Fermat's Last Theorem and Modular Curves over Real Quadratic Fields

Philippe Michaud-Jacobs

Abstract

In this paper we study the Fermat equation $x^n + y^n = z^n$ over quadratic fields $\mathbb{Q}(\sqrt{d})$ for squarefree d with $26 \leq d \leq 97$. By studying quadratic points on the modular curves $X_0(N)$, d-regular primes, and working with Hecke operators on spaces of Hilbert newforms, we extend work of Freitas and Siksek to show that for most squarefree d in this range there are no non-trivial solutions to this equation for $n \geq 4$.

Contents

1 Introduction

There has been much recent interest in the study of the Fermat equation

$$x^n + y^n = z^n$$

over number fields. Following in the footsteps of Wiles [41], we would ideally like to show that this equation has no non-trivial solutions for $n \geq 4$ and $x, y, z \in K$, a number field. By a *non-trivial* solution, we mean $xyz \neq 0$. The study of the Fermat equation over number fields dates back to the work of Maillet in the late 19th century [13, p. 578].

Asymptotic versions of Fermat's Last Theorem over number fields (proving there are no non-trivial solutions if all the prime factors of n are greater than some bound dependent on K) have been proven over various number fields (see [16, 14] for example). In this paper, we are concerned with trying to prove the non-existence of non-trivial solutions for *all* $n \geq 4$ over a real quadratic field K. Jarvis and Meekin proved this statement over the field $\mathbb{Q}(\sqrt{2})$ in [22]. This work was then extended by Freitas and Siksek [18] to the quadratic fields $\mathbb{Q}(\sqrt{d})$, with d squarefree, $d \neq 5, 17$ in the range $3 \leq d \leq 23$, where it was shown that there are no non-trivial solutions for $n \geq 4$. Kraus, in [29], proved that for K a cubic field of discriminant $148, 404$, or 564 there are no non-trivial solutions for $n \geq 4$. The aim of this paper is to extend the result of Freitas and Siksek to squarefree d in the range $26 \leq d \leq 97$, as well as introduce techniques that can be used to study other Diophantine equations, both over the rationals and number fields of low degree. For most values of d in this range, issues arise surrounding irreducibility of Galois representations and the computation of Hilbert newforms. In most cases, we overcome these issues to obtain the following result.

Theorem 1. *The equation*

$$x^n + y^n = z^n, \quad x, y, z \in K,$$

has no non-trivial solutions for $n \geq 4$ *and* $K = \mathbb{Q}(\sqrt{d})$*, when* $d \in \mathcal{D}$*, where* $\mathcal{D} = \{26, 29, 30, 31, 35, 37, 38, 42, 43, 46, 47, 51, 53, 58, 59, 61, 62, 65, 66, 67, 69, 71, 73, 74, 77, 79, 82, 83, 85, 86, 87, 91, 93, 94, 97\}$.

We note that the case $d = 79$ is proven in the paper of Freitas and Siksek [18, p. 14]. We also obtain the following partial results.

Theorem 2. *The equation*

$$x^p + y^p = z^p, \quad x, y, z \in K,$$

has no non-trivial solutions for $p \geq 5, p \neq 23$ *prime, and* $K = \mathbb{Q}(\sqrt{d})$*, when* $d = 34$ *or* 55.

Date: April 2, 2022.

Keywords: Fermat's Last Theorem, Fermat equation, Frey curve, Galois representations, quadratic points, modular curves, irreducibility, Hilbert modular forms.

MSC2010: 11D41, 11F80, 11G18, 11G05, 14G05.

The author is supported by an EPSRC studentship and has previously used the name Philippe Michaud-Rodgers.

In this result, the prime 23 appears as an exception as we are unable to discard certain Hilbert newforms (see Section 5.4). Furthermore, 23 is both 34-irregular and 55-irregular (see Section 6).

In some cases, extending the work of Kraus [28], we can obtain a lower bound on the size p.

Theorem 3. *The equation*

$$x^p + y^p = z^p, \quad x, y, z \in K,$$

has no non-trivial solutions for $5 \leq p \leq 10^7$*, prime, and* $K = \mathbb{Q}(\sqrt{d})$*, when* $d = 17, 33, 41, 57, 89$*. Moreover, if* $d = 89$*, then we also have no non-trivial solutions when* $p \geq 5$ *and* $p \equiv \pm 2 \pmod 5$*.*

Four values of d, with d squarefree and $26 \leq d \leq 97$, do not appear in the above theorems; namely $d = 39, 70, 78$, and 95. This is because the spaces of Hilbert newforms we considered for these values were too large to work with computationally (see Section 5.3).

In order to prove Theorems 1, 2, and 3, one of the key results we use is Theorem 4 below, which extends work of Najman and Turcas [35, p. 2]. For squarefree integers N and d', with $N > 0$, we denote by $X_0^{d'}(N)$ the twist of the modular curve $X_0(N)$ over $\mathbb{Q}(\sqrt{d'})$ by the Atkin-Lehner involution w_N. A rational point on $X_0^{d'}(N)$ can be identified with a pair of Galois conjugate quadratic points on $X_0(N)(\mathbb{Q}(\sqrt{d'}))$ that are interchanged by w_N.

Theorem 4. *Let* $p > 19$*,* $p \neq 37$ *be a prime. Let* E' *be an elliptic curve defined over any quadratic field* $K' = \mathbb{Q}(\sqrt{d'})$*. Let* $q > 5$*,* $q \neq p$ *be a rational prime such that each prime of* K' *above* q *is of multiplicative reduction for* E'*. Then* $\overline{\rho}_{E',p}$ *is irreducible if one of the following two conditions holds:*

(i) the prime q *does not split in* K'*;*

(ii) the prime q *splits in* K' *and* $X_0^{d'}(p)(\mathbb{Q}) = \emptyset$*.*

We note that K' may be an imaginary quadratic field in the statement of this theorem. Using the work of Ozman [37], we can often show that $X_0^{d'}(p)(\mathbb{Q}) = \emptyset$ for given p and d' (see Theorem 4.3 of this paper).

We now outline the rest of the paper. In Section 2 we overview the general proof strategy and state the key properties of the Frey elliptic curve, mainly following [18]. In Sections 3 and 4 we study the question of irreducibility. In Section 3 we use techniques from class field theory and various irreducibility criteria to do this, and in Section 4 we deal with the remaining cases by studying quadratic points on the modular curves $X_0(N)$, using local obstructions, formal immersions, relative symmetric Chabauty, modular parametrisations, and sieving techniques. In Section 5 we work with Hecke operators to partially reconstruct and subsequently eliminate Hilbert newforms. Finally, in Section 6 we consider d-regular primes.

The `Magma` [4] and `Sage` [39] code used to support the computations in this paper can be found at:

`https://warwick.ac.uk/fac/sci/maths/people/staff/michaud/c/`

I would like to express my sincere gratitude to my supervisors Samir Siksek and Damiano Testa for many useful discussions and their support in writing this paper. I would also like to thank Filip Najman for some helpful comments. Finally, I would like to thank the anonymous referee for a careful reading of the paper.

2 The Frey Curve

In this section we provide a brief overview of how one associates an elliptic curve to a putative solution of the Fermat equation, and we state some properties of this curve. We then state the level-lowering theorem used to (hopefully) obtain a contradiction, proving the non-existence of non-trivial solutions. In this section, we mainly follow [18, pp. 4-8].

We start by fixing some notation. Let K be a real quadratic field $\mathbb{Q}(\sqrt{d})$ for some squarefree d with $26 \leq d \leq 97$. We will also use the notation $K' = \mathbb{Q}(\sqrt{d'})$ to denote a general (possibly imaginary) quadratic field. Let ϵ be a fundamental unit for K. Write $\mathrm{Cl}(K)$ for the class group of K. We denote a prime of K by $\mathfrak{q}$. Write $S = \{\mathfrak{q} : \mathfrak{q} \mid 2\}$, which consists of a single prime if 2 is inert or ramifies in K, and two primes if 2 splits in K.

In all cases we consider, $\mathrm{Cl}(K)$ has order 1, 2, or 3. It follows that the quotient group $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$ has size $r = 1$ or 2. If $r = 2$ then choose $\mathfrak{m}$ an odd prime ideal such that $[\mathfrak{m}]$ represents the non-trivial element of $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$. The table in the appendix displays our choice for the ideal $\mathfrak{m}$ in each case.

Although Theorem 1 is stated for any $n \geq 4$ and for $x, y, z \in K$, we can reduce (as in the case of Fermat's Last Theorem over $\mathbb{Q}$) to the case of $n = p$, prime, and $x, y, z \in \mathcal{O}_K$. We therefore study the equation, which we refer to as the *Fermat equation with exponent* p,

$$a^p + b^p + c^p = 0, \qquad a, b, c \in \mathcal{O}_K,\ p \geq 5.$$

As discussed in [18, p. 2], it has been shown that this equation has no non-trivial solutions for primes $5 \leq p \leq 13$ (as well as for the same equation with exponents $n = 4, 6$, and 9) over real quadratic fields, and so we will assume that we have a non-trivial solution (a, b, c) with $p \geq 17$. To this solution we associate the Frey elliptic curve

$$E_{a,b,c,p} : Y^2 = X(X - a^p)(X + b^p),$$

and write $E = E_{a,b,c,p}$. We write $\mathcal{N}$ for the conductor of E which is an ideal in $\mathcal{O}_K$.

Lemma 2.1 (Frey curve invariants, [18, p. 5]). *The curve E has the following invariants*

$$c_4 = 16(a^{2p} - b^p c^p), \qquad c_6 = -32(a^p - b^p)(a^p - c^p)(b^p - c^p),$$
$$\Delta = 16a^{2p}b^{2p}c^{2p}, \qquad j = c_4^3/\Delta.$$

Lemma 2.2 (Reduction of the Frey curve, [18, pp. 5-7]). *The curve E has additive reduction at the primes in S and also at $\mathfrak{m}$ when $r = 2$. If 2 splits or ramifies in K, then E has potentially multiplicative reduction at the primes above 2. If $\mathfrak{q} \notin S$, and $\mathfrak{q} \neq \mathfrak{m}$ (when $r = 2$), then E is semistable at $\mathfrak{q}$ and $p \mid v_\mathfrak{q}(\Delta_\mathfrak{q})$, where $\Delta_\mathfrak{q}$ is the minimal discriminant at $\mathfrak{q}$.*

Even if we know that a prime $\mathfrak{q}$ is of semistable reduction for E, we will not know whether it is of good or multiplicative reduction. The following result gives a way of producing, for a fixed prime p, a prime of multiplicative reduction for $E = E_{a,b,c,p}$.

Lemma 2.3 (Kraus [28, p. 9]). *Let $p \geq 17$ be a prime and suppose there exists a natural number n satisfying the following conditions:*

- *we have $q := np + 1$ is a prime that splits in $\mathcal{O}_K$;*
- *we have $q \nmid \mathrm{Res}(X^n - 1, (X+1)^n - 1)$.*

Then both primes of K above q are of multiplicative reduction for E.

Proof. This result is proven in the case $K = \mathbb{Q}(\sqrt{5})$ in [28, pp. 9-10]. The proof immediately generalises to $\mathbb{Q}(\sqrt{d})$. □

We would like to level-lower the Frey curve E. We introduce the following notation. Let $\mathfrak{f}$ be a Hilbert eigenform of parallel weight 2. We write $\mathbb{Q}_\mathfrak{f}$ for its Hecke eigenfield: the field generated by its eigenvalues under the Hecke operators. When $\mathfrak{f}$ is irrational (i.e. $\mathbb{Q}_\mathfrak{f} \neq \mathbb{Q}$), we write ϖ for a prime above the rational prime p.

Theorem 2.4 (Level-Lowering, [18, p. 4]). *Let $p \geq 17$ and suppose $\overline{\rho}_{E,p}$ is irreducible. Define*

$$\mathcal{N}_p = \mathcal{N} / \prod_{\substack{\mathfrak{q} \| \mathcal{N} \\ p \mid v_\mathfrak{q}(\Delta_\mathfrak{q})}} \mathfrak{q}.$$

Then we can level-lower *E. That is, there exists a Hilbert newform $\mathfrak{f}$ at level $\mathcal{N}_p$ such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$, for some prime ϖ of $\mathbb{Q}_\mathfrak{f}$ above p.*

Proof. As E is defined over a real quadratic field, it is modular [15]. Lemma 2.2 gives the other conditions needed to level lower E, other than irreducibility which is assumed in the statement of the theorem. □

We then need to calculate the various possibilities for the level $\mathcal{N}_p$ obtained by scaling (a, b, c). We use the method described in [18, pp. 4-8] to obtain a list of possibilities for $\mathcal{N}_p$. The table in the appendix displays the possible levels $\mathcal{N}_p$ we obtained. Our code produces the same data as in [18, p. 9] for $d < 26$. At this point, there are three main issues we need to overcome.

1. Proving irreducibility of $\overline{\rho}_{E,p}$.
2. Calculating the Hilbert newforms at each level $\mathcal{N}_p$.
3. Eliminating the Hilbert newforms at each level $\mathcal{N}_p$.

Sections 3 and 4 are devoted to proving irreducibility. Section 5 is then concerned with calculating and eliminating newforms.

3 Irreducibility I: Obtaining a Bound

In order to level-lower our Frey curve (Theorem 2.4), we need irreducibility of the mod-p Galois representation $\overline{\rho}_{E,p}$.

Theorem 3.1. *The representation $\overline{\rho}_{E,p}$ is irreducible for all squarefree d with $26 \leq d \leq 97$ and $p \geq 17$.*

In this section, we reduce the problem to only needing to deal with finitely many primes p. We will in fact often obtain the full irreducibility statement we need.

As before, $E = E_{a,b,c,p}$ denotes our Frey curve defined over the quadratic field $K = \mathbb{Q}(\sqrt{d})$, and we suppose for a contradiction that the mod-p Galois representation $\overline{\rho}_{E,p}$ is reducible. Then

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix},$$

where $\theta, \theta' : G_K \to \mathbb{F}_p$ are the *isogeny characters* of the elliptic curve at p and satisfy $\theta\theta' = \chi_p$, where χ_p is the mod-p cyclotomic character. We can interchange θ and θ' by replacing E with an isogenous curve. The characters θ and θ' are unramified away from p and the additive primes for E. The additive primes for E are the primes of K above 2, and $\mathfrak{m}$ when $r = 2$ (Lemma 2.2). We write $\mathcal{N}_\theta$ and $\mathcal{N}_{\theta'}$ for the conductors of θ and θ' respectively. For $\mathfrak{q}$ an additive prime of E with $\mathfrak{q} \nmid p$, we have that $v_\mathfrak{q}(\mathcal{N})$ is even, and $v_\mathfrak{q}(\mathcal{N}_\theta) = v_\mathfrak{q}(\mathcal{N}_{\theta'}) = v_\mathfrak{q}(\mathcal{N})/2$. So if p is coprime to $\mathcal{N}_\theta$ then from our list of possibilities for $\mathcal{N}_p$ we obtain a list of possibilities for $\mathcal{N}_\theta$, since $\mathcal{N}_\theta$ is the square root of the additive part of $\mathcal{N}$. [18, p. 10].

We now consider two cases. The first is when p is coprime to one of $\mathcal{N}_\theta$ and $\mathcal{N}_{\theta'}$. By interchanging θ and θ' we may assume p is coprime to $\mathcal{N}_\theta$.

Lemma 3.2. *Suppose p is coprime to $\mathcal{N}_\theta$. Let G be the ray class group for the modulus $\mathcal{N}_\theta \infty_1 \infty_2$, where ∞_1, ∞_2 denote the two real places of K. Let n denote the exponent of G. Then E has a point of order p defined over a number field L of degree m, where $m = n$ if n is even, and $m = 2n$ if n is odd.*

Proof. (See [18, p. 10]). The order of θ divides n. We may assume that θ has order n, as otherwise we can reduce to a case where the exponent of G is less than n. Suppose n is odd. As θ has order n it cuts out a field extension of degree n over K, which we denote L, such that $\theta|_{G_L} = 1$. This gives a point of order p over L, and L is a number field of degree $2n$.

Suppose now that n is even. Let L be the field cut out by θ^2. As θ^2 has order $n/2$, L is a number field of degree $2 \cdot n/2 = n$. Then $\theta|_{G_L}$ has order 2, and so twisting by θ gives a point of order p defined over L. □

This lemma then combines with the following classification of p-torsion of elliptic curves defined over number fields, obtained by studying points on the nth symmetric power of $X_1(p)$.

Theorem 3.3 ([11, pp. 1-2])**.** *let L be a number field of degree n. Let E'/L be an elliptic curve with a point of order p over L. We have that*

$$\begin{aligned}
&\text{if } n = 2 \text{ then } p \leq 13;\\
&\text{if } n = 3 \text{ then } p \leq 13;\\
&\text{if } n = 4 \text{ then } p \leq 17;\\
&\text{if } n = 5 \text{ then } p \leq 19;\\
&\text{if } n = 6 \text{ then } p \leq 19 \text{ or } p = 37;\\
&\text{if } n = 7 \text{ then } p \leq 23.
\end{aligned}$$

Moreover, if E' has a point of order 37 defined over a field L of degree 6, then $j(E') = -9317$.

We obtain a ray class group with exponent 6, and consequently a point on E defined over a number field of degree 6, in the cases $d = 37$ and $d = 79$. In each case, the elliptic curves with j-invariant -9317 do not have full two-torsion over $\mathbb{Q}(\sqrt{d})$, and so do not arise from the Frey curve E.

When $n \geq 8$, one possibility is using the following bound of Oesterlé.

Theorem 3.4 (Oesterlé, [11, p. 21])**.** *let L be a number field of degree n. Let E'/L be an elliptic curve with a point of order p over L. Then $p \leq (3^{n/2}+1)^2$.*

In most cases we consider, the exponents of the ray class groups are ≤ 4, and so we obtain an excellent bound on p right away. The cases where an exponent is 6 are discussed above. However, for certain cases, namely when $d = 26, 34, 35, 39, 55, 82$ or 95, a ray class group has exponent 8 (see the table

in the appendix) and so we cannot apply Theorem 3.3. Applying Oesterlé's bound gives $p \leq (3^4+1)^2 = 6724$, which is rather large. Instead we use the following strategy to obtain a better bound on p. The idea revolves around the following result, which builds on work of [35, p. 2].

Theorem 3.5. *Let E' be an elliptic curve defined over any quadratic field K'. Let p be a prime, and suppose $\overline{\rho}_{E',p}$ is reducible. Let $q > 5$, $q \neq p$ be a rational prime that does not split in K', such that the unique prime of K' above q is of multiplicative reduction for E'. Then $p \leq 19$ or $p = 37$.*

We prove this result in Section 4.2 once we have discussed modular curves and formal immersions.

We fix the following notation (which will also be used in Section 5). For $\mathfrak{q}$, a prime of K, write $n_\mathfrak{q}$ for the norm of $\mathfrak{q}$, and define

$$\mathcal{A}_\mathfrak{q} := \{a \in \mathbb{Z} : |a| \leq 2\sqrt{n_\mathfrak{q}}, \quad n_\mathfrak{q} + 1 - a \equiv 0 \pmod 4\}.$$

If $\mathfrak{q}$ is a prime of good reduction for E, we know that $a_\mathfrak{q}(E) \in \mathcal{A}_\mathfrak{q}$. This follows from the Hasse–Weil bounds and the fact that E has full two-torsion over K. We then define, for $a \in \mathcal{A}_\mathfrak{q}$,

$$P_{\mathfrak{q},a} := X^2 - aX + n_\mathfrak{q}.$$

When $a = a_\mathfrak{q}(E)$, this is the characteristic polynomial of Frobenius at $\mathfrak{q}$.

Proposition 3.6. *Suppose $\overline{\rho}_{E,p}$ is reducible with $p \geq 17$. Define $B := \mathrm{Norm}(\varepsilon^{12} - 1)$. Let $\mathfrak{q}$ be a prime of K above q, with $\mathfrak{q} \nmid 2, 3, 5, p, \mathfrak{m}$, and such that q does not split in K. Define $r_\mathfrak{q} = 1$ if $\mathfrak{q}$ is a principal ideal, and $r_\mathfrak{q} = 2$ otherwise. Define*

$$R_q := \mathrm{lcm}\{\mathrm{Res}(P_{\mathfrak{q},a}(X), X^{12r_\mathfrak{q}} - 1) : a \in \mathcal{A}_\mathfrak{q}\},$$

where Res denotes the resultant of the two polynomials. Then

$$p \mid \Delta_K \cdot B \cdot R_\mathfrak{q} \quad \text{or} \quad p \in \{17, 19, 37\}.$$

We can then choose a set of primes $\{\mathfrak{q}_1, \cdots, \mathfrak{q}_t\}$, and let $R := \gcd\{R_{\mathfrak{q}_i}\}$, so that either $p \mid \Delta_K \cdot B \cdot R$ or $p \in \{17, 19, 37\}$. For the cases we considered, we found this to give much better results than applying Oesterlé's bound for $n = 8$.

Proof. Let $\mathfrak{q}$ be a prime as defined in the proposition. Then by Lemma 2.2, $\mathfrak{q}$ is a prime of semistable reduction for E. Suppose $\mathfrak{q}$ is a prime of good reduction. We then apply the result of [17, Theorem 1]: the possible non-constant isogeny characters are $\{12, 0\}$ and $\{0, 12\}$, and we obtain $B = \mathrm{Norm}(\epsilon^{12} - 1)$. It follows that if $p \nmid B \cdot \Delta_K$ then

$$p \mid \mathrm{Res}(P_{\mathfrak{q},a_\mathfrak{q}(E)}(X), X^{12r_\mathfrak{q}} - 1).$$

We do not know $a_{\mathfrak{q}}(E)$, but as discussed above, we know it lies in $\mathcal{A}_{\mathfrak{q}}$, and so $p \mid R_{\mathfrak{q}}$ as defined in the proposition.

If instead, $\mathfrak{q}$ is a prime of multiplicative reduction for E, then we apply Theorem 3.5 to conclude that $p = 17, 19$, or 37. □

We will now consider the cases where p is neither coprime to $\mathcal{N}_\theta$ nor $\mathcal{N}_{\theta'}$. In these cases, p must either split or ramify in K (see [26, p. 247]).

Lemma 3.7. *Suppose p neither coprime to $\mathcal{N}_\theta$ nor $\mathcal{N}_{\theta'}$ and that p ramifies in K. Suppose 2 is not inert in K. Let n be the exponent of the ray class group modulo $\sqrt{\mathcal{N}_A}\infty_1\infty_2$, where $\mathcal{N}_A$ is the additive part of the conductor $\mathcal{N}$. Then $p \mid 2^n - 1$.*

Proof. As 2 is not inert in K, any prime dividing 2 is a prime of potentially multiplicative reduction for E (Lemma 2.2). We then follow the argument of [18, p. 10] and apply [18, Proposition 6.2], which is stated for $K = \mathbb{Q}(\sqrt{p})$ but also holds for $K = \mathbb{Q}(\sqrt{d})$ with p ramifying in K. □

Lemma 3.8 ([18, p. 11])**.** *Suppose p neither coprime to $\mathcal{N}_\theta$ nor $\mathcal{N}_{\theta'}$ and that p splits in K. Set $n = 6$ if 2 is inert in K, and set $n = 2$ otherwise. Then $p \mid \mathrm{Norm}(\varepsilon^n - 1)$ if ε or $-\varepsilon$ is totally positive, and otherwise $p \mid \mathrm{Norm}(\varepsilon^{2n} - 1)$.*

Combining the results stated in this section reduces the problem to dealing with a finite number of primes in each case. These are shown in Table 1. We have not included the primes 17 and 19 in the table, as we will see at the start of Section 4 that $\overline{\rho}_{E,p}$ is irreducible over all real quadratic fields when $p = 17$ or 19.

d	26	29	34	35	37
$p \geq 23$	$37, 101, 103$	29	$23, 37, 59, 71, 83$	$37, 47, 61, 97$	37
d	39	53	55	59	61
$p \geq 23$	$37, 227$	53	$37, 59, 89, 179, 2437$	53	$61, 127$
d	71	73	74	82	89
$p \geq 23$	59	89	43	$37, 41, 109$	53
d	94	95	97		
$p \geq 23$	151	$31, 37, 61, 79, 97, 2027$	467		

Table 1: Irreducibility Step 1

4 Irreducibility II: Modular Curves

In the previous section we saw how to go from proving irreducibility for all primes $p \geq 17$ to a finite (and often empty) subset of primes (see Table 1).

In this section, we study quadratic points on certain modular curves $X_0(N)$ to complete the proof of Theorem 3.1.

4.1 Quadratic Points on Modular Curves

Suppose $\overline{\rho}_{E,p}$ is reducible for $p = 17, 19$, or $p \geq 23$ appearing in Table 1. As E has full two-torsion over K, it gives rise to a non-cuspidal K-point on the modular curves $X_0(p)$, $X_0(2p)$, and $X_0(4p)$. It is therefore enough to show that one of $X_0(p)(K)$, $X_0(2p)(K)$, or $X_0(4p)(K)$ has no points that could arise from E. We write $g(X_0(N))$ for the genus of $X_0(N)$. We write $X_0^{(2)}(N)$ for the symmetric square of $X_0(N)$, and denote its points by pairs: (y, z). A pair of quadratic points on $X_0(N)$ corresponds to a rational point on $X_0^{(2)}(N)$, and we will use this point of view in Section 4.2.

Recent works [38, 7, 5] have studied quadratic points on $X_0(N)$ of genus $2 \leq g \leq 5$, as well as the genus 6 hyperelliptic curve $X_0(71)$. Here, all quadratic points are considered, rather than working over a fixed quadratic field as we wish to do. We note that extending these results to (non-hyperelliptic) curves of genus ≥ 6 quickly becomes computationally impractical, and so we do not seek to do this here. There are two basic cases: either $X_0(N)$ has finitely many quadratic points or infinitely many quadratic points. A curve of genus ≥ 2 will have infinitely many quadratic points if and only if it is hyperelliptic, or bielliptic with bielliptic quotient an elliptic curve of rank ≥ 1 (see [21, p. 352]). Pulling back points on the quotient gives rise to infinitely many quadratic points on the original curve. We call these points *non-exceptional*, and points which do not arise in this way are said to be *exceptional*.

Theorem 4.1 (Ogg [36, p. 451], Bars [1, p. 11])**.** *The curve $X_0(N)$ is hyperelliptic of genus ≥ 2 if and only if $N \in \{22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71\}$. Furthermore, the hyperelliptic involution is of Atkin–Lehner type, unless $N = 37, 40,$ or 48.*

The curve $X_0(N)$ is bielliptic with an elliptic quotient of positive rank if and only if $N \in \{37, 43, 53, 61, 65, 79, 83, 89, 101, 131\}$.

We note that the curve $X_0(37)$ is both hyperelliptic and bielliptic, with an elliptic quotient of positive rank. Consequently, we do not use the terms exceptional and non-exceptional for quadratic points on this curve. For $X_0(N)$ non-hyperelliptic, the degree 2 elliptic quotients of $X_0(N)$ with infinitely many rational points are all of the form $X_0^+(N) = X_0(N)/\langle w_N \rangle$, where w_N denotes the Atkin–Lehner involution corresponding to N. The papers [5, 38] classify all quadratic points in the cases where there are finitely many such points and $2 \leq g \leq 5$. The values N with N of the form $p, 2p$, or $4p$ with $p \geq 17$ in this list are 34 and 38. In these cases, all quadratic points are defined over imaginary quadratic fields [38], and so $\overline{\rho}_{E,p}$ is irreducible for $p = 17$ and $p = 19$ over all real quadratic fields.

When the curve $X_0(N)$ has infinitely many points and $2 \leq g \leq 5$, or $X_0(N)$ is hyperelliptic, the papers [5, 7] obtain a classification of its exceptional quadratic points. In each case, no exceptional points could arise from E: they are either defined over imaginary quadratic fields or over real quadratic fields not appearing in Table 1.

Lemma 4.2. *Suppose $X_0(N)$ is hyperelliptic with $N \neq 37$, and let $P \in X_0(N)(\mathbb{Q}(\sqrt{d}))$ be a non-exceptional quadratic point. Then P corresponds to a rational point on the quadratic twist of $X_0(N)$ by d, which we denote by $X_0^d(N)$.*

Proof. We can take a model for the hyperelliptic curve $X_0(N)$ of the form $y^2 = f(x)$, with the hyperelliptic involution given by $(x, y) \mapsto (x, -y)$. If $P = (u, v) \in X_0(N)(\mathbb{Q}(\sqrt{d}))$ is a non-exceptional quadratic point, then $(u, v) = (u^\sigma, -v^\sigma)$, where σ generates $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. So $u \in \mathbb{Q}$ and $v = b\sqrt{d}$ with $b \in \mathbb{Q}$. So $db^2 = f(u)$, so $(u, b) \in X_0^d(N)(\mathbb{Q})$. □

It follows that if $X_0^d(N)(\mathbb{Q}) = \emptyset$, then we have a contradiction. This is often easily checked by seeing whether or not we have points everywhere locally; we see this in Example 4.1 below. This idea is taken further in [37]: for $X_0(N)$, possibly non-hyperelliptic, we denote by $X_0^d(N)$ the twist of $X_0(N)$ by w_N over $\mathbb{Q}(\sqrt{d})$. As mentioned in the introduction, rational points on $X_0^d(N)$ correspond to pairs of Galois conjugate quadratic points on $X_0(N)(\mathbb{Q}(\sqrt{d}))$ that map to rational points in the quotient $X_0^+(N)$. We then have the following result. The full theorem is stronger than the version we present here.

Theorem 4.3 (Ozman, [37, p. 2])**.** *Let $N > 0$ be squarefree, $K' = \mathbb{Q}(\sqrt{d'})$ a quadratic field, and let $l \nmid N$ be a prime that is ramified K'. Suppose there exists a prime, $\mathfrak{l}$, of $M := \mathbb{Q}(\sqrt{-N})$ above l, which is not a principal ideal. Then $X_0^{d'}(N)(\mathbb{Q}_l) = \emptyset$, so $X_0^{d'}(N)(\mathbb{Q}) = \emptyset$.*

Remark 4.4. The condition '$\mathfrak{l}$ is not principal' in Theorem 4.3 is equivalently stated in [37, p. 18] as '$\mathfrak{l}$ is not totally split in the Hilbert class field of M'.

Example 4.1. We consider the hyperelliptic curve $X_0(31)$. A model for this curve is given by

$$y^2 = x^6 - 8x^5 + 6x^4 + 18x^3 - 11x^2 - 14x - 3.$$

Let $d = 95$. We can check directly that $X_0^d(31)$ has no points over $\mathbb{Q}_5$. Alternatively, we can apply Theorem 4.3 with $l = 5$. The prime l ramifies in $\mathbb{Q}(\sqrt{d})$, and $l \nmid 31$. Write $M = \mathbb{Q}(\sqrt{-31})$ and H for its Hilbert class field, which is a degree 3 extension of M since M has class number 3. The prime $l = 5$ splits in $\mathcal{O}_M$, and the two primes above 5 are not principal ideals in $\mathcal{O}_M$ (equivalently, they are not totally split in H). It follows that $X_0^d(31)(\mathbb{Q}_5) = \emptyset$. We deduce that for $d = 95$, $\overline{\rho}_{E,31}$ is irreducible.

4.2 Formal Immersions and Relative Symmetric Chabauty

We start by reviewing some properties of the Jacobian, $J_0(N)$, of the modular curve $X_0(N)$. We then provide a proof of Theorem 3.5, and see how similar ideas can be used to obtain information about $\overline{\rho}_{E,p}$ when the prime q in Theorem 3.5 splits in K', in order to prove Theorem 4. We then combine this information with Theorem 4.3 to prove irreducibility for most values of p and d in Table 1.

Given $N > 0$, write $g_1, \ldots, g_k$ for representatives of the Galois conjugacy classes of Hecke eigenforms in the space of cuspforms $S_2(N)$. To each g_i is associated a simple abelian variety $A_i/\mathbb{Q}$ and we describe the Galois conjugates of g_i as the *cuspforms attached to* A_i. Each g_i arises from a newform at some level $M_i \mid N$. Writing m_i for the number of divisors of N/M_i, we have

$$J_0(N) \sim A_1^{m_1} \times \cdots \times A_k^{m_k},$$

where $\sim$ denotes isogeny over $\mathbb{Q}$ (see [34, p. 3481], for example). We see that $\mathrm{Rk}(J_0(N)) = \sum_{i=1}^{k} m_i \cdot \mathrm{Rk}(A_i)$.

We are interested in the ranks of the isogeny factors A_i. Write $L(A_i, s)$ for the L-function of A_i. A theorem of Kolyvagin and Logachev [25] asserts that if $L(A_i, 1) \neq 0$, then $\mathrm{Rk}(A_i(\mathbb{Q})) = 0$, and using `Magma` we can verify whether or not $L(A_i, 1)$ is zero. We define $\mathcal{A}_0/\mathbb{Q}$ as the largest rank 0 quotient of $J_0(N)$.

When $N = p$ is prime, we can write

$$J_0(p) \sim J_0^+(p) \times J_0^-(p),$$

where $J_0^+(p)$ is the Jacobian of the modular curve $X_0^+(p)$, and $J_0^-(p) = J_0(p)/(1+w_p)$. When $p > 7$, we denote by $J_e(p)$, or simply J_e, the *Eisenstein quotient* of $J_0(p)$, as constructed by Mazur in [31]. This is a non-trivial factor of $J_0^-(p)$ satisfying $\mathrm{Rk}(J_e(\mathbb{Q})) = 0$. In fact, $J_e(\mathbb{Q})$ is cyclic of order n, where n is the numerator of $(p-1)/12$.

Before proving Theorem 3.5, we first prove the following lemma.

Lemma 4.5 (Formal immersion criterion)**.** *Let $N = p$ or $2p$ such that $g(X_0(N)) \geq 2$. Denote the cusps of $X_0(N)$ by $\infty = c_1, c_2 \ldots, c_m$. Let $f_1, \ldots, f_t$ be cuspforms attached to $\mathcal{A}_0$. Let $(y, z) \in X_0^{(2)}(N)(\mathbb{Q})$. Let $q \neq 2, p$ be a rational prime such that $(y, z)_{\mathbb{F}_q} = (c_i, c_j)_{\mathbb{F}_q}$ for some $1 \leq i, j \leq m$. Denote by $a_n(f, c_k)$ the nth coefficient of f expanded at the cusp c_k, and define matrices*

$$F_\infty := \begin{pmatrix} a_1(f_1,\infty) & a_2(f_1,\infty) \\ \vdots & \vdots \\ a_1(f_t,\infty) & a_2(f_t,\infty) \end{pmatrix} \quad \text{and} \quad F_{\infty,k} := \begin{pmatrix} a_1(f_1,\infty) & a_1(f_1,c_k) \\ \vdots & \vdots \\ a_1(f_t,c_1) & a_1(f_t,c_k) \end{pmatrix}$$

for $2 \leq k \leq m$. If F_∞ and $F_{\infty,k}$ all have rank 2 modulo q then $(y,z) = (c_i, c_j)$.

Proof. Since $N = p$ or $2p$, the cusps of $X_0(N)$ are rational, and the set of Atkin–Lehner involutions acts transitively on the cusps. So we may assume that $(y,z)_{\mathbb{F}_q} = (\infty, c_k)_{\mathbb{F}_q}$, for some $1 \leq k \leq m$. Conisder the following Abel–Jacobi map:

$$\begin{aligned} \iota_k : X_0^{(2)}(p) &\longrightarrow J_0(p) \\ (u,v) &\longmapsto [u + v - (\infty + c_k)]. \end{aligned}$$

Let $h : X_0^{(2)}(N) \to \mathcal{A}_0$ denote the composition of ι_k with the projection map $J_0(p) \to \mathcal{A}_0$. Each cuspform f_i gives rise to an element $\omega_i \in \mathrm{Cot}(\mathcal{A}_0) \hookrightarrow \mathrm{Cot}(J_0(N))$. We then apply the formal immersion criterion as stated in [10, p. 16] to conclude that h is a formal immersion at $(\infty, c_k)_{\mathbb{F}_q}$, and since $\mathrm{Rk}(\mathcal{A}_0) = 0$, we conclude that $(y,z) = (\infty, c_k)$. □

Proof of Theorem 3.5. Suppose $p > 19$, so that $g(X_0(p)) \geq 2$. Since $\overline{\rho}_{E',p}$ is reducible, E' gives rise to a non-cuspidal K'-point, which we denote x, on the modular curve $X_0(p)$. So the pair (x, x^σ), is a rational point on $X_0^{(2)}(p)$. Since there is a unique prime of K' above q, which is of multiplicative reduction for E', it follows that $(x,x^\sigma)_{\mathbb{F}_q} = (\infty,\infty)_{\mathbb{F}_q}$ or $(0,0)_{\mathbb{F}_q}$. After applying the Atkin–Lehner involution w_p to the pair (x,x^σ) if necessary, we may assume that $(x,x^\sigma)_{\mathbb{F}_q} = (\infty,\infty)_{\mathbb{F}_q}$.

We now split into two cases. First, suppose $X_0(p)$ is non-hyperelliptic and denote by ι the Abel–Jacobi map on $X_0^{(2)}(p)$ with base point (∞,∞). We mainly follow the proof of [35, pp. 4-6] which is based on the work of Kamienny in [24, pp. 223-225]. We show that the matrix F_∞ has rank 2 modulo q, as this implies, by Lemma 4.5, that $(x,x^\sigma) = (\infty,\infty)$, a contradiction, since x is a non-cuspidal point. It therefore suffices to find a pair of newforms $f_1 = \sum a_i q^i$ and $f_2 = \sum b_i q^i$ (here $a_1 = b_1 = 1$) attached to J_e such that $a_2 \not\equiv b_2 \pmod{q}$. Equivalently, it is enough to show that the Hecke operator T_2 does not act as a scalar on J_e mod q. For $p > 61$, this is proven in [24, pp. 224-225] using the properties of J_e. For $p = 43, 53$, and 61 (the remaining primes > 19 with $X_0(p)$ non-hyperelliptic), the characteristic polynomial of T_2 on each of the Eisenstein quotients $J_e(p)$ is displayed in [24, p. 226]. We see that T_2 does not act as a scalar modulo any prime > 5, and so we also have a formal immersion at $(\infty,\infty)_{\mathbb{F}_q}$ in these cases too.

For the second case, we suppose that $p \neq 37$, and that $X_0(p)$ is hyperelliptic. We follow the argument of [23]. For these values of p, the Jacobian $J_0(p)$ has rank 0 over $\mathbb{Q}$, and the hyperelliptic involution on $X_0(p)$ is the Atkin–Lehner involution w_p (see Theorem 4.1). Since $J_0(p)$ is finite, arguing similarly to above, $\iota(x,x^\sigma) = 0$ in $J_0(p)(\mathbb{Q})$, so there exists a degree 2 rational function g on $X_0(p)$ satisfying $\mathrm{div}(g) = x + x^\sigma - 2\infty$. As g has degree

2 and $X_0(p)$ is hyperelliptic, the hyperelliptic involution, w_p, must fix ∞, a contradiction, since w_p interchanges the two cusps of $X_0(p)$. □

Unfortunately, it does not seem possible to explicitly construct inert primes of multiplicative reduction for the Frey curve $E_{a,b,c,p}$, and so in our situation, this result seems limited to its use in the proof of Proposition 3.6. We can, however, using Lemma 2.3 (usually) find split primes q, for which both primes of K above q are of multiplicative reduction for E. Although results as strong as Theorem 3.5 are not possible in this case, we can still extract useful information. The key difference for a split prime is that if we try to follow the argument used in the proof above, (x, x^σ) may reduce to $(\infty, 0)_{\mathbb{F}_q}$.

Theorem 4.6. *Let E' be an elliptic curve defined over any quadratic field K'. Let p be a prime, and suppose $\overline{\rho}_{E',p}$ is reducible, so that E' gives rise to a point $x \in X_0(p)(K')$. Let $q > 5$, $q \neq p$ be a rational prime such that q splits in K', and both primes of K' above q are of multiplicative reduction for E'. Then*

(i) either $p \leq 19$ or $p = 37$;

(ii) or $w_p(x) = x^\sigma$ on $X_0(p)$.

The main ingredient in this proof is to use Siksek's relative symmetric Chabauty criterion [40, 223-224].

Lemma 4.7 (Relative symmetric Chabauty criterion)**.** *Let $p > 19$ and let $q \neq 2$, p be a rational prime. Suppose $(y, z) \in X_0^{(2)}(p)(\mathbb{Q})$ satisfies $(y, z)_{\mathbb{F}_q} = (\infty, 0)_{\mathbb{F}_q}$. Then $w_p(y) = z$.*

Proof. Denote by ψ the degree 2 map $X_0(p) \to X_0^+(p)$. Since $q \neq p$, both $X_0(p)$ and $X_0^+(p)$ have good reduction at q, and since $p > 19$, we have $g(X_0(p)) \geq 2$. The argument we use here has links to Mazur's argument in [32, pp. 142-143].

We write $\underline{q} = e^{2\pi i \tau}$, so as to differentiate it from the prime q. Let $f_e = \sum_{i \geq 1} a_i \underline{q}^i$, with $a_1 = 1$, be a newform attached to the Eisenstein quotient, J_e, of $J_0(p)$, and write $\omega_e = \sum_{i \geq 1} a_i \underline{q}^{i-1} d\underline{q} \in \mathrm{Cot}(J_e)$ for the corresponding differential, which we view as a global 1-form on $X_0(p)$ via the inclusion $\mathrm{Cot}(J_e) \hookrightarrow H^0(X_0(p), \Omega^1)$.

We now apply the relative symmetric Chabauty criterion, as stated in [40, 223-224], to the point $(\infty, 0)$. We also use the argument of [33, p. 10] to allow $q = 3$. Using the terminology of [40], $\underline{q}$ acts as a well-behaved uniformiser at ∞. The differential ω_e satisfies three important properties which allows us to apply the criterion.

- The differential ω_e is *annihilating*. Since $J_e(\mathbb{Q})$ has rank 0, ω_e lies in the kernel on the left of the integration pairing described in [40, p. 214].

- The differential ω_e has *zero trace*. The Atkin–Lehner involution w_p induces the trace map (with respect to ψ) on global 1-forms

$$1 + w_p^* : H^0(X_0(p), \Omega^1) \longrightarrow H^0(X_0^+(p), \Omega^1).$$

  Since the projection map $J_0(p) \to J_e$ factors via $J_0^-(p) = J_0(p)/(1 + w_p)$, the 1-form ω_e lies in the kernel of this trace map.

- The differential ω_e has $\underline{q}$-expansion $(a_1 + a_2\underline{q} + a_3\underline{q}^2 + \cdots)d\underline{q}$, with $a_1 = 1 \not\equiv 0 \pmod{q}$.

Applying the criterion, it follows that $(y, z) \in \psi^*(X_0^+(p)(\mathbb{Q}))$. So $w_p(y) = z$. □

Remark 4.8. For $X_0(p)$ hyperelliptic with $p \neq 37$, we could instead prove Lemma 4.7 by repeating the argument of the proof of the hyperelliptic case of Theorem 3.5, replacing (∞, ∞) by $(\infty, 0)$.

The proof of Theorem 4.6 is then a straightforward consequence of this result.

Proof of Theorem 4.6. Since both primes of K' above q are of multiplicative reduction for E', after applying w_p if necessary, $(x, x^\sigma)_{\mathbb{F}_q} = (\infty, \infty)_{\mathbb{F}_q}$ or $(\infty, 0)_{\mathbb{F}_q}$. If $(x, x^\sigma)_{\mathbb{F}_q} = (\infty, \infty)_{\mathbb{F}_q}$, we are in the situation of the proof of Theorem 3.5 and we conclude that $p \leq 19$ or $p = 37$; so we instead suppose that $p > 19$, and that $(x, x^\sigma)_{\mathbb{F}_q} = (\infty, 0)_{\mathbb{F}_q}$. We then apply Lemma 4.7 to conclude that $w_p(x) = x^\sigma$. □

We note that Theorems 3.5 and 4.6 combine to give Theorem 4, which is stated in the introduction.

Example 4.2. We apply Theorems 4.6 and 4.3 to show that $\overline{\rho}_{E,103}$ is irreducible in the case $d = 26$. Using Lemma 2.3, we find that both primes of $\mathbb{Q}(\sqrt{26})$ above 1031 are of multiplicative reduction for E. Applying Theorem 4.6 we deduce that E gives rise to a point $x \in X_0(103)(\mathbb{Q}(\sqrt{26}))$ satisfying $w_p(x) = x^\sigma$. So E gives rise to a rational point on the twisted curve $X_0^{26}(103)$. However, applying Theorem 4.3 with the prime $l = 13$, we find that $X_0^{26}(103)(\mathbb{Q}_{13}) = \emptyset$, a contradiction.

As mentioned in Section 4.1, the case $p = 37$ is rather special, since the modular curve $X_0(37)$ is both hyperelliptic and bielliptic, with an elliptic quotient of positive rank. Moreover, the hyperelliptic involution on $X_0(37)$ is not of Atkin–Lehner type. To prove irreducibility in the case $p = 37$, we choose instead to use Lemma 4.5 and work on the curve $X_0(74)$. Our strategy is similar to that of [10, pp. 19-21].

Lemma 4.9. *Let E' be an elliptic curve defined over any quadratic field K', with a 2-torsion point defined over K'. Suppose there exists a prime $q \neq 2, 37$ such that E' has multiplicative reduction at all primes of K' above q. Then $\overline{\rho}_{E',37}$ is irreducible.*

Proof. Since E' has a 2-torsion point defined over K', it gives rise to a point $x \in X_0(74)(K')$, so that $(x, x^\sigma) \in X_0^{(2)}(74)(\mathbb{Q})$. The Jacobian of $X_0(74)$ decomposes as the following product of abelian varieties:

$$J_0(74) \sim E_a \times E_a \times A_1 \times A_2 \times E_b \times E_b.$$

Here, E_a is the elliptic curve '37a1' of rank 1, E_b is the elliptic curve '37b1' of rank 0, and A_1,A_2 are 2-dimensional abelian varieties of rank 0. We have $\mathcal{A}_0 = A_1 \times A_2 \times E_b \times E_b$. Let $f_1, \ldots, f_6$ be cuspforms attached to $\mathcal{A}_0$ (here, $f_5 = f_6$, so we can exclude f_6 if we like). Using Lemma 4.5, it suffices to check that the matrices $F_\infty, F_{\infty,2}, F_{\infty,3}$, and $F_{\infty,4}$ have rank 2 modulo q (for any $q \neq 2, 37$). We verified that this is the case using `Magma`. Note that to expand some f_i at a cusp other than ∞, we can apply the appropriate Atkin–Lehner involution. □

Using the results of this section in combination with Lemma 2.3 and Theorem 4.3 proves irreducibility for most cases appearing in Table 1. The remaining cases are displayed in Table 2. The techniques we explore in the remainder of this section will eliminate these cases, as well as provide alternative strategies for dealing with many values of p and d appearing in Table 1.

d	29	34	53	59	61	71	74	89
p	29	59	53	53	61	59	43	53

Table 2: Irreducibility Step 2

4.3 Preimages under Modular Parametrisation

Let E' be an elliptic curve defined over $\mathbb{Q}$ of conductor N. Then E' admits a map defined over $\mathbb{Q}$, called the *modular parametrisation* of E':

$$\varphi : X_0(N) \to E'.$$

We will assume E' is *optimal* so that φ is unique up to sign and maps the cusp at infinity on $X_0(N)$ to the identity of E'. Write m for the degree of the modular parametrisation, which we refer to as the *modular degree* of E'. We note here that the curve E' and the Frey curve E are not related. Their

conductors N and $\mathcal{N}$ are also not related. For background on the modular parametrisation map we refer the reader to [12, 42, 9].

Using the map φ to understand quadratic points over a fixed quadratic field is based on the following observation.

Lemma 4.10. *Let E' be an optimal elliptic curve of conductor N and write $\varphi : X_0(N) \to E'$ for its modular parametrisation. Suppose $E'(\mathbb{Q}) = E'(L)$ for L a number field. Then $X_0(N)(L) \subseteq \varphi^{-1}(E'(\mathbb{Q}))$.*

We would like to compute the fields of definition of preimages of points under the modular parametrisation map. For our purposes, this is only useful when $E'(\mathbb{Q}) = E'(K)$ is finite, but the techniques we develop apply even if this is not the case.

Suppose E' is given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in \mathbb{Q}$. Then x and y are rational functions on E' of degree 2 and 3 respectively. We can then pull these back via φ to obtain rational functions on $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$:

$$x(q) = \varphi^*(x) \quad \text{and} \quad y(q) = \varphi^*(y),$$

where $q = e^{2\pi iz}$ for $z \in \mathbb{C}$.

Using `Sage` we can compute the q expansions of $x(q)$ and $y(q)$. The rational functions $x(q)$ and $y(q)$ satisfy the equation of the elliptic curve E', as well as the relation

$$\frac{dx(q)}{2y(q) + a_1x(q) + a_3} = \frac{f(q)dq}{q},$$

where f is the rational newform of level N corresponding to the isogeny class of E'. The rational functions $x(q)$ and $y(q)$ on $X_0(N)$ have degrees $2m$ and $3m$ respectively.

We would like to obtain a planar model for the curve $X_0(N)$ by finding a relation between $x(q)$ (or $y(q)$) and another rational function on $X_0(N)$. Such a relation always exists.

Lemma 4.11 ([9, p. 24])**.** *Let $r(q), s(q) \in \mathbb{Q}(X_0(N))$ be rational functions on $X_0(N)$. Then there exists an irreducible polynomial $F \in \mathbb{Q}[R, S]$, which we call a* minimal polynomial relation*, such that $F(r(q), s(q)) = 0$, and $\deg_R(F) \leq \deg(s(q))$ and $\deg_S(F) \leq \deg(r(q))$.*

Moreover, the following result tells us that we need only check a polynomial relation up to certain precision.

Lemma 4.12 ([9, p. 28])**.** *Let $r(q), s(q) \in \mathbb{Q}(X_0(N))$ be rational functions on $X_0(N)$. Suppose $G \in \mathbb{Q}[R, S]$ satisfies $G(r(q), s(q)) = O(q^M)$ for some integer $M > 2\deg(r)\deg(s)$. Then $G(r(q), s(q)) = 0$.*

Let $r(q), s(q) \in \mathbb{Q}(X_0(N))$ and let $F \in \mathbb{Q}[R, S]$ be a minimal polynomial relation for these rational functions. Then usually F will have degree $\deg(s)$ in R and degree $\deg(r)$ in S. If this is the case then F gives a planar model for the modular curve $X_0(N)$. If the degrees are less than these maxima, then we will obtain a model for a quotient of $X_0(N)$. For example, the equation of the elliptic curve E' is a minimal polynomial relation between $x(q)$ and $y(q)$.

We aim to find a minimal polynomial relation involving between $x(q)$ and another rational function on $X_0(N)$ that will give us a planar model for our modular curve. A natural first choice is the j-function:

$$j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + \mathcal{O}(q^3) \in \mathbb{Q}(X_0(N)) \text{ for all } N.$$

The degree of $j(q)$ is given by the index of $\Gamma_0(N)$ in the full modular group $\mathrm{SL}_2(\mathbb{Z})$. As N gets large, say $N \geq 50$, it quickly becomes impractical to compute a minimal polynomial relation between $x(q)$ and $j(q)$, and so we seek to replace $j(q)$ with a rational function on $X_0(N)$ of smaller degree. We do this using eta products.

First define *Dirichlet's eta function* as

$$\eta(q) := \frac{1}{q^{24}} \prod_{n=1}^{\infty} (1 - q^n).$$

An *eta product of level* N (also referred to in the literature as an eta quotient) is then given by

$$s(q) = \prod_{d|N} \eta(q^d)^{r_d} = \prod_{d|N} \eta_d^{r_d},$$

for some integers r_d, and where we write η_d for $\eta(q^d)$. Such an eta product need not be a rational function on $X_0(N)$, but if the integers r_d satisfy certain conditions, then it is.

Theorem 4.13 (Ligozat's Criteria [30, p. 28])**.** *An eta product of level N, $\prod_{d|N} \eta_d^{r_d}$, is a rational function on $X_0(N)$ if the following conditions are satisfied:*

1. $\displaystyle\sum_d r_d \frac{N}{d} \equiv 0 \pmod{24}$;
2. $\displaystyle\sum_d r_d d \equiv 0 \pmod{24}$;
3. $\displaystyle\sum_d r_d = 0$;
4. $\displaystyle\sum_{d|N} \left(\frac{N}{d}\right)^{r_d} \in \mathbb{Q}^2$.

We note here that the support of the divisor of an eta product $s(q) \in \mathbb{Q}(X_0(N))$ is contained in the set of cusps of $X_0(N)$. Using `Sage` we can find a basis for the group of eta products of level N that are rational functions on $X_0(N)$ (i.e. that satisfy Ligozat's criteria). We can then choose

any one of these (or some combination), say $s(q)$. It is natural to start by choosing a basis element of minimal degree. We find a minimal polynomial relation between $x(q)$ and $s(q)$, and substituting in x-coordinates of points in $E'(\mathbb{Q})$ will give the s-values of the preimages of points under the modular parametrisation map, and from this we can often deduce their field of definition.

There are two issues that can arise here. The first is that the minimal polynomial relation may not be of maximal degree in its two variables. This will occur when the map $x(q) \times s(q) : X_0(N) \to \mathbb{P}^1 \times \mathbb{P}^1$ (viewing $x(q)$ and $s(q)$ as morphisms from $X_0(N)$ to $\mathbb{P}^1$) is not injective, and so the equation we obtain gives a planar model for a curve Y which is a finite quotient of $X_0(N)$. It is still possible to recover some information in this case.

The other issue is that the s-values we obtain may not give the field of definition of the points in the preimage. For example, if a degree 2 rational divisor on $X_0(N)$ has an s-value of $a \in \mathbb{Q}$, with multiplicity 2, then this could be due to two rational points, or a pair of quadratic points. By considering the cusps it is most likely we can conclude it is a pair of quadratic points, but we still do not know their field of definition, which is what we are ultimately interested in. We will see this in the example below.

To overcome both of these problems, we can usually simply replace our eta product by a different one, and if necessary combine information from multiple eta products as we see below.

Example 4.3 (Eta Product Method for $X_0(116)$)**.** We consider here the case $K = \mathbb{Q}(\sqrt{29})$ and $p = 29$. There are no elliptic curves of rank 0 over K with conductor 29 or 58, but the elliptic curve E' with Cremona label '116b1' has Mordell–Weil group $\mathbb{Z}/3\mathbb{Z}$ over both $\mathbb{Q}$ and K. The curve is given by

$$E' : y^2 = x^3 + x^2 - 4x + 4.$$

We have

$$E'(\mathbb{Q}) = E'(\mathbb{Q}(\sqrt{29})) = \{0_{E'}, R, -R\},$$

where R has x-coordinate 0. The modular degree of E' is 8.

We work with the modular curve $X_0(116)$ which is of genus 13 and has six rational points: the six cusps. We denote these cusps by $c_\infty, c_0, c_2, c_4, c_{29}$, and c_{58}. We would like to show in this case that $X_0(116)(\mathbb{Q}(\sqrt{29})) = X_0(116)(\mathbb{Q})$ as this will prove that $\overline{\rho}_{E,29}$ is irreducible.

We find a basis, using `Sage`, for the group of eta products at level 116. This basis has five elements. The first four have degree 12 as rational functions on $X_0(116)$, and the fifth has degree 14. We start by choosing the first basis element and find the minimal polynomial relation $F_1(X, S)$ between $x(q)$ and $s_1(q)$. This polynomial has degree 6 in X and 8 in S, and so does not give a planar model for $X_0(116)$, but rather a degree 2 quotient of $X_0(116)$. Although we can still obtain information from this, we instead

work with the second basis element

$$s_2 = \eta_1^{-3} \cdot \eta_2^4 \cdot \eta_4^{-1} \cdot \eta_{29}^{-1} \cdot \eta_{58}^4 \cdot \eta_{116}^{-3},$$

with divisor

$$(s_2) = -6(c_\infty) - 6(c_0) + 5(c_2) + (c_4) + (c_{29}) + 5(c_{58}).$$

We calculate a minimal polynomial relation $F_2(X, S)$ for $x(q)$ and $s_2(q)$ and find that this time it has degree 12 in X and degree $16 = 2m$ in S, so we have obtained a planar model for our curve. Some terms of this polynomial are as follows

$$F_2(X, S) = X^{12}S^{14} + \cdots + X^6S^{16} + \cdots + 1048576XS^2 - 4194304S^3.$$

Substituting in the value $0 = x(R) = x(-R)$ we find that

$$\begin{aligned} F_2(0, S) = &- 4096(S)^3(S-2)^2(S^2-8S+8)^2(S^2+2S+2) \\ &(S^4-4S^3+6S^2-4S+2). \end{aligned}$$

The factor S^3 corresponds to three cusps in the preimage, $\varphi^{-1}(\{R, -R\})$, of R and $-R$. The factor $S^4 - 4S^3 + 6S^2 - 4S + 2$ corresponds to a tuple of quartic points defined over the cyclotomic extension $\mathbb{Q}(\zeta_8)$, and the factor $S^2 + 2S + 2$ corresponds to a pair of quadratic points defined over $\mathbb{Q}(\sqrt{-1})$. The factor $(S^2 - 8S + 8)^2$ could either correspond to a pair of quadratic points defined over $\mathbb{Q}(\sqrt{2})$, or a tuple of quartic points. The factor $(S-2)^2$ may correspond to a pair of rational points or a quadratic point. We know $|X_0(116)(\mathbb{Q})| = 6$ and so we will shortly be able to see that these rational s_2-values do not arise from a pair of rational points, so $(S-2)^2$ corresponds to a pair of quadratic points, but we cannot say over which quadratic field they are defined. Finally, this factorisation does not display any poles of s_2 appearing in the preimage of R or $-R$. In the factorisation of $T^{16}F_2(0, 1/T)$ (which gives the $1/s_2$-values in the preimage) there is a factor T. This corresponds to a pole of s_2, and shows that there is a fourth cusp in preimage.

In order to understand the preimage of $0_{E'}$ we first define $G_2(Z, S) := Z^{12}F_2(1/Z, S)$, as setting $Z = 0$ will correspond to setting $X = \infty$. We find

$$G_2(0, S) = S^2(S^2 + 2S + 2)^2(S^4 - 4S^3 + 6S^2 - 4S + 2)^2.$$

We note $G_2(0, S)$ is a square since $-0_{E'} = 0_{E'}$. By considering this factorisation in conjunction with $T^{16}G(0, 1/T)$ we see that we have two cusps, a pair of quadratic points defined over $\mathbb{Q}(\sqrt{-1})$, and a tuple of quartic points defined over $\mathbb{Q}(\zeta_8)$.

In order to understand more about the fields of definition of the preimages of R and $-R$, we use the fifth basis element

$$s_5 = \eta_1^2 \cdot \eta_2^{-2} \cdot \eta_4^2 \cdot \eta_{29}^{-2} \cdot \eta_{58}^2 \cdot \eta_{116}^{-2},$$

with divisor

$$(s_5) = -7(c_\infty) + 7(c_0) - 7(c_4) + 7(c_{29}).$$

Note that this divisor is only supported on four of the six cusps. This eta product has degree 14. We find a minimal polynomial relation $F_5(X, S)$. It has degree 14 in X and 16 in S, and we have

$$\begin{aligned} F_5(0,S) =& 16384(S)(S+1)(S+29)(S^2-10S+29)^2(S^2+4S+29) \\ & (S^2+10S+29)(S^4-28S^3+272S^2-812S+841). \end{aligned}$$

As before, we recover four cusps, and a tuple of quartic points. The quadratic factors $(S^2 + 4S + 29)$ and $(S^2 + 10S + 29)$ both correspond to pairs of quadratic points defined over $\mathbb{Q}(\sqrt{-1})$. We could see the field of definition of one of these pairs using s_2, but the other pair had s_2-values 2 and we could not deduce its field of definition. We now see that this quadratic point is defined over $\mathbb{Q}(\sqrt{-1})$. We also note that the factor $(S^2-10S+29)^2$ corresponds to either a pair of quadratic points defined over $\mathbb{Q}(\sqrt{-1})$, or a tuple of quartic points. From its s_2-value, we know it must be either a pair of quadratic points defined over $\mathbb{Q}(\sqrt{2})$, or a tuple of quartic points. Combining these two pieces of information, we conclude it must be a tuple of quartic points, and that its field of definition is a quadratic extension of both $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$, so the points must be defined over $\mathbb{Q}(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\zeta_8)$.

We conclude that $\varphi^{-1}(E'(\mathbb{Q})) = \varphi^{-1}(E'(\mathbb{Q}(\sqrt{29})))$ is made up of six rational cusps, three pairs of quadratic points defined over $\mathbb{Q}(\sqrt{-1})$, and three tuples of quartic points defined over $\mathbb{Q}(\zeta_8)$, making up $24 = 8 \cdot |E'(K)|$ points in total. This proves that $X_0(116)(\mathbb{Q}(\sqrt{29})) = X_0(116)(\mathbb{Q})$, and in fact determines $X_0(116)(L)$ for any number field L with $E'(\mathbb{Q}) = E'(L)$.

We applied the same techniques to prove irreducibility for the remaining values of d and p appearing in Table 2, other than $d = 61, p = 61$ and $d = 74, p = 43$, which we consider in Section 4.4.

4.4 A Mordell–Weil Sieve

In this section, we study the modular curves $X_0(43)$ and $X_0(61)$ to prove irreducibility in the cases $d = 61, p = 61$ and $d = 74, p = 43$, thus completing the proof of Theorem 3.1. The curves $X_0(61)$ and $X_0(43)$ are bielliptic and non-hyperelliptic. Their quotients $X_0^+(43)$ and $X_0^+(61)$ are the elliptic curves with Cremona labels '43a1' and '61a1' respectively, each of which has rank 1 and trivial torsion. We employ a version of the Mordell–Weil sieve to study $X_0^d(N)(\mathbb{Q})$. We illustrate the sieving method for $X_0(61)$, although the same techniques will apply for other curves, and this method also has some overlap with the other methods we have seen. For a general introduction to the (usual) Mordell–Weil sieve, we refer the reader to [6].

The curve $X_0(61)$ has genus 4. Using the 'small modular curves' package in `Magma`, we obtain a smooth model for this curve, the Atkin–Lehner involution w_{61}, and the j-map. We start by obtaining a model for which the Atkin–Lehner involution is diagonalised. We do this by finding a matrix diagonalising w_{61} and applying the corresponding coordinate change to the equations of our curve. We obtain the following model in $\mathbb{P}^3$:

$$\begin{aligned} &-4Y^2 - 4XZ + Z^2 = T^2, \\ &X^3 - X^2Y - 3XY^2 - X^2Z + XYZ + Y^2Z - YZ^2 = 0. \end{aligned}$$

We see that this is the intersection of a quadric and a cubic surface. We write $F(X,Y,Z) = -4Y^2 - 4XZ + Z^2$, and $G(X,Y,Z)$ for the homogeneous cubic in the second defining equation of the above model. The coordinate change we have applied introduces 2 as a prime of bad reduction for this model. The Atkin–Lehner involution is now given by

$$\begin{aligned} w_{61} : X_0(61) &\longrightarrow X_0(61) \\ (x : y : z : t) &\longmapsto (x : y : z : -t). \end{aligned}$$

We see from these equations that we have the degree 2 map

$$\begin{aligned} \psi : X_0(61) &\longrightarrow X_0^+(61) \\ (x : y : z : t) &\longmapsto (x : y : z), \end{aligned}$$

with $X_0^+(61)$ the elliptic curve defined by $G(X,Y,Z) = 0$ in $\mathbb{P}^2$.

We suppose, hoping to obtain a contradiction, that our Frey curve E gives rise to a non-exceptional quadratic point on $X_0(61)(\mathbb{Q}(\sqrt{d}))$, which we denote by P here (instead of x). We are interested in the case $d = 61$, but we in fact obtained a contradiction for all $d > 0$ we tested. As P is a non-exceptional point, $w_{61}(P) = P^\sigma$. It follows that P can be expressed as $P = (x : y : z : b\sqrt{d})$ with $x, y, z, b \in \mathbb{Q}$. As $\psi(P) \in X_0^+(61)(\mathbb{Q})$, we have that $\psi(P) = m \cdot R$, for some $m \in \mathbb{Z}$, where R generates the group $X_0^+(61)(\mathbb{Q}) \cong \mathbb{Z}$.

Choose a prime $l \nmid d$ of good reduction for both $X_0(61)$ and $X_0^+(61)$ (given by the above models); in particular, $l \nmid 2 \cdot 61 \cdot d$. Write N_l for the order of R in the reduction of $X_0^+(61)$ modulo l. Write k for the residue field of K modulo a prime above l. This will either be $\mathbb{F}_l$ or $\mathbb{F}_{l^2}$. We have the following commutative diagram, where $\sim$ denotes reduction modulo l:

$$\begin{array}{ccc} X_0(61) & \xrightarrow{\psi} & X_0^+(61) \\ \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} \\ \widetilde{X}_0(61) & \xrightarrow{\widetilde{\psi}} & \widetilde{X}_0^+(61) \end{array}$$

Since $\psi(P) = m \cdot R$, we see that $\widetilde{\psi}(\widetilde{P}) = \overline{m} \cdot \widetilde{R}$, where $\overline{m} \equiv m \pmod{N_l}$. So $\widetilde{P} \in \widetilde{\psi}^{-1}(\overline{m} \cdot \widetilde{R})$. Fix $m_0 \in \{0, \cdots, N_l - 1\}$. Then we can explicitly compute the set $\widetilde{\psi}^{-1}(m_0 \cdot \widetilde{R}) = \{Q_1, Q_2\}$, where $Q_1 = (u, v, w, s)$ and $Q_2 = \widetilde{w_{61}}(Q_1) = (u, v, w, -s)$, with $u, v, w \in \mathbb{F}_l \subseteq k$ and $s \in k$. We note that we may have $Q_1 = Q_2$.

We would like to try and argue that $\widetilde{P} \notin \{Q_1, Q_2\}$ if possible, as we can then conclude that $m \not\equiv m_0 \pmod{N_l}$. There are two strategies we can use.

1. The point $P = (x : y : z : b\sqrt{d})$ satisfies $F(x, y, z) = db^2$, and so reducing mod l we have

$$F(\widetilde{x}, \widetilde{y}, \widetilde{z}) \cdot \widetilde{d}^{-1} \equiv \widetilde{b}^2 \pmod{l}.$$

   It follows that $F(u, v, w) \cdot \widetilde{d}^{-1}$ is a square mod l, so if this is not the case, then $m \not\equiv m_0 \pmod{N_l}$.

2. The Frey curve E has full two-torsion over K. If $\widetilde{P}$ is not a cusp on the reduced modular curve $\widetilde{X}_0(61)$, then it corresponds to an elliptic curve with full two-torsion over k. Also, since $w_{61}(P)$ corresponds to the elliptic curve E/C where C is a cyclic subgroup of order 61, it follows that $w_{61}(P)$ also has full two-torsion over K. Suppose $l > 3$ (to avoid the j-invariant in characteristic 3). Then if Q_1 is not a cusp, and all elliptic curves over k with j-invariant $\widetilde{j}(Q_1)$ (this consists of two elliptic curves when $\widetilde{j}(Q_1) \not\equiv 0, 1728 \pmod{l}$, and a maximum of six elliptic curves otherwise) do not have full-two torsion over k, then we have a contradiction, and we conclude $m \not\equiv m_0 \pmod{N_l}$.

We combine these two methods of elimination to obtain a list of possibilities for $m \pmod{N_l}$. We then repeat this process with a list of primes $\{l_1, \cdots, l_r\}$, and use the Chinese remainder theorem to obtain a list of possibilities for $m \pmod{N}$, where $N := \gcd(N_{l_1}, \cdots, N_{l_r})$. If this list of possibilities is empty then we obtain our desired contradiction. We choose our primes l_i so that the orders N_{l_i} are small and share many prime factors. This helps avoid a combinatorial explosion due to the Chinese remainder theorem, and also increases the likelihood of obtaining contradictory information. For the curve $X_0(61)$ and $d = 61$, using the primes $5, 7, 11, 13$ sufficed to reach a contradiction.

We note the importance of using both elimination steps in the sieve. If we do not sieve using j-invariants, then we found that the sieve did not eliminate enough possibilities for $m \pmod{N_l}$ and we could not reach a contradiction. If we do not sieve using the first method of elimination, then we are unable to eliminate the possibility that P reduces to a cusp modulo l for each prime in our list (i.e. that each prime is a prime of multiplicative reduction for E), and so we will not obtain a contradiction.

The sieving method for $X_0(43)$ is identical. The curve is of genus 3 and we used the following plane quartic model in $\mathbb{P}^3$:

$$64X^4 + 48X^3Y + 16X^2Y^2 + 8XY^3 - 3Y^4 + \\ (16X^2 + 8XY + 2Y^2)T^2 + T^4 = 0,$$

with the Atkin–Lehner involution given by $(x : y : t) \mapsto (x : y : -t)$, and the map ψ to $X_0^+(43) \in \mathbb{P}(1, 1, 2)$ given by $(x : y : t) \mapsto (x : y : t)$. We applied the sieve for $d = 74$. We obtained a contradiction using the primes $3, 5, 7, 17, 19, 29, 31, 47, 59, 61, 71, 73, 79, 107$.

5 Hecke Operators and Hilbert Newforms

5.1 Bounding the Exponent

Once we have obtained irreducibility of the mod-p Galois representations of our Frey curve, the next step is to apply the level-lowering theorem (Theorem 2.4). By our previous work, we have a list of possible levels $\mathcal{N}_p$ for our Hilbert newform, $\mathfrak{f}$, which are displayed in the appendix. We consider each possibility separately, and aim to discard all isomorphisms between the representations of our Frey curve and the newforms at this level. If we can do this at all the possible levels then we will obtain our desired contradiction.

The standard idea, as used in [18, p. 12], is as follows: compute the newforms at the level $\mathcal{N}_p$ and combine local information mod $\mathfrak{q}$ for many primes to obtain a contradiction, one newform at a time. For $\mathfrak{q}$ a prime of K not dividing $\mathcal{N}_p$, recall from Section 3 the notation

$$\mathcal{A}_\mathfrak{q} := \{a \in \mathbb{Z} : |a| \leq 2\sqrt{n_\mathfrak{q}}, \quad n_\mathfrak{q} + 1 - a \equiv 0 \pmod 4\}.$$

If $\mathfrak{q}$ is a prime of good reduction for E, then as discussed in Section 3, $a_\mathfrak{q}(E) \in \mathcal{A}_\mathfrak{q}$.

The following lemma gives the standard method of bounding the prime p. We use the same notation as in Section 2.

Lemma 5.1 ([18, p. 12])**.** *Suppose $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$. Let $\mathcal{T}$ be a set of prime ideals $\mathfrak{q}$ which do not divide $\mathcal{N}_p$. For each $\mathfrak{q} \in \mathcal{T}$ define the principal ideal*

$$B_{\mathfrak{f},\mathfrak{q}} := \big(n_\mathfrak{q}(n_\mathfrak{q} + 1 - a_\mathfrak{q}\mathfrak{f})(n_\mathfrak{q} + 1 + a_\mathfrak{q}\mathfrak{f}) \prod_{a \in \mathcal{A}_\mathfrak{q}} (a - a_\mathfrak{q}\mathfrak{f})\big) \cdot \mathcal{O}_{\mathbb{Q}_\mathfrak{f}}.$$

Set $B_\mathfrak{f} := \sum_{\mathfrak{q} \in T} B_{\mathfrak{f},\mathfrak{q}}$, and denote by $C_\mathfrak{f}$ the norm of this ideal. Then $p \mid C_\mathfrak{f}$.

If $C_\mathfrak{f}$ is non-zero we obtain a bound on p. If all the prime factors of $C_\mathfrak{f}$ are less than 17, then this discards the isomorphism for all p we are concerned with. We discuss the case $C_\mathfrak{f} = 0$ at the end of this section.

For the levels $\mathcal{N}_p$ appearing in [18] (i.e. when $2 \leq d \leq 23$), this method works as we can compute the newforms, but for larger levels this is not possible with the current Magma implementation, as discussed in [18]. The aim of this section is to provide a work-around for this by working directly with Hecke operators. This is similar to what was done in [2] where the levels obtained were too large to compute the newforms. By working directly with Hecke operators we will be able to reconstruct the eigenvalues of the newforms for the primes $\mathfrak{q} \in \mathcal{T}$. By doing this, we often lose out on knowing what the Hecke eigenfields, $\mathbb{Q}_\mathfrak{f}$, are, and so computing the norm of a sum of ideals in $\mathcal{O}_{\mathbb{Q}_\mathfrak{f}}$ as in Lemma 5.1 is impossible. The following lemma addresses this issue.

Lemma 5.2. *Suppose $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$. Let $\mathcal{T}$ be a set of prime ideals $\mathfrak{q}$ which do not divide $\mathcal{N}_p$. For each $\mathfrak{q}$, define the field $L_\mathfrak{q} := \mathbb{Q}(a_\mathfrak{q}\mathfrak{f})$, and define the element*

$$b_{\mathfrak{f},\mathfrak{q}} := n_\mathfrak{q}(n_\mathfrak{q} + 1 - a_\mathfrak{q}\mathfrak{f})(n_\mathfrak{q} + 1 + a_\mathfrak{q}\mathfrak{f}) \prod_{a \in \mathcal{A}} (a - a_\mathfrak{q}\mathfrak{f}) \in L_\mathfrak{q}.$$

Let $c_{\mathfrak{f},\mathfrak{q}} := \mathrm{Norm}_{L_\mathfrak{q}/\mathbb{Q}}(b_{\mathfrak{f},\mathfrak{q}})$. Write $c_\mathfrak{f} := \gcd\{c_{\mathfrak{f},\mathfrak{q}} : \mathfrak{q} \in T\}$. Then $p \mid c_\mathfrak{f}$.

Proof. We start by noting that the Hecke eigenfield $\mathbb{Q}_\mathfrak{f}$ of $\mathfrak{f}$ contains $L_\mathfrak{q}$ for each $\mathfrak{q} \in \mathcal{T}$, and we view $L_\mathfrak{q}$ as a subfield of $\mathbb{Q}_\mathfrak{f}$. Following the notation of the previous lemma, we note that $b_{\mathfrak{f},\mathfrak{q}} \in B_\mathfrak{f}$ for all $\mathfrak{q} \in \mathcal{T}$. The norm of an ideal is the greatest common divisor of the norm of all of its elements, and so

$$p \quad | \quad C_\mathfrak{f} \quad | \quad \gcd\{\mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(b_{\mathfrak{f},\mathfrak{q}}) : \mathfrak{q} \in \mathcal{T}\}.$$

As $L_\mathfrak{q}$ is a subfield of $\mathbb{Q}_\mathfrak{f}$ we have that

$$\mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(b_{\mathfrak{f},\mathfrak{q}}) = \left(\mathrm{Norm}_{L_\mathfrak{q}/\mathbb{Q}}(b_{\mathfrak{f},\mathfrak{q}})\right)^{[\mathbb{Q}_\mathfrak{f}:L_\mathfrak{q}]},$$

so it follows that $p \mid c_\mathfrak{f}$. □

The prime factors of $C_\mathfrak{f}$ are contained in the set of prime factors of $c_\mathfrak{f}$, and so this version may give worse bounds, but we found that in practice, by considering enough primes $\mathfrak{q}$, the two sets of prime factors coincide.

Remark 5.3. We in fact work directly with the minimal polynomial of $a_\mathfrak{q}(\mathfrak{f})$ over $\mathbb{Q}$, which we denote μ, to define $c_{\mathfrak{f},\mathfrak{q}}$. We have

$$c_{\mathfrak{f},\mathfrak{q}} = n_\mathfrak{q} \cdot \mu(n_\mathfrak{q} + 1) \cdot \mu(-n_\mathfrak{q} - 1) \cdot \prod_{a \in \mathcal{A}} \mu(a).$$

5.2 Reconstructing Hilbert Newforms

Let $\mathfrak{q}$ be a prime of K. Write $T_\mathfrak{q}$ for the Hecke operator on the space of newforms at level $\mathcal{N}_p$, and write $\chi_\mathfrak{q}$ for its characteristic polynomial. We view $T_\mathfrak{q}$ as a matrix. We then have a factorisation into irreducible polynomials

$$\chi_\mathfrak{q}(X) = \prod_{i=1}^{r} e_{\mathfrak{q},i}(X)^{m_i}.$$

The roots of each irreducible factor e_i are the eigenvalues of a Galois conjugacy class of Hilbert newforms. Associated to each e_i, we have the corresponding irreducible subspace

$$V_{\mathfrak{q},i} := \ker(e_{\mathfrak{q},i}(T_\mathfrak{q})),$$

with a basis consisting of members of Galois conjugacy classes of newforms whose eigenvalues at $\mathfrak{q}$ satisfy $e_{\mathfrak{q},i}$. To each $e_{\mathfrak{q},i}$, we also associate a value $c_{\mathfrak{q},i} := c_{\mathfrak{f},\mathfrak{q}}$ for any newform $\mathfrak{f}$ with eigenvalue at $\mathfrak{q}$ a root of $e_{\mathfrak{q},i}$.

Since the Hecke operators $T_\mathfrak{q}$ commute, if $T_{\mathfrak{q}_1}$ and $T_{\mathfrak{q}_2}$ are Hecke operators, and $V_{\mathfrak{q}_1,i_1}$ is some irreducible subspace with respect to $T_{\mathfrak{q}_1}$, then it is preserved by $T_{\mathfrak{q}_2}$ and we can compute the matrix of $T_{\mathfrak{q}_2}$ restricted to $V_{\mathfrak{q}_1,i_1}$. We can then compute the characteristic polynomial of this matrix and decompose $V_{\mathfrak{q}_1,i_1}$ into irreducible subspaces under $T_{\mathfrak{q}_2}$, which we denote by $V_{\mathfrak{q}_1,\mathfrak{q}_2,i_1,i_2}$. Such a subspace will have a basis of newforms whose eigenvalues at $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are roots of $e_{\mathfrak{q}_1,i_1}$ and $e_{\mathfrak{q}_2,i_2}$ respectively. Associated to the subspace $V_{\mathfrak{q}_1,\mathfrak{q}_2,i_1,i_2}$ is the integer $c_{\mathfrak{q}_1,\mathfrak{q}_2,i_1,i_2} := \gcd(c_{\mathfrak{f},\mathfrak{q}_1}, c_{\mathfrak{f},\mathfrak{q}_2})$, where $\mathfrak{f}$ is any newform in the space $V_{\mathfrak{q}_1,\mathfrak{q}_2,i_1,i_2}$.

We continue this process. If a value $c_{\mathfrak{q}_1\cdots\mathfrak{q}_m,i_1,\cdots,i_m}$ has all its prime factors ≤ 13 then we can discard the associated subspace, as we know that $\overline{\rho}_{E,p} \not\sim \overline{\rho}_{\mathfrak{f},\varpi}$ for any newform in this subspace. We aim to discard all possible subspaces, hence obtaining a contradiction.

We carried out this process for values d for which the maximum dimension of the space of newforms is < 9000 (see the table in the appendix) and this proves Theorem 1. The maximum dimension we considered was 8960 in the case $d = 66$. For dimensions larger than this, we found computing the Hecke operators to be computationally impractical.

By considering enough primes $\mathfrak{q}$, we found that in the cases where we *can* compute the full newform decomposition, we were able to completely reconstruct the data using the method described above. We also verified that our results agree with those in [18] when $d < 26$. We could usually eliminate all subspaces at each level. For the values $d = 33, 34, 41, 55, 57, 89$, we obtained a value $c_\mathfrak{f} = 0$. We consider these cases in Section 5.3. Also, in the cases $d = 34$ and $d = 55$, we obtained values $c_\mathfrak{f}$ divisible by 23, which is why 23 appears in the statement of Theorem 2 (but not in Table 1), as we were unable to discard these isomorphisms.

5.3 Remaining Cases

In some cases we can discard an isomorphism, or discard it for certain primes, even if $c_{\mathfrak{f}} = 0$ or has a prime factor ≥ 17. We first consider the following image of inertia argument.

Lemma 5.4 (Image of Inertia [18, p. 13])**.** *Suppose $\mathfrak{f}$ is a Hilbert newform with $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$, and write E' for the elliptic curve associated to $\mathfrak{f}$. Suppose that one of E and E' has potentially multiplicative reduction at a prime $\mathfrak{q}$ and that the other has potentially good reduction at $\mathfrak{q}$. Then $\overline{\rho}_{E,p} \not\sim \overline{\rho}_{\mathfrak{f},\varpi}$.*

We applied this argument when $d = 34$ and $d = 55$, with $\mathcal{N}_p = \mathfrak{p}^8$ in each case, using the (unique) prime above 2 which is of potentially multiplicative reduction for E (Lemma 2.2), but of potentially good reduction for each elliptic curve corresponding to a rational newform with c-value 0. This completes the proof of Theorem 2.

Note that from a rational newform $\mathfrak{f}$ (or equivalently an irreducible subspace of dimension 1) we can obtain the corresponding elliptic curve E' as follows. Using the `EllipticCurveSearch` function in `Magma` we obtain a (potentially incomplete) list of elliptic curves with conductor $\mathcal{N}_p$. We see if we can find a curve E' such that $a_{\mathfrak{q}}(E') = a_{\mathfrak{q}}\mathfrak{f}$, say for a few primes $\mathfrak{q}$. If the values $a_{\mathfrak{q}}(E')$ do not equal $a_{\mathfrak{q}}\mathfrak{f}'$ for any other newform $\mathfrak{f}'$, then by modularity E' must correspond to $\mathfrak{f}$. Even when we cannot compute the full newform decomposition, we can still verify this by considering the eigenvalues associated to each subspace (obtained using the method described in Section 5.2).

We can also often deal with fixed values of p, and hence obtain a bound on p, using a method of Kraus. The following lemma is stated in [28, p. 2] for $K = \mathbb{Q}(\sqrt{5})$, but is easily generalised to $\mathbb{Q}(\sqrt{d})$. It is based on knowing certain primes of multiplicative reduction for E (see Lemma 2.3).

Lemma 5.5 ([28, p. 2])**.** *Let $p \geq 17$ be a prime and suppose there exists a natural number n satisfying the following conditions:*

- *we have $n < p - 2$ and $n \equiv 2 \pmod 4$;*
- *we have $q := np + 1$ is a prime that splits in $\mathcal{O}_K$;*
- *we have $q \nmid \mathrm{Res}(X^n - 1, (X + 1)^n - 1)$.*

Then $\overline{\rho}_{E,p} \not\sim \overline{\rho}_{\mathfrak{f},\varpi}$ for any rational newform $\mathfrak{f}$.

We apply this lemma in the cases $d = 33, 34, 41, 57, 89$, as well as for $d = 17$, to show that $\overline{\rho}_{E,p} \not\sim \overline{\rho}_{\mathfrak{f},\varpi}$ for all but finitely many $p \leq 10^7$ when $c_{\mathfrak{f}} = 0$. We then remove these leftover primes by choosing n appropriately, as in [28, pp. 10-11]. We were able to do this for each leftover prime other than $p = 19$ in the case $d = 57$, which we consider in Section 6.

This strategy does not help eliminate the irrational newforms whose c-values are divisible by 23 in the cases $d = 34$ and $d = 55$, as the prime 23 is appearing as a factor of $(n_{\mathfrak{q}} + 1 - a_{\mathfrak{q}}\mathfrak{f})(n_{\mathfrak{q}} + 1 + a_{\mathfrak{q}}\mathfrak{f})$ for each $\mathfrak{q}$, and so using primes of multiplicative reduction will not help us rule it out. When working over $\mathbb{Q}$, the standard strategy at this point is to apply an argument using a Sturm bound. Although Sturm bounds do exist for Hilbert newforms over quadratic fields (see [8]), they are too large to be of use computationally in these cases (the bound would be much larger than the dimensions of the spaces of newforms, which would already be too large to compute with). We refer to [3] for similar discussions around Sturm bounds, and for other techniques which may be used for eliminating newforms. It may be possible to adapt these methods to this setting.

Finally, in the case $d = 89$, we apply the result of [18, p. 13] (in the same way it was applied in the case $d = 17$ in [18, p. 13]) to conclude that we have no solutions if $p \equiv \pm 2 \pmod 5$.

These results prove Theorem 3, apart from the case $d = 57, p = 19$ which we deal with in the next section.

6 Regular Primes for Quadratic Fields

In this section we see how we can sometimes avoid using the modular method altogether to show that we have no solutions to the Fermat equation over real quadratic fields for certain primes. We also complete the proof of Theorem 3 by showing that the Fermat equation over $\mathbb{Q}(\sqrt{d})$ has no non-trivial solutions for $p = 19$ when $d = 57$. We note in passing that the methods of this section are unsuccessful for most values of p and d appearing in Table 1.

A prime p is said to be *regular* if it does not divide the class number of the cyclotomic extension $\mathbb{Q}(\zeta_p)$, and *irregular* otherwise. Extending this notion, for d' a squarefree integer, a prime p is said to be *d'-regular* if it does not divide the class number of $\mathbb{Q}(\sqrt{d'}, \zeta_p)$, and *$d'$-irregular* otherwise. If p is an irregular prime, then p is also d'-irregular for all d'.

Theorem 6.1. *Let $p \geq 5$ be a d-regular prime, with $d > 0$. If $p \nmid d$ then the Fermat equation with exponent p has no non-trivial solutions in $\mathbb{Q}(\sqrt{d})$. If $d = p \cdot m$, then the Fermat equation with exponent p has no non-trivial solutions in $\mathbb{Q}(\sqrt{d})$ if $-m$ is a square mod p.*

Proof. Let $p \geq 5$ be a d-regular prime with $d > 0$. Suppose $p \nmid d$. If d is a square mod p, the result holds by [20, p. 129]. If d is not a square mod p, then combining the results of [20, p. 126,129] and [27, p. 2] shows there are no non-trivial solutions. In the case that $p \mid d$, we again apply the result of [20, p. 129] to conclude. □

To complete the proof of Theorem 3 it therefore suffices to show that 19 is 57-regular (as -3 is a square mod 19). In general, directly computing the

class numbers of cyclotomic extensions of quadratic fields is not possible, but using the work of Hao and Parry on generalised Bernoulli numbers [19], we can avoid doing this. We note that $\mathbb{Q}(\sqrt{57}, \zeta_{19}) = \mathbb{Q}(\sqrt{-3}, \zeta_{19})$, and so it is equivalent to show that 19 is -3-regular. The tables in [19] show that this is indeed the case. This completes the proof of Theorem 3.

For completeness, we state the following result, which gives a simple criterion, when $p \nmid d$ and $d > 0$, to check if a prime is d-regular.

Proposition 6.2 ([19, p. 276])**.** *Let p be an odd regular prime, let $d > 0$, and suppose $p \nmid d$. Write Δ for the discriminant of $\mathbb{Q}(\sqrt{d})$. Then p is d-regular if and only if for all odd n with $1 \leq n \leq p-2$,*

$$\sum_{j=1}^{p} S_n(j) A_{j\Delta} \not\equiv 0 \pmod{p}.$$

Here,

$$S_n(j) = \sum_{u=0}^{j-1} u^n \quad \text{and} \quad A_{j\Delta} = \sum_{\substack{t=1 \\ t \equiv j\Delta \pmod{p}}}^{\Delta} \left(\frac{\Delta}{t}\right),$$

where $\left(\frac{\Delta}{t}\right)$ denotes the Kronecker symbol.

We note that when p is a regular prime satisfying $p > \Delta$, a similar criterion to test whether p is d-regular is given in [19, p. 279] which is faster to check computationally. We found, using a short `Magma` script, that 23 is both 34-irregular and 55-irregular, which is why we cannot eliminate this prime in Theorem 2. We also checked that the 2- and 5-irregular primes obtained using our code agree with those appearing in the tables in [19].

Appendix

In the table below, n and n_{new} denote the dimensions of the spaces of Hilbert cuspforms and Hilbert newforms respectively. The column denoted RCG records the exponents of the ray class groups appearing in Lemma 3.2. The remaining column headings follow the notation of the paper.

d	S	r	$\mathfrak{m}$	$\mathcal{N}_p$	n	n_{new}	RCG
26	$\mathfrak{p}$	2	$\langle 5, \sqrt{d}+6 \rangle$	$\mathfrak{p}$	18	2	8
				$\mathfrak{m}^2\mathfrak{p}$	388	78	
29	$\mathfrak{p} = 2\mathcal{O}$	1	1	$\mathfrak{p}$	3	1	2
				$\mathfrak{p}^4$	81	45	
30	$\mathfrak{p}$	2	$\langle 3, \sqrt{d} \rangle$	$\mathfrak{p}$	28	0	2, 4
				$\mathfrak{m}^2\mathfrak{p}$	220	28	
				$\mathfrak{p}^8$	2172	544	
				$\mathfrak{m}^2\mathfrak{p}^8$	26108	2720	
31	$\mathfrak{p}$	1	1	$\mathfrak{p}$	16	2	2
				$\mathfrak{p}^4$	93	20	

33	$\mathfrak{p}_1, \mathfrak{p}_2$	1	1	$\mathfrak{p}_1\mathfrak{p}_2$	6	2	2
				$\mathfrak{p}_1\mathfrak{p}_2^4$	34	2	
34	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}+1\rangle$	$\mathfrak{p}$	36	4	2, 4, 8
				$\mathfrak{m}^2\mathfrak{p}$	292	40	
				$\mathfrak{p}^8$	2940	736	
				$\mathfrak{m}^2\mathfrak{p}^8$	35324	3680	
35	$\mathfrak{p}$	2	$\langle 5, \sqrt{d}\rangle$	$\mathfrak{p}$	28	0	2, 8
				$\mathfrak{m}^2\mathfrak{p}$	592	120	
				$\mathfrak{p}^4$	160	38	
				$\mathfrak{m}^2\mathfrak{p}^4$	4580	722	
37	$\mathfrak{p} = 2\mathcal{O}$	1	1	$\mathfrak{p}$	4	2	6
				$\mathfrak{p}^4$	135	75	
38	$\mathfrak{p}$	1	1	$\mathfrak{p}$	18	0	2, 4
				$\mathfrak{p}^8$	1310	328	
39	$\mathfrak{p}$	2	$\langle 5, \sqrt{d}+3\rangle$	$\mathfrak{p}$	36	4	2, 4, 8
				$\mathfrak{p}^4$	236	56	
				$\mathfrak{m}^2\mathfrak{p}$	792	156	
				$\mathfrak{p}^8$	3356	832	
				$\mathfrak{m}^2\mathfrak{p}^4$	6284	984	
				$\mathfrak{m}^2\mathfrak{p}^8$	99900	15808	
41	$\mathfrak{p}_1, \mathfrak{p}_2$	1	1	$\mathfrak{p}_1\mathfrak{p}_2$	6	2	1
42	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}\rangle$	$\mathfrak{p}$	36	4	2, 4
				$\mathfrak{m}^2\mathfrak{p}$	320	36	
				$\mathfrak{p}^8$	3484	864	
				$\mathfrak{m}^2\mathfrak{p}^8$	41468	4320	
43	$\mathfrak{p}$	1	1	$\mathfrak{p}$	20	0	2
				$\mathfrak{p}^4$	127	33	
46	$\mathfrak{p}$	1	1	$\mathfrak{p}$	26	4	2, 4
				$\mathfrak{p}^8$	2390	592	
47	$\mathfrak{p}$	1	1	$\mathfrak{p}$	24	2	2
				$\mathfrak{p}^4$	135	28	
51	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}\rangle$	$\mathfrak{p}$	52	4	2, 4
				$\mathfrak{m}^2\mathfrak{p}$	468	56	
				$\mathfrak{p}^4$	320	84	
				$\mathfrak{m}^2\mathfrak{p}^4$	3740	396	
53	$\mathfrak{p} = 2\mathcal{O}$	1	1	$\mathfrak{p}$	6	2	2
				$\mathfrak{p}^4$	189	105	
55	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}+4\rangle$	$\mathfrak{p}$	68	12	2, 4, 8
				$\mathfrak{p}^4$	412	96	
				$\mathfrak{m}^2\mathfrak{p}$	584	84	
				$\mathfrak{p}^8$	5916	1472	
				$\mathfrak{m}^2\mathfrak{p}^4$	4460	464	
				$\mathfrak{m}^2\mathfrak{p}^8$	70652	7360	
57	$\mathfrak{p}_1, \mathfrak{p}_2$	1	1	$\mathfrak{p}_1\mathfrak{p}_2$	12	4	2
				$\mathfrak{p}_1\mathfrak{p}_2^4$	82	6	
58	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}+1\rangle$	$\mathfrak{p}$	50	10	4
				$\mathfrak{m}^2\mathfrak{p}$	592	90	
59	$\mathfrak{p}$	1	1	$\mathfrak{p}$	32	4	2
				$\mathfrak{p}^4$	177	47	
61	$\mathfrak{p} = 2\mathcal{O}$	1	1	$\mathfrak{p}$	7	3	2
				$\mathfrak{p}^4$	295	165	
62	$\mathfrak{p}$	1	1	$\mathfrak{p}$	32	2	2, 4
				$\mathfrak{p}^8$	2710	672	
65	$\mathfrak{p}_1, \mathfrak{p}_2$	2	$\langle 7, \sqrt{d}+3\rangle$	$\mathfrak{p}_1\mathfrak{p}_2$	24	8	4
				$\mathfrak{m}^2\mathfrak{p}_1\mathfrak{p}_2$	722	54	
66	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}\rangle$	$\mathfrak{p}$	76	8	2, 4
				$\mathfrak{m}^2\mathfrak{p}$	688	88	
				$\mathfrak{p}^8$	7164	688	

				$\mathfrak{m}^2\mathfrak{p}^8$	86012	8960	
67	$\mathfrak{p}$	1	1	$\mathfrak{p}$	36	4	2
				$\mathfrak{p}^4$	247	63	
69	$\mathfrak{p}=2\mathcal{O}$	1	1	$\mathfrak{p}$	10	4	2
				$\mathfrak{p}^4$	330	177	
70	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}+1\rangle$	$\mathfrak{p}$	88	16	2, 4
				$\mathfrak{m}^2\mathfrak{p}$	840	120	
				$\mathfrak{p}^8$	8572	2144	
				$\mathfrak{m}^2\mathfrak{p}^8$	102908	10720	
71	$\mathfrak{p}$	1	1	$\mathfrak{p}$	42	8	2
				$\mathfrak{p}^4$	265	58	
73	$\mathfrak{p}_1, \mathfrak{p}_2$	1	1	$\mathfrak{p}_1\mathfrak{p}_2$	16	4	1
74	$\mathfrak{p}$	2	$\langle 5, \sqrt{d}+3\rangle$	$\mathfrak{p}$	72	12	4
				$\mathfrak{m}^2\mathfrak{p}$	1868	384	
77	$\mathfrak{p}=2\mathcal{O}$	1	1	$\mathfrak{p}$	10	4	2
				$\mathfrak{p}^4$	330	177	
78	$\mathfrak{p}$	2	$\langle 7, \sqrt{d}+6\rangle$	$\mathfrak{p}$	88	8	2, 4
				$\mathfrak{m}^2\mathfrak{p}$	3896	960	
				$\mathfrak{p}^8$	8828	2208	
				$\mathfrak{m}^2\mathfrak{p}^8$	494588	90528	
79	$\mathfrak{p}$	1	1	$\mathfrak{p}$	156	30	6
				$\mathfrak{p}^4$	1077	252	
82	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}+4\rangle$	$\mathfrak{p}$	168	40	8
				$\mathfrak{m}^2\mathfrak{p}$	1940	284	
83	$\mathfrak{p}$	1	1	$\mathfrak{p}$	44	4	2
				$\mathfrak{p}^4$	265	69	
85	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}+5\rangle$	$\mathfrak{p}$	22	10	2, 4
				$\mathfrak{m}^2\mathfrak{p}$	178	44	
				$\mathfrak{p}^4$	966	540	
				$\mathfrak{m}^2\mathfrak{p}^4$	11518	2700	
86	$\mathfrak{p}$	1	1	$\mathfrak{p}$	50	8	2, 4
				$\mathfrak{p}^8$	4958	1240	
87	$\mathfrak{p}$	2	$\langle 3, \sqrt{d}\rangle$	$\mathfrak{p}$	88	16	2, 4
				$\mathfrak{m}^2\mathfrak{p}$	932	116	
				$\mathfrak{p}^4$	656	162	
				$\mathfrak{m}^2\mathfrak{p}^4$	7484	786	
89	$\mathfrak{p}_1, \mathfrak{p}_2$	1	1	$\mathfrak{p}_1\mathfrak{p}_2$	20	4	1
91	$\mathfrak{p}$	2	$\langle 5, \sqrt{d}+1\rangle$	$\mathfrak{p}$	120	20	2, 4, 8
				$\mathfrak{m}^2\mathfrak{p}$	3128	660	
				$\mathfrak{p}^4$	832	206	
				$\mathfrak{m}^2\mathfrak{p}^4$	24740	3914	
93	$\mathfrak{p}=2\mathcal{O}$	1	1	$\mathfrak{p}$	14	6	2
				$\mathfrak{p}^4$	330	177	
94	$\mathfrak{p}$	1	1	$\mathfrak{p}$	68	14	2, 4
				$\mathfrak{p}^8$	6822	1696	
95	$\mathfrak{p}$	2	$\langle 7, \sqrt{d}+2\rangle$	$\mathfrak{p}$	116	20	2, 4, 8
				$\mathfrak{p}^4$	756	180	
				$\mathfrak{m}^2\mathfrak{p}$	4848	1188	
				$\mathfrak{p}^8$	11068	2752	
				$\mathfrak{m}^2\mathfrak{p}^4$	38572	7060	
				$\mathfrak{m}^2\mathfrak{p}^8$	616444	112832	
97	$\mathfrak{p}_1, \mathfrak{p}_2$	1	1	$\mathfrak{p}_1\mathfrak{p}_2$	25	4	1

References

[1] F. Bars. On quadratic points of classical modular curves. *arXiv preprint arXiv:1308.3267v2*, 2013.

[2] M. Bennett, V. Patel, and S. Siksek. Superelliptic equations arising from sums of consecutive powers. *Acta Arithemtica*, 172(4):377–393, 2016.

[3] N. Billerey, I. Chen, L. Dembele, L. Dieulefait, and N. Freitas. Some extensions of the modular method and Fermat equations of signature $(13, 13, n)$. *arXiv preprint arXiv:1802.04330v2*, 2018.

[4] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[5] J. Box. Quadratic points on modular curves with infinite Mordell–Weil group. *Mathematics of Computation*, 90(327):321–343, 2020.

[6] N. Bruin and M. Stoll. The Mordell–Weil sieve: proving non-existence of rational points on curves. *LMS Journal of Computation and Mathematics*, 13:272–306, 2010.

[7] P. Bruin and F. Najman. Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields. *LMS Journal of Computation and Mathematics*, 18(1):578–602, 2015.

[8] J. Burgos Gil and A. Pacetti. Hecke and Sturm bounds for Hilbert modular forms over real quadratic fields. *Mathematics of Computation*, 86(306):1949–1978, 2017.

[9] H. Chen. *Computational aspects of modular parametrizations of elliptic curves*. PhD thesis, University of Washington, 2016.

[10] M. Derickx, A. Etropolski, M. van Hoeij, J. Morrow, and D. Zureick-Brown. Sporadic cubic torsion. *arXiv preprint arXiv:2007.13929*, 2020.

[11] M. Derickx, S. Kamienny, W. Stein, and M. Stoll. Torsion points on elliptic curves over number fields of small degree. *arXiv preprint arXiv:1707.00364v2*, 2017.

[12] F. Diamond and J. Shurman. *A First Course in Modular Forms*, volume 228. Springer, 2005.

[13] L. Dickson. *History of the theory of numbers: Diophantine Analysis*, volume 2. Courier Corporation, 2013.

[14] N. Freitas, A. Kraus, and S. Siksek. Class field theory, Diophantine analysis and the asymptotic Fermat's Last Theorem. *Advances in Mathematics*, 363:106964, 2020.

[15] N. Freitas, B. Le Hung, and S. Siksek. Elliptic curves over real quadratic fields are modular. *Inventiones mathematicae*, 201(1):159–206, 2015.

[16] N. Freitas and S. Siksek. The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields. *Compositio Mathematica*, 151(8): 1395–1415, 2015.

[17] N. Freitas and S. Siksek. Criteria for irreducibility of mod p representations of Frey curves. *Journal de Théorie des Nombres de Bordeaux*, 27(1):67–76, 2015. (Used arXiv:1309.4748v3).

[18] N. Freitas and S. Siksek. Fermat's Last Theorem over some small real quadratic fields. *Algebra & Number Theory*, 9(4):875–895, 2015. (Used arXiv:1407.4435).

[19] F. Hao and C. Parry. Generalized Bernoulli numbers and m-regular primes. *Mathematics of Computation*, 43(167):273–288, 1984.

[20] F. Hao and C. Parry. The Fermat equation over quadratic fields. *Journal of Number Theory*, 19(1):115–130, 1984.

[21] J. Harris and J. Silverman. Bielliptic curves and symmetric products. *Proceedings of the American Mathematical Society*, 112(2):347–356, 1992.

[22] F. Jarvis and P. Meekin. The Fermat equation over $\mathbb{Q}(\sqrt{2})$. *Journal of Number Theory*, 109(1):182–196, 2004.

[23] S. Kamienny. Torsion points on elliptic curves over all quadratic fields II. *Bulletin de la Société Mathématique de France*, 114:119–122, 1986.

[24] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Inventiones mathematicae*, 109(1):221–229, 1992.

[25] V. Kolyvagin and D. Logachëv. Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[26] A. Kraus. Courbes elliptiques semi-stables et corps quadratiques. *Journal of Number Theory*, 60(2):245–253, 1996.

[27] A. Kraus. Équation de Fermat et nombres premiers inertes. *International Journal of Number Theory*, 11(08):2341–2351, 2015. (Used arXiv:1411.7537).

[28] A. Kraus. Sur le théorème de Fermat sur $\mathbb{Q}(\sqrt{5})$. *Annales mathématiques du Québec*, 39(1):49–59, 2015. (Used arXiv:1410.2420).

[29] A. Kraus. Le théoreme de Fermat sur certains corps de nombres totalement réels. *Algebra & Number Theory*, 13(2):301–332, 2019.

[30] G. Ligozat. *Courbes modulaires de genre 1*, volume 43. Société mathématique de France, 1975.

[31] B. Mazur. Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977.

[32] B. Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44(2):129–162, 1978.

[33] P. Michaud-Rodgers. Quadratic points on non-split Cartan modular curves. *arXiv preprint arXiv:2011.00590*, 2020.

[34] M. Murty and K. Sinha. Factoring newparts of Jacobians of certain modular curves. *Proceedings of the American Mathematical Society*, 138, 10:3481–3494, 2010.

[35] F. Najman and G. Turcas. Irreducibility of mod p Galois representations of elliptic curves with multiplicative reduction over number fields. *International Journal of Number Theory*, pages 1–10, 2021. (Used arXiv:2004.07611v3).

[36] A Ogg. Hyperelliptic modular curves. *Bulletin de la Société Mathématique de France*, 102:449–462, 1974.

[37] E. Ozman. Local points on quadratic twists of $X_0(N)$. *Acta Arithemtica*, 152:323–348, 2012. (Used arXiv:0911.4536).

[38] E. Ozman and S. Siksek. Quadratic points on modular curves. *Mathematics of Computation*, 88(319):2461–2484, 2019. (Used arXiv:1806.08192v3).

[39] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2021. `https://www.sagemath.org`.

[40] S. Siksek. Chabauty for symmetric powers of curves. *Algebra & Number Theory*, 3(2):209–236, 2009.

[41] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Annals of Mathematics*, 141:443–551, 1995.

[42] Y. Yang. Defining equations of modular curves. *Advances in Mathematics*, 204(2):481–508, 2006.

Mathematics Institute, University of Warwick, CV4 7AL, United Kingdom
E-mail address: `p.rodgers@warwick.ac.uk`