Some Generalized Fermat-type Equations via Q-Curves and Modularity

Nuno Ricardo Barroso de Freitas

Universitat de Barcelona

Some Generalized Fermat-type Equations via $\mathbb{Q}$-Curves and Modularity

Nuno Ricardo Barroso de Freitas

Some Generalized Fermat-type Equations via $\mathbb{Q}$-Curves and Modularity

Nuno Ricardo Barroso de Freitas
Supervised by Luis V. Dieulefait

Memòria presentada per a optar al grau de
Doctor en Matemàtiques

Universitat de Barcelona
Departament d'Àlgebra i Geometria

2010 Mathematics Subject Classification:
Primary 11D41; Secondary 11F80, 11G05.

This research was supported by the scholarship with reference SFRH / BD / 44283 / 2008 from *Fundação para a Ciência e a Tecnologia*, Portugal.

Aos meus pais e avô

Acknowledgements

I would like to acknowledge everyone who directly or indirectly influenced this thesis.

My first and greatest thanks go to my thesis advisor Luis Dieulefait. I would like to thank him for providing the interesting topic and for patiently supporting me through it. Mostly, I want to thank him for all the insight and motivation he transmitted me during our meetings.

I want to thank Nicolas Billerey and Gabor Wiese for their numerous comments and suggestions that greatly improved the manuscript.

Roger Picken and Bernat Anton for reviewing part of the text.

John Voight for his help computing newforms that were fundamental to part of the argument. John Cremona for providing a useful list of elliptic curves.

I also want to thank all the people with whom I discussed and learned about mathematics during the last four years. I am particularly grateful to Ariel Pacetti, Nicolas Billerey, Bernat Anton, Sara Arias de Reyna, Gabor Wiese, John Voight, Klara Stokes, Samuele Anni, Piermarco Milione, Miguel Hernaiz, Iván Blanco and specially Panagiotis Tsaknias.

I want to thank Gabor Wiese for having me at his research group for three months.

Ricardo Garcia for kindly tutoring me during my first year in Barcelona.

Finally, I thank all my friends and family who encouraged and assisted me. My parents deserve a special acknowledgment for the constant support and curiosity.

Contents

Introduction

The main purpose of this thesis is to apply the *modular approach* to study some Fermat-type Diophantine equations of signature (r, r, p).

We begin by recalling Fermat's Last Theorem (FLT) whose proof was a turning point in the way that people looked at Diophantine equations.

Theorem 0.0.1 *(Fermat-Wiles) Let $n > 2$ be an integer. Then, the equation $x^n + y^n = z^n$ has no solutions (a, b, c) such that $abc \neq 0$.*

The strategy that led to the proof of FLT is called the *modular approach* and makes a remarkable use of elliptic curves, modular forms and Galois representations. It started with ideas which came from Frey, Hellegouarch and Serre, followed up by Ribet and taken to a conclusion by Andrew Wiles (see [76]). After Wiles' completion of the proof, the original strategy was strengthened and several mathematicians achieved great success in solving other equations that previously seemed intractable. As a consequence of these efforts, the generalized Fermat equation

$$Ax^p + By^q = Cz^r, \quad \text{where} \quad 1/p + 1/q + 1/r < 1, \tag{1}$$

with p, q, r primes and A, B, C pairwise coprime integers became the new center of attention. We call the triple of exponents (p, q, r) as in (1) the *signature* of the equation. In general, for fixed pairwise coprime integers A, B, C, equation (1) may have infinitely many solutions for a fixed signature. For example, if $z = a^3 + b^3$, $x = az$, $y = bz$ then (x, y, z) satisfies $x^3 + y^3 = z^4$. However, if we assume the *abc*-conjecture it follows that there are only a finite number of solutions (a, b, c) to the generalized Fermat equation (1) satisfying $\gcd(a, b, c) = 1$ (see Section 5.2 in [20] and the references there). More precisely,

Conjecture 0.0.2 *Let $A, B, C \in \mathbb{Z}$ be fixed and pairwise coprime. There is only a finite number of sextuples (a, b, c, p, q, r) satisfying:*

1. *$p, q, r \in \mathbb{Z}$ primes such that $1/p + 1/q + 1/r < 1$,*
2. *$(a, b, c) \in (\mathbb{Z} \setminus \{0\})^3$ and $\gcd(a, b, c) = 1$ (primitive solutions),*
3. *$Aa^p + Bb^q = Cc^r$.*

Remark 0.0.3 *For the conjecture we count solutions like* $1^p + 2^3 = 3^2$ *only once.*

As evidence for this conjecture, an important result due to Darmon-Granville [20] states that for fixed A, B, C as above and a fixed triple (p, q, r) such that $1/p + 1/q + 1/r < 1$ there exists only a finite number of primitive solutions. Also, the modular approach has been successfully used to prove the non-existence of solutions for several particular cases, including infinite subfamilies. For example, $x^p + y^p = z^2$ or $x^p + y^p = z^3$ were settled by Darmon-Merel [21] and both are special cases of the important equation $x^p + y^q = z^r$. Another important step forward was the work of Ellenberg on the representations attached to $\mathbb{Q}$-curves. It allowed him to introduce the use of $\mathbb{Q}$-curves as Frey curves and, in particular, allowed him to solve the equations $x^4 + y^2 = z^p$ (see [29]). For a recent overview and summary of known results on Fermat-type equations see the introduction in [3] and [18].

Another important subfamily are the equations of signature (r, r, p) for r a fixed prime, i.e.

$$Ax^r + By^r = Cz^p \quad (p \text{ is allowed to vary}).$$

Concerning these equations there are works for signature $(3, 3, p)$ by Kraus [45], Bruin [10], Chen-Siksek [16] and Dahmen [18]; for $(5, 5, p)$ by Billerey [5] and Billerey-Dieulefait [6].

The successive generalizations of the modular approach to attack new equations are all highly dependent on the specific equation under analysis. As a general method to attack the generalized Fermat equation of signature (p, q, r) there is a remarkable program explained by Darmon in [19] which makes use of Frey abelian varieties of higher dimension. However, it seems that currently little is known about these varieties and in [19] only a few particular cases of the equation $x^p + y^p = z^r$ (for small values of r) are solved.

Broadly speaking, we can divide the modular approach to Diophantine equations into three main steps:

(I) [Construction of a Frey curve] Attach an appropriate elliptic curve E (often called a Frey or Hellegouarch-Frey curve) to a putative solution (of a certain type);

(II) [Modularity/Level Lowering] Prove modularity of E and irreducibility of some Galois representations attached to it, to conclude (via level lowering results), that the Frey curve (or a related object) corresponds to a (Hilbert) modular form whose level is almost independent of the choice of the solution;

(III) [Contradiction] Contradict the previous step by showing that among the (finitely many) (Hilbert) modular forms of predicted type, none of them corresponds to E.

In this thesis we will use the modular approach to go further into equations of signature (r, r, p) of the particular form $x^r + y^r = Cz^p$, where C is an integer divisible only by primes $q \not\equiv 1, 0$ modulo r. In particular, we will improve the results for $r = 5$ and provide new results for $r = 7$ and $r = 13$. Furthermore, using elliptic curves, we will outline a strategy

that can be used to attack the previous equation for any prime r. Indeed, we complete Step (I) and partly Step (II) of the modular approach for all r (Step (III) is highly dependent on r). Moreover, we will also prove a modularity result of independent interest for elliptic curves with good reduction at 3 over certain number fields.

The results in Chapter 2 regarding the equation $x^5 + y^5 = Cz^p$ have been accepted for a joint publication with L. Dieulefait in *Mathematics of Computation* (see [27]).

Thesis outline and statement of results

We will now describe the content of each chapter in this thesis. In particular, we will state the results that we obtained and comment on the main strategies used.

In this work we will call a solution $(a, b, c) \in \mathbb{Z}^3$ to $x^r + y^r = Cz^p$ *primitive* if $\gcd(a, b) = 1$. Moreover, we will say it is *trivial* if $|abc| \leq 1$ and *non-trivial* otherwise. In particular, our primitive solutions are primitive in the sense that $\gcd(a, b, c) = 1$ as above. We will also say that a primitive solution is *a first case solution* if $r \nmid c$ and *a second case solution* otherwise.

Chapter 1 is mainly devoted to cover background material necessary to the modular approach via elliptic curves over $\mathbb{Q}$. It includes the basic definitions and theorems about elliptic curves, modular forms and their attached representations. In particular, we will prove in detail a theorem due to Hellegouarch about the ramification of the mod p representations attached to some elliptic curves that will be used recurrently in later chapters. We will also state modularity theorems over $\mathbb{Q}$, Ribet's level lowering theorem and Serre's conjecture. We end Chapter 1 with a sketch of the proof of Fermat's Last Theorem as motivation for the generalizations in subsequent chapters.

In Chapter 2 we will work with equations of the form $x^5 + y^5 = Cz^p$. Regarding these equations the following theorem is a consequence of the work of Billerey [5] later improved by Billerey-Dieulefait in [6].

Theorem 0.0.4 *Let $C = 2^\alpha 3^\beta 5^\gamma$ where $\alpha \geq 2$, $\beta, \gamma \geq 0$, or $C = 7, 13$. Then, for $p > 19$ the equation $x^5 + y^5 = Cz^p$ has no non-trivial primitive solution.*

Note that in their theorem $|C| \geq 4$. We will improve on their result by proving the following.

Theorem 0.0.5 *Let β be an integer divisible only by primes $l \not\equiv 1 \pmod 5$. Suppose that $p \equiv 1 \pmod 4$ or $p \equiv \pm 1 \pmod 5$. Then,*

(A) *If $p > 13$, the equation $x^5 + y^5 = 2\beta z^p$ has no non-trivial primitive solutions.*

(B) *If $p > 73$, the equation $x^5 + y^5 = 3\beta z^p$ has no non-trivial primitive solutions.*

Along this chapter, we will introduce the necessary theory used in the proof of this theorem. In particular, we will cover material on the theory of abelian varieties attached to $\mathbb{Q}$-curves

and embedding problems from the works of J. Quer [54], [55]. Moreover, Ellenberg's results on the Galois representations attached to $\mathbb{Q}$-curves from [29] are also stated and used.

The first important idea for the proof of the previous theorem is to relate a non-trivial primitive solution of $x^5+y^5 = Cz^p$ to a solution (a, b, c) of a related equation (not depending on C and defined over $\mathbb{Q}$) satisfying $C \mid a + b$. Then we apply the modular approach with $\mathbb{Q}$-curves to show that the solution (a, b, c) to the latter equation cannot exist. For this purpose, we first attach to (a, b, c) a Frey curve $E_{(a,b)}$ over $\mathbb{Q}(\sqrt{5})$ and we prove that it is a $\mathbb{Q}$-curve (Step (I)). Second, using Quer's theory from [54], [55] we produce a suitable twist $E_\gamma(a, b)$ of $E_{(a,b)}$ completely defined over a certain cyclic number field K of degree four. The idea of using embedding problems to determine E_γ is not new in the literature (see [20]), but it seems to be the first time that a cyclic extension of degree four is necessary, which makes the computations technically difficult. We then show that the Weil restriction (denoted B) from K to $\mathbb{Q}$ of E_γ is a product of varieties of GL_2-type. This is fundamental, because we are able to compute all the Serre invariants associated with a representation $\bar{\rho}$ attached to B and then we apply Serre's conjecture to it, concluding Step (II). Finally, to complete the proof we have to perform Step (III). This is done by a case-by-case analysis of the newforms in the spaces predicted by Serre's conjecture. We use several known methods for eliminating newforms and we introduce a new one via a theorem of Carayol. Up to this point we will have proved a weaker version of the previous theorem. Then, we introduce an extra Frey curve F and making use of Siksek's multi-Frey technique (see [11]) we complete its proof.

Chapter 3 is devoted to developing a new general strategy to attack infinitely many equations of signature (r, r, p) for each fixed prime $r \geq 7$. On the one hand, in [19] Darmon develops a program to attack Fermat equations of general signature (p, q, r) using higher dimensional abelian varieties. On the other hand, there is no general algorithm that performs Step (I) for a random Diophantine equation, even of Fermat type. Our method, despite being limited to signature (r, r, p) has the advantage that it gives an algorithm for constructing several Frey elliptic curves. This is an advantage over [19] because it allows a better understanding of the representations involved.

We start Chapter 3 by introducing Hilbert modular forms and the level lowering theorems due to Jarvis, Rajaei and Fujiwara. Then we proceed to the description of a general method that allows one to complete Step (I) and part of Step (II) of the modular approach for infinitely many equations of the form $x^r + y^r = Cz^p$. In the next paragraphs we will summarize the main ideas.

Fix a prime $r \geq 7$ and let K^+ be the maximal totally real subfield of $\mathbb{Q}(\zeta_r)$. Let $C \neq 0$ be an integer divisible only by primes $q \neq r$ not congruent to 1 (mod r). Generalizing the idea in Chapter 2, we start by relating a non-trivial primitive solution (a, b, c') to $x^r + y^r = Cz^p$ to solutions (a, b, c), such that $C \mid a + b$, of several other Diophantine equations (not depending on C) defined over K^+. Then we attach Frey curves $E = E_{(a,b)}$ to solutions of the latter equations. Very briefly: we let $\phi_r(x, y) = (x^r + y^r)/(x + y)$ and pick a certain

three different factors f_1, f_2, f_3 defined over K^+ of $\phi_r(x, y)$; then we find α, β, γ such that $\alpha f_1 + \beta f_2 + \gamma f_3 = 0$ and we apply over K^+ the original construction of Frey. Since E will only depend on a, b and these are constant during the process we obtain several Frey curves attached to the initial solution (a, b, c'). This completes Step (I) in complete generality.

Although Step (II) (modularity / irreducibility) is a classical application of deep results mainly due to Mazur, Ribet and Wiles when the curve E is defined over $\mathbb{Q}$, the situation is much more complicated when E is defined over a bigger field. In particular, analogues of these results are mostly conjectural. In this direction, we will prove a rather general result regarding irreducibility of the mod p representations attached to some elliptic curves and a new modularity statement for elliptic curves over totally real number fields under certain local conditions at 3. More precisely, we will prove the following theorems

Theorem 0.0.6 *Let F be a totally real number field and C/F be an elliptic curve with conductor N_E. Let A be the factor of N_E corresponding to the additive primes. Suppose further that $\mathfrak{q} \nmid N_C$ is a fixed prime of good reduction. Then, there exists an explicit constant $M(F, A, \mathfrak{q})$ such that, if*

1. *p is odd and unramified in F,*
2. *all primes $\mathfrak{p} \mid p$ are of semistable reduction for C,*
3. *$p > M(F, A, \mathfrak{q})$,*

then, the representation $\bar{\rho}_{C,p}$ is absolutely irreducible.

Theorem 0.0.7 *Let F be a totally real abelian number field and C an elliptic curve defined over F. Suppose that 3 splits in F and C has good reduction at the primes above 3. Then C is modular.*

A fundamental step in the proof of the modularity statement is to guarantee residual modularity of $\bar{\rho}_{C,p}$ which is achieved as a consequence of a deep theorem due to Langlands-Tunnell. The rest of the proof is divided into three cases: (i) $\bar{\rho}_{C,3}$ and $\bar{\rho}_{C,3}|G_{F(\sqrt{-3})}$ both abs. irreducible; (ii) $\bar{\rho}_{C,3}$ abs. irreducible and $\bar{\rho}_{E,3}|G_{F(\sqrt{-3})}$ reducible; (iii) $\bar{\rho}_{C,3}$ reducible. In each case we have to show that all the conditions are satisfied for a suitable modularity lifting theorem due to Kisin or Skinner-Wiles to apply. In particular, we need to use Savitt and Breuil's work to guarantee the existence of ordinary liftings.

The previous theorems provide a complete answer to the irreducibility part of Step (II) and a partial answer regarding the modularity part. More precisely, it is a consequence of the irreducibility theorem that for each prime $r \geq 7$ there exists a constant $M(r)$ such that, if $p > M(r)$ then the representation $\bar{\rho}_{E,p}$ is absolutely irreducible. Moreover, it is a corollary of the modularity statement that our method of constructing Frey curves is able to produce modular Frey curves for $r = 7$ and $r = 13$. The main obstacle to proving modularity of the Frey curves for all r is the difficulty in guaranteeing the existence of modular nearly-ordinary

liftings (in the residually locally reducible case) when 3 is unramified and non-split in F. Nevertheless, we will also discuss a method that for particular values of r may allow one to check if a Frey curve is modular.

Finally, we will compute the conductors of all Frey curves E and for p a semistable prime for E we also compute the Artin conductors of $\bar{\rho}_{E,p}$ and prove that $\bar{\rho}_{E,p}$ is finite at all $\mathfrak{p} \mid p$. We will also include the statements of the level lowering results for Hilbert modular forms due to Jarvis, Rajaei and Fujiwara and explain how to apply them in our situation, leading to a modular approach via HMF. The limitations of our method will become clear in Chapter 4 when performing Step (III) in the cases $r = 7, 13$. Nevertheless, in Chapter 3 we also include a discussion concerning the two major limitations of the method: 1) limitations due to the existence of trivial solutions; 2) computational limitations. Limitations of type 1) lead one to solve equations only for first case solutions. Furthermore, regarding limitations of type 2) we will prove that when r is congruent to 1 modulo 6, one can construct a Frey curve defined over the totally real subfield of K^+ of degree $(r-1)/6$. This observation will be crucial when dealing with specific examples in Chapter 4, as it considerably reduces the amount of computations that are needed to perform Step (III).

In Chapter 4 we will apply the general strategy developed in Chapter 3 to some specific values of r and C. In particular, we will give explicit examples of Frey curves for $r = 7, 11, 13, 17, 19$ and complete Step (III) in the cases $r = 7$ and $r = 13$. To our knowledge, no arithmetic results on equations of signature $(7, 7, p)$ and $(13, 13, p)$ were previously known. Moreover, the case $r = 13$ seems to be the first occurrence where the Weil restrictions of the Frey curves involved are not of GL_2-type over $\mathbb{Q}$. In particular, this means that instead of classical cuspforms one must use Hilbert cuspforms (in this case over $\mathbb{Q}(\sqrt{13})$). So, leaving aside the intrinsic interest of the arithmetic statements obtained, the results in Chapter 4 illustrate the strengths of the general methods developed in the previous chapter.

We start Chapter 4 by completing Step (III) for $r = 7$ by proving the following

Theorem 0.0.8 *Let $d = 2^{s_0}3^{s_1}5^{s_2}$ and γ be an integer only divisible by primes $l \not\equiv 1, 0 \pmod 7$. Then, if $p \geq 17$ we have that*

- *(I) The equation $x^7+y^7 = d\gamma z^p$ has no non-trivial first case solutions if (s_0, s_1, s_2) satisfies any of the following three conditions $(\geq 2, \geq 0, \geq 0)$, $(= 1, \geq 1, \geq 0)$ or $(= 0, \geq 0, \geq 1)$.*
- *(II) The equation $x^{14} + y^{14} = d\gamma z^p$ has no non-trivial primitive solutions if $s_1 > 0$ or $s_2 > 0$ or $s_0 \geq 2$.*

With similar techniques to those in the proof of the previous theorem we will also prove

Theorem 0.0.9 *Let $p > 254^{2873}$ be a prime. Then the equation*

$$x^6 - x^5y + x^4y^2 - x^3y^3 + x^2y^4 - xy^5 + y^6 = 71z^p$$

has no solutions $(x, y, z) = (a, b, c)$ such that $(a, b) = 1$ and $|abc| > 1$.

Although the Frey curve used in the proof of these theorems was known (but obtained by different methods), no previous arithmetic application of it seemed to exist. Finally, we will perform Step (III) for $r = 13$. The curve used in this case is new and its Hilbert modularity follows from the results in Chapter 3. In particular, we will prove

Theorem 0.0.10 *Let $d = 3, 5, 7$ or 11 and γ be an integer divisible only by primes $l \not\equiv 1, 0 \pmod{13}$. If $p > 4992539$ is a prime, then:*

(I) The equation $x^{13} + y^{13} = d\gamma z^p$ has no non-trivial primitive first case solutions.

(II) The equation $x^{26} + y^{26} = 10\gamma z^p$ has no non-trivial primitive solutions.

The large bounds for the exponent p in the previous two theorems may look surprising at a first glance. The reason for them is that computing completely the relevant spaces of newforms is computationally impossible. Nevertheless, we are able to complete Step (III) by computing only the newforms with the field of coefficients $\mathbb{Q}$ (and some partial information about the other newforms in the case $r = 13$). To compensate this lack of information we will use theoretical arguments that require to impose the bounds. In particular, for the proof in the case $r = 13$ we needed to compute Hilbert newforms over $\mathbb{Q}(\sqrt{13})$ with level 104 and 208 of parallel weight 2. This was beyond our computational resources, but John Voight was able to compute for us all the newforms with coefficient field equal to $\mathbb{Q}$ and the factorization of the characteristic polynomial of one Hecke operator in the whole space (the data he computed can be found in the appendix).

In Chapter 5 we will propose two more Frey curves attached to solutions of $x^r + y^r = Cz^p$ for primes $r = 4m + 1$. To do this we will adapt the ideas in Chapter 3 on how to relate solutions of different equations and then we generalize the method that led to the $\mathbb{Q}$-curves E and F in Chapter 2. The resulting curves are defined over K^+ and we will show that they are k-curves, where k is the only number field such that $[K^+ : k] = 2$. Then we compute their discriminant and the Artin conductor of its attached mod p representations, showing that they satisfy the required properties to be a useful Frey curve. To end the chapter, we will discuss how the theory of J. Quer on embedding problems can be applied to extend the representations of G_{K^+} attached to the new Frey curves to representations of G_k.

Notation

We fix algebraic closures $\overline{\mathbb{Q}}$, $\overline{\mathbb{R}} = \mathbb{C}$ and $\overline{\mathbb{Q}}_p$ for all p. Choose embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and $\overline{\mathbb{Q}}_p$ for all p so that we can identify $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with decomposition subgroups of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. $G_{\mathbb{Q}}$ is endowed with the Krull topology.

K will always denote a number field (i.e. a finite extension of $\mathbb{Q}$) and $\mathcal{O}_K$ its ring of integers. For any number field K we fix an embedding into $\overline{\mathbb{Q}}$ so we can write $G_K = \mathrm{Gal}(\overline{K}/K) = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ as an open subgroup of $G_{\mathbb{Q}}$.

In a number field K, the symbols $\mathfrak{P}$, $\mathfrak{P}_q$ will denote primes in K above the rational prime p or q and $\mathrm{Frob}_{\mathfrak{P}}$ a corresponding Frobenius element.

For a prime ideal $\mathfrak{P}$ we let $v_{\mathfrak{P}}$ denote the normalized $\mathfrak{P}$-adic valuation and $K_{\mathfrak{P}}$ the $\mathfrak{P}$-adic completion of the number field K. L will denote a finite extension of $\mathbb{Q}_l$.

$\mathbb{F}_{p^f}$ will denote the finite field with p^f elements with discrete topology. $\overline{\mathbb{F}}_p$ is a fixed algebraic closure of $\mathbb{F}_p$ and we denote its Galois group by $G_{\mathbb{F}_p} = Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p)$.

An elliptic curve will always be denoted by E or C.

For $a, d \in K$ the symbol (a, b) will denote the quaternion algebra with basis $\{1, i, j, k\}$ and product determined by $i^2 = a$, $j^2 = d$,$ij = -ji = k$.

$\mathrm{rad}(c)$ will denote the product of the prime (ideals) factors of the algebraic integer c.

Chapter 1

The Modular Approach to Fermat's Last Theorem

In this chapter we will introduce some of the ideas and tools that are part the modular approach. Then we will prove Fermat's Last Theorem (FLT) as motivation for the work in later chapters. All the content in this chapter is standard in the literature and can be found in [25], [51], [35] and [66].

1.1 Galois Representations

The core of the modular approach is the interplay between Galois representations arising from distinct mathematical objects. In this section we will briefly recall some well established facts (some very deep) about representations arising from elliptic curves and modular forms.

Let K be a number field and recall that we are considering the absolute Galois groups G_K endowed with the Krull topology.

Definition 1.1.1 *Let L be a finite extension of $\mathbb{Q}_l$. A continuous group homomorphism $\rho : G_K \to GL_d(L)$ is called a d-dimensional l-adic Galois representation. Any two d-dimensional l-adic representations ρ, ρ' are said to be isomorphic ($\rho \sim \rho'$) over the field $L' \subset \bar{\mathbb{Q}}_l$ if $L \subset L'$ and there exists an element $M \in GL_d(L')$ such that $\rho'(\sigma) = M\rho(\sigma)M^{-1}$ for all $\sigma \in G_K$.*

For ρ as above, if L coincides with K_λ, the localization of a number field K at a prime $\lambda \mid l$, we say that ρ is a λ-adic representation. For example, we will see that λ-adic representations arise naturally from modular forms.

Proposition 1.1.2 *Let $\rho : G_K \to GL_d(L)$ be an l-adic representation. Then ρ is isomorphic to a representation $\rho' : G_K \to GL_d(\mathcal{O}_L)$*

Proof: See [25] Proposition 9.3.5 for the case $K = \mathbb{Q}$. The general case follows analogously, because the core of the argument is the compacity of $G_{\mathbb{Q}}$ which is also true for G_K.

■

Definition 1.1.3 *A d-dimensional mod p Galois representation is a continuous group homomorphism $\rho : G_K \to GL_d(\bar{\mathbb{F}}_p)$. Any two d-dimensional mod p representations ρ, ρ' are said to be isomorphic ($\rho \sim \rho'$) over the field $\mathbb{F}_{p^r} \subset \bar{\mathbb{F}}_p$ if there exists an element $M \in GL_d(\mathbb{F}_{p^r})$ such that $\rho'(\sigma) = M\rho(\sigma)M^{-1}$ for all $\sigma \in G_K$.*

Given an l-adic representation ρ of G_K by Proposition 1.1.2 we can suppose it has values in $\mathrm{GL}_d(\mathcal{O}_L)$. This corresponds to finding a lattice that is invariant under G_K. Then by reducing modulo the maximal ideal of $\mathcal{O}_L$ we obtain a mod l representation $\bar{\rho} : G_K \to \mathrm{GL}_d(k)$, where $k = \mathbb{F}_{l^r}$ is the residue field of L. A representation $\bar{\rho}$ constructed this way is called *a residual representation of* ρ. Changing the lattice would give us a different representation, but it is know that this process is well defined up to semisiplification. In particular, if one $\bar{\rho}$ is irreducible then all residual representations obtained from ρ are isomorphic.

We will now briefly recall the definitions and some facts about the Frobenius elements inside $G_{\mathbb{Q}}$ (see [25]).

Definition 1.1.4 *Let p be a prime and $\mathfrak{P} \subset \bar{\mathbb{Z}}$ any maximal ideal over p. The decomposition and inertia groups at $\mathfrak{P}$ are defined by*

$$\begin{aligned} D_{\mathfrak{P}} &= \{\sigma \in G_{\mathbb{Q}} : \mathfrak{P}^\sigma = \mathfrak{P}\} \\ I_{\mathfrak{P}} &= \{\sigma \in D_{\mathfrak{P}} : x^\sigma \equiv x \ (mod\ \mathfrak{P}) \text{ for all } x \in \bar{\mathbb{Z}}\} \end{aligned}$$

Then $\sigma \in D_{\mathfrak{P}}$ acts on $\bar{\mathbb{Z}}/\mathfrak{P} = \bar{\mathbb{F}}_p$ as $(x+\mathfrak{P})^\sigma = x^\sigma + \mathfrak{P}$ and $I_{\mathfrak{P}}$ is the kernel of the reduction $D_{\mathfrak{P}} \to G_{\mathbb{F}_p}$. An (absolute) Frobenius element over p is any preimage $Frob_{\mathfrak{P}} \in D_{\mathfrak{P}}$ of the Frobenius automorphism in $G_{\mathbb{F}_p}$ ($x \mapsto x^p$).

$\mathrm{Frob}_{\mathfrak{p}}$ is defined only up to the inertia subgroup at $\mathfrak{p}$. For each number field K the restriction map $G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q})$ takes an absolute Frobenius to a corresponding Frobenius for K (see sec. 9.1 in [25]). There is a natural isomorphisms between $D_{\mathfrak{P}}$ and the local absolute Galois group $G_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. For a finite extension F/K, if p is a prime in K below $\mathfrak{p}$ in F we have $D_{\mathfrak{p}} \simeq \mathrm{Gal}(F_{\mathfrak{p}}/K_p)$.

Theorem 1.1.5 *(Chebotarev) For each maximal ideal $\mathfrak{P}$ of $\overline{\mathbb{Z}}$ lying over any but a finite set of rational primes p, choose an absolute Frobenius element $Frob_{\mathfrak{P}}$. The set of such elements is a dense subset of $G_{\mathbb{Q}}$.*

Definition 1.1.6 *Let ρ be a Galois representation of G_K and let $\mathfrak{p}$ be a prime in K. Then ρ is said to be unramified at $\mathfrak{p}$ if the inertia subgroup $I_{\mathfrak{P}}$ is contained in $ker\rho$ for some maximal ideal $\mathfrak{P} \subset \bar{\mathbb{Z}}$ lying over $\mathfrak{p}$.*

Theorem 1.1.7 *Let ρ and ρ' be two irreducible continuous l-adic or mod p Galois representations both ramified only at a finite set of primes. If for all but finitely many primes q,*

where both representations are unramified, we have

$$\begin{aligned} Trace(\rho(Frob_q)) &= Trace(\rho'(Frob_q)) \\ Det(\rho(Frob_q)) &= Det(\rho'(Frob_q)) \end{aligned}$$

then ρ and ρ' are isomorphic.

Let F be a totally real number field F of degree d and ι_i for $i = 1, .., d$ its embeddings into $\mathbb{C}$. Since F is totally real, each ι_i sends F into $\mathbb{R}$ and induces an inclusion ϕ_i of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ into G_F. To the image of the generator of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ via ϕ_i we call *a complex conjugation.*

Definition 1.1.8 *Let F be a totally real field. A 2-dimensional Galois representation ρ of G_F is said to be totally odd if $det(\rho(c)) = -1$, for c any complex conjugation.*

1.1.1 Elliptic Curves

Elliptic curves are algebraic curves of genus 1 having a specified base point. They play a key role in the modular approach since we will attach to a putative solution of a particular Diophantine equation an elliptic curve.

Definition 1.1.9 *Let k be a field and $\bar{k}$ an algebraic closure of k. A Weierstrass equation over k is any cubic equation of the form*

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

where all $a_i \in k$. If $char(k) \neq 2, 3$, by a change of coordinates, it can be written in the form

$$y^2 = x^3 + Ax + B, \quad A, B \in k$$

and has discriminant $\Delta(E) = -16(4A^3 + 27B^2)$. If $\Delta(E) \neq 0$ then E is nonsingular and the set

$$E = \{(x, y) \in \bar{k}^2 \text{ satisfying } E(x, y)\} \cup \{\infty\}$$

is an elliptic curve over k.

Let E be an elliptic curve defined over a number field K. It is known that there is a group structure on E and for $n \geq 1$ let $V = E(\bar{\mathbb{Q}})[n]$ be the n-torsion points. V is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2 and the group G_K acts linearly on V. Indeed, if P_1, P_2 is a basis of V, for each element $\sigma \in G_K$ we have

$$(\sigma(P_1), \sigma(P_2)) = (P_1, P_2) \begin{bmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{bmatrix}.$$

If Q_1, Q_2 is an arbitrary pair of points in V such that

$$\begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix} = \begin{bmatrix} \lambda & \nu \\ \mu & \delta \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$$

then by linearity we have

$$\begin{pmatrix} \sigma(Q_1) \\ \sigma(Q_2) \end{pmatrix} = \begin{bmatrix} \lambda & \nu \\ \mu & \delta \end{bmatrix} \begin{bmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}.$$

Also it can easily be checked that

$$\begin{bmatrix} a_{\sigma\circ\tau} & b_{\sigma\circ\tau} \\ c_{\sigma\circ\tau} & d_{\sigma\circ\tau} \end{bmatrix} = \begin{bmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{bmatrix} \begin{bmatrix} a_\tau & b_\tau \\ c_\tau & d_\tau \end{bmatrix}$$

and in particular,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{bmatrix} \begin{bmatrix} a_{\sigma^{-1}} & b_{\sigma^{-1}} \\ c_{\sigma^{-1}} & d_{\sigma^{-1}} \end{bmatrix}.$$

Hence we have,

Theorem 1.1.10 *The action of G_K on V defines a representation*

$$\bar{\rho}_{E,n} : G_K \longrightarrow GL_2(\mathbb{Z}/n\mathbb{Z}).$$

The image is isomorphic to the Galois group of the extension $K(E[n])/K$.

Proposition 1.1.11 *Let p be a prime. The representations $\bar{\rho}_{E,p} : G_K \to GL_2(\mathbb{F}_p)$ arising from the p-torsion of elliptic curves E defined over a totally real field K are totally odd.*

An important step of the modular method is to guarantee the absolute irreducibility of the representations $\bar{\rho}_{E,p}$ for primes p greater than a constant.

Proposition 1.1.12 *Let p be an odd prime. Let F be a totally real field and $\bar{\rho} : G_F \to GL_2(\mathbb{F}_p)$ a totally odd representation. Then $\bar{\rho}$ is irreducible if and only if it is absolutely irreducible.*

Proof: If $\bar{\rho}$ is absolutely irreducible then it is irreducible. Suppose that $\bar{\rho}$ is not absolutely irreducible and let c be a complex conjugation. Since $\det(\bar{\rho}(c)) = -1$ and c has order 2 it follows that there exist a matrix $M \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $M\bar{\rho}(c)M^{-1}$ is a diagonal matrix having distinct eigenvalues 1 and -1. Furthermore, we have that $\bar{\rho}(c)$ has two 1-dimensional eigenspaces, generated by, $v_+, v_- \in \mathbb{F}_p^2$. Since $\bar{\rho}$ is absolutely reducible there exists a basis such that $\bar{\rho}$ is upper triangular leaving invariant a one dimensional subspace generated by $w \in \bar{\mathbb{F}}_p^2$. In particular, w is an eigenvector of $\bar{\rho}(c)$, hence v_+ or v_- is a scalar multiple of w and we obtain a 1-dimensional subspace of $\mathbb{F}_p^2$ left invariant by $\bar{\rho}$, i.e. $\bar{\rho}$ is not irreducible.

■

We will say that an elliptic curve E is semistable if all primes of bad reduction are of multiplicative reduction. In particular, the conductor of E is square-free. For semistable elliptic curves over $\mathbb{Q}$ there is Theorem 1.1.13 below (due to Mazur [48]), regarding irreducibility of $\bar{\rho}_{E,p}$ (see also Theorem 22 in [18]). However, for curves over number fields we need to use other arguments that depend on the particular curve E. This will be clear in later chapters.

Theorem 1.1.13 *(Mazur) Let E be an elliptic curve over $\mathbb{Q}$ and p a prime.*

(i) If $p \geq 11$ and E is semistable, or

(ii) If $p \geq 5$, E is semistable and all the 2-torsion is rational.

Then, the representation $\bar{\rho}_{E,p}$ is irreducible

Together with irreducibility of $\bar{\rho}_{E,p}$ we are also interested in studying its ramification. Let E/K be an elliptic curve and l a prime in K. $\bar{\rho}_{E,p}$ ramifies at l if and only if the action of $I_\mathfrak{l}$ on $E[p]$ is non-trivial if and only if the field extension $K_p = K(E[p])/K$ has non-trivial inertia subgroup at l, that is K_p ramifies at l. The next theorem will be used over $\mathbb{Q}$ in the proof of FLT and over number fields in later chapters.

Theorem 1.1.14 *(Hellegouarch) Let E/K be an elliptic curve and l an odd prime unramified in K not above the rational prime p. Let $\Delta(E)$ be the discriminant of a minimal model at l of E. If l is a prime of multiplicative reduction and $p \mid v_l(\Delta)$ then $\bar{\rho}_{E,p}$ is unramified at l.*

Proof: We start by showing that K_p always contain a primitive p-root of unity ζ_p. It is known (see Section III.8 in [66]) that there exists a Weil pairing $e_p : E[p] \times E[p] \to \mu_p(\bar{\mathbb{Q}})$, where $\mu_p(\bar{\mathbb{Q}})$ are the p-roots of unity. This pairing is bilinear, alternating, non-degenerate and compatible with the action of G_K in the sense that $e_p(S,T)^\sigma = e_p(S^\sigma, T^\sigma)$ for all $\sigma \in G_K$. In particular, since $E[p] \subset K_p$ we have for each pair of p-torsion points (S,T)

$$e_p(S,T)^\sigma = e_p(S^\sigma, T^\sigma) = e_p(S,T) \text{ for all } \sigma \in G_{\bar{\mathbb{Q}}/K_p}.$$

Hence $e_p(S,T) \in K_p$ thus $\mu_p(\bar{\mathbb{Q}}) \subset K_p$.

In what follows l will be used to denote both a prime in K and a normalizer of the valuation corresponding to it. The rest of the argument follows from the theory of Tate curves (see Chapter 5 in [67]). Since we want to know if K_p ramifies at l we can suppose that K and K_p are localized at l. Since l is of multiplicative reduction we have that $v_l(j(E)) < 1$ then $|j|_l > 1$ and from Tate's uniformization theorem (see Chapter 5, Theorem 5.3 in [67]) there exists $q \in K^*$ with $|q|_l < 1$ such that E_q is equivalent to E at most over a quadratic extension of K. Suppose that the isomorphism is over K and let $L = K(\zeta_p)$. Then from

Tate's theorem we have $E_q(L)$ isomorphic to $L^*/\langle q\rangle$. Since $j = c_3^3/\Delta$ by the hypothesis we conclude that $j = \mu l^{-pk}$ in L with μ an unit. On the other hand $j = 1/q+744+196884q+...$ and by multiplying both sides by q we get $q\mu l^{-pk} = 1 + 744q + 196884q^2 + ...$ meaning that $q = \mu' q'^p$ for some $\mu', q' \in L^*$ with μ' a unit. Thus, $\langle \zeta_p, q'\rangle/\langle q\rangle$ is contained in $L^*/\langle q\rangle$. Since $\langle \zeta_p, q'\rangle/\langle q\rangle$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ we conclude that $L^*/\langle q\rangle \simeq E_q(L)$ already contains all the p-torsion, implying $K_p \subset L$. Since L is unramified at l we have that K_p also is.

If the isomorphism above were over a quadratic extension K'/K, since E has multiplicative reduction at l it is know from Tate's theorem that K'/K is unramified. Then the same argument works by replacing K by K'.

■

For a generic elliptic curve E/K it is usually the case that $\mathrm{End}_{\bar{K}}(E) \cong \mathbb{Z}$. In the exceptional cases, $\mathbb{Z}$ is strictly contained in $\mathrm{End}_{\bar{K}}(E)$ and $\mathrm{End}_{\bar{K}}(E)$ is isomorphic to an order in an imaginary quadratic field. In the later case we say that E *has complex multiplication*. Before proceeding to the construction of p-adic representations attached to elliptic curves we will prove a useful result regarding the image of $\bar{\rho}_{E,p}$ for elliptic curves with complex multiplication.

Definition 1.1.15 *Let R be a subring of $Mat_{2\times 2}(\mathbb{F}_p)$ with $R \simeq \mathbb{F}_p \times \mathbb{F}_p$ or $R \simeq \mathbb{F}_{p^2}$. A subgroup subgroup G of $GL_2(\mathbb{F}_p)$ such that $G \simeq R^*$ is called a Cartan subgroup. If $R \simeq \mathbb{F}_p \times \mathbb{F}_p$ then G is called split, otherwise G is called non-split.*

Lemma 1.1.16 *Let E/K be an elliptic curve with complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic number field F. If p does not divide the discriminant $\Delta(\mathcal{O})$, then the image of $\bar{\rho}_{E,p}$ is contained in the normalizer of a split (resp. non-split) Cartan subgroup of $GL_2(\mathbb{F}_p)$ if p splits (resp. is inert) in F.*

Proof: Denote by $E[p]$ the p-torsion points of E and let $\pi : \mathcal{O} \sim \mathrm{End}(E) \to \mathrm{End}(E[p])$ be the restriction homomorphism. It is clear that $p\mathcal{O} \subset \mathrm{Ker}(\pi)$. We will now show that $\mathrm{Ker}(\pi) \subset p\mathcal{O}$. Given an ideal I in $\mathcal{O}$ and a set of points $X \subset E$ we define

$$\begin{aligned} E[I] &= \{P \in E : \phi(P) = 0 \text{ for all } \phi \in I\}, \\ \mathrm{Ann}(X) &= \{\phi \in \mathrm{End}(E) : \phi(P) = 0 \text{ for all } P \in X\}. \end{aligned}$$

Let $\mathfrak{p}_i$ for $i = 1, 2$ denote the ideals in $\mathcal{O}_F$ above p (if p is inert $\mathfrak{p}_1 = \mathfrak{p}_2$) and define I_i to be the maximal ideals in $\mathcal{O}$ given by $\mathcal{O} \cap \mathfrak{p}_i$. We have $I_i \subset \mathrm{Ann}(E[I_i]) \neq \mathcal{O}$ as ideals then $\mathrm{Ann}(E[I_i]) = I_i$ by maximality. Also, $E[p] = E[(p)]$ and $p\mathcal{O} \subset I_i$ then $E[I_i] \subset E[p]$. Then we can write $\mathrm{Ker}(\pi) = \mathrm{Ann}(E[p]) \subset \mathrm{Ann}(E[I_i]) = I_i$ for both i. Thus we have $\mathrm{Ker}(\pi) \subset I_1 \cap I_2 = p\mathcal{O}$. We conclude that $p\mathcal{O} = \mathrm{Ker}(\pi)$.

Let $R = \mathrm{Im}(\pi)$. Since $p \nmid \Delta(\mathcal{O})$ we have $R \sim \mathcal{O}/(p) \sim \mathcal{O}_F/(p)$, which is isomorphic to $\mathbb{F}_p \times \mathbb{F}_p$ or $\mathbb{F}_p^2$ depending on whether p splits or is inert in F. So R^* is a split resp. non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Consider the natural action of G_K on $\mathrm{End}(E)$ given

by $\phi_\sigma(P) := \phi(P^{\sigma^{-1}})^\sigma$, where $\sigma \in G_K$ and $\phi \in \mathrm{End}(E)$. It induces an action of G_K on R and on R^*. Recall that $\bar{\rho}_{E,p}(\sigma)(P) = P^\sigma$ for $P \in E[p]$. One easily checks that for $\psi \in R^*$ we have $\bar{\rho}_{E,p}(\sigma)\psi\bar{\rho}_{E,p}(\sigma)^{-1} = \psi_\sigma \in R^*$ and so $\mathrm{Im}(\bar{\rho}_{E,p})$ is contained in the normalizer of R^*.

■

Fix a prime l. We will now attach to E an l-adic Galois representation. Consider the representations of the l^n-torsion for all $n \in \mathbb{N}$ and put them all together in the following sequence

$$E[l] \longleftarrow E[l^2] \longleftarrow E[l^3] \longleftarrow \quad ...,$$

where the arrows correspond to multiplication by l (denoted $[l]$). By taking the inverse limit we obtain the *l-adic Tate module of E*,

$$T_l(E) = \varprojlim_n \{E[l^n]\}.$$

For each n, choose a basis (P_n, Q_n) of $E[l^n]$ compatible with $[l]$, that is $[l]P_{n+1} = P_n$ and $[l]Q_{n+1} = Q_n$. Each basis determines an isomorphism between $E[l^n]$ and $(\mathbb{Z}/l^n\mathbb{Z})^2$, hence

$$T_l(E) \cong \mathbb{Z}_l \oplus \mathbb{Z}_l.$$

Moreover, the action of G_K commutes with $[l]$ so there is a continuous action of G_K on $\mathbb{Z}_l$, which is thus an $\mathbb{Z}_l[G_K]$-module. Since each basis (P_n, Q_n) determines an isomorphism between $Aut(E[l^n])$ and $GL_2(\mathbb{Z}/l^n\mathbb{Z})$ we have $Aut(T_l(E)) \xrightarrow{\sim} GL_2(\mathbb{Z}_l)$ and also a continuous homomorphism

$$\rho_{E,l} : G_K \to GL_2(\mathbb{Z}_l) \subset GL_2(\mathbb{Q}_l).$$

We say that $\rho_{E,l}$ is the *2-dimensional l-adic Galois representation attached to E/K*. For a prime $\mathfrak{p}$ of good reduction for E denote by $\tilde{E}$ the reduction mod $\mathfrak{p}$ of a minimal model at $\mathfrak{p}$ of E. Let also p^f denote the number of elements in the residue field at $\mathfrak{p}$ and define

$$a_\mathfrak{p}(E) = p^f + 1 - \#\tilde{E}(\mathbb{F}_{p^f}) \tag{1.1}$$

Theorem 1.1.17 *Let l be a prime and E be an elliptic curve over K with conductor N (an ideal in $\mathcal{O}_K$). The Galois representation $\rho_{E,l}$ is unramified at every prime $\mathfrak{p} \nmid lN$. For any such $\mathfrak{p}$ let $\mathfrak{P} \subset \bar{\mathbb{Z}}$ be any maximal ideal over $\mathfrak{p}$. Then the characteristic equation of $\rho_{E,l}(Frob_\mathfrak{P})$ is*

$$x^2 - a_\mathfrak{p}(E)x + Norm(\mathfrak{p}) = 0.$$

The Galois representation $\rho_{E,l}$ is irreducible.

The information on the ramification in the previous theorem follows from

Theorem 1.1.18 *(Néron-Ogg-Shafarevich) Let E/K be an elliptic curve and l a prime of K. E has good reduction at l if and only if $\rho_{E,p}$ is unramified at l for some prime $p \neq l$ if*

and only if $\rho_{E,p}$ is unramified at l for all primes $p \neq l$.

1.1.2 Modular Forms

Modular forms are functions on the complex upper half plane which are nearly invariant under the action of a certain group and satisfy some holomorphy conditions. The *modular group* is the group of 2-by-2 matrices with integer entries and determinant 1,

$$SL_2(\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$$

which is generated by the two matrices

$$T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \text{ and } S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Let N be a positive integer. The *principal congruence subgroup of level N* is

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ mod N} \right\}$$

This subgroup is the kernel of the natural homomorphism $SL_2(\mathbb{Z}) \longrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$ so it is normal in $SL_2(\mathbb{Z})$.

Definition 1.1.19 *A subgroup Γ of $SL_2(\mathbb{Z})$ is a congruence subgroup if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$. We say that Γ is a congruence subgroup of level N.*

Every congruence subgroup Γ has finite index in $SL_2(\mathbb{Z})$. Besides $\Gamma(N)$, the most important congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \text{ mod N} \right\}$$

(where "$*$" means unspecified) and

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \text{ mod N} \right\}.$$

Let the upper half plane be denoted by $\mathcal{H} = \{\tau \in \mathbb{C} : \Im(\tau) > 0\}$.

Definition 1.1.20 *Let $\Gamma \subset SL_2(\mathbb{Z})$ be a congruence subgroup of level N. An holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight $k \geq 2$ with respect to Γ if*

(1) *For all* $\tau \in \mathcal{H}$ *and* $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,

$$f(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^k f(\tau)$$

(2) *For all* $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, *there exists a Fourier expansion*

$$(c\tau + d)^{-k} f(\frac{a\tau + b}{c\tau + d}) = \sum_{n=0}^{\infty} c_n q^{n/N}$$

where $q = e^{2\pi i \tau}$.

When $\alpha = Id$ *we denote the Fourier coefficients* c_n *in* (2) *by* $a_n(f)$. *If* $c_0 = 0$ *in all the Fourier expansions above we say that* f *is a cusp form. We denote by* $\mathcal{S}_k(\Gamma)$ *the space of all modular cusp forms of weight* k *respect to* Γ.

$\mathcal{S}_k(\Gamma)$ forms a vector space over $\mathbb{C}$ of finite dimension. For $k \geq 2$ there are formulas to compute its dimension and algorithms to compute their elements. In particular, $\mathcal{S}_2(\Gamma_0(2^t)) = \{0\}$ for $t \in \{0, 1, 2, 3, 4\}$ and $\mathcal{S}_2(\Gamma_0(32))$ has dimension 1.

Remark 1.1.21 *Not being able to compute these spaces for large levels is one of the barriers to the application of the modular approach to more equations. This will be clear in later chapters.*

Given a cusp for $f \in S_k(\Gamma_1(M))$ it is clear that it can be thought also as a cusp form in $f \in S_k(\Gamma_1(N))$ of any level N multiple of M. Fix a level N. For each M strictly dividing N there are various degeneracy maps sending the cusp forms on $S_k(\Gamma_1(M))$ into $S_k(\Gamma_1(N))$. The subspace of $S_k(\Gamma_1(N))$ spanned by the cusp forms of smaller levels under the various degeneracy maps is called the *old space* (of level N). If $f \in S_k(\Gamma_1(N))$ does not belong to the old space we say it is a *new* cusp form (of level N). We denote by $\mathcal{S}_k^{new}(\Gamma_1(N))$ the subspace of all new cusp forms in $\mathcal{S}_k(\Gamma_1(N))$.

We do not intend to define it here, but there is a family of operators $\{T_n\}_{n \in \mathbb{N}}$, called the Hecke operators, that act on the space $\mathcal{S}_k(\Gamma_1(N))$. It can be shown that $\mathcal{S}_k^{new}(\Gamma)$ admits a basis of simultaneous eigenvectors for all the operators T_n. To such a cusp form f we will call *eigenform* and if $a_1 = 1$ we say it is *normalized*. To a new normalized eigenform (of level N) we call it a *newform* (of level N).

Proposition 1.1.22 *Let* $f = \sum_{n=1}^{\infty} a_n q^n$ *be an eigenform, say* $T_n f = \lambda(n) f$ *for all* n. *Then* $a_n = \lambda(n) a_1$.

Let $J_1(N)$ be the Jacobian of the modular curve $X_1(N)$. Since it is an abelian variety, similarly to what happen with elliptic curves, from the torsion points of $J_1(N)$ we can

construct associated l-adic Galois representations. These representations, after extending scalars, decompose into 2-dimensional representations associated to modular forms. Indeed, we have

Theorem 1.1.23 *Let $f \in \mathcal{S}_2(\Gamma_0(N))$ be a normalized eigenform and denote by $\mathbb{Q}_f$ the number field generated by its Fourier coefficients. For each maximal ideal λ of $\mathcal{O}_{\mathbb{Q}_f}$ lying over l there is a Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} :\to GL_2(\mathbb{Q}_{f,\lambda}).$$

This representation is unramified at every prime $p \nmid lN$. For any such p let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over p. Then $\rho_{f,\lambda}(Frob_{\mathfrak{p}})$ satisfies the polynomial equation

$$x^2 - a_p(f)x + p = 0.$$

There exists a decomposition

$$S_k(\Gamma_1(N)) = \bigoplus_{\epsilon} S_k(N, \epsilon),$$

where the sum is over the Dirichlet characters ϵ of modulus N. Moreover, if $f \in S_k(N, \epsilon)$ then

$$f(\frac{a\tau + b}{c\tau + d}) = \epsilon(d)(c\tau + d)^k f(\tau)$$

for matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$. Note that for trivial ϵ we have $S_k(N, \epsilon) = \mathcal{S}_k(\Gamma_0(N))$. Actually, due to the work of Deligne (see [22]), the previous theorem with suitable modifications is also true for weight $k > 2$ and non trivial ϵ .

Theorem 1.1.24 *Let $f \in \mathcal{S}_k(N, \epsilon)$ be a normalized eigenform. Let l be a prime. For each maximal ideal λ of $\mathcal{O}_{\mathbb{Q}_f}$ lying over l there is an irreducible 2-dimensional Galois representation*

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_{f,\lambda}).$$

This representation is unramified at every prime $p \nmid lN$. For any such p let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over p. Then $\rho_{f,\lambda}(Frob_{\mathfrak{p}})$ satisfies the polynomial equation

$$x^2 - a_p(f)x + \epsilon(p)p^{k-1} = 0.$$

Given a newform $f \in \mathcal{S}_2(N, \epsilon)$ we can also attach a mod l representation to f. Indeed, up to similarity we may assume that the representation $\rho_{f,\lambda}$ maps to $GL_2(\mathcal{O}_{\mathbb{Q}_f,\lambda})$, hence it reduces modulo the maximal ideal to a representation

$$\bar{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\mathbb{Q}_f,\lambda}/\lambda\mathcal{O}_{\mathbb{Q}_f,\lambda}) \simeq \mathrm{GL}_2(\mathbb{F}_{l^r}).$$

1.2 Modularity and level lowering over $\mathbb{Q}$

Since we now know that there are Galois representations attached to modular forms it is natural to ask when a given representation ρ arises this way.

Definition 1.2.1 *Let L be a finite extension of $\mathbb{Q}_l$ and consider a Galois representation $\rho : G_{\mathbb{Q}} \to GL_2(L)$. Suppose that ρ is irreducible, odd and that $\det \rho = \epsilon\chi_l^{k-1}$ where ϵ has finite image. Then ρ is modular of level M_f if there exists a newform $f \in \mathcal{S}_k(M_f, \epsilon)$ and a prime λ above l such that $\mathbb{Q}_{f,\lambda}$ embeds in L and such $\rho_{f,\lambda} \sim \rho$.*

Wiles proved [76] that the l-adic Galois representations attached to all semistable elliptic curves over $\mathbb{Q}$ are modular. Then, Breuil, Conrad, Diamond and Taylor in [9] generalized the result for all elliptic curves over $\mathbb{Q}$. This general version of Wiles' Theorem is known as Modularity Theorem and there are several equivalent versions of it. Below we will state two versions: the first one is the more arithmetic and the other uses Galois representations. The proof of the equivalence between the two statements can be found in [25].

Let $E/\mathbb{Q}$ be an elliptic curve (with defining coefficients a_i) and for primes p of good reduction denote by $\tilde{E}$ the reduction mod p of a minimal model of E. Let N_E be the conductor of E and define

$$\begin{cases} a_p(E) = \#\{ \text{ solutions of } x^2 + a_1 x - a_2 \equiv 0 \pmod{p}\} - 1 \text{ if } p \mid N_E \\ a_p(E) = p + 1 - \#\tilde{E}(\mathbb{F}_p) \text{ if } p \nmid N_E \end{cases}$$

Theorem 1.2.2 *(Modularity Theorem) Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E. Then for some newform $f \in \mathcal{S}_2(\Gamma_0(N_E))$,*

$$a_p(f) = a_p(E) \quad \text{for all primes } p.$$

Theorem 1.2.3 *(Modularity Theorem) Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. Then for some newform $f \in \mathcal{S}_2(\Gamma_0(N))$ with number field $\mathbb{Q}_f = \mathbb{Q}$,*

$$\rho_{f,l} \sim \rho_{E,l} \text{ for all } l.$$

Before proceeding to Ribet's level lowering theorem and Serre's conjecture we need to extend the idea of modularity for mod l representations and introduce a few more concepts related to mod l Galois representations.

Definition 1.2.4 *An irreducible representation $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_l)$ is modular of type (N, k, ϵ) if there exists a newform $f \in \mathcal{S}_k(N, \epsilon)$ and a maximal ideal $\lambda \subset \mathcal{O}_{\mathbb{Q}_f}$ lying over l such that $\bar{\rho}_{f,\lambda} \sim \bar{\rho}$*

In order to formulate his conjecture Serre gives recipes to compute three quantities: *Serre's level* $N(\bar{\rho})$, *Serre's weight* $k(\bar{\rho})$ and *Serre's character* $\epsilon(\bar{\rho})$ attached to a given representation

$\bar{\rho}$ (see Conjecture 1.2.7 and [64]). Here we will recall only the definition of $N(\bar{\rho})$ that measures the minimal level of the modular forms giving rise to the given $\bar{\rho}$. Indeed, given a 2-dimensional Galois representation $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ we can think of it given by the action of $G_{\mathbb{Q}}$ in a two dimensional $\bar{\mathbb{F}}_p$ vector space V. Let $l \neq p$ be a prime number and choose an extension to $\bar{\mathbb{Q}}$ of the l-adic valuation on $\mathbb{Q}$. Let $G_0 \supset G_1 \supset ... \supset G_i \supset ...$ be the sequence of ramification subgroups corresponding to that valuation (see [65], Chap. IV) and let V_i be the subspace of V fixed by the action of G_i. Moreover, define also

$$n(l, \bar{\rho}) = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \mathrm{dim} V/V_i.$$

Finally, Serre's level $N(\bar{\rho})$ is defined to be the *Artin conductor* (as in characteristic zero cf. [65]) taken outside of p. That is,

$$N(\bar{\rho}) = \prod_{l \neq p} l^{n(l,\bar{\rho})}.$$

We want to emphasize that $p \nmid N(\bar{\rho})$ by construction. Analogously we can define the Artin conductor outside of p for representations of G_K, in which case none of the primes above p divides it.

In the rest of this work, when talking about the conductor of a mod p representation $\bar{\rho}$ we will be always considering it outside of p. In particular, by abuse of language, given a mod p representation $\bar{\rho}$ we will refer to its Artin conductor outside of p (i.e. Serre's level) simply by its Artin conductor.

Another important idea is the notion of $\bar{\rho}$ being *finite* at p. This notion has a quite involved definition and can be defined by means of group schemes or in a more Galois theoretical way. For details and the definition in complete generality see [64]. In our applications we will always check finiteness of $\bar{\rho}$ via the following criterion.

Lemma 1.2.5 *Let E/K be an elliptic curve and put $\bar{\rho} := \bar{\rho}_{E,p}$.*

(1) *Let $K = \mathbb{Q}$, L_0 be the maximal unramified extension of $\mathbb{Q}_p$ and $\bar{\chi}_p$ be the mod p cyclotomic character. Suppose that E has multiplicative reduction at p and is such that*

$$\bar{\rho}|I_p = \begin{pmatrix} \bar{\chi}_p & * \\ 0 & 1 \end{pmatrix}.$$

The image of $\bar{\rho}|I_p$ is isomorphic to the Galois group of some totally ramified extension L/L_0. Let L_t be the biggest tamely ramified extension of L_0 inside L. It follows from Kummer theory that $L = L_t(x_1^{1/p}, ..., x_m^{1/p})$ with $p^m = [L : L_t]$ and x_i elements in L_0^*/L_0^{*p}. If υ_p is the valuation in L_0 normalized by $\upsilon_p(p) = 1$ and $\upsilon_p(x_i) \equiv 0 \pmod p$ then $\bar{\rho}$ is finite at p.

(2) *If E/K has multiplicative reduction at $\mathfrak{p}$ and $p \mid \upsilon_{\mathfrak{p}}(\Delta)$ then $\bar{\rho}$ is finite at $\mathfrak{p}$.*

(3) *If* $\mathfrak{p}$ *is of good reduction for* E/K *then* $\bar{\rho}$ *is finite at* $\mathfrak{p}$.

Proof: See pages 186-191 in [64].

■

In what follows, whenever we need to check finiteness of a representation $\bar{\rho}$ we will use (2) or (3) in the lemma above. We decided to also include (1) because it is close to the definition in the case of elliptic curves over $\mathbb{Q}$ (it does not include the good supersingular reduction) and it is used on the proof of parts (2) and (3) of the previous lemma.

It was Ribet's level lowering theorem (see [57]) that reduced the proof of FLT to the Shimura-Tanyama conjecture for semistable elliptic curves over $\mathbb{Q}$.

Theorem 1.2.6 *(Mazur-Ribet) Let* $p \geq 3$ *be a prime. Let* $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_{p^r})$ *be irreducible over* $\bar{\mathbb{F}}_p$ *and modular of type* $(N, 2, 1)$. *If* $\bar{\rho}$ *is finite at* p *then it is modular of type* $(N(\bar{\rho}), 2, 1)$.

In later chapters we will make use of results similar to this but for Hilbert modular forms. In particular, we will be interested in the difference between the conductor of the representation attached to Frey curves and the Artin conductor of its residual representation. Let ρ be a modular representation such that $\bar{\rho}$ is irreducible. It is known from the work of Carayol (see [14]) that the possible differences between its conductor N_ρ and the Artin conductor $N(\bar{\rho})$ at primes $\mathfrak{P}$ not above the characteristic l are given by Table 1.1.

$\upsilon_{\mathfrak{p}}(N_\rho)$	$n+2 (n \geq 1)$	2	2	1
$\upsilon_{\mathfrak{p}}(N(\bar{\rho}))$	$n+1 (n \geq 1)$	1	0	0

Table 1.1: Conductors differences

Furthermore, it is also known from Carayol's work that in order for the level lowering to happen there is a congruence between the prime p and the characteristic l that must be satisfied. Only in the case corresponding to the last column the level lowering is independent of such a congruence. In particular, for a fixed prime p and l big enough this implies that only the last case of level lowering can happen. This fact will be very important in later chapters when we will lower the level of representations attached to our Frey curves.

We end this section by stating Serre's conjecture regarding the modularity of mod l representations (see [64]). Nowadays the conjecture is known to be true, but at the time of the proof of FLT it was still a conjecture.

Conjecture 1.2.7 *(Serre) Let* $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$ *be odd and irreducible. The* $\bar{\rho}$ *is modular of type* $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$.

Theorem 1.2.8 *(Khare-Wintenberger) Serre's conjecture holds.*

Proof: See [39] and [40].

1.3 Fermat's Last Theorem

To end this chapter we will prove FLT. The reason for this is twofold. On one hand we want to recall the original application of the modular approach. On the other hand this way we hope to motivate the generalizations of some aspects of the approach that we will make in the next chapters.

Theorem 1.3.1 *(Fermat-Wiles) Let $p \geq 3$ be a prime. The equation $x^p + y^p = z^p$ has no solutions (a, b, c) such that $gcd(a, b, c) = 1$ (primitive) and $abc \neq 0$ (non-trivial).*

Proof: We will prove it for $p \geq 5$. If (a, b, c) is a non-trivial primitive solution of Fermat's equation it is easy to see that we can suppose that b is even and a, c are odd and also that $a \equiv -1 \pmod 4$ (if $a \equiv 1 \pmod 4$ we take the solution $(-a, -b, -c)$).

Now consider the Frey curve

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

which has discriminant of the form $\Delta = 2^4(abc)^{2p}$. Since $p \geq 5$ from Tate's algorithm can be seen that E is semistable and has conductor $N_E = \mathrm{rad}(abc)$. From the modularity theorem $\rho_{E,p}$ is modular of level N_E, hence $\bar{\rho}_{E,p}$ is modular of type $(N_E, 2, 1)$. By Theorem 1.1.13 the representation $\bar{\rho}_{E,p}$ is irreducible. $\bar{\rho}_{E,p}$ is finite at p by the paragraph following Definition 1.2.4, hence by the Mazur-Ribet Theorem $\bar{\rho}_{E,p}$ is modular of type $(N(\bar{\rho}), 2, 1)$. From Proposition 1.3.2 below and since $\bar{\rho}_{E,p}$ is finite at p we have $N(\bar{\rho}_{E,p}) = 2$. Recall that $\mathcal{S}_2(\Gamma_0(2)) = \{0\}$ hence $\bar{\rho}_{E,p}$ can not be modular. We have a contradiction.

■

Proposition 1.3.2 *If $p \geq 5$ then $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ is unramified outside $2p$.*

Proof: Let $l \neq p$ be an odd prime. If $l \nmid abc$ then $l \nmid \Delta$ and E has good reduction at l. By theorem 1.1.18 we have that $\rho_{E,p}$ is unramified at l, hence $\bar{\rho}_{E,p}$ also is. If $l | abc$ then the given equation is minimal at l and by Hellegouarch theorem follows that $\bar{\rho}_{E,p}$ is unramified at l. Thus $\bar{\rho}_{E,p}$ is unramified outside $2p$.

■

As a final observation, we could have made the proof above shorter by applying Serre's conjecture. Instead, we decided to illustrate the use of a level lowering theorem. Despite of the existence of an analogous statement of Serre's conjecture for totally real fields due to Buzzard, Diamond and Jarvis (see [12]) it is still a conjecture. On the other hand, the level lowering theorems for totally real fields are completely proved and we will extensively use them in the rest of this work.

Chapter 2

Equations of signature $(5, 5, p)$ via $\mathbb{Q}$-curves

The use of $\mathbb{Q}$-curves in the modular approach was introduced by Ellenberg in [29] to deal with the equation $x^4+y^2 = z^p$. Since then other Diophantine equations were solved through $\mathbb{Q}$-curves, as in work from Dieulefait-Jimenez [28], I.Chen [15] and Bennett-Chen [3].

In this chapter we will study equations of the form $x^5+y^5 = Cz^p$ via a multi-Frey approach with $\mathbb{Q}$-curves. In section 2.1 we start with some comments on Galois representations attached to elliptic curves and we state results from Ellenberg that we need later. In section 2.2 and 2.3 we will prove (modulo the proof of Theorem 2.1.10) Theorem 2.0.3 below. In section 2.4 and 2.5 we will introduce tools from the theory of abelian varieties attached to $\mathbb{Q}$-curves and embedding problems. The material in these two sections can be found in detail in [54] and [55]. Finally, in the last section we will give a proof of Theorem 2.1.10.

Theorem 2.0.3 *Let β be an integer divisible only by primes $l \not\equiv 1$ (mod 5). Suppose that $p \equiv 1$ mod 4 or $p \equiv \pm 1$ mod 5. Then, the equation*

$$x^5 + y^5 = Cz^p, \tag{2.1}$$

has no non-trivial primitive solutions if

(A) $C = 2\beta$ *and* $p > 13$ *or*

(B) $C = 3\beta$ *and* $p > 73$.

2.1 A Frey curve to the equations $x^5 + y^5 = Cz^p$

In this section, to a putative solution (a, b, c) of (2.1) we will attach a Frey curve $E_\gamma(a, b)$ over a number field K. Despite $E_\gamma(a, b)$ being defined over a number field we will show that there is a mod p Galois representation of $G_\mathbb{Q}$ attached to it, to which we can apply Serre's Conjecture. Recall that to a triple (a, b, c) such that $a^5 + b^5 = Cc^p$ we call a *primitive* solution if $(a, b) = 1$ and a *trivial* solution if $|abc| \leq 1$.

2.1.1 $\mathbb{Q}$-curves and Galois representations.

Definition 2.1.1 *Let C be an elliptic curve over $\bar{\mathbb{Q}}$. We say that C is a $\mathbb{Q}$-curve if for every $\sigma \in G_{\mathbb{Q}}$ there is an isogeny $\phi_\sigma : {}^\sigma C \to C$. We say that a $\mathbb{Q}$-curve C is completely defined over a number field K if all the conjugates of C and the isogenies between them are defined over K.*

To an elliptic curve C over $\mathbb{Q}$ we can attach an l-adic representations $\rho_{C,l}$ of $G_{\mathbb{Q}}$. Since the isomorphism class of $\rho_{C,l}$ depends only on the isogeny class of C it is natural to expect that if C/K is a $\mathbb{Q}$-curve then we can also attach to its isogeny class one (or more) Galois representations $\rho'_{C,l} : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{Q}}_l)$. This is indeed the case and we may think of it as $\rho'_{C,l}$ being attached to an abelian variety of GL_2-type over $\mathbb{Q}$ admitting C as a factor over $\bar{\mathbb{Q}}$. Then $\rho'_{C,l}|G_K$ agrees with the Galois representation obtained from the action of G_K on the l-adic Tate module of C. Moreover, if we start with a $\mathbb{Q}$-curve C we can always find a suitable field of complete definition K' such that the representation $\rho_{C,l} : G_{K'} \to GL_2(\mathbb{Q}_l)$ extends to a Galois representation of $G_{\mathbb{Q}}$ after a suitable twist.

It is a consequence of Serre's conjecture that $\mathbb{Q}$-curves are modular. However, modularity results from Ellenberg-Skinner [31] were previously available under a local condition at 3. In our argument we will use Serre's conjecture, although since our curves will have good reduction at 3 their modularity would follow from [31]. We will now state two results due to Ellenberg (Propositions 3.2 and 3.4 in [29]) about representations attached to $\mathbb{Q}$-curves that we need in the following sections. Given a mod p Galois representation $\bar{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ we will denote its projectivization into $\mathrm{PGL}_2(\mathbb{F}_p)$ by $\mathbb{P}\bar{\rho}$.

Theorem 2.1.2 *(Ellenberg) Let K be a quadratic field, E/K be a $\mathbb{Q}$-curve admitting a cyclic isogeny of degree d to its Galois conjugate. Suppose $\mathbb{P}\bar{\rho}_{E,p}$ is reducible for some $p = 11$ or $p > 13$ with $(p, d) = 1$. Then E has potentially good reduction at all primes of K of characteristic greater than 3.*

Theorem 2.1.3 *(Ellenberg) Let K be a quadratic field, E/K be a $\mathbb{Q}$-curve admitting a cyclic isogeny of degree d to its Galois conjugate. Suppose the image of $\mathbb{P}\bar{\rho}_{E,p}$ lies in the normalizer of a split Cartan subgroup of $PGL_2(\mathbb{F}_p)$, for $p = 11$ or $p > 13$ with $(p, d) = 1$. Then E has good reduction at all primes of K not dividing 6.*

2.1.2 A pair of Diophantine equations

From now on we will consider a, b to be coprime integers, thus we will always be talking about primitive solutions. The first observation in order to solve equation (2.1) is that we will use the factorization

$$a^5 + b^5 = (a + b)(a^4 - a^3b + a^2b^2 - ab^3 + b^4) \tag{2.2}$$

to relate a solution of (2.1) with a solution of another Diophantine equation. With that in mind, we let $\phi(a,b) = a^4 - a^3b + a^2b^2 - ab^3 + b^4$ and we will prove a few elementary results about the factorization (2.2). Given integers m, n, s we will say that m, n are coprime outside s if $\gcd(m,n)$ is divisible at most by the prime factors of s.

Lemma 2.1.4 *Let l be a prime number dividing $a+b$. Then, $\phi(a,b) \equiv 5a^2b^2 \pmod{l^2}$.*

Proof: Let l be a prime number dividing $a+b$. We have $a^2+b^2 \equiv -2ab \pmod{l^2}$. Since $\phi(a,b) = (a^2+b^2)^2 - ab(a^2+b^2+ab)$, then $\phi(a,b) \equiv 5a^2b^2 \pmod{l^2}$.

■

Lemma 2.1.5 *The integers $a+b$ and $\phi(a,b)$ are coprime outside 5. Moreover, if 5 divides $a+b$ then $v_5(\phi(a,b)) = 1$*

Proof: Let l be a prime divisor of $a+b$. If $l \neq 5$ we have $5a^2b^2 \not\equiv 0 \pmod{l}$ because $l \nmid ab$ and by the previous lemma we conclude that l does not divide $\phi(a,b)$. If $l = 5$ then the congruence in the lemma implies that $l | \phi(a,b)$ and $\nu_5(\phi(a,b)) = 1$.

■

Lemma 2.1.6 *Let $l \not\equiv 1 \pmod 5$ be a prime number dividing a^5+b^5. Then, l divides $a+b$.*

Proof: Since $l | a^5+b^5$ and $(a,b) = 1$ then $l \nmid ab$. Let b' be the inverse of $-b \bmod l$. Since $a^5 \equiv (-b)^5 \pmod{l}$ we have $(ab')^5 \equiv 1 \pmod{l}$. Hence ab' has order 1 or 5. If ab' has order 1 then $a+b \equiv 0 \pmod{l}$. Hence if $l \nmid a+b$ then ab' must have order 5 thus $5 | l-1$, i.e $l \equiv 1 \pmod 5$.

■

Corollary 2.1.7 *Suppose $(a,b) = 1$. If a prime number $q \neq 5$ divides $\phi(a,b)$ then $q \equiv 1 \pmod 5$. Also, if $5 \nmid a+b$ then $\nu_5(\phi(a,b)) = 0$.*

Proof: Let $q \neq 5$ be a prime dividing $\phi(a,b)$. Then $q \mid a^5+b^5$ by (2.2) and $q \nmid a+b$ by Lemma 2.1.5. Hence by Lemma 2.1.6 we must have $q \equiv 1 \pmod 5$. Since $5 \not\equiv 1 \pmod 5$, if $5 \nmid a+b$ it follows from Lemma 2.1.6 that $5 \nmid a^5+b^5$ thus $5 \nmid \phi(a,b)$.

■

The following lemma relates two Diophantine equations.

Lemma 2.1.8 *Suppose there exists a non-trivial primitive solution (a,b,c') to $x^5+y^5 = Cz^p$ with $C \neq 0$ an integer divisible only by primes $q \neq 5$ satisfying $q \not\equiv 1 \pmod 5$. Then there exists a solution (a,b,c) such that $(a,b) = 1$ (primitive) and $|abc| > 1$ (non-trivial) to*

$$\phi(a,b) = c^p \quad \text{or} \tag{2.3}$$

$$\phi(a,b) = 5c^p \tag{2.4}$$

which satisfies $5 \nmid a+b$ *in case* (2.3) *and* $5 \mid a+b$ *in case* (2.4)*. Moreover:*

- *if* $d \mid C$*, then* $d \mid a+b$*;*
- *the prime divisors of* c *are all congruent to* $1 \pmod 5$*. In particular, neither* 2*, nor* 5 *divide* c*.*

Proof: This follows from the equalities $x^5+y^5 = (x+y)\phi(x,y) = Cz^p$, Lemma 2.1.6 and Corollary 2.1.7. Also, it is a particular case of Lemma 3.2.6.

■

From the lemma above we see that Theorem 2.0.3 will follow if we prove that there are no solutions (a,b,c) to (2.3) and (2.4) such that $(a,b) = 1$ (primitive), $|abc| > 1$ (non-trivial) and $C \mid a+b$. We want to remark that despite of $C = 2\beta$ or $C = 3\beta$ in the statement of Theorem 2.0.3, in its proof we will only need $2 \mid C$ or $3 \mid C$, because this already implies that $2 \mid a+b$ or $3 \mid a+b$ which is enough to prove part (A) or part (B), respectively.

2.1.3 The $\mathbb{Q}$-curve

To apply the modular approach we need to find an appropriate Frey $\mathbb{Q}$-curve. Consider the polynomial

$$\phi(x,y) = x^4 - x^3y + x^2y^2 - xy^3 + y^4$$

and its factorization over $\mathbb{Q}(\sqrt{5})$

$$\phi(x,y) = \phi_1(x,y)\phi_2(x,y),$$

where

$$\begin{aligned} \phi_1(x,y) &= x^2 + \omega xy + y^2, \\ \phi_2(x,y) &= x^2 + \bar{\omega} xy + y^2, \\ \omega &= \frac{-1+\sqrt{5}}{2}, \\ \bar{\omega} &= \frac{-1-\sqrt{5}}{2}. \end{aligned}$$

Proposition 2.1.9 *If* (a,b) *is a pair of coprime integers then* $\phi_1(a,b)$ *and* $\phi_2(a,b)$ *are coprime outside* 5*.*

Proof: Suppose that l is a prime in $\mathbb{Q}(\sqrt{5})$ dividing both $\phi_i(a,b)$, then l also divides $\phi_1 - \phi_2 = \sqrt{5}ab$. If l divides ab, then we can suppose that l divides a, but dividing a and $\phi_1(a,b)$ implies that divides b which is a contradiction since a, b are coprime. Thus we conclude that l is above 5.

■

Let (a, b, c) be a non-trivial primitive solution to (2.3) or (2.4), we define an elliptic curve over $\mathbb{Q}(\sqrt{5})$

$$E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 - \bar{\omega}\phi_1(a,b)x.$$

To ease notation we will omit the pair (a, b) when writing $E_{(a,b)}$, $\phi(a,b)$, $\phi_1(a,b)$, $\phi_2(a,b)$. Observing that $(a+b)^2 = -\bar{\omega}\phi_1 - \omega\phi_2$ we compute

$$\Delta(E) = 2^6\bar{\omega}\phi\phi_1. \tag{2.5}$$

Consider the Galois conjugated curve for the non-trivial element in $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$

$$^{\sigma}E : y^2 = x^3 + 2(a+b)x^2 - \omega\phi_2 x,$$

and the 2-isogeny $\mu : {}^{\sigma}E \to E$ given by

$$(x, y) \mapsto (-\frac{y^2}{2x^2}, \frac{\sqrt{-2}}{4}\frac{y}{x^2}(\omega\phi_2 + x^2)).$$

with dual isogeny $\hat{\mu} : E \to {}^{\sigma}E$ given by

$$(x, y) \mapsto (-\frac{y^2}{2x^2}, -\frac{\sqrt{-2}}{4}\frac{y}{x^2}(\bar{\omega}\phi_1 + x^2)),$$

showing that E is a $\mathbb{Q}$-curve. In order to apply the modular approach to our equation, we need to find a twist of E, E_γ such that its Weil restriction decomposes as a product of abelian varieties of GL_2-type. That is the content of the following theorem, whose proof we postpone until section 2.3.3.

Theorem 2.1.10 *Let $K = \mathbb{Q}(\theta)$ where $\theta = \sqrt{\frac{1}{2}(5+\sqrt{5})}$ is a root of the polynomial $x^4 - 5x^2 + 5$, and put $\gamma = 2\theta^2 - \theta - 5$. Then, the twisted curve*

$$E_\gamma : y^2 = x^3 + 2\gamma(a+b)x^2 - \gamma^2\bar{\omega}\phi_1(a,b)x$$

is completely defined over K and its Weil restriction from K to $\mathbb{Q}$ decomposes as the product of two non-isogenous abelian surfaces of GL_2-type each of them with endomorphism algebra over $\mathbb{Q}$ isomorphic to $\mathbb{Q}(i)$.

2.1.4 The conductor of E_γ and $E_{\gamma,2}$

Now we will determine the conductor of E_γ. These conductors are needed to compute the conductor of Weil restriction of E_γ and consequently the level of the associated modular forms. Let $K = \mathbb{Q}(\theta)$ and denote by $\mathfrak{P}_2$ and $\mathfrak{P}_5$ the only primes above 2 and 5, respectively. Also, denote the conductor of E_γ by N_{E_γ} and let $\mathrm{rad}(c)$ be the product of the prime factors

of c. The curves $E_\gamma(a,b)$ have associated the following quantities

$$\begin{aligned}\Delta(E_\gamma) &= \gamma^6\Delta(E) = \gamma^6 2^6\bar{\omega}\phi\phi_1,\\ c_4(E_\gamma) &= \gamma^2\Delta(E) = -\gamma^2 2^4(\bar{\omega}\phi_1 - 2^2\omega\phi_2),\\ c_6(E_\gamma) &= \gamma^3\Delta(E) = -\gamma^3 2^6(a+b)(\bar{\omega}\phi_1 - 2^3\omega\phi_2)\end{aligned}$$

Recall that $\phi = \phi_1\phi_2$ over $\mathbb{Q}(\sqrt{5})$. If $\phi(a,b) = c^p$ or $\phi(a,b) = 5c^p$ then $\phi_i(a,b) = c_i^p$ or $\phi_i(a,b) = \sqrt{5}c_i^p$ up to units, with $c_i \in \mathcal{O}_{\mathbb{Q}(\sqrt{5})}$. In the proofs of this section we follow the tables of Papadopoulos in [52].

Proposition 2.1.11 *Let $\mathfrak{P}$ be a prime in K distinct from $\mathfrak{P}_2$, $\mathfrak{P}_5$. Then E_γ has good ($\upsilon_{\mathfrak{P}}(N_{E_\gamma}) = 0$) or multiplicative ($\upsilon_{\mathfrak{P}}(N_{E_\gamma}) = 1$) reduction if $\mathfrak{P} \nmid c$ or $\mathfrak{P} \mid c$, respectively.*

Proof: Observe that ω and $\bar{\omega}$ are units. Then $\upsilon_{\mathfrak{P}}(\Delta) = p\upsilon_{\mathfrak{P}}(c) + p\upsilon_{\mathfrak{P}}(c_1)$. Hence, if $\mathfrak{P} \nmid c$ we have $\upsilon_{\mathfrak{P}}(\Delta) = 0$ and the curve has good reduction. If $\mathfrak{P} \mid c$ we have $\upsilon_{\mathfrak{P}}(\Delta) > 0$ and since $\mathfrak{P}$ divides only one of the c_i it is clear from the form of c_4 that $\upsilon_{\mathfrak{P}}(c_4) = 0$, thus the curve has multiplicative reduction.

■

Proposition 2.1.12 *Let $\mathfrak{P} = \mathfrak{P}_5$. The curve E_γ has bad additive reduction ($\upsilon_{\mathfrak{P}}(N) = 2$) or good reduction if $5 \nmid a+b$ or $5 \mid a+b$, respectively.*

Proof: Note that $\gamma\mathcal{O}_K = \mathfrak{P}_5$. If $5 \nmid a+b$ we have $\upsilon_{\mathfrak{P}}(\Delta) = \upsilon_{\mathfrak{P}}(\gamma^6 2^6\bar{\omega}c^p c_1^p) = 6$ and $\upsilon_{\mathfrak{P}}(c_4) > 0$ then by table I in [52] the curve has bad additive reduction and $\upsilon_{\mathfrak{P}}(N) = 2$.

In $5 \mid a+b$ we have

$$\begin{aligned}\upsilon_{\mathfrak{P}}(\Delta) &= \upsilon_{\mathfrak{P}}(\bar{\omega}\gamma^6 2^6 5\sqrt{5}c^p c_1^p) = \upsilon_{\mathfrak{P}}(\gamma^6) + \upsilon_{\mathfrak{P}}(5) + \upsilon_{\mathfrak{P}}(\sqrt{5}) =\\ &= 6 + 4 + 2 = 12.\end{aligned}$$

This means that the equation is not minimal. Any change of variable leading to a minimal equation will decrease the valuation of the discriminant by 12, hence $\upsilon_{\mathfrak{P}}(\Delta) = 0$, i.e. the curve as good reduction.

■

Let $\pi = \mathfrak{P}_2$ and we note that $\upsilon_\pi(2) = 2$

Proposition 2.1.13 *The conductor at π of E_γ satisfies:*

$$\upsilon_\pi(N_{E_\gamma}) = \begin{cases} 8 \text{ or } 6 & \text{if } 2 \nmid a+b,\\ 8 & \text{if } 2 \parallel a+b,\\ 0 & \text{if } 4 \parallel a+b,\\ 4 & \text{if } 8 \mid a+b,\end{cases}$$

Proof: Observe that $(\upsilon_\pi(c_4), \upsilon_\pi(c_6), \upsilon_\pi(\Delta)) = (8, 12+2\upsilon_2(a+b), 12)$. According to Table V in [52] these values can correspond to the Tate cases 3, 6, 7(ν odd), 7(ν even), 9, 10 or non-minimal. The fact $\upsilon_\pi(\Delta) = 12$ tells us that if arrive at the non-minimal case then the curve has good reduction hence we go through each case only once. Observe from Proposition 6 in [52] that π^{10} is the highest power of π appearing in the congruences used to decide in which case we are for each (a, b). Since between our possible cases the coordinate changes are translations it follows that all the possible values for the conductor at π must appear by considering the pairs $(a, b) \pmod{2^5}$. Using SAGE we compute these conductors and easily observe that they divide into categories according to the statement.

■

Let $E_{\gamma,2}$ be the twist of E_γ by 2 and denote its conductor by $N_{E_{\gamma,2}}$. This conductor will later be used to reach a contradiction when analyzing representations coming from newforms. Actually, we will only need it in the case of congruences between representations coming from newforms with level 1600 and $E_\gamma(a, b)$ where $2 \parallel a + b$.

Proposition 2.1.14 *Suppose that* (a, b, c) *is a solution to* (2.3) *or* (2.4) *such that* $2 \parallel a+b$. *Then the conductor at* π *of* $E_{\gamma,2}$ *is* π^0 *or* π^4.

Proof: Observe that when twisting a curve by 2 the quantities Δ, c_4 and c_6 change by the factors 2^6,2^2 and 2^3, respectively. Then for $E_{\gamma,2}$ we have $(\upsilon_\pi(c_4), \upsilon_\pi(c_6), \upsilon_\pi(\Delta)) = (12, 18 + 2\upsilon_2(a + b), 24)$ and by table V in [52] follows that the equation is not minimal. After the change $(x, y) = (\pi^2 x, \pi^3 y)$ we have $(\upsilon_\pi(c_4), \upsilon_\pi(c_6), \upsilon_\pi(\Delta)) = (8, 12+2\upsilon_2(a+b), 12)$. Now exactly as above but with the extra condition $2 \parallel a + b$ we use SAGE to compute the conductors.

■

2.1.5 Modularity of E_γ

Here we go into determining the precise Serre's parameters $k(\bar{\rho})$, $N(\bar{\rho})$ and $\epsilon(\bar{\rho})$, where $\bar{\rho}$ is the residual representation of a p-adic representation attached to a GL_2-type abelian variety given by Theorem 2.1.10.

Let $B = \mathrm{Res}_{K/\mathbb{Q}}(E_\gamma/K)$, where $K = \mathbb{Q}(\theta)$ is the cyclic Galois extension in Theorem 2.1.10, and denote its conductor by N_B. To compute this conductor we will use a formula of Milne (see [50]), which in our case tells us that the conductor satisfies

$$N_B = \mathrm{Nm}_{K/\mathbb{Q}}(N_{E_\gamma})\mathrm{Disc}(K/\mathbb{Q})^2,$$

where Disc and Nm denote the discriminant and norm of $K/\mathbb{Q}$, respectively. Since c is odd and $\mathrm{Disc}(K/\mathbb{Q}) = 2^4 5^3$, then the primes dividing c do not ramify in K. Being $K/\mathbb{Q}$ of

degree 4 we have that a prime p dividing c is inert, splits completely or is the product of two primes in K with residual degree 2 thus $\mathrm{Nm}((c)) = c^4$. Also, $\mathrm{Nm}(\mathfrak{P}_5) = 5$ and $\mathrm{Nm}(\mathfrak{P}_2) = 4$. By applying the above formula we obtain the following results:

Proposition 2.1.15 *If (a, b, c) is a primitive solution of equation (2.3) then B has conductor:*

$$N_B = \begin{cases} 2^{24}5^8 rad(c)^4 \text{ or } 2^{20}5^8 rad(c)^4 & \text{if} \quad 2 \nmid a+b, \\ 2^{24}5^8 rad(c)^4 & \text{if} \quad 2 \parallel a+b, \\ 2^{8}5^8 rad(c)^4 & \text{if} \quad 4 \parallel a+b, \\ 2^{16}5^8 rad(c)^4 & \text{if} \quad 8 \mid a+b. \end{cases}$$

Proposition 2.1.16 *If (a, b, c) is a primitive solution of equation (2.4) then B has conductor:*

$$N_B = \begin{cases} 2^{24}5^6 rad(c)^4 \text{ or } 2^{20}5^6 rad(c)^4 & \text{if} \quad 2 \nmid a+b, \\ 2^{24}5^6 rad(c)^4 & \text{if} \quad 2 \parallel a+b, \\ 2^{8}5^6 rad(c)^4 & \text{if} \quad 4 \parallel a+b, \\ 2^{16}5^6 rad(c)^4 & \text{if} \quad 8 \mid a+b. \end{cases}$$

We know from Theorem 2.1.10 that $B \simeq S_1 \times S_2$ where S_i are two non $\mathbb{Q}$-isogenous abelian surfaces of GL_2-type with $\mathbb{Q}$-endomorphism algebras equal to $\mathbb{Q}(i)$. So the conductor of B satisfies $N_B = N_{S_1} N_{S_2}$.

For a prime l and each S_i the action on the Tate module $T_l S_i$ induces a 4-dimensional l-adic representation of $G_{\mathbb{Q}}$ that decomposes into two 2-dimensional λ-adic representations $\rho_{S_i,\lambda}$ and $\rho^{\sigma}_{S_i,\lambda}$, where λ is a prime of $\mathbb{Q}(i)$ above l. Then we have four 2-dimensional representations of $G_{\mathbb{Q}}$ extending the l-adic representation $\rho_{E_\gamma,l}$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ induced by the action on the Tate module of E_γ. Since extensions of absolutely irreducible representations are unique up to twists we have the following relations between them:

$$\begin{cases} \rho_{S_1,\lambda} \otimes \epsilon \sim \rho^{\sigma}_{S_1,\lambda} \\ \rho_{S_1,\lambda} \otimes \epsilon^2 \sim \rho_{S_2,\lambda} \\ \rho_{S_1,\lambda} \otimes \epsilon^3 \sim \rho^{\sigma}_{S_2,\lambda} \end{cases}$$

where ϵ is the character of K (see section 2.3.3, formula (2.10)) and ϵ^2 is the character of $\mathbb{Q}(\sqrt{5})$. It is known that the conductors of $\rho_{S_i,\lambda}$ and $\rho^{\sigma}_{S_i,\lambda}$ are equal and that their product is equal to the conductor of S_i, which means that every prime in the conductor of S_i appears to an even power. From the second relation and the fact that ϵ^2 has conductor 5 we see that the only possible difference in the conductors of $\rho_{S_1,\lambda}$ and $\rho_{S_2,\lambda}$ may occur at 5. Furthermore, the conductor at 5 of $\rho_{S_1,\lambda} \otimes \epsilon^2$ is smaller or equal to the least common multiple between the conductor at 5 of $\rho_{S_1,\lambda}$ and $\mathrm{cond}_5(\epsilon^2)^2$, that is

$$\mathrm{cond}_5(\rho_{S_1,\lambda} \otimes \epsilon^2) \leq \mathrm{lcm}(\mathrm{cond}_5(\rho_{S_1,\lambda}), \mathrm{cond}_5(\epsilon^2)^2) = \mathrm{lcm}(\mathrm{cond}_5(\rho_{S_1,\lambda}), 5^2).$$

The inequality may hold only if the conductor at 5 of $\rho_{S_1,\lambda}$ is equal to 5^2. Using these facts together with a case checking allow us to determine all the possibilities for the conductors of the four 2-dimensional representations (see Table 2.1).

Equation	$\nu_2(a+b)$	$\rho_{S_1,\lambda}$	$\rho^{\sigma}_{S_1,\lambda}$	$\rho_{S_2,\lambda}$	$\rho^{\sigma}_{S_2,\lambda}$
(2.3)	0	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5^2 c_0$
(2.3)	0	$2^5 5^2 c_0$	$2^5 5^2 c_0$	$2^5 5^2 c_0$	$2^5 5^2 c_0$
(2.3)	1	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5^2 c_0$
(2.3)	2	$2^2 5^2 c_0$	$2^2 5^2 c_0$	$2^2 5^2 c_0$	$2^2 5^2 c_0$
(2.3)	≥ 3	$2^4 5^2 c_0$	$2^4 5^2 c_0$	$2^4 5^2 c_0$	$2^4 5^2 c_0$
(2.4)	0	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5 c_0$	$2^6 5 c_0$
(2.4)	0	$2^5 5^2 c_0$	$2^5 5^2 c_0$	$2^5 5 c_0$	$2^5 5 c_0$
(2.4)	1	$2^6 5^2 c_0$	$2^6 5^2 c_0$	$2^6 5 c_0$	$2^6 5 c_0$
(2.4)	2	$2^2 5^2 c_0$	$2^2 5^2 c_0$	$2^2 5 c_0$	$2^2 5 c_0$
(2.4)	≥ 3	$2^4 5^2 c_0$	$2^4 5^2 c_0$	$2^4 5 c_0$	$2^4 5 c_0$

Table 2.1: Values of conductors, where $c_0 = \mathrm{rad}(c)$

Now pick a prime λ in $\mathbb{Q}(i)$ above p, let $\rho := \rho_{S_1,\lambda}$ and $\bar{\rho} := \bar{\rho}_{S_1,\lambda}$ be its residual representation. Recall that by Theorem 1.1.14 a prime of semistable reduction of an elliptic curve C which appear in the discriminant of C to a p-power will not ramify in the mod p representation induced by the p-torsion points. From formula (2.5), Proposition 2.1.9 and the fact that the primes in K dividing c are of semistable reduction for E_γ we can apply Theorem 1.1.14 to conclude that the restriction $\bar{\rho}_{|G_K}$ of $\bar{\rho}$ to $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$, which coincides with $\bar{\rho}_{E_\gamma,p}$, will not ramify at primes dividing c. Since K only ramifies at 2 and 5 then we see that $\bar{\rho}$ can not ramify outside 2 and 5. On the other hand it is known (see comments after Table 1.1) that in the presence of wild ramification the conductor does not decrease when reducing mod p, so the possible conductors of $\bar{\rho}$ are exactly the values in the third column of Table 2.1 without the factor c_0. Thus we have determined Serre's level $N(\bar{\rho})$.

Proposition 2.1.17 *The representation $\bar{\rho}$ has character $\epsilon(\bar{\rho}) = \bar{\epsilon}$ (complex conjugate of ϵ).*

Proof: By Theorem 5.12 of [53] we know that the character associated to $\rho_{S_1,\lambda}$ is equal to ϵ^{-1} where ϵ is the splitting character defined by formula (2.10) in section 2.3.3. Furthermore, since ϵ has order 4, for any prime p distinct from 2 the representation $\bar{\rho}$ has the same character of the non residual one. Then $\bar{\rho}$ is modular with character $\epsilon^{-1} = \bar{\epsilon}$.

■

Proposition 2.1.18 *The Serre weight of the representation $\bar{\rho}$ is $k(\bar{\rho}) = 2$.*

Proof: We divide in two cases. If $p \nmid c$ then S_1 has good reduction at p and $\bar{\rho}$ comes from an abelian variety with good reduction at p hence $k = 2$. If $p \mid c$, the fact that $p \mid \nu_{\mathfrak{P}}(\Delta)$ for any $\mathfrak{P}$ above p implies by Proposition 1.2.5 (see also [29]) that $\bar{\rho}$ is finite and so $k = 2$.

■

Finally, to apply the Serre's conjecture we still need irreducibility.

Proposition 2.1.19 *The representation $\bar{\rho}$ is absolutely irreducible.*

Proof: If (a, b, c) is a non-trivial solution then there is a prime of characteristic greater that 3 of semistable reduction, hence by Theorem 2.1.2 we conclude that $\bar{\rho}$ irreducible for $p > 13$.
■

Now from Serre's strong conjecture we know that there is a newform f in the space $\mathcal{S}_2(M, \bar{\epsilon})$ with $M = 1600$, 800, 400 or 100 and $\mathfrak{P} \mid p$ in $\mathbb{Q}_f$ such that the residual representation $\bar{\rho}_{f,\mathfrak{P}}$ attached to f is isomorphic to our residual representation $\bar{\rho}$.

2.2 Eliminating Newforms

Using software we will compute the newforms in the spaces $\mathcal{S}_2(M, \bar{\epsilon})$ with $M = 1600$, 800, 400 or 100, determined in the previous section. Then, in order to reach a contradiction, we need to show that our representation $\bar{\rho}$ can not be isomorphic to a representation of the form $\bar{\rho}_{f,\mathfrak{P}}$ where f is one of the computed newforms.

Note that equations $\phi(a, b) = \pm 1$ and $\phi(a, b) = \pm 5$ have trivial solutions $(\pm 1, 0)$, $(0, \pm 1)$, $(1, 1)$, $(-1, -1)$ and $(1, -1)$, $(-1, 1)$, respectively. This means that for these pairs (a, b) the Frey $\mathbb{Q}$-curves do exist and so if their corresponding newforms lie in level 100, 400, 800 or 1600 and *a priori* we may not be able to eliminate those forms. From now on, when we say 'eliminate a newform f' we mean that we show that the isomorphism $\bar{\rho} \sim \bar{\rho}_{f,\mathfrak{P}}$ can not hold for any prime $\mathfrak{P} \mid p$. Recall that when treating the cases $2 \mid C$ or $3 \mid C$ we have $a+b$ even or $3 \mid a+b$, respectively. As we will see this will turn out to be a key information. Now observe that $(\pm 1, 0)$, $(0, \pm 1)$ will not be a problem for equation (2.1) when $2 \mid C$, because $a + b$ is odd; since the elliptic curves $E_{(-1,1)}$, $E_{(1,-1)}$, $E_{(1,1)}$ and $E_{(-1,-1)}$ correspond to newforms with complex multiplication we will also be able to eliminate them.

To eliminate the newforms we will separate them into three sets and then we apply a different strategy for each of the sets. Given a newform f let $\mathbb{Q}_f = \mathbb{Q}(\{a_q(f)\})$ be its field of coefficients and note that for those we will compute we have $\mathbb{Q}(i) = \mathbb{Q}(\epsilon) \subseteq \mathbb{Q}_f$. Now let S1, S2 and S3 be as follows:

S1: Newforms with CM (Complex Multiplication),

S2: Newforms without CM and field of coefficients strictly containing $\mathbb{Q}(i)$,

S3: Newforms without CM and field of coefficients $\mathbb{Q}(i)$

In the following two sections we will find a contradiction for each set above, first in the case $2 \mid C$ and second when $3 \mid C$, which will give us the partial results in Theorem 2.2.1 and Theorem 2.2.2. We want to remark that up to the end of section 2.2.2 everything will be done using only the Frey curves $E = E_\gamma(a, b)$.

Finally, we will introduce a new Frey $\mathbb{Q}$-curve F (see equation (2.7)) and, from the fact that the pairs $E_{(1,-1)}$, $F_{(1,-1)}$ and $E_{(1,1)}$, $F_{(1,-1)}$ have CM by different field, together with the multi-Frey technique we will finish the proof of Theorem 2.0.3.

2.2.1 The case $2 \mid C$

Since $2 \mid a + b$ then $800 = 2^5 5^2$ is not a possible level. We compute the spaces $\mathcal{S}_2(M, \bar{\epsilon})$ with $M = 1600$, 400 and 100 and divide the newforms into the sets S1, S2 and S3 defined above.

`Newforms in S1`: Modulo Galois conjugation there are 8 newforms with complex multiplication, half of them with CM by $\mathbb{Q}(i)$ and the other half by $\mathbb{Q}(\sqrt{-5})$. If there is a non-trivial solution (a, b, c) to equation (2.3) or (2.4) then there exists a prime not dividing 6 of semistable reduction for E. Hence if $p > 13$ by Theorem 2.1.3 the images of $\bar{\rho}$ will not lie in the normalizer of a split Cartan subgroup. Then if p splits in both $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-5})$, i.e. $p \equiv 1 \pmod 4$ and $p \equiv \pm 1 \pmod 5$ we can not have $\bar{\rho} \sim \bar{\rho}_{f,\mathfrak{P}}$ for f in S1. This is because by Lemma 1.1.16 we know that for p's that are split on the field of complex multiplication the image of the attached representation will be in a normalizer of a split Cartan subgroup.

`Newforms in S2:` There are 12 newforms (modulo conjugation) in this group. For each prime q of good reduction for S_1 we consider the quantity

$$a_q(S_1) := \mathrm{Trace}(\rho_{S_1,\lambda}(\mathrm{Frob}_q)).$$

We know that it satisfies $a_q(S_1) = \bar{a}_q(S_1)\bar{\epsilon}(q)$ from propositions 4.3 and 3.4 in [59]. In the previous equality ϵ is the character of order 4 defined in section 2.3.3; in particular, the inner twist implies that

$$a_q(S_1) = \begin{cases} t & \text{if } q \equiv 1 \text{ or } 19 \bmod 20 \\ it & \text{if } q \equiv 9 \text{ or } 11 \bmod 20 \\ t - it & \text{if } q \equiv 3 \text{ or } 17 \bmod 20 \\ t + it & \text{if } q \equiv 7 \text{ or } 13 \bmod 20 \end{cases}$$

where t is an integer. Recall from Table 2.1 that a prime $q \neq 2, 5$ of bad reduction for S_1 must divide c, that is, it must divide $\phi(a, b)$. Since $3 \not\equiv 1 \pmod 5$ it follows from Corollary 2.1.7 that 3 is a prime of good reduction for S_1. Hence, $a_3(S_1)$ must be of the form $t - ti$ and from the Weil bound $|a_3(S_1)| \leq 2\sqrt{3}$ follows that $|t| \leq 2$. If $f = q + \sum_{n=2} c_n q^n$ is one

of these 12 newforms in S2 then the congruence

$$a_3(S_1) \equiv c_3(f) \pmod{\mathfrak{P}} \tag{2.6}$$

for a prime $\mathfrak{P}$ in $\bar{\mathbb{Q}}$ above p, must hold. Now for each newform in S2 we use the coefficient $c_3(f)$ to derive a contradiction, because none of them has $c_3(f)$ of the form $t-ti$. As an example, there is a newform f in S2 of level 400 with $c_3(f)$ having minimal polynomial x^2+10i; thus if the congruence (2.6) holds we must have $c_3(f) \equiv t - it \pmod{\mathfrak{P}}$ with $t = 0, \pm 1, \pm 2$. Taking fourth powers we get $100 \equiv 4t^4 \pmod{\mathfrak{P}}$ which means $25 - t^4 \equiv 0 \pmod{\mathfrak{P}}$ and finally, substituting for the possible values of t we reach a contradiction if $p > 5$. A similar argument works for every newform in S2 and we conclude that if $p > 7$ the newform predicted by Serre's conjecture can not be in S2.

`Newforms in S3:` There are 10 newforms in this group all with level 1600. Recall that $\bar{\rho} := \bar{\rho}_{S_1,\lambda}$ and suppose that $\bar{\rho} \sim \bar{\rho}_{f,\mathfrak{P}}$ for some f in S3. *A priori* all newforms in S3 are inconvenient, in the sense that their Fourier coefficients $a_q(f)$ behave exactly as those of our surface S_1. That is, each $a_q(f)$ lies in $\mathbb{Q}(i)$, they respect the rule $a_q(f) = \bar{a}_q(f)\bar{\epsilon}(p)$ (by construction) and they are even (this is true for our surface because E_γ has a 2-torsion point). To deal with this problem we will twist each newform in S3 by the character of $\mathbb{Q}(\sqrt{2})$, which we denote by χ. Note that $\mathrm{cond}(\chi)^2 = 8^2 = 2^6$ and the power of 2 in 1600 is also 2^6 so as mentioned before we are in a situation where the power of 2 in the level of the twist can decrease. Indeed, using SAGE, we pick f in S3, we consider $f \otimes \chi$ and compare the coefficients of $f \otimes \chi$ up to the Sturm bound with those of the newforms with level dividing 1600 to find that $f \otimes \chi$ is a newform of level 800 for all f in S3.

On the other hand, let $E_{\gamma,2}$ be as in section 2.1.4 and $\rho_{E_{\gamma,2},p}$ be the representation coming from the action of G_K on the Tate module $T_pE_{\gamma,2}$. Note that

$$(\rho_{S_1,\lambda} \otimes \chi)_{|K} = (\rho_{S_1,\lambda})_{|K} \otimes \chi_{|K} = \rho_{E_\gamma,p} \otimes \chi_{|K},$$

that is $\rho_{S_1,\lambda} \otimes \chi$ extends $\rho_{E_\gamma,p} \otimes \chi_{|K}$ and this one is precisely $\rho_{E_{\gamma,2},p}$. The same is true for the other three representations coming from the Weil restriction $B \simeq S_1 \times S_2$. Moreover, $\rho_{B,p} = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho_{E_\gamma,p}$ and we have

$$\rho_{B,p} \otimes \chi = (\mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho_{E_\gamma,p}) \otimes \chi = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} (\rho_{E_\gamma,p} \otimes \chi_{|K}) = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \rho_{E_{\gamma,2},p},$$

and this means that $\rho_{B,p} \otimes \chi$ is the representation coming from the action of $G_\mathbb{Q}$ on the p-adic Tate module of $\mathrm{Res}_{K/\mathbb{Q}}(E_{\gamma,2}/K)$. Let ρ_1 denote the 2-dimensional factor $\rho_{S_1,\lambda} \otimes \chi$ of $\rho_{B,p} \otimes \chi$. From Proposition 2.1.14, Milne's formula and an analysis identical to that used to compute Table 2.1 we conclude that $N(\bar{\rho}_1) = 400$ or 100. $\bar{\rho}_1$ is also irreducible and has character and Serre's weight equal to those of $\bar{\rho}$, because the same arguments hold. We now apply Serre's strong conjecture to $\bar{\rho}_1$ and we conclude that there must be a newform g in level 400 or 100 and a prime $\mathfrak{P}'$ above p such that $\bar{\rho}_1 \sim \bar{\rho}_{g,\mathfrak{P}'}$. But at the same time we also

have

$$\bar{\rho}_1 = \overline{\rho_{S_1,\lambda} \otimes \chi} \sim \bar{\rho} \otimes \chi \sim \bar{\rho}_{f,\mathfrak{P}} \otimes \chi \sim \bar{\rho}_{f\otimes\chi,\mathfrak{P}} \sim \bar{\rho}_{f',\mathfrak{P}},$$

where f' is of level 800 by the previous paragraph. Hence the isomorphism

$$\bar{\rho}_{g,\mathfrak{P}'} \sim \bar{\rho}_{f',\mathfrak{P}}$$

must hold between a newform of level 800 and another of level 400 or 100, but as we know this kind of level lowering can not happen. At this point we have proved

Theorem 2.2.1 *Let β be an integer divisible only by primes $\not\equiv 1$ (mod 5). For any $p > 13$ such that $p \equiv 1$ mod 4 and $p \equiv \pm 1$ mod 5, the equation $x^5 + y^5 = 2\beta z^p$ has no non-trivial primitive solutions.*

2.2.2 The case $3 \mid C$

In this case $a + b$ may be odd, hence we also need to consider level 800, but in our favor we have $3 \mid a + b$. We compute the spaces $\mathcal{S}_2(M, \bar{\epsilon})$ with $M = 1600$, 800, 400 or 100 and again we divide them into the sets S1, S2 and S3. This time we will also need to make some further subdivisions according to the parity of $a + b$ and the level. Let $\mathfrak{P}_3$ be the prime of K above 3 and note that for $a+b$ odd the possible levels are only 800 or 1600.

$a+b$ `odd and level 800:` There are 4 newforms of type S2 and 10 of type S3 and none of type S1. Recall from the previous section that 3 is a prime of good reduction for S_1 because $3 \nmid \phi(a, b)$.

`Newforms in S2:` We use the same type of argument as for $2 \mid C$. Indeed, we already know that $a_3(S_1) = t - it$, with $t \in \mathbb{Z}$ such that $|t| \leq 2$. Again, if $f = q + \sum_{n=2} c_n q^n$ is a newforms in S2 then the congruence

$$a_3(S_1) \equiv c_3(f) \pmod{\mathfrak{P}}$$

for a prime $\mathfrak{P}$ in $\bar{\mathbb{Q}}$ above p, must hold. In particular, there is a newform in S2 having $c_3(f)$ with minimal polynomial $x^2 \pm (2 - 2i)x + i$. For such a form we apply the polynomial to both sides of the congruence above and then replace x by all its possible values to find a contradiction with $p > 73$. By repeating this process for all forms in S2 we find that 73 works as bound for all cases.

`Newforms in S3:` First recall that $\rho|_{G_K} = \rho_{E_\gamma,p}$. Suppose now that $\bar{\rho} \sim \bar{\rho}_{f,\mathfrak{P}}$ for some newform f in S3, in particular, $\bar{\rho}|_{G_K} \sim \bar{\rho}_{f,\mathfrak{P}}|_{G_K}$. Let $a_{\mathfrak{P}_3}(f) = \mathrm{tr}(\rho_{f,\mathfrak{P}}|_{G_K}(\mathrm{Frob}_{\mathfrak{P}_3}))$, which is an integer by Proposition 2.2.3. By evaluating both sides in the previous isomorphism at

$\mathrm{Frob}_{\mathfrak{P}_3}$ and taking traces we see that

$$a_{\mathfrak{P}_3}(E_\gamma) = \mathrm{tr}(\rho|_{G_K}(\mathrm{Frob}_{\mathfrak{P}_3})) \equiv a_{\mathfrak{P}_3}(f) \pmod{p}.$$

On one hand, for a prime $\mathfrak{L}$ of good reduction for E_γ, the quantity $a_{\mathfrak{L}}(E_\gamma)$ is equal to $l^s + 1 - \#\tilde{E}_\gamma(\mathbb{F}_{l^s})$, where l^s is the number of elements of the residue field at $\mathfrak{L}$ and $\tilde{E}_\gamma$ is the elliptic curve obtained by reducing E_γ modulo $\mathfrak{L}$. It is easy to see that the hypothesis $3 \mid a+b$ implies that E_γ mod $\mathfrak{P}_3$ is the same for any pair (a,b) and by direct computation with SAGE we check that E_γ has $a_{\mathfrak{P}_3}(E_\gamma) = -18$ for all a, b. On the other hand, looking for the $a_3(f)$ coefficients of the newforms of type S3 we find four possibilities $\pm(2i-2)$ and $\pm(i-1)$. It is known that if α, β are the roots of the polynomial $x^2 - a_3(f)x + \bar{\epsilon}(3)3$ (the characteristic polynomial of $\rho_{f,\mathfrak{P}}(\mathrm{Frob}_3)$), then $a_{\mathfrak{P}_3}(f) = \alpha^4 + \beta^4$. Since $\bar{\epsilon}(3) = -i$, by substituting for each of the four values of $a_3(f)$ we find out that $a_{\mathfrak{P}_3}(f) = 14$ or 2. Hence $\bar{\rho} \sim \bar{\rho}_{f,\mathfrak{P}}$ is not possible if $p > 3$.

$a+b$ `odd and level 1600:`

`Newforms in S1:` The newforms with complex multiplication by $\mathbb{Q}(\sqrt{-5})$ verify $a_3(f) = \pm(i-1)$ then we use the argument we have just described to get a contradiction with $3 \mid a+b$. Thus we have to eliminate only newforms with CM by $\mathbb{Q}(i)$ and for that we use the same argument as for the case $2 \mid C$. For $p > 13$, if we suppose that p is split in $\mathbb{Q}(i)$, i.e. $p \equiv 1 \pmod 4$, we have a contradiction with Theorem 2.1.3.

`Newforms in S2:` Since we have considered separately the newforms of level 800 the set S2 that we are considering now is a subset of the one considered for $2 \mid C$. Also, we are assuming $p > 73$ then the exact same argument as for $2 \mid C$ holds, i.e. the argument in the Section 2.2.1 in paragraph starting with "`Newforms in S2:`..".

`Newforms in S3:` For f in S3 we first twist them by the Dirichlet character of $\mathbb{Q}(\sqrt{2})$ and we already know that $f \otimes \chi$ is a newform of level 800. On the other hand we twist the Frey curve $E_\gamma(a,b)$ by the same character. If the conductor at 2 of the twisted curve is not 2^5 we have a contradiction via Carayol as in the case $2 \mid C$; if it is 2^5, then since $E_\gamma \otimes \chi$ modulo $\mathfrak{P}_3$ is equal to $E_\gamma(a,b)$ mod $\mathfrak{P}_3$ we are in the same situation as above (with forms of level 800 and type S3) and the argument used there with the values of $a_{\mathfrak{P}_3}(E_\gamma)$ and $a_{\mathfrak{P}_3}(f)$ gives us the desired contradiction.

$a+b$ `even and any level:` In this case $6 = 2 \times 3 \mid a+b$ then all the arguments described for both cases $2 \mid C$ and $3 \mid C$ can be used. For newforms of type S2 and S3 we apply exactly the same arguments used in section 2.2.1 for $2 \mid C$ but with $p > 73$. For newforms of type S1 we only need to suppose that is $p \equiv 1 \pmod 4$ to get a contradiction. As we already

observed, this is because the newforms with CM by $\mathbb{Q}(\sqrt{-5})$ satisfy $a_3 = \pm(i-1)$ which contradicts $3 \mid a+b$. Up to now we have just proved

Theorem 2.2.2 *Let β be an integer divisible only by primes $\not\equiv 1$ (mod 5). For any $p > 73$ such that $p \equiv 1$ mod 4, the equation $x^5 + y^5 = 3\beta z^p$ has no non-trivial primitive solutions.*

2.2.3 The multi-Frey approach

In this section we end the proof of Theorem 2.0.3 via Siksek multi-Frey technique. As it name suggests the multi-Frey approach is a modular approach which makes use of more than one Frey curve. This technique was introduced by Siksek in [11] and further generalized in [3]. The main observation being that if we have n distinct modular Frey curves E_i for $2 \leq i \leq n$ attached to a putative solution (a, b, c) then this will imply several simultaneous isomorphisms between the Galois representations $\bar{\rho}_{E_i,p}$ and the representations $\bar{\rho}_{f_i,\mathfrak{P}_i}$ attached to their corresponding modular forms. In general, this should allow to give a better bound for the exponent p in (2.1).

We start by giving a second Frey curve. From the relation

$$(\frac{-3}{10}\sqrt{5} + \frac{1}{2})\phi_1 + (\frac{3}{10}\sqrt{5} + \frac{1}{2})\phi_2 = (a-b)^2$$

we can consider the curves $F_{(a,b)}$ defined also over $\mathbb{Q}(\sqrt{5})$ and given by

$$F = F_{(a,b)} : y^2 = x^3 + 2(a-b)x^2 + (\frac{-3}{10}\sqrt{5} + \frac{1}{2})\phi_1(a,b)x. \tag{2.7}$$

We have checked that these are $\mathbb{Q}$-curves and after applying Quer's theory analogously to what we did for $E_{(a,b)}$ we find that the same splitting character/field and twist γ computed previously work also for F. After computing the conductor of F_γ/K, applying Milne's formula and Serre's conjecture we find that we need to eliminate newforms with level 100, 400 or 1600 if $8 \mid a+b$, $4 \parallel a+b$ or $2 \parallel a+b$, respectively. Also, if $2 \nmid a+b$ we can suppose that a is even and we are in level 800 or 1600 if $4 \mid a$ or $4 \nmid a$, respectively. Moreover, it also follows from the conductor of F_γ that if $l \nmid 2, 5$ is a prime in K of bad reduction for F_γ then l must divide $\phi(a,b)$.

We now recall that, in the previous sections, when working with E_γ we needed to eliminate newforms with level 400, 100 or 1600 if $8 \mid a+b$, $4 \parallel a+b$ or $2 \parallel a+b$, respectively. Also, when $2 \nmid a+b$ and a is even we were in level 800 or 1600 depending if $4 \mid a$ or $4 \nmid a$, respectively. Thus interchanging E_γ by F_γ only switches the levels 100 and 400. The reason for this observation will be clear below.

To apply the multi-Frey technique with the curves $E_{(a,b)}$ and $F_{(a,b)}$ we first need to give the definitions according to our case. For that we will need

Proposition 2.2.3 *Let f be one of the computed newforms with coefficient field $\mathbb{Q}_f = \mathbb{Q}(i)$. Let $\mathfrak{P}$ be a prime in $K = \mathbb{Q}(\theta)$. Then $a_{\mathfrak{P}}(f) = tr(\rho_{f,\lambda}|G_K(Frob_{\mathfrak{P}}))$ is an integer number.*

Proof: The nebentypus $\bar{\epsilon}$ fixes K. Let $F = \mathbb{Q}(\{a_{\mathfrak{P}}(f)\})$ be the field generated by all the traces $a_{\mathfrak{P}}(f) = \mathrm{tr}(\rho_{f,\lambda}|G_K(\mathrm{Frob}_{\mathfrak{P}}))$. Actually, we can generate F by adjoining to $\mathbb{Q}$ only the values $a_{\mathfrak{P}}(f)$ corresponding to primes $\mathfrak{P} \mid p$ such that p splits in K.

Since f satisfies $a_p(f) = \bar{a}_p(f)\bar{\epsilon}(p)$, in particular, for $\mathfrak{P} \mid p$ a prime splitting in K we have

$$a_{\mathfrak{P}}(f) = a_p(f) = \bar{a}_p(f)\bar{\epsilon}(p) = \bar{a}_p(f) = \bar{a}_{\mathfrak{P}}(f)$$

and we see that $a_{\mathfrak{P}}(f)$ belongs to the maximal totally real subfield of $\mathbb{Q}_f$, that is $\mathbb{Q}$. Thus $F = \mathbb{Q}$.

■

Recall that $K = \mathbb{Q}(\theta)$ is of degree 4 and for an inert prime q denote by $\mathfrak{P}_q$ the only prime of K above q. Let $q \in \mathbb{Z}$ be a prime inert in K of good reduction to both families $E_{(a,b)}$, $F_{(a,b)}$. Given a newform f, if α, β are the roots of the characteristic polynomial of $\rho_{f,\mathfrak{P}}(\mathrm{Frob}_q)$, i.e. $x^2 - a_q(f)x + \bar{\epsilon}(q)q$ then $a_{\mathfrak{P}_q}(f) = \alpha^4 + \beta^4$ (in the previous section, in the sub-case corresponding to $a + b$ odd and level 800, we used this for $q = 3$). Now, let f be a newform satisfying the hypothesis of Proposition 2.2.3. Then, $a_{\mathfrak{P}_q}(f)$ is an integer and for a non-zero pair $(x, y) \in \mathbb{F}_{q^4} \times \mathbb{F}_{q^4}$ we can define the following quantities

$$\begin{aligned} E_{(x,y)}(q, f) &:= a_{\mathfrak{P}_q}(E_{(x,y)}) - a_{\mathfrak{P}_q}(f), \\ F_{(x,y)}(q, f) &:= a_{\mathfrak{P}_q}(F_{(x,y)}) - a_{\mathfrak{P}_q}(f). \end{aligned}$$

Moreover, given a pair of such newforms (f, g) we put

$$A_q(f, g) := \prod_{(x,y)\in\mathbb{F}_{q^4}^2 - \{(0,0)\}} \gcd(E_{(x,y)}(q, f), F_{(x,y)}(q, g)).$$

Now, if (a, b, c) is a primitive solution to (2.3) or (2.4) there is a pair of newforms (f, g) and primes $\mathfrak{P}$ and $\mathfrak{P}'$ above p such that

$$\begin{cases} \bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}|G_K \\ \bar{\rho}_{F,p} \sim \bar{\rho}_{g,\mathfrak{P}'}|G_K \end{cases}$$

Instead of eliminating newforms as in the previous section, we are now interested in eliminating pairs, and for that we will use information from both E and F. For example, if both f, g have coefficient field $\mathbb{Q}(i)$ and q is a prime as above then, by evaluating the two isomorphisms above at $\mathrm{Frob}_{\mathfrak{P}_q}$ and taking traces, we see that $p \mid A_q(f, g)$. Thus we can eliminate a pair (f, g) if $A_q(f, g) \neq 0$ by imposing (for example) $p > A_q(f, g)$. Note also that there is only a finite number of pairs to eliminate.

We will now finish the proofs of Theorem 2.0.3. Note that the differences between what we have already proved in the previous two sections and the statement of Theorem 2.0.3 (A) and (B) are the congruence conditions on the exponent p. Those conditions arise from Ellenberg's theorem when eliminating the newforms with CM. We observe that in level 800 there are no newforms with CM and in level 1600 there are four corresponding to the elliptic curves $E_{(1,1)}$, $F_{(1,1)}$, $E_{(1,-1)}$ and $F_{(1,-1)}$. Let f_1,f_2 denote the two forms with CM by $\mathbb{Q}(i)$ and g_1,g_2 those with CM by $\mathbb{Q}(\sqrt{-5})$. Let χ be the character of $\mathbb{Q}(\sqrt{2})$. On level 100 there are three newforms with CM: $g_1 \otimes \chi$, $g_2 \otimes \chi$, $f_1 \otimes \chi$ and on level 400 there is $f_2 \otimes \chi$. Since there are no newforms with CM in level 800 the argument that follows can be applied to both cases $2 \mid C$ and $3 \mid C$.

Given a primitive solution (a, b, c) to (2.3) or (2.4) we have a double isomorphism as explained above

$$\begin{cases} \bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}} | G_K \\ \bar{\rho}_{F,p} \sim \bar{\rho}_{g,\mathfrak{P}'} | G_K \end{cases}$$

where $f \in S_2(M_f, \bar{\epsilon})$ and $g \in S_2(M_g, \bar{\epsilon})$ where the pair of levels (M_f, M_g) may be $(400, 100)$, $(100, 400)$, $(1600, 1600)$ or $(800, 800)$. We consider all the pairs (f, g) of newforms respecting the previous pairs of levels and we divide them in two sets: let SS1 be the set of pairs (f, g) where f has no CM and SS2 the set of those where f has CM. We eliminate a pair (f, g) in SS1 by applying the arguments on f explained in the previous two sections. For pairs (f, g) in SS2 such that g has coefficient field strictly containing $\mathbb{Q}(i)$ we eliminate them by applying to g the exact same argument as in the previous two sections in the subcase `Newforms in S2`. We are left with pairs in SS2 such that both forms have coefficient field $\mathbb{Q}(i)$. Note that $q = 3, 7, 13, 17$ satisfy $q \not\equiv 1 \pmod 5$ hence by Corollary 2.1.7 $q \nmid \phi(a, b)$ thus it is of good reduction to both families $E_{(a,b)}$ and $F_{(a,b)}$. Given (f, g) in SS2 such that both f, g have coefficient field $\mathbb{Q}(i)$ we compute $A_q(f, g)$ using the auxiliary primes $q = 3, 7, 13, 17$ to find that $A_q(f, g) = 0$ for all the auxiliary primes only if f, g have CM by distinct fields. Moreover, when $A_q(f, g) \neq 0$ we check that all prime factors of $A_q(f, g)$ are ≤ 13. Hence there are eight surviving pairs: (f_1, g_1), (f_1, g_2), (g_1, f_1), (g_2, f_2), $(g_1 \otimes \chi, f_2 \otimes \chi)$, $(g_2 \otimes \chi, f_2 \otimes \chi)$, $(f_2 \otimes \chi, g_1 \otimes \chi)$ and $(f_2 \otimes \chi, g_2 \otimes \chi)$. For a prime $p \equiv 1 \pmod 4$ or $p \equiv \pm 1 \pmod 5$ we can eliminate these pairs by conveniently applying Theorem 2.1.3 to E or F. Thus Theorem 2.0.3 follows.

2.3 Finding E_γ

In this section we will first introduce background theory on $\mathbb{Q}$-curves, abelian varieties and embedding problems and then we will give a proof of Theorem 2.1.10.

2.3.1 $\mathbb{Q}$-curves and abelian varieties

From a $\mathbb{Q}$-curve C we are interested in consider the abelian variety obtained by the Weil restriction $B = \mathrm{Res}_{K/\mathbb{Q}}(C/K)$, where K is a large enough number field. The Galois representations attached to B when B is a product of abelian varieties of GL_2-type are going to play a central role in our argument. In order to understand them we first need to know the form of B which we will do via Theorem 5.4 in [54]. Below we will restate the specific case of that theorem that is of interest to us (see Theorem 2.3.3), but first we need to recall some of the machinery in [54].

We say that a $\mathbb{Q}$-curve C is *completely defined* over a number field K if all the conjugates of C and the isogenies between them are defined over K. Let C be a $\mathbb{Q}$-curve without complex multiplication completely defined K. For every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we choose an isogeny $\phi_\sigma : {}^\sigma C \to C$. We denote by $\hat{\phi}_\tau$ the dual isogeny of ϕ_σ and given $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ we define $\phi_\tau^{-1} := (1/\deg(\phi_\tau))\hat{\phi}_\tau$. Moreover, there is an isogeny ${}^\tau\phi_\sigma : {}^{\tau\sigma}C \to {}^\tau C$ that allows to define a map $c_K : \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{End}(C)^* \simeq \mathbb{Q}^*$, given by

$$c_K(\sigma, \tau) = \phi_\sigma {}^\sigma\phi_\tau \phi_{\sigma\tau}^{-1}.$$

The map c_K is known to be a 2-cocycle of $\mathrm{Gal}(K/\mathbb{Q})$ with values in $\mathbb{Q}^*$ with trivial action and the corresponding cohomology class by $\xi_K(C) \in H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ depends only on the K-isogeny class of C. Now for every $\sigma \in G_\mathbb{Q}$ we consider an isogeny corresponding to the action of σ in K; this gives a locally constant set of isogenies $\{\phi_\sigma\}_{\sigma \in G_\mathbb{Q}}$ and we can define as above a continuous 2-cocycle c of $G_\mathbb{Q}$ whose cohomology class $\xi(C)$ is the inflation of $\xi_K(C)$ and depends only on the isogeny class of C. Let $d : G_\mathbb{Q} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ be given by $d(\sigma) = \deg(\sigma)$; this homomorphism depends only on the isogeny class of C. Its fixed field K_d is a polyquadratic number field $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_m})$ and is the smallest field of definition of the curve C up to isogeny. Let also $\{d_1, ..., d_m\}$ be squarefree integers forming a Kummer dual basis for the a_i, i.e. a basis of the group $d(G_\mathbb{Q})$. The pair of sets $\{a_i\}$, $\{d_i\}$ is said to be a *dual basis respect to the degree map.*

Let $\mathrm{Br}_2(\mathbb{Q})$ be the 2-torsion of the Brauer group of $\mathbb{Q}$. Let also $\xi(C)_\pm \in H^2(G_\mathbb{Q}, \{\pm 1\}) \simeq \mathrm{Br}_2(\mathbb{Q})$ denote the cohomology class corresponding to the 2-cocycle given by the sign of the 2-cocycle $\xi(C)$. Then $\xi(C)_\pm$ can be expressed as a product of quaternion algebras in the following way

Theorem 2.3.1 *(Quer) Let C be a $\mathbb{Q}$-curve. Let $\{a_i\}$, $\{d_i\}$ be a dual base to the corresponding degree map. Then,*

$$\xi(C)_\pm = \prod (a_i, d_i),$$

where (a_i, b_i) are quaternion algebras.

A *splitting map* to the cocycle c is a locally constant map $\beta : G_\mathbb{Q} \to \bar{\mathbb{Q}}^*$ such that

$$c(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}, \text{ for } \sigma, \tau \in G_\mathbb{Q}.$$

Let C be a $\mathbb{Q}$-curve, and β a splitting map for a two-cocycle c representing $\xi(C)$. The map $G_{\mathbb{Q}} \to \bar{\mathbb{Q}}^*/\mathbb{Q}^*$ given by $\sigma \mapsto \beta(\sigma)(\text{mod } \mathbb{Q}^*)$ is a group homomorphism, and we denote by K_β the fixed field of its kernel, which is an abelian extension of $\mathbb{Q}$. We will say that K_β is a *splitting field*. In general, there is no minimal splitting field for a $\mathbb{Q}$-curve C, but only fields that are minimal in the set of splitting fields for C. For a splitting map β we define a character $\epsilon(\sigma) := \frac{\beta(\sigma)^2}{d(\sigma)}$ and we let K_ϵ be the fixed field of its kernel. It can be shown that every splitting field is of the form $K_\epsilon K_d$, and we will say that ϵ is a *splitting character corresponding to* β, or simply a *splitting character*.

Any 2-cocycle in $H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ can be viewed as taking values on $\bar{\mathbb{Q}}^*$, considered as a $\text{Gal}(K/\mathbb{Q})$-module with trivial action. To the image of c_K (or its cohomology class $\xi_K(C)$) in $H^2(K/\mathbb{Q}, \bar{\mathbb{Q}}^*)$ we will call the *Schur class of* c_K. Given any Galois character $\epsilon : G_{\mathbb{Q}} \to \bar{\mathbb{Q}}^*$ define

$$\theta_\epsilon(\sigma, \tau) = \sqrt{\epsilon(\sigma)}\sqrt{\epsilon(\tau)}\sqrt{\epsilon(\sigma\tau)}^{-1} \text{ for } \sigma, \tau \in G_{\mathbb{Q}}. \tag{2.8}$$

The map θ_ϵ is a 2-cocycle of $G_{\mathbb{Q}}$ with values in $\{\pm 1\}$ and its cohomology class is independent of the choice of the roots.

Theorem 2.3.2 *(Quer) Let C be a $\mathbb{Q}$-curve. Let $\{a_i\}$, $\{d_i\}$ be a dual base to the corresponding degree map. A Galois character $\epsilon : G_{\mathbb{Q}} \to \bar{\mathbb{Q}}^*$ is a splitting character for $\xi(C)$ if, and only if,*

$$[\theta_\epsilon] = \xi(C)_\pm \text{ in } H^2(G_{\mathbb{Q}}, \{\pm 1\}) \simeq Br_2(\mathbb{Q}).$$

Furthermore, if ϵ is a splitting character then there exists a curve in the isogeny class of C completely defined over $L = K_\epsilon K_d$ such that $\xi_L(C)$ has trivial Schur class.

Furthermore, Quer proves that there exists an element $\gamma \in L$ such that the curve C provided by the previous theorem is obtained by twisting E by γ. He also proves that γ is a solution of a specific embedding problem (see section 2.3.2 for this).

It is useful to note that splitting characters can be determined by local information. From the well known sequence

$$1 \to \text{Br}_2(\mathbb{Q}) \to \oplus \text{Br}_2(\mathbb{Q}_p) \to \{\pm 1\} \to 1,$$

and the usual identification of $\text{Br}_2(\mathbb{Q}_p)$ with $\{\pm 1\}$, an element ξ of $Br_2(\mathbb{Q})$ its completely determined by its local components $\xi_p \in Br_2(\mathbb{Q}_p) = \{\pm 1\}$.

For a quaternion algebra the local components are given by the Hilbert symbol and for the element $[\theta_\epsilon]$ the local component at a finite prime p is given by the parity of the p-component of the character ϵ,

$$[\theta_\epsilon]_p = \epsilon_p(-1)$$

where we identify ϵ with a Dirichlet character by class field theory.

Finally, since we will be interested in finding curves for which $B := \text{Res}_{K/\mathbb{Q}}(E/K)$ decomposes as a product of abelian varieties of GL_2-type we have the following theorem, which is

a particular case of Theorem 5.4 in [54].

Theorem 2.3.3 *(Quer) Let C be a $\mathbb{Q}$-curve without complex multiplication completely defined over a minimal splitting field K and such that $\xi_K(C)$ has trivial Schur class. Let ϵ be a splitting character for $\xi_K(C)$. Let $\{a_i\}$ and $\{d_i\}$ be dual bases with respect to the degree map chosen such that corresponding to C.*

Then, if ϵ has order 4, $K_\epsilon \cap K_d = \mathbb{Q}(\sqrt{a_1})$ and $d_1 = 2$, then the abelian variety B decomposes over $\mathbb{Q}$ as a product of two non $\mathbb{Q}$-isogenous abelian varieties of GL_2-type both of them with $\mathbb{Q}$-endomorphism algebra isomorphic to $\mathbb{Q}(\zeta_8\sqrt{2}, \sqrt{d_2}, ..., \sqrt{d_m})$

2.3.2 $\mathbb{Q}$-curves and embedding problems

Let $K/\mathbb{Q}$ be a number field with group $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\{\pm 1\}$ the cyclic group of order 2 be considered as a G-module with trivial action, and

$$\xi : 1 \to \{\pm 1\} \to \tilde{G} \to G \to 1$$

be a central extension corresponding to the 2-cocycle class $\xi \in H^2(G, \{\pm 1\})$. The extension $K/\mathbb{Q}$ and $\xi \in H^2(G, \{\pm 1\})$ determine an embedding problem that we denote by $(K/\mathbb{Q}, \{\pm 1\}, \xi)$, whose solutions are Galois extensions $\tilde{K}/\mathbb{Q}$ containing K with Galois group $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq \tilde{G}$ and such that the natural map $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$ of Galois theory corresponds to the epimorphisms in the exact sequence ξ. It is known that obstructions to the solvability of this problem is the inflation $\mathrm{Inf}\, \xi \in H^2(G_\mathbb{Q}, \{\pm 1\})$ and that if the problem is unobstructed, then the solutions are the fields $K(\sqrt{\gamma})$ for the elements $\gamma \in K^*$ for which there exist elements $\beta_s \in K^*$ for $s \in G$ with

$$^s\gamma = \beta_s^2\gamma, \text{ and } (s,t) \mapsto \beta_s{}^s\beta_t\beta_{st}^{-1} \text{ has cohomology class } \xi.$$

Conversely, if $s \mapsto \beta_s : G \to K^*$ is a map such that $\xi(s,t) = \beta_s{}^s\beta_t\beta_{st}^{-1}$ takes values into $\{\pm 1\}$ then c is a 2-two cocycle and $(K/\mathbb{Q}, \{\pm 1\}, [\xi])$ is solvable. We call such a map β a *splitting map* for the cocycle ξ. Moreover, we can take a solution to this embedding problem the field $K(\sqrt{\gamma})$ for any element $\gamma \in K^*$ of the form

$$\gamma = \sum_{s \in G} \frac{^s x}{\beta_s^2}, \qquad x \in K^*. \tag{2.9}$$

Now we explain the embedding problem related to $\mathbb{Q}$-curves. Let K be a number field and $G = \mathrm{Gal}(K/\mathbb{Q})$. Assume that C is a $\mathbb{Q}$-curve defined over the field K_d and let $\xi_K \in H^2(K/\mathbb{Q}, \mathbb{Q}^*)$ be an element whose inflation to $G_\mathbb{Q}$ is $\xi(C)$ so that by theorem 2.4 in [54] we know there is a curve C_γ isomorphic to C completely defined over K and such that $\xi_K(C_\gamma) = \xi_K$. Let $L/\mathbb{Q}$ be a Galois extension over which the curve C is completely defined.

Consider the cohomology class in $H^2(KL/\mathbb{Q}, \mathbb{Q}^*)$ defined by

$$\xi_{KL} = \mathrm{Inf}_G^{Gal(KL/\mathbb{Q})}\xi_K(C) \times \mathrm{Inf}_{Gal(L/\mathbb{Q})}^{Gal(KL/\mathbb{Q})}\xi_L(C)^{-1}.$$

Then,

$$\mathrm{Inf}_{Gal(KL/\mathbb{Q})}^{G_\mathbb{Q}}\xi_{KL} = \mathrm{Inf}_G^{G_\mathbb{Q}}\xi_K \times \mathrm{Inf}_{Gal(L/\mathbb{Q})}^{G_\mathbb{Q}}\xi_L^{-1} = \xi(C)\xi(C)^{-1} = 1.$$

From the decomposition $\mathbb{Q}^* = \{\pm 1\} \times \mathbb{Q}^+$ we have the decomposition

$$H^2(KL/\mathbb{Q}, \mathbb{Q}^*) = H^2(KL/\mathbb{Q}, \{\pm 1\}) \times H^2(KL/\mathbb{Q}, \mathbb{Q}^+)$$

and the inflation maps splits as the product of the two corresponding inflation maps. Since $\mathbb{Q}^*$ is torsion free the inflation map on the second factor is injective. Then it follows that ξ_{KL} has only sign component and we can identify it with an element of $H^2(KL/\mathbb{Q}, \{\pm 1\})$ corresponding to an unobstructed embedding problem. Furthermore, it can be seen that we are identifying ξ_{LK} with the product of the sign components of the inflations of ξ_K and ξ_L to $\mathrm{Gal}(KL/\mathbb{Q})$. Moreover, in [54] it is shown that there are solutions γ to this problem associated with particular choices of $\{\beta_s\}$ such that $\gamma \in K$ and not in KL as one would expect.

In order to find γ explicitly we will make use of the theory in [55] of which we now recall the important points.

Let $S \subset \mathbb{Q}^*/\mathbb{Q}^{*2}$ be finite subgroup and $K_2 = \mathbb{Q}(\sqrt{S})$ be the corresponding polyquadratic number field. Every homomorphism $\chi : G = \mathrm{Gal}(K_2/\mathbb{Q}) \to \mathbb{Z}/2\mathbb{Z}$ can be written as ${}^\sigma\sqrt{a} = (-1)^{\chi(\sigma)}\sqrt{a}$ for some $a \in S$; we denote by χ_a this homomorphism. Given $a, b \in S$ let $c_{a,b}$ be the map $G \times G \to \{\pm 1\}$ defined by

$$c_{a,b}(\sigma, \tau) = (-1)^{\chi_a(\sigma)\chi_b(\tau)}, \qquad \sigma, \tau \in G.$$

This is a 2-cocycle, it is multiplicative in a and b and the class $\mathrm{Inf}[c_{a,b}] \in \mathrm{Br}_2(\mathbb{Q}) = H^2(G_\mathbb{Q}, \{\pm 1\})$ is that of the cyclic algebra (a, b). In general, if $A = \{a_i\}_{1 \le i \le m}$ and $B = \{b_i\}_{1 \le i \le m}$ are two ordered sets of elements of S we denote by $c_{A,B}$ the product of the c_{a_i,b_i}.

Let $L/\mathbb{Q}$ be a cyclic extension of degree a power of 2 and let $\epsilon : \mathrm{Gal}(L/\mathbb{Q}) \to \bar{\mathbb{Q}}^*$ be an injective character. Let $M/\mathbb{Q}$ be a polyquadratic extension and $A = \{a_1, ..., a_m\}$ a basis of the subgroup $\mathbb{Q}^*/\mathbb{Q}^{*2}$ corresponding to it by Kummer theory. We assume that if $L \cap M \neq \mathbb{Q}$ then A has been chosen with $L \cap M = \mathbb{Q}(\sqrt{a_1})$. Let $B = \{b_1, ..., b_m\}$ be any subset of $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Put $K = LM(\sqrt{b_1}, ..., \sqrt{b_m})$. Let $\xi_{A,B}$ be the inflation to $\mathrm{Gal}(K/\mathbb{Q})$ of the 2-cocycle class $[c_{A,B}]$ defined above; let $[c_\epsilon]$ be the inflation to $\mathrm{Gal}(K/\mathbb{Q})$ of a the 2-cocycle class corresponding to the 2-cocycle θ_ϵ of $\mathrm{Gal}(L/\mathbb{Q})$ defined by the formula (2.8).

Consider the decomposition of K as a composition of linearly disjoint extensions of $\mathbb{Q}$,

$$K = L \cdot \mathbb{Q}(\sqrt{a_e}) \cdots \mathbb{Q}(\sqrt{a_m}) \cdot N,$$

(with $e = 1$ if $L \cap M = \mathbb{Q}$ or $e = 2$ if $L \cap M = \mathbb{Q}(\sqrt{a_1})$), where N is obtained by adjoining to $\mathbb{Q}$ some of the $\sqrt{b_i}$. Let σ_0 (if $L \neq \mathbb{Q}$), σ_e,...,σ_m,τ_1,...τ_s be a basis of $G = \mathrm{Gal}(K/\mathbb{Q})$ reflecting that decomposition, meaning that each of them only act non-trivially on one component of the composition. Let r be the order of σ_0 and all the other generators σ_i and τ_i have order 2. Denote by $N_\sigma(x)$ the norm of x with respect to the extension $K/K^{\langle\sigma\rangle}$. Letting $[c] = \xi_{A,B}[c_\epsilon]$ we have the following theorem.

Theorem 2.3.4 *(Quer) Under the assumptions of the previous paragraphs, the embedding problem $(K/\mathbb{Q}, \{\pm 1\}, [c])$ is solvable if, and only if, there exist elements α_0, α_e,...,$\alpha_m \in LM$ such that*

(i) If $L \neq \mathbb{Q}$, put $\zeta = c(1,\sigma_0)c(\sigma_0,\sigma_0)c(\sigma_0^2,\sigma_0)...c(\sigma_0^{r-1},\sigma_0)$

$$N_{\sigma_0}(\alpha_0) = \begin{cases} \zeta & \text{if } e = 1 \\ \zeta b_1^{r/2} & \text{if } e = 2 \end{cases},$$

(ii) $N_{\sigma_0}(\alpha_i) = b_i$ for $e \leq i \leq m$, and

(iii) ${}^{\sigma_i - 1}\alpha_j = {}^{\sigma_j - 1}\alpha_i$ for all i, j

Moreover, in that case there exists a splitting map β for the cocycle c with, if $L \neq \mathbb{Q}$,

$$\beta_{\sigma_0} = \begin{cases} \alpha_0 & \text{if } e = 1 \\ \alpha_0/\sqrt{b_1} & \text{if } e = 2 \end{cases},$$

$$\beta_{\sigma_i} = \frac{\alpha_i}{\sqrt{b_i}}, e \leq i \leq m, \beta_{\tau_i} = 1, 1 \leq i \leq s$$

and every solution γ corresponding to it belongs to the subfield $LM \subset K$.

2.3.3 Proof of Theorem 2.1.10

In this section we prove Theorem 2.1.10 by using the theory on the previous two sections. First we need to find an adequate γ and then Theorem 2.1.10 will follows by applying Theorem 2.3.3 to E_γ. We need E_γ not to have complex multiplication.

Theorem 2.3.5 *Let (a, b, c) be a primitive non-trivial solution of equation (2.3) or (2.4). Then the curve $E = E_{(a,b)}$ has no complex multiplication.*

Proof: From Corollary 3.2.8 we have $|c| > 1$. Since the primes dividing c are of semistable reduction of E, the theorem follows from Theorem 2.1.2.

■

The minimal field of definition of E is $K_d = \mathbb{Q}(\sqrt{5})$ and $\{a_1\} = \{5\}$, $\{d_1\} = \{2\}$ is a dual base respect to the corresponding degree map. Since the quaternion algebra $(5, \pm 1) \neq 1$

from Proposition 4.3b of [54] we know that K_d is not a splitting field. Let $L = \mathbb{Q}(\sqrt{5}, \sqrt{-2})$ be a biquadratic field of complete definition of E (i.e. a field where all the conjugates of E and isogenies between them are defined) and let $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ be such that

$$\begin{cases} \sigma(\sqrt{5}) = \sqrt{5} & \text{and} \quad \sigma(\sqrt{-2}) = -\sqrt{-2} \\ \tau(\sqrt{5}) = -\sqrt{5} & \text{and} \quad \tau(\sqrt{-2}) = \sqrt{-2} \end{cases}$$

From the explicit expression for the isogeny we compute $c_L(g,h) = \phi_g{}^g \phi_h \phi_{gh}^{-1}$

		h			
		1	σ	τ	$\sigma\tau$
g	1	1	1	1	1
	σ	1	1	-1	-1
	τ	1	1	-2	-2
	$\sigma\tau$	1	1	2	2

Table 2.2: Values of c_L

From Table 2.2 we see that $c_K(\sigma,\tau) \neq c_K(\tau,\sigma)$ hence we can not find a splitting map $\mathrm{Gal}(L/\mathbb{Q}) \to \bar{\mathbb{Q}}^*$ such that

$$c_K(g,h) = \frac{\beta(g)\beta(h)}{\beta(gh)},$$

hence L does not contain a splitting field for $\xi(C)$. We want to apply the second statement in Theorem 2.3.2. By Theorem 2.3.1 one sees that $\xi(C)_\pm = (5,2)$. Using the first statement in Theorem 2.3.2 and local information we check that the character $\epsilon : (\mathbb{Z}/20\mathbb{Z})^* \to \mathbb{Q}(\zeta_4)$ of order 4 and conductor 20 given by

$$\epsilon = \epsilon_2 \epsilon_5, \tag{2.10}$$

where ϵ_2 is the quadratic character of conductor 4 and ϵ_5 is the character of order 4 and conductor 5 given by $\epsilon_5(2) = \zeta_4 = i$ is an appropriate splitting character. Its fixed field is $K_\epsilon = \mathbb{Q}(\theta)$, where $\theta = \sqrt{\frac{1}{2}(5+\sqrt{5})}$. Then it follows from Theorem 2.3.2 that there is a representative in the isogeny class of E which is completely defined over $K_\beta = K_\epsilon K_d = \mathbb{Q}(\theta)\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\theta)$ and has trivial Schur class. We denote it by E_γ.

Now we will explicitly solve an embedding problem to find γ. As explained before, let

$$\xi_{K_\beta L} = (\mathrm{Inf}_{Gal(K_\beta/\mathbb{Q})}^{Gal(K_\beta L/\mathbb{Q})} c_{K_\beta}(E_\gamma))_\pm (\mathrm{Inf}_{Gal(L/\mathbb{Q})}^{Gal(K_\beta L/\mathbb{Q})} c_L(E))_\pm \tag{2.11}$$

after the identification with an element of $H^2(K_\beta L/\mathbb{Q}, \{\pm 1\})$. The embedding problem associated with $\xi_{K_\beta L}$ is unobstructed and admits solutions $\gamma \in K_\beta$. Applying Theorem 2.3.4 will give one of these solutions, but first we need to restate our embedding problem in a way compatible with the notation of the theorem. Note that $c_L(\mathrm{E})_\pm = c_{A,B}$ with $A = \{-10\}$ and $B = \{5\}$ where $c_L(\mathrm{E})_\pm$ is given by the signs in Table 2.2. Let $\xi_{A,B}$ and

c_ϵ be as in the previous section, where the character ϵ is the one above. Now using to the notation of Theorem 2.3.4 we consider the decomposition

$$K = \mathbb{Q}(\theta, \sqrt{-2}) = LMN = \mathbb{Q}(\theta)\mathbb{Q}(\sqrt{-10})\mathbb{Q},$$

which gives $e = 1$ ($L \cap M = \mathbb{Q}$), $m = 1$ and $s = 0$, and let $\sigma_0, \sigma_1 \in \mathrm{Gal}(K/\mathbb{Q})$ reflect this decomposition, that is

$$\begin{cases} \sigma_0(\sqrt{5}) = -\sqrt{5} & \text{and} \quad \sigma_0(\sqrt{-2}) = -\sqrt{-2} \\ \sigma_1(\sqrt{5}) = \sqrt{5} & \text{and} \quad \sigma_1(\sqrt{-2}) = -\sqrt{-2} \end{cases}.$$

We put $c = \xi_{A,B} c_\epsilon$ and compute $\zeta = c(1, \sigma_0)c(\sigma_0, \sigma_0)c(\sigma_0^2, \sigma_0)c(\sigma_0^3, \sigma_0) = -1$ from the Tables 2.3 and 2.4.

		h							
		1	σ_0	σ_0^2	σ_0^3	σ_1	$\sigma_1\sigma_0$	$\sigma_1\sigma_0^2$	$\sigma_1\sigma_0^3$
g	1	1	1	1	1	1	1	1	1
	σ_0	1	1	1	-1	1	1	1	-1
	σ_0^2	1	1	-1	-1	1	1	-1	-1
	σ_0^3	1	-1	-1	-1	1	-1	-1	-1
	σ_1	1	1	1	1	1	1	1	1
	$\sigma_1\sigma_0$	1	1	1	-1	1	1	1	-1
	$\sigma_1\sigma_0^2$	1	1	-1	-1	1	1	-1	-1
	$\sigma_1\sigma_0^3$	1	-1	-1	-1	1	-1	-1	-1

Table 2.3: Values of θ_ϵ

		h							
		1	σ_0	σ_0^2	σ_0^3	σ_1	$\sigma_1\sigma_0$	$\sigma_1\sigma_0^2$	$\sigma_1\sigma_0^3$
g	1	1	1	1	1	1	1	1	1
	σ_0	1	1	1	1	1	1	1	1
	σ_0^2	1	1	1	1	1	1	1	1
	σ_0^3	1	1	1	1	1	1	1	1
	σ_1	1	-1	1	-1	1	-1	1	-1
	$\sigma_1\sigma_0$	1	-1	1	-1	1	-1	1	-1
	$\sigma_1\sigma_0^2$	1	-1	1	-1	1	-1	1	-1
	$\sigma_1\sigma_0^3$	1	-1	1	-1	1	-1	1	-1

Table 2.4: Values of $\xi_{A,B}$

Theorem 2.3.4 says that the embedding problem $(K/\mathbb{Q}, \{\pm 1\}, [c])$ is solvable if and only if we can find elements α_0, α_1 such that

$$\begin{aligned} N_{\sigma_0}(\alpha_0) &= -1 \\ N_{\sigma_1}(\alpha_1) &= 5 \\ \frac{{}^{\sigma_1}\alpha_0}{\alpha_0} &= \frac{{}^{\sigma_0}\alpha_1}{\alpha_1}. \end{aligned}$$

Since $c = \xi_{K_\beta L}$ (here we are using notation of equation (2.11)) we already know that this problem is unobstructed and a small search leads us to

$$\begin{aligned} \alpha_0 &= \frac{1}{2}(-1+\theta+\theta^2)\sqrt{-2} \\ \alpha_1 &= -5+2\theta^2. \end{aligned}$$

Moreover, the same theorem gives us a splitting map for the cocycle c given by

$$\begin{aligned} \beta_{\mathrm{id}} &= \beta_{\sigma_1} = 1, \\ \beta_{\sigma_0} &= \beta_{\sigma_1\sigma_0} = \alpha_0, \\ \beta_{\sigma_0^2} &= \beta_{\sigma_1\sigma_0^2} = 2-\theta-\theta^2, \\ \beta_{\sigma_0^3} &= \beta_{\sigma_1\sigma_0^3} = \frac{\sqrt{-2}}{2}(-\theta^2-\theta+3). \end{aligned}$$

Finally, taking $x = 1/4$ in formula (2.9) we conclude that $\gamma = 2\theta^2 - \theta - 5 \in K$ is a solution. Now a direct application of Theorem 2.3.3 to E_γ yields Theorem 2.1.10.

■

Chapter 3

Equations of signature (r, r, p)

The objective of this chapter is to describe a general strategy to study some Fermat-type equations of the form signature (r, r, p). In section 3.1 we will recall some background on Hilbert modular forms and state the level lowering results from Jarvis, Rajaei and Fujiwara. In section 3.2 we will give the general method for constructing Frey curves and applying a modular approach via Hilbert modular forms. Finally, in section 3.3 we will recall some modularity results of Kisin and Skinner-Wiles and prove modularity of our Frey curves under certain conditions as well as irreducibility of the mod p representations attached to them.

3.1 Galois representations attached to Hilbert modular forms

In this section we will briefly recall the basics of Hilbert modular forms (HMF) and results on level lowering from Jarvis, Rajaei and Fujiwara. Since elliptic curves correspond to HMF of parallel weigh 2 and trivial character we will only define those here. For details and more general definitions see [24] and the references there. For the level lowering theorems see [56], [36] and [32].

Let F be a totally real number field of degree $d > 1$ and let $\iota_1, ...\iota_d$ be the distinct real embeddings of F. For an element $x \in F$ let $x_i = \iota_i(x)$. There is an embedding of the group $\mathrm{GL}_2(F)$ into $\mathrm{GL}_2(\mathbb{R})^d$ by sending

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longrightarrow \left(\begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \right)_{1 \leq i \leq d}.$$

This embedding allows the group

$$\mathrm{GL}_2(F)^+ = \{\gamma \in \mathrm{GL}_2(F) : \ (\det \gamma)_i > 0 \text{ for } 1 \leq i \leq d\}$$

to act on $\mathcal{H}^d$, the product of d copies of the upper half plane, by the following rule: if

$\gamma \in \mathrm{GL}_2(F)^+$ and $\tau = (\tau_1, .., \tau_d) \in \mathcal{H}^d$, then

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{acts on } \tau \text{ by} \quad \gamma\tau := \left(\frac{a_i\tau_i + b_i}{c_i\tau_i + d_i}\right)_{1 \leq i \leq d}.$$

Let $\mathfrak{d}$ be the different of F and $\mathfrak{n}$ an ideal of F. Let also h be the narrow class number of F and $\mathfrak{c}_j$ a system of representative ideals for the narrow ideal classes of F. Assume further that the $\mathfrak{c}_j$ are coprime to $\mathfrak{n}$ and define

$$\Gamma_0(\mathfrak{c}_j, \mathfrak{n}) := \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \begin{pmatrix} \mathcal{O}_F & (\mathfrak{d}\mathfrak{c}_j)^{-1} \\ \mathfrak{d}\mathfrak{c}_j\mathfrak{n} & \mathcal{O}_F \end{pmatrix} : ad - bc \in \mathcal{O}_F^{\times +} \},$$

where $\mathcal{O}_F^{\times +}$ are the totally positive units of F. If $f : \mathcal{H}^d \to \mathbb{C}$ is an holomorphic function and $\gamma \in \Gamma_0(\mathfrak{c}_j, \mathfrak{n})$ we define

$$(f|_2\gamma)(\tau) = \prod_{i=1}^{d} \det(\gamma)_i (c_i\tau_i + d_i)^{-2} f(\gamma\tau).$$

Definition 3.1.1 *A classic Hilbert modular form of weight* 2 *on* $\Gamma_0(\mathfrak{c}_j, \mathfrak{n})$ *is a holomorphic function on* $\mathcal{H}^d$ *satisfying the transformation rule* $f|_2\gamma = f$ *for all* $\gamma \in \Gamma_0(\mathfrak{c}_j, \mathfrak{n})$. *We denote by* $M_2(\mathfrak{c}_j, \mathfrak{n})$ *the set of all classic Hilbert modular forms of weight* 2 *on* $\Gamma_0(\mathfrak{c}_j, \mathfrak{n})$.

Remark 3.1.2 *There is no holomorphy condition at the cusps as in the case of classic modular forms. This conditions follows from Koecher's principle in the case* $[F : \mathbb{Q}] > 1$ *(see [73], Chapter 1).*

Since $f \in M_2(\mathfrak{c}_j, \mathfrak{n})$ is $\Gamma_0(\mathfrak{c}_j, \mathfrak{n})$-invariant it satisfies $f(\tau + \mu) = f(\tau)$ for all $\tau \in \mathcal{H}^d$ and $\mu \in \mathfrak{c}_j^{-1}$. In particular, it admits a Fourier expansion

$$f(\tau) = c_0^j + \sum_{\mu \in (\mathfrak{c}_j)_+^{-1}} c_\mu e^{2\pi i \mathrm{Tr}(\mu\tau)}, \qquad \text{where } \mathrm{Tr}(\mu\tau) = \sum_i \mu_i\tau_i$$

If f vanishes at the cusps it is called a *cusp form* on $\Gamma_0(\mathfrak{c}_\mathfrak{i}, \mathfrak{n})$. Denote by $S_2(\Gamma_0(\mathfrak{c}_\mathfrak{i}, \mathfrak{n}))$ the set of Hilbert cusp forms on $\Gamma_0(\mathfrak{c}_i, \mathfrak{n})$.

Definition 3.1.3 *Let* h *be the narrow class number of* F. *A cusp form of parallel weight* 2 *and level* $\mathfrak{n}$ *is an* h*-tuple* $(f_i, ..., f_h)$ *where* $f_i \in S_2(\Gamma_0(\mathfrak{c}_\mathfrak{i}, \mathfrak{n}))$. *We denote by* $S_2(\mathfrak{n})$ *the space of Hilbert cusp forms of parallel weight* 2 *and level* $\mathfrak{n}$.

We will say that $f = (f_i) \in S_2(\mathfrak{n})$ is *normalized* if $c_{(1)}(f_i) = 1$ for $i = 1, .., h$. The space $S_2(\mathfrak{n})$ is a finite dimensional vector space over $\mathbb{C}$ and it admits an action of the commuting self-adjoint Hecke operators $T_\mathfrak{p}$ for all prime ideal $\mathfrak{p}$ not dividing $\mathfrak{n}$ (see [74], section 1.2). A cusp form $S_2(\mathfrak{n})$ is called an *eigenform* if it is a simultaneous eigenvector for these operators. For $f = (f_i) \in S_2(\mathfrak{n})$ an eigenform one denotes by $a_\mathfrak{p}(f)$ the eigenvalue of $T_\mathfrak{p}$ acting on f.

In the particular case of F having narrow class number 1, for a non-zero ideal $\mathfrak{n}$ we have that $\mathfrak{n} = v\mathfrak{d}^{-1}$ for some $v \in \mathfrak{d}_+$ and $a_{\mathfrak{n}}(f) = c_v$. Denote by $\mathbb{Q}_f$ the totally real number field field generated by adding to $\mathbb{Q}$ the values $a_{\mathfrak{p}}(f)$. The following theorem is a particular case the work of Shimura, Jacquet-Langlands, Carayol, Wiles and Taylor on representations attached to Hilbert modular forms. References include [75], [13] and [70]. See also [62] for the definition of compatible system of ℓ-adic representations.

Theorem 3.1.4 *Let f be an eigenform in $S_2(\mathfrak{n})$. There exists a compatible system of λ-adic representations unramified outside $\mathfrak{n}l$*

$$\rho_{f,\lambda} : G_K \longrightarrow GL_2(\mathcal{O}_{f,\lambda})$$

for each prime $\lambda \mid l$ in $\mathbb{Q}_f$, satisfying:

$$Trace(\rho_{f,\lambda}(Frob_{\mathfrak{q}})) = a_{\mathfrak{q}}(f), \qquad det(\rho_{f,\lambda}(Frob_{\mathfrak{q}})) = Norm(\mathfrak{q})$$

for all primes $\mathfrak{q}$ not dividing $\mathfrak{n}l$.

We have not defined Hilbert modular forms of more general weight because except for the proof of Theorem 3.3.9 we will always work in parallel weight 2. Nevertheless, we want to stress that for modularity purposes sometimes we want to think more generally, that is, allowing Hilbert eigenforms of any parallel weight $k \geq 2$.

Definition 3.1.5 *Let $\bar{\rho} : G_F \to GL_2(\mathbb{F}_{p^r})$ be a continuous representation. We say that $\bar{\rho}$ is modular of level $\mathfrak{n}$ if there exists an eigenform $f \in S_2(\mathfrak{n})$ over F and a homomorphism $j : \mathcal{O}_{\mathbb{Q}_f} \to \mathbb{F}_{p^r}$ such that, for all primes $\mathfrak{q} \nmid \mathfrak{n}$,*

$$Trace(\bar{\rho}(Frob_{\mathfrak{q}})) = j(a_{\mathfrak{q}}(f))$$

If f can be chosen to be of (parallel) weight k and level $\mathfrak{n}$, we say that $\bar{\rho}$ is modular of (parallel) weight k and level $\mathfrak{n}$.

To end this section we will state level lowering theorems from Fujiwara, Jarvis and Rajaei.

Theorem 3.1.6 *(Fujiwara) Let $\bar{\rho} : G_F \to GL_2(\bar{\mathbb{F}}_p)$ be a continuous irreducible representation attached to an eigenform $f \in S_2(\mathfrak{q}\mathfrak{n})$ where $\mathfrak{q} \nmid p\mathfrak{n}$ is a prime ideal in F. Suppose $[F(\mu_p) : F] \geq 4$. Then if $\bar{\rho}$ is unramified at $\mathfrak{q}$, and $N_{F/\mathbb{Q}}(\mathfrak{q}) \not\equiv 1 \pmod{p}$, there exists a Hilbert cuspidal eigenform $f' \in S_2(\mathfrak{n})$ to which $\bar{\rho}$ is attached.*

Theorem 3.1.7 *(Jarvis) Let F be a totally real number field, and $\mathfrak{p}$ be a prime of F dividing the rational prime p. Suppose that $\bar{\rho} : G_F \to GL_2(\bar{\mathbb{F}}_p)$ is a continuous irreducible representation which is attached to some cusp form $f \in S_2(\mathfrak{p}\mathfrak{n})$, where $\mathfrak{p} \nmid \mathfrak{n}$. Suppose also*

1) *If $[F(\mu_p) : F] = 2$, then $\bar{\rho}$ is not induced from a character of $G_{F(\sqrt{-3})}$.*

2) $e < p-1$, *where* e *denotes the absolute ramification of* $F_{\mathfrak{p}}$.

Then if $\bar{\rho}$ *is finite at* $\mathfrak{p}$, *there exists an Hilbert eigenform* $f' \in S_2(\mathfrak{n})$ *to which* $\bar{\rho}$ *is attached.*

Theorem 3.1.8 *(Rajaei) Let* p *be an odd prime and* $\bar{\rho} : G_F \to GL_2(\bar{\mathbb{F}}_p)$ *an irreducible representation attached to an eigenform* $f \in S_2(\mathfrak{q}\mathfrak{n})$ *where* $\mathfrak{q} \nmid p\mathfrak{n}$ *is a prime ideal in* F. *If* $\mathbb{Q}(\zeta_p)^+ \subset F$ *assume that* $\bar{\rho}$ *is not induced from a character and if* $[F : \mathbb{Q}]$ *is even assume moreover that* f *is either special or supercuspidal at a finite prime* $\mathfrak{q}_0$ *(prime to* $p\mathfrak{q}$*). Then if* $\bar{\rho}$ *is unramified at* $\mathfrak{q}$, $\bar{\rho}$ *comes from an Hilbert cuspidal eigenform in* $S_2(\mathfrak{n})$.

3.2 A Recipe for $x^r + y^r = Cz^p$

For a fixed prime $r > 5$ our method will allow us to attack equations with shape

$$x^r + y^r = Cz^p, \tag{3.1}$$

for C in an infinite family of integers only divisible by primes $q \not\equiv 1, 0 \pmod{r}$. Let (a, b, c) be a triple of integers such that $a^r + b^r = Cc^p$. We say that it is a *primitive* solution if $(a, b) = 1$ and we will say that it is a *trivial* solution if $|abc| \leq 1$. Following the terminology introduced by Sophie Germain in her work on the FLT we will divide solutions to (3.1) into two cases.

Definition 3.2.1 *A primitive solution* (a, b, c) *of* $x^r + y^r = Cz^p$ *is called a first case solution if* r *does not divide* c, *and a second case solution otherwise.*

In general, the method presented here can only succeed in proving the non-existence of primitive first case solutions (see also Remark 3.2.17). Briefly, it goes as follows: we first relate a non-trivial primitive solution (a, b, c') of (3.1) to a non-trivial primitive solution (a, b, c) of another Diophantine equation (independent of C) with coefficients in the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_r)$, denoted by K^+. For the latter equation we will be interested only in the non-existence of solutions (a, b, c) such that $C \mid a + b$. We will attach to such a solution (a, b, c) a Frey curve $E_{(a,b)}$ defined over K^+ which is not a $\mathbb{Q}$-curve. We prove the absolutely irreducibility of $\bar{\rho}_{E,p}$ for p greater than a constant $M(r)$. Then if the Frey curves $E_{(a,b)}$ are supposed modular (in some cases we can prove they actually are) we are able to apply the level lowering results for Hilbert modular forms over K^+ to get an isomorphism $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}$, where f belongs to a space of Hilbert newforms almost not depending on the solution (a, b, c). In the rest of this chapter we will treat in detail the method just described which corresponds to perform steps (I) and (II) of the modular approach as explained in the introduction.

Remark 3.2.2 *Actually, we will relate a solution* $(a, b, c') \in \mathbb{Z}^3$ *of* (3.1) *to solutions* (a, b, c) *of several new equations over* K^+. *We will see that the new solutions differ only in the value*

of $c \in \mathcal{O}_{K^+}$. Since the Frey curves attached to each of the new equations depend only on (a,b) we are able to attach several Frey curves to a single putative solution of (3.1). *In theory, this would allow to apply the multi-Frey technique as in Chapter* 2. *Unfortunately, due to computational limitations, in the application to $r = 13$ in Chapter 4 we are be able to apply the method using only one curve.*

To prove the non-existence of solutions of a particular equation we also need to complete Step (III) which is highly dependent on the value of r. Since the next chapter is mainly devoted to Step (III) for the particular cases $r = 7, 13$, by now we will only make a couple of observations that will became clear later. To contradict the isomorphism $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}$ (step III) we will need to compute newforms in previously determined spaces and use the values $a_q(E)$, the fact that $C \mid a+b$ and $r \nmid c$ (first case solution) to derive a contradiction. Unfortunately, the computation of the newforms is in general impossible. The problem being that the degree of K^+ is $(r-1)/2$, which grows with r, and consequently the dimension of the cusp spaces that we need to consider will grow extremely fast. Actually, already for small values of r we will find impossible computations. Nevertheless, if $r \equiv 1 \pmod 6$ we will show that Frey curves over a subfield K_0 of K^+ exist. In this case K^+ has degree $3k$, K_0 will have degree k and this difference is enough for the computation of newforms to be possible for $r = 7$ and 13 as we will see in the next chapter.

3.2.1 Relating Diophantine equations.

The factorization $x^r + y^r = (x+y)\phi_r(x,y)$ will play a key role in the strategy so we start by proving a few properties about $\phi_r(x,y)$. Let ζ denote a primitive r-th root of unity. Observe that

$$\phi_r(x,y) = \sum_{i=0}^{r-1} (-1)^i x^{r-1-i} y^i.$$

and consider the decomposition over the cyclotomic field $\mathbb{Q}(\zeta)$

$$\phi_r(x,y) = \prod_{i=1}^{r-1} (x + \zeta^i y). \tag{3.2}$$

Proposition 3.2.3 *Let $\mathfrak{P}_r$ be the prime in $\mathbb{Q}(\zeta)$ above the rational prime r and suppose that $(a,b) = 1$. Then, any two different factors $a+\zeta^i b$ and $a+\zeta^j b$ in the factorization* (3.2) *are coprime outside $\mathfrak{P}_r$. Furthermore, if $r \mid a+b$ then $\upsilon_{\mathfrak{P}_r}(a+\zeta^i b) = 1$ for all i.*

Proof: Suppose that $(a,b) = 1$. Let $\mathfrak{P}$ be a prime in $\mathbb{Q}(\zeta)$ above $p \in \mathbb{Q}$ and a common prime factor of $a+\zeta^i b$ and $a+\zeta^j b$, with $i > j$. Observe that $(a+\zeta^i b) - (a+\zeta^j b) = b\zeta^j(1-\zeta^{i-j}) \in \mathfrak{P}$. Since $\mathfrak{P}$ can not divide b because in this case it would also divide a we conclude that $\zeta^i(1-\zeta^{i-j}) \in \mathfrak{P}$ but ζ^i is a unit so $1-\zeta^{i-j} \in \mathfrak{P}$, that is $\mathfrak{P} = \mathfrak{P}_r$. Now for the last statement in the proposition, suppose that $r \mid a+b$. Then,

$$a + \zeta^i b = a + b - b + \zeta^i b = (a+b) + (\zeta^i - 1)b,$$

and since $\upsilon_{\mathfrak{P}_r}(\zeta^i - 1) = 1$ we have $\upsilon_{\mathfrak{P}_r}(a + \zeta^i b) = \min\{(r-1)\upsilon_r(a+b), 1\} = 1$

■

Corollary 3.2.4 *If $(a, b) = 1$, then $a + b$ and $\phi_r(a, b)$ are coprime outside r. Furthermore, if $r \mid a + b$ then $\upsilon_r(\phi_r(a, b)) = 1$.*

Proof: Let p be a prime dividing $a+b$ and $\phi_r(a, b)$ and denote by $\mathfrak{P}$ a prime in $\mathbb{Q}(\zeta)$ above p. $\mathfrak{P}$ must divide at least one of the factors $a + \zeta^i b$. Since a, b are integers $\mathfrak{P}$ can not divide b then it follows from

$$a + b = a + \zeta^i b - \zeta^i b + b = (a + \zeta^i b) + (1 - \zeta^i)b$$

that $\mathfrak{P} = \mathfrak{P}_r$. Moreover, if $r \mid a + b$ it follows from the proposition that $\upsilon_{\mathfrak{P}_r}(a + \zeta^i b) = 1$ for all i then $\upsilon_{\mathfrak{P}_r}(\phi_r(a, b)) = r - 1$ thus $\upsilon_r(\phi_r(a, b)) = 1$.

■

Proposition 3.2.5 *Let $(a, b) = 1$ and $l \not\equiv 1 \pmod r$ be a prime dividing $a^r + b^r$. Then $l \mid a + b$.*

Proof: This is exactly as the proof of Lemma 2.1.6 but with 5 replaced by r.

Since l divides $a^r + b^r$, $l \nmid ab$. Let b_0 be the inverse of $-b$ modulo l. We have $a^r \equiv (-b)^r \pmod l$, hence $(ab_0)^r \equiv 1 \pmod l$. Thus the multiplicative order of ab_0 in $\mathbb{F}_l$ is 1 or r. From the congruence $ab_0 \equiv 1 \pmod l$ it follows $a + b \equiv 0 \pmod l$. If $l \nmid a + b$ then the order of ab_0 is r and $l \equiv 1 \pmod r$.

■

Analogous to what we have done in Chapter 2 we will now relate our initial equation (3.1) with new equations. The following elementary lemma is a generalization of Lemma 2.1.8.

Lemma 3.2.6 *Let p be a prime and suppose there exists a non-trivial primitive solution (a, b, c') to $x^r + y^r = Cz^p$ with $C \neq 0$ an integer divisible only by primes $q \neq r$ satisfying $q \not\equiv 1 \pmod r$. Then there exists a solution $(a, b, c) \in \mathbb{Z}^3$ such that $(a, b) = 1$ (primitive) and $|abc| > 1$ (non-trivial) to*

$$\phi_r(a, b) = c^p \quad \text{or} \tag{3.3}$$

$$\phi_r(a, b) = rc^p \tag{3.4}$$

which satisfies $r \nmid a + b$ in case (3.3) and $r \mid a + b$ in case (3.4). Moreover:

- *if $d \mid C$, then $d \mid a + b$;*
- *the prime divisors of c are all congruent to $1 \pmod r$. In particular, neither 2, nor r divide c.*

Proof: Suppose there exists a non-trivial primitive solution (a, b, c') to $x^r + y^r = Cz^p$ and recall that $a^r + b^r = (a+b)\phi_r(a, b)$. Write $c' = p_1^{n_1}...p_s^{n_s} r^m q_1^{k_1}...q_l^{k_l}$, where for all i p_i, q_i are primes, $p_i \not\equiv 1 \pmod{r}$, $p_i \neq r$ and $q_i \equiv 1 \pmod{r}$.

If a prime $q \not\equiv 1 \pmod{r}$ divides $a^r + b^r$ then by Proposition 3.2.5 we have $q \mid a + b$. Let $c_0 = p_1^{n_1}...p_s^{n_s}$. Then, $Cc_0^p \mid a + b$. Moreover, if $q \neq r$ divides $\phi_r(a, b)$ then $q \mid a^r + b^r$ and by Corollary 3.2.4 $q \nmid a + b$. Hence by Proposition 3.2.5 we have $q \equiv 1 \pmod{r}$.

Suppose $r \nmid a + b$. Hence $m = 0$ in the decomposition of c' and since $a + b$ and $\phi_r(a, b)$ are coprime we have $\phi_r(a, b) = c^p$, where $c' = c_0 c_1 c$, with $c_1 c = q_1^{k_1}...q_l^{k_l}$.

Suppose $r \mid a+b$. Hence $m \neq 0$, and $\phi_r(a, b) = rc^p$ by Corollary 3.2.4, where $c' = c_0 r^m c_1 c$, with $c_1 c = q_1^{k_1}...q_l^{k_l}$.

We will now prove $|abc| > 1$. Suppose we have a non-trivial primitive solution (a, b, c') of $x^r + y^r = Cz^p$, in particular, $|ab| > 1$ or $|c'| > 1$. If $|ab| > 1$ then the new solution (a, b, c) is obviously non-trivial. If $|c'| > 1$ and $|c| > 1$ it is immediately non-trivial. If $|c'| > 1$ but $|c| \leq 1$ we must have that $(c')^p \mid a + b$. This implies $a + b = 0$ or $|a| > 1$ or $|b| > 1$. If $a + b = 0$ then $(a, b) = \pm(1, -1)$ (because $(a, b) = 1$) which implies $c' = 0$ contradicting $|c'| > 1$. Then $|a| > 1$ or $|b| > 1$ and we are done.

■

Proposition 3.2.7 *Let $r \geq 5$ be a prime. The equation*

$$\phi_r(x, y) = 1 \qquad or \qquad \phi_r(x, y) = r$$

admit only the solutions $\pm(1, 0)$, $\pm(0, 1)$, $\pm(1, 1)$ or $\pm(1, -1)$, respectively.

Proof: Recall that $\phi_r(x, y) = \sum_{i=0}^{r-1} (-1)^i x^{r-1-i} y^i$ and suppose (a, b) is a solution of any of the equations in the statement. From the symmetry of ϕ_r and the fact that $r - 1 - i$ and i have the same parity we can suppose that we are in one of three possible cases: (i) $a = 0$ or (ii) $a > 0$ and $b < 0$ or (iii) $a \geq b > 0$.

Case (i): suppose $a = 0$. Replacing on the equations, we have $b^{r-1} = 1$ or $b^{r-1} = r$. The first possibility gives the solutions $\pm(0, 1)$ of the equation $\phi_r(x, y) = 1$ and by symmetry $\pm(1, 0)$. The second is impossible because r is prime > 2.

Case (ii): suppose $a > 0$ and $b < 0$. Then $b = -b_0$, with b_0 positive. We see that $\phi_r(a, b) = \sum_{i=0}^{r-1} a^{r-1-i} b_0^i \geq r$, and it is clear that the equality holds only if $a = 1$ and $b = -1$, corresponding to the solution $(1, -1)$ of the equation $\phi_r(x, y) = r$. We also have $(-1, 1)$ by symmetry.

Case (iii): suppose $a \geq b > 0$. Note that $\phi_r(a, b)$ can be written in the form

$$\phi_r(a, b) = \sum_i (a^{r-1-i} b^i - a^{r-1-(i+1)} b^{(i+1)}) + b^{r-1},$$

where the sum is over the even numbers i satisfying $0 \leq i \leq r-3$. Suppose $a > b$ and observe that

$$a^{r-1-i}b^i - a^{r-1-(i+1)}b^{(i+1)} = a^{r-1-i-1}b^i(a-b) \geq a^{r-1-i-1}b^i \geq 2^{r-1-i-1}.$$

Moreover, $2^{r-1-i-1} \geq 2$ and the equality holds only for $i = r-3$. Thus,

$$\phi_r(a,b) = \sum_i (a^{r-1-i}b^i - a^{r-1-(i+1)}b^{(i+1)}) + b^{r-1} > (r-1)/2 \times 2 + 1 \geq r.$$

This shows that there are no Case (iii) solutions to both equations if $a > b$. Suppose $a = b$, then $\phi_r(a,b) = a^{r-1}$. This can be a solution of $\phi_r(x,y) = 1$ only if $a = b = 1$. It can never be a solution of $\phi_r(x,y) = r$ because r is prime > 2.

■

Corollary 3.2.8 *Let (a,b,c) be a solution to equation* (3.3) *or* (3.4)*. Then (a,b,c) is non-trivial, i.e $|abc| > 1$, if and only if $|c| > 1$.*

Proof: Suppose $|abc| > 1$. Then $|ab| > 1$ or $|c| > 1$. If $|c| > 1$ it is automatic. From Proposition 3.2.7 we see that all solutions with $|c| = 1$ also satisfy $|ab| = 1$, hence, if $|ab| > 1$ we must have $|c| > 1$. The other direction is immediate.

■

Now we will take further the idea of relating different equations, by relating solutions of equations (3.3) and (3.4) to solutions of several equations. Recall that $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ is the maximal totally real subfield of $\mathbb{Q}(\zeta)$ and let h_r^+ be its class number. Let π_r be such that $r\mathcal{O}_{K^+} = (\pi_r)^{(r-1)/2}$. For $r > 5$ a prime, we observe that $r-1 \geq 6$ is even then we can pick three different degree two factors of ϕ_r of the form $f_i = (x + \zeta^{k_i}y)(x + \zeta^{r-k_i}y)$ with coefficients in K^+. We identify this choice of f_i with the triple (k_1, k_2, k_3). Furthermore, we will say that a triple of integers (k_1, k_2, k_3), with $1 \leq k_i \leq r-1$, is *a valid triple* if the corresponding three polynomials f_i are different. Changing the order of the k_i gives us the same set of polynomials. Indeed, without loss of generality we can suppose that $1 \leq k_1 < k_2 < k_3 \leq (r-1)/2$ which implies that there are $\binom{(r-1)/2}{3}$ different valid triples.

Lemma 3.2.9 *Let p be a prime not dividing h_r^+. Suppose there is a non-trivial primitive solution (a,b,c') to $x^r + y^r = Cz^p$ with $C \neq 0$ an integer divisible only by primes $q \neq r$ satisfying $q \not\equiv 1 \pmod{r}$. Pick a valid triple (k_1,k_2,k_3) and let f_1, f_2, f_3 be the corresponding polynomials. Then, there exists a unit $\mu \in \mathcal{O}_{K^+}^\times$ and a solution (a,b,c) in $\mathbb{Z}^2 \times \mathcal{O}_{K^+}$ such that $(a,b) = 1$ (primitive) and $|Norm_{K^+/\mathbb{Q}}(abc)| > 1$ (non-trivial) to*

$$f_1(x,y)f_2(x,y)f_3(x,y) = \mu z^p \quad \text{or} \tag{3.5}$$

$$f_1(x,y)f_2(x,y)f_3(x,y) = \mu\pi_r^3 z^p, \tag{3.6}$$

which satisfies $r \nmid a+b$ in case (3.5) *and $r \mid a+b$ in case* (3.6)*. Moreover:*

- *if $d \mid C$, then $d \mid a+b$;*
- *the primes in K^+ divisors of c are all above primes of $\mathbb{Q}$ that are congruent to 1 (mod r). In particular, neither the primes above 2 nor the primes above r divide c.*

Proof: Suppose that there is a non-trivial primitive solution $(a,b,c') \in \mathbb{Z}^3$ to $x^r+y^r = Cz^p$ and fix a valid triple (k_1,k_2,k_3). Then, by Lemma 3.2.6 there is a non-trivial primitive solution $(a,b,c'') \in \mathbb{Z}^3$ to equation (3.3) or (3.4). By Proposition 3.2.3 we know that the $f_i(a,b)$ are pairwise coprimes outside $\mathfrak{P}_r$. Then since $\mathcal{O}_{K^+}$ is a Dedekind domain we have that: if (a,b,c'') is a solution of (3.3) or (3.4) then $(f_i(a,b)) = \mathcal{I}^p$ or $(f_i(a,b)) = (\pi_r)\mathcal{I}^p$ as ideals in $\mathcal{O}_{K^+}$, respectively. These identities show that the order of $\mathcal{I}$ in the ideal class group of K^+ divides p. Since $p \nmid h_r^+$ we have that $\mathcal{I}$ is principal and we can write $f_i(a,b) = \mu_i c_i^p$ or $f_i(a,b) = \mu_i \pi_r c_i^p$, where $\mu_i, c_i \in \mathcal{O}_{K^+}$ with μ_i an unit and the c_i are pairwise coprime. Thus, by multiplying the f_i, we have transformed the solution (a,b,c'') into a solution (a,b,c) in $\mathbb{Z}^2 \times \mathcal{O}_{K^+}$ of the equation (with coefficients in K^+)

$$f_1(a,b)f_2(a,b)f_3(a,b) = \mu c^p \qquad \text{if } r \nmid a+b \quad \text{or}$$

$$f_1(a,b)f_2(a,b)f_3(a,b) = \mu \pi_r^3 c^p \quad \text{if } r \mid a+b.$$

The conditions $(a,b)=1$, $C \mid a+b$ and the fact that the primes in K^+ dividing c are all above primes of $\mathbb{Q}$ that are congruent to 1 (mod r) follow trivially from the application of Lemma 3.2.6 in this proof.

We are left to show that (a,b,c) is non-trivial. We have $|c''| > 1$ by Corollary 3.2.8 and we have to show that $|Norm_{K^+/\mathbb{Q}}(abc)| > 1$. Let q be a prime dividing c'', hence q is congruent to 1 (mod r), i.e. q splits in $\mathbb{Q}(\zeta)$. Since the factors $a+\zeta^i b$ of $\phi_r(a,b)$ are pairwise coprime, each of them contains a non-trivial prime in $\mathbb{Q}(\zeta)$ above q. Thus, c_i is divisible by some prime, hence (a,b,c) is non-trivial.

■

Corollary 3.2.10 *Let $(a,b,c) \in \mathbb{Z}^2 \times \mathcal{O}_{K^+}$ be a solution to* (3.5) *or* (3.6)*. Then (a,b,c) is non-trivial if and only if $|Norm_{K^+/\mathbb{Q}}(c)| > 1$.*

Proof: Suppose $|Norm_{K^+/\mathbb{Q}}(abc)| > 1$. Then $|ab| > 1$ or $|Norm_{K^+/\mathbb{Q}}(c)| > 1$. In the latter case we are done. Suppose $|ab| > 1$, then by Corollary 3.2.8 there is a prime $q \mid \phi_r(a,b)$ different from r. Since the factors $a+\zeta^i b$ of $\phi_r(a,b)$ are pairwise coprime, each of them contains a non-trivial prime in $\mathbb{Q}(\zeta)$ above q. Thus, any product $(a+\zeta^i b)(a+\zeta^{r-i}b)$ is divisible by some prime. In particular, f_1,f_2,f_3 are divisible by some prime, hence $|Norm_{K^+/\mathbb{Q}}(c)| > 1$. The other direction is immediate.

■

Remark 3.2.11 *From Corollaries* 3.2.8 *and* 3.2.10 *we see that a solution (a,b,c) of* (3.3)*,* (3.4)*,* (3.5) *or* (3.6) *is non-trivial ($|Norm_{K^+/\mathbb{Q}}(abc)| > 1$) if and only if c is divisible by some*

prime. As we will see later the primes dividing c will correspond to multiplicative primes of the Frey curves. Moreover, we will see that they are the primes where level lowering actually happens. We want to keep in mind this way of thinking about non-trivial solutions.

To end this section we now summarize the main idea. As long as $p \nmid h_r^+$, in particular for all $p > h_r^+$, we have related an integer non-trivial primitive solution (a, b, c') of $x^r + y^r = Cz^p$ to a non-trivial primitive solution $(a, b, c) \in \mathbb{Z}^2 \times \mathcal{O}_{K^+}$ of several Diophantine equations not depending on C. That is, equations (3.5) or (3.6) for each valid triple (k_1, k_2, k_3) (hence choice of f_i for $i = 1, 2, 3$).

From now when we talk about solutions (a, b, c) of (3.5) or (3.6) we are always considering solutions in $\mathbb{Z}^2 \times \mathcal{O}_{K^+}$. In the rest of this work we will study these solutions using the modular approach via Hilbert modular forms.

3.2.2 The Frey-Hellegouarch curves

Fix a valid triple (k_1, k_2, k_3). From now on, everytime we will refer to equations (3.5) and (3.6) we are considering them with respect to the fixed triple. We want to attach a Frey curve to a putative primitive solution $(a, b, c) \in \mathbb{Z}^2 \times \mathcal{O}_{K^+}$ to (3.5) or (3.6). Let f_i be the degree two factors of ϕ_r with coefficients in K^+ corresponding to the fixed triple, that is

$$\begin{cases} f_1(x, y) = x^2 + (\zeta^{k_1} + \zeta^{r-k_1})xy + y^2, \\ f_2(x, y) = x^2 + (\zeta^{k_2} + \zeta^{r-k_2})xy + y^2, \\ f_3(x, y) = x^2 + (\zeta^{k_3} + \zeta^{r-k_3})xy + y^2. \end{cases}$$

We are interested in finding a triple (α, β, γ) such that

$$\alpha f_1 + \beta f_2 + \gamma f_3 = 0.$$

We see from the form of the f_i that finding (α, β, γ) is always possible, because it is a solution of a linear system with two equations and three variables. In particular, we choose the solution

$$\begin{cases} \alpha = -(\zeta^{k_2} + \zeta^{r-k_2} - \zeta^{k_3} - \zeta^{r-k_3}), \\ \beta = \zeta^{k_1} + \zeta^{r-k_1} - \zeta^{k_3} - \zeta^{r-k_3}, \\ \gamma = -\zeta^{k_1} - \zeta^{r-k_1} + \zeta^{k_2} + \zeta^{r-k_2}. \end{cases}$$

Finally, given a primitive solution (a, b, c) to equation (3.5) or (3.6) we put

$$A(a, b) = \alpha f_1(a, b), \qquad B(a, b) = \beta f_2(a, b), \qquad C(a, b) = \gamma f_3(a, b),$$

and we attach to (a, b, c) the Frey curves over K^+ with classical form

$$E_{(a,b)} : y^2 = x(x - A(a, b))(x + B(a, b)). \tag{3.7}$$

We want to remark that if we change the valid triple we change the Frey curve attached to a solution of $x^r + y^r = Cz^p$. Actually, we already know that we can find $\binom{(r-1)/2}{3}$ families of Frey curves. Since most of the theory in this chapter holds for any valid triple, we decided not to include the dependence of the curve on (k_1, k_2, k_3) in the notation $E_{(a,b)}$. Whenever we need to change the valid triple it will be made clear in the text.

Suppose that (a, b, c) is a primitive solution to (3.5) or (3.6). The curves $E_{(a,b)}$ have associated the following quantities:

$$\begin{aligned} \Delta(E) &= 2^4(ABC)^2, \\ c_4(E) &= 2^4(AB + BC + AC), \\ c_6(E) &= -2^5(C + 2B)(A + 2B)(2A + B), \\ j(E) &= 2^8\frac{(AB + BC + AC)^3}{(ABC)^2}. \end{aligned}$$

In particular,

$$\Delta(E) = \begin{cases} \mu^2 2^4(\alpha\beta\gamma)^2 c^{2p} & \text{if } r \nmid a + b, \\ \mu^2 2^4(\alpha\beta\gamma)^2 \pi_r^6 c^{2p} & \text{if } r \mid a + b. \end{cases}$$

As expected, c appears to a p-power in the discriminant which is fundamental for the modular approach to work.

Let $\mathfrak{P}$, $\mathfrak{P}_r$ and $\mathfrak{P}_2$ denote a prime in K^+ above p, r and 2, respectively. Denote by $\mathrm{rad}(c)$ the product of the primes dividing c.

Proposition 3.2.12 *Let (a, b, c) be a primitive solution of equation (3.5) or (3.6). The conductor of the curves $E_{(a,b)}$ is of the form*

$$N_E = 2^s \mathfrak{P}_r^t rad(c),$$

where s may be $2, 3$ or 4 and $t = 0$ or 2 if $r \mid a + b$ or $r \nmid a + b$, respectively.

Proof: To the results used in this proof we follow [52]. First note that α, β, γ can be written in the form $\pm\zeta^s(1 - \zeta^t)(1 - \zeta^u)$, where neither t nor u are $\equiv 0 \pmod r$, which means that the only prime dividing $\alpha\beta\gamma$ is $\mathfrak{P}_r$ and $\upsilon_{\mathfrak{P}_r}(\alpha\beta\gamma) = 3$.

Let $\mathfrak{P}$ be a prime in K^+ different from $\mathfrak{P}_r$ and $\mathfrak{P}_2$. Observe that $\upsilon_{\mathfrak{P}}(\Delta(E)) = 2p\upsilon_{\mathfrak{P}}(c)$. Then if $\mathfrak{P} \nmid c$ we have $\upsilon_{\mathfrak{P}}(\Delta) = 0$ and the curve has good reduction. If $\mathfrak{P} \mid c$ then $\upsilon_{\mathfrak{P}}(\Delta) > 0$ and $\mathfrak{P}$ must divide only one among A, B or C (see Proposition 3.2.3). From the form of c_4 it can be seen that $\upsilon_{\mathfrak{P}}(c_4) = 0$ thus E has multiplicative reduction at $\mathfrak{P}$.

Since $(\pi_r) = \mathfrak{P}_r$ we see from the form of $\Delta(E)$ that $\upsilon_{\mathfrak{P}_r}(\Delta) = 6$ or 12 if $r \nmid a + b$ or $r \mid a + b$, respectively. This translate to E bad additive reduction ($\upsilon_{\mathfrak{P}_r}(N_E) = 2$) or good reduction ($\upsilon_{\mathfrak{P}_r}(N_E) = 0$) at $\mathfrak{P}_r$ if $r \nmid a + b$ or $r \mid a + b$, respectively.

Since 2 do not ramifies in $\mathbb{Q}(\zeta)$ we use Table IV in [52]. It is easily seen by from the

shape of Δ, c_4 and c_6 that $\upsilon_{\mathfrak{P}_2}(\Delta) = 4$, $\upsilon_{\mathfrak{P}_2}(c_6) = 5$ and $\upsilon_{\mathfrak{P}_2}(c_4) \geq 4$ for any $\mathfrak{P}_2$ above 2. Then the equation is minimal ($\upsilon_{\mathfrak{P}_2}(\Delta) < 12$) and we check in Table IV [52] for the columns corresponding to the previous valuations and observe that $\upsilon_{\mathfrak{P}_2}(N_E)$ can be $2, 3, 4$ corresponding to Kodaira type II, III or IV.

■

Proposition 3.2.13 *Let (a, b, c) be a primitive solution of equation* (3.5) *or* (3.6) *and $l \neq p$ be a prime in K^+ dividing c. Then, the representation $\bar{\rho}_{E,p}$ attached to the Frey curve $E = E_{(a,b)}$ is unramified at l.*

Proof: l is unramified in K^+ because $l \nmid r$. From $l \mid c$ and Proposition 3.2.12 it follows that l is of multiplicative reduction of E. Since it appears to a p-th power in the discriminant of a minimal model at l of E ($\Delta(E)$) we know by Theorem 1.1.14 that the representation $\bar{\rho}_{E,p}$ will not ramify at l.

■

Corollary 3.2.14 *Let $\bar{\rho}_{E,p}$ be as in the previous proposition. Then, the Artin conductor $N(\bar{\rho}_{E,p})$ is equal to $2^i\mathfrak{P}_r^t$, where i and t are given as in Proposition* 3.2.12.

Proof: Recall that the Artin conductor $N(\bar{\rho}_{E,p})$ is not divisible by primes above p by definition. Also, when reducing $\rho_{E,p}$ to its residual representation $\bar{\rho}_{E,p}$, by the discussion regarding the work of Carayol in the end of section 1.2, the conductor at the bad additive primes do not decrease. Hence, by Propositions 3.2.13 and 3.2.12 we conclude that $N(\bar{\rho}_{E,p}) = 2^i\mathfrak{P}_r^t$.

■

In the next section we will prove the following theorem and a particular case of the conjecture below, but by now we will suppose both to be true.

Theorem 3.2.15 *Suppose that (a, b, c) is a primitive solution to* (3.5) *or* (3.6). *Let $\bar{\rho}_{E,p}$ be the mod p Galois representation attached to $E_{(a,b)}$. Then, there exists a constant $M(r)$ such that if $p > M(r)$ then the representation $\bar{\rho}_{E,p}$ is absolutely irreducible.*

Conjecture 3.2.16 *Suppose that (a, b, c) is a primitive solution to* (3.5) *or* (3.6). *Then, the curves $E_{(a,b)}$ over K^+ are modular.*

For an ideal N of K^+ we denote by $S_2(N)$ the set of Hilbert modular cusp forms of parallel weight 2 and level N. Suppose that (a, b, c) is a primitive solution to (3.5) or (3.6). It follows from modularity that there exists a newform f_0 in $S_2(2^i\mathfrak{P}_r^t\mathrm{rad}(c))$, with $i = 2, 3$ or 4 and $t = 0$ or 2, such that $\rho_{E,p}$ is isomorphic to the p-adic representation attached to f_0, which we denote by $\rho_{f_0,p}$. In this situation, for $p > M(r)$ we have that $\bar{\rho}_{E,p}$ is modular

and irreducible and we can apply the level lowering results for Hilbert modular forms from Jarvis, Rajaei and Fujiwara.

From Corollary 3.2.14 we know that $N(\bar{\rho}_{E,p}) = 2^i\mathfrak{P}_r^t$. We will now apply the level lowering results to show that $\bar{\rho}_{E,p}$ is modular of level $N(\bar{\rho}_{E,p})$. Since K^+ might be of even degree, in order to apply Theorem 3.1.8, we need to add an auxiliary (special or supercuspidal) prime to the level. From [56], section 4, Theorem 5, we can add an auxiliary (special) prime $\mathfrak{q}_0$ that, in particular, satisfies that $\bar{\rho}_{f_0,p}(\mathrm{Frob}_{\mathfrak{q}_0})$ is conjugated to $\bar{\rho}_{f_0,p}(\sigma)$, where σ is complex conjugation. We now apply Theorem 3.1.8 to remove from the level all primes except those above 2, p, the prime $\mathfrak{P}_r$ and $\mathfrak{q}_0$. Now we will remove from the level the primes above p and for that we need $\bar{\rho}_{E,p}|G_{\mathfrak{P}}$ to be finite at all primes $\mathfrak{P} \mid p$. If $\mathfrak{P} \nmid c$ it is of good reduction for E then $\bar{\rho}_{E,p}|G_{\mathfrak{P}}$ is finite by Lemma 1.2.5; if $\mathfrak{P} \mid c$ it is of multiplicative reduction for E and since we have $p \mid \upsilon_{\mathfrak{P}}(\Delta)$ it follows from Lemma 1.2.5 that $\bar{\rho}_{E,p}|G_{\mathfrak{P}}$ is finite. Thus from Theorem 3.1.7 we can remove the primes above p without changing the weight. Finally, from the condition imposed on $\mathfrak{q}_0$ follows that $\mathrm{Nm}(\mathfrak{q}_0) \not\equiv 1 \pmod{p}$ and we can apply Theorem 3.1.6 to remove $\mathfrak{q}_0$ from the level. Then we conclude that there exists a newform f in $S_2(2^i\mathfrak{P}_r^t)$ and a prime $\mathfrak{P} \mid p$ in $\mathbb{Q}_f$ such that its associated residual Galois representation satisfies

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{f_0,p} \sim \bar{\rho}_{f,\mathfrak{P}}. \tag{3.8}$$

As already mentioned, if we show that this congruence can not hold (step (III)) for all the newforms in the corresponding cusp spaces $S_2(2^i\mathfrak{P}_r^t)$ we have proved that our putative non-trivial primitive solution (a, b, c) to (3.5) or (3.6) can not exist hence (3.1) also can not have non-trivial primitive solutions by Lemma 3.2.9. The most common method to contradict the previous isomorphism is to look at the values $a_q(E)$ and $a_q(f)$ and verify that they can not be congruent modulo $\mathfrak{P}$ if p is greater than a constant. However, this method is limited by the existence of trivial solutions. In particular, an intrinsic problem of our method is that for some μ the equations (3.5) and (3.6) have trivial solutions $\pm(1, 0, 1)$, $\pm(0, 1, 1)$, $(1, 1, 1)$ and $(1, -1, 1)$, $(-1, 1, 1)$ that are associated with the Frey curves $E_{(1,0)}$, $E_{(1,1)}$ and $E_{(1,-1)}$, respectively, that do exist. Then we will not be able to eliminate their (conjecturally) associated newforms simply by comparing the values of a_q. However, for suitable values of C the extra condition $C \mid a + b$ will be enough to deal with $E_{(1,0)}$ and $E_{(1,1)}$, but the curve $E_{(1,-1)}$ will survive. To eliminate the newform corresponding to $E_{(1,-1)}$ we need the extra hypothesis $r \nmid a + b$ to achieve a contradiction at the inertia at $\mathfrak{P}_r$. From Proposition 3.2.5 it follows that for a primitive solution (a, b, c) of (3.1) we have $r \nmid a + b \Leftrightarrow r \nmid c$ thus we are limited to solve the equation (3.1) only for first case solutions (see Definition 3.2.1).

Remark 3.2.17 *Our method can be adapted to solve some equations completely, i.e removing the restriction $r \nmid c$. This is the case if we consider the equation $x^{2r} + y^{2r} = Cz^p$ and use the Frey curves $F_{(a,b)} := E_{(a^2,b^2)}$. Since the trivial solutions $(1, -1)$ will correspond to the curve $F_{(1,-1)} = E_{(1,1)}$, in principle, we will be able to eliminate its attached modular form because of the condition $C \mid a + b$. This will be illustrated in the next chapter.*

As we have commented there are computational limitations to the strategy, because the

dimension of K^+ is $(r-1)/2$ and increases with r. In particular, the norm of the ideals (2) and $\mathfrak{P}_r$ will increase and consequently also the norm of the conductor of $E_{(a,b)}$ increases making the dimension of the corresponding space of Hilbert modular cuspforms became very large fast. For example, when $r = 11$ the norm of $2^4\mathfrak{P}_r^2$ is $2^{20}11^2$ and the dimension of $S_2(2^4\mathfrak{P}_r^2)$ is 5406721. Thus, already for small values of r computing the corresponding newspace of Hilbert modular forms of $S_2(2^4\mathfrak{P}_r^2)$ is infeasible.

However, if $r \equiv 1 \pmod 6$ the computational requirements can be reduced. Let $r = 6k+1$ be a prime. The degree of ϕ_r is $6k$ then it admits k factors ϕ_i for $1 \leq i \leq k$ with degree six and coefficients in the totally real subfield of K^+ with degree k, that we denote by K_0. Let σ be the generator of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and let ϕ_1 be the factor of ϕ_r given by

$$\phi_1 = \prod_{i=0}^{5} (x + \sigma^{ik}(\zeta)y).$$

Let also the polynomials f_i be given by

$$\begin{cases} f_1(x,y) = (x+\zeta y)(x+\sigma^{3k}(\zeta)y), \\ f_2(x,y) = (x+\sigma^{2k}(\zeta)y)(x+\sigma^{5k}(\zeta)y), \\ f_3(x,y) = (x+\sigma^{4k}(\zeta)y)(x+\sigma^{k}(\zeta)y). \end{cases}$$

Observe that this choice of polynomials correspond to the valid triple $(1, n_2, n_3)$, where $\zeta^{n_2} = \sigma^{2k}(\zeta)$ and $\zeta^{n_3} = \sigma^{4k}(\zeta)$. Note also that $\phi_1 = f_1 f_2 f_3$ is defined over K_0 hence, in this case, equations (3.5) and (3.6) are defined over K_0. As explained before these factors give rise to the following linear system

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha(\zeta + \sigma^{3k}(\zeta)) + \beta(\sigma^{2k}(\zeta) + \sigma^{5k}(\zeta)) + \gamma(\sigma^{4k}(\zeta) + \sigma^{k}(\zeta)) = 0 \\ \alpha + \beta + \gamma = 0 \end{cases}$$

that obviously has infinitely many solutions. We pick the solution given by

$$\begin{cases} \alpha = -\sigma^{2k}(\zeta) - \sigma^{5k}(\zeta) + \sigma^{4k}(\zeta) + \sigma^{k}(\zeta) \\ \beta = \zeta + \sigma^{3k}(\zeta) - \sigma^{4k}(\zeta) - \sigma^{k}(\zeta) \\ \gamma = \sigma^{2k}(\zeta) + \sigma^{5k}(\zeta) - \zeta - \sigma^{3k}(\zeta) \end{cases}$$

We remark that this choice for (α, β, γ) is the same as before, that is, we could also have obtained it by replacing in the general description the triple (k_1, k_2, k_3) by $(1, n_2, n_3)$. Let $A(a,b) = \alpha f_1(a,b)$, $B(a,b) = \beta f_2(a,b)$, $C(a,b) = \gamma f_3(a,b)$. As before, we have $A+B+C = 0$ then we can consider the Frey curves over K^+ given by

$$E_{(a,b)} : y^2 = x(x - A(a,b))(x + B(a,b)).$$

For the rest of this section the results depend on the specific triple $(1, n_2, n_3)$. Recall that n_2 and n_3 are defined by $\zeta^{n_2} = \sigma^{2k}(\zeta)$ and $\zeta^{n_3} = \sigma^{4k}(\zeta)$.

Proposition 3.2.18 *Let $r = 6k + 1 \geq 7$ be a prime. Fix the triple (k_1, k_2, k_3) to be $(1, n_2, n_3)$. Suppose that (a, b, c) is a primitive solution of (3.5) or (3.6). Then the Frey curves $E_{(a,b)}/K^+$ has a model over K_0.*

Proof: First observe that $\sigma^{2k} \pmod{\sigma^{3k}}$ has order 3 and generates $\mathrm{Gal}(K^+/K_0)$. Since the curves E are defined over K^+ they are invariant under the order 2 element $\sigma^{3k}$and in particular $j(E)$ is invariant under σ^{3k}. Moreover,

$$\sigma^{2k}(\alpha) = \beta, \quad \sigma^{2k}(\beta) = \gamma, \quad \sigma^{2k}(\gamma) = \alpha,$$

and also

$$\sigma^{2k}(f_1) = f_2, \quad \sigma^{2k}(f_2) = f_3, \quad \sigma^{2k}(f_3) = f_1,$$

then

$$\sigma^{2k}(A) = B, \qquad \sigma^{2k}(B) = C, \qquad \sigma^{2k}(C) = A.$$

Since

$$j(E) = 2^8 \frac{(AB + BC + CA)^3}{(ABC)^2}$$

it is clearly invariant under σ^{2k} then the j-invariant actually is in K_0. Now we write $E_{(a,b)}$ in the short Weierstrass form to get a model

$$\begin{cases} E : y^2 = x^3 + a_4 x + a_6, \text{ where} \\ a_4 = -432(AB + BC + CA) \\ a_6 = -1728(2A^3 + 3A^2B - 3AB^2 - 2B^3) \end{cases}$$

Since a_4 is clearly invariant under σ^{2k} and

$$\begin{aligned} a_6 &= -1728(2A^3 + 3A^2B - 3AB^2 - 2B^3) = \\ &= -1728(2(-B - C)^3 + 3(-B - C)^2B - 3(-B - C)B^2 - 2B^3) = \\ &= -1728(2B^3 + 3B^2C - 3BC^2 - 2C^3) = \sigma^{2k}(a_6) \end{aligned}$$

we conclude that the short Weierstrass model is defined over K_0.

■

Let π_2 and π_r denote a prime in K_0 above 2 and r, respectively.

Proposition 3.2.19 *Let $r = 6k + 1 \geq 7$ be a prime. Fix the triple (k_1, k_2, k_3) to be $(1, n_2, n_3)$. Suppose that (a, b, c) is a primitive solution of (3.5) or (3.6). The conductor of the curves $E_{(a,b)}$ over K_0 is of the form*

$$N_E = 2^s \pi_r^2 rad(c),$$

where s may be $2, 3$ or 4.

Proof: Writing a curve in short Weierstrass form changes the values of Δ, c_4 and c_6 by a factor of 6^{12}, 6^4 and 6^6. Since the primes dividing 6 do not ramify in K/K_0 and do not divide c the conductor of E at primes dividing c is the same as before.

Since $\pi_r = \mathfrak{P}_r^3$ in K^+ we see from the third paragraph in the proof of Proposition 3.2.12 that $\upsilon_{\pi_r}(\Delta(E)) = 4$ or 2. Also, $\upsilon_{\pi_r}(c_4(E)) > 0$ and since we are in characteristic ≥ 5 this implies that the equation is minimal and has bad additive reduction with $\upsilon_{\pi_r}(N_E) = 2$.

It easily can be seen that $\upsilon_{\pi_2}(\Delta(E)) = 16$, $\upsilon_{\pi_2}(c_6(E)) = 11$ and $\upsilon_{\pi_2}(c_4(E)) \geq 8$. Table IV in [52] tell us that the equation is not minimal and after a change of variables we have $\upsilon_2(\Delta(E)) = 4$, $\upsilon_{\pi_2}(c_6(E)) = 5$ and $\upsilon_{\pi_2}(c_4(E)) \geq 4$. Now exactly as in the proof of Proposition 3.2.12 we can conclude that $\upsilon_{\pi_2}(N_E)$ may be 2, 3, or 4.

■

The existence of a model over K_0 has advantages. For example, a trivial adaptation of the proof of Theorem 3.2.15 will give us a smaller constant $M(r)$. Also, by arguing exactly as in the proofs of Proposition 3.2.13 and Corollary 3.2.14, where instead of Proposition 3.2.12 we use Proposition 3.2.19, it follows

Proposition 3.2.20 *Let (a, b, c) be a primitive solution of equation* (3.5) *or* (3.6)*. Then,*

1. *If $l \neq p$ is a prime dividing c then the representation $\bar{\rho}_{E,p}$ attached to the Frey curve $E = E_{(a,b)}$ is unramified at l.*
2. *The Artin conductor $N(\bar{\rho}_{E,p})$ is equal to $2^i \pi_r^2$, where i is as in Proposition* 3.2.19*.*

Moreover, assuming modularity of the curves $E_{(a,b)}/K_0$ we can argue exactly as we did over K^+ to apply the results on level lowering. This leads to the computation of Hilbert newforms over K_0 which is a number field of dimension k when *a priori* we were over K^+ of dimension $3k$. In the next chapter we will use this fact to solve equations for $r = 7$ and $r = 13$.

3.3 Modularity of E and Irreducibility of $\bar{\rho}_{E,p}$

Denote by $\rho_{E,p}$ and $\bar{\rho}_{E,p}$ the p-adic and the mod p representations associated with $E_{(a,b)}$. In the discussion in the previous section we postponed two fundamental steps in the modular approach: irreducibility of $\bar{\rho}_{E,p}$ and modularity of the Frey curves (i.e. modularity of $\rho_{E,p}$). The content of this section is devoted to these two steps.

3.3.1 Modularity lifting theorems

We start by recalling important results on modularity and ordinarity lifting from Kisin, Skinner-Wiles, Savitt, Langlands and Tunnel. The definitions and statements below are adapted according to our needs. For their full generality see [68], [69], [41], [8] and [61]. The results in this section will take a main role in the proof of Theorem 3.3.10.

Definition 3.3.1 *Let $\rho : G_F \to GL_2(\bar{\mathbb{Q}}_p)$ be an odd continuous and irreducible representation ramified only at a finite set of primes S and such that $det(\rho) = \epsilon\chi_p^{k-1}$ with ϵ a finite order character and $k > 1$. Let $t \mid p$ be a prime.*

We say that ρ is ordinary at t if $\rho|D_t$ has a rank 1 quotient on which the action of inertia at t is trivial, that is

$$\rho|I_t = \begin{pmatrix} \epsilon'\chi_p^{k-1} & * \\ 0 & 1 \end{pmatrix},$$

where $\epsilon' = \epsilon|I_t$. Moreover, we say that ρ is potentially ordinary at t if the previous condition holds for the restriction of ρ to an open subgroup of D_t.

Furthermore, we say that ρ is nearly-ordinary at t if

$$\rho|D_t = \begin{pmatrix} \psi_1^{(t)} & * \\ 0 & \psi_2^{(t)} \end{pmatrix},$$

with $\psi_2^{(t)}|I_t$ having finite order.

For definitions of (potentially) crystalline and (potentially) Barsotti-Tate representations see [61], [8], section 1.1 of [17] and references there. Later we will need the following result of Savitt that generalizes work of Breuil concerning crystalline ordinary representations.

Theorem 3.3.2 *(Savitt) Let $p > 2$ and $\rho : G_{\mathbb{Q}_p} \to GL_2(\bar{\mathbb{Q}}_p)$ be a potentially Barsotti-Tate Galois representation. Suppose also that $\rho|G_{\mathbb{Q}_p(\zeta_p)}$ is Barsotti-Tate and that $\bar{\rho}$ is reducible. Then ρ is nearly-ordinary. Furthermore, if ρ is Barsotti-Tate then it is ordinary.*

Proof: The first sentence is an application of Theorem 6.11 in [61] as in Theorem 6.1 in [38]. For the last statement: we have ρ nearly-ordinary and Barsotti-Tate (hence crystalline) then by the description of lattices in section 9.1 of [8] we find that we are in case (i). Indeed, from ρ being crystalline it follows that we are in cases (i) or (ii). Moreover, from ρ being nearly-ordinary it follows that we are in the reducible case, hence (i). But in case (i) μ_2 is a unit then ρ is ordinary.

■

We now proceed to the modularity theorems. Let F be a totally real field, S a finite set of finite primes of F and E a finite extension of $\mathbb{Q}_p$. We will denote by $G_{F,S}$ the absolute Galois group of the maximal Galois extension of F unramified outside S. The following

deep theorem is a consequence of the work of Langlands [47] and Tunnell [72]. See also the lectures in [33] for a discussion regarding its proof in the classic case $F = \mathbb{Q}$.

Theorem 3.3.3 *(Langlands-Tunnell) Let $\bar{\rho} : G_F \to GL_2(\mathbb{C})$ be a continuous, irreducible with solvable image in $PGL_2(\mathbb{C})$. Suppose also that $det(\bar{\rho}(c)) = -1$ for all complex conjugations c. Then, there exists a normalized Hilbert eigenform f_1 of parallel weight 1 giving rise to $\bar{\rho}$.*

The following theorem is Corollary 2.1.3 in [41].

Theorem 3.3.4 *(Kisin) Let $p > 2$ and $\rho : G_{F,S} \to GL_2(E)$ be a continuous representation such that $det(\rho) = \epsilon\chi_p$. Suppose that*

(1) *ρ is potentially Barsotti-Tate at each prime $t \mid p$ of F, and if ρ is potentially ordinary at t then $F_t = \mathbb{Q}_p$.*

(2) *$\bar{\rho} \sim \rho_{\bar{f},\lambda}$ for some Hilbert modular form f over F of parallel weight 2.*

(3) *$\bar{\rho}|F(\mu_p)$ is absolutely irreducible, and $[F(\zeta_p) : F] > 2$ if $p = 5$.*

Then $\rho \sim \rho_{f',\lambda}$ for some Hilbert modular form f' over F of parallel weight 2.

Definition 3.3.5 *Let $\bar{\rho} : Gal(\bar{\mathbb{Q}}/F) \to GL_2(\mathbb{F}_p)$ be a Galois representation, and let $\mathfrak{P} \mid p$ be a prime of F. We say that ρ is $D_{\mathfrak{P}}$-distinguished if the semisimplification of the restriction $\bar{\rho}|D_{\mathfrak{P}}$ is isomorphic to $\theta_1 \oplus \theta_2$, with θ_1 and θ_2 distinct characters from $D_{\mathfrak{P}}$ to $\bar{\mathbb{F}}^*$.*

The following two theorems correspond to Theorem 5.1 in [69] and Theorem A in [68], respectively.

Theorem 3.3.6 *(Skinner-Wiles) Let F be a totally real field and $\rho : Gal(\bar{\mathbb{Q}}/F) \to GL_2(\bar{\mathbb{Q}}_p)$ be a continuous odd absolutely irreducible representation ramified only at finitely many primes. Suppose further that $det(\rho) = \epsilon\chi_p^{k-1}$ and*

(1) *ρ is nearly-ordinary at all primes t above p.*

(2) *$\bar{\rho}$ is absolutely irreducible and $D_{\mathfrak{P}}$-distinguished for all primes $t \mid p$.*

(3) *There exists a modular representation $\rho_{f,\lambda}$ nearly-ordinary at all primes above p such that $\bar{\rho}$ and $\bar{\rho}_{f,\lambda}$ are isomorphic.*

Then ρ is modular.

Theorem 3.3.7 *(Skinner-Wiles) Let $p > 2$ and $\rho : Gal(\bar{\mathbb{Q}}/F) \to GL_2(\bar{\mathbb{Q}}_p)$ be a continuous, irreducible and unramified away from a finite number of places of F. Suppose that $\bar{\rho}^{ss}$ is isomorphic to $\chi_1 \oplus \chi_2$. Suppose further that*

(1) *The splitting field* $F(\chi_1/\chi_2)$ *of* χ_1/χ_2 *is abelian over* $\mathbb{Q}$.

(2) $(\chi_1/\chi_2)(z) = -1$ *for each complex conjugation*

(3) $(\chi_1/\chi_2)|D_v \neq 1$ *for each* $v \mid p$

(4) ρ *is potentially ordinary*

(5) $det(\rho) = \epsilon\chi_p^{k-1}$

Then ρ *is modular.*

3.3.2 Modularity of $E_{(a,b)}$

It is known that all elliptic curves over $\mathbb{Q}$ are modular and is expected the same to be true over totally real number fields but there are no complete general results in the latter situation. Thus, in general, we can only conjecture modularity of our Frey curves $E_{(a,b)}$.

Conjecture 3.3.8 *Let* $r > 5$ *be a prime. Let* (k_1, k_2, k_3) *be a valid triple for this* r*. Suppose that* (a, b, c) *is a primitive solution of* (3.5) *or* (3.6)*. Then, the curves* $E_{(a,b)}$ *over* K^+ *or* K_0 *are modular.*

This conjecture holds for specific valid triples. For example, for $r = 7$ there is only one valid triple (up to order) and the corresponding Frey curve is defined over $\mathbb{Q}$ (see section 4.1.1) hence it is modular by the Modularity Theorem; for $r = 13$ and triple $(1, 4, 3)$ it is a consequence of Theorem 3.3.10 below (see section 4.2, in particular Theorem 4.2.3).

The following important consequence of Langlands-Tunnell Theorem is key in the proof of Theorem 3.3.10.

Theorem 3.3.9 *Let* C/F *be an elliptic curve defined over a totally real field* F *and put* $\rho = \rho_{C,3}$*. If* $\bar{\rho}$ *is irreducible then it is modular arising from an Hilbert newform* f *over* F *of parallel weight* 2*.*

Proof: The first step is a consequence of Theorem 3.3.3. Observe that $\bar{\rho} : G_F \to \mathrm{GL}_2(\mathbb{F}_3)$ is totally odd, absolutely irreducible and of solvable image. The discussion after Theorem 5.1 in [76] can be reproduced also over the totally real field F. Indeed, in Lecture I of [33] the details over $\mathbb{Q}$ are given and and with small natural adjustments it directly generalizes to F. Thus there is an Hilbert eigenform f_1 of parallel weight 1 defined over F such that $\bar{\rho} \sim \bar{\rho}_{f_1,\lambda}$, where $\lambda \mid 3$ is a prime in $\bar{\mathbb{Q}}$. This is a known application and can be found, for example, in page 1133 of [30] or in the proof of Theorem 3.3.1 in [2].

From Lemma 1.4.2 in [75] we know there exists a normalized Hilbert modular form θ of parallel weight 2^{i+1} for some integer $i \geq 0$ such that $\theta \equiv 1 \pmod 3$. Consider the product θf_1 of parallel weight $w = 2^{i+1} + 1$. Since $\theta f_1 \equiv f_1 \pmod 3$ we have that θf_1 is a modulo 3

eigenform and by the Deligne-Serre Lemma (see [23], Lemma 6.11) we can find an eigenform f_w of parallel weight w such that $\bar{\rho} \sim \bar{\rho}_{f_w,\lambda}$. Finally, from the comments preceding corollary 2.12 in [12] it follows that there is a Hilbert eigenform f_2 of parallel weight 2 (and level not necessary prime to 3) such that $\bar{\rho} \sim \bar{\rho}_{f_2,\lambda}$ for a prime λ above 3. We take $f = f_2$.

■

Theorem 3.3.10 *Let F be a totally real abelian number field and C and elliptic curve defined over F. Suppose that 3 splits completely in F and C has good reduction at the primes above 3. Then C is modular.*

Proof: Let $\bar{\rho} = \bar{\rho}_{C,3}$ be as before. Observe that $\bar{\rho}$, when irreducible, is modular by Theorem 3.3.9. We now divide the proof into three cases:

(1) Suppose that $\bar{\rho}$ and $\bar{\rho}|G_{F(\sqrt{-3})}$ are both abs. irreducible. Here we will apply Theorem 3.3.4. Condition (1) holds because C has good reduction at the primes above 3 and 3 splits in F. Theorem 3.3.9 guarantees condition (2) and (3) holds by hypothesis. Then ρ is modular.

(2) Suppose that $\bar{\rho}$ is abs. irreducible and $\bar{\rho}|G_{F(\sqrt{-3})}$ abs. reducible. This means that the image of $\mathbb{P}(\bar{\rho})$ is Dihedral. Namely, that the image of $\bar{\rho}$ is contained in the normalizer N of a Cartan subgroup C_0 of $GL_2(\bar{\mathbb{F}}_3)$ but not contained in C_0. Moreover, the restriction to $F(\sqrt{-3})$ of our representation has its image inside C_0. Thus, the composition of $\bar{\rho}$ with the quotient N/C_0,

$$\mathrm{Gal}(\bar{\mathbb{Q}}/F) \to N \to N/C_0, \tag{3.9}$$

gives the quadratic character of $F(\sqrt{-3})/F$ which ramifies at 3 because 3 is unramified in F.

Let t be a prime in F above 3. Since C has good reduction at t and 3 splits in F the restriction of the residual representation $\bar{\rho}$ to the inertia subgroup I_t has only two possibilities

$$\bar{\rho}|I_t = \begin{pmatrix} \bar{\chi} & * \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \psi_2 & 0 \\ 0 & \psi_2^3 \end{pmatrix}, \tag{3.10}$$

where χ is the 3-adic cyclotomic character and ψ_2 is a fundamental character of level 2.

If we suppose that $\bar{\rho}|I_t$ acts through level 2 fundamental characters, the image of I_t by $\mathbb{P}(\bar{\rho})$ gives a cyclic group of order $4 > 2$, thus it has to be contained in $\mathbb{P}(C_0)$ (if it not contained in $\mathbb{P}(C_0)$ and has order 4 it must be isomorphic to $C_2 \times C_2$). But this implies that the quadratic character defined by composition (3.9) should be unramified at 3, contradicting the fact that this character corresponds to $F(\sqrt{-3})$. Thus we can assume that we are in the first case, that is, $\bar{\rho}|I_t$ is reducible.

The previous holds for all primes $t \mid 3$ hence we can apply Lemma 3.3.11 below to $\bar{\rho}$. Let ψ and f_2 be given by applying Lemma 3.3.11 to $\bar{\rho}$. Let ψ_0 be a finite order lifting

of ψ satisfying $\overline{\rho \otimes \psi_0} = \bar{\rho} \otimes \psi$. Note that $\rho_{f_2,\lambda}$ is a nearly-ordinary lifting of $\bar{\rho} \otimes \psi$. Since ρ is Barsotti-Tate (C has good reduction at all $t \mid 3$) then $\rho|D_t$ is ordinary for all t by Theorem 3.3.2. Then $\rho \otimes \psi_0$ satisfy all the conditions of Theorem 3.3.6. Thus $\rho \otimes \psi_0$ is modular hence ρ is also modular.

(3) Suppose that $\bar{\rho}$ is abs. reducible. We want to apply Theorem 3.3.7. Since the representation is totally odd and F is totally real $\bar{\rho}$ is reducible if and only if it is abs. reducible by Proposition 1.1.12, hence reducibility of $\bar{\rho}$ must take place over $\mathbb{F}_3$. Using this, together with C having good reduction at $t \mid 3$, we restrict $\bar{\rho}$ to I_t, we see that the case of the fundamental characters of level 2 in (3.10) can not occur. Thus we have $\bar{\rho}^{ss} = \chi_1 \oplus \chi_2$, where $\chi_1 = \psi\bar{\chi}$, $\chi_2 = \psi^{-1}$ where $\bar{\chi}$ is the mod 3 cyclotomic character and ψ is ramified only at primes dividing the conductor of E. Note also that ψ must be quadratic because $\mathbb{F}_3^*$ has only two elements. Then $\chi_1/\chi_2 = \psi^2\bar{\chi} = \bar{\chi}$ and conditions (2) and (3) are satisfied. Moreover, $\rho|D_t$ is Barsotti-Tate (C has good reduction at t) then by Theorem 3.3.2 we conclude that $\rho|D_t$ is ordinary for all t, which establishes condition (4). Finally, the extension $F(\chi_1/\chi_2) = F(\sqrt{-3})$ of $\mathbb{Q}$ is abelian because F and $\mathbb{Q}(\sqrt{-3})$ are both abelian. This establishes condition (1) and condition (5) holds because ρ arises from an elliptic curve. Thus by Theorem 3.3.7 we conclude that ρ is modular.

■

Lemma 3.3.11 *Let C and F be has in the Theorem* 3.3.10. *Suppose also that for all $t \mid 3$ we have that $\bar{\rho} = \bar{\rho}_{C,3}$ satisfies*

$$\bar{\rho}|I_t = \begin{pmatrix} \bar{\chi} & * \\ 0 & 1 \end{pmatrix}.$$

Suppose further that $\bar{\rho}$ is modular. Then, there is a character ψ of G_F of finite order and a Hilbert modular form f_2 over F of parallel weight 2 such that $\bar{\rho} \otimes \psi \sim \bar{\rho}_{f_2,\lambda}$ for some prime $\lambda \mid 3$. Furthermore, the level N of f_2 divides $\mathfrak{n}3$ for some $\mathfrak{n}$ prime to 3. Moreover, for each $t \mid 3$, f_2 is ordinary or nearly-ordinary at t if $t \nmid N$ or $t \mid N$, respectively.

Proof: From the comments preceding Corollary 2.12 in [12] (also used in the proof of Theorem 3.3.9) it follows that there is a character ψ of finite order and a Hilbert eigenform f_2 of parallel weight 2 such that $\bar{\rho} \otimes \psi \sim \bar{\rho}_{f_2,\lambda}$ for a prime λ above 3. Moreover, the level N of f_2 divides $\mathfrak{n}3$ with 3 and $\mathfrak{n}$ coprime.

Let $t \mid 3$ be a prime and recall that 3 splits in F. We now divide into two cases:

1) Suppose that $t \nmid N$. From f_2 being of parallel weight 2 and 3 unramified in F it follows that $\rho_{f_2,\lambda}|D_t$ is Barsotti-Tate. Since $\bar{\rho}_{f_2,\lambda}|D_t \equiv (\bar{\rho} \otimes \psi)|D_t$ is residually reducible we apply Theorem 3.3.2 to conclude that $\rho_{f_2,\lambda}|D_t$ is ordinary.

2) Suppose that $t \mid N$. We know that in this case t strictly divides N, hence we have two cases: f_2 is Steinberg or principal series at t.

If f_2 is Steinberg at t then $\rho_{f_2,\lambda}|D_t$ is semi-stable non crystalline (see [60], Theorem 1), hence we are in case (iii) of section 9.1 in [8], then $\rho_{f_2,\lambda}$ is ordinary at t.

If f_2 is a principal series of conductor t at t then $\rho_{f_2,\lambda}|D_t$ is potentially Barsotti-Tate and Barsotti-Tate over $\mathbb{Q}_3(\zeta_3)$. From $\bar{\rho}\otimes\psi \sim \bar{\rho}_{f_2,\lambda}$ follows that $\bar{\rho}_{f_2,\lambda}|D_t$ is reducible and by Theorem 3.3.2 $\rho_{f_2,\lambda}|D_t$ is nearly-ordinary at t. The first sentence in the paragraph follows from Theorem 1 in [60] if $[F:\mathbb{Q}]$ is odd and from Lemma 2.9 in [12] followed by Theorem 1 in [60] if $[F:\mathbb{Q}]$ is even.

■

We will now comment on the proof of the general case. To achieve modularity of the Frey curves for all values of r and all valid triples we need Theorem 3.3.10 to hold without the splitting hypothesis on 3. Above we divided the proof into 3 cases: (i) $\bar{\rho}_{E,3}$ and $\bar{\rho}_{E,3}|G_{F(\sqrt{-3})}$ both abs. irreducible; (ii) $\bar{\rho}_{E,3}$ abs. irreducible and $\bar{\rho}_{E,3}|G_{F(\sqrt{-3})}$ reducible; (iii) $\bar{\rho}_{E,3}$ reducible. When trying to mimic the proof for the general case we will have trouble due to the fact that 3 is not necessarily split in K^+, because in that case we can not guarantee the existence of a nearly-ordinary lifting of $\bar{\rho}_{E,3}$ (in the residually ordinary case) by means of Savitt's results. In section 6 of [1] the authors prove modularity lifting without assuming ordinarity at specific places. Unfortunately, the results there are limited for the case $p=3$. However, in a mail conversation with T. Gee we have learned that a generalization of the theorems there to $p=3$ (possibly with some additional restrictions on the image of the mod p Galois representation) should follow from current techniques. In this scenario we can expect the curves $E_{(a,b)}$ to be proven modular in case (i), where we apply this more general result. And if the curve has ordinary good reduction at all primes above 3 also in case (iii), where modularity follows from an application of Theorem 3.3.6. With these observations in mind we may be able to achieve modularity for particular values of r. A possible way is to first check if $\bar{\rho}_{E,3}$ is abs. irreducible, for example via Proposition 3.3.15, to conclude that we are in case (i) or (ii). Then by computing the 3-division polynomial and verifying that it is irreducible over $K^+(\sqrt{-3})$ (or $K_0(\sqrt{-3})$) we conclude that we are in case (i). Alternatively, if we can only prove that we are not in case (ii) modularity also follows if we have that the Frey curves are ordinary at all primes above 3. This can be seen by computing all the possible values $a_{\mathfrak{P}_3}(E_{(a,b)})$ for all $(a,b)\neq(0,0)$ in $\mathbb{F}^2$ where $\mathbb{F}$ is the residual field at $\mathfrak{P}_3$ and checking that $3 \mid a_{\mathfrak{P}_3}$ never happens.

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

In this section we are concerned with the irreducibility of $\bar{\rho}_{E,p}$ that is fundamental ingredient for applying level lowering theorems. We will achieve this objective by proving a more general statement regarding elliptic curves over totally real fields.

Theorem 3.3.12 *Let F be a totally real number field and C/F be an elliptic curve with conductor N_E. Let A be the factor of N_E corresponding to the additive primes. Suppose further that $\mathfrak{q}\nmid N_C$ is a fixed prime of good reduction. Then, there exist an explicit constant $M(F,A,\mathfrak{q})$ such that, if*

1. *p is odd and unramified in F;*

2. *all primes $\mathfrak{p} \mid p$ are of semistable reduction for C;*

3. *$p > M(F, A, \mathfrak{q})$*

Then, the representation $\bar{\rho}_{C,p}$ is absolutely irreducible.

Proof: Let p be a prime satisfying 1. and 2. in the statement of the theorem. Since $\bar{\rho}_{C,p}$ is totally odd and F is totally real $\bar{\rho}_{C,p}$ is absolutely reducible if and only if it is reducible (Proposition 1.1.12). Suppose that $\bar{\rho}_{C,p}$ is abs. reducible. In the rest of this proof we will first determine $M(F, A, \mathfrak{q})$ and then derive a contradiction with $p > M(F, A, \mathfrak{q})$.

Let $\mathfrak{P}$ be a prime above p hence it is of good or multiplicative reduction for C. In sections 1.11 and 1.12 in [63] Serre describers the possibilities for $\bar{\rho}_{C,p}|I_{\mathfrak{p}}$. From that description and since $\bar{\rho}_{C,p}$ must be reducible over $\mathbb{F}_p$, by restricting $\bar{\rho}_{C,p}$ to $I_{\mathfrak{P}}$ we see that the fundamental characters of level ≥ 2 can not occur. Hence $\bar{\rho}_{C,p}$ must have the form

$$\bar{\rho}_{C,p} = \begin{pmatrix} \epsilon^{-1}\bar{\chi}_p & * \\ 0 & \epsilon \end{pmatrix}, \tag{3.11}$$

where $\bar{\chi}_p$ is the mod p cyclotomic character (restricted to G_F) and ϵ is a character of G_F (depending on p) unramified at all $\mathfrak{P} \mid p$ with values in $\mathbb{F}_p^*$.

The Artin conductor of $\bar{\rho}_{C,p}$ is a factor of N_E. The image via $\bar{\rho}_{C,p}$ of the inertia at semistable primes not dividing p is of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ then the conductor of ϵ contains only bad additive primes. Let A_0 be the factor of A such that A_0^2 is the maximal square dividing A. Let c denote the conductor of ϵ and ϵ^{-1} (they are the same), we have $c \mid A_0$. The finite order characters of G_F with conductor dividing A_0 are in correspondence with the characters of a finite group $H = H(F, A)$. Moreover, H is a subgroup of $(\mathcal{O}_F/A_0)^*$. The group of characters of H is dual of H then, in particular, ϵ has order dividing the cardinality of H.

Let $\mathfrak{q} \nmid N_E$ be the fixed prime of good reduction and q^f the order of its residue field. Since C has good reduction at $\mathfrak{q}$ by taking traces on equality (3.11) we get

$$a_{\mathfrak{q}}(C) \equiv \epsilon(\mathrm{Frob}_{\mathfrak{q}}) + q^f \epsilon^{-1}(\mathrm{Frob}_{\mathfrak{q}}) \qquad (\text{mod p}),$$

which implies that $\epsilon(\mathrm{Frob}_{\mathfrak{q}})$ satisfies the polynomial $q_1 := x^2 - a_{\mathfrak{q}}x + q^f \pmod p$. Note that $\epsilon(\mathrm{Frob}_{\mathfrak{q}})$ is also a root of the polynomial $q_2 := x^{|H|} - 1 \pmod p$. Let $\zeta = \zeta_{|H|}$ be a primitive

$|H(F,A)|$-th root of unity and we have the resultant of q_1 and q_2 given by

$$\begin{aligned}\mathrm{res}(q_1,q_2) &= \prod_{i=1}^{|H|}\left(\frac{a_{\mathfrak{q}}+\sqrt{a_{\mathfrak{q}}^2-4q^f}}{2}-\zeta^i\right)\left(\frac{a_{\mathfrak{q}}-\sqrt{a_{\mathfrak{q}}^2-4q^f}}{2}-\zeta^i\right)\\ &= \prod_{i=1}^{|H|}(\zeta^{2i}-a_{\mathfrak{q}}\zeta^i+q^f)\end{aligned}$$

Since $a_{\mathfrak{q}}$ is an integer such that $|a_{\mathfrak{q}}|\leq 2\sqrt{q^f}$ we have

$$|\mathrm{res}(q_1,q_2)|\leq\prod_{i=1}^{|H|}(|\zeta|^{2i}+|a_{\mathfrak{q}}||\zeta|^i+q^f)\leq\prod_{i=1}^{|H|}(1+2\sqrt{q^f}\times 1+q^f)=(1+2\sqrt{q^f}+q^f)^{|H|}$$

We now take $M(F,A,\mathfrak{q})=(1+2\sqrt{q^f}+q^f)^{|H(F,A)|}=(1+\sqrt{q^f})^{2|H(F,A)|}$.

Now note that all the roots of q_2 have absolute value 1 and those of q_1 have absolute value equal to $\sqrt{q^f}$ (see [66], Chapter V, section 2). On one hand, q_1 and q_2 have integer coefficients and no common roots hence $\mathrm{res}(q_1,q_2)$ is a non-zero integer. On the other hand, $\epsilon(\mathrm{Frob}_{\mathfrak{q}})$ is a common root of the $q_i \pmod p$ then $\mathrm{res}(q_1,q_2)\equiv 0 \pmod p$. This is impossible if $p>M(F,A,\mathfrak{q})$.

■

Recall that we have fixed r as the exponent on the left-hand side of the equation (3.1). A major ingredient of our argument is to guarantee irreducibility of the representations $\bar{\rho}_{E,p}$ attached to our Frey curves $E=E_{(a,b)}$. That is the content of the following theorem.

Theorem 3.3.13 *Let $(a,b,c)\in\mathbb{Z}^2\times\mathcal{O}_{K^+}$ be a primitive solution of* (3.5) *or* (3.6)*. There exists a constant $M(r)$ such that, if $p>M(r)$ then the representation $\bar{\rho}_{E,p}$ is absolutely irreducible.*

Proof: In the previous proof we let $F=K^+$, $C=E_{(a,b)}$; From Proposition 3.2.12 we see that we can also take $A=\mathfrak{P}_2^4\mathfrak{P}_r^2$ (hence $A_0=\mathfrak{P}_2^2\mathfrak{P}_r$) and $\mathfrak{q}=\mathfrak{P}_3$ (a prime above 3) with residue field of order $3^{f(r)}$. This gives us that F, A and $3^{f(r)}$ only depend on r and we denote $M(F,A,\mathfrak{q})$ by $M(r)$. Now, if $p>M(r)$ then $p>r$ and conditions 1. and 2. on the previous theorem are automatically satisfied, because of our specific F and C. Then we conclude $\bar{\rho}_{E,p}$ is irreducible for $p>M(r)$ by the previous theorem.

■

For proving the previous theorem we used little information about our specific Frey curves. Actually, by using more information about them we will now prove a much better result in some cases (Theorem 3.3.15).

Theorem 3.3.14 *Let F be a number field and $\mathfrak{P}_2\mid 2$ a prime in F with inertial degree $f=f(\mathfrak{P}_2/2)$. Let C/F be an elliptic curve with potentially good reduction at $\mathfrak{P}_2$ and define*

$\Phi_{\mathfrak{P}_2}$ *as in the introduction of* [43]. *Then, if* $|\Phi_{\mathfrak{P}_2}|$ *does not divide* $2^{nf}(2^f-1)$ *for all* $n \geq 0$ *the representation* $\bar{\rho}_{C,p}$ *is irreducible for all* $p \geq 3$.

Proof: This theorem is just a particular case of Proposition 3.3 in [4], where we are considering $\mathfrak{q} = \mathfrak{P}_2$.

■

Recall that $K^+ = \mathbb{Q}(\zeta_r + \zeta_r^{-1})/\mathbb{Q}$ is Galois then inertial degree $f(r) = f(\mathfrak{P}_2/2)$ is the same for all primes $\mathfrak{P}_2$ above 2.

Theorem 3.3.15 *Let* r *be such that the inertial degree* $f(r) = f(\mathfrak{P}_2/2)$ *in* K^+ *is odd. Let* $(a,b,c) \in \mathbb{Z}^2 \times \mathcal{O}_{K^+}$ *be a primitive solution of* (3.5) *or* (3.6) *for this fixed* r. *Then* $\bar{\rho}_{E,p}$ *is irreducible for all primes* $p \geq 3$.

Proof: It is clear from the expression of $j(E)$ that $\upsilon_{\mathfrak{P}_2}(j(E)) \geq 0$ then E has potentially good reduction at $\mathfrak{P}_2$. Also, $\upsilon_{\mathfrak{P}_2}(\Delta) = 4 \not\equiv 0 \pmod 3$, where Δ is minimal at $\mathfrak{P}_2$, then we are in case (ii) of Theorem 3 in [43]. Then, from the same Theorem 3 we conclude $|\Phi_{\mathfrak{P}_2}| = 3, 6, 24$. Moreover, $2^{nf}(2^f-1)$ is divisible by 3 only if f is even. Since we have $f(r)$ odd we apply Theorem 3.3.14 to conclude that $\bar{\rho}_{E,p}$ is irreducible for all primes $p \geq 3$.

■

Chapter 4

The cases $r = 7$, $r = 13$ and further examples.

In this chapter we will particularize the strategy in Chapter 3 to solve equations for $r = 7$ and $r = 13$. Then, we will end by giving examples of Frey curves generated by our method for $r = 11, 17, 19$.

4.1 The equation $x^7 + y^7 = Cz^p$

We will prove the following theorem

Theorem 4.1.1 *Let $d = 2^{s_0}3^{s_1}5^{s_2}$ and γ be an integer only divisible by primes $l \not\equiv 1, 0 \pmod 7$. Then, if $p \geq 17$ we have that*

(*I*) *The equation $x^7+y^7 = d\gamma z^p$ has no non-trivial first case solutions if (s_0, s_1, s_2) satisfies any of the following three conditions $(\geq 2, \geq 0, \geq 0)$, $(= 1, \geq 1, \geq 0)$ or $(= 0, \geq 0, \geq 1)$.*

(*II*) *The equation $x^{14} + y^{14} = d\gamma z^p$ has no non-trivial primitive solutions if $s_1 > 0$ or $s_2 > 0$ or $s_0 \geq 2$.*

We will start by proving (I) by following the strategy delineated in the previous chapter. First note that $7 = 6k+1$ for $k = 1$ then we are in a case of less computational requirements and K_0 has degree 1, that is $K_0 = \mathbb{Q}$.

Let $(a, b, c') \in \mathbb{Z}^3$ be a non-trivial primitive solution to the equation

$$x^7 + y^7 = (x + y)\phi_7(x, y) = d\gamma z^p. \tag{4.1}$$

Note that ϕ_7 is of degree 6 then the only factor of ϕ_7 defined over $K_0 = \mathbb{Q}$ is ϕ_7. Then, in the notation of the previous chapter $\phi_1 = \phi_7 = f_1 f_2 f_3$. From Lemma 3.2.9 there must exists a non-trivial primitive solution (a, b, c) in $\mathbb{Z}^3$ to

$$f_1(x, y)f_2(x, y)f_3(x, y) = z^p, \tag{4.2}$$

with $d\gamma \mid a+b$ and $7 \nmid a+b$ or to

$$f_1(x,y)f_2(x,y)f_3(x,y) = 7z^p \tag{4.3}$$

with $d\gamma \mid a+b$ and $7 \mid a+b$, where in both cases c is only divisible by primes congruent to 1 modulo 7. Even though $d\gamma \mid a+b$, it will became clear in the sequel that for the proof of Theorem 4.1.1 we will only need $d \mid a+b$.

We now construct the Frey curves attached to a primitive solution (a,b,c) of (4.2) or (4.3). Let $\zeta = \zeta_7$ be a primitive 7-th root of unity. Following the construction in the previous section we get $\phi_1 = f_1 f_2 f_3$, where the f_i correspond to the valid triple $(1,4,5)$, that is,

$$\begin{aligned} f_1(x,y) &= x^2 + (\zeta + \zeta^6)xy + y^2 \\ f_2(x,y) &= x^2 + (\zeta^4 + \zeta^3)xy + y^2 \\ f_3(x,y) &= x^2 + (\zeta^5 + \zeta^2)xy + y^2 \end{aligned} .$$

and we find a triple (α,β,γ) such that $\alpha f_1 + \beta f_2 + \gamma f_3 = 0$ given by

$$\begin{cases} \alpha = \zeta^5 - \zeta^4 - \zeta^3 + \zeta^2 \\ \beta = -2\zeta^5 - \zeta^4 - \zeta^3 - 2\zeta^2 - 1 \\ \gamma = \zeta^5 + 2\zeta^4 + 2\zeta^3 + c^2 + 1. \end{cases} .$$

This results in the Frey curves with short Weierstrass model $E_{(a,b)} : y^2 = x^3 + a_4 x + a_6$ defined over $\mathbb{Q}$, where

$$\begin{cases} a_4 = -3024(a^4 - a^3b + 3a^2b^2 - ab^3 + b^4) \\ a_6 = 12096(a^6 - 15a^5b + 15a^4b^2 - 29a^3b^3 + 15a^2b^4 - 15ab^5 + b^6). \end{cases}$$

These curves were already known to Kraus (in [46] he gives a Frey curve with the same short Weierstrass model of ours) and Dahmen also found a twist of them with a different method in [18]. Since $\alpha\beta\gamma = -7$ the discriminant is of the form

$$\Delta(E) = 2^{16}3^{12}7^{2+s}c^2, \tag{4.4}$$

where $s = 0$ or $s = 2$ if (a,b,c) is a solution to (4.2) or (4.3), respectively.

Proposition 4.1.2 *Let (a,b,c) be a primitive solution of* (4.2) *or* (4.3)*. Then, the curves $E_{(a,b)}$ have conductor given by*

$$N_E = \begin{cases} 2^2 7^2 rad(c) \text{ or } 2^3 7^2 rad(c) & \text{if } 2 \nmid a+b \\ 2^4 7^2 rad(c) & \text{if } 2 \parallel a+b \\ 2^3 7^2 rad(c) & \text{if } 4 \mid a+b \end{cases}$$

Moreover, if $2 \nmid a+b$ we can suppose that a is even and the conductor is

$$N_E = \begin{cases} 2^2 7^2 rad(c) & \text{if } 4 \mid a \\ 2^3 7^2 rad(c) & \text{if } 4 \nmid a \end{cases}$$

Proof: From Proposition 3.2.19 we know the set of possible values for the conductor. With the help of SAGE we compute the values of the conductor for all pairs (a, b) mod 2^6 and observe how they relate to $a + b$.

■

From Proposition 3.2.20 we have that $N(\bar{\rho}_{E,p})$ is $2^s 7^2$, where $s = 2, 3$ or 4. Lemma 1.2.5 guarantees that $\bar{\rho}_{E,p}$ is finite at p. For a non-trivial primitive solution (a, b, c) of (4.2) or (4.3) there exists a prime greater than six and dividing c, i.e. of multiplicative reduction for $E_{(a,b)}$. Then if $p \geq 17$ we have that $\bar{\rho}_{E,p}$ is absolutely irreducible (see Theorem 22 in [18]). Let $S_2(M)$ denote the set of cusp forms of weight 2, trivial nebentypus and level M. By Serre's conjecture there must exist a newform $f \in S_2(2^s 7^2)$ with $s = 2, 3$ or 4 and a prime $\mathfrak{P} \mid p$ in $\bar{\mathbb{Q}}$ such that

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}. \tag{4.5}$$

To finish the argument we need to contradict (4.5). Using SAGE software we compute the newforms in $S_2(2^s 7^2)$ with $s = 2, 3$ or 4 and we divide them into two sets

S1: Newforms with $\mathbb{Q}_f = \mathbb{Q}$

S2: Newforms such that $\mathbb{Q}$ is strictly contained in $\mathbb{Q}_f$

Now we will look for a contradiction to (4.5) for each newform in both sets, starting with S1. For each pair (a, b) mod l with $l \in \{3, 5, 11, 13, 17, 19, 23\}$ we computed with SAGE all the possible values $a_l(E)$ for our Frey curves $E = E_{(a,b)}$:

$$\begin{cases} a_3(E) & \in \{-1, 3\}, \\ a_5(E) & \in \{-3, -1, 1, 3\}, \\ a_{11}(E) & \in \{-5, -3, 1, 3\}, \\ a_{13}(E) & \in \{-6, -2, 2, 6\}, \\ a_{17}(E) & \in \{-5, -3, 1, 3, 5\}, \\ a_{19}(E) & \in \{-7, -5, 1, 5, 7\}, \\ a_{23}(E) & \in \{-9, -7, -5, -1, 1, 3\} \end{cases}$$

Furthermore, we also see that

$$a_l(E_{(a,b)}) = -1 \quad \text{if} \quad l = 3 \text{ or } 5 \quad \text{and} \quad l \mid a + b. \tag{4.6}$$

Given a newform f in S1 we want to find a prime l such that $a_l(f)$ is not in the corresponding set above, because this will give a contradiction if p is large enough. Indeed, as

long as $p > 7$, by comparing the coefficients of the newforms in S1 against the values in the previous sets we find a contradiction to the isomorphism (4.5) for all f in S1 except for the newforms corresponding to the curves $E_{(0,1)}$, $E_{(1,-1)}$ and $E_{(1,1)}$. These three forms were expected to survive since $(0,1,1)$ and $(1,1,1)$ are solutions of (4.2) and $(1,-1,1)$ is a solution of (4.3). Since these curves have no complex multiplication in order to eliminate them we need to use the information $d \mid a+b$. By Proposition 4.1.2 we see that if (s_0, s_1, s_2) satisfies the conditions $(\geq 0, \geq 0, \geq 1)$, $(= 1, \geq 1, \geq 0)$ or $(\geq 2, \geq 0, \geq 0)$ to finish the proof we have to eliminate $\{E_{(0,1)},\ E_{(1,-1)},\ E_{(1,1)}\}$, $\{E_{(1,-1)},\ E_{(1,1)}\}$ or $E_{(1,-1)}$, respectively. Observing that

$$(a_3(E_{(0,1)}), a_3(E_{(1,-1)}), a_3(E_{(1,1)})) = (-1,-1,3)$$

and

$$(a_5(E_{(0,1)}), a_5(E_{(1,-1)}), a_5(E_{(1,1)})) = (-3,-1,1)$$

we see that the conditions in (s_0, s_1, s_2) together with (4.6) are enough to deal with the newforms associated with $E_{(0,1)}$ and $E_{(1,1)}$ but not with $E_{(1,-1)}$. Recall that this was expected, because $d \mid (1 + (-1)) = 0$.

To eliminate the newform corresponding to $E_{(1,-1)}$ we will use the inertia at 7 by following Kraus [43]. Let $C/\mathbb{Q}_7$ be an elliptic curve and $\Phi_7(C)$ be the Galois group of the extension (of the maximal unramified extension of $\mathbb{Q}_7$) where C acquire good reduction at 7. From Proposition 1 in [43] we see that

$$|\Phi_7(C)| = \text{ denominator of } (\frac{\upsilon_7(\Delta_{\min}(C))}{12}),$$

and by formula (4.4) we find that $|\Phi_7(E_{(a,b)})| = 3$ or 6, if $7 \mid a+b$ or $7 \nmid a+b$, respectively. In particular $|\Phi_7(E_{(1,-1)})| = 3$ and (4.5) can not hold if $7 \nmid a+b$, because the inertia at 7 will not match if $p > 7$. This eliminates all the newforms in S1 if our putative solution (a,b,c) is a non-trivial primitive first case solution (see Definition 3.2.1).

Now suppose that (4.5) holds for some f in S2 then the congruence

$$a_3(E) \equiv c_3(f) \pmod{\mathfrak{P}} \tag{4.7}$$

must hold, for some newform $f = q + \sum_{n\geq 2} c_n q^n$ in S2 and a prime $\mathfrak{P}$ in $\bar{\mathbb{Q}}$ above p. This is not possible if $p > 7$. Indeed, for all newforms in S2 the minimal polynomial of the Fourier coefficient c_3 is $x^2 - 2$ or $x^2 - 8$ then, for example, in the latter case we must have

$$0 \equiv c_3^2 - 8 \equiv a_3^2 - 8 \pmod{p}.$$

Since our curves verify $a_3 \in \{-1, 3\}$ the previous congruence implies that $0 \equiv -7, 1 \pmod{p}$ which is impossible if $p > 7$. The same holds with the other minimal polynomial and this concludes the proof of part (I) of Theorem 4.1.1.

■

We will now prove part (II). Recall that $d = 2^{s_0}3^{s_1}5^{s_3}$ and suppose that (a, b, c_0) is a non-trivial primitive solution to $x^{14} + y^{14} = dz^p$. Observe that we have the factorization

$$a^{14} + b^{14} = (a^2 + b^2)\phi_7(a^2, b^2) = dc_0^p$$

and also that $d \mid a^2 + b^2$. By looking modulo 3 and 4 we find that $a^2 + b^2$ with $(a, b) = 1$ is never divisible by 3 or 4. Thus for $s_0 \geq 2$ or $s_1 > 0$ Theorem 4.1.1 (II) immediately holds. We are left to deal with the exponent s_2. By looking modulo 7 we find that $a^2 + b^2$ is never divisible by 7 then the solution $a^{14} + b^{14} = (a^2 + b^2)\phi_7(a^2, b^2) = dc_0^p$ will correspond to a solution (a, b, c) of the equation

$$\phi_7(a^2, b^2) = c^p \qquad \text{with} \qquad d \mid a^2 + b^2 \tag{4.8}$$

Given a primitive solution (a, b, c) of (4.8) we attach to it $E = E_{(a^2,b^2)}$ as a Frey curve. From the fact $4 \nmid a^2 + b^2$, Proposition 4.1.2 and Serre's conjecture it follows that there exist a newform $f \in S_2(M)$ with $M = 2^2 7^2$ or $2^4 7^2$ satisfying $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}$. We do as above and divide the newforms into the same sets S1 and S2. Since the newform associated with the solution $(1, -1, 0)$ has level $2^3 7^2$ it will not belong to S1 nor to S2. Hence the restriction $7 \nmid c$ is not needed. If $s_2 > 0$ then $5^{s_2} \mid a^2 + b^2$ and we have $a_5(E_{(a^2,b^2)}) = -1$. We already know that this condition is enough to eliminate the newforms associated with $E_{(0,1)}$ and $E_{(1,1)}$. This eliminates all the newforms in S1 and we treat those in S2 exactly as in the proof of (I).

■

4.1.1 The equation $\phi_7(x, y) = 71z^p$

From the discriminant of the curves $E_{(a,b)}$ it is clear that we can use them to attack equations of the form $\phi(x, y) = \phi_7(x, y) = dz^p$, where

$$\phi(x, y) = x^6 - x^5y + x^4y^2 - x^3y^3 + x^2y^4 - xy^5 + y^6.$$

Recall that if $(a, b) = 1$ then $\phi(a, b)$ is only divisible by primes congruent to 1 modulo 7. We will now prove the following result

Theorem 4.1.3 *If $p > 254^{2873}$ is a prime, then the equation*

$$\phi(x, y) = 71z^p \tag{4.9}$$

has no non-trivial primitive solutions.

Since $\phi = \phi_7$ is the same of the previous section, for a putative primitive solution (a, b, c) of (4.9) we will use the same Frey curves $E_{(a,b)}$ as before. That is, we let $A(a, b) = \alpha f_1(a, b)$,

$B(a,b) = \beta f_2(a,b)$ and $C(a,b) = \gamma f_3(a,b)$ and we obtain the curves

$$\begin{cases} E_{(a,b)} : y^2 = x^3 + a_4 x + a_6, \quad \text{with} \\ a_4 = -3024(a^4 - a^3b + 3a^2b^2 - ab^3 + b^4) \\ a_6 = 12096(a^6 - 15a^5b + 15a^4b^2 - 29a^3b^3 + 15a^2b^4 - 15ab^5 + b^6). \end{cases}$$

This time, from the form of (4.9) we have that

$$\Delta(E) = 2^{16}3^{12}7^s71^2c^{2p}.$$

Denote by c_0 the product of the primes $q \neq 71$ dividing c.

Proposition 4.1.4 *The curves $E_{(a,b)}$ have conductor given by*

$$N_E = 2^s7^271c_0,$$

where $s \in \{2,3,4\}$.

Proof: The same proof of Proposition 4.1.2 works for all primes $p \neq 71$. For $p = 71$ we have $\upsilon_p(\Delta) \geq 2$ for all (a,b). Observe that 71 splits in $K^+ = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ (degree 3) and also that A, B, C are conjugate and coprime at primes outside 7. Then, A, B, C are divisible by exactly one different prime above 71 in K^+. From

$$c_4 = 2^4(AB + BC + AC)$$

it follows that $\upsilon_{71}(c_4) = 0$. Then $E_{(a,b)}$ has multiplicative reduction at $p = 71$.

■

Since all the primes q dividing c_0 are of multiplicative reduction we can apply again Hellegouarch argument to conclude that $\bar{\rho}_{E.p}$ will not ramify at $q \mid c_0$. Furthermore, as in the previous section we have that $\bar{\rho}_{E,p}$ is finite at p and absolutely irreducible for $p \geq 17$. Then again by Serre's conjecture there must exist a newform f in $S_2(N(\bar{\rho}_{E,p}))$ where $N(\bar{\rho}_{E,p}) = 2^s7^271$ with $s \in \{2,3,4\}$ such that

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}, \tag{4.10}$$

where $\mathfrak{P} \mid p$ is a prime in $\bar{\mathbb{Q}}$. The space $S_2^{new}(2^47^271)$ is too large to compute completely its eigenforms. Nevertheless, we are able to finish the proof but the price for it is the large bound for p in the statement of Theorem 4.1.3. As before we divide the newforms in the spaces $S_2(2^s7^271)$ where $s \in \{2,3,4\}$ into two sets:

S1: Newforms with $\mathbb{Q}_f = \mathbb{Q}$

S2: Newforms such that $\mathbb{Q}$ is strictly contained in $\mathbb{Q}_f$

Since the newforms in S1, by the Modularity Theorem, correspond to elliptic curves over $\mathbb{Q}$ we use SAGE to consult Cremona's Table of elliptic curves for conductors up to 130000 to get the complete list of elliptic curves with conductor 2^s7^271 for $s = 2, 3, 4$. For each curve C in the list we computed the values $a_q(C)$ for $q \in \{3, 5, 11, 13, 17, 19, 23\}$. Comparing the values $a_q(C)$ obtained this way with the possibilities allowed by our Frey curves that we computed in the previous section (see the list above (4.6)) we can eliminate all the curves. Since $p > 254^{2873}$, here we can eliminate the newforms exactly as in the previous section, by checking if the values $a_q(C)$ for the curves in Cremona's list do not belong to our corresponding list.

To deal with the newforms $f = q + \sum_{n\geq 2} c_n(f)q^n$ in S2 we will use the Weil bound $|c_l(f)| \leq 2\sqrt{l}$ and the following proposition.

Proposition 4.1.5 *If f is a newform of level N such that $\mathbb{Q}_f \neq \mathbb{Q}$ then there exists a prime number $q \leq SB$ such that the coefficient $c_q(f)$ does not belong to $\mathbb{Q}$, where SB (Sturm bound) is given by*

$$SB = \frac{N}{6} \prod_{primes\ q|N} (1 + \frac{1}{q})$$

.

Proof: See [44], Lemme 1.

Now suppose that (4.10) holds for an f in S2 and let q be a prime given by the proposition above. We can suppose that f is of level 2^47^271 because the smaller levels would give smaller bounds for p. We use SAGE to compute the dimension D of the space $S_2^{new}(2^47^271)$, which gives $D = 1435$ and the Sturm bound $SB = 16128$. Then we have

$$\begin{cases} |a_q(E)|, |c_q(f)| \leq 2\sqrt{q} \leq 2\sqrt{SB} \leq 254 \\ [\mathbb{Q}_f : \mathbb{Q}] \leq D = 1435 \end{cases}$$

and also

$$a_q(E) \equiv c_q(f) \pmod{\mathfrak{P}}.$$

Let $p_f(x)$ be the minimal polynomial of $c_q(f)$, which is of degree at most D, and can not have integer roots because $c_q(f)$ is not an integer. Then $p_f(a_q(E)) \neq 0$ and

$$p_f(a_q) \equiv p_f(c_q) \equiv 0 \pmod{\mathfrak{P}}.$$

Since there are only a finite number of possibilities for $a_q(E)$ then also for $p_f(a_q(E))$ thus there is a constant C_f such that if $p > C_f$, the congruence $p_f(a_q(E)) \equiv 0 \pmod{p}$ can not hold. Thus (4.10) can not hold for this f.

Now we proceed to the computation of a concrete value for C that works for all f. First observe that the roots r_i of p_f are the Galois conjugates c_q^σ of c_q and they also satisfy $|r_i| \leq 2\sqrt{q} \leq 254$. Let b_n be the coefficients of $p_f = \sum b_n x^n$. Since we know that the b_n

are given by the symmetric functions in r_i we can find a upper bound for each b_n easily, for example

$$b_{n-2} = r_0r_1 + r_0r_2 + ... + r_{n-2}r_{n-1} \leq \binom{1435}{2}254^2,$$

and the biggest upper bound that we find this way is $\binom{1435}{1430}254^{1430}$. Hence we have

$$|p_f(x)| \leq 1435(\max\{b_n\})|x|^{1435}$$

and thus

$$|p_f(a_q(E))| \leq 1435\binom{1435}{1429}254^{1429}254^{1435} \leq 254^2254^7254^{2864} \leq 254^{2873},$$

where the last two inequalities were taken only for aesthetic purposes. Then taking $C = 254^{2873}$ ends the proof of Theorem 4.1.3.

4.2 The equations $x^{13} + y^{13} = Cz^p$

In this section we will apply our method to equations with form

$$x^{13} + y^{13} = Cz^p \tag{4.11}$$

and prove the following result

Theorem 4.2.1 *Let $d = 3, 5, 7$ or 11 and γ be an integer divisible only by primes $l \not\equiv 1, 0$ (mod 13). If $p > 4992539$ is a prime, then:*

(I) The equation $x^{13} + y^{13} = d\gamma z^p$ has no non-trivial primitive first case solutions.

(II) The equation $x^{26} + y^{26} = 10\gamma z^p$ has no non-trivial primitive solutions.

In what follows we will first prove part (I) of Theorem 4.2.1 and in the end we will explain the small tweak needed to conclude part (II). Observe that in part (II) replacing 10 by twice d for $d = 3, 7, 11$ the statement is also true but trivial, because the left-hand side is a sum of two relatively prime squares.

We have $x^{13} + y^{13} = (x + y)\phi(x, y)$, where

$$\begin{aligned}\phi(x,y) &= x^{12} - x^{11}y + x^{10}y^2 - x^9y^3 + x^8y^4 - x^7y^5 + x^6y^6 \\ &- x^5y^7 + x^4y^8 - x^3y^9 + x^2y^{10} - xy^{11} + y^{12}.\end{aligned}$$

Suppose that there exists a primitive solution (a, b, c') to (4.11) with $C = d\gamma$, where d and γ are as in Theorem 4.2.1. Then it follows that there exists a primitive solution (a, b, c_0) to

$$\phi(a, b) = c_0^p, \tag{4.12}$$

with $C \mid a + b$ and $13 \nmid a + b$ or to

$$\phi(a, b) = 13c_0^p \tag{4.13}$$

with $C \mid a + b$ and $13 \mid a + b$, where in both cases c_0 is only divisible by primes congruent to 1 modulo 13. Now consider the degree 6 factor of ϕ with coefficients in $\mathbb{Q}(\sqrt{13})$ given by

$$\phi_1(x, y) = (x + \zeta y)(x + \zeta^{12}y)(x + \zeta^4 y)(x + \zeta^9 y)(x + \zeta^3 y)(x + \zeta^{10}y).$$

By the method in the previous chapter then for some unit μ there exists a solution (a, b, c) (with c an integer in $\mathbb{Q}(\sqrt{13})$) to the equation

$$\phi_1(a, b) = \mu c^p, \tag{4.14}$$

with $C \mid a + b$ and $13 \nmid a + b$ or to

$$\phi_1(a, b) = \mu\sqrt{13}c^p, \tag{4.15}$$

with $C \mid a + b$ and $13 \mid a + b$, respectively. Recall that that $13 \mid c$ is equivalent to $13 \mid a + b$. Then, we will prove Theorem 4.2.1 (I) if we prove that there are no primitive solutions (a, b, c) to (4.14) or (4.15) such that $|\mathrm{Norm}_{\mathbb{Q}(\sqrt{13})/\mathbb{Q}}(abc)| > 1$, $C = d\gamma \mid a + b$ and $13 \nmid a + b$. As for $r = 7$, in the proof that follows, we will only need to use that $d \mid a + b$.

We now construct the Frey curves. Consider the factorization $\phi_1 = f_1 f_2 f_3$ where

$$\begin{cases} f_1(x, y) = (x + \zeta y)(x + \zeta^{12}y) = x^2 + (\zeta + \zeta^{12})xy + y^2 \\ f_2(x, y) = (x + \zeta^4 y)(x + \zeta^9 y) = x^2 + (\zeta^4 + \zeta^9)xy + y^2 \\ f_3(x, y) = (x + \zeta^3 y)(x + \zeta^{10}y) = x^2 + (\zeta^3 + \zeta^{10})xy + y^2 \end{cases}$$

are the degree two factors of ϕ_1 with coefficients in K^+. As before, solving a linear system in the coefficients of the f_i we find that one of its infinite solutions in $\mathcal{O}_{K^+}^3$ is given by

$$\begin{cases} \alpha = -\zeta^{10} + \zeta^9 + \zeta^4 - \zeta^3 \\ \beta = \zeta^{12} - \zeta^9 - \zeta^4 + \zeta \\ \gamma = -\zeta^{12} + \zeta^{10} + \zeta^3 - \zeta \end{cases}$$

and satisfies $\upsilon_{\mathfrak{P}_{13}}(\alpha) = \upsilon_{\mathfrak{P}_{13}}(\beta) = \upsilon_{\mathfrak{P}_{13}}(\gamma) = 1$.

This results in the Frey curves with short Weierstrass form over $\mathbb{Q}(\sqrt{13})$ given by

$$E_{(a,b)} : y^2 = x^3 + a_4(a, b)x + a_6(a, b),$$

$$
\begin{aligned}
a_4(a,b) &= (216w-2808)a^4+(-1728w+5616)a^3b \\
&\quad +(1728w-11232)a^2b^2+(-1728w+5616)ab^3 \\
&\quad +(216w-2808)b^4, \\
a_6(a,b) &= (-8640w+44928)a^6+(49248w-235872)a^5b \\
&\quad +(-129600w+471744)a^4b^2+(152928w-662688)a^3b^3+ \\
&\quad +(-129600w+471744)a^2b^4+(49248w-235872)ab^5+ \\
&\quad +(-8640w+44928)b^6+(50193w+182520)b^6,
\end{aligned}
$$

where $w^2=13$. Note that 2 is inert in $\mathbb{Q}(\sqrt{13})$. In what follows we use 2 and w to denote also the ideals in $\mathbb{Q}(\sqrt{13})$ above 2 and 13, respectively.

Proposition 4.2.2 *The possible values for the conductors of $E_{(a,b)}$ are*

$$N_E = 2^s w^2 rad(c),$$

where $s=3,4$ and $rad(c)$ is the product of the prime factors of c. Moreover, if $2 \mid a+b$ then $s=3$ if $4 \mid a+b$ and $s=4$ if $4 \nmid a+b$.

Proof: From Proposition 3.2.19 we know the set of possible values for the conductor and using SAGE we easily check for all pairs (a,b) mod 2^6 that $s=2$ does not happen.

■

The next two theorems follow easily from the theory on Chapter 3 and are fundamental for our argument.

Theorem 4.2.3 *Let (a,b,c) be a non-trivial primitive solution of* (4.14) *or* (4.15)*. Then the Frey curves $E_{(a,b)}$ over $\mathbb{Q}(\sqrt{13})$ are modular.*

Proof: $\mathbb{Q}(\sqrt{13})$ is an abelian extension in which 3 splits. Since the primes $t \mid 3$ in $\mathbb{Q}(\sqrt{13})$ do not divide c (because $3 \nmid \phi(a,b)$) it follows from Proposition 3.2.12 that $E_{(a,b)}$ has good reduction at all $t \mid 3$. Now the result is immediate from Theorem 3.3.10.

■

Theorem 4.2.4 *Let $p > 97$ be a prime. The representation $\bar{\rho}_{E,p}$ is absolutely irreducible.*

Proof: This follows immediately from the proof of Theorem 3.2.15. We just have to replace in there $q=3$ and $H = (\mathcal{O}_{\mathbb{Q}(\sqrt{13})}/2^2 w)^* \cong \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

■

As we have explained in Chapter 3, Theorems 4.2.3 and 4.2.4 allow us to lower the level. In the present case we apply these results along the same lines. For N an ideal in $\mathbb{Q}(\sqrt{13})$ we denote by $S_2(N)$ the set of Hilbert modular cusp forms of parallel weight $(2,2)$ and level

N. It follows from the modularity that there exists a newform f_0 in $S_2(2^i w^2 \mathrm{rad}(c))$ where $i = 3$ or 4 with $\mathbb{Q}_{f_0} = \mathbb{Q}$ such that $\rho_{E,p}$ is isomorphic to the p-adic representation $\rho_{f_0,p}$. Since the primes $\mathfrak{p}$ of multiplicative reduction of E, i.e. $\mathfrak{p} \mid c$, appear to a p-th power in the (minimal at $\mathfrak{p}$) discriminant $\Delta(E)$ we know by Theorem 1.1.14 that the representation $\bar{\rho}_{E,p}$ will not ramify at these primes. Since $\rho_{E,p}$ is modular then $\bar{\rho}_{E,p}$ is also modular and, when irreducible, by the results on level lowering for Hilbert modular forms it is modular of level $2^i w^2$. Thus there exists a newform f in $S_2(2^i w^2)$ and a prime $\mathfrak{P} \mid p$ such that its associated residual Galois representation $\bar{\rho}_{f,\mathfrak{P}}$ satisfies

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{f_0,p} \sim \bar{\rho}_{f,\mathfrak{P}}. \tag{4.16}$$

If now we find a contradiction to (4.16), this shows that the Frey curves associated with primitive non-trivial first case solutions (a, b, c) to equation (4.14) or (4.15) can not exist and ends the proof of part (I) in Theorem 4.2.1. To find the desired contradiction we use the trace values $a_L(\rho_{E,p})$ and $a_L(\rho_{f,p})$ for some primes L of $\mathbb{Q}(\sqrt{13})$ and the Hilbert modular newforms f in $S_2(2^i w^2)$ for $i = 3, 4$. Let $w \in \mathbb{Q}(\sqrt{13})$ be such that $w^2 = 13$ and consider the following prime ideals in $\mathbb{Q}(\sqrt{13})$:

$$\begin{cases} L_2 = \langle 2 \rangle, \quad L_{13} = \langle w \rangle \\ L_3^0 = \langle \frac{1}{2}(w+1) \rangle, \quad L_3^1 = \langle \frac{1}{2}(-w+1) \rangle, \\ L_{17}^0 = \langle \frac{1}{2}(w+9) \rangle, \quad L_{17}^1 = \langle \frac{1}{2}(-w+9) \rangle, \\ L_{23}^0 = \langle \frac{1}{2}(-3w-5) \rangle, \quad L_{23}^1 = \langle \frac{1}{2}(-3w+5) \rangle, \\ L_{29}^0 = \langle \frac{1}{2}(3w+1) \rangle, \quad L_{29}^1 = \langle \frac{1}{2}(3w-1) \rangle, \\ L_5 = \langle 5 \rangle, \quad L_7 = \langle 7 \rangle, \quad L_{11} = \langle 11 \rangle. \end{cases}$$

On one hand, to obtain the values of $a_L(\rho_{f,p})$, with the aid of John Voight we used algorithms to compute Hilbert modular forms implemented in MAGMA [7] (an expository account can be found in [24]). John Voight gave us two lists corresponding to all forms (not necessarily newforms) with integer coefficients such that $a_{L_2} = a_{L_{13}} = 0$ and of levels $2^i w^2$ for $i = 3, 4$. With MAGMA we have done the same to all dividing levels and by putting together both informations we obtained all newforms in the spaces $S_2(2^i w^2)$ for $i = 3, 4$ such that $\mathbb{Q}_f = \mathbb{Q}$. A list of coefficients corresponding to the newforms obtained this way can be found in the appendix (sec. 6.1). Moreover, a consequence of the method used is that any newform in the two previous spaces with $\mathbb{Q}_f$ strictly containing $\mathbb{Q}$ must have a Fourier coefficient outside $\mathbb{Q}$ at the prime L_3^0 above 3. John Voight also computed the factorization of the characteristic polynomial of the Hecke operator $T_{L_3^0}$ in both spaces (see appendix, sec. 6.2).

On the other hand, for every prime L in $\mathbb{Q}(\sqrt{13})$ of good reduction for E, such that L is above a rational prime $l \leq 29$ and $l \neq 19$, we use SAGE to go through all the possible residual elliptic curves for all non-zero pairs $(a, b) \in \mathbb{F}_l \times \mathbb{F}_l$ and compute all the possible

values for $a_L(\rho_{E,p}) = a_L(E)$, that are given by formula (1.1):

$$\begin{cases} a_{L_3^0} \in \{-3,-1\}, \\ a_{L_3^1} \in \{-3,-1,1\}, \\ a_{L_5} \in \{-6,-2,2\}, \\ a_{L_7} \in \{11,-11,-1,-5\}, \\ a_{L_{11}} \in \{-15,3,5,-7,9,-1,15\}, \\ a_{L_{17}^0} \in \{1,3,5,7,-3,-1\}, \\ a_{L_{17}^1} \in \{3,5,7,-7,-5,-3\}, \\ a_{L_{23}^0} \in \{1,3,5,7,-9,-7,-5,-3\}, \\ a_{L_{23}^1} \in \{1,3,7,-9,-3,-1\}, \\ a_{L_{29}^0} \in \{1,3,5,-9,-7,-5,-3,-1\}, \\ a_{L_{29}^1} \in \{1,3,5,9,-9,-7,-5,-3,-1\} \end{cases}$$

Before proceeding to eliminate the newforms we divide them into two sets:

S1: The newforms in $S_2(2^i w^2)$ for $i = 3, 4$ such that $\mathbb{Q}_f = \mathbb{Q}$.

S2: The newforms in the same levels with $\mathbb{Q}_f$ strictly containing $\mathbb{Q}$.

Note that equations (4.14) and (4.15) have trivial solutions $(1,1,1)$, $\pm(0,1,1)$, $\pm(1,0,1)$ and $(1,-1,1)$, $(-1,1,1)$, respectively. These solutions correspond to the Frey curves $E_{(1,1)}$, $E_{(0,1)}$ and $E_{(1,-1)}$ that indeed exist and so there must be newforms associated with them in S1 which *a priori* will not be possible to eliminate only by comparing the a_L.

Going through all the forms in $S1$ and comparing the corresponding values of the $a_L's$ with the possibilities for our Frey curves we immediately eliminate all except 4 newforms. Here we have eliminated a newform f if at least one of its coefficients $a_L(f)$ is not on the corresponding list above. This can be done because the value of p in the statement of Theorem 4.2.1 is very large hence the isomorphism (4.16), when specified at a trace at L for a prime L of small norm, does not hold modulo such large prime p unless $a_L(f) = a_L(E)$ for some $a_L(E)$ in the list. For example, the first form in the appendix satisfies $a_{L_5}(f) = -9$ and since $a_{L_5}(E) \in \{-6,-2,2\}$ it is clear that $-9 \equiv -6,-2,2 \pmod{p}$ can not hold for $p > 11$. The four remaining newforms correspond to the trivial solutions above plus the twist by -1 of $E_{(1,1)}$. The one associated with $E_{(1,1)}$ has level $2^4 w^2$ and the other three $2^3 w^2$. In Table 4.1 we list their first eigenvalues.

To be able to eliminate these remaining newforms we need to use the condition $d \mid a+b$. Recomputing the values for some $a_L(E)$ but with this extra condition we find that $a_{L_3^0} = -3$ and $a_{L_3^1} = -1$ (if $d = 3$) , $a_{L_5} = -2$ (if $d = 5$) , $a_{L_7} = -11$ (if $d = 7$) or $a_{L_{11}} = -15$ (if $d = 11$). By checking in Table 4.1 we see that any of the previous conditions is enough to eliminate all f_i except for f_4. Actually, f_4 is the newform associated with the trivial solution $(1,-1,0)$ and can not be eliminated this way as expected. Finally, if we assume

	$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
f_1	-1	1	7	3	1	7	2	-7	-3	-1	3
f_2	-1	1	3	7	-7	-1	2	-3	-7	-1	3
f_3	-1	-3	-1	-5	5	-9	-6	-3	1	-5	15
f_4	-3	-1	1	-3	-3	-9	-2	-7	5	-11	-15

Table 4.1: Values of a_L

that the solution is first case, that is $13 \nmid c \Leftrightarrow 13 \nmid a+b$, Proposition 3.2.12 says that the conductors at $\mathfrak{P}_{13}$ of $\rho_{f_4,p}|G_{K^+}$ and $\rho_{E,p}|G_{K^+}$ are $\mathfrak{P}_{13}^0$ and $\mathfrak{P}_{13}^2$, respectively. Then, their reduction modulo p will also have different conductors at $\mathfrak{P}_{13}$ if $p > 13$. Thus they can not be isomorphic.

To finish the argument we have to eliminate also the newforms in $S2$. Recall that we know the factorization (see appendix) of the characteristic polynomial of $T_{L_3^0}$ which we denote by p_3. If for f in $S2$ the isomorphism (4.16) holds we also have

$$a_{L_3^0}(E) \equiv c_{L_3^0}(f) \pmod{\mathfrak{P}}.$$

Let $p_f(x)$ be the minimal polynomial of $c_{L_3^0}(f)$ which must be a non-linear factor of p_3, because we also know from J. Voights algorithm that $c_{L_3^0}(f)$ is not in $\mathbb{Q}$. Thus,

$$p_f(a_{L_3^0}(E)) \equiv p_f(c_{L_3^0}(f)) \equiv 0 \pmod{\mathfrak{P}} \tag{4.17}$$

and $p_f(a_{L_3^0}(E)) \neq 0$ because $c_{L_3^0}(f) \notin \mathbb{Z}$. Since $a_{L_3^0}(E) \in \{3, -1\}$ by computing $p_f(3)$ and $p_f(-1)$ for all p_f a non-linear factors of p_3 we have all the possibilities for $p_f(a_{L_3^0}(E))$ and we can see that congruence (4.17) can not hold if $p > 4992539$. Therefore (4.16) also can not hold if $p > 4992539$ and this ends the proof of part (I) in Theorem 4.2.1.

■

Remark 4.2.5 *It is also possible to eliminate the newforms in $S2$ without knowing the factorization of p_3 but this would result in the bound $p > 2^{14546}$ for the exponent. Indeed, let $p_f = \sum r_n x^n$ be the minimal polynomial of a non integer $c_{L_3}(f)$. All the roots $c_{L_3}^\sigma$ satisfy the Weil bound since they are coefficients of the conjugated form f^σ. Moreover, by knowing the dimension of $S_2(2^s w^2)$ we can bound all $|r_n|$ using the binomial coefficients. Putting these bounds together we find only a finite number of possibilities for the non-zero value $p_f(a_{L_3}(E))$. The details for this argument can be found at http://arxiv.org/abs/*1112.4521*. Observe that we have already applied the same strategy for another equation in section* 4.1.1.

Part (II) now follows easily from the proof of part (I). First note that as before it follows from the factorization

$$x^{26} + y^{26} = (x^2 + y^2)\phi(x^2, y^2) = 10z^p, \tag{4.18}$$

Proposition 3.2.5 and Corollary 3.2.4, that a solution (a, b, c) must verify $10 \mid a^2 + b^2$. To a primitive solution (a, b, c) of (4.18) we now attach the Frey curve $E_{(a^2,b^2)}$. Recall that $4 \nmid a^2 + b^2$. It now follows from Proposition 4.2.2, modularity and level lowering that the set S1 will only have newforms of level 2^4w^2. This means that after comparing the values $a_L(E)$ with $a_L(f)$ for f in S1 we eliminate all newforms except for the one corresponding to the curve $E_{(1,1)}$. As we already know, the extra restriction $5 \mid a^2 + b^2$ is enough to deal with this newform. In fact, recall that in this case the Frey curve has $a_5(E) = -2$, and this is different from the corresponding coefficient a_5 of $E_{(1,1)}$. The newforms in S2 can be eliminated exactly as in the proof of part (I).

■

4.3 More examples: the cases $r = 11, 17, 19$

Recall that for each r we constructed Frey curves over $K^+ = \mathbb{Q}(\zeta_r + \zeta_r^{-1})$. Let π_r be such that $(r)\mathcal{O}_{K^+} = (\pi_r)^{(r-1)/2}$

4.3.1 The equation $x^{11} + y^{11} = Cz^p$

Note that $11 \equiv -1 \pmod 6$ so this is computationally difficult case. We have $K^+ = \mathbb{Q}(w)$, where the minimal polynomial of w is $t^5 + t^4 - 4t^3 - 3t^2 + 3t + 1$. We pick $\phi_1 = f_1 f_2 f_3$, where

$$\begin{cases} f_1(x, y) = x^2 + (\zeta + \zeta^{10})xy + y^2, \\ f_2(x, y) = x^2 + (\zeta^2 + \zeta^9)xy + y^2, \\ f_3(x, y) = x^2 + (\zeta^3 + \zeta^8)xy + y^2. \end{cases}$$

Let (a, b, c) be a non-trivial primitive solution of $x^{11} + y^{11} = Cz^p$. Then for some unit $\mu \in \mathcal{O}_{K^+}$ we also have a non-trivial primitive solution of

$$\phi_1(x, y) = \mu z^p \quad \text{or}$$

$$\phi_1(x, y) = \mu\pi_{11}^3 z^p$$

if $11 \nmid a + b$ or $11 \mid a + b$, respectively. The resulting F-H-curves over K^+ is given by

$$E_{(a,b)} : y^2 = x^3 + a_4x + a_6, \text{ where}$$

$$
\begin{aligned}
a_4(a,b) &= (432w^3 - 432w - 2592)a^4 \\
&\quad +(-432w^4 - 3888w^3 + 1296w^2 + 7776w + 3024)a^3b \\
&\quad +(3456w^3 - 432w^2 - 6480w - 8208)a^2b^2, \\
&\quad +(-432w^4 - 3888w^3 + 1296w^2 + 7776w + 3024)ab^3 \\
&\quad +(432w^3 - 432w - 2592)b^4 \\
a_6(a,b) &= (8640w^4 + 25920w^3 - 39744w^2 - 48384w + 5184)a^6 \\
&\quad +(5184w^4 - 98496w^3 + 10368w^2 + 176256w + 139968)a^5b \\
&\quad +(285120w^3 - 57024w^2 - 570240w - 171072)a^4b^2 \\
&\quad +(25920w^4 - 302400w^3 - 5184w^2 + 596160w + 338688)a^3b^3 \\
&\quad +(285120w^3 - 57024w^2 - 570240w - 171072)a^2b^4 \\
&\quad +(5184w^4 - 98496w^3 + 10368w^2 + 176256w + 139968)ab^5 \\
&\quad +(8640w^4 + 25920w^3 - 39744w^2 - 48384w + 5184)b^6
\end{aligned}
$$

We observe that 3 is inert in K^+ and with the help of SAGE we computed $a_3(E_{(a,b)})$ for all pairs $(a,b) \pmod 3$ and obtained that $a_3(E) \in \{-16, 16\}$ which shows that $E_{(a,b)}$ are ordinary at 3.

4.3.2 The equation $x^{17} + y^{17} = Cz^p$

Note that $17 \equiv -1 \pmod 6$ so this is a bad case. We have $K^+ = \mathbb{Q}(w)$, where the minimal polynomial of w is $t^8 + t^7 - 7t^6 - 6t^5 + 15t^4 + 10t^3 - 10t^2 - 4t + 1$. Following the method we pick $\phi_1 = f_1 f_2 f_3$, with

$$
\begin{cases}
f_1(x,y) = x^2 + (\zeta + \zeta^{16})xy + y^2, \\
f_2(x,y) = x^2 + (\zeta^2 + \zeta^{15})xy + y^2, \\
f_3(x,y) = x^2 + (\zeta^3 + \zeta^{14})xy + y^2.
\end{cases}
$$

Let (a,b,c) be a non-trivial primitive solution of $x^{17} + y^{17} = Cz^p$. Then for some unit $\mu \in \mathcal{O}_{K^+}$ we also have a non-trivial primitive solution of

$$\phi_1(x,y) = \mu z^p \quad \text{or}$$

$$\phi_1(x,y) = \mu \pi_{17}^3 z^p$$

if $17 \nmid a+b$ or $17 \mid a+b$, respectively. The resulting F-H-curves over K^+ are given by

$$E_{(a,b)} : y^2 = x^3 + a_4 x + a_6, \text{ where}$$

$$
\begin{aligned}
a_4(a,b) &= (-432w^6+432w^5+2592w^4-1728w^3-3888w^2+1728w-1728)a^4\\
&\quad +(-432w^7+3024w^6+2160w^5-15984w^4-3456w^3+19872w^2\\
&\quad +1728w+432)a^3b+(-3024w^6+1728w^5+16416w^4-6048w^3\\
&\quad -22032w^2+4320w-3888)a^2b^2+(-432w^7+3024w^6+2160w^5\\
&\quad -15984w^4-3456w^3+19872w^2+1728w+432)ab^3+(-432w^6\\
&\quad +432w^5+2592w^4-1728w^3-3888w^2+1728w-1728)b^4
\end{aligned}
$$

$$
\begin{aligned}
a_6(a,b) &= (-8640w^7+25920w^6+46656w^5-143424w^4-62208w^3+196992w^2\\
&\quad +3456w-19008)a^6+(5184w^7-93312w^6+25920w^5+497664w^4\\
&\quad -160704w^3-663552w^2+150336w-20736)a^5b+(-51840w^7\\
&\quad +254016w^6+238464w^5-1316736w^4-295488w^3+1653696w^2\\
&\quad +82944w-72576)a^4b^2+(39744w^7-269568w^6-101952w^5\\
&\quad +1397952w^4-53568w^3-1802304w^2+114048w)a^3b^3\\
&\quad +(-51840w^7+254016w^6+238464w^5-1316736w^4-295488w^3\\
&\quad +1653696w^2+82944w-72576)a^2b^4+(5184w^7-93312w^6\\
&\quad +25920w^5+497664w^4-160704w^3-663552w^2+150336w\\
&\quad -20736)ab^5+(-8640w^7+25920w^6+46656w^5-143424w^4\\
&\quad -62208w^3+196992w^2+3456w-19008)b^6
\end{aligned}
$$

We observe that 3 is inert in K^+ and with the help of SAGE we computed $a_3(E_{(a,b)})$ for all pairs (a,b) (mod 3) and obtained that $a_3(E)\in\{-94,-62,118\}$ which shows that $E_{(a,b)}$ are ordinary at 3.

4.3.3 The equation $x^{19}+y^{19}=Cz^p$

Note that $19\equiv 1 \pmod 6$ so this is a good case. We have $K_0=\mathbb{Q}(w)$, where the minimal polynomial of w is t^3+t^2-6t-7 and following the method we pick $\phi_1=f_1f_2f_3$, with

$$
\begin{cases}
f_1(x,y)=x^2+(\zeta+\zeta^{18})xy+y^2,\\
f_2(x,y)=x^2+(\zeta^{12}+\zeta^7)xy+y^2,\\
f_3(x,y)=x^2+(\zeta^{11}+\zeta^8)xy+y^2.
\end{cases}
$$

Let (a,b,c) be a non-trivial primitive solution of $x^{19}+y^{19}=Cz^p$. Then for some unit $\mu\in\mathcal{O}_{K_0}$ we also have a non-trivial primitive solution of

$$\phi_1(x,y)=\mu z^p \quad \text{or}$$

$$\phi_1(x,y)=\mu\pi_{19}^3 z^p$$

if $19 \nmid a+b$ or $19 \mid a+b$, respectively. The resulting F-H-curves over K_0 are given by

$$E_{(a,b)} : y^2 = x^3 + a_4 x + a_6, \text{ where}$$

$$\begin{aligned}
a_4(a,b) &= (864w^2 - 6480)a^4 \\
&\quad +(-3456w^2 - 432w + 20304)a^3b \\
&\quad +(4320w^2 - 432w - 29808)a^2b^2 \\
&\quad +(-3456w^2 - 432w + 20304)ab^3 \\
&\quad +(864w^2 - 6480)b^4, \\
a_6(a,b) &= (-34560w^2 + 5184w + 195264)a^6 \\
&\quad +(150336w^2 - 25920w - 922752)a^5b \\
&\quad +(-342144w^2 + 31104w + 1985472)a^4b^2 \\
&\quad +(418176w^2 - 76032w - 2548800)a^3b^3 \\
&\quad +(-342144w^2 + 31104w + 1985472)a^2b^4 \\
&\quad +(150336w^2 - 25920w - 922752)ab^5 \\
&\quad +(-34560w^2 + 5184w + 195264)b^6.
\end{aligned}$$

Here 3 is also inert in K_0 and computations allowed to see that $a_3(E) \in \{-1, 7\}$ which shows that the curves $E_{(a,b)}$ are ordinary at 3.

Although we are in a case of favorable computer requirements the dimension of $S(2^4\mathfrak{P}_{19}^2)$ is 437761 which is already too big even for computing with J. Voight algorithm only the newforms with coefficients in $\mathbb{Q}$.

Chapter 5

The case $r = 4m + 1$

In this chapter we will construct two extra Frey curves attached to solutions of the equation $x^r + y^r = Cz^p$ for primes of the form $r = 4m + 1$. This will be achieved in two steps. First, using observations about the factors of ϕ_r as in Chapter 3, we will again relate two Diophantine equations. Second, we will generalize the ideas that led to the construction of the $\mathbb{Q}$-curves in Chapter 2.

We need to introduce the definition of k-curve generalizing the notion of $\mathbb{Q}$-curve.

Definition 5.0.1 *Let k be a number field and $G_k = Gal(\bar{\mathbb{Q}}/k)$ its absolute Galois group. We will say that an elliptic curve C over $\bar{k}$ is a k-curve if for every $\sigma \in G_k$ there exists an isogeny $\phi_\sigma : {}^\sigma C \to C$ defined over $\bar{k}$. We say that a k-curve C is completely defined over a number field $K \supset k$ if all the conjugates of C and the isogenies between them are defined over K.*

Let $r = 4m + 1$ be a prime and $\zeta := \zeta_r$ a r-th primitive root of unity. Recall that $K^+ = \mathbb{Q}(\zeta + \zeta^{-1})$ is the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta)$. Then K^+ has degree $2m$ and there exists a subfield $k \subset K^+$ such that $[K^+/k] = 2$ and $[k/\mathbb{Q}] = m$. Let σ be the generator of $\mathrm{Gal}(K^+/\mathbb{Q})$ then σ^m generates $\mathrm{Gal}(K^+/k)$. Recall that $x^r + y^r = (x + y)\phi_r(x, y)$ and $\phi_r(x, y)$ factors as a product of $2m$ degree two polynomials f_i with coefficients in K^+. Let h_r^+ be the class number of K^+ and π_r be such that $r\mathcal{O}_{K^+} = (\pi_r)^{(r-1)/2}$. The following lemma is similar to Lemma 3.2.9 and relates our initial equation to a new one.

Lemma 5.0.2 *Let p be a prime not dividing h_r^+. Suppose there is a non-trivial primitive solution to $x^r + y^r = Cz^p$ with $C \neq 0$ an integer divisible only by primes $q \neq r$ satisfying $q \not\equiv 1 \pmod{r}$. Let f_1, f_2 be the factors of ϕ_r given by*

$$\begin{cases} f_1(x, y) = x^2 + (\zeta + \zeta^{4m})xy + y^2 \\ f_2(x, y) = x^2 + \sigma^m(\zeta + \zeta^{4m})xy + y^2. \end{cases}$$

Then, there exists a unit $\mu \in \mathcal{O}_{K^+}^\times$ and a solution (a, b, c) in $\mathbb{Z}^2 \times \mathcal{O}_{K^+}$ such that $(a, b) = 1$ (primitive) and $|Norm_{K^+/\mathbb{Q}}(abc)| > 1$ (non-trivial) to

$$f_1(x, y)f_2(x, y) = \mu z^p \quad \text{or} \tag{5.1}$$

$$f_1(x,y)f_2(x,y) = \mu\pi_r^2 z^p, \tag{5.2}$$

which satisfies $r \nmid a+b$ *in case* (5.1) *and* $r \mid a+b$ *in case* (5.2). *Moreover:*

- *if* $d \mid C$, *then* $d \mid a+b$;
- *the primes in* K^+ *divisors of* c *are all above primes of* $\mathbb{Q}$ *that are congruent to* 1 (mod r). *In particular, neither the primes above* 2 *nor the primes above* r *divide* c.

Proof: Exactly the same proof of Lemma 3.2.9 where we use only the two factors f_i in the statement.

■

We are now going to construct Frey curves attached to solutions of equations (5.1) or (5.2). The curves will be defined over K^+ and then we will show that they are k-curves.

In order to construct a useful k-curve we first need to find α, β such that

$$(a+b)^2 = \alpha f_1(a,b) + \beta f_2(a,b).$$

That is, solve the linear system

$$\begin{cases} \alpha + \beta = 1 \\ \alpha(\zeta + \zeta^{4m}) + \beta\sigma^m(\zeta + \zeta^{4m}) = 2, \end{cases}$$

which has a solution for $\alpha, \beta \in K^+$ given by

$$\begin{cases} \alpha = (\sigma^m(\zeta + \zeta^{4m}) - 2)(\sigma^m(\zeta + \zeta^{4m}) - \zeta^{4m} - \zeta)^{-1} \\ \beta = (2 - (\zeta + \zeta^{4m}))(\sigma^m(\zeta + \zeta^{4m}) - \zeta - \zeta^{4m})^{-1}, \end{cases}$$

that easily can be seen to satisfy $\sigma^m(\alpha) = \beta$. Now, given a putative solution (a,b,c) to (5.1) or (5.2) we can consider the Frey curves of the form $y^2 = x^3 + a_2x^2 + a_4x$ defined over K^+ and given by

$$E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 + \alpha f_1(a,b)x.$$

Their Galois conjugate by σ^m is given by

$${}^{\sigma^m}E_{(a,b)} : y^2 = x^3 + 2(a+b)x^2 + \beta f_2(a,b)x,$$

and they admit a 2-isogeny $\mu : {}^{\sigma^m}E \to E$ given by

$$(x,y) \mapsto (-\frac{y^2}{2x^2}, \frac{\sqrt{-2}}{4}\frac{y}{x^2}(-\beta f_2 + x^2)).$$

The dual isogeny $\hat{\mu} : E \to {}^{\sigma}E$ is given by

$$(x,y) \mapsto (-\frac{y^2}{2x^2}, -\frac{\sqrt{-2}}{4}\frac{y}{x^2}(-\alpha f_1 + x^2)).$$

This shows that $E_{(a,b)}$ is a k-curve with $K^+(\sqrt{-2})$ as a field of complete definition. From the proof of Lemma 5.0.2 we know that $f_i(a,b) = \mu_i c_i$ or $f_i(a,b) = \mu_i \pi_r c_i$, with c_1, c_2 coprime. We now compute the discriminant of $E = E_{(a,b)}$

$$\Delta(E) = 16a_4^2(a_2^2 - 4a_4) = 16\alpha^2\beta(4(a+b)^2 - 4\alpha f_1) = 64\alpha^2\beta f_1^2 f_2.$$

In particular,

$$\Delta(E) = \begin{cases} \mu\mu_1 2^6\alpha^2\beta c^p & \text{if } r \nmid a+b, \\ \mu\mu_1 2^6\alpha^2\beta\pi_r^3 c^p & \text{if } r \mid a+b. \end{cases}$$

Moreover, the following quantities are also associated with E

$$\begin{aligned} c_4(E) &= 2^4(\alpha f_1 + 2^2\beta f_2), \\ c_6(E) &= 2^6(a+b)(\alpha f_1 - 2^3\beta f_2) \end{aligned}$$

Proposition 5.0.3 *Let (a,b,c) be a primitive solution to* (5.1) *or* (5.2)*. Then, the conductor of the curves $E_{(a,b)}$ is given by*

$$N_E = \begin{cases} 2^s rad(c) & \text{if } r \nmid a+b, \\ 2^s\pi_r^2 rad(c) & \text{if } r \mid a+b, \end{cases}$$

where $s = 5$ or $s = 6$.

Proof: Recall that μ, μ_i are units. We will now see that α, β are also units. First we observe that the elements of the form $\zeta^c(1-\zeta^a)(1-\zeta^b)$, where $a, b \not\equiv 0 \pmod r$ are divisible only by the prime ideal $(\pi_r) \mid r$ and their (π_r)-adic valuation is 1. Moreover,

$$\zeta^c(1-\zeta^a)(1-\zeta^b) = \zeta^c - \zeta^{a+c} - \zeta^{b+c} + \zeta^{a+b+c} = \zeta^x - \zeta^y - \zeta^z + \zeta^{y+z-x},$$

where the last equality is a change of variables. Note that $2 - \zeta - \zeta^{-1} = (1-\zeta)(1-\zeta^{-1})$ is the numerator of β. Also, $\sigma^m(\zeta + \zeta^{-1}) = \zeta^k + \zeta^{-k}$ for some integer k, then the denominator of β is of the form $\zeta^k - \zeta - \zeta^{-1} + \zeta^{-k}$. Since both numerator and denominator of β are of the shape above we conclude that β is a unit, hence $\alpha = \sigma^m(\beta)$ is also a unit.

Let $\mathfrak{q} \mid c$ be a prime in K^+. We have $v_\mathfrak{q}(\Delta) > 0$ and since $\mathfrak{q}$ divides only one of the c_i it is clear from the form of c_4 that $v_\mathfrak{q}(c_4) = 0$, thus the reduction is multiplicative at $\mathfrak{q}$.

Let $\mathfrak{q} \mid 2$. We have $v_\mathfrak{q}(\Delta) = 6$, $v_\mathfrak{q}(c_4) = 4$, $v_\mathfrak{q}(c_6) = 6$, hence the equation is minimal and $v_\mathfrak{q}(N_E) = 5$ or 6 by Table IV in [52].

Let $\mathfrak{q} = (\pi_r)$. Then $v_\mathfrak{q}(\Delta) = 0$ or $v_\mathfrak{q}(\Delta) = 3$ if $r \nmid a+b$ or $r \mid a+b$, respectively. In particular, $v_\mathfrak{q}(N_E) = 0$ (good reduction) if $r \nmid a+b$. Suppose $r \mid a+b$, then $v_\mathfrak{q}(f_i(a,b)) = 1$, hence $v_\mathfrak{q}(c_4) > 0$. Thus E has additive reduction and $v_\mathfrak{q}(N_E) = 2$ by Table I in [52].

■

The next theorem shows that the curves $E_{(a,b)}$ have the necessary properties in order to be used as Frey curves. In particular, we can combine them with those constructed in Chapter 3 and apply a multi-Frey technique. Unfortunately, in practice we can not do it, because already for $r = 13$ we can not compute the relevant newspaces.

Theorem 5.0.4 *Let (a, b, c) be a primitive solution to* (5.1) *or* (5.2)*. Let $\bar{\rho}_{E,p}$ be the mod p Galois representation arising from the p-torsion of $E_{(a,b)}$. Then,*

1. *The mArtin conductor of $\bar{\rho}_{E,p}$ is not divisible by primes dividing c.*
2. *$\bar{\rho}_{E,p}$ is finite at all primes $\mathfrak{p}$ dividing p.*

Proof: Part (1) follows as in the proof of Proposition The Artin conductor is not divisible by primes dividing p by definition. Let $l \nmid p$ be a prime dividing c, hence l is of multiplicative reduction by Proposition 5.0.3. l is unramified in K^+ because $l \nmid r$. Since it appears to a p-th power in the discriminant of a minimal model at l of E ($\Delta(E)$) we know by Theorem 1.1.14 that the representation $\bar{\rho}_{E,p}$ will not ramify at l. This proves 1.

Let $\mathfrak{p} \mid p$. If $\mathfrak{p} \nmid c$ it is of good reduction for E then $\bar{\rho}_{E,p}$ is finite by Lemma 1.2.5; if $\mathfrak{p} \mid c$ it is of multiplicative reduction for E and since we have $p \mid \upsilon_{\mathfrak{p}}(\Delta)$ it follows from Lemma 1.2.5 that $\bar{\rho}_{E,p}$ is finite. We have proved 2.

■

Proposition 5.0.5 *Let $(a, b, c) \in \mathbb{Z}^2 \times \mathcal{O}_{K^+}$ be a non-trivial primitive solution to* (5.1) *or* (5.2)*. Then $E_{(a,b)}$ has no complex multiplication.*

Proof: $|Norm_{K^+/\mathbb{Q}}(abc)| > 1$ hence $|ab| > 1$ or there is some prime $\mathfrak{p}$ dividing c. In the latter case, the prime $\mathfrak{p} \mid c$ is of multiplicative reduction by Proposition 5.0.3, hence E can not have complex multiplication. Suppose $|ab| > 1$. From the proof of Corollary 3.2.10 we know that for all i, $(a + \zeta^i b)(a + \zeta^{r-i} b)$ is divisible by some prime, hence c is divisible by some prime. Again, this prime is of multiplicative reduction and E can not have CM.

■

Remark 5.0.6 *By looking for α, β such that $(a - b)^2 = \alpha f_1(a, b) + \beta f_2(a, b)$ we can use an analogous construction to get another Frey curve F. The same type of properties proved for E so far would also hold for F.*

The definitions and properties that we use in what follows are generalizations of the work of Quer with $\mathbb{Q}$-curves. Details on the generalizations can be found in X. Guitart thesis (see [34]).

Let (a, b, c) be a non-trivial primitive solution to (5.1) or (5.2) and denote $E_{(a,b)}$ simply by E. From Proposition 5.0.5 E has no complex multiplication. Since E is a k-curve we have for each element $g \in G_k$ an isogeny $\phi_g : {}^g E \to E$ by definition. Analogously to what

we have done in Section 2.3, from this family of isogenies, we can attach to E a 2-cocycle $c_E : G_k \times G_k \to \mathbb{Q}^*$ defined by $c_E(g,h) = \phi_g{}^g \phi_h \phi_{gh}^{-1}$. Let $\xi(E) \in H^2(G_k, \mathbb{Q}^*)[2]$ denote its cohomology class, K_d be a field of complete definition of E and $G = \mathrm{Gal}(K_d/k)$. There is also an analogous cohomology class $[c_{E/K_d}] \in H^2(G, \mathbb{Q}^*)[2]$ that satisfies $\mathrm{Inf}_G^{G_k}[c_{E/K_d}] = \xi(E)$. Moreover, $B = \mathrm{Res}_{K_d/k}(E/K_d)$ has endomorphism algebra isomorphic to the twisted group algebra $\mathbb{Q}^{c_{E/K_d}}[G]$ (Proposition 5.32 in [34]) and B is a product of abelian varieties of GL_2-type if and only if $\mathbb{Q}^{c_{E/K_d}}[G]$ is abelian (Proposition 5.36 in [34]). If G is abelian then the algebra $\mathbb{Q}^{c_{E/K_d}}[G]$ is abelian if and only if the the cocycle c_{E/K_d} is symmetric. Moreover, from Proposition 3.22 in [34] we have a non-canonical isomorphism

$$H^2(G, \mathbb{Q}^*)[2] \simeq H^2(G, \{\pm 1\}) \times \mathrm{Hom}(G, P/P^2)$$

where $P = \mathbb{Q}^*/\{\pm 1\}$. The elements in $\mathrm{Hom}(G, P/P^2)$ are symmetric (because G is abelian) then c_{E/K_d} is symmetric if and only if its component in $H^2(G, \{\pm 1\})$, denoted $c^{\pm}_{E/K_d}$, is symmetric.

We now particularize to our curves. Observe that $K^+ = k(\sqrt{s})$ for some $s \in k$ and take $K_d = k(\sqrt{s}, \sqrt{-2})$ as field of complete definition of E. In this case G is abelian with generators τ and σ^m, where

$$\begin{cases} \sigma^m(\sqrt{s}) = -\sqrt{s} & \text{and} \quad \sigma^m(\sqrt{-2}) = \sqrt{-2} \\ \tau(\sqrt{s}) = \sqrt{s} & \text{and} \quad \tau(\sqrt{-2}) = -\sqrt{-2} \end{cases}$$

The values of c_{E/K_d} were computed from the expressions of μ and $\hat{\mu}$ an can be found in Table 5.1. The sign component $c^{\pm}_{E/K_d}$ is not symmetric and is given by the signs in the same table.

		h			
		1	τ	σ^m	$\sigma^m\tau$
g	1	1	1	1	1
	τ	1	1	-1	-1
	σ^m	1	1	-2	-2
	$\sigma^m\tau$	1	1	2	2

Table 5.1: Values of c_{E/K_d}

Thus we need to look for another field of complete definition K_β satisfying that c_{E/K_β} is symmetric. To achieve this we are going to use the theory on of Quer on embedding problems. A few computations shows that $c^{\pm}_{E/K_d} = c_{-2s,s}$ (we are using the notation in section 2.3.2) then $\mathrm{Inf}_G^{G_k}(c^{\pm}_{E/K_d}) \in H^2(G_k, \{\pm 1\})[2] \simeq \mathrm{Br}_2(k)$ is the quaternion algebra $(-2s, s)$. At this point our aim is to apply Theorem 2.3.4. An application of this theorem is dependent on the value of r, nevertheless in what follows we will show that if m is odd and 2 inert in k it can be done in general.

Suppose $r = 4m + 1$ with m odd. We have $\mathbb{Q}(\sqrt{r}) \subset K^+$ we also have $k(\sqrt{r}) \subset K^+$ and both fields have degree $2m$ thus $K^+ = k(\sqrt{r})$.

Proposition 5.0.7 *Suppose that $r = 4m + 1$ with m odd. If 2 is inert in k then the discriminant of $(-2r, r)$ is $2r$.*

Proof: Let $\mathfrak{P}_r$ be the prime in k above r. If $-2rx^2 + ry^2 - z^2$ represents 0 in $k_{\mathfrak{P}_r} = \mathbb{Q}_r$ then $\mathfrak{P}_r \mid z$ and so $-2x^2 + y^2 \equiv 0 \pmod{\mathfrak{P}_r}$ hence 2 is a square modulo r. Since 2 is never a square modulo $r = 4m + 1$ for m odd we conclude that $(-2r, r)_{\mathfrak{P}_r} = -1$. On one hand, $\iota(-2r), \iota(r)$ have opposite signs for all real places ι of L we conclude that $(-2r, r)$ is not ramified at the infinity primes. On the other hand, $(-2r, r)$ must ramify at an even number of places then the result follows.

■

Let ϵ be a character of $G_{\mathbb{Q}}$ with order 4 and conductor $2^2 r$ thus fixing a totally real cyclic number field K_ϵ. Put $k_\epsilon = K_\epsilon k$, $A = \{-2r\}$, $B = \{r\}$ and according to the notation in section 2.3.2 consider the field $K = LMN = k_\epsilon k(\sqrt{-2r})k$ with Galois group $G = \mathrm{Gal}(K/k)$. Note that $k(\sqrt{r}) \subset k_\epsilon$ and $K_d \subset K$. Let c_ϵ as in section 2.3.2 and $c = \theta_\epsilon c_{A,B}$, where $\theta_\epsilon = \mathrm{Inf}^G_{\mathrm{Gal}(k_\epsilon/k)}[c_\epsilon]$ and $c_{A,B} = \mathrm{Inf}^G_{\mathrm{Gal}(K_d/k)}[c_{-2s,s}]$. After identifying $\mathrm{Inf}^{G_k}_G[\theta_\epsilon]$ with an element of $\mathrm{Br}_2(k)$ we can identify it with an element in $\oplus \mathrm{Br}_2(k_v)$ using the known exact sequence on Brauer groups

$$0 \longrightarrow \mathrm{Br}_2(k) \longrightarrow \oplus \mathrm{Br}_2(k_v) \longrightarrow \{\pm 1\} \longrightarrow 0$$

Now if v is a finite prime the component $(\mathrm{Inf}^{G_k}_G[\theta_\epsilon])_v$ in $\mathrm{Br}_2(k_v)$ is given by the parity of the v-component of ϵ, $\epsilon_v(-1)$. Moreover, k_ϵ is totally real hence $(\mathrm{Inf}^{G_k}_G[\theta_\epsilon])_v = 1$ for all infinite primes v of k. Since $\epsilon_2(-1) = \epsilon_r(-1) = 1$ we have that $(\mathrm{Inf}^{G_k}_G[\theta_\epsilon]) = (-2r, r)$ and the embedding problem $(K/k, \{\pm 1\}, [c])$ is unobstructed because

$$\mathrm{Inf}^{G_k}_G[c] = (\mathrm{Inf}^{G_k}_G[\theta_\epsilon])(\mathrm{Inf}^{G_k}_G[c_{A,B}]) = (-2r, r)(-2r, r) = 1 \in \mathrm{Br}_2(k).$$

Now we see from Theorem 2.3.4 that there must exist elements α_0 and α_1 in $k_\epsilon(\sqrt{-2})$ such that

$$\begin{aligned} N_{\sigma_0}(\alpha_0) &= -1 \\ N_{\sigma_1}(\alpha_1) &= r \\ \frac{{}^{\sigma_1}\alpha_0}{\alpha_0} &= \frac{{}^{\sigma_0}\alpha_1}{\alpha_1}. \end{aligned}$$

For example, suppose that δ is an element of k_ϵ such that $\mathrm{Nm}_{k_\epsilon/k}(\delta) = -4$ and take $\alpha_0 = \frac{\delta}{2}\sqrt{-2}$, $\alpha_1 = \sqrt{r}$. The same Theorem 2.3.4 also gives us a splitting map β for the cocycle c. We observe that in particular $\beta_{\sigma_1} = \alpha_1/\sqrt{r} = 1$, which means that we actually have a splitting map for $[c_\epsilon]$. Now we pick a solution $\gamma \in k_\epsilon$ to the embedding

problem and by construction the twisted curve E_γ satisfies that $c^{\pm}_{E_\gamma/k_\epsilon}$ is symmetric. Thus, as we explained before $B = \mathrm{Res}_{k_\epsilon/k}(E/k_\epsilon)$ is a product of abelian varieties of GL_2 type over k and our initial representation $\rho_{E,p}$ of G_{K^+} extends to G_k. At this point a suitable generalization of Theorem 5.12 in [53] and Theorem 5.4 in [54] would give a description of the exact decomposition of B and the character of $\rho_{E,p}$. We could then compute the exact conductor of an extension of $\rho_{E,p}$ to G_k and proceed with the modular approach. We do not go further in this direction since the spaces of relevant newforms that we would need are already impossible to compute for $r = 13$. For $r = 13$ we need to compute HMF over a cubic field with level of large norm. For $r = 5$ then $k = \mathbb{Q}$ and we are in the case of Chapter 2.

Chapter 6

Appendix

In section 6.1 we provide the tables with the values of $a_L(f)$ of the newforms of level 2^3w^2 and 2^4w^2 such that $\mathbb{Q}_f = \mathbb{Q}$ used in section 4.2. In sec. 6.2 we give the factorization of the polnomial p_3 also used there.

6.1 Tables with values $a_L(f)$

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
-3	-3	-3	-3	-4	-4	-9	2	2	-13	-18
-3	-1	-5	-1	-9	5	-6	1	-3	-5	15
-3	-1	-1	3	3	9	2	-7	5	11	15
-3	-1	1	-3	-3	-9	-2	-7	5	-11	-15
-3	-1	5	1	9	-5	6	1	-3	5	-15
-3	1	-7	-7	3	-1	6	7	-9	1	9
-3	1	7	7	-3	1	-6	7	-9	-1	-9
-1	-3	-3	1	-9	-3	-2	5	-7	-11	-15
-1	-3	-1	-5	5	-9	-6	-3	1	-5	15
-1	-3	1	5	-5	9	6	-3	1	5	-15
-1	-3	3	-1	9	3	2	5	-7	11	15
-1	-1	3	3	-6	-6	1	0	0	5	22
-1	1	-7	-3	-1	-7	-2	-7	-3	1	-3
-1	1	-5	7	5	3	-6	1	5	-1	3
-1	1	5	-7	-5	-3	6	1	5	1	-3
-1	1	7	3	1	7	2	-7	-3	-1	3
-1	3	-1	7	2	2	-7	-8	0	1	6
-1	3	1	-7	-2	-2	7	-8	0	-1	-6
0	0	6	6	8	8	-6	2	2	-10	-18
1	-3	-7	-7	-1	3	6	-9	7	1	9
1	-3	7	7	1	-3	-6	-9	7	-1	-9
1	-1	-7	5	-3	-5	6	5	1	1	-3

Table 6.1: a_L values for newforms of level 2^3w^2

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
1	-1	-3	-7	-7	-1	-2	-3	-7	1	-3
1	-1	3	7	7	1	2	-3	-7	-1	3
1	-1	7	-5	3	5	-6	5	1	-1	3
1	1	-3	-3	-1	-1	6	3	3	13	21
1	1	-3	-3	0	0	-1	6	6	-13	14
1	1	-3	-3	4	4	-9	-6	-6	11	-18
1	1	3	3	-4	-4	9	-6	-6	-11	18

Table 6.2: a_L values for newforms of level 2^3w^2 (cont)

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
1	1	3	3	1	1	-6	3	3	-13	-21
3	-1	-7	1	-2	-2	7	0	-8	-1	-6
3	-1	7	-1	2	2	-7	0	-8	1	6
-3	-3	-3	-3	-1	-1	6	-1	-1	13	-3
-3	-3	3	3	1	1	-6	-1	-1	-13	3
-3	-1	-7	-7	-3	-1	-6	-7	9	1	9
-3	-1	-7	1	-2	2	-7	0	8	-1	-6
-3	-1	7	-1	2	-2	7	0	8	1	6
-3	-1	7	7	3	1	6	-7	9	-1	-9
-3	1	-7	1	2	2	7	0	-8	-1	-6
-3	1	-5	-1	9	5	6	-1	3	-5	15
-3	1	-1	3	-3	9	-2	7	-5	11	15
-3	1	1	-3	3	-9	2	7	-5	-11	-15
-3	1	5	1	-9	-5	-6	-1	3	5	-15
-3	1	7	-1	-2	-2	-7	0	-8	1	6
-3	3	-3	-3	1	-1	-6	1	1	13	-3
-3	3	-3	-3	4	-4	9	-2	-2	-13	-18
-3	3	3	3	-4	4	-9	-2	-2	13	18
-3	3	3	3	-1	1	6	1	1	-13	3
-2	-2	-3	-3	6	6	7	3	3	14	22
-2	-2	3	3	-6	-6	-7	3	3	-14	-22
-2	2	-3	-3	-6	6	-7	-3	-3	14	22
-2	2	-3	-3	-6	6	-1	-9	-9	-2	22

Table 6.3: a_L values for newforms of level 2^4w^2

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
-2	2	3	3	6	-6	1	-9	-9	2	-22
-2	2	3	3	6	-6	7	-3	-3	-14	-22
-1	-3	-7	-7	-1	-3	-6	9	-7	1	9
-1	-3	-1	7	-2	2	7	8	0	1	6
-1	-3	1	-7	2	-2	-7	8	0	-1	-6
-1	-3	7	7	1	3	6	9	-7	-1	-9
-1	-1	-7	-3	1	-7	2	7	3	1	-3
-1	-1	-7	5	-3	5	-6	-5	-1	1	-3
-1	-1	-5	7	-5	3	6	-1	-5	-1	3
-1	-1	-3	-7	-7	1	2	3	7	1	-3
-1	-1	-3	-3	1	1	6	3	3	13	21
-1	-1	3	3	-1	-1	-6	3	3	-13	-21
-1	-1	3	3	0	0	1	6	6	13	-14
-1	-1	3	3	4	4	9	-6	-6	-11	18
-1	-1	3	7	7	-1	-2	3	7	-1	3
-1	-1	5	-7	5	-3	-6	-1	-5	1	-3
-1	-1	7	-5	3	-5	6	-5	-1	-1	3
-1	-1	7	3	-1	7	-2	7	3	-1	3
-1	1	-7	5	3	5	6	5	1	1	-3
-1	1	-3	-7	7	1	-2	-3	-7	1	-3
-1	1	-3	-3	-6	6	1	0	0	-5	-22
-1	1	-3	-3	-1	1	-6	-3	-3	13	21
-1	1	-3	-3	0	0	1	-6	-6	-13	14
-1	1	-3	-3	3	-3	10	9	9	-11	5
-1	1	-3	-3	4	-4	9	6	6	11	-18
-1	1	3	3	-4	4	-9	6	6	-11	18
-1	1	3	3	-3	3	-10	9	9	11	-5
-1	1	3	3	0	0	-1	-6	-6	13	-14
-1	1	3	3	1	-1	6	-3	-3	-13	-21
-1	1	3	3	6	-6	-1	0	0	5	22
-1	1	3	7	-7	-1	2	-3	-7	-1	3
-1	1	7	-5	-3	-5	-6	5	1	-1	3
-1	3	-7	-7	1	-3	6	-9	7	1	9
-1	3	-3	1	9	-3	2	-5	7	-11	-15
-1	3	-1	-5	-5	-9	6	3	-1	-5	15
-1	3	1	5	5	9	-6	3	-1	5	-15

Table 6.4: a_L values for newforms of level 2^4w^2 (cont.)

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
-1	3	3	-1	-9	3	-2	-5	7	11	15
-1	3	7	7	-1	3	-6	-9	7	-1	-9
0	0	-6	-6	-8	8	-6	-2	-2	10	18
0	0	-6	-6	8	-8	-6	-2	-2	10	18
0	0	-6	-6	8	8	6	2	2	10	18
0	0	-3	-3	-4	-4	9	-1	-1	-2	6
0	0	-3	-3	-4	4	-9	1	1	-2	6
0	0	-3	-3	4	-4	-9	1	1	-2	6
0	0	3	3	-4	4	9	1	1	2	-6
0	0	3	3	4	-4	9	1	1	2	-6
0	0	3	3	4	4	-9	-1	-1	2	-6
0	0	6	6	-8	-8	-6	2	2	-10	-18
0	0	6	6	-8	8	6	-2	-2	-10	-18
0	0	6	6	8	-8	6	-2	-2	-10	-18
1	-3	-3	1	-9	3	2	-5	7	-11	-15
1	-3	-1	-5	5	9	6	3	-1	-5	15
1	-3	-1	7	-2	-2	-7	-8	0	1	6
1	-3	1	-7	2	2	7	-8	0	-1	-6
1	-3	1	5	-5	-9	-6	3	-1	5	-15
1	-3	3	-1	9	-3	-2	-5	7	11	15
1	-1	-7	-3	1	7	-2	-7	-3	1	-3
1	-1	-5	7	-5	-3	-6	1	5	-1	3
1	-1	-3	-3	-4	4	9	6	6	11	-18
1	-1	-3	-3	-3	3	10	9	9	-11	5
1	-1	-3	-3	0	0	1	-6	-6	-13	14
1	-1	-3	-3	1	-1	-6	-3	-3	13	21
1	-1	-3	-3	6	-6	1	0	0	-5	-22
1	-1	3	3	-6	6	-1	0	0	5	22
1	-1	3	3	-1	1	6	-3	-3	-13	-21
1	-1	3	3	0	0	-1	-6	-6	13	-14
1	-1	3	3	3	-3	-10	9	9	11	-5
1	-1	3	3	4	-4	-9	6	6	-11	18
1	-1	5	-7	5	3	6	1	5	1	-3

Table 6.5: a_L values for newforms of level 2^4w^2 (cont.)

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
1	-1	7	3	-1	-7	2	-7	-3	-1	3
1	1	-7	-3	-1	7	2	7	3	1	-3
1	1	-7	5	3	-5	-6	-5	-1	1	-3
1	1	-5	7	5	-3	6	-1	-5	-1	3
1	1	-3	-7	7	-1	2	3	7	1	-3
1	1	-3	-3	-6	-6	-1	0	0	-5	-22
1	1	-3	-3	3	3	-10	-9	-9	-11	5
1	1	3	3	-3	-3	10	-9	-9	11	-5
1	1	3	3	6	6	1	0	0	5	22
1	1	3	7	-7	1	-2	3	7	-1	3
1	1	5	-7	-5	3	-6	-1	-5	1	-3
1	1	7	-5	-3	5	6	-5	-1	-1	3
1	1	7	3	1	-7	-2	7	3	-1	3
1	3	-7	-7	1	3	-6	9	-7	1	9
1	3	-3	1	9	3	-2	5	-7	-11	-15
1	3	-1	-5	-5	9	-6	-3	1	-5	15
1	3	-1	7	2	-2	7	8	0	1	6
1	3	1	-7	-2	2	-7	8	0	-1	-6
1	3	1	5	5	-9	6	-3	1	5	-15
1	3	3	-1	-9	-3	2	5	-7	11	15
1	3	7	7	-1	-3	6	9	-7	-1	-9
2	-2	-3	-3	6	-6	-7	-3	-3	14	22
2	-2	-3	-3	6	-6	-1	-9	-9	-2	22
2	-2	3	3	-6	6	1	-9	-9	2	-22
2	-2	3	3	-6	6	7	-3	-3	-14	-22
2	2	-3	-3	-6	-6	1	9	9	-2	22
2	2	3	3	6	6	-1	9	9	2	-22
3	-3	-3	-3	-4	4	9	-2	-2	-13	-18
3	-3	-3	-3	-1	1	-6	1	1	13	-3
3	-3	3	3	1	-1	6	1	1	-13	3
3	-3	3	3	4	-4	-9	-2	-2	13	18

Table 6.6: a_L values for newforms of level 2^4w^2 (cont.)

$a_{L_3^0}$	$a_{L_3^1}$	$a_{L_{17}^0}$	$a_{L_{17}^1}$	$a_{L_{23}^0}$	$a_{L_{23}^1}$	a_{L_5}	$a_{L_{29}^0}$	$a_{L_{29}^1}$	a_{L_7}	$a_{L_{11}}$
3	-1	-7	-7	-3	1	6	7	-9	1	9
3	-1	-5	-1	-9	-5	6	-1	3	-5	15
3	-1	-1	3	3	-9	-2	7	-5	11	15
3	-1	1	-3	-3	9	2	7	-5	-11	-15
3	-1	5	1	9	5	-6	-1	3	5	-15
3	-1	7	7	3	-1	-6	7	-9	-1	-9
3	1	-7	-7	3	1	-6	-7	9	1	9
3	1	-7	1	2	-2	-7	0	8	-1	-6
3	1	-5	-1	9	-5	-6	1	-3	-5	15
3	1	-1	3	-3	-9	2	-7	5	11	15
3	1	1	-3	3	9	-2	-7	5	-11	-15
3	1	5	1	-9	5	6	1	-3	5	-15
3	1	7	-1	-2	2	7	0	8	1	6
3	1	7	7	-3	-1	6	-7	9	-1	-9
3	3	-3	-3	4	4	-9	2	2	-13	-18
3	3	3	3	-4	-4	9	2	2	13	18
-1	-1	-3	-3	-4	-4	-9	-6	-6	11	-18
-1	-1	-3	-3	0	0	-1	6	6	-13	14

Table 6.7: a_L values for newforms of level 2^4w^2 (cont.)

6.2 Factorization of p_3

The polynomial p_3 on $S_2(2^4w^2)$ has the following factors:

$[x-3,38],[x-2,16],[x-1,84],[x,32],[x+1,92],[x+2,12],[x+3,45][x^2-4x+2,6],[x^2-3x-1,17],[x^2-3x+1,39],[x^2-2x-2,4],[x^2-2x-1,10],[x^2-x-5,18],[x^2-x-4,23],[x^2-x-3,33],[x^2-x-1,25],[x^2-8,10],[x^2-5,12],[x^2-3,20],[x^2-2,10],[x^2+x-5,6],[x^2+x-4,22],[x^2+x-3,42],[x^2+x-1,30],[x^2+2x-2,10],[x^2+2x-1,4],[x^2+3x-1,21],[x^2+3x+1,37],[x^2+4x+2,4],[x^3-4x^2+3x+1,4],[x^3-3x^2-4x+13,10],[x^3-2x^2-4x+7,6],[x^3-2x^2-x+1,4],[x^3-7x-7,4],[x^3-7x+7,8],[x^3-4x-1,9],[x^3-4x+1,6],[x^3+2x^2-4x-7,9],[x^3+2x^2-x-1,12],[x^3+3x^2-4x-13,4],[x^3+4x^2+3x-1,6],[x^4-4x^3-x^2+10x+2,6],[x^4-4x^3+8x-1,4],[x^4-3x^3-6x^2+23x-13,4],[x^4-2x^3-9x^2+22x-11,12],[x^4-2x^3-7x^2+8x-1,6],[x^4-2x^3-7x^2+8x+4,4],[x^4-2x^3-6x^2+10x+1,14],[x^4-2x^3-4x^2+8x-2,4],[x^4+2x^3-9x^2-22x-11,6],[x^4+2x^3-7x^2-8x-1,9],[x^4+2x^3-7x^2-8x+4,6],[x^4+2x^3-6x^2-10x+1,8],[x^4+2x^3-4x^2-8x-2,10],[x^4+3x^3-6x^2-23x-13,6],[x^4+4x^3-x^2-10x+2,4],[x^4+4x^3-8x-1,8],[x^6-3x^5-12x^4+36x^3+18x^2-68x+29,10],[x^6-3x^5-11x^4+31x^3+15x^2-25x-4,9],[x^6-3x^5-9x^4+23x^3+15x^2-13x-1,6],[x^6-2x^5-11x^4+16x^3+35x^2-26x-25,4],[x^6-x^5-13x^4+11x^3+49x^2-27x-52,9],[x^6+x^5-13x^4-11x^3+49x^2+27x-52,6],[x^6+2x^5-11x^4-16x^3+35x^2+26x-25,8],[x^6+3x^5-12x^4-36x^3+18x^2+68x+29,4],[x^6+3x^5-11x^4-31x^3+15x^2+25x-4,6],[x^6+3x^5-9x^4-23x^3+15x^2+13x-1,4],[x^8-6x^7+x^6+48x^5-65x^4-54x^3+115x^2-48x+4,8],[x^8-3x^7-20x^6+57x^5+124x^4-327x^3-245x^2+588x+16,4],[x^8+3x^7-20x^6-57x^5+124x^4+327x^3-245x^2-588x+16,2],[x^8+6x^7+$

$x^6-48x^5-65x^4+54x^3+115x^2+48x+4,4],[x^9-4x^8-9x^7+50x^6-5x^5-156x^4+125x^3+50x^2-40x+4,6],[x^9-3x^8-11x^7+32x^6+38x^5-100x^4-47x^3+75x^2+37x+4,4],[x^9-2x^8-17x^7+34x^6+75x^5-158x^4-31x^3+106x^2-20x-4,4],[x^9-x^8-19x^7+16x^6+114x^5-76x^4-251x^3+165x^2+181x-128,6],[x^9+x^8-19x^7-16x^6+114x^5+76x^4-251x^3-165x^2+181x+128,4],[x^9+2x^8-17x^7-34x^6+75x^5+158x^4-31x^3-106x^2-20x+4,6],[x^9+3x^8-11x^7-32x^6+38x^5+100x^4-47x^3-75x^2+37x-4,6],[x^9+4x^8-9x^7-50x^6-5x^5+156x^4+125x^3-50x^2-40x-4,4],[x^{12}-x^{11}-22x^{10}+30x^9+153x^8-276x^7-317x^6+863x^5-182x^4-513x^3+242x^2+22x-1,4],[x^{12}+x^{11}-22x^{10}-30x^9+153x^8+276x^7-317x^6-863x^5-182x^4+513x^3+242x^2-22x-1,8],[x^{16}-2x^{15}-26x^{14}+48x^{13}+261x^{12}-442x^{11}-1300x^{10}+2024x^9+3449x^8-4958x^7-4874x^6+6520x^5+3355x^4-4294x^3-776x^2+1104x-74,6],[x^{16}+2x^{15}-26x^{14}-48x^{13}+261x^{12}+442x^{11}-1300x^{10}-2024x^9+3449x^8+4958x^7-4874x^6-6520x^5+3355x^4+4294x^3-776x^2-1104x-74,4],[x^{18}-6x^{17}-22x^{16}+184x^{15}+101x^{14}-2206x^{13}+1048x^{12}+13080x^{11}-12983x^{10}-39490x^9+52906x^8+54352x^7-91701x^6-23122x^5+56412x^4+5600x^3-13034x^2-1480x+568,4],[x^{18}-4x^{17}-33x^{16}+150x^{15}+387x^{14}-2233x^{13}-1578x^{12}+16799x^{11}-4197x^{10}-65971x^9+59322x^8+117310x^7-188308x^6-21264x^5+190984x^4-132221x^3+32604x^2-1200x-379,6],[x^{18}-3x^{17}-28x^{16}+82x^{15}+318x^{14}-915x^{13}-1870x^{12}+5426x^{11}+5939x^{10}-18603x^9-9152x^8+37297x^7+2528x^6-41228x^5+10028x^4+20669x^3-9779x^2-1970x+1259,4],[x^{18}-3x^{17}-28x^{16}+84x^{15}+308x^{14}-921x^{13}-1692x^{12}+4994x^{11}+4927x^{10}-13943x^9-7648x^8+19011x^7+6382x^6-10700x^5-3212x^4+2003x^3+627x^2-20x-1,4],[x^{18}-3x^{17}-26x^{16}+78x^{15}+270x^{14}-815x^{13}-1436x^{12}+4416x^{11}+4153x^{10}-13377x^9-6258x^8+22693x^7+3772x^6-20184x^5+782x^4+7699x^3-1277x^2-514x+13,4],[x^{18}-3x^{17}-26x^{16}+80x^{15}+264x^{14}-837x^{13}-1362x^{12}+4500x^{11}+3737x^{10}-13433x^9-4682x^8+22123x^7-202x^6-18304x^5+5878x^4+5249x^3-3531x^2+688x-43,4],[x^{18}-2x^{17}-34x^{16}+64x^{15}+461x^{14}-802x^{13}-3208x^{12}+4968x^{11}+12385x^{10}-15862x^9-26994x^8+24760x^7+31587x^6-14558x^5-16140x^4-640x^3+910x^2+56x-8,6],[x^{18}+2x^{17}-34x^{16}-64x^{15}+461x^{14}+802x^{13}-3208x^{12}-4968x^{11}+12385x^{10}+15862x^9-26994x^8-24760x^7+31587x^6+14558x^5-16140x^4+640x^3+910x^2-56x-8,4],[x^{18}+3x^{17}-28x^{16}-84x^{15}+308x^{14}+921x^{13}-1692x^{12}-4994x^{11}+4927x^{10}+13943x^9-7648x^8-19011x^7+6382x^6+10700x^5-3212x^4-2003x^3+627x^2+20x-1,6],[x^{18}+3x^{17}-28x^{16}-82x^{15}+318x^{14}+915x^{13}-1870x^{12}-5426x^{11}+5939x^{10}+18603x^9-9152x^8-37297x^7+2528x^6+41228x^5+10028x^4-20669x^3-9779x^2+1970x+1259,8],[x^{18}+3x^{17}-26x^{16}-80x^{15}+264x^{14}+837x^{13}-1362x^{12}-4500x^{11}+3737x^{10}+13433x^9-4682x^8-22123x^7-202x^6+18304x^5+5878x^4-5249x^3-3531x^2-688x-43,6],[x^{18}+3x^{17}-26x^{16}-78x^{15}+270x^{14}+815x^{13}-1436x^{12}-4416x^{11}+4153x^{10}+13377x^9-6258x^8-22693x^7+3772x^6+20184x^5+782x^4-7699x^3-1277x^2+514x+13,6],[x^{18}+4x^{17}-33x^{16}-150x^{15}+387x^{14}+2233x^{13}-1578x^{12}-16799x^{11}-4197x^{10}+65971x^9+59322x^8-117310x^7-188308x^6+21264x^5+190984x^4+132221x^3+32604x^2+1200x-379,4],[x^{18}+6x^{17}-22x^{16}-184x^{15}+101x^{14}+2206x^{13}+1048x^{12}-13080x^{11}-12983x^{10}+39490x^9+52906x^8-54352x^7-91701x^6+23122x^5+56412x^4-5600x^3-13034x^2+1480x+568,6],[x^{27}-3x^{26}-55x^{25}+164x^{24}+1304x^{23}-3858x^{22}-17519x^{21}+51323x^{20}+147499x^{19}-427049x^{18}-812192x^{17}+2322310x^{16}+2957083x^{15}-8374150x^{14}-7010721x^{13}+19892990x^{12}+10323950x^{11}-30317349x^{10}-8509315x^9+28202264x^8+2963409x^7-14792310x^6+220229x^5+3889959x^4-397376x^3-380960x^2+72460x-2647,6],[x^{27}-3x^{26}-53x^{25}+160x^{24}+$

$1210x^{23}-3680x^{22}-15631x^{21}+47937x^{20}+126405x^{19}-390929x^{18}-670268x^{17}+2085994x^{16}+2381831x^{15}-7410738x^{14}-5717857x^{13}+17541450x^{12}+9224648x^{11}-27292133x^{10}-9719725x^9+27067090x^8+6187223x^7-16180684x^6-1937401x^5+5264635x^4+99800x^3-738836x^2+47264x+14987,6],[x^{27}+3x^{26}-55x^{25}-164x^{24}+1304x^{23}+3858x^{22}-17519x^{21}-51323x^{20}+147499x^{19}+427049x^{18}-812192x^{17}-2322310x^{16}+2957083x^{15}+8374150x^{14}-7010721x^{13}-19892990x^{12}+10323950x^{11}+30317349x^{10}-8509315x^9-28202264x^8+2963409x^7+14792310x^6+220229x^5-3889959x^4-397376x^3+380960x^2+72460x+2647,4],[x^{27}+3x^{26}-53x^{25}-160x^{24}+1210x^{23}+3680x^{22}-15631x^{21}-47937x^{20}+126405x^{19}+390929x^{18}-670268x^{17}-2085994x^{16}+2381831x^{15}+7410738x^{14}-5717857x^{13}-17541450x^{12}+9224648x^{11}+27292133x^{10}-9719725x^9-27067090x^8+6187223x^7+16180684x^6-1937401x^5-5264635x^4+99800x^3+738836x^2+47264x-14987,4]$

The polynomial p_3 on $S_2(2^3w^2)$ has the following factors:

$[x-3,8],[x-2,8],[x-1,20],[x,12],[x+1,28],[x+2,4],[x+3,15],[x^2-4x+2,2],[x^2-3x-1,3],[x^2-3x+1,11],[x^2-2x-1,6],[x^2-x-5,12],[x^2-x-4,5],[x^2-x-3,3],[x^2-x-1,5],[x^2-8,2],[x^2-5,4],[x^2-3,4],[x^2-2,2],[x^2+x-4,4],[x^2+x-3,12],[x^2+x-1,10],[x^2+2x-2,6],[x^2+3x-1,7],[x^2+3x+1,9],[x^3-3x^2-4x+13,6],[x^3-7x+7,4],[x^3-4x-1,3],[x^3+2x^2-4x-7,3],[x^3+2x^2-x-1,8],[x^3+4x^2+3x-1,2],[x^4-4x^3-x^2+10x+2,2],[x^4-2x^3-9x^2+22x-11,6],[x^4-2x^3-6x^2+10x+1,6],[x^4+2x^3-7x^2-8x-1,3],[x^4+2x^3-7x^2-8x+4,2],[x^4+2x^3-4x^2-8x-2,6],[x^4+3x^3-6x^2-23x-13,2],[x^4+4x^3-8x-1,4],[x^6-3x^5-12x^4+36x^3+18x^2-68x+29,6],[x^6-3x^5-11x^4+31x^3+15x^2-25x-4,3],[x^6-3x^5-9x^4+23x^3+15x^2-13x-1,2],[x^6-x^5-13x^4+11x^3+49x^2-27x-52,3],[x^6+2x^5-11x^4-16x^3+35x^2+26x-25,4],[x^8-6x^7+x^6+48x^5-65x^4-54x^3+115x^2-48x+4,4],[x^8-3x^7-20x^6+57x^5+124x^4-327x^3-245x^2+588x+16,2],[x^9-4x^8-9x^7+50x^6-5x^5-156x^4+125x^3+50x^2-40x+4,2],[x^9-x^8-19x^7+16x^6+114x^5-76x^4-251x^3+165x^2+181x-128,2],[x^9+2x^8-17x^7-34x^6+75x^5+158x^4-31x^3-106x^2-20x+4,2],[x^9+3x^8-11x^7-32x^6+38x^5+100x^4-47x^3-75x^2+37x-4,2],[x^{12}+x^{11}-22x^{10}-30x^9+153x^8+276x^7-317x^6-863x^5-182x^4+513x^3+242x^2-22x-1,4],[x^{16}-2x^{15}-26x^{14}+48x^{13}+261x^{12}-442x^{11}-1300x^{10}+2024x^9+3449x^8-4958x^7-4874x^6+6520x^5+3355x^4-4294x^3-776x^2+1104x-74,2],[x^{18}-4x^{17}-33x^{16}+150x^{15}+387x^{14}-2233x^{13}-1578x^{12}+16799x^{11}-4197x^{10}-65971x^9+59322x^8+117310x^7-188308x^6-21264x^5+190984x^4-132221x^3+32604x^2-1200x-379,2],[x^{18}-2x^{17}-34x^{16}+64x^{15}+461x^{14}-802x^{13}-3208x^{12}+4968x^{11}+12385x^{10}-15862x^9-26994x^8+24760x^7+31587x^6-14558x^5-16140x^4-640x^3+910x^2+56x-8,2],[x^{18}+3x^{17}-28x^{16}-84x^{15}+308x^{14}+921x^{13}-1692x^{12}-4994x^{11}+4927x^{10}+13943x^9-7648x^8-19011x^7+6382x^6+10700x^5-3212x^4-2003x^3+627x^2+20x-1,2],[x^{18}+3x^{17}-28x^{16}-82x^{15}+318x^{14}+915x^{13}-1870x^{12}-5426x^{11}+5939x^{10}+18603x^9-9152x^8-37297x^7+2528x^6+41228x^5+10028x^4-20669x^3-9779x^2+1970x+1259,4],[x^{18}+3x^{17}-26x^{16}-80x^{15}+264x^{14}+837x^{13}-1362x^{12}-4500x^{11}+3737x^{10}+13433x^9-4682x^8-22123x^7-202x^6+18304x^5+5878x^4-5249x^3-3531x^2-688x-43,2],[x^{18}+3x^{17}-26x^{16}-78x^{15}+270x^{14}+815x^{13}-1436x^{12}-4416x^{11}+4153x^{10}+13377x^9-6258x^8-22693x^7+3772x^6+20184x^5+782x^4-7699x^3-1277x^2+514x+$

$13, 2], [x^{18} + 6x^{17} - 22x^{16} - 184x^{15} + 101x^{14} + 2206x^{13} + 1048x^{12} - 13080x^{11} - 12983x^{10} + 39490x^9 + 52906x^8 - 54352x^7 - 91701x^6 + 23122x^5 + 56412x^4 - 5600x^3 - 13034x^2 + 1480x + 568, 2], [x^{27} - 3x^{26} - 55x^{25} + 164x^{24} + 1304x^{23} - 3858x^{22} - 17519x^{21} + 51323x^{20} + 147499x^{19} - 427049x^{18} - 812192x^{17} + 2322310x^{16} + 2957083x^{15} - 8374150x^{14} - 7010721x^{13} + 19892990x^{12} + 10323950x^{11} - 30317349x^{10} - 8509315x^9 + 28202264x^8 + 2963409x^7 - 14792310x^6 + 220229x^5 + 3889959x^4 - 397376x^3 - 380960x^2 + 72460x - 2647, 2], [x^{27} - 3x^{26} - 53x^{25} + 160x^{24} + 1210x^{23} - 3680x^{22} - 15631x^{21} + 47937x^{20} + 126405x^{19} - 390929x^{18} - 670268x^{17} + 2085994x^{16} + 2381831x^{15} - 7410738x^{14} - 5717857x^{13} + 17541450x^{12} + 9224648x^{11} - 27292133x^{10} - 9719725x^9 + 27067090x^8 + 6187223x^7 - 16180684x^6 - 1937401x^5 + 5264635x^4 + 99800x^3 - 738836x^2 + 47264x + 14987, 2]$

6.3 Resumen en Castellano

Introducción:

El objetivo principal de esta tesis es aplicar el *método modular* para estudiar algunas ecuaciones de Fermat generalizadas de tipo (r, r, p).

Empecemos por recordar el Último Teorema de Fermat (UTF), la demonstración del cual ha proporcionado una técnica completamente novedosa en la resolución de ecuaciones Diofánticas.

Teorema 6.3.1 *(Fermat-Wiles) Si $n > 2$ es un entero, entonces la ecuación $x^n + y^n = z^n$ no tiene soluciones (a, b, c) tales que $abc \neq 0$.*

La estrategia que llevó a la prueba del UTF se llama el *método modular* y utiliza de forma notable curvas elípticas, formas modulares y representaciones de Galois. Esta estrategia ha empezado con ideas de Frey, Hellegouarch y Serre, seguidas de progresos de Ribet y finalmente concluida por A. Wiles (ver [76]). Desde la prueba de Wiles la estrategia inicial ha sido mejorada y varios matemáticos lograron tener éxito en solucionar ecuaciones que previamente parecían intratables. Una consecuencia de estos esfuerzos ha sido que la ecuación de Fermat generalizada

$$Ax^p + By^q = Cz^r, \quad \text{donde} \quad 1/p + 1/q + 1/r < 1, \tag{6.1}$$

con p, q, r primos y A, B, C enteros coprimos dos a dos, se ha convertido en el nuevo centro de atención. Llamaremos a la terna de exponentes (p, q, r) en (6.1) el *tipo* de la ecuación. En general, fijados A, B, C y el tipo, la ecuación (6.1) admite infinitas soluciones. Por ejemplo, si $z = a^3 + b^3$, $x = az$, $y = bz$ entonces (x, y, z) satisface $x^3 + y^3 = z^4$. Sin embargo, suponiendo cierta la conjetura *abc* se demuestra que solo existe un número finito de soluciones (a, b, c) de la ecuación (6.1) que satisfacen $\gcd(a, b, c) = 1$ (ver Sección 5.2 en [20]). Más exactamente,

Conjetura 6.3.1 *Sean $A, B, C \in \mathbb{Z}$ coprimos dos a dos. Entonces, existe solo un número finito de (a, b, c, p, q, r) que satisfacen:*

1. *$p, q, r \in \mathbb{Z}$ primos tales que $1/p + 1/q + 1/r < 1$,*
2. *$(a, b, c) \in (\mathbb{Z} \setminus \{0\})^3$ y $\gcd(a, b, c) = 1$ (soluciones primitivas),*
3. *$Aa^p + Bb^q = Cc^r$.*

Observación 6.3.2 *Para la conjetura consideramos que soluciones del tipo $1^p + 2^3 = 3^2$ cuentan como una única solución.*

Un resultado importante en esta dirección es un teorema de Darmon-Granville [20] que demuestra que dados A, B, C y fijados (p, q, r) existe solo un número finito de soluciones primitivas. Además, el método modular ha sido utilizado con éxito para dar evidencia a esta conjectura, permitiendo la demostración de que no existen soluciones primitivas en varios casos particulares, incluyendo familias infinitas. Por ejemplo, $x^p + y^p = z^2$ o $x^p + y^p = z^3$ han sido solucionadas por Darmon-Merel [21]. Estas ecuaciones son casos particulares de $x^p + y^q = z^r$. Otro progreso importante ha sido el trabajo de Ellenberg sobre las representaciones asociadas con $\mathbb{Q}$-curvas. Su trabajo ha permitido introducir el uso de $\mathbb{Q}$-curvas como curvas de Frey y, en particular, le permitió solucionar la ecuación $x^4 + y^2 = z^p$ (ver [29]). En las introducciones de [3] y [18] se puede encontrar una perspectiva actualizada y un resumen de resultados conocidos sobre la ecuación $x^p + y^q = z^r$.

Otra familia interesante está constituida por las ecuaciones de tipo (r, r, p) con r un número primo fijado, es decir,

$$Ax^r + By^r = Cz^p \quad \text{(donde } p \text{ varía)}.$$

En esta clase de ecuaciones hay trabajos para tipo $(3, 3, p)$ de Kraus [45], Bruin [10], Chen-Siksek [16] y Dahmen [18] y para tipo $(5, 5, p)$ de Billerey [5], Billerey-Dieulefait [6].

Las distintas generalizaciones del método modular para atacar nuevas ecuaciones dependen de la ecuación en cuestión. Una estrategia universal para atacar la ecuación de Fermat generalizada de tipo (p, q, r) ha sido desarollada por Darmon en [19]. Su método utiliza variedades abelianas de Frey de gran dimensión. Sin embargo, al dia de hoy, poco se conoce sobre tales variedades y en [19] Darmon solo consigue solucionar ecuaciones de la forma $x^p + y^p = z^r$ en casos particulares y para valores de r pequeños.

Brevemente, el método modular se puede dividir en 3 partes:

(I) [Construcción de una curva de Frey] Asociar una curva elíptica E con ciertas propiedades a una posible solución de una ecuación diofántica.

(II) [Modularidad / Bajada de Nivel] Demostrar que la curva E es modular, que su representación asociada $\bar{\rho}_{E,p}$ es absolutamente irreducible y aplicar resultados de bajada

de nivel que darán lugar a un isomorfismo $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{P}}$, donde f es una forma modular clásica o de Hilbert con un nivel adecuado.

(III) [Contradicción] Contradecir el isomorfismo de representaciones residuales anterior para todas las posibilidades para f.

En esta tesis, utilizaremos el método modular para profundizar en el estudio de las ecuaciones de tipo (r, r, p), más concretamente las de forma $x^r + y^r = Cz^p$, donde C es un entero divisible solo por primos $q \not\equiv 1, 0$ modulo r. En particular, mejoraremos los resultados existentes para $r = 5$ y daremos nuevos resultados para $r = 7$ y $r = 13$. Además, haciendo uso de curvas elípticas, delinearemos una estrategia que puede ser utilizada para atacar la ecuación anterior para cualquier primo r. En efecto, completaremos la parte (I) y parcialmente la parte (II) del método modular para cada r (la parte (III) depende del valor de r). En el camino, en particular, demostraremos un resultado de modularidad para curvas elípticas con buena reducción en 3 definidas sobre ciertos cuerpos de numeros.

Los resultados contenidos en el Capitulo 2 sobre la ecuación $x^5 + y^5 = Cz^p$ han sido aceptados para publicación en un articulo conjunto con L. Dieulefait en la revista *Mathematics of Computation* (ver [27]).

Resultados:

A continuación describiremos el contenido de cada capítulo de esta tesis. En particular, enunciaremos los resultados obtenidos y comentaremos las estrategias utilizadas.

En este trabajo, una solución $(a, b, c) \in \mathbb{Z}^3$ de $x^r + y^r = Cz^p$ se dirá *primitiva* si $(a, b) = 1$ y *trivial* si $|abc| \leq 1$. En particular, nuestras soluciones primitivas también lo son en el sentido de que $\gcd(a, b, c) = 1$ como arriba. Además, a una solución primitiva le diremos solución de primer tipo si $r \nmid c$ y de segundo tipo si $r \mid c$.

El Capítulo 1 cubre los requisitos previos que constituyen el método modular via curvas elípticas sobre $\mathbb{Q}$. Incluiremos las definiciones y teoremas básicos de la teoría de curvas elípticas, formas modulares y sus representaciones de Galois asociadas. En particular, demostraremos en detalle un teorema de Hellegouarch, sobre la ramificación de la representación modulo p asociadas con algunas curvas, que será utilizado en todos los capítulos posteriores. Enunciaremos también el teorema de modularidad sobre $\mathbb{Q}$, el teorema de bajada de nivel de Ribet y la conjetura de Serre. Terminaremos el capítulo con la idea de la prueba del Último Teorema de Fermat para motivar las generalizaciones que estudiaremos en los capítulos siguientes.

En el Capítulo 2 nos dedicaremos a ecuaciones de la forma $x^5 + y^5 = Cz^p$. El teorema siguiente es una consecuencia del trabajo de Billerey [5] y Billerey-Dieulefait [6],

Teorema 6.3.2 *Sea $C = 2^\alpha 3^\beta 5^\gamma$ donde $\alpha \geq 2$, $\beta, \gamma, \geq 0$, o $C = 7, 13$. Entonces, para $p > 19$, la ecuación $x^5 + y^5 = Cz^p$ no tiene soluciones primitivas no triviales.*

Nótese que en su teorema todos los valores de C satisfacen $|C| \geq 4$. Nosotros demostraremos el resultado siguiente

Teorema 6.3.3 *Sea β un entero divisible solo por primos $l \not\equiv 1 \pmod 5$. Supongamos que $p \equiv 1 \pmod 4$ o $p \equiv \pm 1 \pmod 5$. Entonces,*

(A) *Si $p > 13$, la ecuación $x^5 + y^5 = 2\beta z^p$ no tiene soluciones primitivas no triviales.*

(B) *Si $p > 73$, la ecuación $x^5 + y^5 = 3\beta z^p$ no tiene soluciones primitivas no triviales.*

A lo largo de este capítulo introduciremos la teoría necesaria para la prueba del teorema anterior. En particular, cubriremos los requisitos previos de la teoria de variedades abelianas asociadas con $\mathbb{Q}$-curvas y de *embedding problems* de los trabajos de J. Quer [54], [55]. Además, enunciaremos y utilizaremos los resultados de Ellenberg en [29] sobre las representaciones asociadas con $\mathbb{Q}$-curvas.

La primera idea importante de la prueba del teorema anterior es relacionar una solución primitiva no trivial de $x^5 + y^5 = Cz^p$ con una solución (a, b, c) de una ecuación relacionada (que no depende de C y esta definida sobre $\mathbb{Q}$) satisfaciendo $C \mid a + b$. Después aplicamos el metodo modular con $\mathbb{Q}$-curvas para demostrar que la solución (a, b, c) de la nueva ecuación no puede existir. Para esto, primero asociamos a (a, b, c) una curva de Frey $E_{(a,b)}$ sobre $\mathbb{Q}(\sqrt{5})$ y demostraremos que es una $\mathbb{Q}$-curva (Paso (I)). Segundo, utilizando la teoría de Quer produciremos una curva adecuada $E_\gamma(a, b)$ twisteada de $E_{(a,b)}$ completamente definida sobre un cierto cuerpo de numeros K, cíclico de grado cuatro. La idea de utilizar *embedding problems* para determinar E_γ no es nueva en la literatura (ver [20]), pero parece ser la primera vez que una extensión cíclica de grado cuatro es necesaria, lo que hace los cálculos técnicamente bastante difíciles. Después demostramos que la restricción de Weil (denotada B) de K hasta $\mathbb{Q}$ de E_γ es un producto de variedades de tipo GL_2. Esto es fundamental, porque así somos capaces de calcular todos los invariantes de Serre asociados con una representación $\bar{\rho}$ asociada a B y aplicarle la conjectura de Serre, concluyendo el Paso (II). Por fin, para completar la demostración, tenemos que ejecutar el Paso (III). Esto se hace mediante una análisis caso por caso de las forma nuevas en los espacios previstos por la conjectura de Serre. En particular, utilizaremos varios métodos conocidos para eliminar formas nuevas y introduciremos un nuevo método via un teorema de Carayol. Hasta este punto tendremos demostrado una versión más débil de nuestro resultado. Finalmente, introduciremos otra curva de Frey F que, utilizando el método multi-Frey de Siksek, nos permitirá terminar la prueba.

El Capítulo 3 está dedicado a desarollar una estrategia general para atacar un número infinito de ecuaciones de tipo (r, r, p) para cada primo $r \geq 7$. Por un lado, en [19], Darmon describe un programa para atacar ecuaciones de Fermat generales de tipo (p, q, r) utilizando variedades abelianas de gran dimensión. Por otro lado, no existe ningún algoritmo para ejecutar el Paso (I) del método modular para una ecuación Diophantica aleatoria, ni siquiera para las de tipo Fermat. Nuestro método, aunque esté limitado para ecuaciones de tipo

(r, r, p) tiene la ventaja de que da un algoritmo para construir varias curvas elípticas de Frey. Esto es una mejora respecto a [19] porque nos permite obtener un mejor entendimiento de las representaciones de Galois involucradas.

Empezamos el Capítulo 3 introduciendo formas modulares de Hilbert y los teoremas de bajada de nivel de Jarvis, Rajaei y Fujiwara. Después procedemos a la descripción de un método general que nos permite completar el Paso (I) y parcialmente el Paso (II) del método modular para un número infinito de ecuaciones de la forma $x^r + y^r = Cz^p$. En los próximos párrafos resumiremos las ideas principales.

Fijemos un primo $r \geq 7$ y sea K^+ el subcuerpo totalmente real maximal del cuerpo ciclotómico $\mathbb{Q}(\zeta_r)$. Sea $C \neq 0$ un entero divisible solo por primos $q \neq r$ congruentes con 1 (mod r). Generalizando la idea en el Capitulo 2, empezamos por relacionar una solución primitiva no trivial (a, b, c') de $x^r + y^r = Cz^p$ con soluciones (a, b, c), tales que $C \mid a + b$, de varias otras ecuaciones diofánticas (que no dependen de C) definidas sobre K^+. En seguida, asociaremos curvas de Frey $E_{(a,b)}$ a las soluciones de las nuevas ecuaciones. Brevemente, sea $\phi_r(x, y) = (x^r + y^r)/(x + y)$ y escojemos tres factores f_1, f_2, f_3 de ϕ_r distintos, de grado 2 y definidos sobre K^+; después encontraremos α, β, γ tales que $\alpha f_1 + \beta f_2 + \gamma f_3 = 0$ y aplicaremos la construción de Frey original sobre K^+. Como E dependerá solamente de a, b y estos son constante durante todo el proceso, acabamos construyendo varias curvas de Frey asociadas a la ecuancion inicial (a, b, c'). Esto completa el Paso (I) con total generalidad.

A pesar de que el Paso (II) (modularidad / irreducibilidad) es una aplicación clásica de resultados profundos de Mazur, Ribet y Wiles cuando la curva E está definida sobre $\mathbb{Q}$, la situación se complica cuando E está definida sobre un cuerpo más grande. En particular, análogos de estos teoremas son en su mayoría conjecturas. En esta dirección, demostraremos un resultado con cierta generalidad sobre la irreducibilidad de las representaciones modulo p asociadas con ciertas curvas elípticas y un resultado de modularidad nuevo para curvas elípticas sobre cuerpos totalmente reales con ciertas condiciones locales en 3. Más exactamente, demostraremos los teoremas siguientes

Teorema 6.3.4 *Sea F un cuerpo de números totalmente real y C/F una curva elíptica de conductor N_E. Sea A el factor de N_E que corresponde a los primos de reducción aditiva. Supongamos además que $\mathfrak{q} \nmid N_C$ es un primo fijado de buena reducción. Existe una constante explícita $M(F, A, \mathfrak{q})$ tal que, si*

1. *p is impar y no ramificado en F;*
2. *todos los primos $\mathfrak{p} \mid p$ son de reducción semistable para C;*
3. *$p > M(F, A, \mathfrak{q})$.*

Entonces, la representación $\bar{\rho}_{C,p}$ es absolutamente irreducible.

Teorema 6.3.5 *Sea F un cuerpo de números abeliano totalmente real y C una curva*

elíptica definida sobre F. Supongamos que 3 descompone totalmente en F y que C es de buena reducción en todos los primos encima de 3. Entonces C es modular.

Un paso fundamental en la prueba del teorema de modularidad es garantizar modularidad residual de $\bar{\rho}_{C,3}$, lo que se consigue como consecuencia de un teorema profundo de Langlands-Tunnell. El resto de la demostración esta dividida en tres casos: (i) $\bar{\rho}_{C,3}$ y $\bar{\rho}_{C,3}|G_{F(\sqrt{-3})}$ ambas abs. irreducibles; (ii) $\bar{\rho}_{C,3}$ abs. irreducible y $\bar{\rho}_{E,3}|G_{F(\sqrt{-3})}$ reducible; (iii) $\bar{\rho}_{C,3}$ reducible. En cada caso tenemos que verificar que todas las condiciones son satisfechas para aplicar adecuadamente un teorema de levantamento de modularidad de Kisin o Skinner-Wiles. En particular, necesitaremos utilizar el trabajo de Breuil y Savitt para garantizar la existencia de levantamentos ordinarios.

Los dos teoremas anteriores contestan de forma completa a la parte de irreducibilidad del Paso (II) y parcialmente a la parte de modularidad. Más exactamente, es una consecuencia del teorema de irreducibilidad que para cada primo $r \geq 7$ existe una constante $M(r)$ tal que, si $p > M(r)$ entonces la representación $\bar{\rho}_{E,p}$ es absolutamente irreducible. Además, es un corolario del teorema de modularidad que en los casos $r = 7$ y $r = 13$ nuestro método de construir curvas de Frey produce curvas que demostraremos modulares. El principal obstáculo para demostrar modularidad de las curvas de Frey para todo r es la dificultad de garantizar la existencia de levantamentos modulares ordinarios (en el caso residualmente localmente reducible) cuando 3 es no ramificado y no descompone totalmente en F. No obstante, también discutiremos ciertos resultados de modularidad recientes que para valores particulares de r nos podrían permitir verificar si una curva de Frey es modular.

Finalmente, calcularemos los conductores de todas las curvas de Frey E, para primos p semistables para E también determinaremos los conductores de Artin de $\bar{\rho}_{E,p}$ y demostraremos que $\bar{\rho}_{E,p}$ es finita para todo primo $\mathfrak{p} \mid p$. Incluiremos los enunciados de los teoremas de bajada de nivel para formas modulares de Hilbert (FMH) de Jarvis, Rajaei y Fujiwara, y explicaremos como aplicarlos en nuestra situación, lo que nos lleva a un método modular via FMH. Las limitaciones de nuestro método quedarán claras en el Capítulo 4 cuando ejecutemos el Paso (III) en los casos $r = 7$ y $r = 13$. Sin embargo, en el Capítulo 3 también incluiremos una discusión de las dos mayores limitaciones del metodo: 1) limitaciones debido a la existencia de soluciones triviales; 2) limitaciones computacionales. Las limitaciones de tipo 1) resultan en que solo logramos solucionar las ecuaciones en el caso de soluciones de primer tipo. Respecto a las de tipo 2) demostraremos que cuando r es congruente con 1 modulo 6 se pueden construir curvas de Frey definidas sobre el subcuerpo de K^+ con grado $(r-1)/6$. Esta observación es crucial a la hora de calcular ejemplos específicos en el Capítulo 4, pues reduce considerablemente la cantidad de cálculos necesarios para completar el Paso (III).

En el Capítulo 4 aplicaremos la estrategia desarollada en el Capitulo 3 para algunos valores especificos de r. En particular, daremos ejemplos explícitos de curvas de Frey para $r = 7, 11, 13, 17, 19$ y completaremos el Paso (III) en los casos $r = 7$ y $r = 13$. Por lo que sabemos, ningún resultado aritmético sobre ecuaciones de tipo $(7, 7, p)$ y $(13, 13, p)$

era conocido. Además, el caso $r = 13$ parece ser la primera vez donde las curvas de Frey involucradas no són $\mathbb{Q}$-curvas. En particular, esto significa que en lugar de formas modulares clásicas uno está forzado a utilizar formas de Hilbert (en este caso sobre $\mathbb{Q}(\sqrt{13})$). Por lo tanto, además del interés propio de los resultados aritméticos, los teoremas obtenidos en el Capítulo 4 también ilustran la fuerza de los métodos generales desarollados en el capítulo anterior.

Empezaremos el Capítulo 4 por completar el Paso (III) para $r = 7$ demostrando el siguiente teorema

Teorema 6.3.6 *Sea $d = 2^{s_0}3^{s_1}5^{s_2}$ y γ un entero divisible solo por primos $l \not\equiv 1, 0 \pmod 7$. Entonces, si $p \geq 17$ se tiene que*

(*I*) *La ecuación $x^7 + y^7 = d\gamma z^p$ no tiene soluciones primitivas no triviales de primer tipo si (s_0, s_1, s_2) satisface alguna de las siguientes condiciones $(\geq 2, \geq 0, \geq 0)$, $(= 1, \geq 1, \geq 0)$ o $(= 0, \geq 0, \geq 1)$.*

(*II*) *La ecuación $x^{14} + y^{14} = d\gamma z^p$ no tiene soluciones primitivas no triviales si $s_1 > 0$ o $s_2 > 0$ o $s_0 \geq 2$.*

Con técnicas análogas a la demostración del teorema anterior, también demostraremos

Teorema 6.3.7 *Si $p > 254^{2873}$ es un primo, entonces la ecuación*

$$x^6 - x^5y + x^4y^2 - x^3y^3 + x^2y^4 - xy^5 + y^6 = 71z^p$$

no tiene soluciones $(x, y, z) = (a, b, c)$ tales que $(a, b) = 1$ and $|abc| > 1$.

A pesar de que la curva de Frey utilizada en las demostraciones de los teoremas anteriores ya era conocida (habiéndose obtenido por métodos distintos a los aquí presentados), ningúna aplicación aritmética de ella era conocida. Finalmente, completaremos el Paso (III) para $r = 13$. La curva de Frey en este caso es nueva, y su modularidad (de Hilbert) es consecuencia de los resultados en el Capitulo 3. En particular, demostraremos

Teorema 6.3.8 *Sea $d = 3, 5, 7, 11$ y γ un entero divisible solo por primos $l \not\equiv 1, 0$ (mod 13). Si $p > 4992539$ es primo, entonces:*

(I) La ecuación $x^{13} + y^{13} = d\gamma z^p$ no tiene soluciones primitivas no triviales de primer tipo.

(II) La ecuación $x^{26} + y^{26} = 10\gamma z^p$ no tiene soluciones primitivas no triviales.

Las grandes cotas obtenidas para el exponente p en los dos teoremas anteriores pueden parecer sorprendentes. Su razón de ser es que calcular completamente los espacios relevantes de formas nuevas no es factible. Sin embargo, somos capaces de completar el Paso (III)

calculando solamente las formas nuevas con cuerpo de coeficientes $\mathbb{Q}$ (y alguma información parcial más sobre las demás formas en el caso $r = 13$). Compensaremos esta falta de información con argumentos teóricos para los cuales hace falta introducir tales cotas. En particular, para la prueba del caso $r = 13$ necesitamos calcular formas nuevas de Hilbert sobre $\mathbb{Q}(\sqrt{13})$ con nivel 104 y 208 de peso paralelo 2. Estos cálculos estaban fuera de alcance para los medios computacionales disponibles, pero gracias a los recursos aportados por John Voight, fue posible el cómputo de todas las formas nuevas con cuerpo de coeficientes $\mathbb{Q}$ y la factorización del polinomio característico de un operador de Hecke sobre todo el espacio (los resultados de sus cálculos están en el Apéndice 6.1 y 6.2).

En el Capítulo 5 propondremos dos curvas de Frey extra asociadas con soluciones de $x^r + y^r = Cz^p$ para primos de la forma $r = 4m + 1$. Para lograrlo adaptaremos las ideas en el Capitulo 3 sobre como relacionar soluciones de ecuaciones distintas además de generalizar el método que llevó a las $\mathbb{Q}$-curvas E y F en el Capitulo 2. Las curvas resultantes estan definidas sobre K^+, y demostraremos que son k-curvas, donde k es el único cuerpo de números que satisface $[K^+ : k] = 2$. Después calcularemos su discriminante y conductor de Artin de las representaciones mod p asociadas y así verificamos que las curvas satisfacen las propriedades adecuadas para que sean útiles como curvas de Frey. Para terminar el capítulo discutiremos como la teoria de J. Quer sobre embedding problems puede ser aplicada para extender las representaciones de G_{K^+} asociadas con las nuevas curvas de Frey a representaciones de G_k.

Bibliography

[1] T. Barnet-Lamb, T. Gee, and D. Geraghty. Congruences betwen Hilbert modular forms: constructing ordinary lifts. *To appear Duke Math Journal*.

[2] T. Barnet-Lamb, T. Gee, and D. Geraghty. Congruences betwen Hilbert modular forms: constructing ordinary lifts II (preprint). available at `http://www2.imperial.ac.uk/~tsg/Index_files/ordinaryHMFpostBLGGTversion.pdf`.

[3] M. Bennett and I. Chen. Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^p$. Available at `http://people.math.sfu.ca/~ichen/pub/BeCh2.pdf`.

[4] N. Billerey. Critéres d'irréductibilité pour les représentations des courbes elliptiques. *To appear in Intern. Journal of Number Theory*.

[5] N. Billerey. Équations de Fermat de Type $(5, 5, p)$. *Bull. Austral. Math. Soc.*, 76 (2):161–194, 2007.

[6] N. Billerey and L. Dieulefait. Solving Fermat-type equations $x^5 + y^5 = dz^p$. *Math. Comp.*, 79:535–544, 2010.

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24:235–265, 1997.

[8] C. Breuil. p-adic Hodge theory, deformations and local Langlands. notes of a course at crm, bellaterra, spain, july 2001, available at `http://www.math.u-psud.fr/~breuil/PUBLICATIONS/Barcelone.pdf`.

[9] 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 4:843–939, 2001.

[10] N. Bruin. On powers as sums of two cubes. *Algorithmic Number Theory (edited by W. Bosma), Lecture Notes in Comput. Sci. 1838, Springer, Berlin*.

[11] Y. Bugeaud, M. Mignotte, and S. Siksek. A multi-Frey approach to some multi-parameter families of Diophantine equations. *To appear in Canad. J. Math*.

[12] K. Buzzard, F. Diamond, and F. Jarvis. On Serre's Conjecture for mod l Galois representations over totally real fields. *Duke Math J.*, 155, 2010.

[13] H. Carayol. Sur le représentation l-adiques associées aux forme modulaires de Hilbert. *Ann. Sci. Ec. Norm. Sup.*, 19:409–468, 1986.

[14] H. Carayol. Sur le représentation Galoisienne modulo l attacheé aux forme modulaires. *Duke Math. J.*, 59 No 3:785–801, 1989.

[15] I. Chen. On the equation $a^2 + b^{2p} = c^5$. *Acta Arith.*, 143:345–375, 2010.

[16] I. Chen and S. Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra*, 322:638–656, 2009.

[17] B. Conrad, F. Diamond, and R. Taylor. Modularity of certain potentially barsotti-tate representations. *J. Amer. Math. Soc.*, 12 No 2:521–567, 1999.

[18] S. Dahmen. Classical and modular methods applied to Diophantine equations. *PhD thesis, University of Utrecht, 2008, avaliable at* `igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UUindex.html`.

[19] H. Darmon. Rigid local systems, Hilbert modular forms, and Fermat's Last Theorem. *Duke Math. J.*, 102:413–449, 2000.

[20] H. Darmon and A. Granville. On the equations $z^m = f(x, y)$ and $ax^p + by^q = cz^r$. *Bull. of London Math. Soc.*, 27:513–543, 1995.

[21] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's Last Theorem. *J. Reine Angew.*, 490:81–100, 1997.

[22] P. Deligne. Forms modulaires et représentations ℓ-adiques. *Lecture Notes in Math.*, 179:139–172, 1971.

[23] P. Deligne and J-P. Serre. Formes modulaires de poids 1. *Ann. Sci. Ec. Norm. Sup.*, 4 Serie 7:507–530, 1974.

[24] L. Dembélé and J. Voight. Explicit methods for Hilbert modular forms. *Elliptic curves, Hilbert modular forms and Galois deformations. Diamond et al. (eds.). Birkhauser, Progress in Mathematics, to appear.*

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

[26] L. Dieulefait. Modularity of abelian surfaces with quaternionic multiplication. *Math. Research. Letters*, 10:145–150, 2003.

[27] L. Dieulefait and N. Freitas. The Fermat-type equations $x^5 + y^5 = 2z^p$ or $3z^p$ solved through $\mathbb{Q}$-curves. *To appear in Math. Comp.*

[28] L. Dieulefait and J. Jiménez. Solving Fermat-type equations $x^4 + dy^2 = z^p$ via modular $\mathbb{Q}$-curves over polyquadratic fields. *J. Reine Angew. Math.*, 633:183–196, 2009.

[29] J. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math*, 126:763–787, 2004.

[30] J. Ellenberg. Serre's conjecture over $\mathbb{F}_9$. *Annals of Math.*, 161:1111–1142, 2005.

[31] J. Ellenberg and C. Skinner. On the modularity of $\mathbb{Q}$-curves. *Duke Math. J.*, 109 (1):97–122, 2001.

[32] K. Fujiwara. Level optimisation in the totally real case, preprint. 2006.

[33] S. Gelbart. *Three Lectures on the modularity of $\bar{\rho}_{E,p}$ and Langlands Reciprocity Conjecture. Modular forms and Fermat's Last Theorem (Boston, MA, 1995).* Springer, New York.

[34] X. Guitart. Arithmetic properties of abelian varieties under Galois conjugation. PhD thesis, Universitat Politecnica de Catalunya, 2010, available at `http://www-ma2.upc.es/xguitart/index_files/thesis.pdf`.

[35] Y. Hellegouarch. *Invitation to the Mathmatics of Fermat-Wiles.* Academic Press, 2002.

[36] F. Jarvis. Correspondences on Shimura curves and Mazur's Principle at p. *Pacific J. Math.*, 213:267–280, 2004.

[37] F. Jarvis and J. Manoharmayum. On the modularity of supersingular elliptic curves over certain totally real number fields. *J. Number Theory*, 128 (3):589–618, 2008.

[38] C. Khare. Serre's modularity conjecture: The level one case. *Duke. Math. J.*, 134:557–589, 2006.

[39] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (I). *Invent. Math.*, 178 (3):485–504, 2009.

[40] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (II). *Invent. Math.*, 178 (3):505–586, 2009.

[41] M. Kisin. Modularity of 2-dimensional Galois representations. *Current Developments in Mathematics*, pages 191–230, 2005.

[42] M. Kisin. Moduli of finite flat group schemes, and modularity. *Ann. of Math.*, 170:1082–1180, 2009.

[43] A. Kraus. Sur le défaut de semi-stabilité des courbes elliptiques á réduction additive. *Manuscripta mathematica*, 69:353–386, 1968.

[44] A. Kraus. Majorations effectives pour l'équation de fermat généralisée. *Canad. J. Math*, 49 No 6:1139–1161, 1997.

[45] A. Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7:1–13, 1998.

[46] A. Kraus. On the equation $x^p+y^q = z^r$: A Survey. *The Ramanujan Journal*, 3:315–335, 1999.

[47] R. P. Langlands. Base Change for GL(2). *Annals of Math. Studies. Vol 96, Princeton University Press, Princeton, NJ*, 1980.

[48] B. Mazur. Rational isogenies of prime degree. *Invent. Math*, 44:129–162, 1978.

[49] B. Mazur. *An introduction to Deformation theory of Galois representations. Modular forms and Fermat's Last Theorem (Boston, MA, 1995)*. Springer, New York, 1997.

[50] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.

[51] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006.

[52] I. Papadopoulos. Sur la classification de néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *Journal of Number Theory*, 44:119–152, 1993.

[53] E. E. Pyle. Abelian varieties over $\mathbb{Q}$ with large endomorphisms algebras and their simple components over $\bar{\mathbb{Q}}$. *Progress in Mathematics*, 224:189–234, 2004.

[54] J. Quer. $\mathbb{Q}$-curves and Abelian varieties of GL_2-type. *Proc. London Math. Soc.*, (3) 81:285–317, 2000.

[55] J. Quer. Embedding problems over abelian groups and an application to elliptic curves. *J. Algebra*, 237:186–202, 2001.

[56] A. Rajaei. On the levels of mod l Hilbert modular forms. *J. Reine Angew.*, 537:33–65, 2001.

[57] K. Ribet. On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.*, 100:431–476, 1990.

[58] K. Ribet. On the equations $a^p + 2^\alpha b^p + c^p = 0$. *Acta Arith.*, 79 No 1:7–16, 1997.

[59] K. Ribet. Abelian Varieties over $\mathbb{Q}$ and modular forms. *Progress in Mathematics*, 224:241–261, 2004.

[60] T. Saito. Hilbert modular forms and p-adic Hodge theory. *Compositio Math.*, 145 (5):1081–1113, 2009.

[61] D. Savitt. On a conjecture of Conrad, Diamond and Taylor. *Duke Math. J.*, 128 No 1:141–197, 2005.

[62] J.-P. Serre. *Abelian ℓ-adic Representations and Elliptic Curves, volume 7 of Research Notes in Mathematics.* A K Peters Ltd., Wellesley, MA 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[63] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.

[64] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. *Duke Math J.*, 54 No 1:179–230, 1987.

[65] J.-P. Serre. *Local Fields*. Springer, 1995.

[66] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1986.

[67] J. H. Silverman. *Advances Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.

[68] C. Skinner and A. Wiles. Residually reducible representations and modular forms. *Publ. Math. IHES*, 89:5–126, 1999.

[69] C. Skinner and A. Wiles. Nearly ordinary deformations of irreducible residual representations. *Ann. Fac. Sci. Toulouse Math.*, 10:185–215, 2001.

[70] R. Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98:265–280, 1989.

[71] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.*, 141:553–572, 1995.

[72] J. Tunnell. Artin's conjecture for representations of octahedral type. *Bull. AMS*, 5 (new series):173–175, 1981.

[73] Gerard van der Geer. *Hilbert modular surfaces*. Springer-Verlag, Berlin, 1988.

[74] A. Wiles. On p-adic representations for totally real fields. *Ann. of Math.*, 123:407–456, 1986.

[75] A. Wiles. On ordinary λ-adic representations associated to modular forms. *Invent. Math.*, 94:529–573, 1988.

[76] A. Wiles. Modular elliptic curves and Fermat's Last Theorem. *Ann. of Math*, 141, 1995.