The generalized Fermat equation over totally real number fields

by

Heline Deconinck

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Warwick Mathematics Institute

July 2016

THE UNIVERSITY OF
WARWICK

Contents

Acknowledgments

This thesis would not have been possible without the support of my brilliant supervisor Samir Siksek. His number theory course and especially his stories about Sophie Germain sparked my interest in the subject. I was lucky to work with him on my fourth year project which inspired me to pursue my PhD under his excellent guidance. Thank you for all the help, encouragement, support, inspiration and chocolates! I am also grateful to the staff and my fellow students at the Warwick Mathematics Institute for their support, especially the Number Theory group. I would like to extend my gratitude to the EPSRC and the Warwick Mathematics Institute for their financial support during my PhD research. Finally, I would like to give my special thanks to my parents, siblings and Dan for their continued love and support.

Declarations

Chapters 2 and 3 summarize background results found in the literature and is not my own work, except for presentation. Chapter 4 extends Siksek's paper [34]. Chapter 5 is the background for the rest of the thesis and is based on Freitas and Siksek's paper [13]. Chapters 6 extends the work of Freitas and Siksek [13] and has been published in Acta Arithmetica [8]. Chapter 7 extends the work of Freitas and Siksek [14]. Finally chapter 8 extends the work of Halberstadt and Kraus [18] following the exposition of Charollois [4].

Abstract

This thesis studies the modular approach to a generalized Fermat equation

$$Ax^p + By^p + Cz^p = 0,$$

with p a rational prime and $A, B, C \in \mathcal{O}_K$ where K is a totally real number field with $\mathcal{O}_K$ the ring of integers of K. The first part of the thesis is concerned with rational solutions (i.e. $x, y, z \in \mathbb{Q}$). After an overview of the literature on this subject, a new result for the equation $x^p + y^p + 31z^p = 0$ is proven, using quadratic reciprocity. The second part of this thesis is concerned with generalized Fermat equations over totally real number fields. After an overview of known results, a theorem is presented for the generalized Fermat equation $Ax^p + By^p + Cz^p = 0$ where $A, B, C \in \mathcal{O}_K$ are fixed and $x, y, z \in \mathcal{O}_K$ where K is a totally real field. This theorem relates the equation to solving an S-unit equation (where S is a finite list of primes). Next we prove a specific result for the equation $x^p + y^p + q^r z^p = 0$ where q is a rational prime and $p \equiv 5 \pmod 8$ over real quadratic number fields $\mathbb{Q}(\sqrt{d})$ where $d \equiv 5 \pmod 8$ and $\left(\frac{d}{q}\right) = -1$, by solving the specific S-unit equation by case analysis. We then solve some generalized Fermat equations over small real quadratic fields. In these equations ABC is divisible by exactly one odd prime ideal (taken from a finite set), and the number field is $\mathbb{Q}(\sqrt{d})$ where $d = 2, 3, 6, 7$ or 11. This is done by explicit calculations of the conductor, the level and the newforms at this level. We finish this thesis by using the Weil pairing and the symplectic criterion to get a result for a generalized Fermat equation over $\mathbb{Q}(\sqrt{2})$ for a set of prime exponents of positive density.

Chapter 1

Introduction

In 1637 according to the legend, Pierre de Fermat wrote in a copy of Arithmetica that there are no integers a, b, c such that $a^n + b^n = c^n$ if n is greater or equal to 3. Fermat wrote that had a marvellous proof of this which unfortunately was too large to fit in the margin. This theorem is called Fermat's Last Theorem, despite the fact that it was not proved yet. Also no proof of this statement by Fermat ever surfaced and the general consensus is that Fermat did not have a general proof for this. Progress towards a proof was made over the years, establishing that it suffices to prove the theorem for $n = 4$ and $n = p$ where p is a prime. Various people contributed to the small cases and even classes of primes were dealt with. However, the full proof seemed out of reach and Fermat's Last Theorem even made the Guinness book of records as the most difficult mathematical problem. In 1995, a full proof was published by Andrew Wiles using elliptic curves, Galois representations and newforms [40].

Theorem 1.0.1. *(Wiles) Suppose that $x^p + y^p + z^p = 0$ with $x, y, z \in \mathbb{Q}$ and $p \geq 3$ then $xyz = 0$.*

In chapter 3 we we give an overview of the proof. This thesis is concerned with the generalized Fermat equation

$$Ax^p + By^p + Cz^p = 0$$

for p a prime and some (fixed) A, B, C. We call a solution (x, y, z) to this equation trivial if $xyz = 0$ and non-trivial if not. The first part of the thesis assumes that $x, y, z \in \mathbb{Q}$ (and $A, B, C \in \mathbb{Q}$). Chapters 2 and 3 form the background mainly following Siksek's exposition [34]. Chapter 4 is concerned with the equation

$$x^p + y^p + 31z^p = 0$$

where $x, y, z \in \mathbb{Q}$. The chapter starts with a result of Kraus which bounds the prime p from below.

Theorem 1.0.2. *(Kraus) Suppose $L = 31$. Then equation $x^p + y^p + L^r z^p = 0$ does not have any non-trivial rational solutions if $11 \leq p \leq 10^6$.*

Next, still following [34] we look at the following result of Halberstadt and Kraus.

Theorem 1.0.3. *(Halberstadt and Kraus) The equation $x^p + y^p + 31z^p = 0$ does not have non-trivial rational solutions if $p \equiv 3 \pmod 4$*

This result by Halberstadt and Kraus eliminates half of the number of prime exponents. The rest of the chapter works towards proving the following new theorem which combines quadratic reciprocity and the modular approach to get rid of even more prime exponents.

Theorem 1.0.4. *Suppose that p is an odd prime and one of the following holds:*

- $p \equiv 1 \pmod 3$*,* $p \equiv 1, -2 \pmod 5$*,* $p \equiv \pm 1 \pmod 7$ *and* $p \equiv 2, 6, 7, 8, 10 \pmod{11}$ *(denoted situation 1)*

- $p \equiv -1 \pmod 3$*,* $p \equiv -1, 2 \pmod 5$*,* $p \equiv \pm 1 \pmod 7$ *and* $p \equiv 1, 3, 4, 5, 9 \pmod{11}$ *(denoted situation 2)*

Then there are no non-trivial solutions (x, y, z) *that satisfy the equation*

$$x^p + y^p + 31z^p = 0.$$

Recent progress in modularity for elliptic curves over totally real fields and Hilbert newforms has made it possible to look at Diophantine equations over totally real fields. In 2004, Jarvis and Meekin proved Fermat's Last Theorem over $\mathbb{Q}(\sqrt{2})$ in [22].

Theorem 1.0.5. *(Jarvis and Meekin) The equation* $x^n + y^n = z^n$ *with* $x, y, z \in \mathbb{Z}[\sqrt{2}]$ *has no solutions with* $xyz \neq 0$ *when* $n \geq 4$*.*

Freitas and Siksek [13] then proved Fermat's Last Theorem for many real quadratic fields.

Theorem 1.0.6. *(Freitas and Siksek) Let* $d \geq 2$ *be squarefree, satisfying one of the following conditions*

1. $d \equiv 3 \pmod 8$*,*

2. $d \equiv 6$ *or* $10 \pmod{16}$*,*

3. $d \equiv 2 \pmod{16}$ *and* d *has some prime divisor* $q \equiv 5$ *or* $7 \pmod 8$*,*

4. $d \equiv 14 \pmod{16}$ *and* d *has some prime divisor* $q \equiv 3$ *or* $5 \pmod 8$*.*

Then there exists an effective computable constant B_K *which only de-*

pends on K such that if $p \geq B_K$ Fermat's Last Theorem holds over $K = \mathbb{Q}(\sqrt{d})$.

This thesis extends this work to generalized Fermat equations and these results have been published in Acta Arithmetica [8].

Theorem 1.0.7. *Let $d \geq 13$ be squarefree, satisfying $d \equiv 5 \pmod 8$ and $q \geq 29$ be a prime such that $q \equiv 5 \pmod 8$ and $\left(\frac{d}{q}\right) = -1$. Let $K = \mathbb{Q}(\sqrt{d})$ and assume the Eichler-Shimura conjecture (see chapter 5) for K. Then there is an effectively computable constant $B_{K,q}$ such that for all primes $p > B_{K,q}$, the Fermat equation*

$$x^p + y^p + q^r z^p = 0$$

(where $0 \leq r < p$) has no non-trivial solutions with prime exponent p.

In [14], Freitas and Siksek look at Fermat's Last Theorem for small real quadratic fields for which they prove the following.

Theorem 1.0.8. *Let $3 \leq d \leq 23$ squarefree, $d \neq 5, 17$. Then the Fermat equation*

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

does not have any non-trivial solutions over $\mathbb{Q}(\sqrt{d})$ with exponent $n \geq 4$.

This thesis extends this for some generalized Fermat equations over some small real quadratic fields.

Theorem 1.0.9. *Let $d = 2$ or 3, $R = \mathrm{Rad}(ABC)$ [1] be a prime ideal of $K = \mathbb{Q}(\sqrt{d})$ dividing $3 \times 5 \times 7 \times 11$, or if $d = 6$ or 7 let R be a prime ideal*

[1] For $\alpha \in K$, where K is a field, define $\mathrm{Rad}(\alpha)$ as the product of all prime ideals that divide α.

dividing 15*, or if* $d = 11$ *let* R *be a prime ideal dividing* 3*. Then the Fermat equation* (6.1) *does not have any non-trivial solutions over* K *if* $p \geq 17$ *if* $d = 2$ *or if* $d \neq 2$ *if* $p \geq (1 + 3^{12})^2$.

The last chapter of this thesis generalizes the result of Halberstadt and Kraus [18] following the exposition by Charollois [4].

Theorem 1.0.10. *(Halberstadt and Kraus) Let* a, b, c *be odd pairwise coprime integers. Then there is a set of primes* $\mathcal{P} = \mathcal{P}(a, b, c)$ *of positive density such that if* $p \in \mathcal{P}$*, then the equation*

$$ax^p + by^p + cz^p = 0$$

has only trivial rational solutions $(x, y, z) \in \mathbb{Q}^3$

This theorem uses the Weil pairing and this thesis extends the field from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{2})$.

Theorem 1.0.11. *Let* K *be the number field* $\mathbb{Q}(\sqrt{2})$*. Let* $A, B, C \in \mathcal{O}_K$ *be odd with* $\pm A \pm B \pm C \neq 0$ *for any choice of signs and* ABC *not a unit. There is a set of primes* $\mathcal{P} = \mathcal{P}(A, B, C)$ *of positive density such that if* $p \in \mathcal{P}$ *then the equation*

$$Ax^p + By^p + Cz^p = 0 \tag{1.1}$$

has only trivial solutions $(x, y, z) \in (\mathcal{O}_K)^3$.

Chapter 2

Link between elliptic curves and newforms

The modular approach to solving Diophantine equations exploits the relationship between elliptic curves and newforms of weight 2. In this chapter we give the necessary background.

2.1 Elliptic curves

This section is based on various parts of [35] and [36]. First we give the formal definition of an elliptic curve.

Definition 2.1.1. *An elliptic curve over a field K is a smooth, projective algebraic curve of genus one, on which there is a specified point $\mathcal{O}$.*

Using Riemann-Roch it can be shown (for example in [35], III.3) that every elliptic curve over a field K can be written as a plane model given by the Weierstrass equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with coefficients $a_1, a_2, a_3, a_4, a_6 \in K$, $\mathcal{O} = [0 : 1 : 0]$ which is called *the point at infinity of* E. By using non-homogeneous coordinates, we obtain an affine Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

If the characteristic of K is not equal to 2 or 3, we can write the elliptic curve E over K in short Weierstrass form

$$E : Y^2 = X^3 + AX + B$$

where $A, B \in K$. An equation in the (short or long) Weierstrass form is not always smooth and hence not necessarily an elliptic curve. However, every smooth Weierstrass cubic is an elliptic curve (see [35], III.3). We define the following quantities for a (long) Weierstrass equation of an elliptic curve.

$$b_2 = a_1^2 + 4a_4, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

$$c_4 = b_2^2 - 24b_4, \qquad j = c_4^3/\Delta.$$

Definition 2.1.2. *In the notation above, Δ is called the discriminant of the*

Weierstrass equation and j the j-invariant of the elliptic curve.

We then have the following theorem (see [35] III.1).

Theorem 2.1.3. *The curve given by a Weierstrass equation satisfies:*

1. *It is singular if and only if the discriminant is zero.*
2. *It has a node if and only if the discriminant is zero and if $c_4 \neq 0$.*
3. *It has a cusp if and only if the discriminant is zero and $c_4 = 0$.*

Let $P = (X, Y) \in K$ that satisfies the Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

This P is called a *point on the elliptic curve E* over K.

For a field L define

$$E(L) = \{(X, Y) \in L^2 : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6\} \cup \{\mathcal{O}\}.$$

We denote by $\#E(L)$ the number of points in $E(L)$. Considering the geometric aspect of an elliptic curve E allows us to define addition on an elliptic curve (see for example [35], III.2). It can be shown that the points on the elliptic curve form a group under addition with identity element $\mathcal{O}$. Let P be a point on the elliptic curve E and $m \in \mathbb{Z}$. Then P is said to have order m if $mP = \mathcal{O}$ and $nP \neq \mathcal{O}$ for any $n \in \mathbb{Z}$ with $0 < n < m$. The set of points of finite order of an elliptic curve E/K form a group, denoted $E(K)_{\text{tors}}$. The *m-torsion subgroup of* $E(L)$, denoted $E(L)[m]$ is the set of all points $P \in E(L)$ such that $mP = \mathcal{O}$, which can be shown is a group. Moreover, from [35], VI.5 we get the following.

Theorem 2.1.4. *Let $E/\mathbb{C}$ be an elliptic curve and let $m \geq 1$ be an integer. Then there is an isomorphism of abstract groups*

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

In this thesis, we talk about elliptic curves up to isomorphism. In order to do this the j-invariant will be useful (see [35], III.1).

Theorem 2.1.5. *Two elliptic curves are isomorphic over $\bar{K}$ if and only if they both have the same j-invariant.*

Sometimes in this thesis it is only possible to define an elliptic curve up to quadratic twist.

Definition 2.1.6. *Let E be an elliptic curve over K given by short Weierstrass form*

$$E : Y^2 = X^3 + AX + B.$$

Let $\delta \in K$ then

$$E_\delta : \delta Y^2 = X^3 + AX + B$$

is called the quadratic twist of E by δ.

Definition 2.1.7. *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. We define the trace of Frobenius $a_q(E)$ of the finite field $\mathbb{F}_q$ to be the quantity such that $\#(E(\mathbb{F}_q)) = q + 1 - a_q(E)$.*

Let $\mathfrak{P}$ be a prime of a number field K, recall that $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$. We then have the following.

Theorem 2.1.8. *Let E be an elliptic curve over a number field K in short Weierstrass equation $E : Y^2 = X^3 + AX + B$ and let $E_\delta : \delta Y^2 = X^3 + AX + B$ be a quadratic twist of E. Then $a_{\mathfrak{P}}(E_\delta) = \pm a_{\mathfrak{P}}(E)$ for all primes $\mathfrak{P} \nmid \delta$ of K.*

Proof. Let E be an elliptic curve in short Weierstrass equation $E : Y^2 = X^3 + AX + B$. We count the number of points over a finite field by checking for which values of X the value $X^3 + AX + B$ is a square in the finite field. Each such X leads to two possible values for Y. Also the point at infinity $\mathcal{O}$ is included in the number of points. As the Legendre symbol returns 1 for a square and -1 for a non-square, the following formula holds

$$\#E(\mathbb{F}_{\mathfrak{P}}) = 1 + \sum_{X \in \mathbb{F}_{\mathfrak{P}}} \left(\left(\frac{X^3 + AX + B}{\mathfrak{P}} \right) + 1 \right).$$

And hence

$$\#E(\mathbb{F}_{\mathfrak{P}}) = 1 + \#\mathbb{F}_{\mathfrak{P}} + \sum_{X \in \mathbb{F}_{\mathfrak{P}}} \left(\frac{X^3 + AX + B}{\mathfrak{P}} \right).$$

So $a_{\mathfrak{P}}(E) = -\sum_{X \in \mathbb{F}_{\mathfrak{P}}} \left(\frac{X^3+AX+B}{\mathfrak{P}} \right)$. For the quadratic twist E_δ, if δ is a square in $\mathbb{F}_{\mathfrak{P}}$ we need the value $X^3 + AX + B$ to be a square in order for X to be the x-coordinate of a point and if δ is not a square we need $X^3 + AX + B$ to not be a square. And so

$$\#E_\delta(\mathbb{F}_{\mathfrak{P}}) = 1 + \#\mathbb{F}_{\mathfrak{P}} + \left(\frac{\delta}{\mathfrak{P}} \right) \sum_{X \in \mathbb{F}_{\mathfrak{P}}} \left(\frac{X^3 + AX + B}{\mathfrak{P}} \right).$$

So $a_{\mathfrak{P}}(E_\delta) = -\left(\frac{\delta}{\mathfrak{P}} \right) a_{\mathfrak{P}}(E) = \pm a_{\mathfrak{P}}(E)$ which finishes the proof. □

In ([35], VII.1) the minimal discriminant is discussed. Let K be a local field with discrete valuation v, R the ring of integers of K with uniformizer π. Let E/K be an elliptic curve with Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then $(x, y) \mapsto (u^{-2}x, u^{-3}y)$ leads to a new Weierstrass equation with a_i replaced by u^ia_i, and so by choosing a sufficient power of π we can assume that $a_i \in R$, and so $v(\Delta) \geq 0$. Now since v is discrete, we can call the *minimal discriminant of E at v* the Weierstrass equation that minimizes $v(\Delta)$ with $a_i \in R$. The following lemma is in ([35], VII.1).

Lemma 2.1.9. *In this notation, if $a_i \in R$ and $v(\Delta) < 12$ then the equation is minimal. If $a_i \in R$ and $v(c_4) < 4$ then the equation is minimal.*

An important invariant associated to an elliptic curve over a number field K is the conductor which measures how the elliptic curve behaves at each prime of K. But first following ([35], VII.5) let us look at all the possible behaviours.

Definition 2.1.10. *Let L be a local field, with ring of integers R and $\mathcal{M}$ the maximal ideal of R. Let E be an elliptic curve over L. Let $\tilde{E}$ be the reduction modulo $\mathcal{M}$ of a minimal Weierstrass equation for E.*

- *E has good reduction if $\tilde{E}$ is non-singular.*
- *E has multiplicative reduction if $\tilde{E}$ has a node.*
- *E has additive reduction if $\tilde{E}$ has a cusp.*

In the multiplicative and additive case we say that E has bad reduction.

We can use the following theorem (VII.5.1 in [35]) to find out what type of reduction we are dealing with.

Theorem 2.1.11. *Let E is an elliptic curve in minimal Weierstrass form for $\mathfrak{q}$ with Δ and c_4 the usual invariants. Then the following hold:*

(i) E has good reduction at $\mathfrak{q}$ if and only if $ord_{\mathfrak{q}}(\Delta) = 0$

(ii) E has multiplicative reduction at $\mathfrak{q}$ if and only if $ord_{\mathfrak{q}}(\Delta) > 0$ and $ord_{\mathfrak{q}}(c_4) = 0$

(iii) E has additive reduction at $\mathfrak{q}$ if and only if $ord_{\mathfrak{q}}(\Delta) > 0$ and $ord_{\mathfrak{q}}(c_4) > 0$.

Definition 2.1.12. *Let E be an elliptic curve over a number field K. The conductor N of E is defined as*

$$N = \prod_{\mathfrak{q} \in \mathbb{P}} \mathfrak{q}^{f_{\mathfrak{q}}}$$

where $\mathbb{P}$ is the set of all primes of K,

$$f_{\mathfrak{q}} = \begin{cases} 0 & \text{if } E \text{ has good reduction at } \mathfrak{q} \\ 1 & \text{if } E \text{ has multiplicative reduction at } \mathfrak{q} \\ 2 + \delta_{\mathfrak{q}} & \text{if } E \text{ has additive reduction at } \mathfrak{q} \end{cases}$$

Here $\delta_{\mathfrak{q}}$ is the measure of the wild reduction in the action of the inertia group on the l-adic Tate module $T_l(E)$ (see [36]). In particular if $\mathfrak{q} \nmid 6$ then $\delta_{\mathfrak{q}} = 0$.

Note that when $\mathfrak{q} \mid 6$ and $\mathfrak{q}$ has additive reduction, one can look at specific tables (for example Ionnas Papadopoulos' tables [31]) or use Tate's algorithm, as demonstrated in [36] (which we will use later in this thesis).

An elliptic curve E over K is said to be *semi-stable* if at a prime of K it has either good or multiplicative reduction at that prime. It follows that an elliptic curve is semi-stable if and only if the conductor is squarefree.

We need the following definition.

Definition 2.1.13. *Let E/K be an elliptic curve. E has potentially good (respectively potentially multiplicative) reduction at a prime l if there is a finite extension of K'/K such that E has good (respectively multiplicative) reduction at $l' \mid l$ over K'.*

The following lemma will be useful in calculations in this thesis.

Lemma 2.1.14. *Let E/K be an elliptic curve. Then E has potentially multiplicative reduction at l if and only if $\mathrm{ord}_l(j(E)) < 0$.*

In the final chapter of this thesis we use the theory of the Tate curves, which can be found in ([36], V.3). We give the highlights that are needed for that chapter.

Theorem 2.1.15. *(Tate) Let K be a p-adic field with absolute value $|\cdot|$, let $q \in K^*$ satisfy $|q| < 1$, and let*

$$s_k(q) = \sum_{n\geq 1} \frac{n^k q^n}{1-q^n}, \qquad a_4(q) = s_3(q), \qquad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12}.$$

1. *The series $a_4(q)$ and $a_6(q)$ converge in K. Define the Tate curve E_q by the equation*

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q).$$

2. The Tate curve is an elliptic curve defined over K with discriminant

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$$

and j-invariant

$$j(E_q) = \frac{1}{q} + 744 + 196884q + ... = \frac{1}{q} + \sum_{n \geq 0} c(n) q^n,$$

where $c(n)$ are integers.

We need the following theorem from [36].

Theorem 2.1.16. *(Tate) Let K be a p-adic field, let E/K be an elliptic curve with $|j(E)| > 1$. Then there is a unique $q \in K^*$ with $|q| < 1$ such that E is isomorphic over $\bar{K}$ to the Tate curve E_q.*

Now we look at the Galois representation of the elliptic curve. Before we do this, we need to fix some notation. Let K be either a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$ with p a prime, $\bar{K}$ its algebraic closure and $G_K = \text{Gal}(\bar{K}/K)$ its absolute Galois group. Let E/K be an elliptic curve and $m \in \mathbb{Z}_{\geq 2}$. Let $\sigma \in G_K$, $P \in E[m]$, then

$$m\sigma(P) = \sigma(P) + \sigma(P) + \cdots + \sigma(P) = \sigma(P + P + \cdots + P) = \sigma(mP) = \sigma(\mathcal{O}) = 0.$$

So G_K acts on $E[m]$. Pick a basis P_1, Q_1 for $E[m]$. Then

$$\begin{cases} \sigma(P_1) &= aP_1 + cQ_1 \\ \sigma(Q_1) &= bP_1 + dQ_1 \end{cases}$$

so obtain a representation:

$$\begin{aligned} G_K &\to Aut(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \end{aligned}$$

Definition 2.1.17. *Let l be a rational prime. The mod l representation of the elliptic curve E is defined as*

$$\bar{\rho}_{E,l} : G_K \to \text{ Aut(E[l])} \cong GL_2(\mathbb{Z}/l\mathbb{Z})$$

The following theorem is used extensively in the literature on the modular approach.

Theorem 2.1.18. *Let E be an elliptic curve over a number field K and l a rational prime. Then $\bar{\rho}_{E,l}$ is reducible if and only if E has an l-isogeny.*

Proof. Suppose $\bar{\rho}_{E,l}$ is reducible. Then we can choose a basis for $E[l]$, namely P_1, P_2 such that

$$\bar{\rho}_{E,l} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Now $\sigma(P_1) = \alpha_\sigma P_1$ for all $\sigma \in G_K$. Let $C =< P_1 >$, which is a subgroup of $E[l]$ of order l and hence cyclic. Then C is rational (i.e. fixed by G_K). So there is an l-isogeny $E \to E/C$. Conversely, suppose that E has an l-isogeny defined over $K : E \to E'$. Let C be the kernel; this has order l. Let P_1 be a generator of C. We can extend P_1 to a basis P_1, P_2 for $E[l]$. Then

$$\sigma(P_1) = aP_1$$
$$\sigma(P_2) = bP_1 + dP_2$$

so

$$\bar{\rho}_{E,l}(\sigma) = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Thus $\bar{\rho}_{E,l}$ is reducible. □

2.2 Link between elliptic curves and newforms

This section links an elliptic curve E over $\mathbb{Q}$ to a rational newform f of weight 2 and follows the exposition of [34]. Note that a newform is a normalized cuspidal modular form of weight two that has not been defined at a previous level (see for example [10]). This thesis will focus on the elliptic curve aspect of the modular approach, so for this thesis these facts about newforms will suffice.

- The set of modular forms of level N and weight 2 is a finite dimensional vector space over $\mathbb{C}$, so the set of cuspidal modular forms (which is a subspace) is finite dimensional too.

- Each newform of level N has a q-expansion, namely

  $$f = q + \sum_{n \geq 2} c_n q^n.$$

  Note that $c_0 = 0$ as f is a cuspform and $c_1 = 1$ as it is normalized.

- There are no newforms of weight 2 and level 1,2,3,4,5,6,7,8,9,10,12,13,16,18,22,25,28 and 60.

- If c_i are the coefficients of a newform f and $K = \mathbb{Q}(c_2, c_3, ...)$ then K is a totally real finite extension of $\mathbb{Q}$. Furthermore, c_i belong to the ring of integers of the number field K.

Definition 2.2.1. *Let $f = q + \sum_{n \geq 2} c_n q^n$ be a newform. Then f is said to be rational if $c_n \in \mathbb{Q}\ \forall n$, irrational if it is not rational.*

What is useful about newforms is that there is an algorithm due to William Stein [38] and John Cremona [5] which computes the newforms of a given level which has been implemented in `MAGMA` [2].

Now we can look at the modularity theorem. The Taniyama-Shimura-Weil conjecture states that every elliptic curve over $\mathbb{Q}$ is a modular elliptic curve and this was proved by Andrew Wiles [40] (with the help of his former student Richard Taylor) [39] for semi-stable elliptic curves. Christophe Breuil, Brian Conrad, Fred Diamond and Richard Taylor [3] later proved the Taniyama-Shimura-Weil conjecture for all elliptic curves over $\mathbb{Q}$.

Theorem 2.2.2. *(Wiles, Breuil, Conrad, Diamond, Taylor) (The Modularity Theorem) Associated to any rational newform f of level N and weight 2 is an elliptic curve $E_f/\mathbb{Q}$ of conductor N so that for all primes $l \nmid N$*

$$c_l = a_l(E_f)$$

where c_l is the l-th coefficient in the q-expansion of f and $a_l(E_f) = l + 1 - \#E_f(\mathbb{F}_l)$. For any given positive integer N, the association $f \mapsto E_f$ is a *bijection between rational newforms of level N and isogeny classes of elliptic curves of conductor N.*

Following [34] we define the following.

Definition 2.2.3. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, and suppose that f is a newform of level N' with q-expansion $f = q + \sum_{n\geq 2} c_n q^n$, and coefficients c_i generating the number field $K/\mathbb{Q}$. We shall say that the curve E arises modulo p from the newform f (and write $E \sim_p f$) if there is some prime ideal $\mathfrak{P} \mid p$ of K such that for almost all primes l, we have $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$.*

A different formulation which is more useful from a computational point of view is the following is also given in [34].

Proposition 2.2.4. *Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{P} \mid p$ of K such that for all primes l*

(i) if $l \nmid pNN'$ then $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$, and

(ii) if $l \nmid pN'$ and $l \mid\mid N$ then $l + 1 \equiv \pm c_l \pmod{\mathfrak{P}}$

where $l \mid\mid N$ if and only if $l \mid N$ and $l^2 \nmid N$.

By Theorem 2.2.2 every rational newform f of weight 2 corresponds to some elliptic curve F. If E arises modulo p from f then we shall also say that E arises modulo p from F (and write $E \sim_p F$). From [34] we get the following.

Proposition 2.2.5. *Suppose that E, F are elliptic curves over $\mathbb{Q}$ with conductors N and N' respectively. Suppose that E arises modulo p from F. Then for all primes l*

(i) if $l \nmid NN'$ *then* $a_l(E) \equiv a_l(F) \pmod{p}$*, and*

(ii) if $l \nmid N'$ *and* $l \mid\mid N$ *then* $l + 1 \equiv \pm a_l(F) \pmod{p}$*.*

Note that this Proposition looks a lot like Proposition 2.2.4 and maybe even a restatement. But Proposition 2.2.5 is a lot stronger, as it handles the case when $l = p$. Because p is usually unknown, this is a very useful improvement by Kraus and Oesterlé [27]. Also note that $l \nmid NN'$ is equivalent to both elliptic curves E and F having good reduction at l. On the other hand, $l \nmid N'$ and $l \mid\mid N$ means that E has multiplicative reduction at l, whilst F has good reduction at l.

Chapter 3

The generalized Fermat equation over $\mathbb{Q}$

This chapter gives the background necessary to provide a basic understanding of the modular approach to Diophantine equations. The modular approach uses the relationship between elliptic curves and newforms of weight 2. These are the mathematical ingredients of Wiles' proof of Fermat's Last Theorem for which we provide a sketch at the end of this chapter.

3.1 Frey curve

The history of the Frey elliptic curve is quite interesting. Yves Hellegouarch reaccounts on his website [19] that he associated an elliptic curve to the Fermat equation $x^p + y^p + z^p = 0$ during the Journées Arithmétiques de Bordeaux of 1969 in order to prove a proposition. However, this proposition was disproved on the spot by Jean-Pierre Serre. Therefore, it was not included in the notes on that day, so was not documented. But the idea is great and has been studied in depth by Gerhard Frey as he was convinced that this elliptic curve might not be modular [16].

First we explain what a Frey elliptic curve is. A Frey elliptic curve is an elliptic curve over the rationals but instead of having known coefficients, it has coefficients depending on the hypothetical solutions to a Diophantine equation. By construction it has a nice discriminant, making it possible to prove properties of the associated Diophantine equation.

Start off with a Diophantine equation $Ax^p+By^p+Cz^p=0$ with $x,y,z\in\mathbb{Q}$ and A,B,C pairwise coprime and $ABC\neq 0$. Suppose (x,y,z) is a solution with $xyz\neq 0$. Suppose that a p-th power of a prime divides A (resp. B, resp. C). Then this prime can be absorbed into x (resp. y, resp. z) and hence we can assume that the solution is pairwise coprime. We call such a solution a non-trivial, primitive solution. Note that exactly one of Ax^p, By^p, Cz^p has to be even when we reduce the equation modulo 2, which we can assume to be By^p without loss of generality. Since Ax^p is odd either $Ax^p\equiv 1 \pmod 4$ or $Ax^p\equiv -1 \pmod 4$. In the first case, we can just consider the solution $(-x,-y,-z)$ instead, hence we can assume that $Ax^p\equiv -1 \pmod 4$.

Definition 3.1.1. *For primes $p\geq 3$, let (x, y, z) be a non-trivial primitive solution to the Fermat equation $Ax^p+By^p+Cz^p=0$. Assume that By^p is even and that $Ax^p\equiv -1 \pmod 4$. Then $E_{A,B,C}: Y^2=X(X-Ax^p)(X+By^p)$ is called the Frey elliptic curve.*

Note that the discriminant of this model is

$$\Delta = 16(Ax^pBy^p(Ax^p+By^p))^2 = 16(ABC)^2(xyz)^{2p},$$

and so by Theorem 2.1.3 this is an elliptic curve if and only if $xyz\neq 0$, i.e.

(x, y, z) is a non-trivial solution. In some cases the next step is showing that no such elliptic curve exist for example in the case of Fermat's Last Theorem (FLT). Even if an elliptic curve exists partial information can be extracted.

3.2 Level lowering

Once the Frey elliptic curve is constructed (even if the coefficients are not known, but at least they obey the Diophantine equation), in order to relate the elliptic curves with modular forms, Ribet's Level Lowering Theorem [33] is used. In [34], Siksek describes the importance of Ribet's Theorem as this theorem gives the level of the newform associated to the Frey elliptic curve.

Theorem 3.2.1. *(A simplified case of Ribet's Level Lowering) Let p be prime $p \geq 5$ and let E be an elliptic curve over $\mathbb{Q}$ without p-isogenies. Let Δ be the minimal discriminant for E and let N be the conductor. Define*

$$N_p = N \Bigg/ \prod_{\substack{q \| N, \\ p \mid \mathrm{ord}_q(\Delta)}} q.$$

(Here $q \, || \, N$ means $q \mid N$ and $q^2 \nmid N$). Then there exists a newform f of level N_p such that $E \sim_p f$

Before discussing the consequences of the theorem we look at the assumptions. In order to use Ribet's Level Lowering Theorem, we need our elliptic curve to have no p-isogenies.

Definition 3.2.2. *An isogeny ϕ is a rational map of an elliptic curve onto another elliptic curve that is also a group homomorphism. A p-isogeny is an isogeny of degree p (i.e. the size of the kernel is p).*

For an elliptic curve E over $\mathbb{Q}$ is straightforward to check in `MAGMA` [2] if E has p-isogenies. But the Frey elliptic curve has unknown coefficients. The following powerful theorem by Mazur [28] will be useful in practice.

Theorem 3.2.3. *(Mazur) Suppose $E/\mathbb{Q}$ is an elliptic curve and that at least one of the following conditions holds.*

- *$p \geq 17$ and $j(E) \notin \mathbb{Z}[\frac{1}{2}]$,*
- *or $p \geq 11$ and E is a semi-stable elliptic curve,*
- *or $p \geq 5$, $\#E(\mathbb{Q})[2] = 4$, and E is a semi-stable elliptic curve,*

Then E does not have any p-isogenies.

So there often exists an explicit criterion to check whether Ribet's Level Lowering Theorem can be used in practice. We now look at the consequences of Ribet's Level Lowering Theorem. The theorem says that if the assumptions are satisfied there exist a newform of a specific level that is related to the elliptic curve. This will be crucial for proving Fermat's Last Theorem as newforms are (computationally) easier to work with.

3.3 Conductor and $\mathcal{N}_p$ calculations for generalized Fermat equation

Here we present the conductor and $\mathcal{N}_p$ recipes for the generalized Fermat equation over $\mathbb{Q}$ as presented by Siksek in [34] based on work by Kraus [25].

Suppose that A, B, C are non-zero pairwise coprime integers, and $p \geq 5$ a prime. Let

$$R = ABC,$$

and suppose that

$$\mathrm{ord}_q(R) < p$$

for every prime number q. Consider the equation

$$Ax^p + By^p + Cz^p = 0, \tag{3.1}$$

where we assume that

$$A,\ B,\ C \text{ are non-zero and pairwise coprime.}$$

Without loss of generality we also suppose that

$$Ax^p \equiv -1 \pmod 4, \qquad By^p \equiv 0 \pmod 2.$$

We associate to the non-trivial primitive solution (x, y, z) the Frey curve

$$E \;:\quad Y^2 = X(X - Ax^p)(X + By^p).$$

The minimal discriminant is

$$\Delta_{\min} = \begin{cases} 2^4 R^2 (xyz)^{2p} & \text{if } 16 \nmid By^p, \\ 2^{-8} R^2 (xyz)^{2p} & \text{if } 16 \mid By^p. \end{cases}$$

For positive integer R and prime q we define:

$$\mathrm{Rad}_q(R) = \prod_{\substack{l \mid R \text{ prime}, \\ l \neq q}} l.$$

The conductor N is given by

$$N = \begin{cases} 2\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 0 \text{ or } \mathrm{ord}_2(R) \geq 5, \\ 2\,\mathrm{Rad}_2(Rxyz) & \text{if } 1 \leq \mathrm{ord}_2(R) \leq 4 \text{ and } y \text{ is even,} \\ \mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 4 \text{ and } y \text{ is odd,} \\ 2^3\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 2 \text{ or } 3 \text{ and } y \text{ is odd,} \\ 2^5\,\mathrm{Rad}_2(Rxyz) & \text{if } \mathrm{ord}_2(R) = 1 \text{ and } y \text{ is even.} \end{cases}$$

Theorem 3.3.1. *(Kraus [25]) Under the above assumptions, $E \sim_p f$ for some newform f of level N_p where*

$$N_p = \begin{cases} 2\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 0 \textit{ or } \mathrm{ord}_2(R) \geq 5, \\ \mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 4, \\ 2\,\mathrm{Rad}_2(R) & \textit{if } 1 \leq \mathrm{ord}_2(R) \leq 3 \textit{ and } y \textit{ is even,} \\ 2^3\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 2 \textit{ or } 3 \textit{ and } y \textit{ is odd,} \\ 2^5\,\mathrm{Rad}_2(R) & \textit{if } \mathrm{ord}_2(R) = 1 \textit{ and } y \textit{ is odd.} \end{cases}$$

3.4 Sketch of proof of Fermat's Last Theorem

Finally following [34] we can sketch how the modular approach works for Fermat's Last Theorem proved by [40].

Theorem 3.4.1. *(Wiles) The equation $x^p + y^p + z^p = 0$ with $x, y, z \in \mathbb{Z}$ and $p \geq 5$ prime has no non-trivial integer solutions.*

Assume that we have a non-trivial solution (a, b, c). Without loss of generality we can assume it is primitive, that b is even and that $a \equiv -1$

(mod 4). We then construct the Frey elliptic curve

$$E : Y^2 = X(X - a^p)(X + b^p).$$

The discriminant of this elliptic curve is $\Delta = 16(abc)^{2p}$. The conductor is $N = 2\mathrm{Rad}_2(xyz)$. Now since the conductor is squarefree, we know that it is semi-stable. We need to verify that E has no p-isogenies in order to apply Ribet's Level Lowering theorem. Since $E(\mathbb{Q})[2] = 4$ and E is semi-stable, we can use Mazur's theorem. And so applying Ribet's Theorem we get that that $N_p = 2$. From Chapter 2 we know that there are no newforms of level 2 and weight 2. Hence the discriminant of the Frey elliptic curve has to be zero, so the only solutions to Fermat's Last Theorem with $p \geq 5$ are the trivial ones.

Chapter 4

Quadratic reciprocity

This chapter looks at the Diophantine equation

$$x^p + y^p + 31z^p = 0. \tag{4.1}$$

The first sections deal with what is known about this and the more general equation

$$x^p + y^p + L^r z^p = 0 \tag{4.2}$$

where L is an odd prime. The last two sections provide a new theorem that proves that there are no solutions to equation (4.1) for exponent p satisfying certain congruences modulo $3, 5, 7$ and 11.

4.1 Assumptions

Consider the Diophantine equation (4.2) where L is an odd prime, $x, y, z \in \mathbb{Q}$, $p \geq 5$ is a prime and $r \in \mathbb{Z}_{\geq 0}$. If $r \geq p$ then can replace z by Lz to get coefficient L^{r-p}. This process can be repeated until $r < p$ and hence can assume that $r < p$. Call (x, y, z) a solution to this equation if it satisfies the equation and non-trivial if $xyz \neq 0$. Take l to be the lowest common multiple of the denominators of x, y, z. Then (lx, ly, lz) is a also a solution to the Diophantine equation and moreover $lx, ly, lz \in \mathbb{Z}$. Hence we can assume that $x, y, z \in \mathbb{Z}$. Note that, if two of the terms of the equation have a prime factor q in common (where $q \neq L$), then q also divides the third term. If $q = L$ then the condition $r < p$ will guarantee that if two of the variables (x, y, z) are divisible by L then so is the third one. In both cases it is possible to replace (x, y, z) by $(x/q, y/q, z/q)$. This process can be repeated until eventually (x, y, z) are pairwise coprime. In this case the solution is said to be primitive. Hence from now (without loss of generality) it is assumed that (x, y, z) are coprime integers. Finally note that if $r = 0$ then this is the Fermat equation (also known as the equation from Fermat's Last Theorem), and thus we can assume that $0 < r < p$.

4.2 Bounding the exponent p using the corresponding newform

The proof of Fermat's last theorem boils down to the fact that there is no newform of level 2 and weight 2. Unfortunately, quite often there exists a newform of level N_p and weight 2 and sometimes there are even multiple newforms. However, all is not lost and these newforms can sometimes be used to bound the exponent p.

The recipe for the generalized Fermat equation $Ax^p + By^p + Cz^p = 0$ from the previous chapter associates to a hypothetical non-trivial primitive solution (x, y, z) of the Diophantine equation (4.2) the following Frey curve.

$$E : Y^2 = X(X - A)(X + B)$$

where $(A, B, -A - B)$ is a permutation of $(x^p, y^p, L^r z^p)$ such that $A \equiv -1 \pmod 4$ and B is even. The minimal discriminant and conductor of E are

$$\Delta_{\min} = 2^{-8} L^{2r} (xyz)^{2p}, \qquad N = \mathrm{Rad}(Lxyz)$$

and $N_p = 2L$.

Since the conductor N of E is squarefree, we know that the elliptic curve E is semi-stable. As $Lxyz \neq 0$ it follows that $(A, 0), (B, 0), (0, 0)$ are distinct and hence E has full 2-torsion. By Theorem 3.2.3, E does not have p-isogenies since $p \geq 5$. Ribet's Theorem (Theorem 3.2.1) shows that E arises modulo p from some newform f of level $N_p = 2L$ and weight 2. For a specific L, one can calculate the newforms at that level and weight 2. For example, for $L = 31$, `MAGMA` shows that there is exactly one rational newform of level 62 and weight 2 (irrational newforms will be dealt with later on in this chapter).

$$\begin{aligned} f = q + q^2 + q^4 - 2q^5 + q^8 - 3q^9 - 2q^{10} + 2q^{13} + q^{16} - 6q^{17} - 3q^{18} \\ + 4q^{19} - 2q^{20} + 8q^{23} - q^{25} + 2q^{26} + 2q^{29} + O(q^{30}). \end{aligned} \tag{4.3}$$

This has the following elliptic curve over $\mathbb{Q}$ associated to it

$$E : y^2 + xy + y = x^3 - x^2 - x + 1.$$

This elliptic curve has Cremona reference $62a1$. If newforms are found at the predicted level, it is sometimes possible to use these to bound the exponent p of the Diophantine equation. This method is explained in [34] and in some cases it even shows that E does not arise modulo p from a given newform (which has the right level and weight). The following is Proposition 9.1 from [34].

Proposition 4.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and suppose that $t \mid \#E(\mathbb{Q})_{\mathrm{tors}}$. Suppose that f is a newform of level N' and weight 2. Let l be a prime such that $l \nmid N'$ and $l^2 \nmid N$. Let*

$$S_l = \left\{ a \in \mathbb{Z} \ : \quad -2\sqrt{l} \le a \le 2\sqrt{l}, \quad a \equiv l+1 \pmod{t} \right\}.$$

Let c_l be the l-th coefficient of f and define

$$B_l'(f) = \mathrm{Norm}_{K/\mathbb{Q}}((l+1)^2 - c_l^2) \prod_{a \in S_l} \mathrm{Norm}_{K/\mathbb{Q}}(a - c_l)$$

and

$$B_l(f) = \begin{cases} l \cdot B_l'(f) & \text{if } f \text{ is irrational,} \\ B_l'(f) & \text{if } f \text{ is rational.} \end{cases}$$

If $E \sim_p f$ then $p \mid B_l(f)$.

Notice that this proposition bounds p provided there is an l such that $B_l(f) \neq 0$. According to [34] this is guaranteed to succeed in two cases:

(a) Suppose that f is irrational. Then for infinitely many primes l we have that $B_l(f) \neq 0$. This is true since $c_l \notin \mathbb{Q}$ for infinitely many of the coefficients c_l.

(b) Suppose that f is rational and that t is prime or $t = 4$. Suppose that for every elliptic curve F in the isogeny class corresponding to f we have $t \nmid \#F(\mathbb{Q})_{\text{tors}}$. Then there are infinitely many primes l such that $B_l(f) \neq 0$.

If $B_l(f) \neq 0$ for any l then this proposition bounds the exponent p. Moreover if $B_l(f)$ is equal to 1 (or $2^i 3^j$ where $i, j \in \mathbb{Z}$) for any l then it follows (since $p \geq 5$) that there is no such p. The following theorem is proved in [34].

Theorem 4.2.2. *Suppose* $3 \leq L < 100$ *is prime. Then the equation* $x^p + y^p + L^r z^p = 0$ *where* $0 < r < p$*,* $p > 5$ *prime and* $xyz \neq 0$ *has no solutions where x,y,z are pairwise coprime unless* $L = 31$*, in which case* $E \sim_p F$ *where* F *is the elliptic curve with Cremona reference* $62a1$*.*

This theorem indicates that $L = 31$ is a harder equation to solve than any other prime L where $3 \leq L \leq 100$. For the rest of this chapter, it is assumed that $L = 31$. The previous theorem did not result in an upper bound for the exponent p in the equation $x^p + y^p + 31^r z^p = 0$, but maybe it is possible to find a lower bound for p.

4.3 Finding a lower bound for exponent p

Siksek [34] uses Kraus' method [26] to find a lower bound for the exponent p which shows that if $p > 5$ then $p > 10^6$. Such a large bound for p does not only give a good indication that there might be no solutions, but is also very helpful to know that if there is a non-trivial, primitive solution then p has to be very large. We give an explanation of this method following the exposition in [34]. Kraus' method deals with a fixed prime p, and hence iteratively may be used to find a lower bound for p by simply eliminating all options exhaustively. Kraus' method starts with associating a Frey elliptic curve to the Diophantine equation $x^p + y^p + L^r z^p = 0$, where L is a prime and $xyz \neq 0$. We associate the following Frey elliptic curve to a non-trivial primitive solution (x, y, z) of equation (4.2)

$$E : Y^2 = X(X - A)(X + B)$$

where $A, B, -(A + B) = C$ is an appropiate permutation of $x^p, y^p, L^r z^p$. Letting $\delta = (y/x)^p$ then E is the quadratic twist of

$$E_\delta : \quad Y^2 = X(X - 1)(X + \delta),$$

by x^p.

For prime $l \nmid x$, from Theorem 2.1.8 it follows that $a_l(E) = \pm a_l(E_\delta)$.

Lemma 4.3.1. *With notation as above, suppose that $E \sim_p f$ for some newform f with level $2L$ and weight 2. Suppose that l is a prime distinct from 2, L, p. Write $f = q + \sum_{n\geq 2} c_n q^n$.*

- *If $l \mid xyz$ then $p \mid \mathrm{Norm}((l + 1)^2 - c_l^2)$.*
- *If $l \nmid xyz$ then $p \mid \mathrm{Norm}(a_l(E_\delta)^2 - c_l^2)$.*

Proof. Let E be the Frey elliptic curve associated to a non-trivial primitive solution to Equation 4.2. Then E has conductor $\mathrm{Rad}(Lxyz)$ so from Proposition 2.2.4 it follows that

(i) If $l \nmid p \cdot 2L \cdot \mathrm{Rad}(Lxyz)$ then $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$

(ii) If $l \nmid p \cdot 2L$ and $l \mid\mid \mathrm{Rad}(Lxyz)$ then $l + 1 \equiv \pm c_l \pmod{\mathfrak{P}}$, where $\mathfrak{P} \mid p$ is a prime ideal in the field K generated by the c_i coefficients in the q-expansion of f. Now since l is a prime distinct from 2, L and p it follows that $l \nmid p \cdot 2L \cdot \mathrm{Rad}(Lxyz)$ is equivalent to $l \nmid xyz$. Since $\mathrm{Rad}(Lxyz)$ is squarefree, it follows that $l \nmid p \cdot 2L$ and $l \mid\mid \mathrm{Rad}(Lxyz)$ is equivalent to $l \mid xyz$. Hence we get

(i) if $l \nmid xyz$ then $a_l(E) \equiv c_l \pmod{\mathfrak{P}}$

(ii) if $l \mid xyz$ then $l + 1 \equiv \pm c_l \pmod{\mathfrak{P}}$.

Now recall from the discussion above that if $l \nmid x$ it follows that $a_l(E) = \pm a_l(E_\delta)$. Squaring both sides of the equivalences and recalling that $\mathfrak{P} \mid p$ completes the proof. □

Remark. Suppose $l = np + 1$ is prime. Let

$$\mu_n(\mathbb{F}_l) = \left\{ \zeta \in \mathbb{F}_l \quad : \quad \zeta^n = \overline{1} \right\}. \tag{4.4}$$

This is the group of n-th roots of unity in $\mathbb{F}_l$. Note that if $l \nmid xyz$ then the reduction of $\delta = (y/x)^p$ modulo l belongs to $\mu_n(\mathbb{F}_l)$.

Lemma 4.3.2. *Suppose that $p \geq 5$ is a fixed prime and E is as above. Suppose that for each newform f at level $2L$ and weight 2 there exists a positive integer n satisfying the following four conditions:*

(i) $l = np + 1$ is prime.

(ii) $l \neq L$.

(iii) $p \nmid \mathrm{Norm}((l + 1)^2 - c_l^2)$. (Here c_l is the l-th coefficient of f).

(iv) For all $\delta' \in \mu_n(\mathbb{F}_l)$, $\delta' \neq -1$ we have

$$p \nmid \operatorname{Norm}(a_l(E_{\delta'})^2 - c_l^2).$$

Then the equation $x^p + y^p + L^r z^p = 0$ does not have any non-trivial solutions satisfying the usual conditions.

Proof. Suppose there is a non-trivial solution to $x^p + y^p + L^r z^p = 0$. We can assume it is primitive. Let E be the Frey elliptic curve associated to it. Let E_δ be the elliptic curve and f the newform as described above. Suppose there exists a positive integer n satisfying conditions (i)-(iv). Then from (i) and (ii) it follows that $l = np + 1$ is a prime distinct from 2, p and L. Then from Lemma 4.3.1 and (iii) it follows that $l \nmid xyz$. So it follows from Lemma 4.3.1 that $p \mid \operatorname{Norm}(a_l(E_\delta)^2 - c_l^2)$. On the other hand since $l \nmid xyz$ it follows that $\delta = (y/x)^p \in \mathbb{F}_l^*$. $\delta^n = (y/x)^{np} = (y/x)^{l-1} \equiv 1 \pmod{l}$. Hence $\delta \in \mu_n(\mathbb{F}_l)$. If $\delta \equiv -1 \pmod{l}$ then $(y/x)^p \equiv -1 \pmod{l}$, so $x^p + y^p \equiv 0 \pmod{l}$. From Equation 4.2 it follows that $Lz^p \equiv 0 \pmod{l}$ which is impossible as $l \nmid xyz$ and $l \neq L$. So $\delta \neq -1$. From this and (iv) it follows that $p \nmid \operatorname{Norm}(a_l(E_\delta)^2 - c_l^2)$ which leads to a contradiction and hence there is no non-trivial solution to $x^p + y^p + L^r z^p = 0$. □

These lemmas are used by Siksek to prove the following theorem.

Theorem 4.3.3. *Suppose $L = 31$. Then equation $x^p + y^p + L^r z^p = 0$ does not have any solutions satisfying the usual conditions for $11 \leq p \leq 10^6$.*

Proof. (sketch, based on [34]) Suppose $L = 31$. By Theorem 4.2.2 we know that $E \sim_p F$ where F is the elliptic curve $62a1$ with equation

$$F : y^2 + xy + y = x^3 - x^2 - x + 1.$$

For all primes p such that $11 \leq p \leq 10^6$, it is then possible to check if there exists a suitable n as in Proposition 4.3.2.

□

Instead of trying to find an upper or lower bound for the prime exponent p, the next section explains how to get rid of a whole class of prime exponents.

4.4 Halving the number of potential exponents

So far, no one has been able to find an upper bound for the exponent p in equation 4.2 when $L = 31$ and $r = 1$ so that there are no non-trivial solutions for any prime p bigger than this bound. This section explains how Halberstadt and Kraus [18] using the symplectic method prove that for half of the prime exponents p there are no non-trivial solutions to Equation 4.1. The symplectic method will feature prominently in the final chapter of this thesis, so the theorem is included.

Theorem 4.4.1. *(Halberstadt and Kraus) Suppose E and F are elliptic curves over $\mathbb{Q}$ and $p \geq 5$ is a prime such that $E \sim_p F$. Let ℓ_1, ℓ_2 be distinct primes, different from p. Suppose that E and F have multiplicative reduction at ℓ_1, ℓ_2 and that p does not divide $\operatorname{ord}_{\ell_i}(\Delta(E))$ nor $\operatorname{ord}_{\ell_i}(\Delta(F))$ for $i = 1, 2$, where $\Delta(E)$ and $\Delta(F)$ are the minimal discriminants of E and F. Then*

$$\frac{ord_{\ell_1}(\Delta(E))ord_{\ell_2}(\Delta(E))}{ord_{\ell_1}(\Delta(F))ord_{\ell_2}(\Delta(F))}$$

is congruent to a square modulo p.

Halberstadt and Kraus prove the following application.

Theorem 4.4.2. *The equation $x^p + y^p + 31z^p = 0$ does not have non-trivial solutions if $p \equiv 3 \pmod 4$.*

Proof. Suppose there is a non-trivial solution (x, y, z) to Equation 4.1. We may suppose that it is primitive. The following Frey elliptic curve is associated to it

$$E : Y^2 = X(X - A)(X + B)$$

where $A, B, -A - B$ is an appropriate permutation of $x^p, y^p, 31z^p$. We know from Theorem 4.2.2 that $E \sim_p F$ where F is $62a1$. Now we can use the recipes in chapter 2 to calculate the minimal discriminants

$$\Delta(E) = 2^{-8} \cdot 31^2(xyz)^{2p}, \qquad \Delta(F) = -2^4 \times 31,$$

and the conductors

$$N_E = \mathrm{Rad}(31xyz), \qquad N_F = 62.$$

So both curves have multiplicative reduction at 2 and 31. Theorem 4.4.1 can now be used with primes $\ell_1 = 2$ and $\ell_2 = 31$. By Theorem 4.3.3, we know that that $p > 10^6$ and so certainly $p \neq 31$. So applying Theorem 4.4.1, we get that:

$$\frac{\mathrm{ord}_2(\Delta(E))\mathrm{ord}_{31}(\Delta(E))}{\mathrm{ord}_2(\Delta(F))\mathrm{ord}_{31}(\Delta(F))} = \frac{(-8 + 2p\ \mathrm{ord}_2(xyz))(2 + 2p\ \mathrm{ord}_{31}(xyz))}{4 \times 1} \equiv -4 \pmod p$$

must be a square modulo p. Hence $\left(\frac{-1}{p}\right) = 1$. By quadratic reciprocity, it follows that there are no (non-trivial) solutions for $p \equiv 3 \pmod 4$. □

The last step of the proof uses quadratic reciprocity, which will also be used to prove the new theorem of this chapter.

4.5 Possible triples

Before looking at the new theorem, let us first look at the residues of possible primitive solutions (x, y, z) to equation (4.1) modulo the primes $3, 11$ and 29 when $p > 5$, which will be necessary for the next section. Of course, one can trivially take the set of all possible triples $(x, y, z) \pmod q$, so then there are q^3 options for every prime q. However, it is usually possible (especially for small primes q) to eliminate a large amount of the triples.

Lemma 4.5.1. *The only possible triples* $(x, y, z) \pmod 3$ *that correspond to a non-trivial, primitive solution to equation (4.1) are* $(1, 1, 1)$ *and* $(2, 2, 2)$.

Proof. Suppose that $3 \mid xyz$, then Lemma 4.3.1 shows that $p \mid (4^2 - c_3^2)$ where c_3 is the third coefficient of the rational newform at level 62 and weight 2 see Equation 4.3, so $c_3 = 0$ and hence $(4^2 - c_3^2) = 4^2$. This is only possible if $p = 2$ but $p > 5$ so it follows that $3 \nmid xyz$. Then $x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod 3$. Now consider the condition $0 = x^p + y^p + 31z^p \equiv x + y + z \pmod 3$. The only options are $(1, 1, 1)$ and $(2, 2, 2)$. □

The previous lemma gives such a nice solution because $x^p \equiv x \pmod 3$ for any odd prime p. When one wants to look at solutions modulo the primes 11 and 29 these will depend on p. However since $x^{10} \equiv 1 \pmod{11}$ provided $11 \nmid x$ and similarly $x^{28} \equiv 1 \pmod{29}$ provided $29 \nmid x$ [by Fermat's Little Theorem] it is enough to consider primes p modulo 10 when looking at solutions modulo

11 and primes p modulo 28 when looking at solutions modulo 29. As p is assumed to be odd, and because of Theorem 4.4.2, can assume that $p \equiv 1 \pmod 4$, it is enough to consider the prime p modulo 5 (for 11) and 7 (for 29). Note that the following holds:

Lemma 4.5.2. *Let (x, y, z) be a non-trivial primitive solution to Equation 4.1 with $p > 7$. Then $11 \nmid xyz$ and $29 \nmid xyz$.*

Proof. Suppose that (x, y, z) is a non-trivial primitive solution to Equation 4.1, then because of Lemma 4.3.1 if $p \nmid ((q+1)^2 - c_q^2)$ then $q \nmid xyz$, where c_q is the q-th coefficient of the rational newform of level 62 and weight 2. The rational newform at level 62 is given by Equation 4.3. So $c_{11} = 0$ and $c_{29} = 2$. Then $((11+1)^2 - c_{11}^2)) = 12^2$ and $((29+1)^2 - 2^2) = 896 = 2^7 \cdot 7$. Hence if $p > 7$ is a prime then $p \nmid ((q+1)^2 - c_q^2)$ hence $q \nmid xyz$ for both $q = 11$ and $q = 29$. □

Instead of looking at possible triples (x, y, z) modulo 11 and 29 where (x, y, z) is a solution to the Diophantine equation, it is necessary to start looking at possible triples for (A', B', C') where (A', B', C') is an appropiate permutation of $(x^p, y^p, 31z^p)$. These possible triples are only listed up to permutation. The Hasse bounds for elliptic curves will be used in the algorithm.

Theorem 4.5.3. *(Hasse's theorem for elliptic curves) Let $E(\mathbb{F}_q)$ be the number of points of an elliptic curve E over the finite field with q elements $\mathbb{F}_q$. Then the following inequality holds.*

$$|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$$

Lemma 4.5.4. *Assume (x, y, z) is a non-trivial primitive solution to Equation 4.1 with $p > 7$. The possible triples for $(x^p, y^p, 31z^p)$ modulo 11 (re-*

spectively modulo 29) up to permutation are given by $(\lambda, \lambda, -2\lambda)$ *(respectively* $(\lambda, 2\lambda, -3\lambda)$ *or* $(\lambda, 4\lambda, -5\lambda)$*) where* $\lambda \in \mathbb{F}_{11}^*$ *(respectively* $\lambda \in \mathbb{F}_{29}^*$*).*

Proof. First we construct the elliptic curve F associated to the rational newform of level 62 and weight 2 (see Equation 4.3, it has Cremona reference 62a1). The rest of the proof is is done by running through an algorithm. Let $(A', B', C') = (x^p, y^p, 31z^p)$. First take A', B' any elements in the finite field with 11 (respectively 29) elements. Then $C' = -A' - B'$ since $x^p + y^p + 31z^p = 0$. Now by Lemma 4.3.1, it follows that $11 \nmid xyz$ (respectively $29 \nmid xyz$) and so $A'B'C' \not\equiv 0 \pmod{11}$ (respectively $A'B'C' \not\equiv 0 \pmod{29}$). Next construct the Frey elliptic curve E associated to the solution (x, y, z). As A', B', C' is a permutation of $x^p, y^p, 31z^p$ and since it is unclear what their residues are modulo 4, it is only possible to construct this elliptic curve up to quadratic twist. So the Frey elliptic curve (up to quadratic twist) is $E : Y^2 = X(X - A')(X + B')$. Now because of Proposition 2.2.5 and 2.1.8, it follows that $a_{11}(E) \equiv \pm a_{11}(F) \pmod{p}$ (respectively $a_{29}(E) \equiv \pm a_{29}(F) \pmod{p}$). By the Hasse bound (see Theorem 4.5.3), it follows that $|a_{11}(E) \mp a_{11}(F)| \leq 4\sqrt{11} < 14$ and since $p \mid (a_{11}(E) \mp a_{11}(F))$ and since $p > 10^6$ (by Theorem 4.3.3), it follows that $a_{11}(E) = \pm a_{11}(F)$ (respectively $a_{29}(E) = \pm a_{29}(F)$ since $|a_{29}(E) \mp a_{29}(F)| \leq 4\sqrt{29} < 22$). If the traces line up, the triples is added to the possible triples. Running through the finite set of possibilities for A' and B' in $\mathbb{F}_{11}^*$ (resp. $\mathbb{F}_{29}^*$), the possible triples modulo 11 up to permutation are $(\lambda, \lambda, -2\lambda)$ where $\lambda \in \mathbb{F}_{11}*$. The possible triples modulo 29 up to permutation are either $(\lambda, 2\lambda, -3\lambda)$ or $(\lambda, 4\lambda, -5\lambda)$ where $\lambda \in \mathbb{F}_{29}*$. This completes the proof. □

We also need the following lemma.

Lemma 4.5.5. *Let (x, y, z) be a non-trivial solution to Equation 4.1 with prime exponent $p > 5$. Then the following hold:*

(a) $29 \nmid (xy - z^2)$

(b) The following are equivalent

(i) $11 \mid (xy - z^2)$

(ii) $x^p \equiv y^p \pmod{11}$

(iii) $x \equiv y \equiv z \pmod{11}$

Proof. Suppose (x, y, z) is a non-trivial solution to

$$x^p + y^p + 31z^p = 0.$$

This equation together with the identity

$$(x^p + y^p)^2 - (x^p - y^p)^2 = 4x^p y^p$$

leads to

$$(31z^p)^2 - (x^p - y^p)^2 = 4x^p y^p.$$

Subtracting $4z^{2p}$ from both sides results in

$$(31^2 - 4)z^{2p} - (x^p - y^p)^2 = 4(x^p y^p - z^{2p}).$$

Factoring on the right hand side gives

$$(31^2 - 4)z^{2p} - (x^p - y^p)^2 = 4(xy - z^2)f(x, y, z) \tag{4.5}$$

where $f(x, y, z) \in \mathbb{Z}[x, y, z]$ is a polynomial in x, y, z. Now suppose that $29 \mid (xy - z^2)$. Then since $29 \mid (31^2 - 4)$ and by Equation 4.5 it follows that $29 \mid (x^p - y^p)$. Hence $x^p \equiv y^p \pmod{29}$. This is impossible by Lemma 4.5.4 and hence proves (a). For (b) note that if $x \equiv y \equiv z \pmod{11}$ then $11 \mid (xy - z^2)$, so (*iii*) implies (*i*). If $11 \mid (xy - z^2)$, then by Equation 4.5 and since $11 \mid (31^2 - 4)$ it follows that $11 \mid (x^p - y^p)$. This is equivalent to $x^p \equiv y^p \pmod{11}$ and hence (*i*) implies (*ii*). Now suppose that $x^p \equiv y^p \pmod{11}$. Then by Equation 4.1 it follows that $2x^p + 31z^p \equiv 2x^p - 2z^p \pmod{11}$. Since 11 and 2 are coprime it follows that $x^p \equiv y^p \equiv z^p \pmod{11}$. Note that the finite group homomorphism

$$\begin{aligned} \mathbb{F}_{11}^* &\to \mathbb{F}_{11}^* \\ \alpha &\mapsto \alpha^p \end{aligned}$$

is injective if p and 10 are coprime. Since $p > 5$ is a prime, it follows that p and 10 are coprime. Then since it maps to itself, is follows that the homomorphism is surjective and hence bijective. So if $x^p \equiv y^p \equiv z^p \pmod{11}$ then $x \equiv y \equiv z \pmod{11}$. So (*ii*) implies (*iii*). □

4.6 A specific improvement using quadratic reciprocity

In this section we prove a new result using the modular approach together with quadratic reciprocity. First there are some technical lemmas which are used in the theorem.

Lemma 4.6.1. *Let (x, y, z) be a non-trivial primitive solution to Equation 4.1* *with prime exponent p. Then*

$$\left(\frac{(xy-z^2)/3}{3}\right) = \left(\frac{p}{3}\right).$$

Proof. Let (x, y, z) be a non-trivial primitive solution to Equation 4.1. First we look at $\left(\frac{(xy-z^2)/3}{3}\right)$. This is equivalent to finding if there is a $\beta \in \mathbb{F}_3^*$ such that $xy - z^2 \equiv 3\beta^2 \pmod 9$, which we can determine by looking at the triples mod 9. Recall from Lemma 4.5.1 that without loss of generality $x \equiv y \equiv z \equiv 1 \pmod 3$ (since if $x \equiv y \equiv z \equiv -1 \pmod 3$ we can replace (x, y, z) by $(-x, -y, -z)$). So $x = 1 + 3i$, $y = 1 + 3j$ and $z = 1 + 3k$ for some $i, j, k \in \mathbb{Z}$. Now

$$x^p + y^p + 31z^p = 0$$

implies

$$(1+3i)^p + (1+3j)^p + 31(1+3k)^p \equiv 0 \pmod 9$$

by the Binomial Theorem

$$1 + p3i + 1 + p3j + 4 + p12k \equiv 0 \pmod{9}.$$

Hence

$$6 + p3(i + j + 4k) \equiv 0 \pmod 9$$

which is equivalent to

$$-2/p \equiv i + j + k \pmod{3}. \tag{4.6}$$

Now looking at

$$xy-z^2 \equiv (1+3i)(1+3j)-(1+3k)^2 \equiv 1+3(i+i)-1-6k \equiv 3(i+j-2k) \pmod 9$$

which is equivalent to

$$(xy-z^2)/3 \equiv i+j-2k \equiv i+j+k \equiv -2/p \pmod 3$$

where the last part follows from (4.6). Hence

$$\left(\frac{(xy-z^2)/3}{3}\right) = \left(\frac{-2/p}{3}\right) = \left(\frac{p}{3}\right)$$

which concludes the proof of the lemma. □

Lemma 4.6.2. *Suppose that* (x, y, z) *is a non-trivial primitive solution to Equation 4.1 with prime exponent* p *such that* $x \not\equiv y \pmod{11}$ *then*

$$\left(\frac{(xy-z^2)}{11}\right) = \begin{cases} 1 & p \equiv 1, -2 \pmod 5, \\ -1 & p \equiv -1, 2 \pmod 5. \end{cases}$$

Proof. Now look at $\left(\frac{(xy-z^2)}{11}\right)$. As $x \not\equiv y \pmod{11}$ the only option for the triples A', B', C' to be $x^p, y^p, 31z^p$ using Lemma 4.5.4 is

$$x^p \equiv \lambda, \quad y^p \equiv -2\lambda, \quad 31z^p \equiv \lambda \pmod{11}$$

where $\lambda \in \mathbb{F}_{11}^*$, which is equivalent to

$$x^p \equiv \lambda, \quad y^p \equiv -2\lambda, \quad z^p \equiv 5\lambda \pmod{11}.$$

Note that it is possible to swap x and y but since we are only interested in $xy - z^2$ which is symmetric in x and y we are reduced to just one option. So since

$$\begin{aligned} \mathbb{F}_{11}^* &\to \mathbb{F}_{11}^* \\ \alpha &\mapsto \alpha^p \end{aligned}$$

is a bijection for $p \equiv 1, -1, 3, -3 \pmod{10}$, it has an inverse, namely

$$\begin{aligned} \mathbb{F}_{11}^* &\to \mathbb{F}_{11}^* \\ \alpha &\mapsto \alpha^{p'} \end{aligned}$$

where $pp' \equiv 1 \pmod{10}$. So

$$x^p \equiv \lambda, y^p \equiv -2\lambda, z^p \equiv 5\lambda \pmod{11}$$

is equivalent to

$$x \equiv \lambda^{p'}, y \equiv (-2\lambda)^{p'}, z \equiv (5\lambda)^{p'} \pmod{11}.$$

Hence $xy - z^2 \equiv ((-2)^{p'} - 5^{2p'})\lambda^{2p'} \pmod{11}$. This is a square modulo 11 if and only if $((-2)^{p'} - 5^{2p'})$ is a square modulo 11. For $p \equiv -1, -3 \pmod{10}$ we calculate that $p' \equiv 9, 3 \pmod{10}$ respectively and so $(-2)^9 - 5^{18} \equiv 1 \pmod{11}$ and $(-2)^3 - 5^6 \equiv 9 \pmod{11}$. On the other hand for $p \equiv 1, 3 \pmod{10}$ we have that $p' \equiv 1, 7 \pmod{10}$ respectively. So $((-2)^{p'} - 5^{2p'}) \equiv 6 \pmod{11}$ in both cases, which is not a square modulo 11.

From this it follows that if $p \equiv -1, 2 \pmod{5}$ then $(xy - z^2)$ is a square mod 11, and if $p \equiv 1, -2 \pmod 5$ then $(xy - z^2)$ is not a square modulo 11.

□

Lemma 4.6.3. *Let (x, y, z) be a non-trivial primitive solution to Equation 4.1 with prime exponent p. If $p \equiv \pm 1 \pmod 7$ then $\left(\frac{xy-z^2}{29}\right) = 1$*

Proof. Let (x, y, z) be a non-trivial primitive solution to Equation 4.1 with prime exponent p. Recall from Lemma 4.5.4 that up to reordering $(x^p, y^p, 31z^p)$ either have residues $(\lambda, 2\lambda, -3\lambda)$ or $(\lambda, 4\lambda, -5\lambda)$ modulo 29 where $\lambda \in \mathbb{F}_{29}^*$. Hence $x^p \equiv a\lambda, y^p \equiv b\lambda, 2z^p \equiv c\lambda \pmod{29}$ where a, b, c are either a reordering of $(1, 2, -3)$ or $(1, 4, -5)$. So

$$a + b + c = 0. \tag{4.7}$$

Suppose that $p \equiv 1 \pmod 7$, then $p \equiv 1 \pmod{28}$ since by Theorem 4.4.1 $p \equiv 1 \pmod 4$. So then $x \equiv a\lambda, y \equiv b\lambda, z \equiv (c/2)\lambda \pmod{11}$. Hence

$$\left(\frac{xy - z^2}{29}\right) = \left(\frac{(ab - c^2)/4}{29}\right) = \left(\frac{4ab - c^2}{29}\right)$$

where the first equality holds as $\lambda \in \mathbb{F}_{11}^*$ and the second because 4 is always a square and $29 \nmid 4$. From equation 4.7 we get

$$\left(\frac{4ab - c^2}{29}\right) = \left(\frac{4ab - (-(a + b))^2}{29}\right) = \left(\frac{(a - b)^2}{29}\right).$$

Now since $a \not\equiv b \pmod{29}$ it follows that if $p \equiv 1 \pmod 7$ then $\left(\frac{xy-z^2}{29}\right) = 1$.

If $p \equiv -1 \pmod 7$, then $p \equiv 13 \pmod{28}$ since $p \equiv 1 \pmod 4$ by Theorem 4.4.1. Note that $13 \cdot 13 \equiv 1 \pmod{28}$ and so the map $x \mapsto x^{13}$ is its own inverse in $\mathbb{F}_{29}^*$. So

$$x^p \equiv a\lambda, \qquad y^p \equiv b\lambda, \qquad z^p \equiv c/2\lambda \pmod{29}$$

now gives

$$x \equiv a^{13}\lambda^{13}, \qquad y \equiv b^{13}\lambda^{13}, \qquad z = (c/2)^{13}\lambda^{13} \pmod{29}.$$

And hence

$$\left(\frac{xy - z^2}{29}\right) = \left(\frac{(ab)^{13} - (c/2)^{26}}{29}\right).$$

Recall from 4.7 that $a + b + c = 0$

$$\left(\frac{(ab)^{13} - (c/2)^{26}}{29}\right) = \left(\frac{(ab)^{13} - ((a+b)/2)^{26}}{29}\right).$$

Let $t = a/b \in \mathbb{F}_{29}^*$ then since $29 \nmid b$ so can divide by b^{26} (which is a square).

$$\left(\frac{(ab)^{13} - ((a+b)/2)^{26}}{29}\right) = \left(\frac{(t)^{13} - ((t+1)/2)^{26}}{29}\right)$$

Running through all options in $\mathbb{F}_{29}^*$ it follows that $\left(\frac{(t)^{13} - ((t+1)/2)^{26}}{29}\right) = -1$ only if $t \equiv 3, 10, 14, 27 \pmod{29}$ (and 1 otherwise). As a, b are two different values in either $(1, 2, -3)$, or $(1, 4, -5)$, we check that $a/b \not\equiv 3, 10, 14, 27 \pmod{29}$ for all options for a, b. So if $p \equiv -1 \pmod{7}$ then $\left(\frac{xy - z^2}{29}\right) = 1$ which completes the proof. □

Lemma 4.6.4. *Let (x, y, z) be a non-trivial primitive solution to Equation 4.1* *with prime exponent p such that* $x \equiv y \equiv z \pmod{11}$ *then*

$$\left(\frac{(xy-z^2)/33}{11}\right) = \begin{cases} 1 & \textit{if } p \equiv 2,6,7,8,10 \pmod{11} \\ -1 & \textit{if } p \equiv 1,3,4,5,9 \pmod{11}. \end{cases}$$

Proof. Let (x, y, z) be a non-trivial primitive solution to Equation 4.1 with prime exponent p such that $x \equiv y \equiv z \pmod{11}$. Since $x \equiv y \equiv z \pmod{11}$, we can set $x = a + i \cdot 11$, $y = a + j \cdot 11$ and $z = a + k \cdot 11$ with $a \not\equiv 0 \pmod{11}$ and $i, j, k \in \mathbb{Z}$ by Lemma 4.5.4. So then $x^p + y^p + 31z^p \equiv 0 \pmod{121}$ becomes

$$(a + i \cdot 11)^p + (a + j \cdot 11)^p + 31(a + k \cdot 11)^p \equiv 0 \pmod{121}.$$

By the Binomial formula

$$a^p + p \cdot i \cdot 11 \cdot a^{p-1} + a^p + p \cdot j \cdot 11 \cdot a^{p-1} + 31a^p + 31 \cdot p \cdot k \cdot 11 \cdot a^{p-1} \equiv 0 \pmod{121}.$$

As $a \not\equiv 0 \pmod{11}$, can divide by a^{p-1}

$$33a + 11p(i + j + 31k) \equiv 0 \pmod{121}$$

which is equivalent to $-3a/p \equiv i + j - 2k \pmod{11}$. So then $xy - z^2 \equiv (a+i\cdot 11)(a+j\cdot 11) - (a+k\cdot 11)^2 \equiv a^2 + ij\cdot 121 + a\cdot 11(i+j) - a^2 - k^2\cdot 121 - 22a\cdot k \equiv 11a(i + j - 2k) \pmod{121}$ which is equivalent to $a(i + j - 2k) \equiv -3a^2/p \pmod{11}$ hence only depends on $\left(\frac{-3/p}{11}\right)$. Now $\left(\frac{-3}{11}\right) = -1$ and if $p \equiv 1, 3, 4, 5, 9 \pmod{11}$ then $\left(\frac{1/p}{11}\right) = 1$ and if $p \equiv 2, 6, 7, 8, 10 \pmod{11}$ then $\left(\frac{1/p}{11}\right) = -1$ which completes the proof of the lemma.

□

Theorem 4.6.5. *Suppose that p is an odd prime and one of the following holds:*

- $p \equiv 1 \pmod 3$*,* $p \equiv 1, -2 \pmod 5$*,* $p \equiv \pm 1 \pmod 7$ *and* $p \equiv 2, 6, 7, 8, 10 \pmod{11}$ *(denoted situation 1)*
- $p \equiv -1 \pmod 3$*,* $p \equiv -1, 2 \pmod 5$*,* $p \equiv \pm 1 \pmod 7$ *and* $p \equiv 1, 3, 4, 5, 9 \pmod{11}$ *(denoted situation 2)*

Then there are no non-trivial solutions $(x, y, z) \in \mathbb{Q}^3$ *that satisfy the equation*

$$x^p + y^p + 31z^p = 0.$$

Proof. Let p be a prime in either situation 1 or situation 2. Then $p \neq 7$. Let $(x, y, z) \in \mathbb{Q}^3$ be a non-zero solution to Equation 4.1. Without loss of generality (x, y, z) are pairwise coprime integers. By Theorem 4.3.3 it follows that $p > 10^6$. By Theorem 4.4.2, $p \equiv 1 \pmod 4$. Using the identity

$$(x^p + y^p)^2 - (x^p - y^p)^2 = 4x^p y^p,$$

since (x, y, z) is a solution to Equation 4.1,

$$(31z^p)^2 - (x^p - y^p)^2 = 4x^p y^p$$

holds. Subtracting $4z^{2p}$ from both sides results in

$$(31^2 - 4)z^{2p} - (x^p - y^p)^2 = 4(x^p y^p - z^{2p}).$$

Factoring on the right hand side gives

$$(31^2 - 4)z^{2p} - (x^p - y^p)^2 = 4(xy - z^2)f(x, y, z)$$

where $f(x, y, z) \in \mathbb{Z}[x, y, z]$ is a polynomial in x, y, z. Now since $x \equiv y \equiv z \pmod 3$ by Lemma 4.5.1 and as $31^2 - 4 = 3 \cdot 11 \cdot 29$, it follows that all terms are divisible by 3. Dividing out by 3 gives

$$(11 \cdot 29)z^{2p} - 3((x^p - y^p)/3)^2 = 4/3(xy - z^2)f(x, y, z). \tag{4.8}$$

We also know that $((x^p - y^p)/3)^2$ and $(xy - z^2)/3$ are integers, and the second one is odd (since exactly one of x, y, z is even). Hence

$$(11 \cdot 29)z^{2p} \equiv 3((x^p - y^p)/3)^2 \pmod{|(xy - z^2)/3|}$$

holds so

$$\left(\frac{(11 \cdot 29)z^{2p}}{|(xy - z^2)/3|}\right) = \left(\frac{3((x^p - y^p)/3)^2}{|(xy - z^2)/3|}\right).$$

Suppose z^{2p} and $(xy - z^2)/3$ have a prime factor q in common. Then $q \mid z$ and $q \mid (xy - z^2)$, so $q \mid z$ and $q \mid xy$, so (x, y, z) are not pairwise coprime, which is a contradiction of our assumptions. Hence z^{2p} and $(xy - z^2)/3$ are coprime so

$$\left(\frac{z^{2p}}{(xy - z^2)/3}\right) = 1.$$

Hence

$$\left(\frac{11 \cdot 29}{|(xy - z^2)/3|}\right) = \left(\frac{3((x^p - y^p)/3)^2}{|(xy - z^2)/3|}\right).$$

There are two cases, either $x \equiv y \equiv z \pmod{11}$ which is denoted Case II, or this is not the case (denoted Case I).

At first we assume that we are in Case I. If $((x^p - y^p)/3)$ and $(xy - z^2)/3$ have a prime factor in common then $\left(\frac{11\cdot 29}{|(xy-z^2)/3|}\right) = 0$, which is only possible if there is a prime factor $q \mid 11 \cdot 29$ such that $q \mid (xy - z^2)$. If $q = 11$ then by Lemma 4.5.5 it follows that $x \equiv y \equiv z \pmod{11}$. This is Case II and will be dealt with later in the proof. So we can assume that $q \neq 11$. So this leaves $q = 29$. But by Lemma 4.5.5 $29 \nmid (xy - z^2)$ hence $q \neq 29$. So $(x^p - y^p)/3$ and $(xy - z^2)/3$ are coprime and hence

$$\left(\frac{11 \cdot 29}{|(xy - z^2)/3|}\right) = \left(\frac{3((x^p - y^p)/3)^2}{|(xy - z^2)/3|}\right) = \left(\frac{3}{|(xy - z^2)/3|}\right).$$

This implies

$$\left(\frac{3 \cdot 11 \cdot 29}{|(xy - z^2)/3|}\right) = 1.$$

Since $(3\cdot11\cdot29)$ is odd and exactly one of x, y, z is even and hence $(xy-z^2)/3$ is odd, we can use Jacobi's reciprocity law together with the fact that $(3\cdot11\cdot29) \equiv 1 \pmod 4$ (which implies that $\left(\frac{-1}{3\cdot11\cdot29}\right) = 1$) to show that

$$\left(\frac{(xy - z^2)/3}{3 \cdot 11 \cdot 29}\right) = 1. \tag{4.9}$$

So now we need to look at $(xy - z^2)/3 \pmod{3 \cdot 11 \cdot 29}$, but we can look at each prime in turn.

$$\left(\frac{(xy - z^2)/3}{3 \cdot 11 \cdot 29}\right) = \left(\frac{(xy - z^2)/3}{3}\right)\left(\frac{(xy - z^2)/3}{11}\right)\left(\frac{(xy - z^2)/3}{29}\right).$$

From Lemma 4.6.1

$$\left(\frac{(xy-z^2)/3}{3}\right)=\left(\frac{p}{3}\right)$$

and so

$$\left(\frac{(xy-z^2)/3}{3}\right)=\begin{cases}-1 \text{ if } p\equiv -1 \pmod 3,\\ 1 \text{ if } p\equiv 1 \pmod 3.\end{cases}$$

Now looking at $\left(\frac{(xy-z^2)/3}{11}\right)$, note that $\left(\frac{(1/3)}{11}\right)=1$. By Lemma 4.6.2

$$\left(\frac{(xy-z^2)/3}{11}\right)=\begin{cases}1 \qquad \text{if } p\equiv 1,-2 \pmod 5,\\ -1 \qquad \text{if } p\equiv -1,2 \pmod 5.\end{cases}$$

By Lemma 4.6.3 if $p\equiv \pm1 \pmod 7$ then $(xy-z^2)$ is always a square modulo 29. Also recall that $\left(\frac{(1/3)}{29}\right)=-1$. Hence $\left(\frac{(xy-z^2)/3}{29}\right)=-1$ if $p\equiv\pm1 \pmod 7$. And so

$$\left(\frac{(xy-z^2)/3}{3\cdot 11\cdot 29}\right)=-1 \text{ if } p\equiv -1 \pmod 3 \text{ and } p\equiv -1,2 \pmod 5 \text{ and } p\equiv \pm1 \pmod 7$$

$$\left(\frac{(xy-z^2)/3}{3\cdot 11\cdot 29}\right)=-1 \text{ if } p\equiv 1 \pmod 3 \text{ and } p\equiv 1,-2 \pmod 5 \text{ and } p\equiv \pm1 \pmod 7$$

which contradicts Equation 4.9. So suppose we have a non-trivial primitive solution (x,y,z) to Equation 4.1 with prime exponent p for which $x\equiv y\equiv z \pmod{11}$ does not holds. Then if $p\equiv -1 \pmod 3$ and $p\equiv -1,2 \pmod 5$ and $p\equiv \pm1\pm 7$ we get a contradiction, so there are no such solutions. This is also the case if $p\equiv 1 \pmod 3$ and $p\equiv 1,-2 \pmod 5$ and $p\equiv\pm1 \pmod 7$

Suppose now that we are in Case II (i.e. $x\equiv y\equiv z \pmod{11}$). Then

$(x^p - y^p)/11 \in \mathbb{Z}$, hence by Equation (4.8),

$$29z^{2p} - 33((x^p - y^p)/33)^2 = 4/33(xy - z^2)f(x, y, z).$$

So

$$29z^{2p} \equiv 33((x^p - y^p)/33)^2 \pmod{(xy - z^2)/33}$$

and hence

$$\left(\frac{29z^{2p}}{|(xy - z^2)/33|}\right) = \left(\frac{33((x^p - y^p)/33)^2}{|(xy - z^2)/33|}\right).$$

We know that z^{2p} and $xy - z^2$ have no prime factor in common so

$$\left(\frac{29}{|(xy - z^2)/33|}\right) = \left(\frac{33((x^p - y^p)/33)^2}{|(xy - z^2)/33|}\right).$$

Now by Lemma 4.5.5, we have that $29 \nmid xy - z^2$ so $\left(\frac{29}{|(xy-z^2)/33|}\right) \neq 0$ and so $((x^p - y^p)/33)^2$ and $(xy - z^2)/33$ are coprime. Hence

$$\left(\frac{29}{|(xy - z^2)/33|}\right) = \left(\frac{33((x^p - y^p)/33)^2}{|(xy - z^2)/33|}\right) = \left(\frac{33}{|(xy - z^2)/33|}\right).$$

Now by Lemma 4.5.5 $29 \nmid xy - z^2$, so it follows that

$$\left(\frac{3 \cdot 11 \cdot 29}{|(xy - z^2)/33|}\right) = 1.$$

By Jacobi's reciprocity law as $3 \cdot 11 \cdot 29 \equiv 1 \pmod 4$ and $\left(\frac{-1}{29}\right) = 1$, so

$$\left(\frac{(xy - z^2)/33}{3 \cdot 11 \cdot 29}\right) = 1. \tag{4.10}$$

Again we can look at each of the prime divisors of $3 \cdot 11 \cdot 29$ separately. Since

$\left(\frac{1/11}{3}\right) = -1$ and by Lemma 4.6.1

$$\left(\frac{(xy-z^2)/33}{3}\right) = \begin{cases} 1 & \text{if } p \equiv -1 \pmod 3, \\ -1 & \text{if } p \equiv 1 \pmod 3. \end{cases}$$

From Lemma 4.6.4 we get that

$$\left(\frac{(xy-z^2)/33}{11}\right) = \begin{cases} 1 & \text{if } p \equiv 2,6,7,8,10 \pmod{11} \\ -1 & \text{if } p \equiv 1,3,4,5,9 \pmod{11}. \end{cases}$$

Also $\left(\frac{1/33}{29}\right) = 1$ combined with Lemma 4.6.3 gives

$$\left(\frac{(xy-z^2)/33}{29}\right) = 1 \text{ if } p \equiv \pm 1 \pmod 7.$$

So

$$\left(\frac{(xy-z^2)/33}{3\cdot 11\cdot 29}\right) = -1 \text{ if } p \equiv -1 \pmod 3 \text{ and } p \equiv \pm 1 \pmod 7$$
$$\text{and } p \equiv 1,3,4,5,9 \pmod{11}$$

$$\left(\frac{(xy-z^2)/33}{3\cdot 11\cdot 29}\right) = -1 \text{ if } p \equiv 1 \pmod 3 \text{ and } p \equiv \pm 1 \pmod 7$$
$$\text{and } p \equiv 2,6,7,8,10 \pmod{11}$$

which contradicts Equation 4.10. So suppose we have a non-trivial primitive solution (x, y, z) to Equation 4.1 with prime exponent p for which $x \equiv y \equiv z \pmod{11}$ holds. Then if $p \equiv -1 \pmod 3$ and $p \equiv 1,3,4,5,9 \pmod{11}$ and $p \equiv \pm 1 \pmod 7$ we get a contradiction, so there are no such solutions. This is also the case if $p \equiv 1 \pmod 3$ and $p \equiv 2,6,7,8,10 \pmod{11}$ and $p \equiv \pm 1$

(mod 7). So combining Case I and II gives the result independent if the congruences $x \equiv y \equiv z \pmod{11}$ hold.

□

Chapter 5

Generalizing over totally real fields: preliminaries

From now on we will look at generalized Fermat equations in the form

$$Aa^p + Bb^p + Cc^p = 0, \qquad a, b, c \in \mathcal{O}_K; \tag{5.1}$$

where K is a totally real field. We assume that $A, B, C \in \mathcal{O}_K$ are pairwise coprime, that $A \pm B \pm C \neq 0$ for any choice of signs and that p is bigger than some constant depending only on A, B, C and K. As we extend the field, we need a generalization of modular forms to totally real fields, the so called Hilbert modular forms. For a background on Hilbert modular forms, see [6] and [9]. In this chapter we will present links between elliptic curves over K and Hilbert newforms of parallel weight 2. We finish by redefining the Frey elliptic curve in this context and presenting a level lowering theorem.

5.1 Eichler-Shimura

We will relate a newform (Hilbert newform in the totally real case) of weight two to an elliptic curve (over a totally real field K) as we have done for rational newforms by using the Eichler–Shimura Theorem in [10, Chapter 8]. However, for some totally real number fields this is only conjectured to be possible and hence in that case the results will be conditional on the following.

Conjecture 5.1.1 ("Eichler–Shimura")**.** *Let K be a totally real field. Let $\mathfrak{f}$ be a Hilbert newform of level $\mathcal{N}$ and parallel weight 2, and write $\mathbb{Q}_{\mathfrak{f}}$ for the field generated by its eigenvalues. Suppose that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same* L*-function as $\mathfrak{f}$.*

Blasius [1] proved based on the work from Hida [20] that this conjecture holds for totally real fields of odd degree.

Theorem 5.1.2 (Blasius, Hida)**.** *Let K be a totally real field and let $\mathfrak{f}$ be a Hilbert newform over K of level $\mathcal{N}$ and parallel weight 2, such that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Suppose that $[K : \mathbb{Q}]$ is odd, then there is an elliptic curve $E_{\mathfrak{f}}/K$ of conductor $\mathcal{N}$ with the same* L*-function as $\mathfrak{f}$.*

In the even degree case, we will need the following results from Freitas and Siksek's paper [13] towards Conjecture 5.1.1.

Lemma 5.1.3. *Let E be an elliptic curve over a totally real field K, and p be an odd prime. Suppose $\overline{\rho}_{E,p}$ is irreducible, and that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},p}$ for some Hilbert newform $\mathfrak{f}$ over K of parallel weight 2 with $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. Let $\mathfrak{q} \nmid p$ be a prime ideal of K such that*

(a) E has potentially multiplicative reduction at $\mathfrak{q}$;

(b) $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$*;*

(c) $p \nmid (\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{q}) \pm 1)$*.*

Then there is an elliptic curve $E_{\mathfrak{f}}/K$ *of conductor* $\mathcal{N}$ *having the same* L*-function as* $\mathfrak{f}$*.*

5.2 The Frey curve and its modularity

Let (a, b, c) be a non-trivial solution to Equation 5.1. We shall define the Frey elliptic curve to be one of the following elliptic curves:

$$\begin{aligned} E_1 &: Y^2 = X(X - Aa^p)(X + Bb^p) \\ E_2 &: Y^2 = X(X - Aa^p)(X + Cc^p) \\ E_3 &: Y^2 = X(X - Cc^p)(X + Bb^p) \end{aligned} \tag{5.2}$$

The following lemma, which is an exercise in [34], tells us that these are either isomorphic or quadratic twists of each other.

Lemma 5.2.1. *Let* K *be a totally real number field,* $A', B', C' \in \mathcal{O}_K$ *be non-zero such that* $A' + B' + C' = 0$*. Let* E *be the elliptic curve*

$$E : Y^2 = X(X - A')(X + B')$$

then any permutation of A', B', C' *will give an elliptic curve which is either isomorphic to* E *or its quadratic twist by* -1*.*

Proof. Take any permutations of the triple A', B', C'. We can decompose it into a product of transpositions. We will prove that the elliptic curve resulting from a transposition will be a quadratic twist of E by -1. If the permutation consists of an even (respectively odd) number of transpositions this will result in an even (respectively odd) number of quadratic twists by -1 and hence an isomorphism (respectively quadratic twist by -1) overall. So it suffices to prove that any transposition of the triple A', B', C' results in a quadratic twist by -1. The transposition $(A'B')$ results in

$$E_d : Y^2 = X(X + A')(X - B').$$

If we swap C' with A' (B' respectively), we get the following elliptic curve

$$E' : Y^2 = X(X{+}A'{+}B')(X{+}B') \qquad (E' : Y^2 = X(X{-}A')(X{-}A'{-}B') \text{ respectively })$$

which we can see is isomorphic to E_d via the isomorphism $X \mapsto X - B', Y \mapsto Y$ ($X \mapsto X + A', Y \mapsto Y$ respectively). To see that E_d is the quadratic twist of E by -1 consider the map

$$\begin{aligned} X &\mapsto (\sqrt{-1})^2 X, \\ Y &\mapsto (\sqrt{-1})^3 Y, \end{aligned}$$

which maps E to

$$E^* : -Y^2 = -X(-X - A')(-X + B') = -X(X + A')(X - B')$$

which is equivalent to $E_d : Y^2 = X(X + A')(X - B')$. □

In this thesis we are only concerned with the Frey elliptic curve up to quadratic twist, and hence this lemma allows us to define the Frey elliptic curve in the following explicit way. We can associate to a non-trivial solution (a, b, c) of (5.1) the following Frey elliptic curve

$$E : Y^2 = X(X - Aa^p)(X + Bb^p). \tag{5.3}$$

Recall that $A, B, C, a, b, c \in \mathcal{O}_K$ where K is a totally real number field. Note $AaBbCc \neq 0$ so E is indeed an elliptic curve and moreover E is defined over K. We say that E is **modular** if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that the Hasse–Weil L-function of E is equal to the L-function of $\mathfrak{f}$. It is conjectured that all elliptic curves over totally real fields are modular. We shall need the following recently proved [12] partial results towards this conjecture as used in Freitas and Siksek's paper [13].

Theorem 5.2.2. *Let K be a totally real field. Up to isomorphism over $\overline{K}$, there are at most finitely many non-modular elliptic curves E over K. Moreover, if K is real quadratic, then all elliptic curves over K are modular.*

The following corollary is a generalization of the corollary in [13] and the proof is mainly the same.

Corollary 5.2.3. *Let K be a totally real field. Suppose $A, B, C \in \mathcal{O}_K$ are such that $A \pm B \pm C \neq 0$ for any choice of signs. Then there is some constant $D := D(K, A, B, C)$ depending only on K and A, B, C such that for any non-trivial solution (a, b, c) of the generalized Fermat equation $Ax^p + By^p + Cz^p = 0$, with prime exponent $p > D$, the Frey curve $E_{a,b,c}$ given by Equation 5.3 is modular.*

Proof. Let (a, b, c) be a non-trivial solution to Equation 5.1 and let $E_{a,b,c}$ be the

Frey curve associated to that solution. Write $\lambda = -Bb^p/Aa^p$. The j-invariant of $E_{a,b,c}$ is

$$j(\lambda) = 2^8 \cdot (\lambda^2 - \lambda + 1)^3 \cdot \lambda^{-2}(\lambda - 1)^{-2}.$$

By Theorem 5.2.2, there are at most finitely many possible $\overline{K}$-isomorphism classes of elliptic curves over K that are non-modular. Let $j_1, \dots, j_n \in K$ be the j-invariants of these classes. Hence if the j-invariant of $E_{a,b,c}$ is different from $j_1, \dots, j_n \in K$, then $E_{a,b,c}$ is modular and we are done. Unfortunately (a, b, c) is only a hypothetical solution so we cannot practically calculate $j(\lambda)$ (also since the finiteness of the number of non-modular elliptic curves relies on Faltings' Theorem [11] which is ineffective). In order to get a contradiction we suppose that $j(\lambda) = j_i$ for some i. Note that $j(\lambda) = j_i$ has at most six solutions $\lambda \in K$. Thus there are values $\lambda_1, \dots, \lambda_m \in K$ (with $m \leq 6n$) such that if $\lambda \neq \lambda_k$ for all k then $E_{a,b,c}$ is modular. If $\lambda = \lambda_k$ then

$$(-b/a)^p = (A/B)\lambda_k, \qquad (-c/a)^p = (A/C)(1 - \lambda_k).$$

This pair of equations results in a bound for p unless $-b/a$ and c/a are both roots of unity, but as K is real, the only roots of unity are ±1. So then

$$-b/a = \pm 1, \qquad -c/a = \pm 1.$$

Hence

$$1 = \lambda_k + (1 - \lambda_k) = \pm \frac{B}{A} \pm \frac{C}{A}.$$

So $A \pm B \pm C = 0$ which contradicts the assumption on A, B, C, hence leads to a contradiction. □

Remark. As in [13], the constant D is ineffective: in [12] it is shown that an elliptic curve E over a totally real field K is modular except possibly if it gives rise to a K-point on one of handful of modular curves of genus ≥ 2, and Faltings' Theorem [11] (which is ineffective) gives the finiteness. If K is quadratic, we can take $D = 0$ by Theorem 5.2.2.

5.3 Level lowering

Ribet's Theorem (Theorem 3.2.1 in this thesis) can be used to associate a newform of weight 2 to a rational Frey elliptic curve. In the totally real case, we need a more generalized version of level lowering, which is done by Freitas and Siksek in [13] derived from the works of Fujiwara [17], Jarvis [21] and Rajaei [32]. For this we need the following notation which follows the notation from [13]. As before, K is a totally real field. Let E/K be an elliptic curve of conductor $\mathcal{N}$ and p a rational prime. For a prime ideal $\mathfrak{q}$ of K denote by $\Delta_\mathfrak{q}$ the discriminant of a local minimal model for E at $\mathfrak{q}$. Let

$$\mathcal{M}_p := \prod_{\substack{\mathfrak{q} \| \mathcal{N}, \\ p \mid \mathrm{ord}_\mathfrak{q}(\Delta_\mathfrak{q})}} \mathfrak{q}, \qquad \mathcal{N}_p := \frac{\mathcal{N}}{\mathcal{M}_p}. \tag{5.4}$$

The ideal $\mathcal{M}_p$ is precisely the product of the primes where we want to lower the level. For a Hilbert eigenform $\mathfrak{f}$ over K, denote the field generated by its eigenvalues by $\mathbb{Q}_\mathfrak{f}$. Now we can present the level-lowering recipe which is derived by Freitas and Siksek in [13].

Theorem 5.3.1. *With the above notation, suppose the following*

(i) $p \geq 5$ *and* p *is unramified in* K

(ii) E *is modular,*

(iii) $\overline{\rho}_{E,p}$ *is irreducible,*

(iv) E *is semi-stable at all* $\mathfrak{q} \mid p$*,*

(v) $p \mid \operatorname{ord}_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$ *for all* $\mathfrak{q} \mid p$*.*

Then, there is a Hilbert eigenform $\mathfrak{f}$ *of parallel weight* 2 *that is new at level* $\mathcal{N}_p$ *and some prime* ϖ *of* $\mathbb{Q}_{\mathfrak{f}}$ *such that* $\varpi \mid p$ *and* $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$*.*

Chapter 6

Generalized Fermat equation over totally real number fields: a general and specific result

In this chapter we will prove a result that holds for all totally real number fields for which the solutions to an S-unit equation satisfy certain conditions. Then by parameterizing solutions to this S-unit equation for specific real quadratic number fields we achieve another result. This generalizes a paper of Freitas and Siksek's [13] which looks at the equation

$$a^p + b^p + c^p = 0$$

where $a, b, c \in \mathcal{O}_K$, p is a prime and K is a totally real number field. We use their results following the same steps and generalize them so they can be applied to

$$Aa^p + Bb^p + Cc^p = 0, \qquad a, b, c \in \mathcal{O}_K; \tag{6.1}$$

where A, B, C are odd elements of $\mathcal{O}_K$, K is a totally real field and p is a prime. We say that $A \in \mathcal{O}_K$ is odd if $A \cdot \mathcal{O}_K$ is coprime to $2 \cdot \mathcal{O}_K$. We shall call this equation *the generalized Fermat equation over K with coefficients A, B, C and exponent p.* A solution (a, b, c) is called **trivial** if $abc = 0$, otherwise **non-trivial**. The following notation follows [13] apart from that the set S is enlarged. The notation shall be fixed from now on throughout this thesis.

$$\begin{gathered}
R = \mathrm{Rad}(ABC) = \prod_{\substack{\mathfrak{q} \mid ABC \\ \mathfrak{q} \text{ prime in } K}} \mathfrak{q} \\
S = \{\mathfrak{P} \ : \ \mathfrak{P} \text{ is a prime of } \mathcal{O}_K \text{ such that } \mathfrak{P} \mid 2R\} \qquad (6.2) \\
T = \{\mathfrak{P} \ : \ \mathfrak{P} \text{ is a prime of } \mathcal{O}_K \text{ above } 2\}, \\
U = \{\mathfrak{P} \in T \ : \ f(\mathfrak{P}/2) = 1\}, \qquad V = \{\mathfrak{P} \in T \ : \ 3 \nmid \mathrm{ord}_{\mathfrak{P}}(2)\}
\end{gathered}$$

where $f(\mathfrak{P}/2)$ denotes the residual degree of $\mathfrak{P}$. As in [13], we need an assumption which we refer to throughout this thesis as (ES):

$$\textbf{(ES)} \qquad \begin{cases} \text{either } [K : \mathbb{Q}] \text{ is odd;} \\ \text{or } U \neq \emptyset; \\ \text{or Conjecture 5.1.1 (see Section 5.1) holds for } K. \end{cases}$$

Remark. Note that in the paper of Freitas and Siksek [13] the set S only contains the prime ideals above 2, and hence is a smaller set than the set we are working with as our set S contains all prime ideals dividing $2R$.

6.1 Irreducibility of mod p representations of elliptic curves

Next we want to associate a Hilbert newform to this Frey elliptic curve. We will use the level lowering section of the previous chapter. In the rational case, we required the Frey elliptic curve to not have any p-isogenies. For totally real fields this condition is often expressed as saying that the mod p Galois representation associated to the Frey elliptic curve is irreducible (see Theorem 2.1.18). The following theorem of Freitas and Siksek [13, Theorem 2], building on earlier work of David [7], Momose [30] and Merel [29], is sufficient for this chapter.

Theorem 6.1.1. *Let K be a totally real field. There is an effective constant $\mathcal{C}_K$, depending only on K, such that the following holds. If $p > \mathcal{C}_K$ is a rational prime, and E is an elliptic curve over K which is semi-stable at some $\mathfrak{q} \mid p$, then $\overline{\rho}_{E,p}$ is irreducible.*

6.2 Conductor calculations

In order to calculate the level of the Hilbert eigenform associated to the Frey elliptic curve we need to calculate the conductor of the Frey elliptic curve corresponding to a non-trivial solution (a, b, c) of the Fermat equation (6.1).

6.2.1 Local computations

The conductor calculations in [13] are proved in greater generality than necessary for that paper. This generalization suffices for the Frey curve associated to the generalized Fermat equation (6.1) and so this section follows the paper very closely. Let u, v, $w \in \mathcal{O}_K$ be such that $uvw \neq 0$ and $u + v + w = 0$. Let

$$E : y^2 = x(x-u)(x+v). \tag{6.3}$$

This is an elliptic curve with full 2-torsion and with invariants c_4, c_6, Δ, j (with the usual notation for elliptic curves) that are given by:

$$\begin{gathered} c_4 = 16(u^2 - vw) = 16(v^2 - wu) = 16(w^2 - uv), \\ c_6 = -32(u-v)(v-w)(w-u), \qquad \Delta = 16u^2v^2w^2, \qquad j = \frac{c_4^3}{\Delta}. \end{gathered} \tag{6.4}$$

The following lemma is proved using Silverman [35, Sections VII.1 and VII.5]. (The lemma is stated without proof in [13]).

Lemma 6.2.1. *With the above notation, let $\mathfrak{q} \nmid 2$ be a prime and let*

$$s = \min\{\mathrm{ord}_{\mathfrak{q}}(u), \mathrm{ord}_{\mathfrak{q}}(v), \mathrm{ord}_{\mathfrak{q}}(w)\}.$$

Write $E_{\min}$ for a local minimal model at $\mathfrak{q}$.

(i) $E_{\min}$ has good reduction at $\mathfrak{q}$ if and only if s is even and

$$\mathrm{ord}_{\mathfrak{q}}(u) = \mathrm{ord}_{\mathfrak{q}}(v) = \mathrm{ord}_{\mathfrak{q}}(w). \tag{6.5}$$

(ii) $E_{\min}$ has multiplicative reduction at $\mathfrak{q}$ if and only if s is even and (6.5) *fails to hold. In this case the minimal discriminant $\Delta_{\mathfrak{q}}$ at $\mathfrak{q}$ satisfies*

$$\mathrm{ord}_{\mathfrak{q}}(\Delta_{\mathfrak{q}}) = 2\,\mathrm{ord}_{\mathfrak{q}}(u) + 2\,\mathrm{ord}_{\mathfrak{q}}(v) + 2\,\mathrm{ord}_{\mathfrak{q}}(w) - 6s.$$

(iii) $E_{\min}$ *has additive reduction if and only if* s *is odd.*

Proof. Let π be the uniformizer of $K_{\mathfrak{q}}$. Suppose that the Weierstrass equation of E is not in minimal form. Then by the contrapositive of Lemma 2.1.9 we have that $\operatorname{ord}_{\mathfrak{q}}(\Delta) \geq 12$. Now since $\pi \nmid 2$, we have that $\pi \mid uvw$. Without loss of generality, $\pi \mid u$. By the contrapositive of the same lemma $\operatorname{ord}_{\mathfrak{q}}(c_4) \geq 4$ and hence $\pi \mid vw$. As $u + v + w = 0$, we have that $\pi \mid u$, $\pi \mid v$ and $\pi \mid w$. Now suppose that $\pi^2 \nmid u$. Then since $\pi^4 \mid c_4$ we have that $\pi^4 \nmid vw$. And so

$$\operatorname{ord}_{\mathfrak{q}}(\Delta) = 2 \operatorname{ord}_{\mathfrak{q}}(uvw) = 2(\operatorname{ord}_{\mathfrak{q}}(u) + \operatorname{ord}_{\mathfrak{q}}(v) + \operatorname{ord}_{\mathfrak{q}}(w)) < 10$$

which is a contradiction. Hence $\pi^2 \mid u$, $\pi^2 \mid v$ and $\pi^2 \mid w$. Now we can use the following change of coordinates

$$x \mapsto \pi^2 x',$$
$$y \mapsto \pi^3 y',$$

to get

$$E' : (y')^2 = x'(x' - \pi^{-2}u)(x' - \pi^{-2}v).$$

Here $\Delta' = \pi^{-12}\Delta$, $c_4' = \pi^{-4}c_4$. We can keep repeating this until the equation is minimal. So now suppose that we have done the following change of coordinates

$$x \mapsto t^2 x',$$
$$y \mapsto t^3 y',$$

to get

$$E' : (y')^2 = x'(x' - t^{-2}u)(x' - t^{-2}v).$$

If the equation was minimal from the start we can take $t = 1$, if not $t = \pi^s$ where s is the number of times we had to do a change of coordinates to get the minimal form. In this minimal form with respect to $\mathfrak{q}$ we have that $u' = t^{-2}u, v' = t^{-2}v$ and $w' = -(u' + v') = -t^{-2}(u + v) = t^{-2}w$. We use theorem 2.1.11 from chapter 2 of this thesis. Applying 2.1.11 (i), we get that E' has good reduction if and only if $\mathrm{ord}_{\mathfrak{q}}(\Delta') = 0$, which is equivalent to $\mathrm{ord}_{\mathfrak{q}}(u'v'w') = 0$ so this holds if and only if $\mathrm{ord}_{\mathfrak{q}}(u') = \mathrm{ord}_{\mathfrak{q}}(v') = \mathrm{ord}_{\mathfrak{q}}(w') = 0$. This is equivalent to $\mathrm{ord}_{\mathfrak{q}}(u) = \mathrm{ord}_{\mathfrak{q}}(v) = \mathrm{ord}_{\mathfrak{q}}(w) = 2\mathrm{ord}_{\mathfrak{q}}(t)$ which proves (i) of this lemma. Using 2.1.11 (ii) we know that E' has multiplicative reduction if and only if $\mathrm{ord}_{\mathfrak{q}}(\Delta') > 0$ and $\mathrm{ord}_{\mathfrak{q}}(c_4') = 0$. This is equivalent to $\pi \mid u'v'w'$ and $\pi \nmid (w'^2 - u'v')$ where $w'^2 - u'v' = v'^2 - w'u' = u'^2 - v'w'$. Note that u', v', w' are symmetric so without loss of generality if $\pi \mid u'v'w'$ we can assume that $\pi \mid u'$. So then as $u' + v' + w' = 0$ have $w'^2 - u'v' = w'^2 + u'(u' + w') = w'^2 + u'^2 + u'w'$ and hence $\pi \mid u'$ and $\pi \nmid c'^4$ if and only if $\pi \mid u'$ and $\pi \nmid w'$. So from $u' + v' + w' = 0$ it immediately follows that $\pi \nmid v'$. So since $\mathrm{ord}_{\mathfrak{q}}(u) = \mathrm{ord}_{\mathfrak{q}}(u') + 2t$, $\mathrm{ord}_{\mathfrak{q}}(v) = \mathrm{ord}_{\mathfrak{q}}(v') + 2t$ and $\mathrm{ord}_{\mathfrak{q}}(w) = \mathrm{ord}_{\mathfrak{q}}(w') + 2t$ and we know exactly one of $\mathrm{ord}_{\mathfrak{q}}(u'), \mathrm{ord}_{\mathfrak{q}}(v'), \mathrm{ord}_{\mathfrak{q}}(w')$ is positive it follows that s is even and $\mathrm{ord}_{\mathfrak{q}}(u) = \mathrm{ord}_{\mathfrak{q}}(v) = \mathrm{ord}_{\mathfrak{q}}(w)$ does not hold. If conversely s is even and $\mathrm{ord}_{\mathfrak{q}}(u) = \mathrm{ord}_{\mathfrak{q}}(v) = \mathrm{ord}_{\mathfrak{q}}(w)$ does not hold, then it follows without loss of generality that $\mathrm{ord}_{\mathfrak{q}}(u) > \mathrm{ord}_{\mathfrak{q}}(v)$ so when taking an appropriate value for t, we have $\mathrm{ord}_{\mathfrak{q}}(v') = 0$. Then from $u' + v' + w' = 0$ it follows that $\pi \mid \Delta'$ and $\pi \nmid c_4'$. Moreover, $\mathrm{ord}_{\mathfrak{q}}(\Delta') = \mathrm{ord}_{\mathfrak{q}}(\Delta) - 12t = \mathrm{ord}_{\mathfrak{q}}(u) + \mathrm{ord}_{\mathfrak{q}}(v) + \mathrm{ord}_{\mathfrak{q}}(w) - 6s$ which proves (ii) of this lemma. Finally from 2.1.11 (iii) we know that E' has additive reduction at $\mathfrak{q}$ if and only if $\mathrm{ord}_{\mathfrak{q}}(\Delta') > 0$ and $\mathrm{ord}_{\mathfrak{q}}(c_4') > 0$. From $\mathrm{ord}_{\mathfrak{q}}(\Delta') > 0$ it follows without loss of generality that $\pi \mid u'$. The proof of (ii) shows us that if π divides exactly one of u', v', w' then $\mathrm{ord}_{\mathfrak{q}}(c_4') = 0$. This is a contradiction, hence we know that π divides at least two of u', v', w'. Now from $u' + v' + w' = 0$ it follows that π divides each of u', v', w'. If π^2 divides each of them, then E' is not minimal Weierstrass form, which is a contradiction and hence s is odd. Conversely if s is odd, suppose we put the equation in minimal Weierstrass form at $\mathfrak{q}$. Then the exponent of π will only decrease by an even number and hence π divides each of u', v', w' and so $\pi \mid \Delta'$ and $\pi \mid c_4'$ which completes the proof.

□

6.2.2 Conductor of the Frey curve

Recall that when we look at the generalized Fermat equation

$$Aa^p + Bb^p + Cc^p = 0$$

over $\mathbb{Z}$, we can scale the solution such that a, b, c are coprime because prime factorization is unique. However in $\mathcal{O}_K$ this is not always that case. If the class number of 1, this will be possible but not in general. So let (a, b, c) be a non-trivial solution to the Fermat equation (6.1), write

$$\mathcal{G}_{a,b,c} = a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K, \tag{6.6}$$

If $K = \mathbb{Q}$ then $\mathcal{G}_{a,b,c} = a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z} = \gcd(a, b, c)\mathbb{Z}$ so we can think of $\mathcal{G}_{a,b,c}$ as the greatest common divisor of a, b, c generalized to number fields. If

$\mathcal{G}_{a,b,c}$ is principal, we can divide out by this greatest common divisor and so if there is a solution we assume that (after scaling by the generator of this principal ideal) that the solution is primitive. However, this will not always be principal, but by the finiteness of the class group of K we can scale a, b, c such that $\mathcal{G}_{a,b,c}$ belongs to a finite set (see below). From Lemma 6.2.1, it follows that the primes that divide all of a, b, c can be additive primes for the Frey curve. Note that the level lowering recipe given above does not remove additive primes and so to be able to control the final level we need to control $\mathcal{G}_{a,b,c}$. Following [13], we fix a set

$$\mathcal{H} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_h\}$$

of prime ideals $\mathfrak{m}_i \nmid 2R$, which is a set of representatives for the ideal classes of $\mathcal{O}_K$. For a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we denote by $[\mathfrak{a}]$ the class of $\mathfrak{a}$ in the class group. We denote $[\mathcal{G}_{a,b,c}]$ by $[a, b, c]$. The following is Lemma 3.2 of [13], and states that we can always scale our solution (a, b, c) so that the greatest common divisor belongs to $\mathcal{H}$. This set is different from [13] but the following lemma and its proof work in exactly the same way.

Lemma 6.2.2. *Let (a, b, c) be a non-trivial solution to (6.1). There is a non-trivial integral solution (a', b', c') to (6.1) such that the following hold.*

(i) For some $\xi \in K^*$,

$$a' = \xi a, \qquad b' = \xi b, \qquad c' = \xi c.$$

(ii) $\mathcal{G}_{a',b',c'} = \mathfrak{m} \in \mathcal{H}$.

(iii) $[a', b', c'] = [a, b, c]$.

Proof. Let $\mathfrak{m} \in \mathcal{H}$ satisfy $[\mathcal{G}_{a,b,c}] = [\mathfrak{m}]$. Thus there is some $\xi \in K^*$ such that $\mathfrak{m} = (\xi) \cdot \mathcal{G}_{a,b,c}$. Let a', b', c' be as in (i). We want to show that a', b', c' are in $\mathcal{O}_K$. Note

$$(a') = (\xi) \cdot (a) = \mathfrak{m} \cdot \mathcal{G}_{a,b,c}^{-1} \cdot (a)$$

which is an integral ideal, since $\mathcal{G}_{a,b,c}$ (by its definition) divides a. Thus a' is in $\mathcal{O}_K$ and similarly so are b' and c'.

For (ii), note that

$$\mathcal{G}_{a',b',c'} = a'\mathcal{O}_K + b'\mathcal{O}_K + c'\mathcal{O}_K = (\xi) \cdot (a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K) = (\xi) \cdot \mathcal{G}_{a,b,c} = \mathfrak{m}.$$

And finally for (iii)

$$[a, b, c] = [\mathcal{G}_{a,b,c}] = [\mathfrak{m}] = [\mathcal{G}_{a',b',c'}] = [a', b', c']$$

□

So as in [13] this lemma allows us to control the greatest common divisor of a non-trivial solution of the Fermat equation, as we can assume after suitable scaling that it belongs to the finite set of prime ideals $\mathcal{H}$. As a consequence (Lemma 6.2.3 below), the Frey curve (5.3) can be assumed to be semi-stable outside $S \cup \mathcal{H}$, where S is defined in (6.2). Hence now we can compute the level lowering level $\mathcal{N}_p$ which together with the proof holds in the same way as in [13].

Lemma 6.2.3. *Let* (a, b, c) *be a non-trivial solution to the Fermat equation* (6.1) *with odd prime exponent* p*, and scaled as in Lemma 6.2.2 so that* $\mathcal{G}_{a,b,c} =$

$\mathfrak{m} \in \mathcal{H}$.

Write $E = E_{a,b,c}$ for the Frey curve in (5.3)*, and let Δ be its discriminant. For a prime $\mathfrak{q}$ we write $\Delta_{\mathfrak{q}}$ for the minimal discriminant at $\mathfrak{q}$. Then at all $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$, the model E is minimal, semi-stable, and satisfies $p \mid \operatorname{ord}_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$. Let $\mathcal{N}$ be the conductor of E, and let $\mathcal{N}_p$ be as defined in* (5.4)*. Then*

$$\mathcal{N} = \mathfrak{m}^{s_{\mathfrak{m}}} \cdot \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r_{\mathfrak{P}}} \cdot \prod_{\substack{\mathfrak{q} \mid abc \\ \mathfrak{q} \notin S \cup \{\mathfrak{m}\}}} \mathfrak{q}\,, \qquad \mathcal{N}_p = \mathfrak{m}^{s'_{\mathfrak{m}}} \cdot \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r'_{\mathfrak{P}}}, \tag{6.7}$$

where $0 \le r'_{\mathfrak{P}} \le r_{\mathfrak{P}} \le 2 + 6 \operatorname{ord}_{\mathfrak{P}}(2)$ for $\mathfrak{P} \mid 2$, and $0 \le r'_{\mathfrak{P}} \le r_{\mathfrak{P}} \le 2$ for $\mathfrak{P} \mid R$, and $0 \le s'_{\mathfrak{m}} \le s_{\mathfrak{m}} \le 2$.

Proof. The discriminant of the model given by E is $16(ABC)^2(abc)^{2p}$, thus the primes appearing in $\mathcal{N}$ will be either primes dividing $2R$ or dividing abc. For $\mathfrak{P} \mid 2$ we have $r_{\mathfrak{P}} = \operatorname{ord}_{\mathfrak{P}}(\mathcal{N}) \le 2 + 6 \operatorname{ord}_{\mathfrak{P}}(2)$ by [36, Theorem IV.10.4]; this proves the correctness of the bounds for the exponents in $\mathcal{N}$ and $\mathcal{N}_p$ at even primes, and we will restrict our attention to odd primes. As E has full 2-torsion over K, the wild part of the conductor of E/K vanishes ([36], page 380) at all odd $\mathfrak{q}$, and so $\operatorname{ord}_{\mathfrak{q}}(\mathcal{N}_p) \le \operatorname{ord}_{\mathfrak{q}}(\mathcal{N}) \le 2$. This proves the correctness of the bounds for the exponents in $\mathcal{N}$ and $\mathcal{N}_p$ at $\mathfrak{q}$ that divide R and for $\mathfrak{q} = \mathfrak{m}$.

It remains to consider $\mathfrak{q} \mid abc$ satisfying $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$. From Lemma 6.2.1 we deduce that the model (5.3) is minimal and has multiplicative reduction at such $\mathfrak{q}$, and it is therefore clear that $p \mid \operatorname{ord}_{\mathfrak{q}}(\Delta) = \operatorname{ord}_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$. It follows that $\operatorname{ord}_{\mathfrak{q}}(\mathcal{N}) = 1$ and, from the recipe for $\mathcal{N}_p$ in (5.4) that $\operatorname{ord}_{\mathfrak{q}}(\mathcal{N}_p) = 0$. This completes the proof.

□

6.3 Level lowering and Eichler–Shimura

To apply the level lowering recipe, we need the following from Freitas and Siksek's paper [13]

Lemma 6.3.1. *Let E be an elliptic curve over a number field K. Suppose that $4 \mid \#E(\mathbb{F}_\mathfrak{q})$ for all but finitely many primes $\mathfrak{q}$ of good reduction for E. Then either E has full 2-torsion, or it is 2-isogenous to some elliptic curve E' having full 2-torsion.*

We also need the following image of inertia lemmas before we can lower the level. The first one is straight from the paper of Freitas and Siksek [13]:

Lemma 6.3.2. *Let E be an elliptic curve over K with j-invariant j. Let $p \geq 5$ and $\mathfrak{q} \nmid p$ be a prime in K. Then $p \mid \#\overline{\rho}_{E,p}(I_\mathfrak{q})$ if and only if E has potentially multiplicative reduction at $\mathfrak{q}$ (i.e. $v_\mathfrak{q}(j) < 0$) and $p \nmid v_\mathfrak{q}(j)$.*

The next lemma needs to be adjusted to our Frey curve.

Lemma 6.3.3. *Let $\mathfrak{q} \notin S$. Let (a, b, c) be a solution to the Fermat equation (6.1) with prime exponent $p \geq 5$ such that $\mathfrak{q} \nmid p$. Let $E := E_{a,b,c}$ be the Frey curve in (5.3). Then $p \nmid \#\overline{\rho}_{E,p}(I_\mathfrak{q})$.*

Proof. Using the previous lemma, it is enough to show that at all $\mathfrak{q} \notin S$, with $\mathfrak{q} \nmid p$ then either $v_\mathfrak{q}(j) \geq 0$, or $p \mid v_\mathfrak{q}(j)$. Now, since $\mathfrak{q} \notin S$, we know that $\mathfrak{q} \nmid ABC$, so if $\mathfrak{q} \mid uvw$ (in the notation of previous section) then $\mathfrak{q} \mid abc$ (as we put $\{u, v, w\} = \{Aa^p, Bb^p, Cc^p\}$). Also if $\mathfrak{q} \nmid \Delta$, then E has good reduction at $\mathfrak{q}$ so $v_\mathfrak{q}(j) \geq 0$. So suppose $\mathfrak{q} \mid \Delta$. As $\mathfrak{q} \nmid 2$, we have that $\mathfrak{q} \mid uvw$, and hence $\mathfrak{q} \mid abc$. If all the valutions are equal (say $v_\mathfrak{q}(a) = v_\mathfrak{q}(b) = v_\mathfrak{q}(c) = v_1$) then we can show that $v_\mathfrak{q}(j) \geq 0$ by contradiction: suppose not, then as $j = \frac{c_4^3}{\Delta}$, we have that $3v_{\mathfrak{q}}(c_4) < 6pv_1$. Now note that $v_{\mathfrak{q}}(c_4) = v_{\mathfrak{q}}(u^2 - vw) \geq 2pv_1$. So we get $6pv_1 \leq 3v_{\mathfrak{q}}(c_4) < 6pv_1$. This is a contradiction.

Now suppose that not all the valuations are equal. Without loss of generality, $v_{\mathfrak{q}}(a) < v_{\mathfrak{q}}(b)$. So then since $\mathfrak{q} \nmid ABC$ it follows that $v_{\mathfrak{q}}(Aa^p) < v_{\mathfrak{q}}(Bb^p)$. So then by the Ultrametric Inequality it follows that $v_{\mathfrak{q}}(Cc^p) = \min(v_{\mathfrak{q}}(-Aa^p), v_{\mathfrak{q}}(-Bb^p)) = v_{\mathfrak{q}}(Aa^p)$. So $v_{\mathfrak{q}}(a) = v_{\mathfrak{q}}(c) < v_{\mathfrak{q}}(b)$ We will prove that $p \mid v_{\mathfrak{q}}(j)$. From the j-invariant, we get that

$$v_{\mathfrak{q}}(j) = 3v_{\mathfrak{q}}(c_4) - v_{\mathfrak{q}}(\Delta) = 3v_{\mathfrak{q}}(c_4) - 2v_{\mathfrak{q}}(uvw) = 3v_{\mathfrak{q}}(c_4) - 2pv_{\mathfrak{q}}(abc),$$

so $p \mid v_{\mathfrak{q}}(j)$ if an only if $p \mid v_{\mathfrak{q}}(c_4) = \min(v_{\mathfrak{q}}(u^2), v_{\mathfrak{q}}(vw))$ (last equality is true since we assume that $v_{\mathfrak{q}}(a) = v_{\mathfrak{q}}(c) < v_{\mathfrak{q}}(b)$). But as $p \mid v_{\mathfrak{q}}(u)$, $p \mid v_{\mathfrak{q}}(v)$ and $p \mid v_{\mathfrak{q}}(w)$, we see that $p \mid v_{\mathfrak{q}}(c_4)$ hence $p \mid v_{\mathfrak{q}}(j)$.

□

We need the following lemma derived in [13] from Kraus [23].

Lemma 6.3.4. *(Kraus) Let E be an elliptic curve over K, and let $p \geq 3$. Let $\mathfrak{P} \in T$ and suppose that E has potentially good reduction at $\mathfrak{P}$. Let Δ be the discriminant of E (not necessarily minimal at $\mathfrak{P}$). Then $3 \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$ if and only if $3 \nmid v_{\mathfrak{P}}(\Delta)$.*

The following lemma and proof come from Freitas and Siksek [13] but it is modified slightly for our setting. For the definition of U, T and V see (6.2).

Lemma 6.3.5. *Let $\mathfrak{P} \in T$. Let (a, b, c) be a solution to the Fermat equation* (6.1) *with prime exponent $p > 4\,\mathrm{ord}_{\mathfrak{P}}(2)$. Let $E = E_{a,b,c}$ be the Frey curve in* (5.3).

(i) If $\mathfrak{P} \in U$ then E has potentially multiplicative reduction at $\mathfrak{P}$, and $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.

(ii) If $\mathfrak{P} \in V$ then either E has potentially multiplicative reduction at $\mathfrak{P}$ and $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$, or E has potentially good reduction at $\mathfrak{P}$ and $3 \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.

Proof. First suppose that $\mathfrak{P} \in U$. Let π be a uniformizer for $K_{\mathfrak{P}}$. Let

$$t = \min\{\mathrm{ord}_{\mathfrak{P}}(a), \mathrm{ord}_{\mathfrak{P}}(b), \mathrm{ord}_{\mathfrak{P}}(c)\}, \qquad \alpha = \pi^{-t}a, \qquad \beta = \pi^{-t}b, \qquad \gamma = \pi^{-t}c.$$

Then α, β, $\gamma \in \mathcal{O}_{\pi}$. As $\mathfrak{P} \nmid ABC$, we have that $A, B, C \in \mathcal{O}_{\pi}$. By the definition of U, the prime $\mathfrak{P}$ has residue field $\mathbb{F}_2$. As $A\alpha^p + B\beta^p + C\gamma^p = 0$, precisely one of $A\alpha^p$, $B\beta^p$, $C\gamma^p$ is divisible by π. But as $\mathfrak{P} \nmid ABC$, it follows that one of α, β, γ is divisible by π. Thus $\mathrm{ord}_{\mathfrak{P}}(a)$, $\mathrm{ord}_{\mathfrak{P}}(b)$, $\mathrm{ord}_{\mathfrak{P}}(c)$ are not all equal; two out of a, b, c have valuation t (say) and one has valuation $t+k$ with $k \geq 1$. From the formulae in (6.4) we have $\mathrm{ord}_{\mathfrak{P}}(j) = 8\,\mathrm{ord}_{\mathfrak{P}}(2) - 2kp$. As $p > 4\,\mathrm{ord}_{\mathfrak{P}}(2)$, we see that $\mathrm{ord}_{\mathfrak{P}}(j) < 0$ and $p \nmid \mathrm{ord}_{\mathfrak{P}}(j)$. Thus (i) follows from Lemma 6.3.2. Now assume that $\mathfrak{P} \in V$. Recall that

$$v_{\mathfrak{P}}(j) = 3v_{\mathfrak{P}}(c_4) - v_{\mathfrak{P}}(\Delta) = 8v_{\mathfrak{P}}(2) + 3v_{\mathfrak{P}}(u^2 - vw) - 2v_{\mathfrak{P}}(uvw)$$

where $\{u, v, w\} = \{Aa^p, Bb^p, Cc^p\}$.

Note that, since $Aa^p + Bb^p + Cc^p = 0$, and $\mathfrak{P} \nmid ABC$, either $v_{\mathfrak{P}}(a) = v_{\mathfrak{P}}(b) = v_{\mathfrak{P}}(c)$, say t, or two of them are equal and one is bigger. In this second case note that as $\mathfrak{P} \nmid ABC$, in that case (without loss of generality) we may suppose that $v_{\mathfrak{P}}(a) = v_{\mathfrak{P}}(b) = t$ and $v_{\mathfrak{P}}(c) = t + k$ where $k \geq 1$.

Suppose we are in the first case, i.e. we assume that $v_{\mathfrak{P}}(a) = v_{\mathfrak{P}}(b) =$

$v_{\mathfrak{P}}(c) = t$ then

$$v_{\mathfrak{P}}(j) \geq 8v_{\mathfrak{P}}(2) + 6pt - 6pt = 8v_{\mathfrak{P}}(2) > 0$$

So E has potentially good reduction at $\mathfrak{P}$. Note that in this case

$$v_{\mathfrak{P}}(\Delta) = 4v_{\mathfrak{P}}(2) + 6tp.$$

As $\mathfrak{P} \in V$, $3 \nmid v_{\mathfrak{P}}(2)$ which implies $3 \nmid v_{\mathfrak{P}}(\Delta)$, so by the previous lemma, we have that $3 \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$.

Now suppose that we are in the second case, i.e. we assume that $v_{\mathfrak{P}}(a) = v_{\mathfrak{P}}(b) = t$ and $v_{\mathfrak{P}}(c) = t + k$ where $k \geq 1$. Then

$$v_{\mathfrak{P}}(j) = 8v_{\mathfrak{P}}(2) + 6pt - 2p(3t + k) = 8v_{\mathfrak{P}}(2) - 2pk$$

Now $p > 4v_{\mathfrak{P}}(2)$, so $v_{\mathfrak{P}}(j) < 0$ and $p \nmid v_{\mathfrak{P}}(j)$. So E has potentially multiplicative reduction at $\mathfrak{P}$ and $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$ by Lemma 6.3.2, which concludes the proof.

□

Now we can finally lower the level as in [13].

Theorem 6.3.6. *Let K be a totally real field satisfying (ES). Let A, B, $C \in \mathcal{O}_K$ be odd. There is a constant $\mathcal{B} = \mathcal{B}(K, A, B, C)$ depending only on K and A, B, C such that the following hold. Let (a, b, c) be a non-trivial solution to the generalized Fermat equation* (6.1) *with prime exponent $p > \mathcal{B}$, and rescale (a, b, c) as in Lemma 6.2.2 so that it remains integral and satisfies $\mathcal{G}_{a,b,c} = \mathfrak{m}$ for some $\mathfrak{m} \in \mathcal{H}$. Write $E = E_{a,b,c}$ for the Frey curve given in* (5.3). *Then* *there is an elliptic curve E' over K such that*

(i) the conductor of E' is divisible only by primes in $S \cup \{\mathfrak{m}\}$;

(ii) $\#E'(K)[2] = 4$;

(iii) $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$;

Write j' for the j-invariant of E'. Then,

(a) for $\mathfrak{P} \in U$, we have $\mathrm{ord}_{\mathfrak{P}}(j') < 0$;

(b) for $\mathfrak{P} \in V$, we have either $\mathrm{ord}_{\mathfrak{P}}(j') < 0$ or $3 \nmid \mathrm{ord}_{\mathfrak{P}}(j')$;

(c) for $\mathfrak{q} \notin S$, we have $\mathrm{ord}_{\mathfrak{q}}(j') \geq 0$.

In particular, E' has potentially good reduction away from S.

Proof. We first observe, by Lemma 6.2.3, that E is semi-stable outside $S \cup \{\mathfrak{m}\}$. By taking $\mathcal{B}$ to be sufficiently large, we see from Corollary 5.2.3 that E is modular, and from Theorem 6.1.1 that $\overline{\rho}_{E,p}$ is irreducible. Applying Theorem 5.3.1 and Lemma 6.2.3 we see that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ for a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}_p$ and some prime $\varpi \mid p$ of $\mathbb{Q}_{\mathfrak{f}}$. Here $\mathbb{Q}_{\mathfrak{f}}$ is the field generated by the Hecke eigenvalues of $\mathfrak{f}$. Note from Lemma 6.2.3 that there is a finite set of explicit options for $\mathcal{N}_p$, namely $cN_p = \mathfrak{m}^{s'_{\mathfrak{m}}} \cdot \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r'_{\mathfrak{P}}}$, where $0 \leq r'_{\mathfrak{P}} \leq 2 + 6\,\mathrm{ord}_{\mathfrak{P}}(2)$ for $\mathfrak{P} \mid 2$, and $0 \leq r'_{\mathfrak{P}} \leq 2$ for $\mathfrak{P} \mid R$, and $0 \leq s'_{\mathfrak{m}} \leq 2$. Hence $\mathcal{N}_p$ depends on $\mathfrak{m} \in \mathcal{H}$, where $\mathcal{H}$ is a fixed finite set depending on the field K and S, which is the set of primes above $2R$. Therefore enlarging the prime p does not change the finite set of possibilities for $\mathcal{N}_p$.

Next we show that we can reduce to the case where $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$, after possibly enlarging $\mathcal{B}$ by an effective amount. This step uses standard ideas, originally due to Mazur and used in the paper of Freitas and Siksek [13]. It goes as follows. Suppose $\mathbb{Q}_{\mathfrak{f}} \neq \mathbb{Q}$ then there exist infinitely many primes $\mathfrak{q}$ such that $a_{\mathfrak{q}}(\mathfrak{f}) \notin \mathbb{Q}$. Choose $\mathfrak{q} \nmid \mathcal{N}_p$. If $\mathcal{N}$ is the conductor of E then we know the following.

(i)' If $\mathfrak{q} \nmid \mathcal{N}$ then $a_{\mathfrak{q}}(E) \equiv a_{\mathfrak{q}}(\mathfrak{f}) \pmod{\varpi}$,

(ii)' If $\mathfrak{q} \mid \mathcal{N}$ then $\pm \mathrm{Norm}(\mathfrak{q}+1) \equiv a_{\mathfrak{q}}(\mathfrak{f}) \pmod{\varpi}$,

where $\varpi \mid p$.

Note that in both cases we have have the difference between the left hand side and the right hand side is non-zero as the left hand side is in $\mathbb{Z}$ and the right hand side is not. Now since $p \mid \mathrm{Norm}(\varpi)$ this bounds p. So for large enough p we can assume that $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$.

We would like to show there is some elliptic curve E'/K having the same L-function as $\mathfrak{f}$. This is immediate if we assume Conjecture 5.1.1, and follows from Theorem 5.1.2 if $[K : \mathbb{Q}]$ is odd. Suppose $U \neq \emptyset$ and let $\mathfrak{P} \in U$. By Lemma 6.3.5, E has potentially multiplicative reduction at $\mathfrak{P}$ and $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$. The existence of E' follows from Lemma 5.1.3 after possibly enlarging $\mathcal{B}$ to ensure $p \nmid (\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{P}) \pm 1)$.

We now know that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ for some E'/K with conductor $\mathcal{N}_p$ given by (6.7) which proves (i) and (iii).

After enlarging $\mathcal{B}$ by an effective amount, and possibly replacing E' by an isogenous curve, we may assume that E' has full 2-torsion. To prove this suppose the opposite. Then by Lemma 6.3.1, there are infinitely many primes $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$ such that $4 \nmid \#E'(\mathbb{F}_{\mathfrak{q}})$.

As there are infinitely many such primes, we may suppose that $\mathfrak{q} \nmid p$ (as there are only finitely many primes that divide p). Now as E' has conductor

$\mathcal{N}_p$ given by (6.7), it follows that E' has good reduction at $\mathfrak{q}$. From (6.7) it follows that E has semi-stable reduction at $\mathfrak{q}$. Suppose that E is multiplicative at $\mathfrak{q}$. Then $\mathrm{Norm}(\mathfrak{q}+1) \equiv \pm a_{\mathfrak{q}}(E) \pmod{\varpi}$. From the Hasse-Weil bounds we get a bound on ϖ and hence p so we suppose that p is bigger than this. If it has good reduction then $a_{\mathfrak{q}}(E) \equiv a_{\mathfrak{q}}(E') \pmod{\varpi}$ (where $\varpi \in \mathbb{Q}_{\mathfrak{f}}$ such that $\varpi \mid p$). However, $4 \nmid \#E'(\mathbb{F}_{\mathfrak{q}})$ and E has full 2-torsion so $4 \mid \#E(\mathbb{F}_{\mathfrak{q}})$. So $a_{\mathfrak{q}}(E) \neq a_{\mathfrak{q}}(E')$, so by Hasse-Weil bound it follows that $p \leq 4\sqrt{\mathrm{Norm}(\mathfrak{q})}$, so we can just take p big enough so that this does not occur. So E' (or a 2-isogenous curve) has full 2-torsion, which proves (ii).

For (c), we know from (i) that the conductor of E' is only divisible by primes in $S \cup \{\mathfrak{m}\}$ and by (ii) we know that E' has full 2-torsion. So there are only finitely many elliptic curves (up to isomorphism) in K with this property (as the exponent of the primes in the conductor is bounded and the number of primes is bounded). So only finitely many possible j-invariants. So after possibly enlarging $\mathcal{B}$ can suppose that for all primes $\mathfrak{q}$ in K, we have that if $v_{\mathfrak{q}}(j') < 0$ then $p \nmid v_{\mathfrak{q}}(j')$ (call this property $(*)$) where j' is the j-invariant of E'. Now from Lemma 6.3.3, we get that if $\mathfrak{q} \notin S$ and $\mathfrak{q} \nmid p$ we have that $p \nmid \#\overline{\rho}_{E,p}(I_{\mathfrak{q}})$. By (iii), we have that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$, so $p \nmid \#\overline{\rho}_{E',p}(I_{\mathfrak{q}})$. Next Lemma 6.3.2 gives us that not both $v_{\mathfrak{q}}(j') < 0$ and $p \nmid v_{\mathfrak{q}}(j')$ can be true. Suppose that $v_{\mathfrak{q}}(j') < 0$ is true, then by $(*)$ $p \nmid v_{\mathfrak{q}}(j')$, which means they are both true, which is a contradiction. Hence $v_{\mathfrak{q}}(j') \geq 0$ for all primes $\mathfrak{q} \notin S$ and $\mathfrak{q} \nmid p$.

Now for $\mathfrak{q} \notin S$ and $\mathfrak{q} \mid p$, if $\mathfrak{q} \notin \{\mathfrak{m}\}$ then by (i) E' has good reduction at $\mathfrak{q}$, hence potentially good reduction, so $v_{\mathfrak{q}}(j') \geq 0$. So left with $\mathfrak{q} \in \{\mathfrak{m}\}$ and $\mathfrak{q} \mid p$. But as $\{\mathfrak{m}\}$ is fixed for every field K and not depending on p, after possibly enlarging $\mathcal{B}$ we can assume that $\mathfrak{q} \nmid p$. This concludes the proof of (c).

For (a), let $\mathfrak{P} \in U$. Applying Lemma 6.3.5 we have $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$ and so $p \mid \#\overline{\rho}_{E',p}(I_{\mathfrak{P}})$. Now by Lemma 6.3.2 we have $\operatorname{ord}_{\mathfrak{P}}(j') < 0$ which proves (a). Finally, for (b), we need to use $(*)$ again, so if $v_{\mathfrak{q}}(j') < 0$ then $p \nmid v_{\mathfrak{q}}(j')$. Now suppose that $\mathfrak{P} \in V$. If $p \mid \#\overline{\rho}_{E',p}(I_{\mathfrak{P}})$, then (as p is odd, $\mathfrak{P} \nmid p$) by Lemma 6.3.2 $v_{\mathfrak{P}}(j') < 0$, so we are done. Now suppose that $p \nmid \#\overline{\rho}_{E',p}(I_{\mathfrak{P}})$, then by $(*)$ and Lemma 6.3.2 (again as p is odd, $\mathfrak{P} \nmid p$) , we have that $v_{\mathfrak{P}}(j') \geq 0$, so $3 \mid \#\overline{\rho}_{E',p}(I_{\mathfrak{P}})$ by Lemma 6.3.5. Then by Lemma 6.3.4, $3 \nmid v_{\mathfrak{P}}(\Delta)$. But

$$v_{\mathfrak{P}}(j') = 3v_{\mathfrak{P}}(c_4) - v_{\mathfrak{P}}(\Delta)$$

so then $3 \nmid v_{\mathfrak{P}}(j')$, which completes the proof.

□

We can now present a result that holds for some totally real fields.

6.4 A result for some totally real fields

Theorem 6.4.1. *Let K be a totally real field satisfying (ES). Let A, B, $C \in \mathcal{O}_K$, and suppose that A, B, C are odd, in the sense that if $\mathfrak{P} \mid 2$ is a prime of $\mathcal{O}_K$ then $\mathfrak{P} \nmid ABC$. Write $\mathcal{O}_S^*$ for the set of S-units of K. Suppose that for every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \qquad \lambda,\, \mu \in \mathcal{O}_S^*\,, \tag{6.8}$$

there is

(A) either some $\mathfrak{P} \in U$ that satisfies $\max\{|\operatorname{ord}_{\mathfrak{P}}(\lambda)|, |\operatorname{ord}_{\mathfrak{P}}(\mu)|\} \leq 4 \operatorname{ord}_{\mathfrak{P}}(2)$,

(B) or some $\mathfrak{P} \in V$ *that satisfies both* $\max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}}(\mu)|\} \leq 4\,\mathrm{ord}_{\mathfrak{P}}(2)$*,*

and $\mathrm{ord}_{\mathfrak{P}}(\lambda\mu) \equiv \mathrm{ord}_{\mathfrak{P}}(2) \pmod 3$*.*

Then there is some constant $\mathcal{B} = \mathcal{B}(K, A, B, C)$ *such that the generalized Fermat equation* (6.1) *with exponent* p *and coefficients* A*,* B*,* C *does not have non-trivial solutions with* $p > \mathcal{B}$*.*

Before we start with the proof, we notice the following.

Lemma 6.4.2. *Let* A*,* B*,* $C \in \mathcal{O}_K$ *be odd, and suppose that every solution* (λ, μ) *to the* S*-unit equation* (6.8) *satisfies either condition (A) or (B) of Theorem 6.4.1. Then* $(\pm 1, \pm 1, \pm 1)$ *is not a solution to equation* (6.1)*.*

Proof. Suppose $(\pm 1, \pm 1, \pm 1)$ is a solution to (6.1). By changing signs of A, B, C, we may suppose that $(1, 1, 1)$ is a solution, and therefore that $A+B+C = 0$. Let $\lambda = -A/C$ and $\mu = -B/C$. Clearly (λ, μ) is a solution to the S-unit equation (6.8).

Suppose first that (A) is satisfied. Then $U \neq \emptyset$, so there is some $\mathfrak{P} \mid 2$ with residue field $\mathbb{F}_2$. As A, B, C are odd, we have $\mathfrak{P} \nmid ABC$. Reducing the relation $A + B + C = 0$ mod $\mathfrak{P}$ we obtain $1 + 1 + 1 = 0$ in $\mathbb{F}_2$, giving a contradiction.

Suppose now that (B) holds. By (B) there is some $\mathfrak{P} \in V$ such that $\mathrm{ord}_{\mathfrak{P}}(\lambda\mu) \equiv \mathrm{ord}_{\mathfrak{P}}(2) \pmod 3$. However, as A, B, C are odd, $\mathrm{ord}_{\mathfrak{P}}(\lambda\mu) = 0$. Moreover, $3 \nmid \mathrm{ord}_{\mathfrak{P}}(2)$ by definition of V. This gives a contradiction. □

6.5 Elliptic curves with full 2-torsion and the solutions to the S-unit equation

Theorem 6.3.6 relates non-trivial solutions of the Fermat equation to elliptic curves with full 2-torsion having good reduction outside S. In order to prove Theorem 6.4.1 we will relate these elliptic curves to S-unit equations. There are practical algorithms for determining the solutions to S-unit equations (e.g. [37]), so the hypotheses of Theorem 6.4.1 can always be checked for specific K, A, B, C. This correspondence between the Frey elliptic curves and the S-unit equations is studied in [13]. Although in [13] the set S is the set of all prime ideals dividing 2, it is usually proved in greater generality (i.e. for S being a finite set of prime ideals). In this thesis S is a bigger set (all prime ideals dividing $2ABC$), so we can follow the paper closely in notation and method but need to generalize where necessary.

We will consider an elliptic curve E' with full 2-torsion over a number field K (not necessarily totally real) and find the corresponding S-unit equation (where S is as in (6.2)).

$$E' \ : \ y^2 = (x - e_1)(x - e_2)(x - e_3). \tag{6.9}$$

As E' has full 2-torsion, e_1, e_2, e_3 are distinct and so their **cross ratio**

$$\lambda = \frac{e_3 - e_1}{e_2 - e_1}$$

belongs to $\mathbb{P}^1(K) - \{0, 1, \infty\}$. Moreover, any $\lambda \in \mathbb{P}^1(K) - \{0, 1, \infty\}$ can be written as a cross ratio of three distinct e_1, e_2, e_3 in K. Write $\mathfrak{S}_3$ for the symmetric group on 3 letters. The obvious action of $\mathfrak{S}_3$ on the triple (e_1, e_2, e_3) extends via the cross ratio in a well-defined manner to an action on $\mathbb{P}^1(K) - \{0, 1, \infty\}$.

The orbit of $\lambda \in \mathbb{P}^1(K) - \{0, 1, \infty\}$ under the action of $\mathfrak{S}_3$ is

$$\left\{ \lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda} \right\}. \tag{6.10}$$

This allows us to identify $\mathfrak{S}_3$ with the following subgroup of $\mathrm{PGL}_2(K)$:

$$\begin{aligned} \mathfrak{S}_3 = \Bigg\{ &\sigma_1(z) = z, \quad \sigma_2(z) = \frac{1}{z}, \quad \sigma_3(z) = 1 - z, \\ &\qquad \sigma_4(z) = \frac{1}{1-z}, \quad \sigma_5(z) = \frac{z}{z-1}, \quad \sigma_6(z) = \frac{z-1}{z} \Bigg\}. \end{aligned} \tag{6.11}$$

By an S**-unit** we mean an $\alpha \in K^*$ such that $\mathrm{ord}_{\mathfrak{P}}(\alpha) = 0$ for all prime ideals $\mathfrak{P} \notin S$. Write $\mathcal{O}_S^*$ for the group of S-units in K^*. Let

$$\Lambda_S = \{(\lambda, \mu) \ : \ \lambda + \mu = 1, \qquad \lambda, \ \mu \in \mathcal{O}_S^*\}. \tag{6.12}$$

The set Λ_S is in fact the set of solutions to the S-unit equation (6.8).

Lemma 6.5.1. *The action of* $\mathfrak{S}_3$ *on* $\mathbb{P}^1(K) - \{0, 1, \infty\}$ *induces an action on* Λ_S *given by*

$$(\lambda, \mu)^\sigma := (\lambda^\sigma, 1 - \lambda^\sigma)$$

for $(\lambda, \mu) \in \Lambda_S$ *and* $\sigma \in \mathfrak{S}_3$.

Proof. Suppose $(\lambda, \mu) \in \Lambda_S$. As λ and $\mu = 1 - \lambda$ belong to $\mathcal{O}_S^*$, we see from (6.11) the entire orbit of λ under $\mathfrak{S}_3$ belongs to $\mathcal{O}_S^*$. Moreover, for $\sigma \in \mathfrak{S}_3$, we have $1 - \lambda^\sigma = \lambda^{\sigma\sigma_3}$ which belongs to the orbit of λ, and so to $\mathcal{O}_S^*$. Thus Λ_S is stable under the action of $\mathfrak{S}_3$. $\square$

We denote by $\mathfrak{S}_3\backslash\Lambda_S$ the set of $\mathfrak{S}_3$-orbits in Λ_S. We now relate these orbits to elliptic curves with good reduction outside S and full 2-torsion.

Lemma 6.5.2. *Let $\mathcal{F}_S$ be set of all elliptic curves E' over K with good reduction outside S and satisfying $\#E'(K)[2] = 4$. Define the equivalence relation $E_1 \sim E_2$ on $\mathcal{F}_S$ to mean that E_1 and E_2 are isomorphic over $\overline{K}$. There is a bijection*

$$\Phi \;:\; \mathcal{F}_S/\!\sim \;\longrightarrow\; \mathfrak{S}_3\backslash\Lambda_S$$

which sends the class of an elliptic curve $E' \in \mathcal{F}_S$ given by (6.9) *to the orbit of*

$$\left(\frac{e_3 - e_1}{e_2 - e_1}, \frac{e_2 - e_3}{e_2 - e_1}\right)$$

in $\mathfrak{S}_3\backslash\Lambda_S$.

Proof. Let E'/K be an elliptic curve with good reduction outside S and full 2-torsion. Write E' as in (6.3), with u, $v \in \mathcal{O}_K$ and let $w = -u - v$. The claimed bijection Φ sends E' to the orbit of $(\lambda, \mu) = (-v/u, -w/u)$ and we must show that this belongs to Λ_S. It is clear that $\lambda + \mu = 1$. We need to show that λ, $\mu \in \mathcal{O}_S^*$. Suppose $\mathfrak{q} \notin S$. Then E' has good reduction at $\mathfrak{q}$. By Lemma 6.2.1

$$\mathrm{ord}_{\mathfrak{q}}(u) = \mathrm{ord}_{\mathfrak{q}}(v) = \mathrm{ord}_{\mathfrak{q}}(w)$$

and so $\mathrm{ord}_{\mathfrak{q}}(\lambda) = \mathrm{ord}_{\mathfrak{q}}(\mu) = 0$. It follows that λ, $\mu \in \mathcal{O}_S^*$.

By [35, Proposition III.1.7] and its proof, two elliptic curves E_1/K, E_2/K having full 2-torsion are isomorphic over $\overline{K}$ if and only if the corresponding cross ratios are equivalent under the action of $\mathfrak{S}_3$. It follows that Φ

is well-defined and injective. Finally, to see that Φ is surjective, let $(\lambda, \mu) \in \Lambda_S$ and consider the Legendre elliptic curve

$$E_\lambda \;:\; y^2 = x(x-1)(x-\lambda). \tag{6.13}$$

The model is integral outside S and has discriminant $16\lambda^2\mu^2$ and so E_λ has good reduction outside S and full 2-torsion. The class of E_λ is sent by Φ to the class of (λ, μ), so Φ is surjective. □

Lemma 6.5.3. *Let $E' \in \mathcal{F}_S$ and $(\lambda, \mu) \in \Lambda_S$. Let j' be the j-invariant of E' and $\mathfrak{P} \in S$. Suppose that $\sim$-equivalence class of E' corresponds via Φ to $\mathfrak{S}_3$-orbit of (λ, μ). Then*

(i) $\operatorname{ord}_{\mathfrak{P}}(j') \geq 0$ *if and only if* $\max\{|\operatorname{ord}_{\mathfrak{P}}(\lambda)|, |\operatorname{ord}_{\mathfrak{P}}(\mu)|\} \leq 4 \operatorname{ord}_{\mathfrak{P}}(2)$,

(ii) $3 \mid \operatorname{ord}_{\mathfrak{P}}(j')$ *if and only* $\operatorname{ord}_{\mathfrak{P}}(\lambda\mu) \equiv \operatorname{ord}_{\mathfrak{P}}(2) \pmod 3$.

Proof. The elliptic curve E' is isomorphic over $\overline{K}$ to E_λ given by (6.13). These share the same j-invariant

$$j' = j(\lambda) = 2^8 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2} = 2^8 \cdot \frac{(1 - \lambda\mu)^3}{(\lambda\mu)^2}. \tag{6.14}$$

Hence

$$\operatorname{ord}_{\mathfrak{P}}(j') = 8 \operatorname{ord}_{\mathfrak{P}}(2) + 3 \operatorname{ord}_{\mathfrak{P}}(1 - \lambda\mu) - 2 \operatorname{ord}_{\mathfrak{P}}(\lambda\mu)$$

which proves (ii). Let

$$m = \operatorname{ord}_{\mathfrak{P}}(\lambda), \qquad n = \operatorname{ord}_{\mathfrak{P}}(\mu), \qquad t = \max(|m|, |n|).$$

If $t = 0$ then $\operatorname{ord}_{\mathfrak{P}}(j') \geq 8 \operatorname{ord}_{\mathfrak{P}}(2) > 0$, and so (i) holds. We may therefore suppose that $t > 0$. Now the relation $\lambda + \mu = 1$ forces either $m = n = -t$, or $m = 0$ and $n = t$, or $m = t$ and $n = 0$. Thus $\mathrm{ord}_{\mathfrak{P}}(\lambda\mu) = -2t < 0$ or $\mathrm{ord}_{\mathfrak{P}}(\lambda\mu) = t > 0$. In either case, from (6.14),

$$\mathrm{ord}_{\mathfrak{P}}(j') = 8\,\mathrm{ord}_{\mathfrak{P}}(2) - 2t.$$

This proves (i). □

6.6 Proof of Theorem 6.4.1

Let K be a totally real field satisfying assumption (ES). Let S, T, U, V be as in (6.2). Let $\mathcal{B}$ be as in Theorem 6.3.6, and let (a, b, c) be a non-trivial solution to the Fermat equation (6.1) with exponent $p > \mathcal{B}$, scaled so that $\mathcal{G}_{a,b,c} = \mathfrak{m}$ with $\mathfrak{m} \in \mathcal{H}$. Applying Theorem 6.3.6 gives an elliptic curve E'/K with full 2-torsion and potentially good reduction outside S whose j-invariant j' satisfies:

(a) for all $\mathfrak{P} \in U$, we have $\mathrm{ord}_{\mathfrak{P}}(j') < 0$;

(b) for all $\mathfrak{P} \in V$, we have $\mathrm{ord}_{\mathfrak{P}}(j') < 0$ or $3 \nmid \mathrm{ord}_{\mathfrak{P}}(j')$.

Let (λ, μ) be a solution to S-unit equation (6.8), whose $\mathfrak{S}_3$-orbit corresponds to the $\overline{K}$-isomorphism class of E' as in Lemma 6.5.2. By Lemma 6.5.3 and (a), (b) we know that

(a') for all $\mathfrak{P} \in U$, we have $\max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}}(\mu)|\} > 4\,\mathrm{ord}_{\mathfrak{P}}(2)$;

(b') for all $\mathfrak{P} \in V$, we have $\max\{|\mathrm{ord}_{\mathfrak{P}}(\lambda)|, |\mathrm{ord}_{\mathfrak{P}}(\mu)|\} > 4\,\mathrm{ord}_{\mathfrak{P}}(2)$ or $\mathrm{ord}_{\mathfrak{P}}(\lambda\mu) \not\equiv \mathrm{ord}_{\mathfrak{P}}(2) \pmod 3$.

These contradict assumptions (A) and (B) of Theorem 6.4.1, completing the proof.

6.7 Real quadratic number fields

We related non-trivial solutions to the generalized Fermat equation over totally real fields to an S-unit equation. In Theorem 6.4.1 we showed that if solutions to this S-unit equation satisfy certain hypotheses then there are no non-trivial solutions to the generalized Fermat equation. However, solutions to S-unit equations depend on the number field K and also on the finite set S. In the remainder of this chapter we solve a generalized Fermat equation over a range of real quadratic number fields with coefficients satisfying some conditions by parameterizing the solutions to the S-unit equation.

Theorem 6.7.1. *Let $d \geq 13$ be squarefree, satisfying $d \equiv 5 \pmod 8$ and $q \geq 29$ be a prime such that $q \equiv 5 \pmod 8$ and $\left(\frac{d}{q}\right) = -1$. Let $K = \mathbb{Q}(\sqrt{d})$ and assume Conjecture 5.1.1 for K. Then there is an effectively computable constant $B_{K,q}$ such that for all primes $p > B_{K,q}$, the Fermat equation*

$$x^p + y^p + q^r z^p = 0$$

(where $0 \leq r < p$) has no non-trivial solutions with prime exponent p.

6.8 The S-unit equation over real quadratic fields

In this section we parameterize the solutions to the S-unit equation (6.8) for real quadratic fields K in order to prove Theorem 6.7.1. For the remainder of this chapter, let $d \geq 2$ be a squarefree integer and let K be the real quadratic field $\mathbb{Q}(\sqrt{d})$. We let S and T be as in (6.2), and Λ_S be the set of solutions (λ, μ) to (6.8) (as in (6.12)). In view of the preceding section, we care about elements of Λ_S only up to the action of $\mathfrak{S}_3$. We note that the three elements $(2, -1)$, $(-1, 2)$, $(1/2, 1/2)$ of Λ_S form a single orbit under this action. Following [13] we call these the **irrelevant solutions** to (6.8), with other solutions being called **relevant**. We call the orbit of irrelevant solutions the **irrelevant orbit**. This orbit corresponds via the the correspondence Φ of Lemma 6.5.2 to the elliptic curve defined over $\mathbb{Q}$ with Cremona reference $32A2$ and j-invariant 1728. We note that the irrelevant orbit satisfies the conditions of Theorem 6.4.1, which explains why they are called irrelevant.

Lemma 6.8.1. *Suppose $|S| = 2$. Let $(\lambda, \mu) \in \Lambda_S$. Then, there is some element $\sigma \in \mathfrak{S}_3$ so that $(\lambda', \mu') = (\lambda, \mu)^\sigma$ satisfies λ', $\mu' \in \mathcal{O}_K$.*

Proof. As $\mu' = 1 - \lambda'$ we need only find some element $\sigma \in \mathfrak{S}_3$ so that $\lambda' = \lambda^\sigma \in \mathcal{O}_K$. Write $S = \{\mathfrak{P}_1, \mathfrak{P}_2\}$. If $\operatorname{ord}_{\mathfrak{P}_i}(\lambda) \geq 0$ for both $i = 1$ and $i = 2$, then take $\lambda' = \lambda$ and $\lambda \in \mathcal{O}_K$. So suppose not. If $\operatorname{ord}_{\mathfrak{P}_i}(\lambda) < 0$ for both $i = 1$ and $i = 2$, then let $\lambda' = (\lambda - 1)/\lambda$, so then $\operatorname{ord}_{\mathfrak{P}_i}(\lambda') = 0 - \operatorname{ord}_{\mathfrak{P}_i}(\lambda)$ so λ' belongs to $\mathcal{O}_K$. Thus without loss of generality we may suppose that $\operatorname{ord}_{\mathfrak{P}_1}(\lambda) = 0$. Now if $\operatorname{ord}_{\mathfrak{P}_2}(\lambda) \geq 0$ then $\lambda' = \lambda \in \mathcal{O}_K$, and if $\operatorname{ord}_{\mathfrak{P}_2}(\lambda) < 0$ then $\lambda' = 1/\lambda \in \mathcal{O}_K$. □

For the remainder of this section d denotes a squarefree integer ≥ 13

that satisfies $d \equiv 5 \pmod 8$ and $q \geq 29$ a prime satisfying $q \equiv 5 \pmod 8$ and $\left(\frac{d}{q}\right) = -1$. Let K denotes the real quadratic field $\mathbb{Q}(\sqrt{d})$. It follows that both q and 2 are inert in K. We let $S = \{2, q\}$.

Lemma 6.8.2. *Let K and S be as above, and let $(\lambda, \mu) \in \Lambda_S$. Then λ, $\mu \in \mathbb{Q}$ if and only if (λ, μ) belongs to the $\mathfrak{S}_3$-orbit $\{(1/2, 1/2),\ (2, -1),\ (-1, 2)\} \subseteq \Lambda_S$.*

Proof. Suppose λ, $\mu \in \mathbb{Q}$. By Lemma 6.8.1 we may suppose that λ and μ belong to $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$ and hence $\lambda = \pm 2^{r_1} q^{s_1}$, $\mu = \pm 2^{r_2} q^{s_2}$ where $r_i \geq 0$ and $s_i \geq 0$. As $\lambda + \mu = 1$ we see that one of r_1, r_2 is 0 and likewise one of s_1, $s_2 = 0$. Without loss of generality $r_2 = 0$. If $s_2 = 0$ too then we have $\lambda \pm 1 = 1$ which forces $(\lambda, \mu) = (2, -1)$ as required. We may therefore suppose that $s_2 > 0$ and $s_1 = 0$. Hence $\pm 2^{r_1} \pm q^{s_2} = 1$. We now easily check that $0 \leq r_1 \leq 2$ are all incompatible with our hypotheses on q. Thus $r_1 \geq 3$ and so $\pm q^{s_2} \equiv 1 \pmod 8$. As $q \equiv 5 \pmod 8$, we have $\pm 2^{r_1} + q^{2t} = 1$ for some integer $t \geq 1$. Hence $(q^t + 1)(q^t - 1) = \mp 2^{r_1}$. This implies that $q^t + 1 = 2^a$ and $q^t - 1 = 2^b$ where $a \geq b \geq 1$. Subtracting we have $2^a - 2^b = 2$ and so $b = 1$. Then $q^t = 3$ which contradicts our assumptions on q a contradiction. □

We now give a parametrization of all relevant elements of Λ_S. This the analogue of [13, Lemma 6.4], and shows that such a parametrization is possible even though our set S is larger, containing the odd prime q.

Lemma 6.8.3. *Up to the action of $\mathfrak{S}_3$, every relevant $(\lambda, \mu) \in \Lambda_S$ has the form*

$$\lambda = \frac{\eta_1 \cdot 2^{2r_1} \cdot q^{2s_1} - \eta_2 \cdot q^{2s_2} + 1 + v\sqrt{d}}{2}, \qquad \mu = \frac{\eta_2 \cdot q^{2s_2} - \eta_1 \cdot 2^{2r_1} \cdot q^{2s_1} + 1 - v\sqrt{d}}{2} \tag{6.15}$$

where

$$\eta_1 = \pm 1, \qquad \eta_2 = \pm 1, \qquad r_1 \geq 0, \qquad s_1, s_2 \geq 0, \qquad s_1 \cdot s_2 = 0, \qquad v \in \mathbb{Z}, \qquad v \neq 0 \tag{6.16}$$

are related by

$$(\eta_1 \cdot 2^{2r_1} \cdot q^{2s_1} - \eta_2 \cdot q^{2s_2} + 1)^2 - dv^2 = \eta_1 \cdot 2^{2r_1+2} \cdot q^{2s_1} \tag{6.17}$$

$$(\eta_2 \cdot q^{2s_2} - \eta_1 \cdot 2^{2r_1} \cdot q^{2s_1} + 1)^2 - dv^2 = \eta_2 \cdot 2^2 \cdot q^{2s_2}. \tag{6.18}$$

Proof. If η_1, η_2, r_1, s_1, s_2 and v satisfy (6.16), (6.17), (6.18) and λ, μ are given by (6.15), it is clear that (λ, μ) is a relevant element of Λ_S.

Conversely, suppose (λ, μ) is a relevant element of Λ_S. By Lemma 6.8.2, we may suppose that λ, $\mu \in \mathcal{O}_K$, and that λ, $\mu \notin \mathbb{Q}$. As $S = \{2, q\}$ we can write $\lambda = 2^{r_1} q^{s_1} \zeta$ and $\mu = 2^{r_2} q^{s_2} \zeta'$ where ζ and ζ' are units. As $\lambda + \mu = 1$ we have $r_1 r_2 = 0$ and $s_1 s_2 = 0$. Swapping λ and μ if necessary, we can suppose that $r_2 = 0$. Let $x \mapsto \overline{x}$ denote conjugation in K. Then

$$\lambda\overline{\lambda} = \eta_1 \cdot 2^{2r_1} \cdot q^{2s_1}, \qquad \mu\overline{\mu} = \eta_2 \cdot q^{2s_2}, \qquad \eta_1 = \pm 1, \qquad \eta_2 = \pm 1.$$

Now,

$$\lambda + \overline{\lambda} = \lambda\overline{\lambda} - (1-\lambda)(1-\overline{\lambda}) + 1 = \lambda\overline{\lambda} - \mu\overline{\mu} + 1 = \eta_1 \cdot 2^{2r_1} \cdot q^{2s_1} - \eta_2 \cdot q^{2s_2} + 1\,.$$

Moreover we can write $\lambda - \overline{\lambda} = v\sqrt{d}$, where $v \in \mathbb{Z}$, and as $\lambda \notin \mathbb{Q}$, we have $v \neq 0$. The expressions for $\lambda + \overline{\lambda}$ and $\lambda - \overline{\lambda}$ give the expression for λ in (6.15), and we deduce the expression for μ from $\mu = 1 - \lambda$. Finally, (6.17) follows from the identity

$$(\lambda+\overline{\lambda})^2-(\lambda-\overline{\lambda})^2=4\lambda\overline{\lambda},$$

and (6.18) from the corresponding identity for μ. □

Lemma 6.8.4. *Let $d \equiv 5 \pmod 8$ be squarefree $d \geq 13$ and $q \geq 29$ a prime such that $q \equiv 5 \pmod 8$ and $\left(\frac{d}{q}\right) = -1$. Then there are no relevant elements of Λ_S.*

Proof. We apply Lemma 6.8.3. In particular, $s_1 s_2 = 0$. Suppose first that $s_1 > 0$. Thus $s_2 = 0$. As $(d/q) = -1$, we have from (6.17) that $q^{s_1} \mid v$ and $q^{s_1} \mid (\eta_2 - 1)$. Hence $\eta_2 = 1$. Now (6.17) can be rewritten as

$$2^{4r_1} q^{2s_1} - d(v/q^{s_1})^2 = \eta_1 2^{2r_1+2}\,.$$

Thus $(d/q) = (-\eta_1/q) = 1$ as $q \equiv 5 \pmod 8$. This is a contradiction.

Thus, henceforth, $s_1 = 0$. Next suppose that $s_2 = 0$. We will consider the sub cases $\eta_2 = -1$ and $\eta_2 = 1$ separately and obtain contradictions in both sub cases showing that $s_2 > 0$. Suppose $\eta_2 = -1$. From (6.18) we have $2^{4r_1} - dv^2 = -4$. If $r_1 = 0$ or 1 then $d = 5$ and if $r_1 \geq 2$ then $d \equiv 1 \pmod 8$, giving a contradiction. Hence suppose $\eta_2 = 1$. From (6.17), we have $2^{4r_1} - dv^2 = \eta_1 2^{2r_1+2}$. If $r_1 = 0,\ 1,\ 2$ then $dv^2 = 1 \pm 4$, $dv^2 = 16 \pm 16$, $dv^2 = 256 \pm 64$ all of which contradict the assumptions on d or the fact that $v \neq 0$ (by (6.16)). If $r_1 \geq 3$ then $2^{2r_1-2} - \eta_1 = d(v/2^{r_1+1})^2$ which forces $d \equiv \pm 1 \pmod 8$, a contradiction.

We are reduced to $s_1 = 0$ and $s_2 > 0$. From (6.18), as $(d/q) = -1$, we have $q^{s_2} \mid v$ and

$$q^{s_2} \mid (\eta_1 2^{2r_1} - 1). \tag{6.19}$$

The conditions $q \geq 29$ and $q \equiv 5 \pmod 8$ force $r_1 \geq 5$. Write $v = 2^t w$ where $2 \nmid w$. Suppose $t \leq r_1 - 1$. From (6.17) we have $\eta_1 2^{2r_1} - \eta_2 q^{2s_2} + 1 = 2^t w'$ where $2 \nmid w'$. Thus $w'^2 - dw^2 \equiv 0 \pmod 8$, contradicting $d \equiv 5 \pmod 8$. We may therefore suppose $t \geq r_1$. Hence $2^{r_1} \mid (\eta_2 q^{2s_2} - 1)$. Thus $\eta_2 = 1$. Therefore $2^{r_1} \mid (q^{s_2} - 1)(q^{s_2} + 1)$. Since $q \equiv 5 \pmod 8$, we have $2 \mid\mid (q^{s_2} + 1)$ and so

$$2^{r_1 - 1} \mid (q^{s_2} - 1).$$

As $q \equiv 5 \pmod 8$ and $r_1 \geq 5$, we see that s_2 must be even, and that $2^{r_1-2} \mid (q^{s_2/2} - 1)$. We can write $q^{s_2/2} = k \cdot 2^{r_1-2} + 1$. From (6.19),

$$k^2 2^{2r_1-4} + k 2^{r_1-1} + 1 = q^{s_2} \leq 2^{2r_1} + 1.$$

Hence $k = 1$, 2 or 3. Moreover, as $q^{s_2/2} \equiv 1 \pmod 8$, we have $4 \mid s_2$. Hence

$$(q^{s_2/4} - 1)(q^{s_2/4} + 1) = k 2^{r_1-2}.$$

Again as $q \equiv 5 \pmod 8$ we have $2 \mid\mid (q^{s_2/4} + 1)$ and so $q^{s_2/4} + 1 = 2$ or 6, both of which are impossible. This completes the proof. □

6.9 Proof of Theorem 6.7.1

We apply Theorem 6.4.1. By Lemma 6.8.4 all solutions to (6.8) are irrelevant, and the irrelevant solutions satisfy condition (A) of Theorem 6.4.1. This completes the proof of Theorem 6.7.1.

Chapter 7

Small real quadratic fields

This chapter looks at the generalized Fermat equation over small real quadratic number fields and is a generalization of Freitas and Siksek's paper [14]. Freitas and Siksek look at the Fermat equation

$$x^p + y^p + z^p = 0 \tag{7.1}$$

where $p \geq 17$ is a rational prime, $x, y, z \in \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{d})$ where $3 \leq d \leq 23$ is squarefree and $d \neq 5$. In this chapter we look at the generalized Fermat equation

$$Ax^p + By^p + Cz^p = 0$$

where $A, B, C, x, y, z \in \mathcal{O}_K$, $K = \mathbb{Q}(\sqrt{d})$, $d = 2, 3, 6, 7$ or 11, $p \geq 17$ if $d = 2$ ($p \geq (1+3^{12})^2$ if not), A, B, C odd, pairwise coprime. Furthermore, we assume that $\text{Rad}(ABC)$ is a prime ideal of K chosen from a finite set to be specified later in this chapter and that $v_{\mathfrak{q}}(ABC) < p$ for all primes $\mathfrak{q}$. Note that this last condition can always be satisfied since the class number of these fields is 1 and p-th powers can be absorbed into x^p, y^p, z^p. For the rest of this chapter it is assumed that all of these conditions hold. Equation 7.1 is the same equation as in the previous chapter (equation 6.1) and we refer to it as the generalized Fermat equation with exponent p over K for fixed $A, B, C \in \mathcal{O}_K$. Recall that a solution (a, b, c) is called **trivial** if $abc = 0$, otherwise **non-trivial**. The main result of this chapter is the following theorem.

Theorem 7.0.1. *Let $d = 2$ or 3, $R = \mathrm{Rad}(ABC)$ be a prime ideal of $K = \mathbb{Q}(\sqrt{d})$ dividing $3 \times 5 \times 7 \times 11$, or if $d = 6$ or 7 let R be a prime ideal dividing 15, or if $d = 11$ let R be a prime ideal dividing 3. For $d = 2$, the Fermat equation (6.1) does not have any non-trivial solutions over K if $p \geq 17$. For $d \neq 2$ there are no non-trivial solutions if $p \geq (1 + 3^{12})^2$.*

Remark. Note that 2 ramifies in all the fields of Theorem 7.0.1 so for this chapter let $\mathfrak{P} = \pi\mathcal{O}_K$ be this unique prime ideal above 2. Since $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$ we know that exactly one of Ax^p, By^p, Cz^p is even so without loss of generality assume that By^p is even. Moreover, since B is odd, we can assume that $\mathfrak{P} \mid y$.

To prove this theorem, we will use a similar approach as in the previous chapter. We will start with a hypothetical non-trivial solution (a, b, c) to the generalized Fermat equation. We associate an elliptic curve to this hypothetical solution called the Frey elliptic curve. Recall from Theorem 5.2.2 that all elliptic curves over real quadratic number fields are modular. So it suffices to show that the mod p Galois representation of this Frey elliptic curve is irreducible in order to use the level lowering theorem (Theorem 5.3.1). By first calculating the conductor of the elliptic curve we can predict which level the associated Hilbert newform has. In some cases there is no such newform and in some other cases we use a result from the penultimate section of this chapter to prove the main theorem over small quadratic fields. However, as in

[14] the following three problems present themselves

1. We need irreducibility of $\overline{\rho}_{E,p}$ in order to apply level lowering theorems.
2. We need to calculate the conductor (to a higher precision than in the previous chapter) to predict the levels of the corresponding newforms.
3. If the newform space is non-zero, we need to deal with the newforms found.

Remark. Even though we need to prove irreducibility in order to apply level lowering theorems, we will calculate the conductor and level first as $\overline{\rho}_{E,p}$ depends on the Frey elliptic curve E which is dependent on the hypothetical non-trivial solution (a, b, c) of the generalized Fermat equation. We will need to scale this solution such that it satisfies certain conditions in order to prove irreducibility. So we will start by calculating the conductor and the level.

We fix the following notation for the rest of this chapter as in chapter 5. Let (a, b, c) be a non-trivial solution to the Fermat equation (6.1), and consider the Frey elliptic curve

$$E_{a,b,c} \ : \ Y^2 = X(X - Aa^p)(X + Bb^p). \tag{7.2}$$

In line with (6.2) from the previous chapter, let R be the prime ideal in $\mathcal{O}_K$ dividing ABC (as A, B, C are chosen to be divisible by exactly 1 prime ideal). Also let $G_K = \mathrm{Gal}(\overline{K}/K)$. For an elliptic curve E/K, we write

$$\overline{\rho}_{E,p} \ : \ G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p), \tag{7.3}$$

for the representation of G_K on the p-torsion of E. An arbitrary prime of K

is denoted by $\mathfrak{q}$ and the unique prime ideal dividing 2 is denoted $\mathfrak{P} = \pi\mathcal{O}_K$.

7.1 Calculating the conductor and the level

In this section we want to calculate the conductor of the Frey elliptic curve associated to a non-trivial solution of the generalized Fermat equation and the level associated to this. Note that we have to be more precise than in the previous chapter where it sufficed to bound the level. Recall that in the previous chapter, we associated to a non-trivial solution (a, b, c) of the generalized Fermat equation (6.1), the following $\mathcal{G}_{a,b,c}$ as given in (6.6), which we thought of as the greatest common divisor of a, b, c. However in this chapter all the quadratic fields we consider (i.e. $K = \mathbb{Q}(\sqrt{d})$ with $d = 2, 3, 6, 7$ or 11) have class number one and hence we can assume that $\mathcal{G}_{a,b,c} = 1 \cdot \mathcal{O}_K$. This will make our calculations considerably easier. As in [14] we will split up the calculations of the even part and the odd part of the conductor of the level. The calculations for the odd part need to be generalized but still follow [14]. However for the calculations for the even part we use Tate's algorithm and not the approach as in [14] as we look at fewer number fields and so can be more precise.

7.1.1 The odd part of the level

We retain the same notation as in [14]. Let (a, b, c) be a non-trivial primitive solution to the Fermat equation (6.1) with odd prime exponent p. Write E for the Frey curve in (5.3). Let $\mathcal{N}$ be the conductor of E and let $\mathcal{N}_p$ be as defined in (5.4). We define the **even parts** of $\mathcal{N}$ and $\mathcal{N}_p$ by

$$\mathcal{N}^{\text{even}} = \mathfrak{P}^{\text{ord}_{\mathfrak{P}}(\mathcal{N})}, \qquad \mathcal{N}_p^{\text{even}} = \mathfrak{P}^{\text{ord}_{\mathfrak{P}}(\mathcal{N}_p)}.$$

We define the **odd parts** of $\mathcal{N}$ and $\mathcal{N}_p$ by

$$\mathcal{N}^{\text{odd}} = \frac{\mathcal{N}}{\mathcal{N}^{\text{even}}}, \qquad \mathcal{N}_p^{\text{odd}} = \frac{\mathcal{N}}{\mathcal{N}_p^{\text{even}}}.$$

The following lemma follows [14], with the addition of considering primes $\mathfrak{q} \mid ABC$.

Lemma 7.1.1. *Let (a, b, c) be a non-trivial solution to the Fermat equation (6.1) over the number field $K = \mathbb{Q}(\sqrt{d})$ where $d = 2, 3, 6, 7$ or 11 with odd prime exponent p, A, B, C odd and pairwise coprime. Write E for the Frey curve in (5.3). Then at all $\mathfrak{q} \neq \mathfrak{P}$, the local minimal model $E_{\mathfrak{q}}$ is semi-stable, and if $\mathfrak{q} \nmid \mathfrak{P}ABC$ then $p \mid \text{ord}_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$. Moreover,*

$$\mathcal{N}^{odd} = \prod_{\substack{\mathfrak{q}\mid abc \\ \mathfrak{q}\neq\mathfrak{P} \\ \mathfrak{q}\nmid ABC}} \mathfrak{q} \prod_{\mathfrak{q}\mid ABC} \mathfrak{q}, \qquad \mathcal{N}_p^{odd} = \prod_{\mathfrak{q}\mid ABC} \mathfrak{q}. \tag{7.4}$$

The proof remains largely the same as in Siksek and Freitas paper [14] apart from dealing with the case when $\mathfrak{q} \mid ABC$

Proof. Clearly, if $\mathfrak{q} \nmid 2abcABC$ then E has good reduction at $\mathfrak{q}$, hence $\mathfrak{q} \nmid \mathcal{N}$, $\mathcal{N}_p$. Suppose $\mathfrak{q} \mid ABC$, then $\mathfrak{q} \mid \Delta$, but as A, B, C are pairwise coprime $\mathfrak{q}$ divides only one of A, B, C, without loss of generality assume it is A. If $\mathfrak{q} \mid abc$ then since the solution (a, b, c) is primitive $\mathfrak{q}$ divides exactly one of them. If this is not a (say b) then from $Aa^p + Bb^p + Cc^p = 0$ we get that either $\mathfrak{q} \mid C$ or

$\mathfrak{q} \mid c$ contradicting the coprimality of A, B, C or the primitiveness of (a, b, c) respectively. So then $\mathfrak{q} \mid a$. In both the cases (i.e. $\mathfrak{q} \mid a$ and $\mathfrak{q} \nmid a$) we have that $\mathfrak{q} \nmid c_4$, so we have multiplicative reduction. From (6.4), $\Delta = 16(ABC)^2(abc)^{2p}$ and $0 < v_{\mathfrak{q}}(ABC) < p$ in both cases we get that $p \nmid v_{\mathfrak{q}}(\Delta)$ and so $\mathfrak{q} \mid \mathcal{N}_p$. Suppose that $\mathfrak{q} \mid abc$ and $\mathfrak{q} \neq \mathfrak{P}$. Since the solution (a, b, c) is primitive the prime $\mathfrak{q}$ divides precisely one of a, b, c. We already discussed at the beginning of this proof what happens if $\mathfrak{q}$ divides both abc and ABC and so we can assume that $\mathfrak{q} \nmid ABC$. In this case we have from (6.4) that $\mathfrak{q} \nmid c_4$ so the model (5.3) is minimal and has multiplicative reduction at $\mathfrak{q}$, and $p \mid \mathrm{ord}_{\mathfrak{q}}(\Delta)$. By (5.4), we see that $\mathfrak{q} \nmid \mathcal{N}_p$ which finishes the proof.

□

7.1.2 Scaling by units and the even part of the level

This section does not follow the paper by Freitas and Siksek [14] as the number fields of this section have additional properties (such as 2 always ramifies) making it easier to apply Tate's algorithm. We will make extensive use of the fact that we can scale equation (7.1) by an element in the unit group. More formally let $\mathcal{O}_K^*$ be the unit group of K. In this section we study the effect on $\mathcal{N}$ and $\mathcal{N}_p$ as calculated in [14] with the addition of scaling equation (7.1) by units in $\mathcal{O}_K^*$. Note that scaling by units does not affect the odd parts of $\mathcal{N}$ and $\mathcal{N}_p$.

Let (a, b, c) be a non-trivial primitive solution to generalized Fermat equation. Recall from the beginning of this chapter that since $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$ we know that exactly one of Aa^p, Bb^p, Cc^p is even, say Bb^p and since A, B and C are odd, we can assume that b is even. The following lemma says that after possibly scaling the non-trivial solution (a, b, c) by units we can determine the following condition which is useful for Tate's algorithm.

Lemma 7.1.2. *Let (a, b, c) be a non-trivial primitive solution to the generalized Fermat equation 7.1. Then after permuting the terms Aa^p, Bb^p, Cc^p and scaling by units if necessary, we can assume that $\mathfrak{P} \mid b$ and if $d = 3, 7$ or 11 that $Aa^p \equiv -1 \pmod{\pi^3}$. If $d = 6$ we can assume that either $Aa^p \equiv -1 \pmod{\pi^4}$ or $Aa^p \equiv \sqrt{6}+1 \pmod{\pi^4}$. If $d = 2$, we can assume that $Aa^p \equiv -1 \pmod{\pi^4}$.*

Proof. Since $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$, we know that exactly one of Aa^p, Bb^p, Cc^p is even. After permuting these elements if necessary we can assume that this is Bb^p. Now since B is odd, we have that $\mathfrak{P} \mid b^p$ and so $\mathfrak{P} \mid b$. Now suppose $d = 3, 7$ or 11. We want to know what Aa^p is modulo π^3. But first we look at $Aa^p \pmod 4$. As $\{1, \sqrt{d}\}$ is a basis for $\mathcal{O}_K$, we have that $Aa^p \equiv m + n\sqrt{d} \pmod 4$ where $m, n \in \mathbb{Z}$, $-1 \leq m, n \leq 2$. Note that we have that $\pi \nmid Aa^p$ and the residue field is $\mathbb{F}_2$, we have that $m + n\sqrt{d} \equiv 1 \pmod{\pi}$. Now since we can take $\pi = \sqrt{3}+1, \sqrt{7}+3$ and $\sqrt{11}+3$ for $d = 3, 7$ and 11 respectively, we have that $\sqrt{d} \equiv 1 \pmod{\pi}$ and so $m + n \equiv 1 \pmod{\pi}$ so m and n have different parity. And so $Aa^p \pmod 4$ is equivalent to one of the following

$$\begin{array}{llll} -1 & \sqrt{d} & 1+2\sqrt{d} & 2+\sqrt{d} \\ -1+2\sqrt{d} & -\sqrt{d} & 1 & 2-\sqrt{d} \end{array}$$

Note that $e + f\sqrt{d}$ and $e' + f'\sqrt{d}$ (with $e, f, e', f' \in \mathbb{Z}$) are equivalent modulo π^3 if and only if $(e - e') + (f - f')\sqrt{d} = 2\pi(g + h\sqrt{d})$ where $g, h \in \mathbb{Z}$. So we can see this is true if and only if both $(e - e')$ and $(f - f')$ are even and

$(e-e')/2+(f-f')\sqrt{d}/2$ is even. So we get that

$$\begin{array}{lclclcl} -1 & \leftrightarrow & 1+2\sqrt{d} & \qquad & -\sqrt{d} & \leftrightarrow & 2+\sqrt{d} \\ -1+2\sqrt{d} & \leftrightarrow & 1 & & \sqrt{d} & \leftrightarrow & 2-\sqrt{d} \end{array}$$

where the double arrow indicates equivalence modulo π^3. If Aa^p is equivalent to an entry in the first column modulo π^3 we can assume that Aa^p is equivalent to a unit modulo π^3 since 1 and -1 are always units in K. Now $\sqrt{3}+2, 3\sqrt{7}+8$ and $3\sqrt{11}+10$ are fundamental units for $d=3,7$ and 11 respectively, so either the first or second entry in the second column is equivalent to a unit modulo π^3. Now since $\sqrt{d}$ and $-\sqrt{d}$ differ by multiplication by -1 which is a unit, we can assume that Aa^p is equivalent to a unit modulo π^3. So after possibly multiplying the Fermat equation by a unit, we can assume that $Aa^p \equiv -1 \pmod{\pi^3}$.

Now let $d=6$, then $\sqrt{6} \equiv 0 \pmod{\pi}$. Let $Aa^p = m+n\sqrt{6}$ where $m,n \in \mathbb{Z}$ since $\{1,\sqrt{d}\}$ is a basis for $\mathcal{O}_K$. We have that since $\pi \nmid Aa^p$, m is odd. And so $Aa^p \pmod{\pi^4}$ is equivalent to one of the following.

$$\begin{array}{llll} -1 & -1+2\sqrt{6} & 1 & 1+2\sqrt{6} \\ -1+\sqrt{6} & -1-\sqrt{6} & 1+\sqrt{6} & 1-\sqrt{6} \end{array}$$

Note that $5+2\sqrt{6}$ is a fundamental unit of $K=\mathbb{Q}(\sqrt{6})$. And $5+2\sqrt{6} \equiv 1+2\sqrt{6} \pmod{4}$ and $-(5+2\sqrt{6}) \equiv -1+2\sqrt{6} \pmod{4}$. We also have that $(5+2\sqrt{6})^2 \equiv 1 \pmod{4}$ and $-(5+2\sqrt{6})^2 \equiv -1 \pmod{4}$ and so if $Aa^p \equiv 1, -1, 1+2\sqrt{6}, -1+2\sqrt{6}$ we can scale the equation by a unit to get that $Aa^p \equiv -1 \pmod{\pi^4}$. On the other hand, note that $-(1+\sqrt{6}) \equiv -1-\sqrt{6}$

(mod 4), $(1+\sqrt{6})(5+\sqrt{6}) \equiv 1-\sqrt{6} \pmod 4$ and $-(1-\sqrt{6}) \equiv -1+\sqrt{6}$ (mod 4). In this case we can assume that after scaling by a unit we have $Aa^p \equiv 1+\sqrt{6} \pmod{\pi^4}$. Now if we assume that $d=2$, then we can take $\pi = \sqrt{2}$ and so $Aa^p \pmod{\pi^4}$ is equivalent to one of the following

-1	$-1+2\sqrt{2}$	1	$1+2\sqrt{2}$
$-1+\sqrt{2}$	$-1-\sqrt{2}$	$1+\sqrt{2}$	$1-\sqrt{2}$

Now $1+\sqrt{2}$ is a fundamental unit and $(1+\sqrt{2})^2 \equiv -1+2\sqrt{2} \pmod 4$, $-(1+\sqrt{2}) \equiv -1-\sqrt{2} \pmod 4$,$-(1+\sqrt{2})^2 \equiv 1+2\sqrt{2} \pmod 4$, $(1+\sqrt{2})^3 \equiv -1+\sqrt{2} \pmod 4$ and $-(1+\sqrt{2})^3 \equiv 1-\sqrt{2} \pmod 4$. And so after possibly scaling by a unit, we may assume that $Aa^p \equiv -1 \pmod{\pi^4}$. □

Using Tate's algorithm, as described in Silverman [36] we can calculate the even part of the conductor for the other fields potentially using the permutation and scaling as discussed in the previous lemma.

Lemma 7.1.3. *Let (a,b,c) be a primitive non-trivial solution to the generalized Fermat equation. We may suppose as in the previous lemma that $\mathfrak{P} \mid b$ and $Aa^p \equiv -1 \pmod{\pi^3}$ (after possibly permutation and scaling). We have that*

1. *if $Aa^p \equiv -1 \pmod{\pi^4}$ then E has multiplicative reduction at $\mathfrak{P}$ and so the even part of the conductor is $\mathcal{N}^{even} = \mathfrak{P}$.*

2. *if not then E has additive reduction at $\mathfrak{P}$. Moreover, in this case the even part of the conductor of E is $\mathcal{N}^{even} = \mathfrak{P}^4$ if $d = 3, 7$ or 11 and $\mathcal{N}^{even} = \mathfrak{P}^8$ if $d = 6$.*

Proof. Let (a, b, c) be a non-trivial solution to the generalized Fermat equation, which we may suppose is primitive. We look at the Frey elliptic curve associated to this solution

$$E : Y^2 = X^3 + (Bb^p - Aa^p)X^2 - Aa^pBb^pX.$$

Suppose we are in the first case ($Aa^p \equiv -1 \pmod{\pi^4}$) then by making a change of coordinates $X \mapsto 4X', Y \mapsto 8Y' + 4X'$ we get

$$64Y'^2 + 64X'Y' = 64X'^3 + 16(Bb^p - Aa^p - 1)X'^2 - 4Aa^pBb^pX'$$

which is equivalent to

$$E : Y'^2 + X'Y' = X'^3 + \frac{Bb^p - Aa^p - 1}{4}X'^2 - \frac{Aa^pBb^p}{16}X'$$

From the hypothesis we get that $\frac{Bb^p-Aa^p-1}{4}, \frac{Aa^pBb^p}{16} \in \mathcal{O}_K$. Recall that the residue field is $\mathbb{F}_2$ and so E is either equivalent to $Y'^2 + X'Y' = X'^3$ or $Y'^2 + X'Y' = X'^3 + X'^2$ modulo π. Both of these have a node, and so the Frey elliptic curve has multiplicative reduction at $\mathfrak{P}$. In this case the minimal discriminant at $\mathfrak{P}$ is given by $\Delta_{\mathfrak{P}} = 2^{-8}A^2a^{2p}B^2b^{2p}C^2c^{2p}$. Now suppose that we are not in this case. So we look at

$$E : Y^2 = X^3 + (Bb^p - Aa^p)X^2 - Aa^pBb^pX$$

and use Tate's algorithm in [36]. In the notation of the algorithm we have that

$$\begin{array}{lllll} a_1 = 0 & a_2 = Bb^p - Aa^p & a_3 = 0 & a_4 = -Aa^pBb^p & a_6 = 0 \\ b_2 = 4(Bb^p - Aa^p) & b_4 = -2Aa^pBb^p & b_6 = 0 & b_8 = -A^2a^{2p}B^2b^{2p} & \\ \Delta = 16A^2a^{2p}B^2b^{2p}C^2c^{2p}. & & & & \end{array}$$

We go through steps 1 to 6 of Tate's algorithm as in Silverman [36] pages 364–369. In step 6 we need to do a change of coordinates such that $\pi \mid a_2$. We let $X' = X$, $Y' = Y + X$. And so the new equation is

$$Y'^2 + 2X'Y' = X'^3 + (Bb^p - Aa^p - 1)X'^2 - Aa^pBb^pX'$$

and hence

$$\begin{array}{lllll} a_1 = 2 & a_2 = Bb^p - Aa^p - 1 & a_3 = 0 & a_4 = -Aa^pBb^p & a_6 = 0 \\ b_2 = 4(Bb^p - Aa^p) & b_4 = -2Aa^pBb^p & b_6 = 0 & b_8 = -A^2a^{2p}B^2b^{2p} & \\ \Delta = 16A^2a^{2p}B^2b^{2p}C^2c^{2p}. & & & & \end{array}$$

Now $\pi \mid a_1$ and a_2, $\pi^2 \mid a_3$ and a_4, and $\pi^3 \mid a_6$. We then look at the polynomial

$$P(T) = T^3 + 1/\pi(Bb^p - Aa^p - 1)T^2 - 1/\pi^2Aa^pBb^pT$$

The reduction $\tilde{P} \pmod{\pi}$ has a triple root at $T = 0$, and so we end up at the end of the algorithm which means that the original Weierstrass equation was not minimal. And so we do another change of coordinates $X = X'/\pi^2, Y =$

Y'/π^3, which gives us

$$Y^2 + (2/\pi)XY = X^3 + (1/2)(Bb^p - Aa^p - 1)X^2 - (1/4)Aa^pBb^p$$

$a_1 = 2/\pi$	$a_2 = 1/2(Bb^p - Aa^p - 1)$	$a_3 = 0$
$a_4 = -1/4Aa^pBb^p$	$a_6 = 0$	$b_2 = 2(Bb^p - Aa^p)$
$b_4 = -1/2Aa^pBb^p$	$b_6 = 0$	$b_8 = -1/16A^2a^{2p}B^2b^{2p}$
$\Delta = 1/4A^2a^{2p}B^2b^{2p}C^2c^{2p}$.		

As $p \geq 17$ steps 1 to 5 are satisfied, and as $Aa^p \equiv -1 \pmod{\pi^3}$ step 6 is as well. Hence we look at the polynomial

$$P(T) = T^3 + 1/\pi^3(Bb^p - Aa^p - 1)T^2 - 1/8Aa^pBb^pT$$

Since $Aa^p \not\equiv -1 \pmod{\pi^4}$ we get that we have a double root at $T = 0$ and hence we are in the sub procedure of step 7. Here we get that the exponent of the even part of the conductor is $f = v_\pi(\Delta) - 2v_\pi(a_4)$, which is $f = -4 + 2pv_\pi(b) - 2pv_\pi(b) + 8 = 4$. Now for $d = 6$, and $Aa^p \equiv -1 + \sqrt{6} \pmod{\pi^3}$ we start at the beginning of Tate's algorithm with the Frey elliptic curve

$$Y^2 = X(X - Aa^p)(X + Bb^p).$$

We quickly proceed through steps 1 to 5. For step 6, we need to have a change of coordinates as before and we end up with

$$Y'^2 + 2X'Y' = X'^3 + (Bb^p - Aa^p - 1)X'^2 - Aa^pBb^pX'$$

as before with the following

$$\begin{array}{lllll} a_1 = 2 & a_2 = Bb^p - Aa^p - 1 & a_3 = 0 & a_4 = -Aa^pBb^p & a_6 = 0 \\ b_2 = 4(Bb^p - Aa^p) & b_4 = -2Aa^pBb^p & b_6 = 0 & b_8 = -A^2a^{2p}B^2b^{2p} & \\ \Delta = 16A^2a^{2p}B^2b^{2p}C^2c^{2p}. & & & & \end{array}$$

Now we look at the polynomial

$$P(T) = T^3 + 1/\pi(Bb^p - Aa^p - 1)T^2 - 1/\pi^2 Aa^pBb^pT$$

and $\tilde{P}$ has a double root at $T = 0$ and so we are in the the sub procedure of step 7. Hence we get that the exponent of the even part of the conductor is $f = v_\pi(\Delta) - 2v_\pi(a_4)$ and so $f = 8 + 2pv_\pi(b) - 2pv_\pi(b) = 8$. □

From this lemma we can deduce the following.

Lemma 7.1.4. *The Frey curve E has potentially multiplicative reduction at $\mathfrak{P}$. Moreover, if the reduction at $\mathfrak{P}$ is multiplicative then $p \nmid \operatorname{ord}_{\mathfrak{P}}(\Delta_{\mathfrak{P}})$.*

Proof. We calculate the j-invariant. Note that

$$j(E) = \frac{c_4^3}{\Delta} = \frac{2^{12}(A^2a^{2p} - Bb^pCc^p)}{2^4A^2a^{2p}B^2b^{2p}C^2c^{2p}}.$$

And so $\operatorname{ord}_{\mathfrak{P}}(j) = 24 - 8 - 2p\operatorname{ord}_{\mathfrak{P}}(b) < 0$ as $\mathfrak{P} \mid b$. If E is multiplicative at $\mathfrak{P}$ then the proof of the previous lemma shows that the minimal discriminant at $\mathfrak{P}$ is $\Delta_{\mathfrak{P}} = 2^{-8}A^2a^{2p}B^2b^{2p}C^2c^{2p}$ and so $p \nmid \operatorname{ord}_{\mathfrak{P}}(\Delta)$. □

7.2 Possibilities for $\mathcal{N}_p$

We can now calculate the level of the newforms associated to the Frey curve of a non-trivial primitive solution (a,b,c) to the generalized Fermat equation.

Corollary 7.2.1. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field with $d = 2, 3, 6, 7$ or 11. Let (a,b,c) be a non-trivial solution to the Fermat equation (6.1) with odd prime exponent $p \geq 17$. Also let A, B, C be odd and pairwise coprime. We may scale (a,b,c) so that it remains integral and $\mathcal{N}_p^{odd}$ is as in Lemma 7.1.1 and $\mathcal{N}_p^{even} = \mathcal{N}^{even}$ where $\mathcal{N}^{even}$ is given by Lemma 7.1.3.*

7.3 Irreducibility

In order to apply the level lowering theorem (Theorem 5.3.1) we need to show that $\overline{\rho}_{E,p}$ is irreducible. In the previous chapter it was possible to achieve this by enlarging p (so p is bigger than some effective constant C_K that is dependent on the number field K see Theorem 6.1.1). In this section we will look at a result by Kraus [24] and recent work by Freitas and Siksek [15] so that we can explicitly state the bounds for each number field that we consider in this chapter. We can sometimes use the following lemma from Kraus [24]

Lemma 7.3.1. *(Kraus) Let K be a real quadratic field with class number one and E an elliptic curve over K which is semi-stable. If $\overline{\rho}_{E,p}$ is reducible then $p \leq 13$ or p divides Disc$(K) \times M_K$ where $M_K = \text{Norm}_{K/\mathbb{Q}}(u^2 - 1)$ where u is a fundamental unit of K.*

Note that for $K = \mathbb{Q}(\sqrt{2})$, $u = \sqrt{2} + 1$, $M_K = -4$ and Disc $(K) = 8$, hence the following corollary holds, as in [22].

Corollary 7.3.2. *For $K = \mathbb{Q}(\sqrt{2})$ and if E is semi-stable we have that if $\overline{\rho}_{E,p}$ is reducible then $p \leq 13$.*

For the other fields we use the following from Freitas and Siksek [15].

Theorem 7.3.3. *Let K be a real quadratic field with class number 1. Let $B = \mathrm{Norm}(\epsilon^{12} - 1)$ where ϵ is the fundamental unit of K, $p \nmid B$ be a rational prime, unramified in K, such that $p \geq 17$. If E is an elliptic curve over K which is semi-stable at all $\varpi \mid p$ and $\overline{\rho}_{E,p}$ is reducible then $p < (1 + 3^{12})^2$.*

Note that for

$d = 3$	$B = -1 \times 2^6 \times 3^3 \times 5^2 \times 13^2$
$d = 6$	$B = -1 \times 2^7 \times 3^5 \times 5^2 \times 11^2 \times 97^2$
$d = 7$	$B = -1 \times 2^{10} \times 3^4 \times 5^2 \times 7 \times 11^2 \times 17^2 \times 23^2$
$d = 11$	$B = -1 \times 2^6 \times 3^4 \times 5^2 \times 7^2 \times 11 \times 19^2 \times 397^2$

It may be possible to reduce these bounds using more advanced ideas found in Section 6 of [14].

7.4 Dealing with newforms

Combining the results from the previous sections with Theorem 5.3.1 we sometimes have Hilbert newforms appearing at the predicted level. In these cases we can sometimes use the following lemma from [14].

Lemma 7.4.1. *Let $\mathfrak{q} \nmid \mathcal{N}_p$ be a prime of K and let E be an elliptic curve over*

K which has full 2-torsion, let

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

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

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

We now have all the tools to prove the main theorem of this chapter (Theorem 7.0.1).

7.5 Proof of Theorem 7.0.1

Let $K = \mathbb{Q}(\sqrt{d})$ with $d = 2, 3, 6, 7$ or 11. We will show that the equation $Ax^p + By^p + Cz^p = 0$ with A, B, C as in the theorem has only trivial solutions in K for $p \ge 17$ if $d = 2$ (or if $d \ne 2$ for $p \ge (1 + 3^{12})^2)$). Now suppose (a, b, c) is a non-trivial solution (which we can assume is primitive) and scale this as in Corollary 7.2.1. Let $E = E_{a,b,c}$ be the Frey curve given by (5.3), and let $\overline{\rho}_{E,p}$ be its mod p representation. We know from Lemma 7.3.1 and Theorem 7.3.3 that $\overline{\rho}_{E,p}$ is irreducible. We now apply Theorem 5.3.1 to deduce that there is a cuspidal Hilbert newform $\mathfrak{f}$ over K of weight $(2, 2)$ and level $\mathcal{N}_p$ (one of the levels predicted by Corollary 7.2.1) such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ for some prime $\varpi \mid p$ of $\mathbb{Q}_{\mathfrak{f}}$. We use the lemma from Freitas and Siksek's paper on small fields that we presented in the previous section. Using `Magma` we computed the newforms $\mathfrak{f}$ at the predicted levels, the fields $\mathbb{Q}_{\mathfrak{f}}$, and eigenvalues $a_{\mathfrak{q}}(\mathfrak{f})$ at primes $\mathfrak{q}$ of K

small norm. We computed for each $\mathfrak{f}$ at level $\mathcal{N}_p$ the ideal

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

where T is the set of prime ideals $\mathfrak{q} \nmid \mathcal{N}_p$ of K with norm < 60. Let $C_{\mathfrak{f}} := \mathrm{Norm}_{\mathbb{Q}_{\mathfrak{f}}/\mathbb{Q}}(B_{\mathfrak{f}})$. If $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ then by the above lemma, $\varpi \mid B_{\mathfrak{f}}$ and so $p \mid C_{\mathfrak{f}}$. Hence, the isomorphism $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ is impossible if $p \nmid C_{\mathfrak{f}}$. Thus, the newforms satisfying $C_{\mathfrak{f}} = 0$ are the problematic ones.

Calculations in `MAGMA` [2] yield the following result. If $d = 2$, then $C_{\mathfrak{f}}$ equals either 1 or 5.

If $d = 3$, then $C_{\mathfrak{f}}$ equals either $2^3, 2^5, 3^2 \times 5, 3^2 \times 7, 2^3 \times 3^2, 2^5 \times 3 \times 5, 2^9, 2^6 \times 13, 2^5 \times 3 \times 5 \times 7, 2^5 \times 3^3 \times 5, 2^3 \times 3^3 \times 5^2, 2^5 \times 3^2 \times 5 \times 11$ or $2^{10} \times 3^3$.

If $d = 6$, then $C_{\mathfrak{f}}$ equals either $1, 2^3, 3^2, 3 \times 5, 2^3 \times 3, 3^2 \times 5, 3^2 \times 7, 2^6, 2^4 \times 3 \times 5, 2^8, 2^6 \times 3^2, 2^4 \times 3^2 \times 5, 2^4 \times 3 \times 5^2$ or $2^8 \times 5$.

If $d = 7$, then $C_{\mathfrak{f}}$ equals $1, 2^3, 2^3 \times 3, 2^6, 2^3 \times 3^2, 2^9$ or $2^3 \times 3^4$.

If $d = 11$ then $C_{\mathfrak{f}}$ equals $2^4 \times 3 \times 5, 2^8, 2^8 \times 5, 2^5 \times 3^2 \times 5, 2^8 \times 3, 2^5 \times 3 \times 5 \times 7$ or $2^{10} \times 5 \times 11^2$.

From these calculations we see that in all the cases of the theorem $C_{\mathfrak{f}} \neq 0$. Moreover, if $p \mid C_{\mathfrak{f}}$ then $p \leq 13$, which proves the theorem.

Chapter 8

Weil pairing

This chapter is a generalization of Halberstadt and Kraus [18]. We will mostly follow the exposition of Charollois [4] which looks at the proof of Theorem 2.1 of [18].

Theorem 8.0.1. *(Halberstadt and Kraus) Let a, b, c be odd pairwise coprime integers. Then there is a set of primes $\mathcal{P} = \mathcal{P}(a, b, c)$ of positive density such that if $p \in \mathcal{P}$, then the equation*

$$ax^p + by^p + cz^p = 0$$

has only trivial rational solutions $(x, y, z) \in \mathbb{Q}^3$

In this chapter we extend this work to the number field $\mathbb{Q}(\sqrt{2})$.

Theorem 8.0.2. *Let K be the number field $\mathbb{Q}(\sqrt{2})$. Let $A, B, C \in \mathcal{O}_K$ be odd with $\pm A \pm B \pm C \neq 0$ for any choice of signs and ABC not a unit. There is a set of primes $\mathcal{P} = \mathcal{P}(A, B, C)$ of positive density such that if $p \in \mathcal{P}$ then the equation*

$$Ax^p + By^p + Cz^p = 0 \tag{8.1}$$

has only trivial solutions $(x, y, z) \in (\mathcal{O}_K)^3$.

In order to prove this we need to look at the Weil pairing and prove the symplectic criterion.

8.1 Weil pairing

This section is based on Silverman ([35],III 3.5 – 6.4). First we need to look at the divisor group on an elliptic curve. Let E be an elliptic curve over K in generalized Weierstrass form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Let f be a function on $K(E) = K[X, Y]$, i.e. in K such that $Y^2+a_1XY+a_3Y = X^3 + a_2X^2 + a_4X + a_6$. We then define the divisor group.

Definition 8.1.1. *The divisor group of an elliptic curve* E*, denoted* $div(E)$*, is the free abelian group generated by the points of* E*. The divisor* $D \in div(E)$ *is a formal sum*

$$D = \sum_{P \in E} n_P(P)$$

where $n_P \in \mathbb{Z}$ *and* $n_P = 0$ *for all but finitely many* $P \in E$*. Suppose that* E *is defined over* K *and let* $f \in \bar{K}(E)^*$*. Then we can associate* f *to the divisor* $div(f)$ *given by*

$$div(f) = \sum_{P \in E} ord_P(f)(P).$$

The following theorem from ([35], III, 3.5) can be used to give a more practical approach to divisors.

Theorem 8.1.2. *Let E be an elliptic curve, $D = \sum n_i(P_i)$ a divisor of E. Then D is the divisor of a function in $\bar{K}(E)^*$ if and only if $\sum n_i = 0$ and $\sum [n_i]P_i = \mathcal{O}$.*

Remark. Note that the first is a sum of integers, while the second is addition on E.

We need the following example of a divisor to define the Weil pairing.

Example 8.1.3. *$T \in E[m]$, $T' \in E(\overline{K})$ s.t. $mT' = T$. By Theorem 8.1.2 there exists $g_T \in K(E)^*$ such that*

$$div(g_T) = \sum_{R \in E[m]} (T' + R) - \sum_{R \in E[m]} R$$

is the divisor of g_T.

Remark. Note in the example: $g_T(X + S)^m = g_T(X)^m$ for all $S \in E[m]$ and $X \in E$.

Next we define the Weil pairing denoted $\hat{e}$.

Definition 8.1.4. *We define the Weil pairing as*

$$\hat{e} : E[m] \times E[m] \to \mu_m$$

where μ_m are the m-th roots of unity, by setting

$$\hat{e}(S, T) = \frac{g_T(X + S)}{g_T(X)}$$

where $X \in E$ is any point such that $g_T(X+S)$ and $g_T(X)$ are both defined and non-zero.

After defining the Weil pairing Silverman [35] proposes the following.

Theorem 8.1.5. *The Weil pairing $\hat{e}$ has the following properties.*

- *Bilinear:*

$$\hat{e}(S_1 + S_2, T) = \hat{e}(S_1, T)\hat{e}(S_2, T)$$
$$\hat{e}(S, T_1 + T_2) = \hat{e}(S, T_1)\hat{e}(S, T_2)$$

  for all $S, S_1, S_2, T, T_1, T_2 \in E[m]$.

- *Alternating:*

$$\hat{e}(T, T) = 1$$

  for all $T \in E[m]$.

- *Non-degenerate: if all $S \in E[m]$, $\hat{e}(S, T) = 1$ then $T = \mathcal{O}$.*

- *Galois invariant:*

$$\hat{e}(S, T)^\sigma = \hat{e}(S^\sigma, T^\sigma)$$

  for all $\sigma \in G_{\bar{K}/K}, S, T \in E[m]$.

We also need the following lemma from ([36], I.1.15)

Lemma 8.1.6. *Let $E/\mathbb{C}$ be the elliptic curve associated to the oriented lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. On*

$$E[m] = m^{-1}\Lambda/\Lambda \subset \mathbb{C}/\Lambda$$

the Weil pairing is given by the following formula

$$\hat{e}\left(\frac{a\omega_1 + b\omega_2}{m}, \frac{c\omega_1 + d\omega_2}{m}\right) = e^{2\pi i(ad-bc)/m}$$

8.2 Symplectic criterion

Assume for now that we have constructed the Frey elliptic curve E associated to a non-trivial primitive solution $x, y, z \in \mathcal{O}_K$ to the generalized Fermat equation

$$Ax^p + By^p + Cz^p = 0$$

where K is a real quadratic number field with class number 1. We then calculate the newforms at the corresponding level using the level lowering theorem (Theorem 5.3.1) as we have done in the previous chapter, provided that p is large enough. These newforms can in turn be associated to an elliptic curve, denoted E'. This section will discuss the relationship between the elliptic curves E and E'.

Theorem 8.2.1. *Let $\mathfrak{P}$ be a prime above 2 in the real quadratic field K. Let E and E' be two elliptic curves over K with minimal discriminant (with respect to the prime $\mathfrak{P}$) Δ, Δ' respectively. Let p be a rational prime number. Assume that the p-torsion groups $E[p]$ and $E'[p]$ are isomorphic as $G_K = Gal(\bar{K}/K)$ modules. Assume that E and E' have multiplicative reduction at a common prime l of $\mathcal{O}_K$ such that $l \nmid p$, such that p does not divide the valuation $v_l(\Delta)$. Then*

(*a*) *The prime p does not divide $v_l(\Delta')$*

(*b*) *The following are equivalent:*

(i) the isomorphism between the representations is symplectic

(ii) the quotient $v_l(\Delta)/v_l(\Delta')$ is a square in $(\mathbb{Z}/p\mathbb{Z})^*$.

We extend Charollois' proof [4] to include real quadratic number fields.

Proof. Let L denote the maximal unramified extension of the field K localized at l. Both E and E' have multiplicative reduction at l, so their j-invariant is not an integer in L. So by the theory of the Tate curve (see chapter 2 of this thesis) E is uniformized over L by the Tate curve $\mathbb{G}_m/q^{\mathbb{Z}}$ where $q \in L$ has valuation $e = -v_l(j(E)) = v_l(\Delta)$. E is uniformized over L by the Tate curve $\mathbb{G}_m/q'^{\mathbb{Z}}$ where $q' \in L$ has valuation $e = -v_l(j(E')) = v_l(\Delta')$. The isomorphism between $E[p]$ and $E'[p]$ as G_K modules and the uniformizations combine to provide a $\mathrm{Gal}(\bar{L}/L) = G_L$ module isomorphism Ψ between $E[p]$ of $\bar{L}^*/q^{\mathbb{Z}}$ and $E'[p]$ of $\bar{L}^*/q'^{\mathbb{Z}}$. Now we look at how G_L and Ψ act on a basis of $E[p]$, which we choose as follows. We choose and fix an embedding $L \hookrightarrow \mathbb{C}$. Since L contains the p-th roots of unity, we can choose and fix ζ, a primitive root of unity such that ζ gets mapped to $e^{\frac{2\pi i}{p}}$ under the embedding. We can also fix $\gamma \in \bar{L}$, a p-th root of q. Then $\{\zeta q^{\mathbb{Z}}, \gamma q^{\mathbb{Z}}\}$ forms a basis for $E[p]$. If G_L acts transitively on the p-th conjugates $\{\zeta^j \gamma, 1 \leq j < p\}$, then there exists a $\sigma \in G_L$ such that $\sigma(\gamma) = \zeta\gamma$. The corresponding matrix is

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

as G_L fixes $\zeta \in L$. So G_L acts trivially on $E[p]$ if and only if $\gamma \in L$ i.e. if $p \mid e = v_l(q) = v_l(\Delta)$. The same holds for $E'[p]$ and e'. So since $p \nmid v_l(\Delta)$ and the Galois modules are isomorphic, it follows that $p \nmid v_l(\Delta')$, which concludes the proof of (a).

We will now look at how Ψ acts on the basis. Since $p \nmid ee'$, there exists $m, n \in \mathbb{Z}$ such that $e' = ne + mp$. Now $q'/q^n l^{mp}$ is a unit in L as $v_l(q') = e', v_l(q^n l^{mp}) = ne + mp$, so $v_l(q'/q^n l^{mp}) = 0$. So it has a p-th root $\alpha \in L$. Now we set $\gamma' = \gamma^n l^m \alpha$ then $\gamma'^p = \gamma^{np} l^{mp} \alpha^p = q^n l^{mp} q'/q^n l^{mp} = q'$. So γ' is a p-th root of q'. Hence $\{\zeta q'^{\mathbb{Z}}, \gamma' q'^{\mathbb{Z}}\}$ is a basis for $E'[p]$. Note that since Ψ is compatible with G_L we have that $\forall g \in G_L$

$$\Psi(\zeta q^{\mathbb{Z}})^g = \Psi((\zeta q^{\mathbb{Z}})^g) = \Psi(\zeta q^{\mathbb{Z}})$$

It follows that Ψ with respect to the basis $\{\zeta q^{\mathbb{Z}}, \gamma q^{\mathbb{Z}}\}$ is upper triangular, say in the form

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Also note that $\sigma(\gamma') = \sigma(\gamma)^n \sigma(l^m \alpha) = \zeta^n \gamma^n l^m \alpha = \zeta^n \gamma'$ as $l^m \alpha \in L$. So compatibility between Ψ and σ can be written in matrix terms:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \tag{8.2}$$

where the left hand side equals

$$\begin{pmatrix} a & a+b \\ 0 & d \end{pmatrix}$$

and the right hand side equals

$$\begin{pmatrix} a & b+nd \\ 0 & d \end{pmatrix}.$$

So from the upper right entry we get that $a = nd$.

We now look at the Weil pairing. Recall that it is a bilinear alternating pairing satisfying the following identities on $E[p]$ and $E'[p]$ respectively, since γ, ζ correspond to $\frac{\omega_1}{p}$, $\frac{\omega_2}{p}$ in the embedding $L \hookrightarrow \mathbb{C}$.

$$\hat{e}(\gamma q^{\mathbb{Z}}, \zeta q^{\mathbb{Z}}) = \zeta$$

and

$$\hat{e}'(\gamma q'^{\mathbb{Z}}, \zeta q'^{\mathbb{Z}}) = \zeta.$$

Now assume that Ψ is symplectic then

$$\zeta = \hat{e}(\gamma q^{\mathbb{Z}}, \zeta q^{\mathbb{Z}}) = \hat{e}'(\Psi(\gamma q^{\mathbb{Z}}), \Psi(\zeta q^{\mathbb{Z}})).$$

We know how Ψ acts on the basis so

$$\hat{e}'(\Psi(\gamma q^{\mathbb{Z}}), \Psi(\zeta q^{\mathbb{Z}})) = \hat{e}'(\zeta^b \gamma^d q^{\mathbb{Z}}, \zeta^a q^{\mathbb{Z}})$$

and now by properties of the Weil pairing

$$\hat{e}'(\zeta^b \gamma^d q^{\mathbb{Z}}, \zeta^a q^{\mathbb{Z}}) = \hat{e}'(\gamma q^{\mathbb{Z}}, \zeta q^{\mathbb{Z}})^{ad} = \zeta^{ad}.$$

So $\zeta = \zeta^{ad}$, hence $ad \equiv 1 \pmod{p}$ and since $a = nd$ it follows that $nd^2 \equiv 1 \pmod{p}$ which tells us that n is a square modulo p. Now $v_l(\Delta') = e' = ne + mp$. So $v_l(\Delta')$ is a square modulo p if and only if $v_l(\Delta)$ is a square modulo p. So their quotient is a square modulo p. Reciprocally if n is a square modulo p then there exists an $r \in \mathbb{Z}$ such that $r^2 n d^2 \equiv 1 \pmod{p}$, so Ψ^r is a symplectic isomorphism because of the following

$$\hat{e}'(\Psi^r(\gamma q^{\mathbb{Z}}), \Psi^r(\zeta q^{\mathbb{Z}})) = \hat{e}'(\zeta^w \gamma^{rd} q^{\mathbb{Z}}, \zeta^{ra} q^{\mathbb{Z}}) = \zeta^{adr^2} = \zeta^{nd^2r^2} = \zeta,$$

where $w \in \mathbb{Z}$. And now since

$$\zeta = \hat{e}(\gamma q^{\mathbb{Z}}, \zeta q^{\mathbb{Z}})$$

we get that

$$\hat{e}(\gamma q^{\mathbb{Z}}, \zeta q^{\mathbb{Z}}) = \hat{e}'(\Psi^r(\gamma q^{\mathbb{Z}}), \Psi^r(\zeta q^{\mathbb{Z}}))$$

which shows us that Ψ^r is a symplectic isomorphism, which concludes the proof.

□

8.3 Proof of Theorem 8.0.2

Suppose there is a non-trivial solution $(x, y, z) \in \mathcal{O}_K$ where $K = \mathbb{Q}(\sqrt{2})$ to the generalized Fermat equation

$$Ax^p + By^p + Cz^p = 0.$$

Since the class number of K is 1, we can assume that the solution is primitive. We associate to this solution the Frey elliptic curve

$$Y^2 = X(X - Ax^p)(X + By^p)$$

as in previous chapters. Using Theorem 5.2.2, since K is quadratic, the Frey curve E is modular. For big enough p, the Frey curve is associated to a rational Hilbert newform and this newform is associated with an elliptic curve E' (see Theorems 5.3.1 and 6.3.6). The conductor of E' is divisible only by a finite set of primes, hence there are a finite number of elliptic curves E_j for $j = 1, .., k$ with such a conductor. We apply the symplectic criterion from the previous section to the pair (E, E_j). The proof of Lemma 7.1.4 shows that the minimal discriminant of E at $\mathfrak{P}$ has the following valuation: $v_{\mathfrak{P}}(\Delta(E)) = -8 + 2pv_{\mathfrak{P}}(a)$. Choose a prime l_1 of $\mathcal{O}_K$ dividing the odd number ABC (since we assumed that ABC is not a unit) and $\mathfrak{P}$ the prime ideal above 2. Note that $v_{l_1}(\Delta(E)) = 2v_{l_1}(ABC) + 2pv_{l_1}(xyz)$. Since we can enlarge p, we can assume that p divides neither $v_{\mathfrak{P}}(\Delta(E))$ nor $v_{l_1}(\Delta(E))$. Note that we do not know if the isomorphism between E and E_j is symplectical or not. But in both cases we get that the product of the two terms

$$\frac{v_{l_1}(\Delta(E))}{v_{l_1}(\Delta(E_j))} \pmod{p} \qquad \text{and } \frac{v_{\mathfrak{P}}(\Delta(E))}{v_{\mathfrak{P}}(\Delta(E_j))} \pmod{p}$$

is a square modulo p because both terms are simultaneously squares or non-squares. The numerator of this product is

$$v_{l_1}(\Delta(E))v_{\mathfrak{P}}(\Delta(E)) \equiv 2v_{l_1}(ABC)(-8) \equiv -16v_{l_1}(ABC) \pmod{p}.$$

The symplectic criterion implies that the integer

$$n_j := -v_{l_1}(ABC)v_{l_1}(\Delta(E_j))v_{\mathfrak{P}}(\Delta(E_j))$$

has to be a square modulo p. Hence for a prime p large enough (with respect to ABC) satisfying

$$\left(\frac{n_j}{p}\right) = -1 \text{ for all } j$$

then the equation

$$Ax^p + By^p + Cz^p = 0$$

has no non-trivial solutions. It remains to show that these conditions are simultaneously satisfied on a set of positive density. We show that there is a set of positive density for which these conditions hold. To do this let p be a prime such that

1. -1 is a non-square modulo p
2. each prime divisor of n_j is a square modulo p

The first condition is equivalent to requiring that $p \equiv 3 \pmod 4$. The second one is equivalent to requiring that for every prime q that divides n_j we want $\left(\frac{q}{p}\right) = 1$. If $q = 2$ this is equivalent to requiring that $p \equiv \pm 1 \pmod 8$ and since $p \equiv 3 \pmod 4$ we need $p \equiv -1 \pmod 8$. If q is odd then $\left(\frac{q}{p}\right) = 1$ is equivalent to

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4 \\ -1 & \text{if } q \equiv 3 \pmod 4. \end{cases} \tag{8.3}$$

Now define α_q in the following way.

$$\left(\frac{\alpha_q}{q}\right) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod 4 \\ -1 & \text{if } q \equiv 3 \pmod 4. \end{cases} \tag{8.4}$$

And so if

$$p \equiv \begin{cases} -1 & \pmod 8 \\ \alpha_q & \pmod q \qquad \forall \text{ odd } q \mid \prod_j n_j \end{cases} \tag{8.5}$$

then $\left(\frac{n_j}{p}\right) = -1$ for all j and so the equation $Ax^p + By^p + Cz^p = 0$ has no non-trivial solutions. Now by the Chinese Remainder Theorem, if we define M as

$$M = 8 \prod_{\text{odd } q \mid \prod_j n_j} q,$$

then there exists an integer k such that

$$k \equiv \begin{cases} -1 & \pmod 8 \\ \alpha_q & \pmod q \qquad \forall \text{ odd } q \mid \prod_j n_j. \end{cases} \tag{8.6}$$

And so if a prime $p \equiv k \pmod M$ then there is no non-trivial solution to the generalized Fermat equation and by Dirichlet's Theorem this has density $\frac{1}{\phi(M)}$, which proves the theorem.

Bibliography

[1] D. Blasius, *Elliptic curves, Hilbert modular forms, and the Hodge conjecture*, Contributions to automorphic forms, geometry, and number theory, 83–103, Johns Hopkins Univ. Press, Baltimore, MD, 2004.

[2] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)

[3] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14 No.4** (2001), 843–939.

[4] P. Charollois, *Generalized Fermat equations (d'après Halberstadt-Kraus)* Clay Mathematics Proceedings, Volume 8, 2009, 83–89.

[5] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1996.

[6] J. E. Cremona, L. Dembélé, *Modular forms over number fields* `http://homepages.warwick.ac.uk/staff/J.E.Cremona/courses/TCC_MF/hmf_notes`

[7] A. David, *Caractère d'isogénie et critères d'irréductibilité*, `arXiv:1103.3892v2`, 8 February 2012.

[8] H. Deconinck, *On the generalized Fermat equation over totally real fields*, 225–237, Acta Arithmetica, 173.3 (2016).

[9] L. Dembélé and J. Voight, *Explicit methods for Hilbert modular forms*, 135–198 of L. Berger et al., *Elliptic curves, Hilbert modular forms and Galois deformations*, Springer, 2013.

[10] F. Diamond and J. Shurman, *A First Course on Modular Forms*, GTM **228**, Springer, 2005.

[11] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.

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

[13] N. Freitas and S. Siksek, *An Asymptotic Fermat's Last Theorem for Five-Sixths of Real Quadratic Fields*, Compositio Mathematica **151** (2015), 1395–1415.

[14] N. Freitas and S. Siksek, *Fermat's Last Theorem for some Small Real Quadratic Fields*, Algebra and Number Theory **9** (2015), 875–895.

[15] N. Freitas and S. Siksek *Criteria for irreducibility of mod p representations of Frey curves*, Journal de Thorie des Nombres de Bordeaux 27 (2015), 67–76

[16] G. Frey *Links between solutions of $A-B=C$ and elliptic curves*, Number Theory (Ulm, 1987), edited by H. P. Schlickewei and E. Wirsing, 31–62, Lecture Notes in Mathematics **1380** Springer-Verlag, New York (1989)

[17] K. Fujiwara, *Level optimisation in the totally real case*, `arXiv:0602586v1`, 27 February 2006.

[18] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. reine angew. Math. **548** (2002), 167–234.

[19] Y. Hellegouarch http://www.math.unicaen.fr/∼nitaj/hellegouarch.html.

[20] H. Hida, *On abelian varieties with complex multiplication as factors of the Jacobians of Shimura curves*, Amer. J. Math. **103** (1981), no. 4, 726–776.

[21] F. Jarvis, *Level lowering for modular mod ℓ representations over totally real fields*, Math. Ann. **313** (1999), no. 1, 141–160.

[22] F. Jarvis and P. Meekin, *The Fermat equation over* $\mathbb{Q}(\sqrt{2})$, Journal of Number Theory **109** (2004), no. 1, 182–196.

[23] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. **69** (1990) no 4, 353–385.

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

[25] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), no. 6, 1139–1161.

[26] A. Kraus, *Sur l'équation* $a^3+b^3=c^p$, Experimental Mathematics **7** (1998), No. 1, 1–13.

[27] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.

[28] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[29] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.

[30] F. Momose, *Isogenies of prime degree over number fields*, Compositio Mathematica **97** (1995), 329–348.

[31] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3, J. Number Theory **44** (1993), 119–152.

[32] A. Rajaei, *On the levels of mod ℓ Hilbert modular forms*, J. Reine Angew. Math. **537** (2001), 33–65.

[33] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Inventiones Math. **100** (1990), 431–476.

[34] S. Siksek, *The Modular Approach to Diophantine Equations*, of Belabas, Lenstra, Gaudry, Stoll, Watkins, McCallum, Poonen, Beukers, Siksek, *Explicit Methods in Number Theory: Rational Points and Diophantine Equations*, Panoramas et Synthèses **36** (2012).

Elliptic curves, Hilbert modular forms and Galois deformations, Springer, 2013.

[35] J. Silverman, *The Arithmetic of Elliptic Curves* GTM **106**, Springer 1986

[36] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves* GTM **151**, Springer 1994

[37] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts **41**, 1998.

[38] W. A. Stein, *Modular Forms: A Computational Approach*, American Mathematical Society, Graduate Studies in Mathematics **79**, 2007.

[39] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.

[40] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.