism of curves - that is, the degree of the extension of function fields induced by the pullback of ϕ - and ϕ is said to be **separable** if this field extension is separable. If N is the degree of ϕ, one says that ϕ is an N-isogeny. If E and E' are both defined over the same field K, ϕ is said to be **K-rational** if it commutes with the natural Galois action on E and E'. It follows from the basic Galois theory of elliptic function fields that a separable K-rational N-isogeny can be decomposed as a chain of K-rational p-isogenies for p prime, so the isogenies of prime degree carry an elevated significance.

We henceforth take K to be a number field - so in particular all isogenies are separable. It is a corollary of a result of Shafarevich from 1962 [13] that an elliptic curve E/K not admitting any complex multiplication over K admits only finitely many K-rational isogenies of prime degree. In the base case of $K = \mathbb{Q}$, no elliptic curve admits complex multiplication over $\mathbb{Q}$, so every rational elliptic curve admits only finitely many prime degree isogenies.

In a seminal paper involving a delicate analysis of the Néron model of the Eisenstein quotient of the Jacobian of the modular curve $X_0(N)$, Mazur succeeded in 1978 in proving an *explicit uniform version* of the above corollary of Shafarevich for $K = \mathbb{Q}$.

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

Theorem 1.1 (Mazur, Theorem 1 in [9]). *Let $E/\mathbb{Q}$ be an elliptic curve possessing a $\mathbb{Q}$-rational p-isogeny. Then p belongs to the set*

$$\mathsf{IsogPrimeDeg}(\mathbb{Q}) := \{2,3,5,7,11,13,17,19,37,43,67,163\}.$$

It is worth stressing that, prior to this theorem, it was not even known that the set $\mathsf{IsogPrimeDeg}(\mathbb{Q})$ of primes p for which there exists an elliptic curve over $\mathbb{Q}$ possessing a $\mathbb{Q}$-rational p-isogeny was even finite!

Naturally one is motivated to determine the uniform set $\mathsf{IsogPrimeDeg}(K)$ of **isogeny primes for** K for other number fields. In general $\mathsf{IsogPrimeDeg}(K)$ may not be finite due to the possible existence of elliptic curves admitting complex multiplication over K. If such curves exist over K, then necessarily $\mathsf{IsogPrimeDeg}(K)$ is infinite, and it is a theorem of Momose [10, Theorem B] that, for quadratic number fields, this is the only way which $\mathsf{IsogPrimeDeg}(K)$ can be infinite. From the arithmetic theory of elliptic curves possessing complex multiplication, this means that, for K a quadratic number field, finiteness of $\mathsf{IsogPrimeDeg}(K)$ is equivalent to K not being one of the nine imaginary quadratic fields of class number one.

In our recent paper [2] we provide - assuming the Generalised Riemann Hypothesis - the first instances of the determination of $\mathsf{IsogPrimeDeg}(K)$ for $K \neq \mathbb{Q}$ since Mazur's work.

Theorem 1.2 ([2]). *Assuming GRH, we have the following.*

$$\begin{aligned} \mathsf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{7})) &= \mathsf{IsogPrimeDeg}(\mathbb{Q}) \\ \mathsf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-10})) &= \mathsf{IsogPrimeDeg}(\mathbb{Q}) \\ \mathsf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{-5})) &= \mathsf{IsogPrimeDeg}(\mathbb{Q}) \cup \{23\} \\ \mathsf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{5})) &= \mathsf{IsogPrimeDeg}(\mathbb{Q}) \cup \{23, 47\}. \end{aligned}$$

This is actually obtained as a corollary of the following more general algorithmic result.

Algorithm 1.3. *Let K be a quadratic field which is not imaginary quadratic of class number 1. Then there is an algorithm which computes a superset of $\mathsf{IsogPrimeDeg}(K)$ as the union of three sets:*

$$\begin{aligned} \mathsf{IsogPrimeDeg}(K) \subseteq \mathsf{PreTypeOneTwoPrimes}(K) &\cup \mathsf{TypeOnePrimes}(K) \\ &\cup \mathsf{TypeTwoPrimes}(K). \end{aligned}$$

The termination of the algorithm relies on the Generalised Riemann Hypothesis.

It is the Sage [15] and PARI/GP [14] implementation of this algorithm that constitutes the software package *Quadratic Isogeny Primes* which is the subject of this submission for a Computation presentation at the conference 'Effective Methods in Algebraic Geometry', to be held in Tromsø, Norway, in June 2021. The package, complete with a command line interface, is available on GitHub [3], and has been released under the GPLv3+ license. If accepted for presentation, our intention will be to explain the ideas of the algorithm as well as to give a live demonstration of how it may be used to obtain results as in Theorem 1.2.

This short paper is organised as follows. In Section 2 we give an overview of the algorithm, which is based on studying the *isogeny types.* The cases of isogenies of **Type 1** and **Type 2** require separate handling; these constitute Section 3 and

Section 4 respectively. Finally in Section 5 we illustrate the use of the package to determine $\mathsf{IsogPrimeDeg}(K)$ in the specific case of $K = \mathbb{Q}(\sqrt{5})$.

2. Overview of the algorithm

This section gives an overview of *Quadratic Isogeny Primes*. More details may be found in [2]. Since the phrase 'quadratic field which is not imaginary quadratic of class number one' arises frequently, we give these objects the name of **isogeny-finite quadratic fields**, in light of Momose's theorem on the finiteness of $\mathsf{IsogPrimeDeg}(K)$ mentioned in the Introduction.

Let E/K be an elliptic curve over a number field possessing a K-rational p-isogeny for some prime $p \geq 5$; write V for the kernel of the isogeny, a one-dimensional G_K-stable module, where $G_K := \mathrm{Gal}(\overline{K}/K)$ denotes the absolute Galois group of K, and denote by λ the *isogeny character*:

$$\lambda : G_K \longrightarrow \mathrm{Aut}\, V(\overline{K}) \cong \mathbb{F}_p^\times.$$

The study of the isogeny character was initiated by Mazur [9, Section 5], and developed by Momose, who provided the following classification, in which θ_p denotes the mod-p cyclotomic character of G_K.

Theorem 2.1 (Momose, Theorem 1 in [10]). *Let K be a number field. Then there exists an effective constant $C_0 = C_0(K)$ such that for any prime $p > C_0$, and for any elliptic curve admitting a K-rational p-isogeny, the isogeny character λ falls into one of the following three types:*

Type 1. λ^{12} *or* $(\lambda\theta_p^{-1})^{12}$ *is unramified.*

Type 2. $\lambda^{12} = \theta_p^6$ *and* $p \equiv 3 \pmod 4$.

Type 3. K contains the Hilbert class field H_L of an imaginary quadratic field L. The rational prime p splits in L:

$$p\mathcal{O}_L = \mathfrak{p}\bar{\mathfrak{p}}.$$

For any prime $\mathfrak{q}$ of K prime to $\mathfrak{p}$, with Frobenius automorphism $\sigma_\mathfrak{q}$,

$$\lambda^{12}(\sigma_\mathfrak{q}) = \alpha^{12} \pmod{\mathfrak{p}}$$

for any $\alpha \in K^\times$ with $\alpha\mathcal{O}_L = \mathrm{Nm}_{K/L}(\mathfrak{q})$.

Therefore, for K an isogeny-finite quadratic field, Type 3 does not arise, so Momose's theorem may be reinterpreted in this case as saying that, outside of a finite set $\mathsf{PreTypeOneTwoPrimes}(K)$, the isogeny character must be of Type 1 or Type 2. While Momose did not make his constant C_0 effective, our algorithm constructs a tight superset of $\mathsf{PreTypeOneTwoPrimes}(K)$, which the rest of this section illustrates.

The first step towards the proof of Momose's theorem is a description of how λ^{12} acts on ideals of K coprime to p (identifying λ with a character of the ideal group $I_K(p)$).

Lemma 2.2 (Momose, Lemma 1 of *loc. cit.*). *Assume that K is Galois over $\mathbb{Q}$, and that p is unramified in K. Then for a fixed prime $\mathfrak{p}$ of K lying over p, there exist integers a_σ satisfying $0 \leq a_\sigma \leq 12$, for $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that*

$$\lambda^{12}((\alpha)) \equiv \alpha^\epsilon \pmod{\mathfrak{p}}$$

for $\epsilon = \sum_\sigma a_\sigma \sigma$ and $\alpha \in K^\times$ prime to p.

Thus, λ^{12} acts (modulo $\mathfrak{p}$) via an element ϵ of the group ring $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$, for which there are only finitely many possibilities. In our case of quadratic K, we may denote ϵ as a pair (a, b) of integers, referring to $a \cdot \mathrm{id} + b \cdot \sigma$, with σ being the non-trivial Galois automorphism.

Lemma 2.3. *The possible values of the group ring character ϵ for a quadratic field K are as follows:*

(1) **Quadratic** *ϵ: the 4 pairs $(12a, 12b)$ for $a, b \in \{0, 1\}$;*
(2) **Quartic** *ϵ: the 12 pairs $(4a, 4b)$ for $a, b \in \{0, 1, 2, 3\}$, excluding the 4 quadratic pairs.*
(3) **Sextic** *ϵ: the 5 pairs $(6a, 6b)$ for $a, b \in \{0, 1, 2\}$, excluding the 4 quadratic pairs;*

Proof. This follows from Remark 1 of *loc. cit.*, where the possible values for the unordered set $\{a, b\}$ are given as

- $\{0, 12\}$;
- $\{0, 4, 8, 12\}$ (possible only if $j(E) \equiv 0 \pmod{\mathfrak{p}}$ and $p \equiv 2 \pmod 3$);
- $\{0, 6, 12\}$ (possible only if $j(E) \equiv 1728 \pmod{\mathfrak{p}}$ and $p \equiv 3 \pmod 4$).

□

It follows from Lemma 2.2 that, if $\epsilon = (0, 0)$ or $(12, 12)$, then λ is of Type 1. Furthermore, Momose shows (Lemma 2 of *loc. cit.*) that, if $\epsilon = (6, 6)$, then λ is of Type 2. These two types will be dealt with separately in the subsequent two sections of this paper, so for the rest of this section we exclude them from consideration.

The 18 remaining possiblities for ϵs are implemented in a global Python dictionary, with keys corresponding to the ϵs, and values giving the type. Here is a snapshot:

```
EPSILONS_PRE_TYPE_1_2 = {

    (0,12): 'quadratic',
    (12,0): 'quadratic',

    (0,4): 'quartic',
    (0,8): 'quartic',
```

Keeping track of the type of ϵ allows us to impose further conditions on any possible isogeny primes that arise from the algorithm, due to the extra restrictions in the quartic and sextic types shown in the proof of Lemma 2.3.

The main idea for computing a tight superset of $\mathsf{PreTypeOneTwoPrimes}(K)$ is that of **auxiliary primes**; these are prime ideals $\mathfrak{q}$ of K of residue degree 1 lying over a rational prime q different to p, the assumed isogeny degree. In short, each auxiliary prime gives rise to a non-zero integer which p must divide; and by taking several auxiliary primes and taking the greatest common divisor of the resulting integers, one can significantly reduce the size of $\mathsf{PreTypeOneTwoPrimes}(K)$.

More precisely, we argue as follows. Let E/K be an elliptic curve over an isogeny-finite quadratic field K admitting a K-rational p-isogeny, where the isogeny character acts via the group ring character ϵ not of Type 1 or 2; and let $\mathfrak{q}$ be an auxiliary prime as above. Considering the reduction type of E at $\mathfrak{q}$, we know that either E has potentially multiplicative reduction at $\mathfrak{q}$, or it has potentially good reduction at $\mathfrak{q}$.

In the potentially multiplicative reduction case, it follows - essentially from Tate's algorithm - that p must divide one of the following two non-zero integers (non-zero because ϵ is not of Type 1):

$$A(\epsilon, \mathfrak{q}) := \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^\epsilon - 1) \quad \text{or} \quad B(\epsilon, \mathfrak{q}) := \mathrm{Nm}_{K/\mathbb{Q}}(\alpha^\epsilon - q^{12h_K}),$$

where h_K denotes the class number of K, and α is a generator of the ideal $\mathfrak{q}^{h_K}$. We refer to primes in the support of these two integers as **Type A** and **Type B** primes, respectively. Observe that each of these integers depends only on ϵ and $\mathfrak{q}$.

In the potentially good reduction case, Momose shows (Lemma 2 of *loc. cit.*) that $\alpha^\epsilon \neq \beta^{12h_K}$ for any root β of the characteristic polynomial of Frobenius of any elliptic curve over $\mathbb{F}_q$; consequently p must divide the following non-zero integer depending only on ϵ and $\mathfrak{q}$:

$$C(\epsilon, \mathfrak{q}) := \mathrm{lcm}(\{\mathrm{Nm}_{K(\beta)/\mathbb{Q}}(\alpha^\epsilon - \beta^{12h_K}) \mid \beta \text{ is a Frobenius root over } \mathbb{F}_q\}).$$

We refer to primes dividing this integer as **Type C** primes. Note that this LCM is being taken over all characteristic polynomials of Frobenius for elliptic curves over $\mathbb{F}_q$.

We write $ABC(\epsilon, \mathfrak{q})$ for the union of the Type A, B, and C primes arising as above, together with the rational prime q lying under $\mathfrak{q}$; we append this single rational prime since the possible isogeny primes of type A, B or C were deemed to be distinct from q. For Aux a finite set of auxiliary primes, we may thus define the set of **pre-Type 1 or 2** primes for K as

$$\mathsf{PreTypeOneTwoPrimes}(K) := \bigcup_{\epsilon} \bigcap_{\mathfrak{q} \in \mathsf{Aux}} ABC(\epsilon, \mathfrak{q}),$$

where the union is taken over the 18 pairs in Lemma 2.3 excluding $(0, 12)$, $(12, 0)$, and $(6, 6)$.

The remainder of this section makes some remarks on the Sage implementation of $\mathsf{PreTypeOneTwoPrimes}(K)$, whose main part is the following block, which computes, for each auxiliary prime $\mathfrak{q}$, a dictionary, whose keys are the 18 ϵs, and the value for each ϵ is the set of primes dividing $ABC(\epsilon, \mathfrak{q})$.

```
for q in aux_primes:
    # these will be dicts with keys the epsilons, values sets of primes
    AB_primes_dict = get_AB_primes(K,q,epsilons, h_K)
    C_primes_dict = get_C_primes(K, q, epsilons, h_K, loop_curves)
    unified_dict = {}
    q_rat = Integer(q.norm())
    assert q_rat.is_prime()
    for eps in epsilons:
        unified_dict[eps] = AB_primes_dict[eps].union(C_primes_dict[eps],
                                                      {q_rat})
    tracking_dict[q] = unified_dict
```

The inner methods `get_AB_primes` and `get_C_primes` then compute the support of the integers $A(\epsilon, \mathfrak{q})$, $B(\epsilon, \mathfrak{q})$, and $C(\epsilon, \mathfrak{q})$. Recall that the computation of $C(\epsilon, \mathfrak{q})$ required one to compute the roots of all characteristic polynomials of Frobenius for all elliptic curves over $\mathbb{F}_q$. This is a potential bottleneck in the runtime, and having to do this for each of the 18 ϵs would significantly reduce the efficiency of the algorithm. To avoid this, while looping through all Weil polynomials over $\mathbb{F}_q$, the possible roots β are extracted, and for each β and ϵ, the quantity $\mathrm{Nm}_{K(\beta)/\mathbb{Q}}(\alpha^{\epsilon} - \beta^{12h_K})$ is computed, and its prime factors stored in a dictionary with key ϵ. The following code snapshot illustrates how this is implemented.

```
for beta in betas:
    if beta in K:
        for eps, eps_type in epsilons.items():
            N = (group_ring_exp(alpha, eps) - beta ** (12*h_K)).absolute_norm()
            N = ZZ(N)
            if N != 0:
                possible_C_primes = N.prime_divisors()
                C_primes_filt = filter_ABC_primes(K, possible_C_primes,
                                                  eps_type)
            else:
                # means no elliptic curve with this Weil poly
                C_primes_filt = []
            output_dict_C[eps] = output_dict_C[eps].union(set(C_primes_filt))
    else:
```

This allows one to only compute factorisations of Weil polynomials of all elliptic curves over $\mathbb{F}_q$ once for each $\mathfrak{q}$, rather than every time for each ϵ.

The function concludes by taking the intersection over all auxiliary primes, followed by the union over all ϵs, completing the determination of PreTypeOneTwoPrimes:

```
    tracking_dict_inv_collapsed = {}
    for eps in epsilons:
        q_dict = {}
        for q in aux_primes:
            q_dict[q] = tracking_dict[q][eps]
        q_dict_collapsed = set.intersection(*(val for val in q_dict.values()))
        tracking_dict_inv_collapsed[eps] = q_dict_collapsed
    output = set.union(*(val for val in tracking_dict_inv_collapsed.values()))
    output = list(output)
    output.sort()
    return output
```

3. TypeOnePrimes(K)

The determination of TypeOnePrimes is very similar to PreTypeOneTwoPrimes: one uses auxiliary primes $\mathfrak{q}$ to compute non-zero integers which an isogeny prime must divide, and one takes the GCD of the resulting integers. More precisely, for an elliptic curve E/K over an isogeny-finite quadratic field admitting a K-rational p-isogeny of Type 1, as before one considers the two types of potential reduction E may have at $\mathfrak{q}$.

If E has potentially multiplicative reduction at $\mathfrak{q}$, then Momose shows that $p-1$ divides $12h_K$.

If E has potentially good reduction at $\mathfrak{q}$, then Momose shows that p must divide the non-zero integer:

$$D(\mathfrak{q}) := \mathrm{lcm}(\{1 + N(\mathfrak{q})^{12h_K} - \beta^{12h_K} - \bar{\beta}^{12h_K} \mid \beta \text{ is a Frobenius root over } \kappa(\mathfrak{q})\}). \tag{3.1}$$

This however makes two assumptions

(1) The possible isogeny prime p is unramified in K.

(2) A certain morphism

$$f : X^{(2)}_{/S} \to \tilde{J}_{/S}$$

from the symmetric square of the modular curve $X_0(p)$ to the Eisenstein quotient of $J_0(p)$ with base $S = \operatorname{Spec}\mathbb{Z}[1/p]$ is a *formal immersion along* (∞, ∞) away from characteristics 2, 3, and 5.

We do not discuss the notion of formal immersion here; it suffices to say that Kamienny proved [7, Proposition 3.2] that the second assumption above is satisfied whenever $p \geq 73$. The first assumption gives the restriction that the possible isogeny primes are deemed not to divide the discriminant Δ_K of K. One therefore has the following superset for the Type 1 primes (again, for Aux a finite set of auxiliary primes):

$$\begin{aligned}\mathsf{TypeOnePrimes}(K) = \mathsf{PrimesUpTo}(71) \cup \{p : p \mid \Delta_K\} \\ \cup \{p : (p-1) \mid 12h_K\} \cup \left(\bigcap_{\mathfrak{q} \in \mathsf{Aux}} \{p : p \mid qD(\mathfrak{q})\}\right).\end{aligned}$$

4. $\mathsf{TypeTwoPrimes}(K)$

Momose gives a necessary condition that an isogeny prime of Type 2 must satisfy, which in [2] is expressed as follows.

Condition CC. Let K be an isogeny-finite quadratic field, and E/K an elliptic curve admitting a K-rational p-isogeny, with p of Type 2. Let q be a rational prime $< p/4$ such that $q^2 + q + 1 \not\equiv 0 \pmod{p}$. Then the following implication holds:

if q splits or ramifies in K, then q does not split in $\mathbb{Q}(\sqrt{-p})$.

This condition may be expressed concretely via the legendre symbols $\left(\frac{D}{q}\right)$ and $\left(\frac{q}{p}\right)$, so may be checked for any prime p as follows:

```
def satisfies_condition_CC(K,p):
    for q in prime_range(p/4):
        if (q**2 + q + 1) % p != 0:
            if not K.ideal(q).is_prime():
                if legendre_symbol(q,p) == 1:  # i.e. not inert
                    return False
    return True
```

The question is then of how far we need to check: can we find an upper bound on Type 2 primes?

It was Larson and Vaintrob who found an effective bound on Type 2 primes assuming GRH, and modulo the determination of an effectively computable absolute constant c_7 (which alas is not effectively computed!), which appears in [8, Corollary 6.3]. Tracing through their proof, and combining it with the best possible bounds in the Effective Chebotarev Density Theorem due to Bach and Sorenson [1, Theorem 5.1], we are able to offer a modest improvement on their bound which removes the dependence on c_7 in our case.

Proposition 4.1. *Assume GRH. Let K be an isogeny-finite quadratic field, and E/K an elliptic curve possessing a K-rational p-isogeny, for p a Type 2 prime.*

Then p satisfies

$$p \leq (16 \log p + 16 \log(12\Delta_K) + 26)^4.$$

In particular, there are only finitely many primes p as above.

See [2, Proposition 4.4] for the proof. For $K = \mathbb{Q}(\sqrt{5})$, this bound on Type 2 primes is approximately 5.65×10^{10}. The algorithm therefore needs to check all primes up to this large bound.

The Sage script has implemented this check; but we found that Sage quickly ran into memory overflow errors when attempting this check up to the bound given by the above proposition. We therefore limited the Sage script to only check Type 2 primes up to 1000, and instead developed an optimised PARI/GP script with parallel threading to carry out the check up to the Type 2 bound. The search range is broken into blocks of size 100,000; the primes in these blocks are then checked to satisfy condition CC via a *parallel for loop*:

```
blockSize=100000;
export(blockSize)

checktypetwo(pBeg) =
{
    my(p,cond);
    forprime(p = pBeg*blockSize, (pBeg+1)*blockSize-1,
             cond=custom_congruence_condition(p,D);
             if(cond,print_satisfiesCC(p)));
}
export(checktypetwo)

howMany=floor(typetwobound/blockSize);

parapply(checktypetwo,[0..howMany]);
```

Remark 4.2. The largest Type 2 prime we have encountered for any isogeny-finite quadratic field is 163. There is a connection between Type 2 primes and an anaglogue of the class number one problem, as discussed in Goldfeld's Appendix to Mazur's paper [9].

5. An example: $\mathsf{IsogPrimeDeg}(\mathbb{Q}(\sqrt{5}))$

We illustrate how the *Quadratic Isogeny Primes* package may be used to exactly determine the set of isogeny primes $\mathsf{IsogPrimeDeg}(K)$ for a given isogeny-finite quadratic field. In this final section we show this for $K = \mathbb{Q}(\sqrt{5})$.

Having cloned the Git repository, the main file in the package is `quadratic_isogeny_primes.py`, which takes one required argument - the integer D for which $K = \mathbb{Q}(\sqrt{D})$ - and several optional arguments, including `--aux_prime_count`, which determines the number of auxiliary primes to take. Increasing this number will reduce the size of the final superset, but will take longer to run. In this example we take 6 auxiliary primes:

```
sage quadratic_isogeny_primes.py 5 --aux_prime_count 6
```

Running this on an old laptop takes about 20 seconds, and shows that the superset for $\mathsf{IsogPrimeDeg}(K)$ is the following:

```
superset = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 163]
```

Note that we are also warned about the following:

```
WARNING: Only checking Type 2 primes up to 1000.
```

As explained in Section 4, Sage encounters a memory error when attempting to check all primes up to the bound on Type 2 primes, which may be attempted by running the script with the option `--rigorous`; this results in the following (truncated) error:

```
type_2_bound = 56546719183
Traceback (most recent call last):
...
cypari2.handle_error.PariError: the PARI stack overflows (current size: 1000000;
 maximum size: 2596085760)
```

To check all primes up to this bound of 56546719183, we navigate to the `gp_scripts` folder, and edit the file `partype2primes.gp` for our desired D and the Type 2 bound:

```
D=5;  \\ change this to desired value
typetwobound=56546719183;
export(D)
```

We initialise PARI/GP with the requisite number of precomputed primes:

```
gp --primelimit 56546719183
```

The user may wish to confirm that their version of PARI/GP has been configured for parallel computing; if so, the number of available threads is declared upon starting the PARI/GP calculator:

```
parisize = 400003072, primelimit = 56546719183, nbthreads = 8
```

One then loads the script `partype2primes.gp` and executes the main 'parallel for loop', which checks all primes up to 56546719183 for whether they are indeed of Type 2; if so, they are printed on screen. Doing this for `D = 5` took just under 70 minutes on an old laptop:

```
? read("partype2primes.gp");
? parapply(checktypetwo,[0..howMany]);
3 is a type 2 prime
7 is a type 2 prime
23 is a type 2 prime
43 is a type 2 prime
47 is a type 2 prime
67 is a type 2 prime
163 is a type 2 prime
cpu time = 9h, 18min, 26,461 ms, real time = 1h, 9min, 55,918 ms.
?
```

Therefore, conditional upon the Generalised Riemann Hypothesis, the superset found by `quadratic_isogeny_primes.py` is indeed a superset, and no Type 2 primes larger than 1000 need to be considered. Since an elliptic curve over $\mathbb{Q}$ may be considered as an elliptic curve over any number field K, we have $\mathsf{IsogPrimeDeg}(\mathbb{Q}) \subseteq \mathsf{IsogPrimeDeg}(K)$, so we need to decide whether or not the following are isogeny primes for $\mathbb{Q}(\sqrt{5})$:

$$\{23, 29, 31, 41, 47, 53, 59, 61, 71, 73, 79\}.$$

This is equivalent to asking, for each p in this list, whether or not the modular curve $X_0(p)$ admits a non-cuspidal $\mathbb{Q}(\sqrt{5})$-rational point.

Such questions are notoriously difficult; but fortunately, many of these ps we need to consider are such that the genus of $X_0(p)$ is fairly small; and most importantly, there has been in recent years much progress in the study of *quadratic points on low-genus modular curves*. Of particular significance are the works of Bruin and Najman [6], Özman and Siksek [12], and most recently Box [5]; taken together, these three works give a complete determination of the quadratic points on $X_0(N)$ when it has genus 2, 3, 4 or 5. In essence, for each such N, there are only finitely many quadratic points which do not correspond to elliptic $\mathbb{Q}$-curves; and these finitely many points are determined explicitly. All of these works utilise Magma [4] in a significant way.

By combining these results with earlier work of Özman in determining local solubility of quadratic twists of $X_0(N)$ [11], together with a fair amount of Sage and Magma computation - notably the Chabauty package - one is able to decide that, out of the primes in the above set, only the primes 23 and 47 are isogeny primes for $\mathbb{Q}(\sqrt{5})$, thereby proving the final assertion of Theorem 1.2. For full details of this, the reader is referred to the final section - *Weeding out the Pretenders* - of [2].

References

1. Eric Bach and Jonathan Sorenson, *Explicit bounds for primes in residue classes*, Mathematics of Computation **65** (1996), no. 216, 1717–1735.
2. Barinder S. Banwait, *Explicit isogenies of prime degree over quadratic fields*, submitted. Preprint available online at `https://arxiv.org/abs/2101.02673`, 2021.
3. ———, *Quadratic Isogeny Primes*, `https://github.com/barinderbanwait/quadratic_isogeny_primes`, 2021, Distributed under the GPL v3+ license.
4. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478
5. Josha Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Mathematics of Computation **90** (2021), 321–343.
6. Peter Bruin and Filip Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS Journal of Computation and Mathematics **18** (2015), no. 1, 578–602.
7. Sheldon Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Inventiones mathematicae **109** (1992), no. 1, 221–229.
8. Eric Larson and Dmitry Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties*, Journal of the Institute of Mathematics of Jussieu **13** (2014), no. 3, 517559.
9. Barry Mazur, *Rational isogenies of prime degree*, Inventiones mathematicae **44** (1978), no. 2, 129–162, With an appendix by Dorian Goldfeld.
10. Fumiyuki Momose, *Isogenies of prime degree over number fields*, Compositio Mathematica **97** (1995), no. 3, 329–348.

11. Ekin Özman, *Points on quadratic twists of* $X_0(N)$, Acta Arithmetica **152** (2012), 323–348.
12. Ekin Özman and Samir Siksek, *Quadratic points on modular curves*, Mathematics of Computation **88** (2019), no. 319, 2461–2484.
13. Igor R. Shafarevich, *Algebraic number fields*, AMS Translations **31** (1962), 25–39, first appeared in Proceedings of the International Congress of Mathematicians, Stockholm.
14. The PARI Group, Univ. Bordeaux, *PARI/GP version 2.14.0*, 2021, available from `http://pari.math.u-bordeaux.fr/`.
15. The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 9.2)*, 2020, `https://www.sagemath.org`.

Barinder S. Banwait, Harish-Chandra Research Institute, Prayagraj, India
Email address: `barinder.s.banwait@gmail.com`