Primitive algebraic points on curves

Maleeha Khawaja

Submitted for the degree of Doctor of Philosophy

School of Mathematics and Statistics

University of Sheffield

Supervisor: Dr. Frazer Jarvis

April 2024

Dedicated to my Dado

Iffat Khawaja

1936 - 2022

Declarations

Chapter 2 is entirely expository, and gives an overview of the modular approach applied in Chapter 3. The results presented in Chapters 3 and 4 are novel, to the best of the author's knowledge, and are the author's own work (unless otherwise stated). Chapter 3 is based on the paper [KJ23] which was written in collaboration with Frazer Jarvis, and is due to appear in *Algebra & Number Theory*. Chapter 4 is based on the paper [KS24b] which was written in collaboration with Samir Siksek, and has been published in *Research in Number Theory*. I have also authored or co-authored the articles [Cop+24], [Kha24], and [KS24a] throughout the course of my PhD. These articles will not be included in my thesis. This thesis has not been submitted for a degree at another university.

Acknowledgements

I am sincerely grateful to my supervisor Dr. Frazer Jarvis for taking me on as a student, and for his support during the course of my PhD. I would like to express my gratitude to the Engineering & Physical Sciences Research Council and the University of Sheffield for providing financial support (grant no: EP/T517835/1). I would also like to thank the wider Sheffield Number Theory group for their encouragement and support. I am grateful to Haluk Şengün and Fred Diamond for examining my thesis and for their many helpful comments. I am indebted to my collaborators (Céline, Diana, Frazer, Mar, Martin, Nirvana, Özge, Samir, Vandita) for the opportunity to work with them, for clearing my confusions, and for all the ideas and wisdom they shared with me. I am deeply grateful to my friends for their moral support and for providing welcomed distractions. Finally, I am eternally grateful to my parents, siblings, family, and bunnies for their ongoing support.

Abstract

In this thesis we investigate various questions concerning rational points on curves defined over number fields. Faltings' finiteness theorem [Fal91] asserts that a curve defined over a number field K of genus greater than 1 has only finitely many points defined over K. This powerful result is ineffective and thus it is an interesting problem to determine all points on a curve defined over a fixed number field. In Chapter 3 we study the Fermat equation over real biquadratic fields, and moreover provide a complete resolution over the smallest (with respect to the discriminant) real biquadratic field. In Chapter 4 we study primitive algebraic points on curves defined over low degree number fields, and prove several sufficient sets of conditions for a curve to have finitely many primitive points of a fixed degree.

Contents

1 Introduction **9**

2 The modular approach over totally real fields **15**

2.1 The modular approach 15

2.2 Modularity of elliptic curves over totally real fields 16

2.3 Irreducibility of $\bar{\rho}_{E,p}$ 18

2.4 Level-lowering 21

3 Fermat's Last Theorem over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ **23**

3.1 Applying level-lowering 24

3.2 Small prime exponents 25

3.3 Outline of the proof 26

3.4 Computing the lowered level 27

3.5 Proving irreducibility of $\bar{\rho}_{E,p}$ 30

3.6 Eliminating Hilbert newforms 40
3.7 Divisors on curves 41
3.8 Small composite exponents 42
3.9 Some more real biquadratic fields 62

4 Primitive algebraic points on curves **64**

4.1 Primitive permutation groups 65
4.2 $\mathbb{P}^1$-isolated points 68
4.3 Finite decomposition of $C^{(d)}(\mathbb{Q})$ 72
4.4 Finitely many primitive points of low degree 73
4.5 A generalisation of Theorems 52 and 54 77
4.6 Infinitely many primitive degree d points 79
4.7 Finiteness of low degree primitive points on some $X_1(N)$ 81
4.8 Finiteness of low degree primitive points on some $X_0(N)$ 83
4.9 Primitive points on curves of low genus 86

Appendices **90**

A Complete Fermat over a cubic field **91**

B The finiteness of low degree primitive points on certain $X_1(N)$ **94**

CHAPTER 1

Introduction

Let C be a curve defined over a number field K; by which we mean a smooth projective geometrically irreducible variety defined over K of dimension 1. There are many directions one can take in the practice of studying points on a curve C; we outline two of these below.

(a) We can try to determine all points on C defined over a fixed number field.

(b) We can try to determine all points on C defined over all number fields of a fixed degree.

Each half of this thesis addresses questions related to each of these two directions.

Perhaps the most recognised curve is the one defined by the equation

$$x^2 + y^2 = z^2. \tag{1.1}$$

If $(a : b : c) \in \mathbb{P}^2(\mathbb{Q})$ satisfy (1.1) then (a, b, c) is known as a Pythagorean triple. It is

well-known that all such Pythagorean triples satisfy

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

where $m, n \in \mathbb{Q}$ and at least one of m, n is non-zero. Thus there are infinitely many rational solutions to (1.1), and we have a parameterisation for these solutions. Let us increase the exponent of each variable in (1.1) by 1; this yields the equation

$$x^3 + y^3 = z^3.$$

After some inspection, it is relatively straightforward to spot the solutions

$$(a, b, c) = (-1, 1, 0), \quad (a, b, c) = (0, 1, 1), \quad (a, b, c) = (1, 0, 1).$$

In fact, using elementary techniques, Euler proved that these are the only rational solutions [Dic66, pp. 545-546].

The Fermat equation over totally real fields. Let K be a number field, and let $n \geq 3$ be an integer. The **Fermat equation** over K with exponent n is given by

$$x^n + y^n = z^n, \qquad x, y, z \in K. \tag{F_n}$$

The **Fermat curve of degree** n is the curve defined by the Fermat equation with exponent n. Note that the genus of the Fermat curve is given by

$$\frac{(n-1)(n-2)}{2}.$$

In particular the Fermat curve of degree $n \geq 4$ has genus ≥ 3; thus, by Faltings' famous finiteness theorem [Fal91], the Fermat curve of degree n has only finitely many points defined over K.

A solution (a, b, c) to (F_n) is **trivial** if $abc = 0$, and **non–trivial** otherwise. In the 17^{th} century, Fermat claimed that if $(a, b, c) \in \mathbb{Q}^3$ satisfy (F_n) then $abc = 0$. That is, the only solutions to (F_n) over $\mathbb{Q}$ are the trivial ones. This statement became known as **Fermat's Last Theorem** from then on. In the late 20^{th} century, Wiles [Wil95] became the first to provide a complete proof of Fermat's claim.

Wiles' approach to showing that Fermat's Last Theorem holds over $\mathbb{Q}$ became known as the **modular approach**, and gave rise to a new method in the resolution of certain Diophantine equations. Jarvis and Meekin [JM04] were the first to extend the work of Wiles to a number field, and showed that there are no non-trivial solutions to (F_n) over $\mathbb{Q}(\sqrt{2})$ for all integers $n \geq 4$. One obstacle in extending the work of Wiles to more real quadratic fields (and, in general, totally real number fields) was the absence of a level-lowering mechanism analogous to Ribet's level-lowering theorem over $\mathbb{Q}$ [Rib90]. This was formulated by Freitas and Siksek [FS15c, Theorem 7] by combining previous work of Fujiwara, Jarvis, and Rajaei; we discuss this in Chapter 2, and give an overview of the modular approach over totally real fields. This led to the resolution of (F_n) over some more real quadratic fields by Freitas and Siksek [FS15b] and Michaud-Jacobs [MJ22]. Kraus [Kra19] provided a partial resolution of (F_n) over various totally real number fields of degrees ≤ 8. By a partial resolution we mean for all prime exponents $n > B_K$, where B_K is a constant depending only on K. We prove the following result in Chapter 3 using the modular approach.

Theorem (Khawaja and Jarvis)**.** Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. There are no non-trivial solutions to (F_n) over K for integers $n \geq 4$.

There are several novel obstacles that arise in the study of (F_n) over real biquadratic fields. We highlight some of these below.

Another important ingredient in Wiles' proof of Fermat's Last Theorem over $\mathbb{Q}$ is Mazur's isogeny theorem [Maz78] which asserts that the mod p Galois representation associated to any elliptic curve over $\mathbb{Q}$ is irreducible for all primes $p > 167$. A result of Freitas and Siksek [FS15a, Theorem 2] gives an explicit bound B such that the mod p Galois representation associated to an elliptic curve (satisfying certain technical assumptions) defined over a totally real Galois number field is irreducible for all primes $p > B$. Furthermore, under the assumption of the Generalised Riemann Hypothesis, Banwait [Ban23] and Banwait and Derickx [BD22] have provided analogous results for certain quadratic and cubic fields. However there is still not an unconditional equivalent

result to Mazur's theorem over any number field. In our setting, the elliptic curve in question has good or multiplicative reduction at p. This allows us to apply work of Kraus [Kra96] to bound p through making use of a class field theory argument inspired by Freitas and Siksek [FS15b] and Kraus [Kra07], as well as work of Derickx, Kamienny, Stein and Stoll [Der+23] on the primes arising as the orders of points on elliptic curves over low degree number fields.

With respect to low degree points on Fermat curves of small composite degree, the quadratic points on the Fermat curve of degree 4 have been completely determined by Aigner [Aig34] and Mordell [Mor67], and the quadratic points on the Fermat curves of degrees 6 and 9 have been completely determined by Aigner [Aig57]. However there are currently no analogous results for quartic points on the Fermat curves of these degrees. Recall that the Fermat curve of degree 4 is isomorphic to the modular curve $X_0(64)$. Moreover the modular curve $X_0(64)$ has infinitely many quartic points, arising from a degree 2 map to the elliptic curve with Cremona label `64a1`, and it is not currently known whether this is the sole source of infinitely many quartic points. To work around this complication, we extend work of Mordell [Mor67] to determine all quartic points on the Fermat curve of degree 4 lying in a quadratic extension of $\mathbb{Q}(\sqrt{2})$. To rule out solutions to (F_n) for $n = 6$ and 9 we work with a degree n hyperelliptic curve obtained from the Fermat curve of degree n. For $n = 6$ we achieve this by studying the map from the aforementioned degree n hyperelliptic curve to the elliptic curve E' with Cremona label `432b1`, as well as the Mordell–Weil group of E' over K. For $n = 9$ we achieve this through studying the Jacobian of the aforementioned degree n hyperelliptic curve.

Primitive algebraic points on curves. The study of low degree points on curves has long been an active area of research; see e.g. [AH91], [DF93], [DK94], [Fre94], [HS91], [KV22], [SV22] for results on general curves, and [Ad23], [Box22], [BD22], [BGG23], [BN15], [DNS20], [FLHS15], [Fre86], [NV23], [OS19] for results on certain families of modular curves. In particular we highlight two classical results due to Harris and Silverman [HS91] and Abramovich and Harris [AH91].

Harris and Silverman [HS91] showed that a curve C defined over a number field K of genus ≥ 2 has infinitely many points defined over degree $d = 2$ extensions of K if and only if C admits a degree $d = 2$ morphism to $\mathbb{P}^1$ or an elliptic curve defined over $\bar{K}$. In recent work, Kadets and Vogt [KV22, Theorem 1.3] showed that this morphism is in fact defined over K. Abramovich and Harris [AH91] extended the result of Harris and Silverman to points of degree 3, as well as points of degree 4 on curves of genus $\neq 7$.

Abramovich and Harris [AH91, pg. 229] conjectured that a more general statement might be true. However, Debarre and Fahlaoui [DF93, pp. 248-249] constructed several examples that disprove this conjecture for $d \geq 4$.

Given that a curve has infinitely many points of a fixed degree, one can ask whether there is a Galois-theoretic description of these points. It seems, however, that this question has received comparatively less attention. The following observation (Theorem 65) supports the need to explore this question further.

Theorem (Khawaja and Siksek)**.** Let C be a hyperelliptic curve defined over $\mathbb{Q}$ with genus 2 or 3. Let J be the Jacobian of C and suppose that $J(\mathbb{Q})$ is trivial. Then there are no quartic points on C with Galois group A_4 or S_4. However, there are infinitely many quartic points on C with Galois group contained in D_4.

In light of this observation, we recall the following definitions. Let K be a number field. We say K is **primitive** if K has no proper subfields i.e.

$$\mathbb{Q} \subseteq L \subseteq K \quad \Rightarrow \quad L = K \text{ or } L = \mathbb{Q},$$

and **imprimitive** otherwise. Let C be a curve defined over $\mathbb{Q}$. Analogously we say an algebraic point $P \in C(\overline{\mathbb{Q}})$ is **primitive** if $\mathbb{Q}(P)$ is a primitive number field, and **imprimitive** otherwise. Let $\widetilde{K}$ denote the Galois closure of K and write $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. By a well-known correspondence, K is primitive if and only if G is a primitive group (see e.g. Lemma 41 for a proof). Going back to the above theorem, the groups A_4 and S_4 are primtive whilst the group D_4 is imprimitive. Thus the theorem describes a setting under which a curve has infinitely many imprimitive quartic points and yet no primitive quartic points.

In Chapter 4, we prove several sets of conditions under which a curve has only finitely many primitive points of a fixed degree. We make use of the notion of $\mathbb{P}^1$-isolated points as introduced in [Bou+19]. A degree d point $P \in C(\overline{\mathbb{Q}})$ is **$\mathbb{P}^1$-isolated** if P does not lie in the pre-image of a non-constant degree d morphism $C \to \mathbb{P}^1$ defined over $\mathbb{Q}$. Write m for the $\mathbb{Q}$-gonality of C. Observe that if $d < m$ then any degree d point on C is $\mathbb{P}^1$-isolated. We provide several sets of conditions under which a primitive degree d point is $\mathbb{P}^1$-isolated even when $d \geq m$. In the other direction, we see that if d is big enough (with respect to the genus of C) then the existence of a single primitive degree d point guarantees the existence of infinitely many (Theorem 60).

We point out that our results are effective. To demonstrate the utility of our results, through the use of the computer algebra system `Magma` [BCP97], we compute all low degree primitive points on the modular curve $X_0(N)$ for $N = 46, 47, 59, 60, 62$ and 71.

CHAPTER 2

The modular approach over totally real fields

2.1 The modular approach

Let K be a number field. Let $n \geq 3$ be an integer. Consider the degree n Fermat equation

$$x^n + y^n = z^n \tag{F_n}$$

defining the n-th Fermat curve. Recall the following breakthrough result of Wiles [Wil95].

Theorem 1 (Wiles)**.** Let $n \geq 3$ be an integer. If $(a, b, c) \in \mathbb{Q}^3$ is a solution to (F_n) then $abc = 0$.

We give a naive sketch of the proof of Theorem 1.

Let $p \geq 5$ be a prime. Suppose $(a, b, c) \in \mathbb{Q}^3$ is a non-trivial solution ($abc \neq 0$) to (F_n) with $n = p$. As noted by Frey and Hellegouarch [Hel74], we can associate the elliptic

curve (Frey curve)

$$E : y^2 = x(x - a^p)(x + b^p)$$

to this solution. The discriminant of E is given by $16(abc)^{2p}$; note that this is non-zero precisely when (a, b, c) is non-trivial.

- **Modularity.** Without loss of generality, we can suppose a, b and c are coprime and

  $$(a, b, c) \in \mathbb{Z}^3, \qquad 2 \mid b, \qquad a^p \equiv -1 \pmod 4,$$

  after possibly scaling or reordering (a, b, c). It then follows that E is semistable, and work of Wiles [Wil95] and Taylor–Wiles [TW95] shows that E is modular.

- **Irreducibility.** Let $\bar{\rho}_{E,p}$ be the mod p Galois representation associated to E. Since E is semistable, Mazur's isogeny theorem [Maz78] asserts that $\bar{\rho}_{E,p}$ is irreducible.

- **Level-lowering.** As E is modular and $\bar{\rho}_{E,p}$ is irreducible, Ribet's level-lowering theorem [Rib90] now guarantees the existence of a newform of weight 2 and level 2 associated to $\bar{\rho}_{E,p}$.

- **Contradiction.** There are no newforms of weight 2 and level 2 contradicting the existence of (a, b, c).

We note, in particular, that applying the modular approach over totally real fields calls for a level-lowering result analogous to Ribet's level-lowering theorem. Thankfully one is readily available for us due to a combination of work done by Fujiwara, Jarvis, and Rajaei. Before stating this result, we give a brief overview of the background closely following the survey [KS24c].

2.2 Modularity of elliptic curves over totally real fields

The newforms referred to in the previous subsection are classical modular forms, and Hilbert modular forms are the corresponding objects over totally real fields. We treat

Hilbert modular forms as black-boxes, and collect some key facts using Dembélé and Voight [DV13] as a reference in place of defining them.

Let K be a totally real number field of degree d, with ring of integers $\mathcal{O}_K$. Let $\mathbf{k} = (k_1, k_2, \ldots, k_d)$ be a list of positive integers of equal parity and length d. For an ideal $\mathcal{N}$ of $\mathcal{O}_K$, the space $S_{\mathbf{k}}(\mathcal{N})$ consists of Hilbert cusp forms of weight $\mathbf{k}$ and level $\mathcal{N}$. In particular, if the k_i are all equal, say to k, then we say $\mathfrak{f} \in S_{\mathbf{k}}(\mathcal{N})$ has parallel weight k. We note that the Hilbert cusp forms that we will be concerned with are of parallel weight 2. Note that every Hilbert modular form has an associated character. However, we omit any mention of this character henceforth since the Hilbert modular forms that we will be concerned with have trivial character.

The space $S_{\mathbf{k}}(\mathcal{N})$ is acted on by a family of linear operators (Hecke operators), and this leads to the notion of Hecke eigenforms. There is also a notion of newforms of weight $\mathbf{k}$ and level $\mathcal{N}$. These are simultaneous eigenvectors to all the Hecke eigenforms that are "new" to the space $S_{\mathbf{k}}(\mathcal{N})$ in the sense that they do not arise from levels dividing $\mathcal{N}$.

Every Hilbert modular form admits a Fourier expansion, where the Fourier coefficients $a_{\mathfrak{n}}$ are indexed by ideals $\mathfrak{n}$ of $\mathcal{O}_K$. Moreover, for every newform $\mathfrak{f} \in S_{\mathbf{k}}(\mathcal{N})$, the Hecke eigenvalues of $\mathfrak{f}$ lie in the ring of integers of some number field (which we denote by $\mathbb{Q}_{\mathfrak{f}}$). In particular there is an associated L-function and Galois representation to every newform $\mathfrak{f} \in S_{\mathbf{k}}(\mathcal{N})$.

There are only finitely many Hilbert newforms $\mathfrak{f}$ of a fixed weight and level. As of date, the `LMFDB` [LMF24] is home to a database of approximately $360,000$ Hilbert newforms over 400 totally real fields of degrees at most 6. More generally, there are effective algorithms for computing Hilbert newforms as well as the Hecke eigenfield $\mathbb{Q}_{\mathfrak{f}}$. We refer the reader to [DV13] for a survey of these algorithms, and note, in particular, that these algorithms have been implemented in `Magma` [BCP97].

Definition 2. Let E be an elliptic curve over a totally real field K of conductor $\mathcal{N}$. Then E is **modular** if there is a Hilbert newform $\mathfrak{f}$ over K of parallel weight 2 and

level $\mathcal{N}$ with rational Hecke eigenvalues such that $L(E,s) = L(\mathfrak{f},s)$.

If $K = \mathbb{Q}$ then a Hilbert newform over $\mathbb{Q}$ is the same as a classical newform over $\mathbb{Q}$, and the modularity of elliptic curves over $\mathbb{Q}$ was established by Wiles [Wil95], Taylor and Wiles [TW95], and Breuil, Conrad, Diamond, and Taylor [Bre+01]. In the last decade or so, there has been significant progress in establishing the modularity of elliptic curves over totally real number fields of low degree, namely, due to work of Jarvis and Manoharmayum [JM08], Freitas, Le Hung and Siksek [FLHS15], Thorne [Tho16], Kalyanswamy [Kal18], Derickx, Najman and Siksek [DNS20], and Box [Box22].

2.3 Irreducibility of $\bar{\rho}_{E,p}$

Let K be a field, and write G_K for the absolute Galois group of K. Let $N \geq 2$ be an integer coprime to the characteristic of K. Let E be an elliptic curve over K. Recall that $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ (see e.g. [Sil09, Corollary 6.4]). Note that G_K acts linearly on $E[N]$. Then $\sigma \in G_K$ induces an automorphism

$$\bar{\rho}_{E,N}(\sigma) : \ E[N] \to E[N], \qquad P \mapsto \sigma(P)$$

which gives us the group representation

$$\bar{\rho}_{E,N} : \ G_K \to \mathrm{Aut}(E[N]).$$

Moreover, let P and Q be a basis for $E[N]$. Then, to each $\sigma \in G_K$, we can associate the matrix

$$\bar{\rho}_{E,N}(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$$

where $a_\sigma, b_\sigma, c_\sigma, d_\sigma \in \mathbb{Z}/N\mathbb{Z}$ are such that

$$\sigma(P) = a_\sigma P + c_\sigma Q, \quad \sigma(Q) = b_\sigma P + d_\sigma Q.$$

Suppose $\tau \in G_K$. Then $\bar{\rho}_{E,N}(\sigma\tau) = \bar{\rho}_{E,N}(\sigma)\bar{\rho}_{E,N}(\tau)$. In particular it follows that $\bar{\rho}_{E,N}(\sigma) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, by taking $\tau = \sigma^{-1}$. This gives us a representation

$$\bar{\rho}_{E,N} : \ G_K \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

which we say is the **mod N Galois representation associated to E**.

The following result is well-known; we give a proof as we are unable to find a reference for a complete proof.

Theorem 3. Let E be an elliptic curve over a field K, let $N \geq 2$ be an integer coprime to the characteristic of K, and let $\bar{\rho}_{E,N}$ denote the mod N Galois representation associated to E. The following statements are equivalent.

(a) E has a cyclic K-rational isogeny of degree N.

(b) $\bar{\rho}_{E,N} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}$, where $\theta,\ \theta' : G_K \to (\mathbb{Z}/N\mathbb{Z})^*$ are characters satisfying $\theta\theta' = \chi_N$, and χ_N denotes the mod N cyclotomic character.

Proof. (b) $\implies$ (a). Let $P,\ Q$ be the basis for $E[N]$ with respect to which

$$\sigma(P) = a_\sigma P, \qquad \sigma(Q) = b_\sigma P + d_\sigma Q$$

where $\theta(\sigma) = a_\sigma, \theta'(\sigma) = d_\sigma$. Then $\langle P \rangle$ is a cyclic subgroup that is stable under the action of G_K.

(a) $\implies$ (b). Let $\phi : E \to E$ denote the cyclic K-rational isogeny of degree N. It follows that the kernel of ϕ is cyclic of order N (see e.g. [Sil09, Theorem 4.10]). In particular we can write $\ker(\phi) = \langle P \rangle$, for some element $P \in E[N]$ of order N. Let $\sigma \in G_K$. Choose $Q \in E[N]$ such that $P,\ Q$ is a basis for $E[N]$. Then

$$\sigma(P) = a_\sigma P + c_\sigma Q, \qquad \sigma(Q) = b_\sigma P + d_\sigma Q,$$

for some $a_\sigma, b_\sigma, c_\sigma, d_\sigma \in \mathbb{Z}/N\mathbb{Z}$. Since the isogeny ϕ is K-rational it follows that the subgroup $\langle P \rangle$ is stable under the action of G_K. Thus $c_\sigma = 0$. Let $\theta,\ \theta' : G_K \to (\mathbb{Z}/N\mathbb{Z})^*$ be given by $\theta(\sigma) = a_\sigma,\ \theta'(\sigma) = d_\sigma$.

One consequence of the properties of the so called Weil pairing is that $\det(\bar{\rho}_{E,N}) = \chi_N$. This is a well-known fact; see e.g. [KS24c, pg. 12-13] for a proof. □

Definition 4. Let p be a prime. We say $\bar{\rho}_{E,p}$ is **reducible** if there exists some non-zero $P \in E[p]$ such that $\sigma(P) = a_\sigma P$ for all $\sigma \in G_K$, and **irreducible** otherwise.

In particular by Theorem 3, $\bar{\rho}_{E,p}$ is reducible if and only if we can write

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

where $\theta, \theta' : G_K \to (\mathbb{Z}/p\mathbb{Z})^*$ are characters satisfying $\theta\theta' = \chi_p$, and χ_p denotes the mod p cyclotomic character. This is a fundamental formulation that we will make crucial use of later on.

Relationship to the modular curve $X_0(N)$

It is often the case that the irreducibility of $\bar{\rho}_{E,p}$ needs to be proved separately for a handful of primes. In our setting, these primes are $p = 13$ and $p = 17$. Since these primes are small, it will be convenient for us to show that $\bar{\rho}_{E,p}$ is irreducible through the use of the family of modular curves $X_0(N)$.

We give an outline of this relationship. We denote the **upper-half plane** by

$$\mathbb{H} = \{x + iy \ : \ x, \ y \in \mathbb{R}, \ y > 0\}$$

Recall that the linear transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

describes a group action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. For an integer $N \geq 1$, let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ \in \ \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\}.$$

The quotient $\Gamma_0(N)\backslash\mathbb{H}$ is a non-compact Riemann surface, which turns out to be isomorphic to the set of complex points $Y_0(N)(\mathbb{C})$, where $Y_0(N)$ is a (non-compact) algebraic curve defined over $\mathbb{Q}$. Let E_1, E_2 be elliptic curves defined over $\mathbb{C}$ and let C_1, C_2 be

cyclic subgroups of order N on E_1 and E_2, respectively. Recall that the pair of elliptic curves (E_1, C_1) and (E_2, C_2) are **isomorphic** if there is an isomorphism $\phi : E_1 \to E_2$ such that $\phi(C_1) = C_2$. There is a one-to-one correspondence

$$Y_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{H} \leftrightarrow \{\text{isomorphism classes of pairs } (E/\mathbb{C},\ C)\}$$

where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of order N on E. We let $X_0(N)$ be the compactification of $Y_0(N)$. We denote the **extended upper-half plane** by $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$. Then,

$$X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{H}^*.$$

The **set of cusps** of $X_0(N)$ is given by $X_0(N)(\mathbb{C}) - Y_0(N)(\mathbb{C})$. See e.g. [DS05, Sections 1,2] for a more thorough construction of the modular curve $X_0(N)$.

Let E be an elliptic curve over K. Suppose $\bar{\rho}_{E,p}$ is reducible. Recall (from Definition 4) that $\bar{\rho}_{E,p}$ is reducible if and only if there is a non-zero point $P \in E[p]$ such that $\sigma(P) = a_\sigma P$ for all $\sigma \in G_K$. In particular the cyclic subgroup $H = \langle P \rangle$ is stable under the action of G_K. This gives us a non-cuspidal point (E, H) on the modular curve $X_0(p)$ defined over K. Furthermore, if E has a K-rational point of order 2, this gives a non-cuspidal point on the modular curve $X_0(2p)$ defined over K.

2.4 Level-lowering

We are now ready to state the level-lowering result analogous to Ribet's level-lowering theorem. This was observed by Freitas and Siksek [FS15c, Theorem 7], and is a combination of work due to Fujiwara [Fuj06], Jarvis [Jar04], and Rajaei [Raj01].

Theorem 5 (Fujiwara, Jarvis, and Rajaei)**.** Let K be a totally real field. Let $p \geq 5$ be a prime. Suppose $\mathbb{Q}(\zeta_p)^+ \not\subseteq K$. Let E be an elliptic curve over K with conductor $\mathcal{N}$. Suppose E is modular and $\bar{\rho}_{E,p}$ is irreducible. Denote by $\Delta_\mathfrak{q}$ the discriminant for a local minimal model of E at a prime ideal $\mathfrak{q}$ of K. Let

$$\mathcal{M}_p \coloneqq \prod_{\substack{\mathfrak{q} \| \mathcal{N}, \\ p | v_\mathfrak{q}(\Delta_\mathfrak{q})}} \mathfrak{q}, \qquad \mathcal{N}_p \coloneqq \frac{\mathcal{N}}{M_p}.$$

Suppose the following conditions are satisfied for all prime ideals $\mathfrak{q} \mid p$:

(i) E is semistable at $\mathfrak{q}$;

(ii) $p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$;

(iii) the ramification index satisfies $e(\mathfrak{q}/p) < p - 1$.

Then, $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$ where $\mathfrak{f}$ is a Hilbert eigenform of parallel weight 2 that is new at level $\mathcal{N}_p$ and ϖ is a prime ideal of $\mathbb{Q}_{\mathfrak{f}}$ that lies above p.

Proof. See [FS15c, p. 1402]. □

We briefly mention the existence of alternative level-lowering results whilst noting that Theorem 5 is sufficient for our purposes. For example, work of Billerey, Chen, Dieulefait and Freitas [Bil+24] on the generalised Fermat equation $x^{11} + y^{11} = z^n$, where $n \geq 2$ is an integer, makes use of a level-lowering result due to Breuil and Diamond [BD14, Theorem 3.2.2]. For more general and precise results on level optimisation, we refer the reader to work of Gee [Gee11].

CHAPTER 3

Fermat's Last Theorem over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

This chapter is based on the paper [KJ23] which was written in collaboration with Frazer Jarvis, and is due to appear in the journal 'Algebra & Number Theory'. We add some more details to this version. All computations were performed in `Magma`, and the scripts can be found in the following public GitHub repository: https://github.com/MaleehaKhawaja/Fermat.

As in [FS15c] we say the **Asymptotic Fermat's Last Theorem** holds over a totally real field K if there is a constant B_K such that there are no non-trivial solutions to the Fermat equation (F_n) over K for all primes $n > B_K$. Freitas and Siksek [FS15c] associate the solution of a certain S-unit equation over a totally real field to a putative solution of the Fermat equation. Using this approach, they prove that Asymptotic Fermat's Last Theorem holds for five-sixths of real quadratic fields. Freitas, Kraus and Siksek [FKS20] subsequently proved that Asymptotic Fermat's Last Theorem holds for several infinite families of totally real number fields. For example they prove the following result [FKS20, Corollary 1.5].

Theorem 6 (Freitas, Kraus and Siksek)**.** Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{\ell})$ where $\ell \equiv 3 \pmod 8$ is a prime. Then the Asymptotic Fermat's Last Theorem holds over K.

We prove the following theorem in this chapter using the modular approach surveyed in Chapter 2.

Theorem 7. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. There are no non-trivial solutions to the Fermat equation

$$x^n + y^n = z^n \tag{F_n}$$

over K for integers $n \geq 4$.

3.1 Applying level-lowering

Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let $p \geq 5$ be a prime. Suppose (a, b, c) is a non-trivial solution to (F_n) with $n = p$ defined over K. Recall that the traditional Frey curve associated to (a, b, c) is the elliptic curve

$$y^2 = x(x - a^p)(x + b^p).$$

Our Frey curve will be a quadratic twist of this elliptic curve by a well-chosen unit $\varepsilon \in \mathcal{O}_K^*$ (see Section 3.4). We write

$$E = E_{a,b,c,\varepsilon} \ : \ y^2 = x(x - \varepsilon a^p)(x + \varepsilon b^p). \tag{3.1}$$

The reason for allowing twists by units is to reduce the number of possibilities for the conductor of the Frey curve. We apply Theorem 5 to E in order to contradict the existence of (a, b, c). Thanks to the following theorem of Box [Box22, Theorem 1.1], we know that E is modular.

Theorem 8 (Box)**.** Let K be a totally real quartic field not containing $\sqrt{5}$. Every elliptic curve over K is modular.

We turn to the question of how to show conditions i) and ii) of Theorem 5 are satisfied. Let $\mathrm{Cl}(K)$ denote the class group of K. Let $\mathcal{H} = \mathrm{Cl}(K)/\mathrm{Cl}(K)^2$. We can

assume, without loss of generality, that any non-trivial solution (a, b, c) to (F_n) is integral. By [FS15b, Lemma 3.1], a, b, c are coprime away from a small set of primes, i.e., $\gcd(a, b, c) = \mathfrak{m} \cdot \tau^2$, where $\mathfrak{m}$ lies in a chosen set of representatives of $\mathcal{H}$ and $\tau \neq \mathfrak{m}$ is an odd prime ideal. We recall the following result of Freitas and Siksek [FS15b, Lemma 3.3].

Lemma 9 (Freitas and Siksek)**.** Let K be a totally real field. Let S denote the set of primes of K above 2. Let $\mathfrak{q}$ be a prime ideal of K such that $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$. Then E is semistable at $\mathfrak{q}$ and $p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$.

A quick check in `Magma` reveals that, in our case, the class group $\mathrm{Cl}(K)$ is trivial. Thus Lemma 9 implies that conditions i) and ii) of Theorem 5 are satisfied for $p \geq 5$. Note that the elliptic curve referred to in Lemma 9 is the traditional Frey curve. However, since our Frey curve is a quadratic twist of this elliptic curve by a unit, the set of primes dividing the conductor remains the same.

3.2 Small prime exponents

The Mordell–Weil group of the Jacobian of the Fermat curves of degrees 5, 7 and 11 is finite. This allows for the study of points on these Fermat curves over number fields of low degree.

Klassen and Tzermias [KT97] have classified all points on the Fermat quintic defined over number fields of degree at most 6. Using this classification, Kraus [Kra18, Theorem 2] has provided an algebraic description of all quartic points on the Fermat quintic.

Theorem 10 (Kraus)**.** Let K be a quartic number field. If there is a non-trivial solution to the Fermat quintic

$$x^5 + y^5 = z^5$$

defined over K then either K is the cyclic field $K = \mathbb{Q}(\alpha)$ with $31\alpha^4 - 36\alpha^3 + 26\alpha^2 - 36\alpha + 31 = 0$ or the Galois closure of K has Galois group D_4.

Tzermias [Tze98, Theorem 1] has determined all points on the Fermat septic defined over number fields of degree at most 5.

Theorem 11 (Tzermias)**.** Write F_7 for the Fermat equation of degree 7. Let ζ denote a primitive 6-th root of unity, and write $\bar{\zeta}$ for its complex conjugate. Let K be a number field of degree at most 5. Then

$$F_7(K) \subseteq F_7(\mathbb{Q}) \cup \{(\zeta, \bar{\zeta}, 1), (\bar{\zeta}, \zeta, 1)\}.$$

Gross and Rohrlich [GR78, Theorem 5.1] have determined all points on (F_n) with exponent $n = 11$ over number fields of degree at most 5.

Theorem 12 (Gross and Rohrlich)**.** Let $p = 3, 5, 7$ or 11. Suppose K is a number field of degree at most $(p-1)/2$. Let ζ denote a primitive 6-th root of unity, and write $\bar{\zeta}$ for its complex conjugate. Write F_p for the Fermat equation of degree n. Then

$$F_p(K) \subseteq F_p(\mathbb{Q}) \cup \{(\zeta, \bar{\zeta}, 1), (\bar{\zeta}, \zeta, 1)\}.$$

3.3 Outline of the proof

Throughout, unless otherwise specified, let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and write $\mathcal{O}_K$ for the ring of integers of K. We can suppose $p \geq 13$ by Theorems 10, 11 and 12. In order to prove Theorem 7 we need to complete the following steps.

1. **Determine the reduction type of E at 2.** In Section 3.4, we determine the reduction type of E at 2 using techniques outlined in [FS15b] in combination with Tate's algorithm [Sil94, Pages 364-368].

2. **Prove that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$.** In Section 3.5, we prove that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$. For $p = 13$ and 17, we prove this by studying the parameterisation of the map $X_0(2p) \to E'$, where E' is an elliptic curve of conductor $2p$. For $p \geq 19$, we use work of Derickx, Kamienny, Stein and Stoll [Der+23] and Kraus [Kra07] to obtain a contradiction if $\bar{\rho}_{E,p}$ is reducible.

3. **Eliminate the Hilbert newforms arising as a result of level lowering.** We apply a standard image of inertia argument in Section 3.6 to achieve this.

4. **Rule out solutions to (F_n) for $n = 4, 6$ and 9.** In Section 3.8, we rule out solutions for certain small integer exponents. To treat $n = 9$ and $n = 6$, we study the hyperelliptic curves obtained from the Fermat curve of degree n. To treat $n = 4$, we extend work of Mordell [Mor67] to determine all quartic points on the Fermat quartic lying in a quadratic extension of $\mathbb{Q}(\sqrt{2})$.

In Section 3.9, we give a brief overview of some obstacles that arise when extending our method to some other real biquadratic fields.

3.4 Computing the lowered level

Write $\mathcal{N}_\varepsilon$ for the conductor of the Frey curve E (3.1) above. We note that $2\mathcal{O}_K = \mathfrak{P}^4$, and $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$. Thus $\mathfrak{P}$ divides exactly one of a, b, c, since $\gcd(a, b, c) = 1$. Without loss of generality, we suppose $\mathfrak{P} \mid b$.

Lemma 13. Suppose that either $p \geq 17$ or $p = 13$ and $\mathrm{ord}_{\mathfrak{P}}(b) \geq 2$. There exists a unit $\varepsilon \in \mathcal{O}_K^*$ such that one of the following holds.

(i) Either E has multiplicative reduction at $\mathfrak{P}$,

(ii) or E has additive potentially multiplicative reduction at $\mathfrak{P}$, and $\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}_\varepsilon) = 4$.

Proof. Write c_4, c_6, Δ and j for the usual invariants attached to the model (3.1). A straightforward computation shows that

$$c_4 = \varepsilon^2 \cdot 16 \cdot (c^{2p} - a^p b^p), \qquad \Delta = \varepsilon^6 \cdot 16 \cdot (abc)^{2p}, \qquad j = c_4^3/\Delta.$$

We recall that $\mathfrak{P} \mid b$. Write $t = \mathrm{ord}_{\mathfrak{P}}(b)$. Then,

$$\mathrm{ord}_{\mathfrak{P}}(j) = 3\,\mathrm{ord}_{\mathfrak{P}}(c_4) - \mathrm{ord}_{\mathfrak{P}}(\Delta) = 32 - 2pt. \tag{3.2}$$

Under the assumptions of the lemma, we have $\mathrm{ord}_{\mathfrak{P}}(j) < 0$, thus we have potentially multiplicative reduction at $\mathfrak{P}$ (irrespective of the choice of ε).

The rest of the lemma is a consequence of [FS15b, Lemma 4.4]. We give some of the details. Let

$$\mathfrak{b} = \mathfrak{P}^{2\,\mathrm{ord}_{\mathfrak{P}}(2)+1} = \mathfrak{P}^9.$$

Consider the natural map

$$\Phi : \mathcal{O}_K^* \to (\mathcal{O}_K/\mathfrak{b})^*/((\mathcal{O}_K/\mathfrak{b})^*)^2.$$

By an explicit computation in `Magma`, we find that the image of Φ has index 2 in the codomain, and that $\lambda_1 = 1$ and $\lambda_2 = -1+2\mu$ are elements of $\mathcal{O}_K$ which represent the cokernel, where $\mu = \sqrt{2}+\sqrt{3}$. Let $n_i = \mathrm{ord}_{\mathfrak{P}}(\Delta(L_i/K))$ where $L_i = K(\sqrt{\lambda_i})$ and $\Delta(L_i/K)$ is the relative discriminant ideal for the extension L_i/K. Clearly $L_1 = K$, and thus $n_1 = 0$. Using `Magma` we find that $n_2 = 2$. Thus, by the aforementioned lemma, there is a unit $\varepsilon \in \mathcal{O}_K^*$ such that $\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}_\varepsilon) = 1$ or 4. The supporting computations can be found at https://github.com/MaleehaKhawaja/Fermat/blob/main/levels.m. □

In Lemma 13, we determined the conductor of the Frey curve E for all primes $p \geq 17$, and a suitable choice of $\varepsilon \in \mathcal{O}_K^*$. In particular, we prove that E either has multiplicative reduction or additive potentially multiplicative reduction at $\mathfrak{P}$. This proof fails for $p = 13$ in the case that $\mathrm{ord}_{\mathfrak{P}}(b) = 1$, and we treat this case in the remainder of the section.

Lemma 14. Suppose $p = 13$ and $\mathrm{ord}_{\mathfrak{P}}(b) = 1$. Then there is a unit $\varepsilon \in \mathcal{O}_K^*$ and $\alpha \in \mathcal{O}_K$ such that

$$\mathfrak{P}^6 \mid (\varepsilon b^{13} - \varepsilon a^{13} - \alpha^2),$$

where $\mathfrak{P} \nmid \alpha$.

Proof. Let

$$\theta : \mathcal{O}_K^* \to U/U^2,$$

where $U = \left(\mathcal{O}_K/\mathfrak{P}^6\right)^*$. We checked that θ is surjective using a straightforward computation in `Magma`. Let $\beta = b^{13} - a^{13}$. Note that $\mathfrak{P} \nmid \beta$. As θ is surjective, there is some $\gamma \in \mathcal{O}_K^*$ such that $\theta(\gamma) = \beta U^2$. Thus $\beta \equiv \gamma\alpha^2 \pmod{\mathfrak{P}^6}$ for some $\alpha \in \mathcal{O}_K \setminus \mathfrak{P}$. Let $\varepsilon = \gamma^{-1} \in \mathcal{O}_K^*$. Then $\varepsilon\beta \equiv \alpha^2 \pmod{\mathfrak{P}^6}$, which proves the lemma. □

Let $\varepsilon \in \mathcal{O}_K^*$ be as in Lemma 14. We begin by working with the Frey curve

$$E_{13,\,\varepsilon} : y^2 = x(x - \varepsilon a^{13})(x + \varepsilon b^{13}). \tag{3.3}$$

We recall that, by Lemma 9, $E_{13,\,\varepsilon}$ is semistable away from $\mathfrak{P}$. Thus in order to determine the conductor of $E_{13,\,\varepsilon}$, it remains to determine the reduction type of $E_{13,\,\varepsilon}$ at $\mathfrak{P}$.

Lemma 15. Suppose $\mathrm{ord}_{\mathfrak{P}}(b) = 1$. The Frey curve $E_{13,\,\varepsilon}$ has additive potentially good reduction at $\mathfrak{P}$. Moreover $\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}) = 5$, where $\mathcal{N}$ is the conductor of $E_{13,\,\varepsilon}$.

Proof. Let $\alpha \in \mathcal{O}_K$ be as in Lemma 14. Recall that K has class number 1 and therefore every ideal is principal. Let π be an generator for $\mathfrak{P}$. For example, we can take

$$\pi = \frac{\mu^3 + \mu^2 - 9\mu - 9}{4},$$

where $\mu = \sqrt{2} + \sqrt{3}$. We make the substitutions

$$x \mapsto \pi^6 x, \qquad y \mapsto \alpha\pi^6 x + \pi^9 y.$$

This yields the model

$$W : y^2 + \frac{2\alpha}{\pi^3}xy = x^3 + \frac{(\varepsilon b^{13} - \varepsilon a^{13} - \alpha^2)}{\pi^6}x^2 - \frac{\varepsilon^2 a^{13} b^{13}}{\pi^{12}}x$$

which is integral by Lemma 14, and has discriminant

$$\Delta(W) = \frac{\Delta(E_{13,\,\varepsilon})}{\pi^{36}} = \frac{16\varepsilon^6 a^{26} b^{26} c^{26}}{\pi^{36}}.$$

Note that $\mathrm{ord}_{\mathfrak{P}}(\Delta(W)) = 6 < 12$. Thus W is minimal at $\mathfrak{P}$. We use Tate's algorithm [Sil94, Pages 364-368] to compute the valuation of the conductor for W. Let $a_1, \ldots, a_6$

be the usual a-invariants for W given in the above model, and let $b_2, \ldots, b_8$ be the corresponding b-invariants:

$$b_2 = \frac{4(\varepsilon b^{13} - \varepsilon a^{13})}{\pi^6}, \quad b_4 = -\frac{2\varepsilon^2 a^{13} b^{13}}{\pi^{12}}, \quad b_6 = 0, \quad b_8 = -\frac{\varepsilon^4 a^{26} b^{26}}{\pi^{24}}.$$

In particular, $\mathfrak{P} \mid a_3$, a_4, b_2, and $\mathfrak{P}^2 \mid a_6$ and $\mathrm{ord}_{\mathfrak{P}}(b_8) = 2$. Thus, by Step 4 of Tate's algorithm the reduction type for W at $\mathfrak{P}$ is III and the valuation of the conductor at $\mathfrak{P}$ is

$$\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}) = \mathrm{ord}_{\mathfrak{P}}(\Delta(W)) - 1 = 5.$$

□

3.5 Proving irreducibility of $\bar{\rho}_{E,p}$

In this section, we prove that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$. In particular, we show that one possible consequence of $\bar{\rho}_{E,p}$ being reducible is that E has a K-rational point of order p. In this instance, for $p \geq 19$, we obtain a contradiction partly through the application of the following result of Derickx, Kamienny, Stein and Stoll [Der+23, Theorem 1.2].

Theorem 16 (Derickx, Kamienny, Stein and Stoll)**.** For a positive integer d, let $S(d)$ denote the set of primes p such that there is an elliptic curve E defined over a degree d number field K such that E has a K-rational point of order p. Then

$$S(4) = \mathrm{Primes}(17);$$
$$S(5) = \mathrm{Primes}(19);$$
$$S(6) = \mathrm{Primes}(19) \cup \{37\};$$
$$S(7) = \mathrm{Primes}(23),$$

where $\mathrm{Primes}(x)$ denotes the set of primes less than or equal to x.

Thus we are required to prove that $\bar{\rho}_{E,p}$ is irreducible for $p = 13$ and 17 using a separate argument.

Demonstrating the irreducibility of $\bar{\rho}_{E,13}$ and $\bar{\rho}_{E,17}$

Recall (from Section 2.3) that if $\bar{\rho}_{E,p}$ is reducible there there is a non-cuspidal K-point on the modular curve $X_0(p)$ and $X_0(2p)$.

We find it convenient to work with the modular curves $X_0(26)$ and $X_0(34)$. In particular, we show that $X_0(26)(K) = X_0(26)(\mathbb{Q})$ and $X_0(34)(K) = X_0(34)(\mathbb{Q})$, and we know that all points in $X_0(26)(\mathbb{Q})$ and $X_0(34)(\mathbb{Q})$ are cuspidal by work of Kenku [Ken82].

Let E' be an elliptic curve defined over $\mathbb{Q}$. By the famous modularity theorem due to [Wil95], [TW95] and [Bre+01], there is a rational map $\pi : X_0(N) \to E'$ for some positive integer N which we say is the **modular parameterisation** of E'. Let F be a number field. Note the inclusion $\pi(X_0(N)(F)) \subseteq E'(F)$. Suppose that $E'(F) = E'(L)$, for a subfield L of F. In this scenario, an explicit parameterisation of π can be used to extract more information about $X_0(N)(F)$.

$p = 13$

Suppose $P \in X_0(26)(K)$. Let $L = \mathbb{Q}(\sqrt{3})$. We prove that one of the following holds.

(a) $P \in X_0(26)(L)$;

(b) $C(L)$ is non-empty, where C is a certain genus 2 hyperelliptic curve.

In case (a) it follows from work of Bruin and Najman [BN15] that $P \in X_0(26)(\mathbb{Q})$. In case (b) we show that $C(L)$ is empty using an elementary local argument.

Lemma 17. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let E be an elliptic curve over K. Then $\bar{\rho}_{E,13}$ is irreducible.

Proof. We prove that $X_0(26)(K) = X_0(26)(\mathbb{Q})$. We work with the model

$$X_0(26) : \ y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1 \tag{3.4}$$

given in `Magma`. Let

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

Then E' is the elliptic curve with Cremona label `26b1`. Suppose $P = (a, b) \in X_0(26)(K)$. Note that if $a = 1$ then $b^2 = -16$, i.e., $P \notin X_0(26)(K)$. We henceforth assume that $a \neq 1$. Using `Magma`, we find the explicit parametrisation

$$\begin{aligned} \pi : X_0(26) &\longrightarrow E' \\ (a, b) &\longmapsto \left(-\frac{(a+1)^2}{(a-1)^2}, \ \frac{-2b + 2a(a-1)}{(a-1)^3} \right). \end{aligned}$$

Let $L = \mathbb{Q}(\sqrt{3})$. Using `Magma` we found that the Mordell–Weil group of E' over K is given by

$$E'(K) = (-1, -2) \cdot \mathbb{Z}/7\mathbb{Z} \oplus (-2\sqrt{3} + 5, 8\sqrt{3} - 14) \cdot \mathbb{Z}.$$

Thus $E'(K) = E'(L)$. It immediately follows that

$$\left(\frac{a+1}{a-1} \right)^2 \in L.$$

Let

$$\sigma : K \to K, \quad \sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}.$$

Then

$$\sigma \left(\frac{a+1}{a-1} \right) = \frac{a+1}{a-1} \quad \text{or} \quad \sigma \left(\frac{a+1}{a-1} \right) = -\frac{a+1}{a-1}.$$

Thus there are two cases to consider:

(1) $(a+1)/(a-1) \in L$;

(2) $(a+1)/(a-1) \in \sqrt{2} \cdot L$.

Case (1) In this case, we have $a \in L$, and it immediately follows from the parameterisation of π that $b \in L$. Observe that $X_0(26)$ has infinitely many quadratic points of the form $(r, \sqrt{f(r)})$, where $r \in \mathbb{Q}$. Such points are called **non-exceptional** and all other quadratic points are called **exceptional**.

Case (1.1) If $a \in L \setminus \mathbb{Q}$ then P is an exceptional quadratic point on $X_0(26)$. Bruin and Najman [BN15, Table 3] have given an explicit description of all quadratic points on $X_0(26)$. In particular they find that all exceptional quadratic points are defined over $\mathbb{Q}(\sqrt{d})$ for $d = -1, -3, -11$ and -23.

Case (1.2) If $a \in \mathbb{Q}$ then $b^2 \in \mathbb{Q}$. Then P is a non-exceptional quadratic point on $X_0(26)$ defined over L. Moreover P corresponds to a rational point on the quadratic twist X_3 of $X_0(26)$ over L given by

$$X_3 : \ y^2 = 3x^6 - 24x^5 + 24x^4 - 54x^3 + 24x^2 - 24x + 3.$$

We checked using `Magma` that the curve X_3 has no points defined over $\mathbb{Q}_3$. Thus $X_3(\mathbb{Q})$ is empty.

Case (2) In this case we have $(a+1)/(a-1) \in \sqrt{2} \cdot L$, i.e.,

$$\frac{a+1}{a-1} = \sqrt{2}\alpha, \quad \text{for some } \alpha \in L. \tag{3.5}$$

Note the following identity:

$$\left(\frac{a+1}{a-1}\right)^2 - 1 = \frac{(a+1)^2 - (a-1)^2}{(a-1)^2} = \frac{4a}{(a-1)^2} = \frac{4a(a-1)}{(a-1)^3}. \tag{3.6}$$

From the parametrisation of π and (3.6), we see that

$$\frac{b}{(a-1)^3} \in L.$$

Note the following identity

$$16\left(\frac{a^6 - 8a^5 + 8a^4 - 18a^3 + 8a^2 - 8a + 1}{(a-1)^6}\right) = -4\left(\frac{a+1}{a-1}\right)^6 - 3\left(\frac{a+1}{a-1}\right)^4 + 10\left(\frac{a+1}{a-1}\right)^2 + 13. \tag{3.7}$$

By combining (3.4) and (3.7), we obtain

$$\left(\frac{4b}{(a-1)^3}\right)^2 = -4\left(\frac{a+1}{a-1}\right)^6 - 3\left(\frac{a+1}{a-1}\right)^4 + 10\left(\frac{a+1}{a-1}\right)^2 + 13.$$

After making the substitutions $\beta = 4b/(a-1)^3$ and (3.5), we obtain

$$\beta^2 = -32\alpha^6 - 12\alpha^4 + 20\alpha^2 + 13.$$

Thus (α, β) is a L-rational point on the curve

$$C : y^2 = -32x^6 - 12x^4 + 20x^2 + 13.$$

Write $\mathcal{O}_L$ for the ring of integers of L. Then $13\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. We checked using `Magma` that there there are no points on C defined over the completion of L at $\mathfrak{p}_1$. Thus $C(L)$ is empty. □

Remark 18. Note that there are infinitely many quartic points on the modular curve $X_0(26)$ arising from the pullback of a quadratic point on the elliptic curve E' with Cremona label `26b1`. The proof of Lemma 17 outlines a sufficient set of conditions under which $X_0(26)(F) = X_0(26)(\mathbb{Q})$ where $F = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ for squarefree $d \neq -1, -3, -11$ or -23. Namely, if:

- $E'(F) = E'(L)$, where $L = \mathbb{Q}(\sqrt{d})$ or $\mathbb{Q}(\sqrt{2d})$;
- there are no rational points on the quadratic twist over $X_0(26)$ over L;
- there are no points on the hyperelliptic curve $y^2 = -32x^6 - 12x^4 + 20x^2 + 13$ defined over L

then $X_0(26)(F) = X_0(26)(\mathbb{Q})$. Moreover the steps outlined above involve the determination of rational or certain quadratic points on curves which is generally less computationally challenging than determining quartic points on a curve.

$p = 17$

Suppose $P \in X_0(34)(K)$. Let $L = \mathbb{Q}(\sqrt{2})$. We prove that one of the following holds.

(a) $P \in X_0(34)(L)$;

(b) $C(L)$ is non-empty, where C is the quadratic twist of $X_0(34)$ over $\mathbb{Q}(\sqrt{3})$.

In case (a) it follows from work of Ozman and Siksek that $P \in X_0(34)(\mathbb{Q})$. In case (b) we show that $C(L)$ is empty using an elementary local argument.

Lemma 19. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Let E be an elliptic curve over K. Then $\bar{\rho}_{E,17}$ is irreducible.

Proof. We prove that $X_0(34)(K) = X_0(34)(\mathbb{Q})$. We work with the model

$$X_0(34) : \ x^4 - y^4 + x^3 + 3xy^2 - 2x^2 + x + 1 = 0 \tag{3.8}$$

given in `Magma`. Making the change of variables $x \mapsto x,\ y \mapsto y^2$ yields the curve

$$C' : \ x^4 - y^2 + x^3 + 3xy - 2x^2 + x + 1 = 0.$$

We checked using `Magma` that there is an isomorphism

$$C' \to E', \qquad (x, y) \mapsto \big(2(x^2 - 2x + y),\ 4x(x^2 - 2x + y)\big) \tag{3.9}$$

where

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

is the elliptic curve with Cremona label `34a1`. This gives the parametrisation

$$\begin{aligned} \pi : X_0(34) &\longrightarrow E' \\ (x, y) &\longmapsto \big(2(x^2 - 2x + y^2),\ 4x(x^2 - 2x + y^2)\big)\,. \end{aligned}$$

Let $L = \mathbb{Q}(\sqrt{2})$. Using `Magma` we found that the Mordell–Weil group of E' over K is given by

$$E'(K) = (0, 1) \cdot \mathbb{Z}/6\mathbb{Z} \oplus (\sqrt{2}, -1) \cdot \mathbb{Z}.$$

It immediately follows that $E'(K) = E'(L)$. Suppose $P = (a, b) \in X_0(34)(K)$. Since

$$2(a^2 - 2a + b^2), \qquad 4a(a^2 - 2a + b^2) \in L,$$

it follows that either $a^2 - 2a + b^2 = 0$ or $a \in L$. Suppose $b^2 = 2a - a^2$. We substitute this into (3.8) to find that $2a^3 + a + 1 = 0$. Thus $a \notin K$. Thus, $a \in L$ and hence $b^2 \in L$. Either $b \in L$ or $b = \sqrt{3}\beta$ for some $\beta \in L$.

If $b \in L$ then $P \in X_0(34)(L)$. Ozman and Siksek [OS19] have determined all quadratic points on $X_0(34)$, and found that there are no real quadratic points on $X_0(34)$. Thus $P \in X_0(34)(\mathbb{Q})$ in this case.

Suppose $b = \sqrt{3}\beta$ for some $\beta \in L$. Thus, (a, β) is an L-rational point on the curve

$$C : \ x^4 - 9y^4 + x^3 + 9xy^2 - 2x^2 + x + 1 = 0.$$

Note that 3 is inert in L. We checked using `Magma` that there there are no points on C defined over the completion of L at $3\mathcal{O}_L$. Thus $C(L)$ is empty. □

Remark 20. The proof of Lemma 19 outlines a sufficient set of conditions under which $X_0(34)(F) = X_0(34)(\mathbb{Q})$ where $F = \mathbb{Q}(\sqrt{2}, \sqrt{d})$. Namely, if:

- $E'(F) = E'(L)$, where $L = \mathbb{Q}(\sqrt{2})$;
- there are no L-rational points on the curve

$$x^4 - d^2y^4 + x^3 + 3dxy^2 - 2x^2 + x + 1 = 0$$

then $X_0(34)(F) = X_0(34)(\mathbb{Q})$.

$p \geq 19$

We let $E = E_{a,b,c,\varepsilon}$ where $\varepsilon \in \mathcal{O}_K^*$ is chosen so that one of the two possibilities in Lemma 13 holds. Suppose $\overline{\rho}_{E,p}$ is reducible. Then

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

where θ, θ' are characters $G_K \to \mathbb{F}_p^*$. Recall that $\chi_p = \det(\overline{\rho}_{E,p}) = \theta\theta'$ where χ_p denotes the mod p cyclotomic character (see Theorem 3). We let $\mathcal{N}_\theta$ and $\mathcal{N}_{\theta'}$ denote the conductors of θ and θ', respectively. We shall require the following result of Freitas and Siksek [FS15b, Lemma 6.3].

Lemma 21 (Freitas and Siksek)**.** Let E be an elliptic curve defined over a number field K with conductor $\mathcal{N}$. Let $p \geq 5$ be a prime, and let $\mathfrak{q} \nmid p$ be a prime of K. Suppose $\bar{\rho}_{E,p}$ is reducible. Let θ and θ' be defined as above. Then

$$\mathrm{ord}_{\mathfrak{q}}(\mathcal{N}_\theta) = \mathrm{ord}_{\mathfrak{q}}(\mathcal{N}_{\theta'}) = \begin{cases} 0 & \text{if } E \text{ has good or multiplicative reduction at } \mathfrak{q}; \\ \dfrac{\mathrm{ord}_{\mathfrak{q}}(\mathcal{N})}{2} \in \mathbb{Z} & \text{if } E \text{ has additive reduction at } \mathfrak{q}. \end{cases}$$

Lemma 22. Let $p \geq 19$ be a prime. Let E be the Frey curve as in (3.1). Then $\overline{\rho}_{E,p}$ is irreducible.

Proof. Suppose $\bar{\rho}_{E,p}$ is reducible. The only primes that ramify in K are 2 and 3, and thus p is unramified in K. Recall that E has good or multiplicative reduction at $\mathfrak{p} \mid p$ by Section 3.1, and E has additive or multiplicative reduction at $\mathfrak{P}$ by Lemma 13. Thus a result of Kraus [Kra96, Lemma 1] asserts that both characters θ, θ' are unramified away from $\mathfrak{P}$ and the primes above p, and moreover, for any $\mathfrak{p} \mid p$, precisely one of the characters θ, θ' is ramified at $\mathfrak{p}$.

We first suppose that either of θ, θ' is unramified at all $\mathfrak{p} \mid p$ (and thus the other is ramified at all $\mathfrak{p} \mid p$). We note that replacing E by a p-isogenous elliptic curve, if necessary, allows us to swap θ and θ' – this is true for elliptic curves in general. Thus we may suppose that θ is unramified at all the primes above p and hence θ is unramified away from $\mathfrak{P}$.

We shall use Lemma 21 to determine $\mathcal{N}_\theta$. Suppose we are in case (i) of Lemma 13, and E has multiplicative reduction at $\mathfrak{P}$. Then by Lemma 21, we have $\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}_{\theta'}) = \mathrm{ord}_{\mathfrak{P}}(\mathcal{N}_\theta) = 0$. Suppose now that we are in case (ii) of Lemma 13, and E has additive reduction at $\mathfrak{P}$. Then by Lemma 21, we have

$$\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}_\theta) = \mathrm{ord}_{\mathfrak{p}}(\mathcal{N}_{\theta'}) = \frac{1}{2}\,\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}_\varepsilon) = 2.$$

Hence either $\mathcal{N}_\theta = 1$ or $\mathfrak{P}^2$. Let $\infty_1, \ldots, \infty_4$ denote the four real places of K. Let $\mathfrak{m}_\infty = \infty_1 \cdots \infty_4$ and $\mathfrak{m} = \mathfrak{P}^2 \cdot \mathfrak{m}_\infty$. Let L be the field fixed by the kernel of θ. A result of Kraus [Kra07, Proposition 2] asserts that L is a subfield of the ray class field $K^{\mathfrak{m}_\infty}$ in the first case, and a subfield of the ray class field $K^{\mathfrak{m}}$ in the second case. Using `Magma` we find that $K^{\mathfrak{m}_\infty} = K^{\mathfrak{m}}$ is a quadratic extension of K. Thus $[L : K] \leq 2$ and the order of θ divides 2. If θ is trivial then E has a K-rational point of order p. In the case that θ has order 2, let E' be the quadratic twist of E by θ. Then

$$\overline{\rho}_{E',p} \sim \begin{pmatrix} \theta^2 & * \\ 0 & \theta\theta' \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & \chi_p \end{pmatrix}.$$

Thus E' has a K-rational point of order p. In both cases, we obtain an elliptic curve with a point of order p defined over K. By Theorem 16, we have $p \leq 17$. We obtain a contradiction since $p \geq 19$.

Fix $\mathfrak{p}_0$ to be a prime ideal of $\mathcal{O}_K$ above p. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Then G acts transitively on the primes $\mathfrak{p} \mid p$. Let S be the set of $\tau \in G$ such that θ is ramified at $\tau(\mathfrak{p}_0)$. We know from the above that S is a proper subset of G, i.e., $S \neq \emptyset$ and $S \neq G$. For a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ we write $I_\mathfrak{q}$ for the inertia subgroup of G_K corresponding to $\mathfrak{q}$. Thus $\theta|_{I_\mathfrak{q}} = 1$ for all

$$\mathfrak{q} \notin \{\mathfrak{P}\} \cup \{\tau(\mathfrak{p}_0) : \tau \in S\}.$$

By Lemma 13, E has potentially multiplicative reduction at $\mathfrak{P}$. Thus by the theory of the Tate curve [Dav12, Proposition 1.2] we have $\theta^2|_{I_\mathfrak{P}} = 1$. Let $\phi = \theta^2$. Then $\phi|_{I_\mathfrak{q}} = 1$ for all

$$\mathfrak{q} \notin \{\tau(\mathfrak{p}_0) : \tau \in S\}.$$

Recall that θ' is unramified at $\mathfrak{q} \in \{\tau(\mathfrak{p}_0) : \tau \in S\}$. Since $\theta\theta' = \chi_p$, we conclude that

$$\phi|_{I_\mathfrak{q}} = \begin{cases} \chi_p^2|_{I_\mathfrak{q}} & \mathfrak{q} \in \{\tau(\mathfrak{p}_0) : \tau \in S\} \\ 1 & \text{otherwise.} \end{cases} \tag{3.10}$$

Let $u \in \mathcal{O}_K^*$. We define the twisted norm of u attached to S to be

$$\mathfrak{N}_S(u) = \prod_{\tau \in S} (\tau(u))^2.$$

We claim that

$$\mathfrak{p}_0 \mid (\mathfrak{N}_S(u) - 1). \tag{3.11}$$

We assume that the claim holds and finish the proof. Let $\mu = \sqrt{2} + \sqrt{3}$, and let

$$u_1 = \mu,\ u_2 = -\sqrt{2} + 1,\ u_3 = (\mu^3 - \mu^2 - 9\mu + 5)/4;$$

this is a basis for $\mathcal{O}_K^*/\{\pm 1\}$. Then, $p \mid B_S$ where

$$B_S = \mathrm{Norm}\left(\sum_{i=1}^{3} (\mathfrak{N}_S(u_i) - 1) \cdot \mathcal{O}_K \right).$$

We used `Magma` to compute B_S for all non-empty proper subsets S of $G = \mathrm{Gal}(K/\mathbb{Q})$. In all cases we found that if $p \mid B_S$ then $p = 2$ or 3. Thus we obtain a contradiction. It remains to prove (3.11). We note the existence of similar claims in the literature; see e.g. [Dav12, Proposition 2.6], [FS15a, Proposition 2.2]. The proof of our claim is an application of a class field theory argument due to Kraus [Kra07, Appendice A]; see also [AS16, Proposition 2.1] for a translated sketch of Kraus' proof. We give some of the details. Let L be the field fixed by the kernel of θ. We can view θ as a homomorphism $\theta : \mathrm{Gal}(L/K) \to \mathbb{F}_p^*$ since $\mathrm{Gal}(L/K) = G_K/\ker(\theta) \cong \mathrm{Im}(\theta) \trianglelefteq \mathbb{F}_p^*$. Denote by M_K the places of K. For $\nu \in M_K$, let $\Theta_\nu : K_\nu^* \to \mathrm{Gal}(L/K)$ be the local Artin map. Then by Artin reciprocity

$$\prod_{\nu \in M_K} \Theta_\nu(u) = 1 \in \mathrm{Gal}(L/K)$$

for any $u \in K^*$. Thus

$$\prod_{\nu \in M_K} \theta(\Theta_\nu(u)) = \bar{1} \in \mathbb{F}_p^*$$

for any $u \in K^*$. Denote by M_K^∞ the infinite places of K and denote by M_K^0 the finite places of K. Fix $u \in \mathcal{O}_K^*$. Since u^2 is positive under all embeddings of K, it follows that $\Theta_\nu(u^2) = 1$ for all $\nu \in M_K^\infty$. Now let $\nu \in M_K^0$. Then by local class field theory $\Theta_\nu(u) \in I_\nu$. First suppose $\nu \in M_K^0 \setminus \{\tau(\mathfrak{p}_0) : \tau \in S\}$. Then by (3.10), $\theta^2|_{I_\nu} = 1$, and in particular $\theta(\Theta_\nu(u^2)) = \theta^2(\Theta_\nu(u)) = \bar{1} \in \mathbb{F}_p^*$. Now suppose $\nu = \mathfrak{p} \in \{\tau(\mathfrak{p}_0) : \tau \in S\}$. Then

$$\begin{aligned}
&\theta(\Theta_\mathfrak{p}(u^2)) \\
&= \theta^2(\Theta_\mathfrak{p}(u)) \\
&= \chi_p^2(\Theta_\mathfrak{p}(u)) && \text{by (3.10)} \\
&= \chi_p(\Theta_\mathfrak{p}(u^2)) \\
&= \mathrm{Norm}_{\mathbb{F}_\mathfrak{p}/\mathbb{F}_p}(u^2 \mod \mathfrak{p})^{-1} && \text{by [Kra07, Proposition 1, Appendice A].}
\end{aligned}$$

On the other hand, from above we see that

$$\prod_{\mathfrak{p} \in \{\tau(\mathfrak{p}_0) \,:\, \tau \in S\}} \theta(\Theta_\mathfrak{p}(u^2)) = \bar{1} \in \mathbb{F}_p^*.$$

This completes the proof. □

Let

$$\mathcal{N}_0 = \begin{cases} \mathfrak{P} & \text{if we are in case (i) of Lemma 13;} \\ \mathfrak{P}^4 & \text{if we are in case (ii) of Lemma 13;} \\ \mathfrak{P}^5 & \text{if } p = 13 \text{ and } \operatorname{ord}_{\mathfrak{P}}(b) = 1. \end{cases}$$

Applying level lowering (i.e. Theorem 5) we obtain

$$\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\mathfrak{p}}$$

where $\mathfrak{f}$ is a Hilbert newform of parallel weight 2 and level $\mathcal{N}_0$, and $\mathfrak{p}$ is some prime above p in $\mathbb{Q}_{\mathfrak{f}}$, the Hecke eigenvalue field of $\mathfrak{f}$. Using `Magma` we find that there are no newforms with parallel weight 2 and level $\mathfrak{P}$ or level $\mathfrak{P}^5$, obtaining a contradiction in these cases.

We thus suppose we are in case (ii) of Lemma 13. For the level $\mathfrak{P}^4$ we find that there are two newforms $\mathfrak{f}_1$, $\mathfrak{f}_2$ and for both the corresponding Hecke eigenvalue field is $\mathbb{Q}$. Let E_1/K, E_2/K be the following elliptic curves:

$$E_1 : y^2 + (\mu+1)xy = x^3 + \frac{1}{4}(-\mu^3 - \mu^2 - 3\mu + 5)x^2 + \frac{1}{2}(-\mu^3 - 5\mu)x + \frac{1}{4}(\mu^3 + 7\mu^2 - 9\mu - 3)$$

$$E_2 : y^2 + \frac{1}{4}(\mu^3 + \mu^2 + 3\mu + 3)y = x^3 + \frac{1}{2}(-\mu^2 - 1)x^2 + \mu^2 x + \frac{1}{4}(-3\mu^3 - 17\mu^2 - \mu + 1),$$

where $\mu = \sqrt{2} + \sqrt{3}$. These elliptic curves have conductors $\mathfrak{P}^4$ and were found using the `Magma` command `EllipticCurveSearch`. These are non-isogenous as $a_{\mathfrak{q}}(E_1) = 6$ and $a_{\mathfrak{q}}(E_2) = -6$ where $3\mathcal{O}_K = \mathfrak{q}^2$. By the work of Box [Box22], E_1, E_2 are modular and thus correspond to the two Hilbert newforms $\mathfrak{f}_1$, $\mathfrak{f}_2$ of parallel weight 2 and level $\mathfrak{P}^4$. Thus $\overline{\rho}_{E,p} \sim \overline{\rho}_{E_i,p}$ where $i = 1$ or 2. To obtain a contradiction we shall use a standard image of inertia argument (see e.g. [FS15c, Lemma 3.5]).

Let j be the j-invariant of the Frey curve E. By (3.2) we have $\operatorname{ord}_{\mathfrak{P}}(j) < 0$ and $p \nmid \operatorname{ord}_{\mathfrak{P}}(j)$. Thus, $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$ [Sil94, Proposition 6.1, Chapter 5]. However, we find that E_1, E_2 have j-invariants

$$j_1 = 0 \quad \text{and} \quad j_2 = -853632\mu^3 + 7682688\mu + 2417472,$$

respectively. As $\mathrm{ord}_{\mathfrak{P}}(j_i) \geq 0$, we have that E_1, E_2 have potentially good reduction at $\mathfrak{P}$. It follows that $\#\overline{\rho}_{E_i,p}(I_{\mathfrak{P}}) \mid 24$ from the work of Kraus [Kra90, Introduction]. As $\overline{\rho}_{E,p} \sim \overline{\rho}_{E_i,p}$, for $i = 1$ or 2, we obtain $p \mid 24$ giving a contradiction.

Thus we have so far shown that there are no non-trivial solutions to (F_n) over K for all primes $n \geq 5$.

3.7 Divisors on curves

In this subsection, we briefly recall some important facts about divisors on curves that we shall need in Section 3.8 as well as throughout Chapter 4.

Let C be a curve defined over $\mathbb{Q}$. When we speak of divisors on C we in fact mean rational divisors.

Definition 23. Let C be a curve defined over $\mathbb{Q}$. A **divisor** D on C is a finite formal integral linear combination $D = \sum a_i P_i$ of algebraic points P_i that is stable under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

- We say D is **effective** and write $D \geq 0$ if and only if $a_i \geq 0$ for all i.
- An **irreducible divisor** is an effective divisor that cannot be written as the sum of two non-zero effective divisors.
- Suppose there is a degree d point $P \in C(\overline{\mathbb{Q}})$ such that $D = P_1 + P_2 + \cdots + P_d$ where $\{P_1, \ldots, P_d\}$ is the Galois orbit of P. We say that D is **the irreducible divisor corresponding** to P.

For a divisor D on C we denote by $L(D)$ the corresponding **Riemann–Roch space** defined by

$$L(D) \;=\; \{0\} \cup \{f \in \mathbb{Q}(C)^{\times} \;:\; \mathrm{div}(f) + D \geq 0\},$$

and we let $\ell(D) = \dim L(D)$. We make frequent use of the Riemann–Roch theorem which we recall now (see e.g. [Sil09, Section II, Theorem 5.4]).

Theorem 24 (Riemann–Roch)**.** Let C be a curve defined over $\mathbb{Q}$. Let D be a divisor on C. Then

$$\ell(D) - \ell(K_C - D) \;=\; \deg(D) - g + 1;$$

where K_C is any canonical divisor on C, and g is the genus of C.

Recall that $\deg(K_C) = 2g - 2$. Therefore, if $\deg(D) \geq 2g - 1$ then $K_C - D$ has negative degree and cannot be linearly equivalent to an effective divisor. In that case $\ell(K_C - D) = 0$ (see e.g. [Sil09, Corollary 5.5]).

We shall also require Clifford's theorem [Har77, Theorem IV.5.4] on special effective divisors.

Definition 25. Let C be a curve defined over $\mathbb{Q}$. Let D be a divisor on C. We say D is **special** if $\ell(K_C - D) > 0$, and we say $i(D) \coloneqq \ell(K_C - D)$ is the **speciality index** of D.

Theorem 26 (Clifford)**.** Let D be an effective special divisor on a curve C. Then

$$\ell(D) \;\leq\; \frac{\deg(D)}{2} + 1.$$

Moreover, equality occurs if and only if $D = 0$, or D is a canonical divisor, or C is hyperelliptic and D is a multiple of a hyperelliptic divisor.

Recall that a hyperelliptic curve C is equipped with a degree 2 morphism $\pi : C \to \mathbb{P}^1$; a **hyperelliptic divisor** on C is $\pi^*(\alpha)$ for any $\alpha \in \mathbb{P}^1$.

3.8 Small composite exponents

We have thus far shown that there are no solutions to (F_n) over K for prime $n = p \geq 5$. In order to complete the proof of Theorem 7, it remains to rule out solutions to (F_n) for $n = 4, 6, 9$.

Recall that the Fermat cubic is isomorphic to the elliptic curve E_3 with Cremona label `27a1`. A quick search on `Magma` yields that the elliptic curve E_3 has rank 2 over K. We

find that there are points that are defined over K, and not over a quadratic subfield; e.g.

$$\left(\frac{1}{2}(-9\sqrt{2}-3\sqrt{6}+24), \frac{1}{2}(-27\sqrt{2}+54\sqrt{3}-27\sqrt{6}+8)\right) \in E_3(K).$$

$n = 9$

The purpose of this section is to prove the following result. We thank Samir Siksek for useful conversations that lead to the proof of this theorem.

Theorem 27. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. There are no non-trivial solutions to (F_n) over K for $n = 9$.

Write F_9 for the Fermat curve of degree 9. Suppose $P \in F_9(K)$. Let $L = \mathbb{Q}(\sqrt{3})$. We first show that P corresponds to an L-rational point on C, where C is some hyperelliptic curve. We then show that $C(L)$ only consists of the point at infinity, from which it easily follows that P is a trivial point.

We find it convenient to let

$$F_9 \ : \ x^9 + y^9 + z^9 = 0.$$

Lemma 28. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and let $L = \mathbb{Q}(\sqrt{3})$. Let

$$C : \ y^2 = 2(-4x^9 + 1)$$

and denote the point at infinity by ∞. If $F_9(K)$ consists of a non-trivial point then $\{\infty\} \subsetneq C(L)$.

Proof. We recall that $2\mathcal{O}_K = \mathfrak{P}^4$ and that K has class number 1. Suppose $P = (\alpha : \beta : \gamma) \in F_9(K)$ with $\gamma \neq 0$. We may suppose that α, β, $\gamma \in \mathcal{O}_K$ and that they are coprime. We recall that $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$ and

$$F_9(\mathbb{F}_2) = \{(1:1:0), \ (1:0:1), \ (0:1:1)\}.$$

Hence, by permuting α, β, γ appropriately, we may suppose $(\alpha : \beta : \gamma) \equiv (1 : 1 : 0)$ (mod $\mathfrak{P}$). Thus

$$\mathfrak{P} \mid \gamma, \qquad \mathfrak{P} \nmid \alpha\beta. \tag{3.12}$$

Observe the identity

$$\gamma^{18} - (\alpha^9 - \beta^9)^2 \;=\; (\alpha^9 + \beta^9)^2 - (\alpha^9 - \beta^9)^2 \;=\; 4(\alpha\beta)^9.$$

After making the substitutions

$$u = \frac{\alpha\beta}{\gamma^2}, \qquad v = \frac{\alpha^9 - \beta^9}{\gamma^9}, \tag{3.13}$$

we see that $Q_1 = (u, v) \in C_1(K)$ where

$$C_1 \;:\; y^2 = -4x^9 + 1.$$

Let

$$E_1 \;:\; y^2 = 4x^3 + 1.$$

Let π_1 denote the corresponding map i.e.

$$\pi_1 : C_1 \to E_1, \qquad (x, y) \mapsto (-x^3, y).$$

The elliptic curve E_1 has minimal Weierstrass model

$$E_1' \;:\; z^2 + z = x^3$$

which is obtained from E_1 by the substitution $y = 2z+1$. This has Cremona label `27a3`. In particular E_1' has good reduction away from 3. Let $R_1 = \pi_1(Q_1) = (-u^3, v) \in E_1(K)$. Then R_1 corresponds to the point

$$S_1 = (-u^3, (v-1)/2) \in E_1'(K).$$

Let $\sigma : K \to K$ be the automorphism satisfying

$$\sigma(\sqrt{2}) = -\sqrt{2}, \qquad \sigma(\sqrt{3}) = \sqrt{3}.$$

Note that the fixed field of σ is $L = \mathbb{Q}(\sqrt{3})$. Thus $S_1 + S_1^\sigma \in E_1'(L)$. We checked using `Magma` that E_1' has rank 0 over L, and indeed

$$E_1'(L) \;=\; \{\mathcal{O}, (0,0), (0,-1)\} \;\cong\; \mathbb{Z}/3\mathbb{Z}. \tag{3.14}$$

Thus $S_1 + S_1^\sigma$ is one of these three points. However, $\mathrm{ord}_{\mathfrak{P}}(u) < 0$ by (3.12) and (3.13). It follows that

$$S_1 \equiv \mathcal{O} \pmod{\mathfrak{P}}.$$

Hence

$$S_1^\sigma \equiv \mathcal{O}^\sigma = \mathcal{O} \pmod{\mathfrak{P}^\sigma}.$$

However, $\mathfrak{P}$ is a totally ramified prime, so $\mathfrak{P}^\sigma = \mathfrak{P}$. Thus $S_1^\sigma \equiv \mathcal{O} \pmod{\mathfrak{P}}$, and

$$S_1 + S_1^\sigma \equiv \mathcal{O} \pmod{\mathfrak{P}}.$$

By (3.14) and the injectivity of torsion upon reduction modulo primes of good reduction (see e.g. [Sil09, Chapter VII, Proposition 3.1.]) we conclude that

$$S_1 + S_1^\sigma = \mathcal{O}.$$

Hence

$$R_1 + R_1^\sigma = \mathcal{O}.$$

Hence

$$(-u^3)^\sigma = -u^3, \qquad v^\sigma = -v.$$

As the only cube root of 1 in K is 1, we have $u^\sigma = u$ and so $u \in L$. Moreover, $v^2 = -4u^9 + 1 \in L$ and $v^\sigma = -v$, so $v = w/\sqrt{2}$ where $w \in L$. Hence $(u, w) \in C(L)$ where C is the hyperelliptic curve given by

$$C \;:\; y^2 = 2(-4x^9 + 1).$$

□

Lemma 29. Let

$$C \;:\; y^2 = 2(-4x^9 + 1).$$

Let $L = \mathbb{Q}(\sqrt{3})$. Then $C(L) = \{\infty\}$.

By Lemma 28, if $C(L) = \{\infty\}$ then $F_9(K)$ only consists of trivial points thus proving Theorem 27. We shall prove Lemma 29 through studying $J(\mathbb{Q})$ where J is the Jacobian of C.

Proof. Let

$$E \ : \ y^2 = x^3 + 2,$$

which is the elliptic curve with Cremona label `1728a1`. Let

$$\pi : C \to E, \qquad (x, y) \mapsto (-2x^3, y), \qquad \infty \mapsto \infty. \tag{3.15}$$

We find using `Magma` that E has zero torsion and rank 1 over $\mathbb{Q}$ and that, in fact, we have

$$E(\mathbb{Q}) = \mathbb{Z} \cdot (-1, 1).$$

We write $\mathrm{Pic}^0(E)$ for the group of rational degree 0 divisor classes on $E/\mathbb{Q}$ and $\mathrm{Pic}^0(C)$ for the group of rational degree 0 divisor classes on $C/\mathbb{Q}$. We recall the standard isomorphism [Sil09, Proposition III.3.4]

$$E(\mathbb{Q}) \cong \mathrm{Pic}^0(E), \qquad P \mapsto [P - \infty], \tag{3.16}$$

where $[D]$ denotes the linear equivalence class of a divisor D. Thus

$$\mathrm{Pic}^0(E) = \mathbb{Z} \cdot \mathcal{Q}, \qquad \mathcal{Q} = [(-1, 1) - \infty].$$

We also recall the standard isomorphism $J(\mathbb{Q}) \cong \mathrm{Pic}^0(C)$, and we will represent elements of the Mordell–Weil group $J(\mathbb{Q})$ as elements of $\mathrm{Pic}^0(C)$. We first compute the torsion subgroup $J(\mathbb{Q})_{\mathrm{tors}}$ of $J(\mathbb{Q})$ using the standard fact that $J(\mathbb{Q})_{\mathrm{tors}}$ injects into $J(\mathbb{F}_p)$ when p is a prime of good reduction (see e.g. [Kat81, Appendix]). Using `Magma` we find that J has good reduction away from 2 and 3 and furthermore

$$J(\mathbb{F}_5) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}, \qquad J(\mathbb{F}_{13}) \cong \mathbb{Z}/19\mathbb{Z} \times \mathbb{Z}/31\mathbb{Z} \times \mathbb{Z}/73\mathbb{Z}.$$

As these two groups have coprime orders we conclude that J has trivial torsion over $\mathbb{Q}$. We now want to determine the rank of J over $\mathbb{Q}$. Using `Magma`, we find that J has

2-Selmer rank 1 over $\mathbb{Q}$, so J has rank at most 1 over $\mathbb{Q}$. The morphism π in (3.15) has degree 3 and induces the homomorphisms

$$\pi_* \ : \ \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(E), \qquad \left[\sum a_i P_i\right] \mapsto \left[\sum a_i \pi(P_i)\right],$$

and

$$\pi^* \ : \ \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(C), \qquad \left[\sum b_j Q_j\right] \mapsto \left[\sum b_j \sum_{P \in \pi^{-1}(Q_j)} e_\pi(P) \cdot P\right]$$

where $e_\pi(P)$ denotes the ramification degree of π at P (see [Sil09, Section II.3]). In particular since $\mathcal{Q} \in \mathrm{Pic}^0(E)$, we have $\pi^*(\mathcal{Q}) \in \mathrm{Pic}^0(C)$. Let

$$\mathcal{P} = \pi^*(\mathcal{Q}) \ = \ [(1/\sqrt[3]{2}, 1) + (\omega/\sqrt[3]{2}, 1) + (\omega^2/\sqrt[3]{2}, 1) - 3\infty] \in \mathrm{Pic}^0(C) \cong J(\mathbb{Q})$$

where ω is a primitive cube root of 1. Since $J(\mathbb{Q})_{\mathrm{tors}}$ is trivial, the point $\mathcal{P}$ has infinite order on $J(\mathbb{Q})$. Thus J has rank exactly 1 over $\mathbb{Q}$. Therefore $J(\mathbb{Q}) = \mathbb{Z} \cdot \mathcal{P}'$, for some $\mathcal{P}' \in J(\mathbb{Q}) = \mathrm{Pic}^0(C)$. Hence

$$\mathcal{P} = k\mathcal{P}'$$

where k is a non-zero integer. Applying π_* to both sides we obtain

$$k\pi_*(\mathcal{P}') = \pi_*(\mathcal{P}) = 3\mathcal{Q}.$$

However, $\pi_*(\mathcal{P}') \in \mathrm{Pic}^0(E) = \mathbb{Z} \cdot \mathcal{Q}$, so

$$\pi_*(\mathcal{P}') = \ell \cdot \mathcal{Q}$$

for some $\ell \in \mathbb{Z}$. Hence $k\ell = 3$, so $k = \pm 1$ or ± 3. We checked using `Magma` that the image of $\mathcal{P}$ under the composition

$$J(\mathbb{Q}) \to J(\mathbb{F}_5) \to J(\mathbb{F}_5)/3J(\mathbb{F}_5)$$

is non-zero. Thus $k \neq \pm 3$, so $k = \pm 1$, hence

$$J(\mathbb{Q}) = \mathrm{Pic}^0(C) = \mathbb{Z} \cdot \mathcal{P}.$$

Suppose $P \in C(L)$. Let $\tau : L \to L$ be the non-trivial automorphism. Then $[P + P^\tau - 2\infty] \in \mathrm{Pic}^0(C)$. Thus

$$[P + P^\tau - 2\infty] \;=\; n \cdot \mathcal{P} \;=\; n \cdot \pi^*(\mathcal{Q}) \;=\; \pi^*(n \cdot \mathcal{Q})$$

for some integer n. We claim that $n = 0$. Suppose otherwise, then $n \cdot \mathcal{Q} \in \mathrm{Pic}^0(E) \setminus \{0\}$ and by the isomorphism in (3.16) we have $n \cdot \mathcal{Q} = [Q - \infty]$ where $Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Write $Q = (a, b) \in E(\mathbb{Q})$ with a, $b \in \mathbb{Q}$. Then

$$[P + P^\tau - 2\infty] \;=\; \pi^*([(a, b) - \infty]) \;=\; [D - 3\infty]$$

where

$$D = P_1 + P_2 + P_3, \qquad P_j \;=\; \left(-\omega^{j-1}\sqrt[3]{a/2}\,,\, b\right), \qquad j = 1, 2, 3.$$

Hence

$$D \;\sim\; D', \qquad D' = P + P^\tau + \infty$$

where $\sim$ denotes linear equivalence on C. Write $|D|$ for the complete linear system of effective divisors of C linearly equivalent to D. Let $r(D) = \dim|D|$. Note that $D' \in |D|$ and $D' \neq D$, therefore $r(D) \geq 1$. By Riemann–Roch (Theorem 24),

$$r(D) - i(D) \;=\; \deg(D) - g = -1,$$

where $i(D) \geq 0$ is the speciality index of D, and $g = 4$ is the genus of C. It follows that $i(D) > 0$, and therefore that D is a special divisor. By Clifford's theorem on special divisors (Theorem 26) we have

$$r(D) \;\leq\; \frac{\deg(D)}{2} = \frac{3}{2}.$$

Hence $r(D) = 1$. Thus the complete linear system $|D|$ is a g^1_3. In particular as C is hyperelliptic, by [Arb+85, page 13], we have $|D| = g^1_2 + p$ where p is a fixed base point of the linear system. In particular, every divisor in $|D|$ is the sum of p and two points interchanged by the hyperelliptic involution. We apply this to D itself. Thus two of the points P_1, P_2, P_3 are interchanged by the hyperelliptic involution. However, they

all have the same y-coordinate b, so $b = 0$. But $(a, b) \in E(\mathbb{Q})$, so $a \in \mathbb{Q}$ and $a^3 = -2$ giving a contradiction. Hence $n = 0$, and so

$$P + P^\tau \sim 2\infty.$$

Thus P, P^τ are interchanged by the hyperelliptic involution. We recall that we want to show that $P = \infty$. Suppose otherwise. Then we can write $P = (c, d)$ where c, $d \in L$ and $c^\tau = c$, $d^\tau = -d$. Thus $c \in \mathbb{Q}$, and $d = e/\sqrt{3}$ with $e \in \mathbb{Q}$. Thus $P' = (c, e) \in C'(\mathbb{Q})$ where

$$C' \ : \ y^2 = 6(-4x^9 + 1).$$

Let J' be the Jacobian of C', and

$$E' \ : \ y^2 = 6(4x^3 + 1).$$

Using `Magma` we find that $E'(\mathbb{Q}) = \mathbb{Z} \cdot (1/2, 3)$. Let $\mathcal{Q}' = [(1/2, 3) - \infty] \in \mathrm{Pic}^0(E')$, so $\mathrm{Pic}^0(E') = \mathbb{Z} \cdot \mathcal{Q}$. Let

$$\pi' : C' \to E', \qquad (x, y) \mapsto (-x^3, y).$$

Using `Magma` we find that J' has trivial torsion and 2-Selmer rank 1, and following the same steps as before show that $J'(\mathbb{Q}) = \mathrm{Pic}^0(C) = \mathbb{Z} \cdot \mathcal{P}'$, where $\mathcal{P}' = (\pi')^*(\mathcal{Q})$. Now $[P' - \infty] = n\mathcal{P}'$ where n is an integer, and must be non-zero as $P' \neq \infty$. Let $(f, g) = n \cdot (1/2, 3) \in E'(\mathbb{Q}) \setminus \{\mathcal{O}\}$. As before, we find that

$$P' + 2\infty \sim P'_1 + P'_2 + P'_3, \qquad P'_j = (-\omega^{j-1} \cdot \sqrt[3]{f}\,, g).$$

Following the same steps as before, it follows that $g = 0$, so $f^3 = -1/4$ contradicting $f \in \mathbb{Q}$. We can thus conclude that if $P \in C(L)$ then $P = \infty$. This completes the proof of Lemma 29 and therefore Theorem 27. □

$n = 6$

We write F_6 for the Fermat curve of degree 6. The curve F_6 is of genus 10 and we avoid working with it directly. We use an identity to work with a genus 2 curve instead.

Theorem 30. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. There are no non-trivial solutions to (F_n) over K for $n = 6$.

Proof. Consider the Fermat curve of degree 6 given by

$$F_6 : x^6 + y^6 = z^6.$$

We will prove that $F_6(K) = \{(0 : -1 : 1), (-1 : 0 : 1), (0 : 1 : 1), (1 : 0 : 1)\}$, i.e., $F_6(K)$ consists only of trivial solutions. Suppose $(\alpha : \beta : \gamma) \in F_6(K)$ is a non-trivial solution. We may suppose that α, β, $\gamma \in \mathcal{O}_K$ and that they are coprime. Similar to the proof of Theorem 27, note that

$$\gamma^{12} - (\alpha^6 - \beta^6)^2 = (\alpha^6 + \beta^6)^2 - (\alpha^6 - \beta^6)^2 = 4(\alpha\beta)^6.$$

Let

$$a = \frac{\alpha\beta}{\gamma^2}, \qquad b = \frac{\alpha^6 - \beta^6}{\gamma^6}.$$

Then $P = (a, b) \in C(K)$ where

$$C : \ y^2 = -4x^6 + 1.$$

Let

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

This is the elliptic curve with Cremona label `432b1`. Let

$$\pi : C \to E, \qquad (x, y) \mapsto \left(\frac{1}{x^2}, \frac{y}{x^3}\right), \qquad (0, \pm 1) \mapsto \infty_E, \qquad \pm\infty_C \mapsto (0, \pm 2i).$$

We checked using `Magma` that E has rank 1 over K (and $\mathbb{Q}$) and that

$$E(K) = E(\mathbb{Q}) \cong \mathbb{Z} \cdot (2, 2).$$

Since $\pi(P) \in E(\mathbb{Q})$, it immediately follows that $a^2 \in \mathbb{Q}$ and hence $b^2 \in \mathbb{Q}$. We remark that a and b are necessarily defined over the same quadratic subfield of K since $b/a \in \mathbb{Q}$. Thus either $a \in \mathbb{Q}$ and hence $b \in \mathbb{Q}$ or

$$a = \frac{a'}{\sqrt{d}}, \qquad b = \frac{b'}{\sqrt{d}}, \qquad \text{for } \ d \in \{2, 3, 6\}, \qquad a', b' \in \mathbb{Q}.$$

If $a, b \in \mathbb{Q}$ then $P \in C(\mathbb{Q})$. The Jacobian of C has rank 1 over $\mathbb{Q}$. Using the Chabauty implementation in `Magma`, we find that $C(\mathbb{Q}) = \{(0,\ \pm 1)\}$. If $a = 0$ then it's clear that $(\alpha : \beta : \gamma)$ is a trivial solution. Thus $(a',\ b'd) \in C_d(\mathbb{Q})$ where

$$C_d :\ y^2 = -4x^6 + d^3.$$

Suppose $d = 3$ or 6. We checked using `Magma` that there are no points on C_d defined over $\mathbb{Q}_2$. Thus $C_3(\mathbb{Q}) = C_6(\mathbb{Q}) = \emptyset$. It remains to determine $C_2(\mathbb{Q})$. We work with the model

$$C_2 :\ y^2 = -x^6 + 2. \tag{3.17}$$

Note that on this model of C_2, we have $(a', b') \in C_2(\mathbb{Q})$. The curve C_2 has genus 2. Using `Magma`, we find that the rank of the Jacobian of C_2 over $\mathbb{Q}$ is 2. We are therefore are unable to determine $C_2(\mathbb{Q})$ using the method of Chabauty. Instead, we used Bruin's elliptic curve Chabauty method [Bru03] to do so as we now demonstrate.

Let $\theta = \sqrt[6]{2}$, and note that θ is a root of the hyperelliptic polynomial for C_2 given in (3.17). Let $L = \mathbb{Q}(\theta)$. Consider the map

$$\varphi : C_2(\mathbb{Q}) \to L^*/(L^*)^2, \qquad (x, y) \to (x - \theta) \cdot (L^*)^2.$$

The method of two-cover descent, due to Bruin and Stoll [BS09], uses sieving information to determine a small finite set containing the image of φ. This is implemented in `Magma`, and applying it we find that

$$\varphi(C_2(\mathbb{Q})) \subseteq \{(1 + \theta) \cdot (L^*)^2,\ (1 - \theta) \cdot (L^*)^2\}.$$

Thus for a rational point $(x, y) \in C_2(\mathbb{Q})$ we have

$$x - \theta \ = \ (1 \pm \theta)\beta^2 \tag{3.18}$$

with $\beta \in L^*$. Now let $F = \mathbb{Q}(\sqrt[3]{2})$, and note that $x^2 - \sqrt[3]{2} = \mathrm{Norm}_{L/F}(x - \theta)$. Observe that

$$\mathrm{Norm}_{L/F}(1 \pm \theta) = (1 - \theta)(1 + \theta) = 1 - \sqrt[3]{2}.$$

Taking norms in (3.18) gives

$$x^2 - \sqrt[3]{2} = (1 - \sqrt[3]{2})w^2, \qquad w = \mathrm{Norm}_{L/F}(\beta) \in F^*.$$

Note the factorisation

$$C_2 : \; y^2 = -x^6 + 2 = -(x^2 - \sqrt[3]{2})(x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2).$$

Thus for $(x, y) \in C_2(\mathbb{Q})$ we have

$$x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2 = \frac{-y^2}{x^2 - \sqrt[3]{2}} = \frac{-1}{(1 - \sqrt[3]{2})} \cdot \frac{y^2}{w^2}.$$

Let $\epsilon = -1/(1-\sqrt[3]{2}) = 1+\sqrt[3]{2}+\sqrt[3]{2}^2 \in F^*$, and $z = y/w \in F^*$. Then, for $(x, y) \in C_2(\mathbb{Q})$ we have

$$x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2 = \epsilon z^2. \tag{3.19}$$

Let

$$X = \epsilon x^2 \;\text{ and } Y = \epsilon^2 xz. \tag{3.20}$$

Then $(X, Y) \in E_2(F)$ where E_2/F is the elliptic curve

$$E_2 : \; Y^2 = X^3 + \epsilon\sqrt[3]{2}X^2 + \epsilon^2\sqrt[3]{2}^2 X.$$

Using `Magma` we found that the Mordell–Weil group is given by

$$E_2(F) \;=\; (\mathbb{Z}/2\mathbb{Z}) \cdot (0, 0) \oplus \mathbb{Z} \cdot \left(1 + \sqrt[3]{2} + \sqrt[3]{2}^2, 5 + 4\sqrt[3]{2} + 3\sqrt[3]{2}^2\right).$$

We are interested in points $(X, Y) \in E_2(F)$ which satisfy (3.20) where $(x, y) \in C_2(\mathbb{Q})$. In particular, to determine $C_2(\mathbb{Q})$, it is enough to find all points $Q = (X, Y) \in E_2(F)$ such that $f(Q) \in \mathbb{Q}$, where $f(X, Y) = X/\epsilon$. Bruin's elliptic curve Chabauty method [Bru03] is one that can sometimes be used to provably determine all F-points Q on an elliptic curve E defined over a number field F, such that $f(Q) \in \mathbb{Q}$ for a given non-constant function $f \in F(E)$, provided that the degree $[F : \mathbb{Q}]$ exceeds the rank of E over F. In our situation, the degree is $[F : \mathbb{Q}] = 3$ and the rank of E over F is 1. We applied the implementation of elliptic curve Chabauty available in `Magma` to our E_2/F and f. This succeeded in showing that the only $(X, Y) \in E_2(F)$ with $X/\epsilon \in \mathbb{Q}$ are

$$(X, Y) = (0, 0), \quad \left(\epsilon,\; 5 + 4\sqrt[3]{2} + 3\sqrt[3]{2}^2\right), \quad \left(\epsilon,\; -5 - 4\sqrt[3]{2} - 3\sqrt[3]{2}^2\right).$$

Thus $X = 0$ or ϵ, and hence if $(x, y) \in C_2(\mathbb{Q})$, then $x = 0$ or ± 1. It immediately follows that

$$C_2(\mathbb{Q}) = \{(\pm 1,\ \pm 1)\}.$$

Thus, $(a',\ b') \in \{(\pm 1,\ \pm 1)\}$ and if $P = (a, b) \in C(K)$ then $P \in \{(\pm\ 1/\sqrt{2},\ \pm\ 1/\sqrt{2})\}$. Recall that

$$b = \frac{\alpha^6 - \beta^6}{\gamma^6},$$

where $(\alpha : \beta : \gamma) \in F_6(K)$. It immediately follows that $(b + 1)/2$ is a square in K. For each $b \in \{\pm 1/\sqrt{2}\}$, we check using `Magma` that $(b+1)/2$ is not a square in K. We have reached a contradiction. This completes the proof. □

$n = 4$

Points on the Fermat quartic over quadratic fields were first studied by Aigner [Aig34]. Somewhat later, Faddeev [Fad60] gave another proof which also classified the points over cubic fields, using quite intricate algebraic geometry, and Mordell [Mor67] then found an elementary proof of the same result.

Mordell starts with the knowledge that there are no non-trivial points on the Fermat quartic over $\mathbb{Q}$, and studies points over all quadratic extensions. We generalise his method, observing that we can also classify points over quadratic extensions of certain quadratic fields. More precisely, if L is any field for which there are no points on the Fermat quartic, and if the two elliptic curves with Cremona labels `32a1` and `64a1` have rank 0 over L, then we give a procedure to write down all the points on the Fermat quartic over quadratic extensions of L.

We note that we require only that the elliptic curves with Cremona labels `32a1` and `64a1` have rank 0 over L. Of course this does not always hold. For example, let $L = \mathbb{Q}(\sqrt{3})$. Then the elliptic curve with Cremona label `64a1` has rank 1 over L (the other has rank 0). Similarly, if $L = \mathbb{Q}(\sqrt{6})$ then the elliptic curve with Cremona label `32a1` has rank 1 over L (and the other has rank 0).

We previously conjectured that there are no points on the Fermat quartic over any real biquadratic field. We thank Pedro José Cazorla Garcia for pointing out to us that the point $(\sqrt{3}, 2, \sqrt{5})$ lies on the Fermat quartic over $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

After the completion of this work, we were made aware that Ishitsuka, Ito and Ohshita [IIO19, Theorem 7.3] have previously determined all points on the Fermat quartic lying in a quadratic extension of $\mathbb{Q}(\zeta_8)$. Since $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_8)$, this is indeed stronger than the statement of Theorem 31.

We note that the authors of the aforementioned work study the Jacobian of the Fermat quartic over $\mathbb{Q}(\zeta_8)$ and that the proof of Theorem 31, extending work of Mordell [Mor67], makes use of a different strategy.

Theorem 31. All points on the Fermat quartic lying in quadratic extensions of $\mathbb{Q}(\sqrt{2})$ are defined over one of the following number fields:

$$\mathbb{Q}(\sqrt{2}, i), \quad \mathbb{Q}(\sqrt{2}, \sqrt{-7}), \quad \mathbb{Q}(\sqrt[4]{2}), \quad \mathbb{Q}(\sqrt[4]{2}i).$$

We remark that the points on the Fermat quartic defined over $\mathbb{Q}(\sqrt{2}, i)$ and $\mathbb{Q}(\sqrt{2}, \sqrt{-7})$ are in fact defined over the quadratic fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-7})$, respectively.

Proof. Let $L = \mathbb{Q}(\sqrt{2})$, and let K be a quadratic extension of L. We shall determine all points on the Fermat quartic

$$F_4 : \ x^4 + y^4 = 1$$

in K. Let $t = \frac{1-x^2}{y^2}$, so that $x^2 + ty^2 = 1$. This gives a parameterisation

$$x^2 = \frac{1-t^2}{1+t^2}, \quad y^2 = \frac{2t}{1+t^2}.$$

Observe that if $x, y \in K$ then $t \in K$.

Case (A). Suppose first that $t \in L$. Then $x^2, y^2 \in L$. In order for x and y to lie in the same quadratic extension K of L, either $x \in L$, $y \in L$ or $x/y \in L$. This means that one of

$$\frac{1-t^2}{1+t^2}, \quad \frac{2t}{1+t^2} \quad \text{or} \quad \frac{2t}{1-t^2}$$

is a square in L. Equivalently, $(1-t^2)(1+t^2)$, $2t(1+t^2)$ or $2t(1-t^2)$ is a square in L. These correspond to L-rational points on one of the curves

$$u^2 = (1-t^2)(1+t^2), \quad u^2 = 2t(1+t^2), \quad u^2 = 2t(1-t^2).$$

Both of the first two possibilities are isomorphic to $E_1 : y^2 = x^3 + 4x$ (the elliptic curve with Cremona label `32a1`) via the maps $(t,u) \mapsto \left(\frac{2t+2}{1-t}, \frac{u}{(1-t)^2}\right)$ and $(t,u) \mapsto (2t, 2u)$ respectively, and the third to $E_2 : y^2 = x^3 - 4x$ (the elliptic curve with Cremona label `64a1`) via $(t,u) \mapsto (-2t, 2u)$. We checked using `Magma` that E_1 and E_2 have rank 0 over L. We find that

$$E_1(L) = E_1(\mathbb{Q}) = \{\mathcal{O}, (0,0), (2, \pm 4)\}$$

These points correspond on the first curve to $t = \pm 1$ and $t = 0$, and on the second to $t = 0$, $t = 1$ and $t = \infty$. These values of t give points

$$(x^2, y^2) = \{(1,0), (-1,0), (0,1), (0,-1)\},$$

corresponding to points on F_4 defined over $\mathbb{Q}$ or $\mathbb{Q}(i)$. Similarly,

$$E_2(L) = \{\mathcal{O}, (-2,0), (0,0), (2,0), (2+2\sqrt{2}, \pm(4+4\sqrt{2}), (2-2\sqrt{2}, \pm(4-4\sqrt{2})\},$$

and the rational points correspond to $t = \pm 1$ and $t = 0$, and the point at infinity to $t = \infty$, as before. The points in $E(L) \setminus E(\mathbb{Q})$ correspond to $t = -1 \pm \sqrt{2}$, and these give

$$(x^2, y^2) \in \{(1/\sqrt{2}, 1/\sqrt{2}),\ (-1/\sqrt{2}, -1/\sqrt{2})\},$$

corresponding to solutions in the quadratic extensions of $\mathbb{Q}(\sqrt{2})$ obtained by adjoining $\sqrt[4]{2}$ or $\sqrt[4]{2}i$. In particular, we recover the solutions

$$1^4 + 1^4 = \sqrt[4]{2}^4, \qquad 1^4 + 1^4 = (i\sqrt[4]{2})^4,$$

and similar points obtained by negating one or more of the terms.

Case (B). We now suppose $t \in K, t \notin L$. We write $F(t) = t^2 + \beta t + \gamma$ for the minimal polynomial of t over L, so $\beta, \gamma \in L$. We let $A = (1+t^2)xy$ and $B = (1+t^2)y$, so that

$$A^2 = 2t(1-t^2), \qquad B^2 = 2t(1+t^2).$$

Since $A^2, B^2 \in K$ and $K = L(t)$, we can write

$$A = \lambda + \mu t, \quad B = \lambda' + \mu' t, \qquad \lambda,\ \mu,\ \lambda',\ \mu' \in L.$$

Comparing the two expressions for A yields

$$(\lambda + \mu t)^2 = 2t(1 - t^2).$$

In particular, the equation

$$(\lambda + \mu z)^2 - 2z(1 - z^2) = 0$$

has a root $z = t$. As the equation is defined over L, the left-hand side is divisible by the minimal polynomial $F(z)$, and, as this is a cubic, we have

$$(\lambda + \mu z)^2 - 2z(1 - z^2) = F(z)(\rho + \sigma z),$$

a factorisation over L (where $\rho,\ \sigma \in L$). From comparing the coefficients of z^3, we see that $\sigma = 2$ i.e.

$$(\lambda + \mu z)^2 - 2z(1 - z^2) = F(z)(\rho + 2z). \tag{M1}$$

Then $z = -\rho/2$ is a solution to the right-hand side of (M1) defined over L. In particular, we have a solution with $z \in L$ to

$$Y^2 = 2z(1 - z^2) = -2z^3 + 2z,$$

where $Y = \lambda + \mu z \in L$. Thus we get an L-point on the elliptic curve $Y^2 = -2X^3 + 2X$, which is isomorphic to the elliptic curve E_2, and the points in $E_2(L)$ correspond to $z = \pm 1$, $z = 0$ and $z = -1 \pm \sqrt{2}$. In exactly the same way, looking at B^2, we will get a solution over L to

$$(\lambda' + \mu' z)^2 - 2z(1 + z^2) = F(z)(\rho' - 2z), \tag{M2}$$

and therefore a solution over L to $Y^2 = 2z(1 + z^2)$, which is isomorphic to E_1. The points in $E_1(L)$ correspond to $z = 0$ and $z = 1$.

We will now consider all these cases, as in Mordell. We write (z_1, z_2) for the situation where the equation (M1) is solved by z_1 and equation (M2) is solved by z_2. We resultingly obtain two expressions for $F(z)$ (or $G(z) \cdot F(z)$, where $G(z)$ is a specified linear expression in z defined over L). Comparing these two expressions will then either lead to a contradiction or to a value of t such that $F(t) = 0$. In the first case, the pair (z_1, z_2) doesn't correspond to a point on the Fermat quartic over K. In the second case, we are lead to the point $(x, y) \in F_4(K)$ corresponding to the value of t for which $F(t) = 0$. Although these calculations are elementary, we include all the details for completeness.

1. $(0, 0)$

This is exactly the same as Mordell's case (I). If $z_1 = 0$, then $\lambda^2 = 0$, so $\lambda = 0$, and similarly $z_2 = 0$ gives $\lambda' = 0$. Moreover $z_1 = -\rho/2 = 0$ and $z_2 = \rho'/2 = 0$ imply that $\rho = \rho' = 0$. Now from equation (M1) we see that

$$F(z) = \frac{\mu^2 z - 2(1 - z^2)}{2}$$

and from equation (M2) we see that

$$F(z) = -\frac{\mu'^2 z - 2(1 + z^2)}{2}.$$

Comparing the constant term of both expressions for $F(z)$ then leads to a contradiction.

2. $(-1, 1)$

This is Mordell's case (VI). If $z_1 = -1$ is a root of the left-hand side of (M1) then $\lambda = \mu$. Similarly, if $z_2 = 1$ is a root of the left-hand side of (M2) then $\lambda' + \mu' = \pm 2$. Moreover since $z_1 = -\rho/2 = -1$, we have $\rho = 2$. Then from equation (M1) we see that

$$F(z) = \frac{\lambda^2(1 + z) - 2z(1 - z)}{2}.$$

From $z_2 = \rho'/2 = 1$, we see that $\rho' = 2$. We rewrite equation (M2) as

$$2(1 - z)F(z) = (\lambda' + \mu' z)^2 - 2z(1 + z^2).$$

Recall that $Y = \lambda' + \mu'$ is the y-coordinate of an L-point on the elliptic curve E_1. In particular, this implies that we are free to choose the sign of $\lambda' + \mu'$, and we choose $\lambda' + \mu' = 2$. After making this substitution and dividing through by $2(1 - z)$ we see that equation (M2) gives

$$F(z) = \frac{2z^2 + (2 - \mu'^2)z + (2 - \mu')^2}{2}.$$

From comparing the constant term of both expressions for $F(z)$ we see that $\lambda^2 = (2 - \mu')^2$, and from comparing the coefficient of z in both expressions for $F(z)$ we see that $\lambda^2 - 2 = 2 - \mu'^2$. All solutions to this system of equations are given by $(\lambda, \mu') = (0, 2)$ and $(\lambda, \mu') = (\pm 2, 0)$. Suppose $(\lambda, \mu') = (0, 2)$. In this case $F(z) = -z(1 - z)$. This is a contradiction since $F(t) = 0$ and $t \notin L$. Suppose now that $(\lambda, \mu') = (\pm 2, 0)$. Then it is straightforward to see that $F(z) = z^2 + z + 2$. Thus $t = \frac{-1 \pm \sqrt{-7}}{2}$ and $K = L(\sqrt{-7})$. Moreover, these values of t correspond to the point

$$(x, y) = \left(\frac{1 + \sqrt{-7}}{2}, \frac{-1 + \sqrt{-7}}{2} \right)$$

and similar points obtained by negation and conjugation.

3. $(1, 0)$

This is Mordell's case (II). If $z_1 = 1$ then $(\lambda + \mu)^2 = 0$, so $\lambda + \mu = 0$. Furthermore $z_1 = -\rho/2 = 1$ implies that $\rho = -2$. Then from equation (M1) we see that

$$F(z) = \frac{\mu^2(-1 + z) + 2z(1 + z)}{2}$$

and recall from case 1 that equation (M2) implies

$$F(z) = \frac{-\mu'^2 z + 2(1 + z^2)}{2}.$$

Comparing the constant term of both expressions yields $\mu^2 = -2$. This is a contradiction since $\mu \in L$.

4. $(-1, 0)$

This is Mordell's case (III). From case 2, we see that

$$F(z) = \frac{\lambda^2(1+z) - 2z(1-z)}{2},$$

and from case 3, we see that

$$F(z) = \frac{-\mu'^2 z + 2(1+z^2)}{2}.$$

Comparing the constant term of both expressions yields $\lambda^2 = 2$. Then from comparing the coefficient of z in both expressions, we see that $\mu' = 0$. Recall that $\lambda' = 0$ from case 3. Then $Y = \lambda' + \mu' t = 0$. Recall that $Y^2 = 2t(1+t^2)$. Thus $t = 0$. This contradicts the assumption that $t \notin L$.

5. $(-1+\sqrt{2}, 0)$

From $z_1 = -\rho/2 = -1+\sqrt{2}$, we see that $\rho = 2 - 2\sqrt{2}$. Thus we can write equation (M1) as

$$F(z)(2 - 2\sqrt{2} + 2z) = (\lambda + \mu z)^2 - 2z(1-z^2).$$

Recall from case 1 that

$$F(z) = \frac{-\mu'^2 z + 2(1+z^2)}{2}$$

which yields

$$F(z)(2 - 2\sqrt{2} + 2z) = -(1 - \sqrt{2} + z)\mu'^2 + 2(1 - \sqrt{2} + z)(1+z^2).$$

after multiplying by $2-2\sqrt{2}+2z$. From comparing the constant term of both expressions for $F(z)(2 - 2\sqrt{2} + 2z)$, we see that $\lambda^2 = 2(1-\sqrt{2}) < 0$. This is a contradiction since $\lambda \in L$.

6. $(-1-\sqrt{2},0)$

From $z_1 = -\rho/2 = -1-\sqrt{2}$, we see that $\rho = 2+2\sqrt{2}$. Then we can write equation (M1) as

$$F(z)(2+2\sqrt{2}+2z) = (\lambda+\mu z)^2 - 2z(1-z^2).$$

Recall from case 1 that

$$F(z) = \frac{-\mu'^2 z + 2(1+z^2)}{2}$$

from which we see that

$$F(z)(2+2\sqrt{2}+2z) = -(1+\sqrt{2}+z)\mu'^2 z + 2(1+\sqrt{2}+z)(1+z^2)$$

after multiplying by $2+2\sqrt{2}+2z$. By comparing the constant term of both expressions for $F(z)(2+2\sqrt{2}+2z)$, we see that $\lambda^2 = 2(1+\sqrt{2})$. This is a contradiction since $\lambda \in L$.

7. $(0,1)$

This is Mordell's case (IV). Recall that equation (M1) yields the expression

$$F(z) = \frac{\mu^2 z - 2(1-z^2)}{2}$$

from case 1. We recall from case 2 that equation (M2) yields

$$F(z) = \frac{2z^2 + (2-\mu'^2)z + (2-\mu')^2}{2}$$

Comparing the constant term in both expressions for $F(z)$ implies that $(\mu'-2)^2 = -2$. This gives a contradiction since $\mu' \in L$.

8. $(1,1)$

This is Mordell's case (V). Recall from case 3 that in this case equation (M1) becomes

$$F(z) = \frac{\mu^2(-1+z) + 2z(1+z)}{2},$$

and recall that

$$F(z) = \frac{2z^2 + (2-\mu'^2)z + (2-\mu')^2}{2}$$

from case 2. From comparing the constant term in each expression for $F(z)$, we see that $-\mu^2 = (2-\mu')^2$. Thus $\mu' = 2$ and $\mu = 0$ since -1 is not a square in L. If $\mu = 0$ then $F(z) = z(1+z)$. This is a contradiction since $F(t) = 0$ and $t \notin L$.

9. $(-1+\sqrt{2}, 1)$

Recall from case 2 that that equation (M1) yields the expression

$$F(z)(2 - 2\sqrt{2} + 2z) = (\lambda + \mu z)^2 - 2z(1-z^2).$$

From case 5 we see that equation (M2) implies that

$$F(z)(2 - 2\sqrt{2} + 2z) = (2z^2 + (2-\mu'^2)z + (2-\mu')^2)(1 - \sqrt{2} + z)$$

Comparing the constant terms for both expression for $F(z)(2-2\sqrt{2}+2z)$ yields $\lambda^2 = (1-\sqrt{2})(2-\mu')^2$. This implies $\mu' = 2$ as otherwise $\lambda^2 < 0$. If $\mu' = 2$ then $F(z) = z^2 - z$. This is a contradiction since $F(t) = 0$ and $t \notin L$.

10. $(-1-\sqrt{2}, 1)$

From case 6, recall that if $z_1 = -1 - \sqrt{2}$ then

$$F(z)(2 + 2\sqrt{2} + 2z) = (\lambda + \mu z)^2 - 2z(1-z^2).$$

From case 2, we see that equation (M2) implies that

$$F(z)(2 + 2\sqrt{2} + 2z) = (2z^2 + (2-\mu'^2)z + (2-\mu')^2)(1 + \sqrt{2} + z)$$

Comparing the constant terms for both expressions for $F(z)(2+2\sqrt{2}+2z)$ yields $\lambda^2 = (1+\sqrt{2})(2-\mu')^2$. This implies that $\mu' = 2$ since $1+\sqrt{2}$ is not a square in L. If $\mu' = 2$ then $F(z) = z^2 - z$. This leads to a contradiction since $F(t) = 0$ and $t \notin L$.

□

This completes the proof of Theorem 7.

3.9 Some more real biquadratic fields

We give examples of obstacles that arise in generalising the proof of Theorem 7 to some other real biquadratic fields. By Section 3.2, we can assume $p \geq 13$. As in the proof of Theorem 7, we apply level-lowering (Theorem 5) to the Frey curve (3.1) for $p \geq 17$ and $E_{13,\epsilon}$ for $p = 13$.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$

In order to apply level-lowering (Theorem 5), one needs to demonstrate the modularity of the Frey curve over K. It has not yet been proven that elliptic curves over totally real quartic fields containing $\sqrt{5}$ are modular; see [Box22, Section 7.1] for a discussion concerning this problem. We remark however that establishing the modularity of the Frey curve over this particular field K may be possible through the application of [FLHS15, Theorem 7].

$K = \mathbb{Q}(\sqrt{2}, \sqrt{7})$

Write $\mathcal{O}_K$ for the ring of integers of K. A straightforward computation in `Magma` returns that K has class number 1, and $2\mathcal{O}_K = \mathfrak{P}^4$. A straightforward generalisation of Lemmata 13, 14 and 15 returns that the lowered level is $\mathfrak{P}^t$ where $t = 1, 5, 8$ or 16. In particular, the dimension of Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^{16}$ is 40960 making the elimination step currently computationally infeasible in this case.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$

Write $\mathcal{O}_K$ for the ring of integers of K. Using `Magma`, we find that K has class number 1, and $2\mathcal{O}_K = \mathfrak{P}^4$. By a direct generalisation of the techniques outlined in Section 3.5 it is straightforward to see that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$.

A straightforward generalisation of Lemmata 13, 14 and 15 returns that the lowered

level is $\mathfrak{P}^t$ where $t = 1, 4$ or 5. As is true for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, there are no Hilbert newforms of parallel weight 2 and level $\mathfrak{P}$ over K. There are 44 Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^4$ and 76 Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^5$ over K. In order to get a contradiction, we make use of the standard method of eliminating newforms given by the following lemma [FS15b, Lemma 7.1].

Lemma 32 (Freitas and Siksek)**.** Let K be a totally real field, and let $p \geq 5$ be a prime. Let E be an elliptic curve over K of conductor $\mathcal{N}$, and let $\mathfrak{f}$ be a newform of parallel weight 2 and level $\mathcal{N}_p$. Let $\mathfrak{q} \nmid \mathcal{N}_p$ be a prime ideal of $\mathcal{O}_K$ and let

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

If $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$ then ϖ divides the principal ideal

$$B_{\mathfrak{f},\mathfrak{q}} = \mathrm{Norm}(\mathfrak{q})((\mathrm{Norm}(\mathfrak{q}) + 1)^2 - a_\mathfrak{q}(\mathfrak{f})^2) \prod_{a \in \mathcal{A}_\mathfrak{q}} (a - a_\mathfrak{q}(\mathfrak{f})) \cdot \mathcal{O}_{\mathbb{Q}_\mathfrak{f}}.$$

Proof. See [FS15b, pp. 890–891]. □

We briefly explain how to apply Lemma 32. Let

$$B_\mathfrak{f} = \sum_{\mathfrak{q} \in T} B_{\mathfrak{f},\mathfrak{q}},$$

where T is a small set of chosen prime ideals $\mathfrak{q}$ of K such that $\mathfrak{q} \nmid \mathcal{N}_p$. Let $C_\mathfrak{f} = \mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(B_\mathfrak{f})$. Then Lemma 32 asserts that $p \mid C_\mathfrak{f}$. We wrote a short program to implement Lemma 32 in `Magma` with $\mathcal{N}_p = \mathfrak{P}^4$ or $\mathfrak{P}^5$ and T equal to the set of prime ideals $\mathfrak{q} \neq \mathfrak{P}$ of K with norm less than 90. From this implementation we found that if $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$, where E is our Frey curve and $\mathfrak{f}$ is a newform of level $\mathcal{N}_p$ then $p = 2$ or 3 which gives us the desired contradiction.

We remark that the proofs of Theorems 27 and 30 do not readily generalise to K. This leads to the following result.

Theorem 33. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$. There are no non-trivial solutions to (F_n) over K for all primes $n \geq 5$.

CHAPTER 4

Primitive algebraic points on curves

This chapter is based on joint work with Samir Siksek [KS24b] and has been published in the journal 'Research in Number Theory'.

Let C be a curve defined over $\mathbb{Q}$. Throughout this chapter we assume that C has genus ≥ 2. As discussed in the Introduction (Chapter 1), in this chapter, we will prove several sufficient conditions under which C has only finitely many primitive points of a given degree. We begin by recalling the integral notion of a primitive number field.

Definition 34. We say a number field K is **primitive** if

$$\mathbb{Q} \subseteq L \subseteq K \qquad \Rightarrow \qquad L = K \text{ or } L = \mathbb{Q},$$

and **imprimitive** otherwise. In other words, a number field is primitive if it has no proper subextensions. Analogously, we say a point $P \in C(\overline{\mathbb{Q}})$ is **primitive** if the number field $\mathbb{Q}(P)$ is primitive, and **imprimitive** otherwise.

Example 35. Let K be a number field.

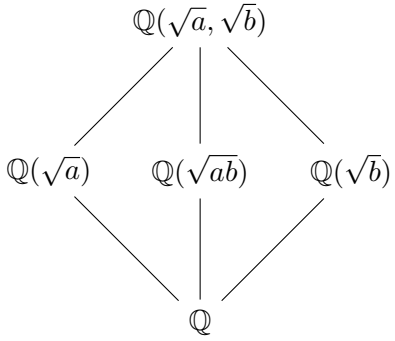


Figure 4.1: The number field $\mathbb{Q}(\sqrt{a},\sqrt{b})$ is imprimitive.

- Suppose $[K:\mathbb{Q}] = \ell$, where ℓ is prime. Then K is primitive. This is an immediate consequence of the Tower Law for field extensions.
- Suppose $[K:\mathbb{Q}] = d$ and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) = A_d$ or S_d, where $\widetilde{K}$ is the Galois closure of K. Then K is primitive (see Section 4.1).
- Let $K = \mathbb{Q}(\sqrt{a},\sqrt{b})$ where a, b are square-free integers. Then K is imprimitive (see Figure 4.1).

4.1 Primitive permutation groups

Let K be a number field, and let $\widetilde{K}$ denote its Galois closure. In this section, we demonstrate that if $[K:\mathbb{Q}] = d$ and $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) = A_d$ or S_d then K is primitive. This result is well-known. We give proofs of some of the intermediate results as we are unable to find convenient references.

Let X be a non-empty set, and let G be a group acting transitively on X.

Definition 36. The **trivial partitions** of X are $\{X\}$ and $\{\{x\} : x \in X\}$. A partition $\mathcal{P}$ of X is said to be **G-stable** if $\sigma(Z) \in \mathcal{P}$ for all $\sigma \in G$ and $Z \in \mathcal{P}$.

Observe, as the action of G on X is transitive, that G also acts transitively on any G-stable partition $\mathcal{P}$, and that any two elements of $\mathcal{P}$ therefore have the same cardinality.

Definition 37. We say that G **acts imprimitively** on X if X admits a G-stable non-trivial partition. If X does not have a G-stable non-trivial partition then we say that G **acts primitively on** X.

The following lemma is an immediate consequence of this definition.

Lemma 38. Let G be a group acting transitively on a set X. Let G' be a subgroup of G and suppose that G' acts primitively on X. Then G acts primitively on X.

Proof. Suppose X has a G-stable non-trivial partition $\mathcal{P}$. Then

$$\sigma(Z) \in \mathcal{P}, \quad \text{for all } \sigma \in G \text{ and } Z \in \mathcal{P}.$$

In particular

$$\sigma(Z) \in \mathcal{P}, \quad \text{for all } \sigma \in G' \text{ and } Z \in \mathcal{P},$$

i.e., X admits a G'-stable non-trivial partition. □

Lemma 39. Let G be a group acting transitively on a set X. The action is imprimitive if and only if there is a proper subset Y of X, with at least two elements, such that

$$\forall \sigma \in G, \qquad \text{if } \sigma(Y) \cap Y \neq \emptyset \text{ then } \sigma(Y) = Y. \tag{4.1}$$

Proof. See e.g. [Mil21, Proposition 4.43]. Suppose G acts imprimitively on X, and let $\mathcal{P}$ be a G-stable non-trivial partition of X. We can take Y to be any element of $\mathcal{P}$. As $\mathcal{P}$ is a partition, Y clearly satisfies (4.1), and as $\mathcal{P}$ is non-trivial, Y is a proper subset of X with at least two elements.

Conversely, suppose Y is a proper subset of X containing at least two elements and satisfying (4.1). We easily check that $\mathcal{P} = \{\tau(Y) : \tau \in G\}$ is a G-stable non-trivial partition. □

Lemma 40. Let G be a finite group acting transitively on a non-empty finite set X. Let $x \in X$, and write $\mathrm{Stab}(x)$ for the stabilizer of x in G. The action of G on X is imprimitive if and only if $\mathrm{Stab}(x)$ is a non-maximal proper subgroup of G.

Proof. This lemma is a straightforward consequence of Lemma 39. See e.g. [Mil21, Theorem 4.45]. Let $x \in X$ and assume the existence of a subgroup $\mathrm{Stab}(x) \subsetneq H \subsetneq G$. Let $Y = \{\tau(x) : \tau \in H\}$. Then, $\#Y = [H : \mathrm{Stab}(x)]$ and so $2 \leq \#Y < [G : \mathrm{Stab}(x)] = \#X$. Moreover, suppose $\sigma \in G$ and $z \in \sigma(Y) \cap Y$. Then there are τ_1, $\tau_2 \in H$ such that $\sigma\tau_2(x) = z = \tau_1(x)$. Thus $\tau_1^{-1}\sigma\tau_2 \in \mathrm{Stab}(x) \subseteq H$. Hence $\sigma \in H$, and so $\sigma(Y) = Y$. Therefore (4.1) is satisfied and so the action is imprimitive.

Conversely, suppose the existence of a proper subset Y of X with at least two elements satisfying (4.1). As the action is transitive, we may in fact suppose that $x \in Y$. Let $H = \{\sigma \in G \ : \ \sigma(Y) = Y\}$. As G is transitive, H is a proper subgroup of G. Moreover, $\mathrm{Stab}(x)$ is contained in H. Let $x' \in Y$, $x' \neq x$. Then there is some $\sigma \in G$ such that $\sigma(x) = x'$. Thus $\sigma(Y) = Y$, and so $\sigma \in H$ but $\sigma \notin \mathrm{Stab}(x)$. It follows that $\mathrm{Stab}(x)$ is a proper subgroup in H, and so is non-maximal as a subgroup of G. □

Lemma 41. Let $K = \mathbb{Q}(\theta)$ be a number field and let $\widetilde{K}$ be its Galois closure. Let $G = \mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. Let $d = [K : \mathbb{Q}]$ and let $\theta_1, \ldots, \theta_d \in \widetilde{K}$ be the Galois conjugates of θ. Then G acts primitively on $\{\theta_1, \ldots, \theta_d\}$ if and only if the extension $K/\mathbb{Q}$ is primitive.

Proof. Let $X = \{\theta_1, \ldots, \theta_d\}$. Then G acts transitively on X. We let $x = \theta \in X$ and note that the stabilizer $\mathrm{Stab}(\theta)$ is in fact $\mathrm{Gal}(\widetilde{K}/K)$. By the Galois correspondence, K is imprimitive if and only if the subgroup $\mathrm{Gal}(\widetilde{K}/K)$ is proper and non-maximal in G, which by Lemma 40 if equivalent to the action of G being imprimitive. □

The following result is well-known. We thank Fred Diamond for the following proof.

Lemma 42. Let C be a curve defined over $\mathbb{Q}$. Let $d \geq 3$ be an integer and let P be a degree d point on C with Galois group S_d or A_d. Then P is primitive.

Proof. It is easy to check the statement for $d = 4$. We henceforth suppose $d = 3$ or $d \geq 5$. Thus A_d is a simple group. Let $K = \mathbb{Q}(P)$. Suppose $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) = A_d$. By Lemma 41, $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$ is a primitive permutation group if and only if K is a primitive number field. We show that K is a primitive number field. Suppose L is a subfield

of K. By the Galois correspondence, $\mathrm{Gal}(\widetilde{K}/\widetilde{L})$ corresponds to a normal subgroup of $\mathrm{Gal}(\widetilde{K}/\mathbb{Q})$. The only normal subgroups of A_d are $\{1\}$ and A_d. Thus either $\widetilde{L} = \mathbb{Q}$ or $\widetilde{L} = \widetilde{K}$. If $\widetilde{L} = \mathbb{Q}$ then $L = \mathbb{Q}$. If $\widetilde{L} = \widetilde{K}$ then $L = K$. Thus K is primitive, as required. The statement for S_d now follows immediately from Lemma 38.

□

4.2 $\mathbb{P}^1$-ISOLATED POINTS

The following definition was first introduced in [Bou+19].

Definition 43. Let C be a curve defined over $\mathbb{Q}$. We say a degree d point $P \in C(\overline{\mathbb{Q}})$ is **$\mathbb{P}^1$-isolated** if P does not lie in the pre-image of a non-constant degree d morphism $C \to \mathbb{P}^1$ defined over $\mathbb{Q}$.

In this section, we prove several sets of sufficient conditions under which all primitive points on C of low degree (with respect to the genus) are $\mathbb{P}^1$-isolated. We make use of the classical Castelnuovo–Severi inequality which we state below.

Theorem 44 (Castelnuovo–Severi inequality)**.** Let k be a perfect field, and let X, Y, Z be curves over k. Denote the genera of these curves by $g(X)$, $g(Y)$ and $g(Z)$ respectively. Let $\pi_Y : X \to Y$ and $\pi_Z : X \to Z$ be non-constant morphisms defined over k, having degrees m and n respectively. Suppose

$$g(X) \;>\; m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1). \tag{4.2}$$

Then there is a curve X' defined over k, and a morphism $X \to X'$ also defined over k and of degree > 1 through which both π_Y and π_Z factor.

Proof. See e.g. [KS24b, p. 6]. □

The following well-known lemma illustrates how Theorem 44 can be used to extract useful information about the arithmetic of a curve. Recall that a curve C over a field

k is **bielliptic** if the genus of C is at least 2 and, furthermore, C admits a degree 2 morphism $C \to E$, defined over k, where E is an elliptic curve defined over k.

Lemma 45. Let C be a hyperelliptic curve of genus g defined over a perfect field k. If $g \geq 4$ then C is not bielliptic.

Proof. Suppose $g \geq 4$. Let

$$\pi : C \to \mathbb{P}^1$$

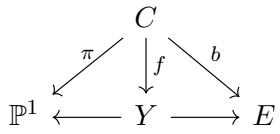
be the (degree 2) hyperelliptic morphism. Suppose C is bielliptic and let

$$b : C \to E$$

denote the corresponding (degree 2) morphism. Suppose π and b don't factor through a non-trivial morphism. Then by the Castelnuovo–Severi inequality (Theorem 44),

$$g \leq 2 \cdot 0 + 2 \cdot 1 + (2-1)(2-1) = 3.$$

Thus there is a non-trivial factorisation as demonstrated in the following commutative diagram.



Observe that $\deg(f) \mid \deg(\pi) = 2$. On the other hand, $\deg(f) > 1$ since the factorisation is non-trivial. Thus $\deg(f) = 2$. It immediately follows that Y is isomorphic to $\mathbb{P}^1$ and Y is isomorphic to E. We have reached a contradiction. Therefore C is not bielliptic. □

Before stating the main results of this subsection, we recall the following definition.

Definition 46. Let C be a curve defined over a field K. The K-gonality of C is the minimum degree of a non-constant morphism from C to $\mathbb{P}^1$ defined over K.

For example, a hyperelliptic curve defined over a field K has K-gonality equal to 2.

Theorem 47. Let C be a curve defined over $\mathbb{Q}$ with genus g and $\mathbb{Q}$-gonality $m \geq 2$. Let $d \geq 2$ be an integer satisfying

$$d \neq m, \qquad d < 1 + \frac{g}{m-1}. \tag{4.3}$$

Let $P \in C(\overline{\mathbb{Q}})$ be a degree d point on C that is not $\mathbb{P}^1$-isolated. Then $\mathbb{Q}(P)$ contains a subfield of index d' satisfying

$$1 < d' < d, \qquad d' \mid \gcd(d, m).$$

In particular, the following hold.

(i) If $\gcd(d, m) = 1$ or d is prime then any degree d point $P \in C(\overline{\mathbb{Q}})$ is $\mathbb{P}^1$-isolated.

(ii) If $P \in C(\overline{\mathbb{Q}})$ is a primitive degree d point then P is $\mathbb{P}^1$-isolated.

Proof. Let $P \in C(\overline{\mathbb{Q}})$ be a degree d point. Suppose P is not $\mathbb{P}^1$-isolated. By definition, P lies in the pre-image of a non-constant degree d morphism $f : C \to \mathbb{P}^1$ defined over $\mathbb{Q}$. Write $f(P) = \alpha$, where $\alpha \in \mathbb{P}^1(\mathbb{Q})$. Recall that m denotes the $\mathbb{Q}$-gonality of C; let $\pi : C \to \mathbb{P}^1$ be the corresponding degree m morphism defined over $\mathbb{Q}$. Since m and d satisfy (4.3), the Castelnuovo–Severi inequality (Theorem 44) asserts that f and π factor through a non-trivial morphism of curves as demonstrated in the following commutative diagram.

$$\begin{array}{ccccc} & & C & & \\ & \swarrow^{f} & \downarrow{\scriptstyle h} & \searrow^{\pi} & \\ \mathbb{P}^1 & \xleftarrow{u} & Y & \xrightarrow{v} & \mathbb{P}^1 \end{array} \tag{4.4}$$

Write $d' = \deg(h) > 1$. Note that $d' \mid d = \deg(f)$ and $d' \mid m = \deg(\pi)$. Thus $d' \mid \gcd(d, m)$. Note that if $\gcd(d, m) = 1$ then $d' = 1$. This contradicts the fact that $d' > 1$. Thus if $\gcd(d, m) = 1$ then P is $\mathbb{P}^1$-isolated. Suppose $d' = d$. Then $d \mid m$. By the minimality of π, we have $m \leq d$. Thus $m = d$; this contradicts the assumption in (4.3). Therefore, $1 < d' < d$. We note it also follows that if d is prime then P is $\mathbb{P}^1$-isolated. Let $Q = h(P) \in Y$. We point out that $f^{-1}(\alpha)$ consists precisely of the Galois orbit of P. Since $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts transitively on $f^{-1}(\alpha)$, it acts transitively on

$u^{-1}(\alpha)$. Hence Q has degree $\deg(u) = d/d'$ and $\mathbb{Q}(Q) \subseteq \mathbb{Q}(P)$. Thus the field $\mathbb{Q}(P)$ of degree d contains the subfield $\mathbb{Q}(Q)$ of index d'. This completes the proof. □

We now prove a variation of this result.

Theorem 48. Let $\pi : C \to C'$ be a morphism of curves defined over $\mathbb{Q}$ of degree $m \geq 2$. Write g and g' for the genera of C and C' respectively, and suppose $g' \geq 1$. Let $d \geq 2$ be an integer satisfying

$$d < 1 + \frac{g - mg'}{m - 1}. \tag{4.5}$$

Let $P \in C(\overline{\mathbb{Q}})$ be a degree d point on C that is not $\mathbb{P}^1$-isolated. Then $\mathbb{Q}(P)$ contains a subfield of index d' satisfying

$$1 < d' < d, \qquad d' \mid \gcd(d, m).$$

In particular, the following hold.

(i) If $\gcd(d, m) = 1$ or d is prime then any degree d point $P \in C(\overline{\mathbb{Q}})$ is $\mathbb{P}^1$-isolated.

(ii) If $P \in C(\overline{\mathbb{Q}})$ is a primitive degree d point, then P is $\mathbb{P}^1$-isolated.

Proof. The proof is almost identical to the proof of Theorem 47; we include some details for completeness. Let $P \in C(\overline{\mathbb{Q}})$ be a degree d point. Suppose P is not $\mathbb{P}^1$-isolated. By definition, P lies in the pre-image of a non-constant degree d morphism $f : C \to \mathbb{P}^1$ defined over $\mathbb{Q}$. Write $f(P) = \alpha$, where $\alpha \in \mathbb{P}^1(\mathbb{Q})$. Recall that $m \geq 2$ is the degree of the cover $\pi : C \to C'$. Since m and d satisfy (4.5), the Castelnuovo–Severi inequality (Theorem 44) asserts that f and π factor through a non-trivial morphism of curves as demonsrated in the following commutative diagram.

$$\begin{array}{ccccc} & & C & & \\ & \swarrow^{f} & \downarrow{\scriptstyle h} & \searrow^{\pi} & \\ \mathbb{P}^1 & \xleftarrow[u]{} & Y & \xrightarrow[v]{} & C' \end{array} \tag{4.6}$$

Write $d' = \deg(h) > 1$. If $\deg(u) = 1$ then $Y \cong \mathbb{P}^1$; we have thus reached a contradiction since we are assuming $g' \geq 1$. Therefore $\deg(u) > 1$ and $1 < d' < d$. The remainder of the proof is now identical to that of Theorem 47. □

4.3 Finite decomposition of $C^{(d)}(\mathbb{Q})$

We denote the d-th symmetric power of C by $C^{(d)}$. Recall that $C^{(d)}(\mathbb{Q})$ can be identified with the set of effective degree d divisors on C. Let D be an effective divisor on C. Recall from the proof of Lemma 29 that $|D|$ denotes the **complete linear series containing** D given by

$$|D| = \{D + \mathrm{div}(f) : f \in L(D)\},$$

where $L(D)$ is as defined in Section 3.7. In other words, $|D|$ is the set of effective divisors linearly equivalent to D. The purpose of this section is to prove the following proposition.

Proposition 49. Let C be a curve over $\mathbb{Q}$ of genus $g \geq 2$, and let J be the Jacobian of C. Let d be a positive integer. Suppose either of the following two conditions hold:

(a) $J(\mathbb{Q})$ is finite;

(b) or $d \leq g - 1$ and J is simple over $\mathbb{Q}$.

Then there are finitely many effective degree d divisors $D_1, D_2, \ldots, D_n$ such that

$$C^{(d)}(\mathbb{Q}) = \bigcup_{i=1}^{n} |D_i|. \tag{4.7}$$

The proposition is a consequence of the following famous theorem due to Faltings [Fal94].

Theorem 50 (Faltings)**.** Let B be an abelian variety defined over a number field K, and let $V \subset B$ be a subvariety defined over K. Then there are a finite number of abelian subvarieties $B_1, \ldots, B_m$ of B, defined over K, and a finite number of points $x_1, \ldots, x_m \in V(K)$ such that the translates $x_i + B_i$ are contained in V, and, moreover, such that

$$V(K) = \bigcup_{i=1}^{m} x_i + B_i(K). \tag{4.8}$$

Proof of Proposition 49. If $C^{(d)}(\mathbb{Q}) = \emptyset$ then there is nothing to prove. Now suppose $C^{(d)}(\mathbb{Q}) \neq \emptyset$ and fix $D_0 \in C^{(d)}(\mathbb{Q})$. Let $W_d(C)$ be the image of $C^{(d)}$ under the Abel–Jacobi map

$$\iota : C^{(d)} \to J, \qquad D \mapsto [D - D_0].$$

We claim that $W_d(C)(\mathbb{Q})$ is finite. This is trivially true if (a) holds, so suppose (b). In particular $d \leq g - 1$ and so $W_d(C)$ is birational to $C^{(d)}$ (e.g. [Mil86, Theorem 5.1]) and so has dimension d. Thus $W_d(C)$ is a proper subvariety of J. Moreover since J is simple over $\mathbb{Q}$, the only abelian subvarieties of J defined over $\mathbb{Q}$ are $\{0\}$ and J. In the notation of Theorem 50 with $B = J$ and $V = W_d(C)$, we have $B_i = \{0\}$ for all i. Thus $W_d(C)(\mathbb{Q})$ is finite by Theorem 50, proving our claim.

Let $W_d(C)(\mathbb{Q}) = \{R_1, \ldots, R_n\}$ and choose $D_1, \ldots, D_n \in C^{(d)}(\mathbb{Q})$ mapping to $R_1, \ldots, R_n$ respectively. If $D \in C^{(d)}(\mathbb{Q})$ then $\iota(D) = R_i$ for some i, and so $[D - D_0] = [D_i - D_0]$. Hence $[D - D_i] = 0$, so $D \in |D_i|$. This completes the proof. □

4.4 Finitely many primitive points of low degree

In this section, we prove several sets of sufficient conditions under which a curve has finitely many primitive points of a fixed degree. Before doing so we give an alternative definition of a point being $\mathbb{P}^1$-isolated.

Let C be a curve defined over $\mathbb{Q}$. We say the **associated degree d divisor** of a degree d point P is the effective degree d divisor obtained by taking the sum of the Galois conjugates of P.

The following lemma is well-known. We give a proof as we are unable to find a reference.

Lemma 51. Let C be a curve defined over $\mathbb{Q}$. Let D be an irreducible degree d divisor on C. The following are equivalent.

(a) $\dim|D| = 0$ i.e. $|D| = \{D\}$.

(b) $\ell(D) = 1$.

(c) If $P \in C(\overline{\mathbb{Q}})$ is in the support of D then P is $\mathbb{P}^1$-isolated.

Proof. (a)$\iff$(b) Recall that $|D| \cong \mathbb{P}^{\ell(D)-1}(\mathbb{Q})$. Note that $\ell(D) \geq 1$ since $\mathbb{Q} \subseteq L(D)$ for any effective divisor D. In particular, $|D| = \{D\}$ if and only if $\ell(D) = 1$.

(c) $\implies$ (b) Suppose $\ell(D) \geq 2$ and let $f \in L(D)$ be such that 1 and f are linearly independent over $\mathbb{Q}$. Write $\mathrm{div}_\infty(f)$ for the divisor of the set of poles of D. Then

$$0 < \mathrm{div}_\infty(f) \leq D.$$

Since D is irreducible, we have $D = \mathrm{div}_\infty(f)$. We can view f as a degree d morphism $f : C \to \mathbb{P}^1$ defined over $\mathbb{Q}$. Then $f(P) = \alpha$ for some $\alpha \in \mathbb{P}^1(\mathbb{Q})$ i.e. P is not $\mathbb{P}^1$-isolated.

(b) $\implies$ (c) Suppose P is not $\mathbb{P}^1$-isolated i.e. P is in the preimage of a non-constant degree d morphism $f : C \to \mathbb{P}^1$ defined over $\mathbb{Q}$. After composing with an automorphism of $\mathbb{P}^1$, we can suppose $f(P) = \infty$. Thus P is in the support of $\mathrm{div}_\infty(f)$. Since D and $\mathrm{div}_\infty(f)$ are Galois stable, we have $D \leq \mathrm{div}_\infty(f)$. Therefore $D = \mathrm{div}_\infty(f)$ since both divisors have degree d. Thus $\ell(D) \geq 2$ since $f \in L(D)$ is non-constant. □

We are now able to state and prove the main results of this chapter.

Theorem 52. Let C be a curve defined over $\mathbb{Q}$ with genus g and $\mathbb{Q}$-gonality $m \geq 2$. Let $d \geq 2$ be an integer satisfying (4.3). Let J be the Jacobian of C. Suppose either of the following hold:

(a) $J(\mathbb{Q})$ is finite;

(b) or $d \leq g - 1$ and J is simple over $\mathbb{Q}$.

Then C has finitely many primitive degree d points. Moreover, if $\gcd(d, m) = 1$ or d is prime then C has finitely many degree d points.

Proof of Theorem 52. By Proposition 49, $C^{(d)}(\mathbb{Q})$ has a finite decomposition as in (4.7), where $D_1, \ldots, D_n$ are effective degree d divisors. Suppose $\ell(D_i) \geq 2$. By Lemma 51, any degree d point in the support of D_i is not $\mathbb{P}^1$-isolated. By Theorem 47, the divisor

D_i is not the Galois orbit of a primitive point. Furthermore, by the aforementioned theorem, if $\gcd(d, m) = 1$ or d is prime then D_i is not the Galois orbit of a degree d point i.e. D_i is reducible. If $\ell(D_i) = 1$ then $|D_i| = \{D_i\}$. This completes the proof since there are only finitely many D_i. □

We point out that by restricting Theorem 52 and its proof to $m = 2$ we obtain the following result for hyperelliptic curves.

Corollary 53. Let C be a hyperelliptic curve defined over $\mathbb{Q}$ with genus g. Let J be the Jacobian of C and let d be a positive integer. Suppose either of the following hold:

(a) $3 \leq d \leq g$ and $J(\mathbb{Q})$ is finite;

(b) or $3 \leq d \leq g - 1$ and J is simple over $\mathbb{Q}$.

Then C has finitely many primitive degree d points. More precisely, the following hold.

(i) If d is odd, then C has finitely many degree d points.

(ii) If d is even, then for all but finitely many degree d points P on C, the field $\mathbb{Q}(P)$ contains a subfield of index 2.

Proof of Corollary 53. Note that the $\mathbb{Q}$-gonality of C is $m = 2$. Suppose either of hypotheses (a), (b) of Corollary 53 is satisfied. Then C, g, m, d satisfy the hypotheses of Theorem 52. In particular, if d is odd then C has finitely many degree d points.

Suppose d is even. By Proposition 49, we have that (4.7) holds where $D_1, \ldots, D_n$ is a finite collection of effective degree d divisors on C. Let P be a degree d point and let D be the corresponding irreducible divisor. Then $D \in |D_i|$ for some i. Suppose $D \neq D_i$. Then $\ell(D) \geq 2$ and so by Lemma 51 the point P is not $\mathbb{P}^1$-isolated. It follows from Theorem 47 that $\mathbb{Q}(P)$ contains a subfield of index $d' = 2$. Thus, for all but finitely many degree d points P we have that $\mathbb{Q}(P)$ contains a subfield of index 2. □

In a similar fashion we can deduce the finiteness of primitive points of a fixed degree upon replacing the gonality map with a covering.

Theorem 54. Let $\pi : C \to C'$ be a morphism of curves defined over $\mathbb{Q}$ of degree $m \geq 2$. Let g, g' for the genera of C, C' respectively, and suppose $g' \geq 1$. Let $d \geq 2$ be an integer satisfying (4.5). Write J for the Jacobian of C and suppose $J(\mathbb{Q})$ is finite. Then C has finitely many primitive degree d points. Moreover, if $\gcd(d, m) = 1$ or d is prime then C has finitely many degree d points.

Proof of Theorem 54. The proof is almost identical to the proof of Theorem 52; we include the details for completeness. By Proposition 49, $C^{(d)}(\mathbb{Q})$ has a finite decomposition as in (4.7), where $D_1, \ldots, D_n$ are effective degree d divisors. Suppose $\ell(D_i) \geq 2$. By Lemma 51, any point in the support of D_i is not $\mathbb{P}^1$-isolated. By Theorem 48, the divisor D_i is not the Galois orbit of a primitive point. Furthermore, by the aforementioned theorem, if $\gcd(d, m) = 1$ or d is prime then D_i is not the Galois orbit of a degree d point i.e. D_i is reducible. If $\ell(D_i) = 1$ then $|D_i| = \{D_i\}$. This completes the proof as there are only finitely many D_i. □

Similarly if we restrict Theorem 54 and its proof to $m = 2$ we obtain the following result for bielliptic curves.

Corollary 55. Let C be a bielliptic curve defined over $\mathbb{Q}$ with genus g. Let J be the Jacobian of C and suppose $J(\mathbb{Q})$ is finite. Let $2 \leq d \leq g-2$. Then C has finitely many primitive degree d points. More precisely, the following hold.

(i) If $d = 2$ or d is odd, then C has finitely many degree d points.

(ii) If $d \geq 4$ and even, then for all but finitely many degree d points P on C, the field $\mathbb{Q}(P)$ contains a subfield of index 2.

Proof of Corollary 55. We have a degree $m = 2$ morphism $C \to E$ defined over $\mathbb{Q}$, where E is an elliptic curve defined over $\mathbb{Q}$. Suppose $J(\mathbb{Q})$ is finite and $2 \leq d \leq g - 2$.

Then C, g, m, d satisfy the assumptions of Theorem 54. In particular if $d = 2$ or d is odd then C has finitely many degree d points.

Suppose $d \geq 4$ and even. By Proposition 49, we have that (4.7) holds where $D_1, \ldots, D_n$ is a finite collection of effective degree d divisors on C. Let P be a degree d point and let D be the corresponding irreducible divisor. Then $D \in |D_i|$ for some i. Suppose $D \neq D_i$. Then $\ell(D) \geq 2$ and so by Lemma 51 the point P is not $\mathbb{P}^1$-isolated. It follows from Theorem 48 that $\mathbb{Q}(P)$ contains a subfield of index $d' = 2$. Thus, for all but finitely many degree d points P we have that $\mathbb{Q}(P)$ contains a subfield of index 2. □

Remark 56. Let C and d satisfy the hypotheses of Theorem 52 or Theorem 54. Then $C^{(d)}(\mathbb{Q})$ can be decomposed into a finite union of complete linear systems as in (4.7). Suppose that we are able to explicitly compute the representatives D_i in (4.7). Then we have an effective strategy for computing all primitive degree d points. Indeed, if $\ell(D_i) \geq 2$ then $|D_i|$ contains no primitive divisors by Theorem 47 or Theorem 48. We are left to consider $|D_i|$ for $\ell(D_i) = 1$. However, if $\ell(D_i) = 1$, then $|D_i| = \{D_i\}$ and we simply need to test D_i to determine if it is the Galois orbit of a primitive degree d point. Moreover, if $\gcd(d, m) = 1$ or d is prime then we can compute all degree d points by a slight modification of the strategy: if $\ell(D_i) = 1$ then simply test D_i for irreducibility.

We remark that the decomposition (4.7) can often be computed using symmetric power Chabauty (e.g. [Sik09] or [BGG23]) provided $r + d \leq g$ where r is the rank of the Mordell–Weil group $J(\mathbb{Q})$.

4.5 A generalisation of Theorems 52 and 54

The following result is a straightforward generalisation of the proofs of Theorems 52 and 54 that was not included in the original article. In particular, we point out that we do not assume that the Jacobian of the curve is simple or that it has finite Mordell–Weil group.

Theorem 57. Let C be a curve defined over $\mathbb{Q}$ with genus g and $\mathbb{Q}$-gonality $m \geq 2$. Let J be the Jacobian of C. Let $d \geq 2$ be an integer satisfying the following assumptions:

(a) $d \leq g - 1$;

(b) $d \neq m$;

(c) $d < 1 + \frac{g}{m-1}$;

(d) $\frac{d}{2} < \dim(\mathcal{A})$ for any proper abelian subvariety $\mathcal{A}$ of J defined over $\mathbb{Q}$.

Then C has finitely many primitive points of degree d. Furthermore, if $\gcd(d, m) = 1$ or d is prime then C has finitely many points of degree d.

Example 58. We consider the modular curve $X_0(239)$ which has genus $g = 20$ and $\mathbb{Q}$-gonality $m = 6$ (see [NO24, Table 3]). A straightforward computation in `Magma` shows that the Jacobian $J_0(239)$ of $X_0(239)$ factors as

$$J_0(239) \sim \mathcal{A}_3 \times \mathcal{A}_{17},$$

where $\mathcal{A}_3$ and $\mathcal{A}_{17}$ are abelian varieties of dimension 3 and 17, respectively. Thus the hypotheses of Theorem 57 are satisfied for $C = X_0(239)$ with $d = 2, 3$ and 4, and we conclude that $X_0(239)$ has finitely many quadratic, cubic and primitive quartic points.

In order to prove Theorem 57 we shall need the following result of Debarre and Fahlaoui [DF93, Corollary 3.6]. Let C be a curve defined over $\mathbb{Q}$. For integers $d, r \geq 0$, let $W_d^r(C)$ be the set of equivalence classes of degree d divisors D on C such that $\ell(D) \geq r + 1$. In particular $W_d^0(C) = W_d(C)$.

Theorem 59 (Debarre and Fahlaoui)**.** Let C be a curve defined over $\mathbb{C}$ with genus $g \geq 1$. Suppose $W_d^r(C)$ contains an abelian variety $\mathcal{A}$, where $d \leq g - 1 + r$. Then $\dim(\mathcal{A}) \leq \frac{d}{2} - r$.

Proof of Theorem 57. We assume the existence of a point $D_0 \in C^{(d)}(\mathbb{Q})$ as there is nothing to prove otherwise. We recall the assumption that $d \leq g - 1$. In particular,

$W_d(C)$ is a proper subvariety of J since $d < g$. We apply the theorem of Debarre and Fahlaoui (Theorem 59) with $r = 0$. We recall the assumption

$$\frac{d}{2} < \dim(\mathcal{A}),$$

for any proper abelian subvariety $\mathcal{A}$ of J. It then immediately follows from Theorem 59 with $r = 0$ that $W_d(C)$ does not contain a proper abelian subvariety of J. Thus by Faltings' Theorem on abelian subvarieties (Theorem 50), $W_d(C)(\mathbb{Q})$ is finite. As in the proof of Proposition 49, it then follows that we have a finite decomposition

$$C^{(d)}(\mathbb{Q}) = \bigcup_{i=1}^{n} |D_i|.$$

The theorem now follows immediately from Theorem 47 as in the proof of Theorem 52.

□

4.6 Infinitely many primitive degree d points

The previous sections of this chapter are concerned with finiteness criteria for low degree primitive points. In this section we focus on constructing a hyperelliptic curve with infinitely many primitive points of a fixed degree. We make use of the following theorem [KS24b, Theorem 12]. We give an overview of the strategy and refer the reader to [KS24b, Section 7] for the proof.

Theorem 60. Let C be a curve defined over $\mathbb{Q}$. Let $d \geq g + 1$ where g is the genus of C. Suppose there exists a primitive degree d point on C. Then there are infinitely many primitive degree d points on C.

Proof of Theorem 60. Suppose $P \in C(\overline{\mathbb{Q}})$ is primitive of degree $d \geq g + 1$, and let D be the corresponding irreducible divisor. By Riemann–Roch (Theorem 24),

$$\ell(D) \;\geq\; d - g + 1 \;\geq\; 2.$$

It immediately follows from Lemma 51 and its proof that there is a degree d morphism $f : C \to \mathbb{P}^1$ defined over $\mathbb{Q}$ such that $f^*(\infty) = D$. The theorem now follows

from applying [KS24b, Proposition 23] with $\alpha = \infty \in \mathbb{P}^1(\mathbb{Q})$ in the notation of that proposition. □

Let C be a curve defined over $\mathbb{Q}$, and let $d \geq g+1$ where g is the genus of C. Theorem 60 asserts the existence of infinitely many primitive degree d points on C provided there is at least one. However, the existence of a primitive degree d point is not guaranteed, as illustrated by the following lemma.

Lemma 61. Let $g \geq 2$ be even. Let C be a degree $2g+1$ genus g curve defined over $\mathbb{Q}$

$$C \ : \ Y^2 \ = \ a_{2g+1}X^{2g+1} + a_{2g}X^{2g} + \cdots + a_0.$$

Suppose $J(\mathbb{Q})$ is trivial, where J is the Jacobian of C. Then C has no points of degree $g+1$.

Proof. Write ∞ for the single point at infinity on the given model. Write $D_0 = (g+1)\infty$. Let D be an effective degree $g+1$ divisor. Then $D - D_0 = \mathrm{div}(f)$ for some $f \in L(D_0)$, since $J(\mathbb{Q})$ is trivial. Note that X has a double pole at ∞. Thus $1, X, \ldots, X^{g/2} \in L(D_0)$. By Riemann–Roch (Theorem 24), we have

$$\ell(D_0) - i(D_0) = d - g + 1 = (g+1) - g + 1 = 0,$$

where $i(D_0)$ is the speciality index of D_0. Recall that $\ell(D_0) \geq 1$. Thus $i(D_0) \geq 1$ i.e. D_0 is a special divisor. By Clifford's theorem on special divisors (Theorem 26) we have $\ell(D_0) \leq (g/2) + 3/2$. However, since g is even and $\ell(D_0)$ is an integer, we have $\ell(D_0) \leq (g/2) + 1$. Therefore, $1, X, \ldots, X^{g/2}$ is a $\mathbb{Q}$-basis for $L(D_0)$. Thus, $f = \alpha_0 + \alpha_1 X + \cdots + \alpha_{g/2}X^{g/2}$, for some $\alpha_0, \ldots, \alpha_{g/2} \in \mathbb{Q}$. In particular $f \in L(g\infty)$. Thus

$$D - \infty \ = \ D_0 + \mathrm{div}(f) - \infty \ = \ g\infty + \mathrm{div}(f)$$

is effective. Hence D is reducible. It follows that C has no degree $g+1$ points. □

In a positive direction, we can use Theorem 60 to construct curves with infinitely many primitive points.

Lemma 62. Let $g \geq 2$. Let $d = g + 1$. Then there is a hyperelliptic curve $C/\mathbb{Q}$ of genus g with infinitely many primitive degree d points.

Proof. Let $K = \mathbb{Q}(\theta)$ be any primitive number field of degree d. Let $\theta_1, \ldots, \theta_d$ be the conjugates of θ in a fixed Galois closure $\widetilde{K}$ of K. Choose a rational number α such that $2\alpha \neq \theta_i + \theta_j$ for any pair $1 \leq i,\ j \leq d$. Let $\phi = \theta - \alpha$. The conjugates of ϕ are $\phi_i = \theta_i - \alpha$ with $1 \leq i \leq d$, and satisfy $\phi_i \neq \pm\phi_j$ for any pair i, j. Let $f \in \mathbb{Q}[X]$ be the minimal polynomial of ϕ^2. Since K is primitive, f is irreducible of degree d. Let $h = f(X^2)$. The roots of h are $\pm\phi_1, \ldots, \pm\phi_d$ which are pairwise distinct and hence h is separable of degree $2d = 2g + 2$. Let C be the genus g hyperelliptic curve

$$C\ :\ Y^2\ =\ h(X).$$

Note that this has the primitive degree d point $(\phi, 0)$. Hence by Theorem 60 there are infinitely many primitive degree d points on C. □

4.7 Finiteness of low degree primitive points on some $X_1(N)$

Mazur [Maz77] showed that all rational points on $X_1(p)$ are cuspidal for prime $p \geq 11$. Merel's uniform boundedness theorem [Mer96] asserts that for prime p, and for d satisfying $(3^{d/2} + 1)^2 \leq p$, the only degree d points on $X_1(p)$ are cuspidal. The exact set of primes p such that $X_1(p)$ has degree d non-cuspidal points have been determined by:

- Kamienny [Kam92] for $d = 2$;
- Parent [Par00],[Par03] for $d = 3$;
- Derickx, Kamienny, Stein and Stoll [Der+23] for $4 \leq d \leq 7$;
- the author [Kha24] for $d = 8$.

Less is known about the low degree points on $X_1(N)$ for composite N, though several authors consider the somewhat easier problem of determining the values of N such

$X_1(N)$ has infinitely many degree d points for given small d (see for example [Bou+19] and [DS17] for two different approaches to studying this problem).

In the following example, we illustrate how our results can be applied to modular curves $X_1(N)$ provided the analytic rank of $J_1(N)$ is 0 and we have information about the quotients or gonality of $X_1(N)$.

Example 63. Consider the modular curve $X_1(64)$. The `LMFDB` [LMF24] gives the following information:

(a) $X_1(64)$ has genus 93;

(b) $X_1(64)$ is a degree 2 cover of a genus 37 curve;

(c) $J_1(64)$ has analytic rank 0.

It follows from a theorem of Kato [Kat04, Corollary 14.3] that the Mordell–Weil group $J(\mathbb{Q})$ is finite where $J = J_1(64)$, and so by Theorem 54, $X_1(64)$ has only finitely many degree d points for

$$d = 2 \quad \text{and} \quad 3 \leq d \leq 19 \quad \text{such that } d \text{ is odd},$$

and only finitely many primitive degree d points for

$$4 \leq d \leq 18 \quad \text{such that } d \text{ is even}.$$

We point out that the $\mathbb{Q}$-gonality of $X_1(64)$ appears to be currently unknown; according to the `LMFDB` it belongs to the interval $16 \leq m \leq 32$. Moreover the application of Theorem 52 to $X_1(64)$ and m in the range stated above yields a substantially weaker finiteness statement than the one given by Theorem 54.

The `LMFDB` [LMF24] contains a database of modular curves $X_1(N)$ for $1 \leq N \leq 293$. The analytic rank of these curves has been computed for $1 \leq N \leq 70$. For 61 of these curves the Jacobian $J = J_1(N)$ has analytic rank 0. It follows from a theorem of Kato [Kat04, Corollary 14.3] that the Mordell–Weil group $J(\mathbb{Q})$ is finite. We are able to

apply Theorem 54 to around half of these curves in order to deduce the finiteness of primitive points of certain low degrees. We note that it is common for $X_1(N)$ to cover multiple curves, and in these instances we apply Theorem 54 to the covered curve C' that gives the most generous range for d in inequality (4.5). We record the results in Tables B.1.

4.8 Finiteness of low degree primitive points on some $X_0(N)$

The computational study of quadratic points on modular curves is an active area of research (see e.g. [Ad23], [BN15], [FLHS15], [NV23], [OS19], to name but a few works). Comparatively less is known about points defined over number fields of higher degree. Still, there is reason to be hopeful. Establishing the modularity of all elliptic curves over totally real cubic fields [DNS20], and totally real quartic fields not containing $\sqrt{5}$ [Box22] required the study of cubic, and quartic points on certain modular curves. Banwait and Derickx [BD22] have determined all cubic points on $X_0(N)$ for $N \in \{41, 47, 59, 71\}$. Box, Gajović, and Goodman [BGG23] have determined all cubic points on $X_0(N)$ for $N \in \{53, 57, 61, 65, 67, 73\}$, and all quartic points on $X_0(65)$.

A famous theorem of Ogg [Ogg74] asserts that there are 19 values of N for which which $X_0(N)$ is hyperelliptic. Of these, the only one for $J_0(N)(\mathbb{Q})$ is infinite is $N = 37$. The remaining 18 values are

- genus 2: $N = 22$, 23, 26, 28, 29, 31, 50;
- genus 3: $N = 30$, 33, 35, 39, 40, 41, 48;
- genus 4: $N = 47$;
- genus 5: $N = 46$, 59;
- genus 6: $N = 71$.

For these N, the quadratic points on $X_0(N)$ have been determined by Bruin and Najman [BN15]. It is straightforward to apply Corollary 53 to these curves and derive

conclusions about algebraic points of degree $3 \leq d \leq g$, where g is the genus of $X_0(N)$. We illustrate this in the following example by giving some details of the computation of all primitive degree 6 points on $X_0(71)$.

Example 64. By Corollary 53 we know that there are only finitely many points on $C = X_0(71)$ of degrees 3 and 5, and finitely many primitive points of degrees 4 and 6. We point out that we can in fact go further and compute these finite sets of points, as sketched in Remark 56. We make use of information found in [BN15] concerning the model and the Mordell–Weil group. A model for $X_0(71)$ is given by

$$\begin{aligned} X_0(71) \ : \ Y^2 \ = \ & X^{14} + 4X^{13} - 2X^{12} - 38X^{11} - 77X^{10} - 26X^9 + 111X^8 \\ & + 148X^7 + X^6 - 122X^5 - 70X^4 + 30X^3 + 40X^2 + 4X - 11. \end{aligned}$$

The only rational points are the two rational points at infinity which we denote by ∞_+ and ∞_- (these are in fact the two cusps of $X_0(71)$). Write

$$D_0 = \infty_+ - \infty_-, \qquad D_\infty = \infty_+ + \infty_-.$$

Then,

$$J(\mathbb{Q}) \ = \ (\mathbb{Z}/35\mathbb{Z}) \cdot [D_0],$$

where $J = J_0(71)$ is the Jacobian of C. Let P be a primitive degree 6 point on $X_0(71)$, and let D be the corresponding effective irreducible degree 6 divisor. Hence $[D - 3D_\infty] \in J(\mathbb{Q})$. It follows that

$$D \in |D_a|, \qquad D_a = a \cdot D_0 + 3D_\infty, \qquad -17 \leq a \leq 17.$$

We find that $\ell(D_a)$ is 4 for $a = 0$, is 3 for $a = \pm 1$, is 2 for $a = \pm 2$ and is 1 for all other values of a. If $\ell(D_a) \geq 2$ then, by Theorem 47, we know that $|D_a|$ does not contain primitive divisors. Thus $D \in |D_a|$ for $-17 \leq a \leq -3$ or $3 \leq a \leq 17$ whence $\ell(D_a) = 1$. For each of these values, $L(D_a) = \mathbb{Q} \cdot f_a$ where f_a is a non-zero function on $X_0(71)$. Moreover, if $D \in |D_a|$ then $D = D_a + \mathrm{div}(f_a)$. We obtain 30 potential possibilities for the divisor D. We find that for $a = \pm 3$, the divisor $D_a + \mathrm{div}(f_a)$ is reducible, and for $a = \pm 5$, ± 7, ± 12, the divisor $D_a + \mathrm{div}(f_a)$ is the Galois orbit of an imprimitive point.

The remaining 22 values of a yield the Galois orbit of a primitive degree 6 point. We conclude that there are precisely 22 primitive degree 6 points on $X_0(71)$ up to Galois conjugacy. All computations were performed in `Magma`.

We carried out similar computations for the hyperelliptic $X_0(N)$ with $N \in \{46, 47, 59, 71\}$, and for degrees d in the range $3 \leq d \leq \max(g, 6)$ where g is the genus of $X_0(N)$. The outcome of these computations is summarized in Table 4.1. Here we were helped by the fact that these values of N, the Mordell–Weil group $J_0(N)(\mathbb{Q})$ has been computed by Bruin and Najman [BN15]. Furthermore, models for the curves are readily available in `Magma` [BCP97] via the `Small Modular Curve package`.

In view of Corollary 55, it is natural to also consider bielliptic $X_0(N)$. Bars [Bar99] shows that $X_0(N)$ is bielliptic for precisely 41 values of N. Of these, $J_0(N)$ has analytic rank 0 for 30 of these values:

- genus 2: $N = 22, 26, 28, 50$;
- genus 3: $N = 30, 33, 34, 35, 39, 40, 45, 48, 64$;
- genus 4: $N = 38, 44, 54, 81$;
- genus 5: $N = 42, 51, 55, 56, 63, 72, 75$;
- genus 7: $N = 60, 62, 69$;
- genus 9: $N = 95$;
- genus 11: $N = 94, 119$.

Again, it is straightforward to apply Corollary 55 to these curves. We computed all primitive points of certain low degrees on the genus 7 bielliptic curves $X_0(60)$ and $X_0(62)$. For these two curves the size of the Mordell–Weil group has been computed by Najman and Vukorepa [NV23]. We computed models for these curves and Mordell–Weil generators using a `Magma` package developed by Ozman and Siksek [OS19], Adžaga,

N	g	$J(\mathbb{Q})$	Number of primitive degree d points on $X_0(N)$			
			$d=3$	$d=4$	$d=5$	$d=6$
46	5	$\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/22\mathbb{Z}$	2	4	88	–
47	4	$\mathbb{Z}/23\mathbb{Z}$	2	12	–	–
59	5	$\mathbb{Z}/29\mathbb{Z}$	1	2	16	–
60	7	$\mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/24\mathbb{Z})^3$	0	0	120	–
62	7	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/120\mathbb{Z}$	2	0	0	–
71	6	$\mathbb{Z}/35\mathbb{Z}$	0	0	0	22

Table 4.1: This table gives the conclusions of our computations of primitive points on $X_0(N)$ of certain low degrees d and for the values of N is the first column. Here g is the genus of $X_0(N)$, and $J(\mathbb{Q})$ is in fact the structure of the Mordell–Weil group where $J = J_0(N)$. The table gives the number of primitive degree d points on $X_0(N)$ up to Galois conjugacy. The symbol $-$ indicates that our method is inapplicable for that particular N and d.

Keller, Michaud-Jacobs, Najman, Ozman and Vukorepa [Ad23], and Najman and Vukorepa [NV23]. All computations were performed in `Magma`.

We summarize our results in Table 4.1, and refer the reader to

`https://github.com/MaleehaKhawaja/Primitive`

for the supporting code as well as a description of the points.

We also give a description of all effective degree d divisors D with $\ell(D) = 1$, and refer the reader to Table 4.2 for this summary.

4.9 Primitive points on curves of low genus

Note that Theorems 52 and 54 allow us to deduce the finiteness of primitive points of low degree (with respect to the genus) under certain additional assumptions. As such,

N	$d=3$		$d=4$			$d=5$		$d=6$		
	$n_{3,p}$	$n_{3,r}$	$n_{4,p}$	$n_{4,i}$	$n_{4,r}$	$n_{5,p}$	$n_{5,r}$	$n_{6,p}$	$n_{6,i}$	$n_{6,r}$
46	2	20	4	10	42	88	128	–	–	–
47	2	2	12	2	6	–	–	–	–	–
59	1	2	2	0	4	16	8	–	–	–
60	0	364	0	22	1349	120	4440	–	–	–
62	2	28	0	0	58	0	100	–	–	–
71	0	2	0	0	2	0	2	22	6	2

Table 4.2: For each pair (N, d), the table gives a description of the effective degree d divisors D with $\ell(D) = 1$ on the modular curve $X_0(N)$. We denote by $n_{d,r}$ the number of such divisors that are reducible, $n_{d,p}$ the number of such divisors that are irreducible and primitive, and $n_{d,i}$ the number of such divisors that are irreducible but imprimitive. The symbol $-$ indicates that we did not carry out the computation for the pair (N, d).

using these theorems, we are unable to make any conclusions about primitive points of any degree on genus 2 curves. We are, however, able to obtain the following result.

Theorem 65. Let C be a hyperelliptic curve defined over $\mathbb{Q}$ with genus 2 or 3. Let J be the Jacobian of C and suppose that $J(\mathbb{Q})$ is trivial. Then there are no primitive quartic points on C. However, there are infinitely many imprimitive quartic points on C.

Example 66. Consider the genus 2 modular curve

$$X_0(26): \ y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1.$$

Bruin and Najman [BN15, Table 3] have determined that $J_0(26)(\mathbb{Q}) \cong \mathbb{Z}/21\mathbb{Z}$, where $J_0(26)$ is the Jacobian of $X_0(26)$. Let C be the quadratic twist of $X_0(26)$ over $\mathbb{Q}(\sqrt{5})$ given by

$$C: \ y^2 = 5x^6 - 40x^5 + 40x^4 - 90x^3 + 40x^2 - 40x + 5.$$

A straightforward computation in `Magma` returns that C admits a degree 2 map to the elliptic curve with Cremona label `650f1`, as well the elliptic curve with Cremona label

`650h2`. Thus C has multiple sources of infinitely many quartic points. A straightforward computation in `Magma` returns that $J(\mathbb{Q})$ is trivial, where J is the Jacobian of C. Applying Theorem 65 we conclude that C has no primitive quartic points, and infinitely many imprimitive quartic points.

Before diving into the proof of Theorem 65, we prove the following preliminary result.

Lemma 67. Let C be a hyperelliptic curve defined over $\mathbb{Q}$. Let $d \geq 4$ be an even integer. Then C has infinitely many imprimitive degree d points.

Proof of Lemma 67. We may suppose C has an affine model

$$C \ : \ Y^2 = F(X) \tag{4.9}$$

where $F \in \mathbb{Q}[X]$ is a squarefree polynomial. Let L be any number field of degree $d/2$ and choose $\theta \in L$ such that $L = \mathbb{Q}(\theta)$. By Faltings' theorem [Fal91], $C(L)$ is finite. Thus there are infinitely many $a \in \mathbb{Q}$ such that $F(\theta + a)$ is a non-square in L. For a fixed value of a, let $P = (\theta + a, \sqrt{F(\theta + a)})$. This is a degree d point on C, and is imprimitive as $\mathbb{Q}(P)$ contains the index 2 subfield L. □

We are now able to prove Theorem 65.

Proof of Theorem 65. Let C be as in the statement of Theorem 65. We may suppose C has an affine model as in (4.9) where $F \in \mathbb{Q}[X]$ is a squarefree polynomial of degree $2g + 1$ or $2g + 2$. By Lemma 67, there are infinitely many imprimitive quartic points on C. It remains to show that there are no primitive quartic points on C.

If $\deg(F) = 2g + 1$ we let ∞ be the single point at infinity on this model, and write $D_0 = 4\infty$. If $\deg(F) = 2g + 2$ we let ∞_+ and ∞_- be the two points at infinity, and write $D_0 = 2\infty_+ + 2\infty_-$. In either case D_0 is twice a hyperelliptic divisor.

Let P be a quartic point on C, and let D be the corresponding irreducible degree 4 divisor. Since $J(\mathbb{Q})$ is trivial, $D - D_0 \sim 0$ where $\sim$ denotes linear equivalence on C.

That is,

$$D = D_0 + \mathrm{div}(f),$$

where $f \in L(D_0)$. We claim that $1, X, X^2$ is a $\mathbb{Q}$-basis of $L(D_0)$. Let us first assume our claim and use it to complete the proof. We have $f = a_0 + a_1X + a_2X^2$ for some $a_0,\ a_1,\ a_2 \in \mathbb{Q}$. Moreover, f is non-constant as $D \neq D_0$. Since P is a zero of f, the X-coordinate $X(P)$ of P satisfies the non-constant polynomial $a_0 + a_1U + a_2U^2 \in \mathbb{Q}[U]$. Since $\mathbb{Q}(P) = \mathbb{Q}(X(P), Y(P))$ is a quartic field, and $Y(P)^2 = F(X(P))$, we see that $\mathbb{Q}(X(P))$ is quadratic and contained in the quartic field $\mathbb{Q}(P)$. Therefore P is imprimitive.

It remains to prove our claim that $1, X, X^2$ is a $\mathbb{Q}$-basis of $L(D_0)$. Note that X has a double pole at infinity and no other poles if $\deg(F) = 2g + 1$; and also X has a simple pole at ∞_+ and ∞_-, and has no other poles if $\deg(F) = 2g + 2$. Therefore, 1, X, X^2 belong to $L(D_0)$, and so $\ell(D_0) \geq 3$. It is enough to show that $\ell(D_0) = 3$. We now make use of our assumption that $g = 2$ or 3. If $g = 2$ then Riemann–Roch (Theorem 24) immediately gives $\ell(D_0) = 3$. Suppose $g = 3$. Then Riemann–Roch tells us that D_0 is special, and then Clifford's theorem (Theorem 26) gives the equality $\ell(D_0) = 3$. □

Appendices

APPENDIX A

Complete Fermat over a cubic field

Kraus [Kra19] rules out the existence of non-trivial solutions to the Fermat equation (F_n) over several number fields K of degree ≤ 8 for prime $n > B_K$, where B_K is a constant depending on K. Thus, as far as we know, Theorem 7 is the first instance of a complete resolution of the Fermat equation over a number field of degree > 2. We make the following observation, which is essentially due to Kraus [Kra19] with the addition of a couple of elementary observations.

Theorem 68. Let $K = \mathbb{Q}(\alpha)$ where $\alpha^3 - \alpha^2 - 3\alpha + 1 = 0$. There are no non-trivial solutions to (F_n) over K for integers $n \geq 3$.

Proof. We first consider $n = 3$ i.e. the Fermat cubic. The Fermat cubic is isomorphic to the elliptic curve E_3 with Cremona label `27a1`. It is straightforward to check using `Magma` that $E_3(K) = E_3(\mathbb{Q})$.

We now show that $F_4(K) = F_4(\mathbb{Q})$, where F_4 is the Fermat quartic. This was observed in [KS24c, Section 29]; we repeat the argument here for the convenience of the reader.

The Fermat quartic F_4 is a cover of the elliptic curve

$$E_4 : \ y^2 = x(x^2 - 4)$$

with Cremona label `64a1`. The cover $\pi : F_4 \to E_4$ is given by

$$\pi : F_4 \to E_4 \quad (x, y, z) \mapsto \left(\frac{z^4}{x^2 y^2}, \frac{z^2(x^4 - y^4)}{x^3 y^3} \right).$$

It is straightforward to check using `Magma` that $E_4(K) = E_4(\mathbb{Q}) = \{0_E, (0,0), (\pm 2, 0)\}$. Note the inclusion

$$\pi(F_4(K)) \subseteq E_4(K) = E_4(\mathbb{Q}),$$

from which it immediately follows that $F_4(K) = F_4(\mathbb{Q})$.

Klassen and Tzermias [KT97] showed that there are no non-trivial cubic points on F_5, and Gross and Rohrlich (Theorem 12) showed that there are no non-trivial cubic points on F_7 and F_{11}. Kraus [Kra19, Theorem 6] proved that there are no non-trivial solutions to (F_n) over K for prime $n = p \geq 13$. We give a brief sketch of Kraus' proof. Let $p \geq 13$ be a prime. Suppose (a, b, c) is a non-trivial solution to the Fermat equation (F_n) over K for $n = p$. Let $E : \ y^2 = x(x - a^p)(x + b^p)$ be the usual Frey curve associated to (a, b, c). Freitas and Siksek [FLHS15, Theorem 7] prove that if an elliptic curve over a totally real field satisfies some local conditions then that elliptic curve is modular. Kraus applies this criterion to show that E/K is modular. The so-called narrow class group of K is trivial. Kraus uses this fact to show that if $\bar{\rho}_{E,p}$ is reducible then either E has a K-rational point of order p or $p \mid D_K R_K$, where D_K is the discriminant of K, and R_K is a computable constant depending only on K. In the first case, Parent's bound [Par00; Par03] immediately asserts that $p \leq 13$, and in the second case Kraus uses ray class groups to assert the existence of an elliptic curve with a K-rational point of order p. To prove that $\bar{\rho}_{E,13}$ is irreducible, Kraus demonstrates that $X_0(52)(K) = X_0(52)(\mathbb{Q})$. The modular curve $X_0(52)$ admits a degree 3 map to the elliptic curve E_{52} with Cremona label `52a1`. It is straightforward to check using `Magma` that $E_{52}(K) = E_{52}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. It immediately follows that $X_0(52)(K) = X_0(52)(\mathbb{Q})$ since $X_0(52)(\mathbb{Q})$ consists of 6 points. Level-lowering (Theorem 5) then asserts the

existence of a Hilbert newform of parallel weight 2 and level $\mathfrak{P}$, where $\mathfrak{P}$ is the unique prime above 2. This yields the desired contradiction since there are no Hilbert newforms of parallel weight 2 and level $\mathfrak{P}$.

□

APPENDIX B

The finiteness of low degree primitive points on certain $X_1(N)$

This table summarises our conclusions upon applying Theorem 54 to $C = X_1(N)$ for the values of N in the first column. Here g denotes the genus of $X_1(N)$; the integer m denotes the degree of the morphism $X_1(N) \to C'$; g' denotes the genus of C'. The sixth column gives the values of d furnished by the theorem for which there are only finitely many points of degree d. The final column gives the values of d (not appearing in the previous column) for which the theorem asserts that there are only finitely primitive degree d points.

N	g	C' (LMFDB label)	g'	m	$X_1(N)$ has finitely many degree d points	$X_1(N)$ has finitely many primitive degree d points
19	7	19.120.1-19.a	1	3	$d = 2$	-
22	6	$X_1(11)$	1	3	$d = 2$	-

24	5	24.192.1-24.dg.2.1	1	2	$2 \leq d \leq 3$	-
26	10	$X_1(13)$	2	3	$d = 2$	-
27	13	27.216.1-27.a.1.1	1	3	$2 \leq d \leq 5$	-
28	10	28.288.4-28.d.1.1	4	2	$d = 2$	-
30	9	$X_1(15)$	1	3	$2 \leq d \leq 3$	-
31	26	31.320.6-31.c.1.2	6	3	$2 \leq d \leq 4$	-
32	17	32.384.5-32.bu.1.1	5	2	$2 \leq d \leq 7$ $d \neq 4, 6$	$d = 4, 6$
34	21	$X_1(17)$	5	3	$2 \leq d \leq 3$	-
36	17	36.288.3-36.c.1.1	3	3	$2 \leq d \leq 4$	-
38	28	$X_1(19)$	7	3	$2 \leq d \leq 4$	-
39	33	39.448.9-39.a.3.1	9	3	$2 \leq d \leq 3$	-
40	25	40.576.9-40.bh.1.1	9	2	$2 \leq d \leq 7$ $d \neq 4, 6$	$d = 4, 6$
42	25	$X_1(21)$	5	3	$2 \leq d \leq 5$	-
44	36	44.720.16-44.e.1.1	16	2	$2 \leq d \leq 3$	$d = 4$
45	41	45.576.9-45.a.4.1	9	3	$2 \leq d \leq 7$ $d \neq 6$	$d = 6$
46	45	$X_1(23)$	12	3	$2 \leq d \leq 5$	-
48	37	48.768.13-48.nt.1.1	13	2	$2 \leq d \leq 11$ $d \neq 4, 6, 8, 10$	$d = 4, 6, 8, 10$
49	69	49.336.3-49.b.1.2	3	7	$2 \leq d \leq 8$	-
50	48	50.360.4-50.a.2.2	4	5	$2 \leq d \leq 7$	-
52	55	52.1008.25-52.p.1.1	25	2	$2 \leq d \leq 5$ $d \neq 4$	$d = 4$
54	52	54.648.10-54.a.1.1	10	3	$2 \leq d \leq 11$ $d \neq 6, 9$	$d = 6, 9$

56	61	56.1152.25-56.bq.1.1	25	2	$2 \leq d \leq 11$ $d \neq 4, 6, 8, 10$	$d = 4, 6, 8, 10$
60	57	60.1152.25-60.eb.2.1	25	2	$2 \leq d \leq 7$ $d \neq 4, 6$	$d = 4, 6$
62	91	$X_1(31)$	26	3	$2 \leq d \leq 7$ $d \neq 6$	$d = 6$
64	93	64.1536.37-64.ef.1.1	37	2	$d = 2$ $3 \leq d \leq 19$, odd d	$4 \leq d \leq 18$ even d
66	81	$X_1(33)$	21	3	$2 \leq d \leq 9$ $d \neq 6, 9$	$d = 6, 9$
68	105	68.1728.49-68.ba.1.1	49	2	$2 \leq d \leq 7$ $d \neq 4, 6$	$d = 4, 6$
70	97	$X_1(35)$	25	3	$2 \leq d \leq 11$ $d \neq 6, 9$	$d = 6, 9$

Table B.1: The table description is given before the table is displayed.

Bibliography

[AH91] Dan Abramovich and Joe Harris. "Abelian varieties and curves in $W_d(C)$". *Compositio Math.* 78.2 (1991), 227–238.

[Ad23] Nikola Adžaga, Timo Keller, Philippe Michaud-Jacobs, Filip Najman, Ekin Ozman, and Borna Vukorepa. "Computing quadratic points on modular curves $X_0(N)$". *Math. Comp* (Oct. 2023).

[Aig57] Alexander Aigner. "Die Unmöglichkeit von $x^6 + y^6 = z^6$ und $x^9 + y^9 = z^9$ in quadratischen Körpern". *Monatsh. Math.* 61 (1957), 147–150.

[Aig34] Alexander Aigner. "Über die Möglichkeit von $x^4+y^4 = z^4$ in quadratischen Körpern." German. *Jahresber. Dtsch. Math.-Ver.* 43 (1934), 226–228.

[AS16] Samuele Anni and Samir Siksek. "Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2\ell}+y^{2m} = z^p$". *Algebra Number Theory* 10.6 (2016), 1147–1172.

[Arb+85] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris. Geometry of algebraic curves. Vol. I. Springer-Verlag, New York, 1985.

[Ban23] Barinder S. Banwait. "Explicit isogenies of prime degree over quadratic fields". *Int. Math. Res. Not. IMRN* 14 (2023), 11829–11876.

[BD22] Barinder S. Banwait and Maarten Derickx. *Explicit isogenies of prime degree over number fields*. 2022. arXiv: 2203.06009 [math.NT].

[Bar99] Francesc Bars. "Bielliptic modular curves". *J. Number Theory* 76.1 (1999), 154–165.

[Bil+24] Nicolas Billerey, Imin Chen, Luis Dieulefait, and Nuno Freitas. *On Darmon's program for the generalized Fermat equation, I*. 2024. arXiv: 2205.15861 [math.NT].

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. "The Magma algebra system. I. The user language". *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), 235–265.

[Bou+19] Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray. "On the level of modular curves that give rise to isolated j-invariants". *Adv. Math.* 357 (2019), 106824, 33.

[Box22] Josha Box. "Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular". *Trans. Amer. Math. Soc.* 375.5 (2022), 3129–3172.

[BGG23] Josha Box, Stevan Gajović, and Pip Goodman. "Cubic and quartic points on modular curves using generalised symmetric Chabauty". *Int. Math. Res. Not. IMRN* 7 (2023), 5604–5659.

[BD14] Christophe Breuil and Fred Diamond. "Formes modulaires de Hilbert modulo p et valeurs d'extensions entre caractères galoisiens". *Ann. Sci. Éc. Norm. Supér. (4)* 47.5 (2014), 905–974.

[Bre+01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. "On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises". *J. Amer. Math. Soc.* 14.4 (2001), 843–939.

[Bru03] Nils Bruin. "Chabauty methods using elliptic curves". *J. Reine Angew. Math.* 562 (2003), 27–49.

[BS09] Nils Bruin and Michael Stoll. "Two-cover descent on hyperelliptic curves". *Math. Comp.* 78.268 (2009), 2347–2370.

[BN15] Peter Bruin and Filip Najman. "Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields". *LMS J. Comput. Math.* 18.1 (2015), 578–602.

[Cop+24] Nirvana Coppola, Mar Curcó-Iranzo, Maleeha Khawaja, Vandita Patel, and Özge Ülkem. "On perfect powers that are sums of cubes of a nine term arithmetic progression". *Indag. Math. (N.S.)* 35.3 (2024), 500–515.

[Dav12] Agnès David. *Caractère d'isogénie et critères d'irréductibilité*. 2012. arXiv: 1103.3892 [math.NT].

[DF93] Olivier Debarre and Rachid Fahlaoui. "Abelian varieties in $W_d^r(C)$ and points of bounded degree on algebraic curves". *Compositio Math.* 88.3 (1993), 235–249.

[DK94] Olivier Debarre and Matthew J. Klassen. "Points of low degree on smooth plane curves". *J. Reine Angew. Math.* 446 (1994), 81–87.

[DV13] Lassina Dembélé and John Voight. "Explicit methods for Hilbert modular forms". In: *Elliptic curves, Hilbert modular forms and Galois deformations*. Adv. Courses Math. CRM Barcelona. Birkhäuser/Springer, Basel, 2013, 135–198.

[DNS20] Maarten Derickx, Filip Najman, and Samir Siksek. "Elliptic curves over totally real cubic fields are modular". *Algebra Number Theory* 14.7 (2020), 1791–1800.

[DS17] Maarten Derickx and Andrew V. Sutherland. "Torsion subgroups of elliptic curves over quintic and sextic number fields". *Proc. Amer. Math. Soc.* 145.10 (2017), 4233–4245.

[Der+23] Maarten Derickx, Sheldon Kamienny, William Stein, and Michael Stoll. "Torsion points on elliptic curves over number fields of small degree". *Algebra Number Theory* 17.2 (2023), 267–308.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms*. Vol. 228. Graduate Texts in Mathematics. Springer-Verlag, New York, 2005, xvi+436.

[Dic66] L. E. Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966, xxv+803.

[Fad60] D. K. Faddeev. "Group of divisor classes on the curve defined by the equation $x^4 + y^4 = 1$". *Soviet Math. Dokl.* 1 (1960), 1149–1151.

[Fal91] Gerd Faltings. "Diophantine approximation on abelian varieties". *Ann. of Math. (2)* 133.3 (1991), 549–576.

[Fal94] Gerd Faltings. "The general case of S. Lang's conjecture". In: *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991)*. Vol. 15. Perspect. Math. Academic Press, San Diego, CA, 1994, 175–182.

[FKS20] Nuno Freitas, Alain Kraus, and Samir Siksek. "Class field theory, Diophantine analysis and the asymptotic Fermat's last theorem". *Adv. Math.* 363 (2020), 106964, 37.

[FLHS15] Nuno Freitas, Bao V. Le Hung, and Samir Siksek. "Elliptic curves over real quadratic fields are modular". *Invent. Math.* 201.1 (2015), 159–206.

[FS15a] Nuno Freitas and Samir Siksek. "Criteria for irreducibility of mod p representations of Frey curves". *J. Théor. Nombres Bordeaux* 27.1 (2015), 67–76.

[FS15b] Nuno Freitas and Samir Siksek. "Fermat's last theorem over some small real quadratic fields". *Algebra Number Theory* 9.4 (2015), 875–895.

[FS15c] Nuno Freitas and Samir Siksek. "The asymptotic Fermat's last theorem for five-sixths of real quadratic fields". *Compos. Math.* 151.8 (2015), 1395–1415.

[Fre86] Gerhard Frey. "A remark about isogenies of elliptic curves over quadratic fields". *Compositio Math.* 58.1 (1986), 133–134.

[Fre94] Gerhard Frey. "Curves with infinitely many points of fixed degree". *Israel J. Math.* 85.1-3 (1994), 79–83.

[Fuj06] K. Fujiwara. Level optimization in the totally real case. 2006. arXiv: math/0602586 [math.NT].

[Gee11] Toby Gee. "Automorphic lifts of prescribed types". *Math. Ann.* 350.1 (2011), 107–144.

[GR78] Benedict H. Gross and David E. Rohrlich. "Some results on the Mordell-Weil group of the Jacobian of the Fermat curve". *Invent. Math.* 44.3 (1978), 201–224.

[HS91] Joe Harris and Joe Silverman. "Bielliptic curves and symmetric products". *Proc. Amer. Math. Soc.* 112.2 (1991), 347–356.

[Har77] R. Hartshorne. Algebraic geometry. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Hel74] Yves Hellegouarch. "Points d'ordre $2p^h$ sur les courbes elliptiques". *Acta Arith.* 26.3 (1974/75), 253–263.

[IIO19] Yasuhiro Ishitsuka, Tetsushi Ito, and Tatsuya Ohshita. "Explicit calculation of the mod 4 Galois representation associated with the Fermat quartic". *Int. J. Number Theory* 16 (2019), 881–905.

[Jar04] Frazer Jarvis. "Correspondences on Shimura curves and Mazur's principle at p". *Pacific J. Math.* 213.2 (2004), 267–280.

[JM08] Frazer Jarvis and Jayanta Manoharmayum. "On the modularity of supersingular elliptic curves over certain totally real number fields". *J. Number Theory* 128.3 (2008), 589–618.

[JM04] Frazer Jarvis and Paul Meekin. "The Fermat equation over $\mathbb{Q}(\sqrt{2})$". *J. Number Theory* 109.1 (2004), 182–196.

[KV22] Borys Kadets and Isabel Vogt. *Subspace configurations and low degree points on curves*. 2022. arXiv: 2208.01067 [math.NT].

[Kal18] Sudesh Kalyanswamy. "Remarks on automorphy of residually dihedral representations". *Math. Res. Lett.* 25.4 (2018), 1285–1304.

[Kam92] Sheldon Kamienny. "Torsion points on elliptic curves and q-coefficients of modular forms". *Invent. Math.* 109.2 (1992), 221–229.

[Kat04] Kazuya Kato. "p-adic Hodge theory and values of zeta functions of modular forms". In: 295. Cohomologies p-adiques et applications arithmétiques. III. 2004, ix, 117–290.

[Kat81] Nicholas M. Katz. "Galois properties of torsion points on abelian varieties". *Invent. Math.* 62.3 (1981), 481–502.

[Ken82] Monsur A. Kenku. "On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class". *J. Number Theory* 15.2 (1982), 199–202.

[Kha24] Maleeha Khawaja. "Torsion primes for elliptic curves over degree 8 number fields". *Res. Number Theory* 10.2 (2024), Paper No. 48, 9.

[KJ23] Maleeha Khawaja and Frazer Jarvis. *Fermat's Last Theorem over* $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. *To appear in Algebra & Number Theory*. 2023. arXiv: 2210.03744 [math.NT].

[KS24a] Maleeha Khawaja and Samir Siksek. *A single source theorem for primitive points on curves*. 2024. arXiv: 2401.03091 [math.NT].

[KS24b] Maleeha Khawaja and Samir Siksek. "Primitive algebraic points on curves". *Res. Number Theory* 10.3 (2024), Paper No. 57, 20.

[KS24c] Maleeha Khawaja and Samir Siksek. *The modular approach to Diophantine equations over totally real fields*. 2024. arXiv: 2401.03099 [math.NT].

[KT97] Matthew Klassen and Pavlos Tzermias. "Algebraic points of low degree on the Fermat quintic". *Acta Arith.* 82.4 (1997), 393–401.

[Kra96] Alain Kraus. "Courbes elliptiques semi-stables et corps quadratiques". *J. Number Theory* 60.2 (1996), 245–253.

[Kra07] Alain Kraus. "Courbes elliptiques semi-stables sur les corps de nombres". *Int. J. Number Theory* 3.4 (2007), 611–633.

[Kra19] Alain Kraus. "Le théorème de Fermat sur certains corps de nombres totalement réels". *Algebra Number Theory* 13.2 (2019), 301–332.

[Kra18] Alain Kraus. "Quartic points on the Fermat quintic". *Ann. Math. Blaise Pascal* 25.1 (2018), 199–205.

[Kra90] Alain Kraus. "Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive." *Manuscripta Math.* 69.4 (1990), 353–386.

[LMF24] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. http://www.lmfdb.org. [Online; accessed 18 Jan 2024]. 2024.

[Maz77] Barry Mazur. "Modular curves and the Eisenstein ideal". *Inst. Hautes Études Sci. Publ. Math.* 47 (1977). With an appendix by Mazur and M. Rapoport, 33–186 (1978).

[Maz78] Barry Mazur. "Rational isogenies of prime degree (with an appendix by D. Goldfeld)". *Invent. Math.* 44.2 (1978), 129–162.

[Mer96] Loïc Merel. "Bornes pour la torsion des courbes elliptiques sur les corps de nombres". *Invent. Math.* 124.1-3 (1996), 437–449.

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

[Mil86] J. S. Milne. "Jacobian varieties". In: *Arithmetic geometry (Storrs, Conn., 1984)*. Springer, New York, 1986, 167–212.

[Mil21] James S. Milne. *Group Theory*. https://www.jmilne.org/math/CourseNotes/GT.pdf. 2021.

[Mor67] Louis J. Mordell. "The Diophantine equation $x^4 + y^4 = 1$ in algebraic number fields". *Acta Arith.* 14 (1967/68), 347–355.

[NO24] Filip Najman and Petar Orlić. "Gonality of the modular curve $X_0(N)$". *Math. Comp.* 93.346 (2024), 863–886.

[NV23] Filip Najman and Borna Vukorepa. "Quadratic points on bielliptic modular curves". *Math. Comp.* 92 (2023), 1791–1816.

[Ogg74] Andrew P. Ogg. "Hyperelliptic modular curves". *Bull. Soc. Math. France* 102 (1974), 449–462.

[OS19] Ekin Ozman and Samir Siksek. "Quadratic points on modular curves". *Math. Comp.* 88.319 (2019), 2461–2484.

[Par03] Pierre Parent. "No 17-torsion on elliptic curves over cubic number fields". *J. Théor. Nombres Bordeaux* 15.3 (2003), 831–838.

[Par00] Pierre Parent. "Torsion des courbes elliptiques sur les corps cubiques". *Ann. Inst. Fourier (Grenoble)* 50.3 (2000), 723–749.

[Raj01] Ali Rajaei. "On the levels of mod ℓ Hilbert modular forms". *J. Reine Angew. Math.* 537 (2001), 33–65.

[Rib90] Kenneth A. Ribet. "On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms". *Invent. Math.* 100.2 (1990), 431–476.

[Sik09] Samir Siksek. "Chabauty for symmetric powers of curves". *Algebra Number Theory* 3.2 (2009), 209–236.

[Sil94] J. H. Silverman. Advanced Topics in the Arithmetic of Elliptic Curves. Springer-Verlag New York, 1994.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, xx+513.

[SV22] Geoffrey Smith and Isabel Vogt. "Low degree points on curves". *Int. Math. Res. Not. IMRN* 1 (2022), 422–445.

[TW95] Richard Taylor and Andrew Wiles. "Ring-theoretic properties of certain Hecke algebras". *Ann. of Math. (2)* 141.3 (1995), 553–572.

[Tho16] Jack A. Thorne. "Automorphy of some residually dihedral Galois representations". *Math. Ann.* 364.1-2 (2016), 589–648.

[Tze98] Pavlos Tzermias. "Algebraic points of low degree on the Fermat curve of degree seven". *Manuscripta Math.* 97.4 (1998), 483–488.

[Wil95] Andrew Wiles. "Modular elliptic curves and Fermat's last theorem". *Ann. of Math. (2)* 141.3 (1995), 443–551.