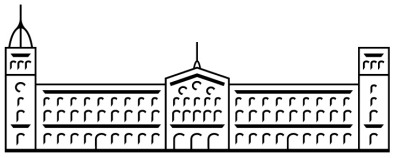

Treball final de màster

MÀSTER DE MATEMÀTICA AVANÇADA

Facultat de Matemàtiques
Universitat de Barcelona

Generalization of Fermat's Last Theorem to Real Quadratic Fields

Autor: Alex Cebrian Galan

Director: Dr. Luis Victor Dieulefait
Realitzat a: Departament de Matemàtiques

Barcelona, 11 de setembre de 2016

Contents

Introduction

The main purpose of this master thesis is to study a generalization of Fermat's Last Theorem for real quadratic fields.

As it is well-known, Fermat's Last Theorem states that the equation

$$a^n + b^n = c^n, \qquad abc \neq 0$$

has no integer solutions when the exponent n is greater or equal than 3. It was enunciated by Fermat around 1630 and stood unsolved for more than 350 years, until 1994 Andrew Wiles finally took that last step by proving the modularity conjecture for semistable elliptic curves. The whole proof of FLT involves mathematical tools which are widely used in Number Theory. Namely, elliptic curves, modular forms and Galois representations. It entangles contributions by many authors, for instance; the work of Frey, who attached an elliptic curve with some "remarkable" properties to a given solution to Fermat equation, the results of Mazur about rational torsion points on elliptic curves, Ribet's Level Lowering Theorem for modular forms, and the previously mentioned Wiles result.

Fermat's Last Theorem is not known to have an analog for number fields in general. However, for some totally real fields, it can be shown that there is a bound (depending on the field) on the exponent of any non-trivial solution to the Fermat equation. For a given totally field K, this statement is called *asymptotic Fermat's Last Theorem over* K. In the article [10] Nuno Freitas and Samir Siksek give some results towards the determination of whether a totally real field satisfies the asymptotic Fermat's Last Theorem, and a particular criterion for d in case $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field. We will follow this article restricting ourselves, for simplicity, to the real quadratic case, and focusing on the proof of this particular criterion. The strategy followed for proving it is inspired on the proof of the classical FLT, and uses analogs to real quadratic fields of the results mentioned in the last paragraph. In the same way, the mathematical tools involved are elliptic curves, Galois representations and Hilbert modular forms, a generalization of modular forms to totally real fields.

The structure of the thesis is the following: the first three chapters are devoted to introduce the theoretical background required for dealing with both the asymptotic and classical FLT, that is, Galois representations, elliptic curves, modular forms and Hilbert modular forms. We do not include the proofs of most of the results of the first three chapters, since they would require a more detailed insight into these theories, which is beyond the scope of this work. The last chapter is ded-

icated to the asymptotic Fermat's Last Theorem, and it also includes an overview of the proof of FLT.

In Chapter 1 we give some basic notions of Galois representations. The ideas of inertia subgroup and ramification of a Galois representation at a prime are introduced.

In Chapter 2 we explain some elliptic curve theory. Concepts like reduction of an elliptic curve at a prime, minimal discriminant and conductor are introduced. The most important section of this chapter is devoted to Galois representations attached to elliptic curves, in which we give some results about their irreducibility and ramification.

In Chapter 3 we introduce modular forms. Notions of modular form with respect to a congruence subgroup, Hecke operator, newform and Galois representation attached to a modular form are explained. In the last section we introduce some theory on Hilbert modular forms.

Chapter 4 makes use of the machinery introduced in the previous ones to handle both classical and asymptotic FLT. We begin with an overview of the proof of FLT. Before going through the asymptotic Fermat's Last Theorem we show how the precise proof of the FLT fails when dealing with extensions of $\mathbb{Q}$. Next we state some strong theorems about irreducibility of representations, level-lowering of Hilbert modular forms and modularity of elliptic curves over real quadratic fields. Finally, we study the proof of the asymptotic Fermat's Last Theorem for certain real quadratic fields, which is the main goal of this thesis.

Acknowledgements

I would like to thank Dr. Luis Victor Dieulefait, my thesis advisor, his guidance and support throughout this work. I would also like to express my gratitude to Eduardo Soto for his help and interest on this thesis.

Chapter 1

Galois Representations

Galois representations are a main ingredient on the proof of FLT because they relate elliptic curves with modular forms. In this chapter Galois representations are defined, and concepts such as a representation being unramified or irreducible are introduced. Throughout this chapter we mainly follow [8].

1.1 The absolute Galois group

First of all we need to explain some algebraic number theory. Henceforth we take $K/\mathbb{Q}$ to be a number field. Let $\mathfrak{p}$ be a prime in K above a prime $p \in \mathbb{Z}$ and denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$. Then $K_\mathfrak{p}$ is a local field with a non-archimedean absolute value $|\cdot|_\mathfrak{p}$, discrete valuation ring $\mathcal{O}_\mathfrak{p}$ and maximal ideal $\mathfrak{m}_\mathfrak{p}$. For the residue fields we shall use the notation

$$\mathbb{F}_\mathfrak{p} \coloneqq \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}.$$

Let L/K be a finite Galois extension of number fields and $\mathfrak{P}/\mathfrak{p}$ prime ideals in these fields. The *decomposition subgroup of* $\mathfrak{P}$ is defined as

$$D(\mathfrak{P}/\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(L/K) \colon \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

It is naturally isomorphic to the local Galois group $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$. Indeed, since L is dense in $L_\mathfrak{P}$ and K is dense in $K_\mathfrak{p}$, any automorphism $\sigma \in D(\mathfrak{P}/\mathfrak{p})$ can be uniquely extended by continuity to an automorphism in the local Galois group. In the converse direction one just restricts the automorphism to L.

Given a Galois extension of local fields $L_\mathfrak{P}/K_\mathfrak{p}$ we can consider the reduction mod $\mathfrak{P}$ of all the elements in $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p})$, since each of them fixes the valuation rings.

Proposition 1.1. *The reduction map*

$$\pi(\mathfrak{P}/\mathfrak{p})\colon \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \longrightarrow \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}),$$

is surjective.

A canonical generator of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is given by the *Frobenius endomorphism*, $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$, defined as $x \mapsto x^q$, where $q = p^f = \#\mathbb{F}_{\mathfrak{p}}$. The kernel of the reduction map is called the *inertia group*, and denoted by $I(\mathfrak{P}/\mathfrak{p})$, thus we have an exact sequence

$$0 \longrightarrow I(\mathfrak{P}/\mathfrak{p}) \longrightarrow \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \xrightarrow{\pi(\mathfrak{P}/\mathfrak{p})} \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}) \longrightarrow 0.$$

Recall that $[L_{\mathfrak{P}}\colon K_{\mathfrak{p}}] = ef$, where e is the ramification index and f is the inertial degree $f = [\mathbb{F}_{\mathfrak{P}}\colon \mathbb{F}_{\mathfrak{p}}]$. If the extension is unramified, that is if $e = 1$, then the inertia group is trivial and hence the reduction map is an isomorphism.

Any other prime in L above $\mathfrak{p}$ has the form $\sigma(\mathfrak{P})$, with $\sigma \in \mathrm{Gal}(L/K)$. This implies that

$$D(\sigma(\mathfrak{P}/\mathfrak{p})) = \sigma \circ D(\mathfrak{P}/\mathfrak{p}) \circ \sigma^{-1},$$

and similarly for the inertia group. Consequently, if L/K is unramified at one prime $\mathfrak{P}$ above $\mathfrak{p}$, so it is at all primes above $\mathfrak{p}$, whence we say that L/K is unramified at $\mathfrak{p}$. In the same way, if $\pi(\mathfrak{P}/\mathfrak{p})$ is an isomorphism, then $\mathrm{Frob}(\mathfrak{P}/\mathfrak{p})$ can be seen as an element of $D(\mathfrak{P}/\mathfrak{p})$, and therefore

$$\mathrm{Frob}(\sigma(\mathfrak{P})/\mathfrak{p}) = \sigma \circ \mathrm{Frob}(\mathfrak{P}/\mathfrak{p}) \circ \sigma^{-1},$$

so that the Frobenius elements of the primes lying over $\mathfrak{p}$ form a conjugacy class of $\mathrm{Gal}(L/K)$. We will usually refer to the element in the decomposition subgroup when we write $\mathrm{Frob}_{\mathfrak{p}}$. The Frobenius elements play an important role in the theory of Galois representations, as we will see in the next section, mainly because of the Chebotarev Density Theorem.

Theorem 1.2 (Chebotarev)**.** *Let L/K be a Galois extension of K unramified outside a finite set of primes S. Then $\bigcup_{\mathfrak{p}\notin S}[\mathrm{Frob}_{\mathfrak{p}}]$ is dense in* $\mathrm{Gal}(L/K)$.

Here the brackets of $[\mathrm{Frob}_{\mathfrak{p}}]$ denote its conjugacy class.

Now we pass to the absolute Galois extension. We denote by $G_K = \mathrm{Gal}(\bar{K}/K)$ the absolute Galois group of K. Recall that G_K can be expressed as

$$G_K \cong \varprojlim_L \mathrm{Gal}(L/K),$$

where L runs over all finite Galois extensions of K. Since $\mathrm{Gal}(L/K)$ are finite, G_K is a profinite group. In order to treat the absolute Galois group, it is useful to take an embedding point of view on primes. We fix once and for all algebraic closures $\bar{\mathbb{Q}}$ and $\bar{\mathbb{Q}}_p$ for all primes p. Let still $K \subseteq \bar{\mathbb{Q}}$ be a number field. A prime $\mathfrak{p}$ lying over p is the same as an embedding of K into $\bar{\mathbb{Q}}_p$, and given an embedding $\iota\colon K \hookrightarrow \bar{\mathbb{Q}}_p$ we obtain an ideal $\mathfrak{p}$ as the inverse image under ι of the valuation ideal of $\bar{\mathbb{Q}}_p$. Hence the role of the choice of a prime above $\mathfrak{p}$ is now played by embeddings.

Fix an embedding $\iota_{\mathfrak{p}}\colon K \hookrightarrow \bar{\mathbb{Q}}_p$. Consider an embedding $\iota\colon \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ extending $\iota_{\mathfrak{p}}$. It corresponds to choices of prime ideals above $\mathfrak{p}$ for every extension $K \subseteq L \subset \bar{\mathbb{Q}}$ compatible with intersections. We obtain an embedding of absolute Galois groups

$$G_{K_{\mathfrak{p}}} \hookrightarrow G_K, \quad \sigma \longmapsto \iota^{-1} \circ \sigma \circ \iota.$$

If we have two such embeddings ι_1 and ι_2, then the two embeddings of Galois groups are conjugate by $\iota_1 \circ \iota_2^{-1}$, as in the case of finite primes.

Now, let $K_\mathfrak{p} \subset L_\mathfrak{P} \subset M_{\tilde{\mathfrak{P}}}$ be finite degree subfields of $\bar{\mathbb{Q}}_p$. We obtain a projective system of short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I(\tilde{\mathfrak{P}}/\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(M_{\tilde{\mathfrak{P}}}/K_\mathfrak{p}) & \xrightarrow{\pi(\tilde{\mathfrak{P}}/\mathfrak{p})} & \mathrm{Gal}(\mathbb{F}_{\tilde{\mathfrak{P}}}/\mathbb{F}_\mathfrak{p}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I(\mathfrak{P}/\mathfrak{p}) & \longrightarrow & \mathrm{Gal}(M_{\mathfrak{P}}/K_\mathfrak{p}) & \xrightarrow{\pi(\mathfrak{P}/\mathfrak{p})} & \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_\mathfrak{p}) & \longrightarrow & 0 \end{array}$$

Since the projective limit over compact sets is exact we obtain an exact sequence

$$0 \longrightarrow I_{K_\mathfrak{p}} \longrightarrow G_{K_\mathfrak{p}} \xrightarrow{\pi_\mathfrak{p}} G_{\mathbb{F}_\mathfrak{p}} \longrightarrow 0,$$

where $I_{K_\mathfrak{p}} = I_\mathfrak{p}$ is the projective limit of the inertia groups, which we call the *inertia group* of $K_\mathfrak{p}$ or of K at $\mathfrak{p}$. By $\mathrm{Frob}_\mathfrak{p}$ we denote both the Frobenius element in $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_\mathfrak{p})$ and its preimage in $G_{K_\mathfrak{p}}$ whenever $I_\mathfrak{p}$ is trivial. Complex conjugation can be seen as a variant of this. Suppose there is an embedding τ_∞ of K into $\mathbb{R}$. Then for any embedding $\tau\colon \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ extending τ_∞, the map

$$\tau^{-1} \circ (\text{ complex conjugation in } \mathbb{C}/\mathbb{R}) \circ \tau$$

define an element of G_K, which is called a *complex conjugation*. All complex conjugations are conjugate.

1.2 Galois Representations

Let k be a topological field. By a *n-dimensional Galois representation* we mean a continuous homomorphism

$$\rho\colon G_K \longrightarrow \mathrm{GL}_n(k).$$

The representation ρ is called an *ℓ-adic representation* if $k \subseteq \bar{\mathbb{Q}}_\ell$ and a mod ℓ *representation* if $k \subseteq \bar{\mathbb{F}}_\ell$. Two n-dimensional representations ρ_1 and ρ_2 of G_K are called *equivalent* if there is a matrix $M \in \mathrm{GL}_n(k)$ such that

$$\rho_1(g) = M\rho_2(g)M^{-1}$$

for all $g \in G_K$. Equivalence of representations is denoted $\rho_1 \sim \rho_2$. Let V be a subspace of k^n which is invariant under the action of ρ, that is, $\rho(g) \cdot v \in V$ for all $v \in V$ and $g \in G_K$, then the restriction of ρ to $\mathrm{GL}(V)$ is a *subrepresentation* of ρ. A representation is called *irreducible* if it has no proper non-trivial subrepresentations, and *semisimple* if it can be decomposed as a direct sum of irreducible representations. Note that an irreducible representation is thus semisimple. In

terms of matrices, a representation is irreducible if and only if its image is not equivalent to matrices of block triangular form

$$\begin{pmatrix} \boxed{A} & \boxed{*} & \cdots & \boxed{*} \\ \boxed{0} & \boxed{B} & \cdots & \boxed{*} \\ \vdots & \vdots & \ddots & \vdots \\ \boxed{0} & \boxed{0} & \cdots & \boxed{Z} \end{pmatrix}.$$

Let $\bar{k}$ be the algebraic closure of k. A representation $\rho\colon G_K \longrightarrow \mathrm{GL}_n(k)$ is called *absolutely irreducible* if it is irreducible as a representation over $\mathrm{GL}_n(\bar{k})$ obtained by extension of scalars.

Suppose k is a local field with ring of integers $\mathcal{O}$, maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F} = \mathcal{O}/\mathfrak{m}$. Then given a ℓ-adic representation $\rho\colon G_K \longrightarrow \mathrm{GL}_n(\mathcal{O}) \subseteq \mathrm{GL}_2(k)$ we define the mod ℓ *reduction of* ρ as

$$\bar{\rho}\colon G_K \longrightarrow \mathrm{GL}_n(\mathcal{O}) \xrightarrow{\text{natural projection}} \mathrm{GL}_n(\mathbb{F}).$$

Definition 1.3. Let $K_\mathfrak{p}$ be a finite extension of $\mathbb{Q}_p$ and let k be any topological field. Consider a local Galois representation $\rho\colon G_{K_\mathfrak{p}} \longrightarrow \mathrm{GL}_n(k)$. We say that ρ is unramified if $\rho(I_\mathfrak{p}) = 0$.

If we have global Galois representation $\rho\colon G_K \longrightarrow \mathrm{GL}_n(k)$ we say that ρ is unramified at $\mathfrak{p}$ if the restriction of ρ to $G_{K_\mathfrak{p}}$ is unramified.

Proposition 1.4. *A semisimple mod ℓ or ℓ-adic representation*

$$\rho\colon G_K \longrightarrow \mathrm{GL}_n(k)$$

with $\ell > n$ which is unramified outside a finite set of primes S is determined by $\mathrm{Tr}(\rho(\mathrm{Frob}_\mathfrak{p}))$ *on the primes $\mathfrak{p} \notin S$.*

This is a consequence of the Chebotarev Density Theorem. For ℓ-adic representations this result is proved in [2, Ch.VIII, Proposition 12.1.3], and for mod ℓ representations it is proved in [5, (30.16)].

Let ρ be a global Galois representation with $n = 1, 2$. We say that ρ is *odd* if $\det \rho(c) = -1$ for all complex conjugations c.

Example. Let K be a number field and $\bar{K}$ its algebraic closure. Let

$$\mu_m(\bar{K}) = \bar{K}^*[m]$$

be the m-torsion points of $\bar{K}^*$. By choosing a compatible system of roots of unity ζ_{ℓ^n} we obtain the isomorphism of projective systems

$$\begin{array}{ccc} \mathbb{Z}/\ell^n\mathbb{Z} & \xrightarrow[\sim]{1\mapsto\zeta_{\ell^n}} & \mu_{\ell^n}(\bar{K}) \\ \downarrow{\scriptstyle 1\mapsto 1} & & \downarrow{\scriptstyle x\mapsto x^\ell} \\ \mathbb{Z}/\ell^{n-1}\mathbb{Z} & \xrightarrow[\sim]{1\mapsto\zeta_{\ell^{n-1}}} & \mu_{\ell^{n-1}}(\bar{K}) \end{array}$$

giving rise to an isomorphism

$$\mathbb{Z}_\ell \cong \varprojlim_n \mu_{\ell^n}(\bar{K}^*) =: T_\ell(\bar{K}^*).$$

The object on the right is called the ℓ-adic Tate module of $\bar{K}^*$. Note that G_K acts compatibly on all objects on the right. Thus we can define a Galois representation

$$\chi_\ell \colon G_K \longrightarrow \mathrm{Aut}(T_\ell(\bar{K}^*)) \cong \mathbb{Z}_\ell^* = \mathrm{GL}_1(\mathbb{Z}_\ell) \hookrightarrow \mathrm{GL}_1(\mathbb{Q}_\ell),$$

which is called the *ℓ-adic cyclotomic character*.

Proposition 1.5. *Let K be a number field. The cyclotomic character χ_ℓ over K is a 1-dimensional global Galois representation, which is unramified at all primes $\mathfrak{p} \nmid l$ and is characterized by*

$$\chi_\ell(\mathrm{Frob}_p) = N(\mathfrak{p}).$$

More generally,

$$\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$$

for all $\zeta \in \mu_{\ell^n}(\bar{K}^*)$, all n and all $\sigma \in G_K$. In particular χ_ℓ is odd.

Here $N(\mathfrak{p})$ denotes the norm of $\mathfrak{p}$ in $\mathbb{Q}$, which in particular is equal to $\#\mathbb{F}_\mathfrak{p}$. Given a representation

$$\rho \colon G_K \longrightarrow \mathrm{GL}_n(\mathbb{Z}_\ell),$$

we say that ρ has determinant χ_ℓ if the composition

$$G_K \xrightarrow{\rho} \mathrm{GL}_n(\mathbb{Z}_\ell) \xrightarrow{\det} \mathbb{Z}_\ell^*$$

is equal to χ_ℓ.

Chapter 2

Elliptic Curves

In this chapter we expose some elliptic theory. We begin by the basic definitions of elliptic curve, Weierstrass equation and their main invariants. Next we introduce the concept of reduction of an elliptic curve at a prime. Finally define the Galois representations attached to elliptic curves and state some relevant results about their ramification.

The main reference for this chapter is [18], although we also follow [19] in some sections.

2.1 Basic definitions

An *elliptic curve* over a field K is a non-singular plane cubic curve E defined over K and such that $E(K) \neq \emptyset$. A *normalized Weierstrass form* for a cubic plane curve C over a field K is an equation of the form

$$y^2 = f(x) = x^3 + ax^2 + bx + c, \tag{2.1}$$

with $a, b, c \in K$. In this configuration C has only one point at infinity, given by $O = [0 : 1 : 0]$. Let us denote by $e_1, e_2, e_3 \in \bar{K}$ the roots of $f(x)$. We define the quantities

$$\begin{aligned}
\Delta &= 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2, \\
c_4 &= 16((e_1 - e_2)^2 - (e_2 - e_3)(e_3 - e_1)), \\
c_6 &= -32(e_1 - e_2)(e_2 - e_3)(e_3 - e_1).
\end{aligned}$$

The first one is called the *discriminant* of the Weierstrass equation. The point O is never singular, hence any singular point (x_0, y_0) in C must satisfy $y_0 = f(x_0) = 0$. Therefore C is an elliptic curve if and only if $f(x)$ does not have repeated roots, that is if and only if $\Delta \neq 0$. Moreover, if $\Delta = 0$ then C has a node (i.e. two repeat roots) if $c_4 \neq 0$ and a cusp (i.e. three repeated roots) if $c_4 = 0$. If C is an elliptic curve we can define the *j-invariant* as

$$j = c_4^3/\Delta.$$

Any elliptic curve over a field K with $\mathrm{char}(K) \neq 2$ can be expressed as a Weierstrass equation uniquely up to a change of coordinates of the form

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t, \end{aligned} \tag{2.2}$$

with $u, r, s, t \in \bar{K}$ and $u \neq 0$. Further, if $\mathrm{char}(K) \neq 3$, there is a Weierstrass equation with $a = 0$. We will mainly use the model (2.1) above, except in particular cases where the assumption $a = 0$ makes the computations more comfortable. Under a change of variables of the form (2.2) the old and new discriminant and c_4, c_6 invariants are related by

$$\Delta' = u^{-12}\Delta, \qquad c_4' = u^{-4}c_4, \qquad c_6' = u^{-6}c_6, \tag{2.3}$$

while the j-invariant remains unchanged. Moreover,

Proposition 2.1. *Two elliptic curves over K are isomorphic (over $\bar{K}$) if and only if they have the same j-invariant.*

Given an elliptic curve E/K as

$$E\colon y^2 = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3),$$

the substitution

$$x = (e_2 - e_1)x' + e_1, \;\; y = (e_2 - e_1)^{3/2}y'$$

yields an equation of the form

$$y^2 = x(x - 1)(x - \lambda), \;\; \lambda = \frac{e_3 - e_1}{e_2 - e_1}.$$

Such an equation is called *Legendre form* for E. Observe that λ is well defined because as stated above, the three roots must be different. By the symmetry of the roots, we could permute them to obtain six different Legendre forms. If μ is the result of one of these permutations on λ then

$$\mu \in \left\{\lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1 - \lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda}\right\}.$$

In terms of λ the j-invariant of E is given by

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

2.2 The Group Law

Let E be an elliptic curve given by a Weierstrass equation. Recall that $E \subset \mathbb{P}^2$ consists of the points (x, y) satisfying the equation together with the point at infinity $O = [0 : 1 : 0]$. By Bézout's theorem any line intersects E at three points,

counting multiplicities. We can construct consequently the following composition law, which we denote by $+$: given two points $P, Q \in E$, let L be the line passing throught P and Q. We call $P * Q$ be the third point of intersection of L and E. Now let L' be the line passing through O and $P * Q$, then $P + Q$ is the third intersection point of E and L'. In other words, $P + Q = (P * Q) * O$.

It is clear that $P + O = (P * O) * O = P$. Note that the point O is an inflection point of E, this implies that $P + P * O = (P * (P * O)) * O = O * O = O$, and we will call $P * O = -P$. In coordinates, if $P = (x, y)$ then $-P = (x, -y)$, because the line connecting P and O is the vertical line crossing P.

Proposition 2.2. *The composition law makes E into an abelian group.*

Observe that if E is defined over fields $K \subset L$ then $E(K)$ is a subgroup of $E(L)$, because the intersection of lines defined in K lies in K, hence by the construction and the fact that $O \in K$ we see that the addition of two points in K lies in K.

We denote, for $P \in E$ and $m > 0$,

$$[0]P = O,$$
$$[m]P = P + \cdots + P \ \ (m \text{ times}).$$

The points which satisfy $[m]P = O$ are called *m-torsion* points of E. We do not give explicit equations for the addition law, but it follows from the fact that they are rational functions on the coordinates and the coefficients of the Weierstrass equation that any torsion point is the root of a polynomial in K, hence any torsion point is algebraic over K. We will denote by $E[m]$ the set of m-torsion points of E over an algebraically closed field, that is, the full set of m-torsion points, otherwise we will specify by $E(K)[m]$ the set of m-torsion points over K. It is clear that the sum of m-torsion points is an m-torsion point, hence $E[m]$ is a subgroup of $E(\bar{K})$ and $E(K)[m]$ is a subgroup of $E(K)$. The full torsion subgroup of E is denoted E_{tors}.

For instance, if $P = (x, y) \in E$ and $[2]P = O$, then $P = -P$, which implies that $(x, y) = (x, -y)$ and therefore $y = 0$. Thus x must be a root of the polynomial f, so E has four 2-torsion points, the three roots of f and O. If $[3]P = O$ then $[2]P = -P$, or what is the same $P * P = P$, which means that P is an inflection point. Any smooth cubic curve over an algebraically closed field of characteristic 0 has nine inflection points, it follows that in this case E has nine 3-torsion points. In general we have

Proposition 2.3. *Let E be an elliptic curve and $m > 0$. Let K be a field of characteristic 0. Then*

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

At the moment we have seen that an elliptic curve has two distinct structures, namely the structure of algebraic variety and the structure of abelian group. Thus to define morphisms between elliptic curves it is natural to ask for both of them to be respected. However, the following theorem asserts that any morphism as algebraic curves between elliptic curves satisfying an additional weak condition preserves the group structure.

Theorem 2.4. *Let E and E' be two elliptic curves with identity elements O and O' respectively, and let ϕ be a morphism of algebraic curves from E to E'. Then ϕ is a group homomorphism from E to E' if and only if $\phi(O) = O'$.*

A non-constant map satisfying this property is called an *isogeny*. By the previous theorem an isogeny satisfies $\phi(P + P') = \phi(P) + \phi(P')$ for all $P, P' \in E$, where addition on the left is on the curve E, while addition on the right is on the curve E'. An isogeny is always surjective and has finite kernel.

2.3 Elliptic curves over local fields

For this section we set K to be a complete local field, which we can think of the localization at some prime of a number field, and we set the following notation

- $\mathcal{O}$ the ring of integers,
- $\mathfrak{m}$ the maximal ideal of $\mathcal{O}$,
- π a uniformizer of $\mathfrak{m}$,
- $\mathbb{F}$ the residue field of $\mathcal{O}$, $\mathbb{F} = \mathcal{O}/\mathfrak{m}$,
- v the normalized valuation on K.

Let E/K be an elliptic curve, and let

$$y^2 = x^3 + ax^2 + bx + c$$

be a Weierstrass equation for E/K. By a change of coordinates as in (2.2) with u divisible by large powers of π we can find a Weierstrass equation with $a, b, c \in \mathcal{O}$. In this case $\Delta \in \mathcal{O}$ also, and since v is discrete there is a Weierstrass equation with $v(\Delta)$ as small as possible. A Weierstrass equation with minimum $v(\Delta)$ and $a, b, c, \in \mathcal{O}$ is called *minimal Weierstrass equation* for E. As any two Weierstrass equations are related by a change of coordinates as in (2.2) we have that $v(\Delta)$ can only be changed by multiples of 12 and $v(c_4)$ by multiples of 4. Hence if given an equation either $v(\Delta) < 12$ or $v(c_4) < 4$ it follows that it is minimal.

Now we look at the reduction modulo π operation, which we denote by a tilde. For example the natural map $\mathcal{O} \to \mathbb{F}$ is denoted by $t \mapsto \tilde{t}$. Given a minimal Weierstrass equation for E/K, we can reduce its coefficients modulo π to obtain a curve over $\mathbb{F}$, namely

$$\tilde{E}\colon y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c}.$$

If $P \in E(K)$, then we can find homogenous coordinates such that $P = (x_0 : y_0 : z_0)$ with $x_0, y_0, z_0 \in \mathcal{O}$ and at least one of them in $\mathcal{O}^*$. Then the reduced point $\tilde{P} = (\tilde{x}_0 : \tilde{y}_0 : \tilde{z}_0)$ belongs to $\tilde{E}(\mathbb{F})$. This gives a reduction map $E(K) \to \tilde{E}(\mathbb{F})$ given by $P \mapsto \tilde{P}$. The curve $\tilde{E}/K$ may or not be singular, but it is one of the three types mentioned in section 2.1, and we can classify E according to these possibilities.

Definition 2.5. Let E/K be an elliptic curve, and let $\tilde{E}$ be its reduction modulo π.

(a) E has *good reduction* over K if $\tilde{E}$ is non-singular.

(b) E has *multiplicative reduction* over K if $\tilde{E}$ has a node.

(c) E has *additive reduction* over K if $\tilde{E}$ has a cusp.

In cases (a) and (b) E is said to be *semistable*, and in cases (b) and (c) it is naturally said to have *bad reduction*. Furthermore, if E has multiplicative reduction, then the reduction is said to be *split* if the slope of the tangent lines at the node are in $\mathbb{F}$, and *non-split* if the tangent lines at the node are not in $\mathbb{F}$. The reduction type of an elliptic curve can be read off from its minimal Weierstrass equation.

Proposition 2.6. *Let E/K be an elliptic curve with minimal discriminant Δ and c_4 as usual.*

(a) *E has good reduction if and only if $v(\Delta) = 0$ (i.e. $\Delta \in \mathcal{O}^*$).*

(b) *E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$ (i.e. $\Delta \in \mathfrak{m}$ and $c_4 \in \mathcal{O}^*$).*

(c) *E has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$ (i.e. $\Delta, c_4 \in \mathfrak{m}$).*

Even if an elliptic curve E/K has bad reduction, it is often useful to know whether it attains good reduction over some extension of K. Thus, E is said to have *potentially good reduction* if there is a finite extension K'/K such that E has good reduction over K'. Equivalently E is said to have *potentially multiplicative reduction* if there is a finite extension K'/K such that E has multiplicative reduction over K'. The next two results give a characterization of the reduction of curves over field extensions.

Proposition 2.7. *Let E/K be an elliptic curve.*

(a) *Let K'/K be an unramified extension. Then the reduction type of E of K is the same as the reduction type of E over K'.*

(b) *Let K'/K be any field extension. If E has either good or multiplicative reduction over K, then it has the same reduction type over K'.*

(c) *There exists a finite extension K'/K so that E has either good or split multiplicative reduction over K'.*

Proposition 2.8. *Let E/K be an elliptic curve. Then E has potentially good reduction if and only if its j-invariant is integral.*

Since Proposition 2.7 tells us that E has either potentially good or multiplicative reduction we also have that E has potentially multiplicative reduction if and only if its j-invariant is non integral. The precise extension where an elliptic curve attains split multiplicative reduction can be deduced from the theory of the Tate curve, which we briefly explain in the next section.

If K is a number field and E/K is an elliptic curve, then the reduction type of E at a prime $\mathfrak{p}$ is the reduction type of E as a curve in $K_{\mathfrak{p}}$, and E is called *semistable* if it is semistable at every prime.

2.4 Discriminant, Conductor and L-series

Let K be a number field and E/K an elliptic curve. For each prime ideal $\mathfrak{p}$ of K we can consider a minimal Weierstrass equation for the local field $K_\mathfrak{p}$, and the minimal discriminant $\Delta_\mathfrak{p}$ of this equation. The *minimal discriminant* of E/K is the integral ideal

$$\Delta_E = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\Delta_\mathfrak{p})}.$$

If K has class number 1 then it is possible to find an equation with discriminant Δ_E. Such an equation is called *global minimal Weierstrass equation*.

More generally, let S be finite set of primes in K, we define the ring of S-integers as

$$\mathcal{O}_S = \{x \in K \colon v_\mathfrak{p}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}.$$

Then if $\mathcal{O}_S$ contains the prime ideals above 2 and 3 and it is a principal ideal domain every elliptic curve E/K has a model

$$E \colon y^2 = x^3 + Ax + B$$

such that $A, B \in \mathcal{O}_S$ and its discriminant $\Delta = -16(4A^3 + 27B^2)$ satisfies

$$\Delta_E \mathcal{O}_S = \Delta \mathcal{O}_S.$$

Such an equation is called *S-minimal Weierstrass equation*. Let us see where the existence of this model comes from. Let $y^2 = x^3 + Ax + B$ be any Weierstrass equation for E. Then for each $\mathfrak{p} \notin S$ we choose a $u_\mathfrak{p} \in K^*$ such that the substitution $x = u_\mathfrak{p}^2 x'$ and $y = u_\mathfrak{p}^3 y'$ gives a minimal equation at $\mathfrak{p}$. Since $\mathcal{O}_S$ is principal there is a $u \in K^*$ such that $v_\mathfrak{p}(u) = v_\mathfrak{p}(u_\mathfrak{p})$ for all $\mathfrak{p} \notin S$. As a consequence the equation

$$y^2 = x^3 + u^{-4}Ax + u^{-6}B$$

is S-minimal.

Theorem 2.9. *Let S be a finite set of primes in K. Then, up to isomorphism, there are only finitely many elliptic curves E/K having good reduction outside S.*

Proof. Note that we are proving something stronger if we enlarge S. Hence we may assume that S contains all prime ideals above 2 and 3 and further that the ring of S-integers $\mathcal{O}_S$ is a principal ideal domain. Under this assumptions we know that any elliptic curve E/K has a global S-minimal equation

$$E \colon y^2 = x^3 + Ax + B \qquad A, B \in \mathcal{O}_S,$$

with discriminant $\Delta = -16(4A^3 + 27B^2)$ satisfying $\Delta_E \mathcal{O}_S = \Delta \mathcal{O}_S$. Observe that since E has good reduction outside S then $v_\mathfrak{p}(S) = 0$ for all $\mathfrak{p} \notin S$. Therefore $\Delta \in \mathcal{O}_S^*$.

Consider the class of Δ into $\mathcal{O}_S^*/(\mathcal{O}_S^*)^{12}$. By the Dirichlet unit theorem for number fields this group is finite, and hence there is a finite number of classes of

discriminants. Thus we can restrict our attention to one such class. Denote by $E_1, E_2, \ldots$ the elliptic curves with bad reduction outside S and discriminant in our particular class. Write also A_i, B_i, Δ_i for their corresponding quantities. Then we may write, for all i, $\Delta_i = CD_i^{12}$ for a fixed $C \in \mathcal{O}_S^*$and some $D_i \in \mathcal{O}_S^*$.

The formula $\Delta = -16(4A^3 + 27B^2)$ implies that for each i, the point

$$(-12A_i/D_i^{12}, 108B_i/D_i^6)$$

is an S-integral point on the elliptic curve

$$Y^2 = X^3 - 27C.$$

By Siegel's theorem ([18], IX.3) there are only finitely many such points, and so only finitely many possibilities for A_i/D_i^4 and B_i/D_i^6. Moreover, if $A_i/D_i^4 = A_j/D_j^4$ and $B_i/D_i^6 = B_j/D_j^6$ then the change of variables

$$x = (D_i/D_j)^2 x', \qquad y = (D_i/D_j)^3 y'$$

gives an isomorphism from E_i to E_j. Therefore there is finitely many K-isomorphism classes of elliptic curves with good reduction outside S. □

The minimal discriminant is a measure of bad reduction of E. Another such a measure is the *conductor* of E/K. This is an ideal

$$N_{E/K} = \prod_{\mathfrak{p}} \mathfrak{p}^{f_{\mathfrak{p}}(E/K)},$$

where the exponents are given by

$$f_{\mathfrak{p}}(E/K) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } \mathfrak{p}, \\ 1 & \text{if } E \text{ has multiplicative reduction at } \mathfrak{p}, \\ 2 & \text{if } E \text{ has bad reduction at } \mathfrak{p} \text{ and } \mathfrak{p} \nmid 6. \end{cases}$$

If $\mathfrak{p}$ has residue characteristic 2 or 3 and E has additive reduction at $\mathfrak{p}$ then $f_{\mathfrak{p}}(E/K) = 2 + \delta_{\mathfrak{p}}$, where $\delta_{\mathfrak{p}} \geq 0$. The only fact towards the determination of $\delta_{\mathfrak{p}}$ we will state is the following proposition, which follows from [19, p. 380-381].

Proposition 2.10. *Let E/K be an elliptic curve with additive reduction at a prime ideal $\mathfrak{p}$ above 2 or 3. If there is a prime ℓ such that $\mathfrak{p} \nmid \ell$ and such that E has full ℓ-torsion over K (i.e. $\#E(K)[\ell] = \ell^2$) then $\delta_{\mathfrak{p}} = 0$.*

Note that if E is semistable then the conductor is just the product of the bad primes.

Finally, let us introduce the L-function of an elliptic curve. For a prime $\mathfrak{p}$ of good reduction, define

$$a_{\mathfrak{p}} = N(\mathfrak{p}) + 1 - \#E(\mathbb{F}_{\mathfrak{p}}),$$

where $\#E(\mathbb{F}_{\mathfrak{p}})$ is the number of points of the elliptic curve reduced to the residue field $\mathbb{F}_{\mathfrak{p}}$. There is a bound on the number $a_{\mathfrak{p}}$ which we will be useful later on.

Theorem 2.11 (Hasse)**.** $a_{\mathfrak{p}} \leq 2\sqrt{N(\mathfrak{p})}$.

The *local factor of the L-series* of E at $\mathfrak{p}$ is the polynomial

$$L_{\mathfrak{p}}(T) = \begin{cases} 1 - a_{\mathfrak{p}}T + N(\mathfrak{p})T^2 & \text{if } E \text{ has good reduction at } \mathfrak{p}, \\ 1 - T & \text{if } E \text{ has split multiplicative reduction at } \mathfrak{p}, \\ 1 + T & \text{if } E \text{ has non-split multiplicative reduction at } \mathfrak{p}, \\ 1 & \text{if } E \text{ has additive reduction at } \mathfrak{p}. \end{cases}$$

The *Hasse-Weil L-series* of E/K is defined by the Euler product

$$L(E/K, s) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(N(\mathfrak{p})^{-s})^{-1}.$$

2.5 Galois representations

For this section we assume K to be a number field. Let E/K be an elliptic curve given by a Weierstrass equation

$$E\colon y^2 = x^3 + ax^2 + bx + c.$$

Since the coefficients of this equation belong to K, we have that for any $\sigma \in G_K$

$$\sigma(y)^2 = \sigma(x^3 + ax^2 + bx + c) = \sigma(x)^3 + a\sigma(x)^2 + b\sigma(x) + c,$$

so that the absolute Galois group G_K acts on E. Furthermore, if we denote by $\sigma(P)$ the image of $P \in E$ we have that $[m]\sigma(P) = \sigma([m]P)$. As a consequence G_K takes m-torsion points to m-torsion points. We thus obtain a representation

$$\bar{\rho}_{E,\ell}\colon G_K \longrightarrow \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

where the isomorphism involves choosing a basis for $E[m]$. Now, let ℓ be a prime different from $\mathrm{char}(K)$. Analogously to the construction of the ℓ-adic Tate module of a field K, we can construct the ℓ-adic *Tate module* associated to E,

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

where the inverse limit is taken with respect to the natural maps given by multiplication by $[\ell]$.

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Since $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$, we have that as a $\mathbb{Z}_\ell$-module

$$T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell.$$

Now, since the action of G_K on $E[\ell^n]$ commutes with the multiplication map used in the inverse limit, we have that G_K acts naturally on the Tate module, and thus we obtain a representation

$$\rho_{E,\ell}\colon G_K \longrightarrow \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell),$$

where again the isomorphism involves choosing a $\mathbb{Z}_\ell$ basis for $T_\ell(E)$. The reduction of $\rho_{E,\ell}$ to $\mathrm{GL}_2(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell) \cong \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is precisely the representation $\bar{\rho}_{E,\ell}$.

Proposition 2.12. *The determinant of $\rho_{E,\ell}$ is the cyclotomic character χ_ℓ.*

Theorem 2.13. *Let E be an elliptic curve over K. Then $\rho_{E,\ell}$ is unramified at a prime $\mathfrak{p}$ if $\mathfrak{p} \nmid \ell$ and $\mathfrak{p}$ is a prime of good reduction.*

This is consequence of the Criterion of Néron-Ogg-Shafarevich [18, Theorem VII.7.1]. If $\mathfrak{p}$ is such a prime, we can speak about the image of a Frobenius element, and in fact since the determinant of $\rho_{E,\ell}$ is the cyclotomic character we have $\det \rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p}) = N(\mathfrak{p})$. Furthermore,

$$\mathrm{Tr}(\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})) = a_\mathfrak{p}.$$

It is clear that if $\rho_{E,\ell}$ is unramified at a prime $\mathfrak{p}$ then so is its reduction $\bar{\rho}_{E,\ell}$. However, the representation $\bar{\rho}_{E,\ell}$ can be unramified at more primes than $\rho_{E,\ell}$. To characterize the ramification of the reduced representation we need to introduce the Tate curve. For more details on the theory of the Tate curve we refer to [19, Ch. V].

For the sake of notation we take now K to be a local field, which we can imagine as the localization at some prime $\mathfrak{p}$ of a number field, and we follow the same notation as in Section 2.3. Any $q \in K^*$ with $v(q) > 0$ generates a discrete subgroup $K^*/q^{\mathbb{Z}}$, where

$$q^{\mathbb{Z}} = \{q^i \colon i \in \mathbb{Z}\}.$$

For any such a q, there is an analytic isomorphism from $K^*/q^{\mathbb{Z}}$ to an elliptic curve E_q defined over K, which is called the Tate curve.

Theorem 2.14. *Let $q \in K^*$ with $v(q) > 0$. There is an elliptic curve E_q/K and a v-analytic isomorphism*

$$\phi\colon \bar{K}^*/q^{\mathbb{Z}} \longrightarrow E_q(\bar{K}).$$

Moreover, the map ϕ is compatible with the action of the Galois group, in the sense that $\phi(\sigma(u)) = \sigma(\phi(u))$ for all $u \in \bar{K}^*$ and $\sigma \in G_K$. In particular, ϕ induces an isomorphism $L^*/q^{\mathbb{Z}} \xrightarrow{\sim} E(L)$ when restricted to any algebraic extension L/K.

The j-invariant of E_q can be written in terms of q as a power series,

$$j(E_q) = \frac{1}{q} + 744 + 196884q + \cdots \in \frac{1}{q} + \mathbb{Z}[[q]].$$

It is clear from this expression that $v(j(E_q)) = -v(q) < 0$, so that the j-invariant is non-integral, and hence a necessary condition for an elliptic curve E to be isomorphic (over $\bar{K}$) to an E_q is $v(j(E)) < 0$. This condition is also sufficient, and moreover for any j such that $v(j) < 0$ there is a unique E_q such that $j(E_q) = j$.

In fact, in this case E is isomorphic to E_q over either K or a quadratic extension of K. To characterize these two cases we need to define the invariant

$$\gamma(E/K) = -c_4/c_6 \in K^*/K^{*2}$$

attached to a Weierstrass equation for E. It is straight forward to see that $\gamma(E/K)$ is well-defined as an element of K^*/K^{*2}, since for any other Weierstrass equation we will have $c_4'/c_6' = u^2 c_4/c_6$, with $u \in K^*$.

Theorem 2.15. *Let E/K be an elliptic curve with $v(j(E)) < 0$ and let $\gamma(E/K)$ be defined as above.*

(a) The following are equivalent.

(i) E is isomorphic to E_q over K.

(ii) E has split multiplicative reduction.

(iii) $\gamma(E/K) = 1$.

(b) Suppose $\gamma(E/K) \neq 1$. Note that then

$$L = K\left(\sqrt{\gamma(E/K)}\right)$$

is a quadratic extension. Let

$$\chi\colon G_K \longrightarrow G_{L/K} \longrightarrow \{\pm 1\}$$

be the quadratic character associated to the extension L/K. Then there is an isomorphism

$$\psi\colon E \longrightarrow E'$$

over L such that $\psi(\sigma(P)) = \chi(\sigma)\sigma(\psi(P))$ for all $\sigma \in G_K$ and $P \in E$.

The relation between E_q and E in case (b) can also be expressed by saying that E_q is the *twist* of E by the quadratic character χ, and denoted by $E_q = E \otimes \chi$. In terms of Weierstrass equations, suppose E is given by

$$E\colon y^2 = x^3 + ax^2 + bx + c,$$

and to simplify notation call $\gamma = \sqrt{\gamma(E/K)}$. Then $E \otimes \chi$ has an equation

$$E \otimes \chi\colon \gamma y^2 = x^3 + ax^2 + bx + c.$$

Now, let us return to K the role of number field. Let $\mathfrak{q}$ be a prime of K, $\mathbb{F}_\mathfrak{q}$ its residue field and denote by q the number of elements in $\mathbb{F}_\mathfrak{q}$When we reduce

the equations above to $\mathbb{F}_q$ then γ may be a square or not. If it is a square then $\#E(\mathbb{F}_\mathfrak{q}) = \#E \otimes \chi(\mathbb{F}_\mathfrak{q})$, and if it is not a square then

$$\#E(\mathbb{F}_\mathfrak{q}) + \#E \otimes \chi(\mathbb{F}_\mathfrak{q}) = 2q + 2.$$

If $\mathfrak{q}$ is a prime of good reduction of E, the last equalities can be written as

$$a_\mathfrak{q}(E) = \chi(\mathfrak{q}) a_\mathfrak{q}(E \otimes \chi),$$

where χ is a quadratic character attached to some cyclic extension of K which takes the value 1 if γ is a square in $\mathbb{F}_\mathfrak{q}$ and -1 if it is not. In case $K = \mathbb{Q}$ this character is precisely the Legendre symbol $\left(\frac{q}{\gamma}\right)$.

By using the Tate curve we can prove the following two results about the ramification of the reduced Galois representation associated to an elliptic curve.

Theorem 2.16. *Let K be a number field and E/K an elliptic curve. Let $\mathfrak{p}$ be a prime of K where E has potentially multiplicative reduction and let $\ell \geq 3$ be a rational prime. Suppose that $\ell \nmid v_\mathfrak{p}(j(E))$. Then the reduced representation $\bar{\rho}_{E,\ell}$ is ramified at $\mathfrak{p}$.*

Proof. We will show that there is an element in the inertia subgroup $I_\mathfrak{p}$ which acts on the ℓ torsion subgroup $E[\ell]$ via a matrix of the form $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Note that in particular this implies that $\ell \mid \#\bar{\rho}_{E,\ell}(I_\mathfrak{q})$.

Observe that it is enough to find a finite extension $L/K_\mathfrak{p}$ and an element σ in the inertia subgroup I_L of G_L acting as mentioned above, since $I_L \subseteq I_\mathfrak{q}$. Recall that by Theorem 2.15 E is isomorphic to a Tate curve E_q either over $K_\mathfrak{p}$ or over a quadratic extension of $K_\mathfrak{p}$. Thus replacing $K_\mathfrak{p}$ by this extension it suffices to prove the theorem for E_q. We will also assume that K contains a primitive ℓ^{th}-root of unity ζ.

Let $Q = q^{\frac{1}{\ell}}$ be a fixed ℓ^{th}-root of q. Since $v_\mathfrak{p}(q) = -v_\mathfrak{p}(j)$ is not divisible by ℓ, the extension $K_\mathfrak{p}(Q)/K_\mathfrak{p}$ is totally ramified. As a consequence there exists an element $\sigma \in I_\mathfrak{p}$ such that $\sigma(Q) = \zeta Q$.

Now, by Theorem 2.14 there is an isomorphism

$$\phi\colon \bar{K}^*/q^{\mathbb{Z}} \xrightarrow{\sim} E_q(\bar{K}_\mathfrak{p})$$

satisfying $\phi(\sigma(P)) = \sigma(\phi(P))$ for all $P \in \bar{K}^*$. It is clear that under this isomorphism we have

$$\phi\colon (\zeta^{\mathbb{Z}} \cdot Q^{\mathbb{Z}})/q^{\mathbb{Z}} \xrightarrow{\sim} E_q[\ell].$$

Therefore if we take as basis of $E_q[\ell]$ the elements $P_1 = \phi(\zeta)$ and $P_2 = \phi(Q)$ we have that

$$\begin{aligned} \sigma(P_1) &= \sigma(\phi(\zeta)) = \phi(\sigma(\zeta)) = \phi(\zeta) = P_1, \\ \sigma(P_2) &= \sigma(\phi(Q)) = \phi(\sigma(Q)) = \phi(\zeta Q) = P_1 + P_2, \end{aligned}$$

as we wanted to see. □

The converse is true if we change the condition on E of having potentially multiplicative reductional $\mathfrak{p}$ by the stronger condition of having multiplicative reduction at $\mathfrak{p}$ and if we suppose that $\mathfrak{p} \nmid \ell$.

Proposition 2.17. *Let K be a number field and E/K an elliptic curve. Let $\mathfrak{p}$ be a prime of K where E has multiplicative reduction and let $\ell \geq 3$ be a rational prime such that $\mathfrak{p} \nmid \ell$. Suppose that $\ell \mid v_{\mathfrak{p}}(j(E))$. Then the reduced representation $\bar{\rho}_{E,\ell}$ is unramified at $\mathfrak{p}$.*

Proof. By Theorem 2.15 we have that E is isomorphic to E_q for some q, and that

$$\phi\colon (\zeta^{\mathbb{Z}} \cdot Q^{\mathbb{Z}})/q^{\mathbb{Z}} \xrightarrow{\sim} E[\ell],$$

where as before $Q = q^{\frac{1}{\ell}}$. Moreover the Galois action satisfies

$$\phi(\sigma(P)) = \chi(\sigma)\sigma(\phi(P)),$$

where χ is trivial if E has split multiplicative reduction and the quadratic character attached to $K_{\mathfrak{p}}(\sqrt{\gamma})/K_{\mathfrak{p}}$ if E has non-split multiplicative reduction. Since $\mathfrak{p} \nmid \ell$ and $\ell \mid v_{\mathfrak{p}}(q)$ we have that the extension $K_{\mathfrak{p}}(\zeta, Q)$ is unramified. Therefore, in principle, the inertia subgroup can only act on $E[\ell]$ through the character χ. However since E has multiplicative reduction we have that $v_p(\gamma) = v_{\mathfrak{p}}(c_4/c_6) = 0$, so that the extension $K_{\mathfrak{p}}(\sqrt{\gamma})/K_{\mathfrak{p}}$ is unramified. This implies that $\chi(\sigma) = 1$ for all $\sigma \in I_{\mathfrak{p}}$. As a consequence $E[\ell]$ is unramified, as we wanted to see.

□

Note that in this case, since E has multiplicative reduction at $\mathfrak{p}$, we have that $v_{\mathfrak{p}}(c_4) = 0$, so that we could change the condition $\ell \mid v_{\mathfrak{p}}(j)$ by $\ell \mid v_{\mathfrak{p}}(\Delta)$, in view of the equality $j = c_4^3/\Delta$.

For $\mathfrak{p} \mid \ell$ there is a result which states that with the conditions of Proposition 2.17 the reduced representation $\bar{\rho}_{E,\ell}$ is flat at $\mathfrak{p}$. Both the notion of flatness and the proof of this result are beyond the scope of this work and we refer the reader to [6, Ch. V] for more information.

We also state the following result towards the ramification of elliptic curves with potentially good reduction which is developed for example in [15].

Proposition 2.18. *Let E/K be an elliptic curve with potentially good reduction at a prime $\mathfrak{p}$ of K, then $\#\rho_{E,\ell}(I_{\mathfrak{p}}) \mid 24$ for all primes ℓ.*

Chapter 3

Modular Forms

In this sections we give the necessary information about modular forms for dealing with FLT. We begin with the notions of congruence subgroup and modular form with a congruence subgroup. Next we explain Hecke operators and introduce the notion of newform. Then we introduce the L-function and the Galois representations attached to modular forms. In the last section we introduce Hilbert modular forms.

The main references for this chapter are [8] and [14] for the modular forms part and [3] and [1] for the Hilbert modular forms section.

3.1 The Modular Group

We define the the *modular group* as,

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Let $\hat{\mathbb{C}}$ denote $\mathbb{C} \cup \{\infty\}$, i.e. the Riemann sphere. Given a point $z \in \hat{\mathbb{C}}$ we define

$$\alpha(z) = \frac{az + b}{cz + d} \qquad \text{for all} \qquad \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

This is understood to mean that if $c \neq 0$ then $-d/c$ maps to ∞ and ∞ maps to a/c, and if $c = 0$ then ∞ maps to ∞. These maps are called fractional linear transformations of the Riemann sphere. It is easy to check that the map defined above defines a group action on the set $\hat{\mathbb{C}}$, that is, $\alpha_1(\alpha_2(z)) = (\alpha_1 \cdot \alpha_2)(z)$. Note that each pair of matrices $\pm\alpha \in \mathrm{SL}_2(\mathbb{Z})$ gives a single transformation. Hence we actually have an action of $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$ on $\hat{\mathbb{C}}$.

Let $\mathcal{H} \subset \mathbb{C}$ denote the upper half plane $\mathcal{H} = \{z \in \mathbb{C} \colon \mathrm{Im}(z) > 0\}$. Then an easy calculation shows that

$$\mathrm{Im}(\alpha(z)) = \frac{\mathrm{Im}(z)}{|cz + d|^2},$$

which implies that if $z \in \mathcal{H}$ then $\alpha(z) \in \mathcal{H}$, so that the modular group acts on the upper half plane. When we study modular forms we will be interested in the action on $\mathcal{H}$ of some subgroups of de modular group, the congruence subgroups. Given a positive integer N, the *principal congruence subgroup of level* N is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

where the matrix congruence is interpreted coefficient wise. In particular we denote $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Observe that $\Gamma(N)$ is the kernel of the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ so that it is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a *congruence subgroup* if $\Gamma(N) \subset \Gamma$. The main examples of congruence subgroups are

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

where $*$ means unspecified, and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

satisfying $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$, and furthermore all these are normal subgroup inclusions.

The action of a subgroup G of $\mathrm{SL}_2(\mathbb{Z})$ divides $\mathcal{H}$ into equivalence classes. We say that two points $z_1, z_2 \in \mathcal{H}$ are *G-equivalent* if there exists $g \in G$ such that $gz_1 = z_2$. Let F be a closed region in $\mathcal{H}$. We say that F is a *fundamental domain* for the subgroup G if every $z \in H$ is G-equivalent to a point in F, but no two distinct points in the interior of F are G-equivalent (two boundary points are permitted to be equivalent). The most usual example of fundamental domain is the fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$, given by

$$F = \{z \in H \colon -\frac{1}{2} \leq \Re(z) \leq \frac{1}{2} \text{ and } |z| \geq 1\}.$$

Let $\hat{\mathcal{H}}$ denote the set $\mathcal{H} \cup \{\infty\} \cup \mathbb{Q}$. That is, we add to $\mathcal{H}$ a point at infinity and also the rational numbers on the real axis. These points $\{\infty\} \cup \mathbb{Q}$ are called *cusps*. It is not difficult to see that $\mathrm{SL}_2(\mathbb{Z})$ permutes the cusps transitively. For instance, for any a/c in lower terms there is a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $ad - bc = 1$, and this matrix maps ∞ to a/c. Therefore all rational numbers are in the same $\mathrm{SL}_2(\mathbb{Z})$-equivalence class as ∞.

We can extend the usual topology on $\mathcal{H}$ to the set $\mathcal{H}$ as follows. First, a fundamental system of open neighborhoods of ∞ is

$$N_C = \{z \in \mathcal{H} \colon \mathrm{Im}(z) > C\} \cup \{\infty\}$$

for any $C > 0$. Note that under the map $z \mapsto q = e^{2\pi i z}$ and $\infty \mapsto 0$ the open sets N_C map to the disk of radius $e^{-2\pi C}$ centered at the origin. We can use this map to

define an analytic structure on $\mathcal{H} \cup \{\infty\}$, that is, given a function on $\mathcal{H}$ of period 1, we say that it is meromorphic at ∞ if it can be expressed as a power series in the variable q having at most finitely many negative terms. That is

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n$$

with $a_n = 0$ for $n << 0$. We say that $f(z)$ is holomorphic at ∞ if $a_n = 0$ for all $n < 0$, and we say that $f(z)$ vanishes at ∞ if $a_n = 0$ for all $n \leq 0$. More generally, if $f(z)$ has period N we use the map $z \mapsto q_N = e^{2\pi i z/N}$ to map $\mathcal{H} \cup \{\infty\}$ to the open unit disk.

Next, we set as fundamental system of open neighborhoods of a given $a/c \in \mathbb{Q}$ as the images $\alpha^{-1} N_C$, where $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Note that the resulting open sets are disks tangent to the real axis at a/c with decreasing radius as C increases.

3.2 Modular Forms

Let $f(z)$ be a meromorphic function on the upper half plane $\mathcal{H}$, and let k be an integer. Suppose that there is a $k \in \mathbb{Z}$ such that $f(z)$ satisfies the relation

$$f(\alpha z) = (cz + d)^k f(z) \text{ for all } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

This relation will be called *modularity condition*. Note that in particular, since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, the modularity condition tells us that

$$f(z + 1) = f(z).$$

This implies that it has a Fourier expansion

$$f(z) = \sum_{n \in \mathbb{Z}} a_n q^n.$$

If $f(z)$ is holomorphic at ∞, i.e. $a_n = 0$ for all $n < 0$, then $f(z)$ is called a *modular form* of weight k for $\mathrm{SL}_2(\mathbb{Z})$. The set of such functions is denoted by $M_k(\mathrm{SL}_2(\mathbb{Z}))$. If we further have that $f(z)$ vanishes at infinity, i.e. $a_n = 0$ for all $n \leq 0$, then $f(z)$ is called a *cusp form* of weight k for $\mathrm{SL}_2(\mathbb{Z})$. The set of such functions is denoted by $S_k(\mathrm{SL}_2(\mathbb{Z}))$. For a given $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ we define the operator $[\alpha]_k$ as

$$f[\alpha]_k(z) = (cz + d)^{-k} f(\alpha z).$$

Using this operator the modularity condition can be rewritten as

$$f[\alpha]_k = f.$$

Note that if k is odd then $M_k(\mathrm{SL}_2(\mathbb{Z})) = 0$ since for $\alpha = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ we have $f(z) = f(\alpha z) = -f(z)$, which implies that f is 0. Observe also that the conditions are preserved under addition and scalar multiplication, so that the sets of modular forms and cusp forms of some fixed weight are complex vector spaces. In addition the product of two modular forms of weights k_1 and k_2 is a modular form of weight $k_1 + k_2$, and the quotient of a modular form of weight k_1 by a nonzero modular form is a modular form of weight $k_1 - k_2$.

We now develop the definition of modular form with respect to a congruence subgroup. Let k be an integer and Γ a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. A function $\mathcal{H} \longrightarrow \mathbb{C}$ is a modular form of weight k with respect to Γ if it satisfies

$$f[\alpha]_k = f \text{ for all } \alpha \in \Gamma, \tag{3.1}$$

and some holomorphy condition to be described below. Each congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ contains a translation matrix of the form

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} : z \longmapsto z + h$$

for some minimal $h \mid N$, since Γ contains $\Gamma(N)$. For instance for both $\Gamma_0(N)$ and $\Gamma_1(N)$ we have $h = 1$. Thus, every function $f\colon \mathcal{H} \to \mathbb{C}$ that is modular with respect to Γ is $h\mathbb{Z}$-periodic, so that it has a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n q_h^n,$$

where $q_h = e^{2\pi i z/h}$. We define such f to be *holomorphic at* ∞ if $a_n = 0$ for all $n < 0$. Note that unlike in the $\mathrm{SL}_2(\mathbb{Z})$ case, not all the cusps (i.e. $\mathbb{Q} \cup \{\infty\}$) are Γ-equivalent, so that the holomorphy at ∞ condition does not imply homolorphy at all the cusps. Thus, this last condition has to be imposed. A way to express it is by saying the $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. Note that it makes sense to speak about holomorphy at ∞ of $f[\alpha]_k$ because $f[\alpha]_k$ is modular with respect to $\alpha^{-1}\Gamma\alpha$, which is again a congruence subgroup. In summary we have

Definition 3.1. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let k be an integer. A function $f\colon \mathbb{C} \longrightarrow \mathcal{H}$ is a *modular form of weight k with respect to* Γ if

(a) f is holomorphic,

(b) $f[\alpha]_k = f$,

(c) $f[\alpha]_k$ is holomprohic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

If in addition

(d) $a_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$,

then f is a *cusp form* of weight k with respect to Γ. The modular forms of weight k with respect to Γ are denoted by $M_k(\Gamma)$, and the cusp forms by $S_k(\Gamma)$.

Both sets are again vector spaces over $\mathbb{C}$. From now on we will focus on modular forms for the congruence subgroup $\Gamma_0(N)$, and we will call modular form (cusp form) of weight k and level N the modular forms in $M_k(\Gamma_0(N))$ ($S_k(\Gamma_0(N))$. There are explicit formulas for computing the dimension of the spaces of modular forms. Next we give the formula for the particular case of cusp forms of weight 2, which is of major importance in the proof of FLT.

Proposition 3.2. *Let p be a prime. Then*

$$\dim(S_2(\Gamma_0(p)) = \begin{cases} \lfloor \frac{p+1}{12} \rfloor - 1 & \text{if } p+1 \equiv 2 \pmod{12}, \\ \lfloor \frac{p+1}{12} \rfloor & \text{otherwise.} \end{cases}$$

Let $f(z) = \sum_{n=0}^{\infty} a_n z^n \in M_k(\Gamma_0(N))$, and let χ be a Dirichlet character modulo M, then we define the *twist* of f by χ as

$$f \otimes \chi(z) = \sum_{n=0}^{\infty} \chi(n) a_n z^n.$$

The twist of a modular form is always again a modular form, although not necessarily with respect to a congruence subgroup Γ_0. More precisely, if χ is not quadratic $f \otimes \chi$ is a modular form with respect to another congruence subgroup, and if χ is quadratic then $f \otimes \chi \in M_k(\Gamma_0(NM^2))$. Moreover if f is a cusp form $f \otimes \chi$ is again a cusp form.

3.3 Hecke Operators

The spaces $M_k(\Gamma_0(N))$ and $S_k(\Gamma_0(N)$ are equipped with an action of pairwise commuting diagonalizable operators. They arise from double coset decompositions of the group $\Gamma_0(N)$ inside $\mathrm{SL}_2(\mathbb{Z})$.

Definition 3.3. Let $N \in \mathbb{Z}^+$ and p a prime. The operator T_p is defined as

$$T_p f = \begin{cases} \displaystyle\sum_{j=0}^{p-1} f \left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right]_k & \text{if } p \mid N, \\ \displaystyle\sum_{j=0}^{p-1} f \left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right]_k + f \left[\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right]_k & \text{if } p \nmid N. \end{cases}$$

It holds that $T_p T_q = T_q T_p = T_{pq}$ for all distinct primes. This allows us to extend T_p to T_n for any n. First define, for prime powers,

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} T_{p^{r-2}}, \quad \text{for } r \geq 2,$$

and note that inductively from the commutativity for primes we have also that $T_{p^r}T_{q^s} = T_{q^s}T_{p^r}$. Thus we can extend the definition multiplicatively to n,

$$T_n = \prod T_{p_i^{e_i}}, \quad \text{where } n = \prod p_i^{e_i}.$$

Note that

$$T_nT_m = T_mT_n \quad \text{if } \gcd(n,m) = 1.$$

Proposition 3.4. *Let $f \in M_k(\Gamma_0(N))$ have Fourier expansion*

$$f(z) = \sum_{m=0}^{\infty} a_m(f)q^m, \quad \textit{where } q = e^{2\pi iz}.$$

Then for all $n \in \mathbb{Z}^+$, T_nf has Fourier expansion

$$(T_nf)(z) = \sum_{m=0}^{\infty} a_m(T_nf)q^m,$$

where

$$a_m(T_nf) = \sum_{d|(m,n)} d^{k-1}a_{mn/d^2}(f).$$

It is natural to ask whether a given modular form of level N comes from a lower level or not. This gives rise to the idea of oldforms and newforms. Let us formally develop the meaning of those concepts. The most trivial way to move between levels is to observe that if $M \mid N$ then $S_k(\Gamma_0(M)) \subset S_k(\Gamma_0(N))$.

Another way to embed $S_k(\Gamma_0(M))$ into $S_k(\Gamma_0(N))$ is composing with the multiply by d map, where d is any factor of N/M. That is, for any such d and $f \in S_k(\Gamma_0(M))$ then $f(dz) \in S_k(\Gamma_0(N))$. Note that for $d = 1$ we get the embedding $S_k(\Gamma_0(M)) \subset S_k(\Gamma_0(N))$ again.

We say that a given modular form $f \in S_k(\Gamma_0(N))$ is an *oldform* if it is a linear combination of functions of type $g(dz)$ where g is a modular form of level $M \mid N$ and d is a divisor of N/M. The subspace of old forms is denoted $S_k(\Gamma_1(N))^{\text{old}}$. In order to define the space of newforms we need to first define the Petersson inner product.

The space of cusp forms of a given weight for a given congruence subgroup is equipped with a product which is of major importance in Hecke theory. Let Γ be a congruence subgroup, and let D_Γ be a fundamental domain of $\mathcal{H}$ for the action of Γ. Recall that a cusp form for Γ is a modular form for Γ which vanishes at the cusps of D_Γ. Let $S_k(\Gamma)$ be the space of cusp forms for the group Γ of weight $k > 0$ and k even, and let $d\mu$ denote the invariant measure on $\mathcal{H}$ defined by

$$d\mu(z) \coloneqq \frac{1}{y^2}dxdy = -\frac{1}{2iy^2}dz\overline{dz},$$

where $z = x + iy$. This measure is invariant under the automorphism group $\mathrm{GL}_2^+(\mathbb{R})$ of $\mathcal{H}$, meaning that $d\mu(\alpha(z)) = d\mu(z)$ for all $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$ and $z \in \mathcal{H}$. Let us define, for $f, g \in S_k(\Gamma)$, a new measure,

$$(f,g)(z) \coloneqq f(z)\overline{g(z)}(\operatorname{Im} z)^k d\mu(z).$$

The exterior form (f,g) satisfies the relations

(a) $(f,g) = \overline{(g,f)}$,

(b) $(f,f) \geq 0$ and $(f,f) = 0$ implies $f = 0$,

(c) $(f,g)(\gamma z) = (f,g)(\tau)$ for every $\gamma \in \Gamma$.

Theorem 3.5. *The space $S_k(\Gamma)$ of cusp forms of weight $k > 0$ and k even for Γ is a Hilbert space of finite dimension with the* Peterson hermitian product*:*

$$(f,g) \coloneqq \int_{D_\Gamma} (f,g)(z) = \int_{D_\Gamma} f(z)\overline{g(z)}y^k d\mu.$$

We define the space of newforms at level N, $S_k(\Gamma_1(N))^{\text{new}}$ as the orthogonal complement of $S_k(\Gamma_1(N))^{\text{old}}$ with respect to the Peterson hermitian product. However, when we speak about newforms, we will refer to a more specific subset of modular forms, defined as follows.

Definition 3.6. A nonzero modular form $f \in M_k(\Gamma_0(N))$ that is an eigenform for the Hecke operators T_n for all $n \in \mathbb{Z}^+$ is a *Hecke form* or simply an *eigenform*. The eigenform $f(z) = \sum_{n=0}^{\infty} a_n q^n$ is normalized if $a_1 = 1$. A *newform* is a normalized eigenform in $S_k(\Gamma_0(N))^{\text{new}}$.

Theorem 3.7. *The subspaces $S_k(\Gamma_0(N))^{old}$ and $S_k(\Gamma_0(N))^{new}$ are stable under the Hecke operators T_n for all $n \in \mathbb{Z}^+$. Furthermore, the set of newforms is an orthogonal basis of the space $S_k(\Gamma_0(N))^{new}$. Each such newform satisfies*

$$T_n f = a_n(f) f$$

for all $n \in \mathbb{Z}^*$. That is, its Fourier coefficients are its T_n-eigenvalues.

It is clear then that, by the definition of the Hecke operators and by this theorem, if f is a newform then its Fourier coefficients satisfy the conditions

(a) $a_1 = 1$,

(b) $a_{p^r} = a_p a_{p^{r-1}} - p^{k-1} a_{p^{r-2}}$ for all p prime and $r \geq 2$.

(c) $a_{mn} = a_m a_n$ when $(m,n) = 1$.

3.4 L-functions

Each modular form $f \in M_k(\Gamma_0(N))$ has an associated series, its *L-function*. Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$, let $s \in \mathbb{C}$ be a complex variable, and write formally

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

If $f \in M_k(\Gamma_0(N))$ is a cusp form then $L(f,s)$ converges absolutely for all s with $\Re(s) > k/2 + 1$. If f is not a cusp form then $L(f,s)$ converges absolutely for all s with $\Re(s) > k$.

Theorem 3.8. *Let $f \in M_k(\Gamma_0(N))$, $f(z) = \sum_{n=0}^{\infty} a_n n^{-s}$. Then f is a normalized eigenform if and only if $L(f,s)$ has an Euler product expansion*

$$L(f,s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{k-1-2s})^{-1} \prod_{p|N} (1 - a_p p^{-s})^{-1},$$

where the product is taken over all primes.

3.5 Galois Repesentations

One of the main importances of modular forms is that one may attach 2-dimensional Galois representations to each normalized cusp eigenform. Let $f \in S_k(\Gamma_0(N))$ be a normalized eigenform. Then the eigenvalues $a_n(f)$ are algebraic integers. Moreover, the field $K_f = \mathbb{Q}(\{a_n\})$ generated by the Fourier coefficients of f is a finite extension of $\mathbb{Q}$.

Theorem 3.9. *Let $f \in S_k(\Gamma_0(N))$ be a normalized eigenform and $K_f = \mathbb{Q}(\{a_n\})$ as above. Let p be a prime and $\mathfrak{p} \in \mathcal{O}_{K_f}$ a prime above p. Then there is a 2-dimensional Galois representation*

$$\rho_{f,\mathfrak{p}} \colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(K_{f,\mathfrak{p}}).$$

This representation is unramified outside pN. Moreover, for all $\ell \nmid pN$,

$$\mathrm{Tr}(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)) = a_\ell(f) \quad \text{and} \quad \det(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)) = \ell^{k-1}.$$

For $k = 2$ the existence of this representation is a consequence of the Eichler-Shimura theory, for which we refer to [8] or to [6, Ch. III]. The Eichler-Shimura theory relates a given modular form with certain abelian variety, and defines the Galois representation attached to the modular form as the Galois representation attached to the abelian variety. In fact, if the coefficient field $K_f = \mathbb{Q}$ this abelian variety is an elliptic curve. For $k > 2$ this result is is due to the work of Deligne [9].

3.6 Hilbert Modular Forms

Hilbert modular forms are a generalization of modular forms to totally real fields. In this section we give a brief introduction to Hilbert modular forms and state the results we will need to deal with FLT. For simplicity and in view of the case we are interested in we will restrict ourselves to the real quadratic case.

Let K be a real quadratic field. Recall that $K = \mathbb{Q}(\sqrt{d})$ for some $d > 1$ squarefree integer. Denote by $\mathcal{O}_K$ the ring of integers of K and by $\mathfrak{d}$ the different ideal of K. Since it is real quadratic, K has two embeddings into $\mathbb{R}$ given by the identity, $\sqrt{d} \mapsto \sqrt{d}$, and the conjugation, $\sqrt{d} \mapsto -\sqrt{d}$. We will denote the conjugation by $x \mapsto x'$. These two embeddings define an embedding of $\mathrm{SL}_2(K)$ into

$\mathrm{SL}_2(\mathbb{R})\times\mathrm{SL}_2(\mathbb{R})$. We define the *full Hilbert modular group* as $\mathrm{SL}_2(\mathcal{O}_K)\subseteq\mathrm{SL}_2(K)$. In analogy with the classical modular forms there is an action of $\mathrm{SL}_2(\mathcal{O}_K)$ over $\mathcal{H}\times\mathcal{H}$, where $\mathcal{H}$ is the complex upper half-plane, given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \left(\frac{az_1+b}{cz_1+d}, \frac{a'z_2+b'}{c'z_2+d'}\right),$$

where $z=(z_1,z_2)\in\mathcal{H}^2$. The *cusps* of $\mathrm{SL}_2(\mathcal{O}_K)$ are the $\mathrm{SL}_2(\mathcal{O}_K)$-equivalence classes of $K\cup\{\infty\}$ where K is viewed as embedded in the real axis of $\mathbb{C}$ and the action over ∞ is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\infty) = \frac{a}{c}.$$

In fact, we can extend the action over $\mathcal{H}^2$ to an action over

$$\mathcal{H}^2\cup\{(\infty,\infty)\}\cup\{(x,x')\in K\times K\},$$

which plays the role of $\hat{\mathcal{H}}$ in classical modular forms. A subgroup Γ of $\mathrm{SL}_2(K)$ is a *congruence subgroup* if $\Gamma\cap\mathrm{SL}_2(\mathcal{O}_K)$ has finite index in both Γ and $\mathrm{SL}_2(\mathcal{O}_K)$. The only example of congruence subgroup we will see is

$$\Gamma_0(\mathfrak{N}) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\mathrm{SL}_2(\mathcal{O}_K)\colon c\in\mathfrak{N}\right\},$$

where $\mathfrak{N}$ is an integral ideal of K.

Definition 3.10. A *Hilbert modular form* of weight (k_1,k_2) for a congruence subgroup Γ is a holomorphic function $f\colon\mathcal{H}^2\longrightarrow\mathbb{C}$ such that

$$f(\alpha z) = (cz_1+d)^{k_1}(c'z_2+d')^{k_2}f(z)$$

for all $\alpha=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma$. When $k_1=k_2=k$ then f is said to have parallel weight k, and if $\Gamma=\Gamma_0(\mathfrak{N})$ then we say that f is a Hilbert modular form of level $\mathfrak{N}$.

The set of Hilber modular forms of weight (k_1,k_2) for a given congruence subgroup Γ is a finite dimensional complex vector space denoted by $M_{k_1,k_2}(\Gamma)$. For a function $f\colon\mathcal{H}^2\longrightarrow\mathbb{C}$ and an element $\alpha=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\mathrm{SL}_2(K)$ define the operator

$$f[\alpha]_{k_1,k_2}(z) = (cz_1+d)^{-k_1}(c'z_2+d')^{-k_2}f(\alpha z).$$

If $k_1=k_2=k$ we just write $[\alpha]_k$. The assignment $f\mapsto f[\alpha]_{k_1,k_2}$ defines a right action of $\mathrm{SL}_2(K)$ on complex valued functions on $\mathcal{H}^2$. Using it the modularity condition can be rewritten as

$$f[\alpha]_{k_1,k_2}(z) = f(z) \quad \text{for all } \alpha\in\Gamma.$$

Note that

$$\left\{\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} : \mu\in\mathcal{O}_K\right\}\subseteq\Gamma_0(\mathfrak{N}),$$

and as a consequence if f is a Hilbert modular form for $\Gamma_0(\mathfrak{N})$ and $h \in \mathcal{O}_K$ then

$$f(z+h) = f(z),$$

where $z + h = (z_1 + \mu, z_2 + \mu') \in \mathcal{H}^2$. Thus in this case f has a Fourier expansion

$$f(z) = \sum_{\nu \in \mathfrak{d}^{-1}} a_\nu e^{2\pi i \operatorname{Tr}(\nu z)},$$

where $\operatorname{Tr}(\nu z) = \nu z_1 + \nu' z_2$, since the inverse of the different ideal is the dual lattice of $\mathcal{O}_K$ with respect to the trace form in K, that is

$$\mathfrak{d}^{-1} = \{\lambda \in K \colon \operatorname{Tr}(\mu\lambda) \in \mathbb{Z} \text{ for all } \mu \in \mathcal{O}_K\}.$$

In contrast to the one-dimensional case, a Hilbert modular form is automatically holomorphic at the cusps by the Götzky-Koecher principle, so that we do not have to impose it in the definition.

Theorem 3.11 (Götzky-Koecher principle)**.** *Let $f \colon \mathcal{H}^2 \longrightarrow \mathbb{C}$ be a Hilbert modular form for a congruence subgroup Γ. Then*

$$a_\nu \neq 0 \Longleftrightarrow \nu = 0 \text{ or } \nu >> 0,$$

where a_ν are its Fourier expansion coefficients.

By $\nu >> 0$ we mean totally positive, that is $\nu > 0$ and $\nu' > 0$. Hence returning to the case $f \in M_{k_1,k_2}(\Gamma_0(\mathfrak{N}))$ we have that the Fourier expansion of f has the form

$$f(z) = a_0 + \sum_{\substack{\nu \in \mathfrak{d}^{-1} \\ \nu >> 0}} a_\nu e^{2\pi i \operatorname{Tr}(\nu z)}.$$

In particular f is holomorphic at infinity. Moreover, if κ is any other cusp, we take $\gamma \in \mathrm{SL}_2(K)$ such that $\gamma\infty = \kappa$. Then the behavior of f at κ is the same as the behavior of $f[\gamma]_{k_1,k_2}$ at ∞, hence f is holomorphic at all cusps. We say that f is a *cusp form* if it vanishes at all cusps, that is, if the constant term a_0 in the Fourier expansion of $f[\gamma]_{k_1,k_2}$ vanishes for all $\gamma \in \mathrm{SL}_2(K)$. We denote by $S_{k_1,k_2}(\Gamma_0(\mathfrak{N}))$ the space of cusp forms of weight (k_1, k_2) for the congruence subgroup $\Gamma_0(\mathfrak{N})$.

Despite this will not be the case in later applications, we assume henceforth that the field K has strict class number 1 for simplicity. Recall that the strict class group is the group of fractional ideals quotient the subgroup of principal ideals generated by totally positive elements. We also restrict to Hilbert modular forms of parallel weight 2, which are the ones which will be important for our purposes.

In this case, if $\mathfrak{n}$ is an integral ideal, then $\mathfrak{n} = \nu\mathfrak{d}$ for some totally positive $\nu \in \mathfrak{d}^{-1}$. We then define $a_\mathfrak{n} = a_\nu$. The modularity condition implies that $a_\mathfrak{n}$ does not depend on the choice of ν, and we call $a_\mathfrak{n}$ the *Fourier coefficient* of f at $\mathfrak{n}$.

Similarly to the modular forms case we may equip the spaces $M_{k_1,k_2}(\Gamma_0(\mathfrak{N}))$ and $S_{k_1,k_2}(\Gamma_0(\mathfrak{N}))$ with an action of pairwise commuting *Hecke operators* $T_\mathfrak{n}$ indexed

by the nonzero integral ideals $\mathfrak{n}$. Let $\mathfrak{p}$ be a prime ideal and p a totally positive generator of $\mathfrak{p}$. Define

$$T_{\mathfrak{p}}f = \begin{cases} \sum_{j=0}^{N(\mathfrak{p})-1} f\left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right]_2 & \text{if } \mathfrak{p} \mid \mathfrak{N}, \\ \sum_{j=0}^{N(\mathfrak{p})-1} f\left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right]_2 + f\left[\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right]_2 & \text{if } \mathfrak{p} \nmid \mathfrak{N}. \end{cases}$$

It holds that $T_{\mathfrak{p}}T_{\mathfrak{q}} = T_{\mathfrak{q}}T_{\mathfrak{p}} = T_{\mathfrak{pq}}$ for all distinct prime ideals. So as before this allows us to extend $T_{\mathfrak{p}}$ to $T_{\mathfrak{n}}$ for any $\mathfrak{n}$. First define, for prime powers,

$$T_{\mathfrak{p}^r} = T_{\mathfrak{p}}T_{\mathfrak{p}^{r-1}} - \mathfrak{p}^{k-1}T_{\mathfrak{p}^{r-2}}, \quad \text{for } r \geq 2,$$

and note that inductively from the commutativity for primes we have that also $T_{\mathfrak{p}^r}T_{\mathfrak{q}^s} = T_{\mathfrak{q}^s}T_{\mathfrak{p}^r}$. Thus we can extend the definition multiplicatively to $\mathfrak{n}$,

$$T_{\mathfrak{n}} = \prod T_{\mathfrak{p}_i^{e_i}}, \quad \text{where } \mathfrak{n} = \prod \mathfrak{p}_i^{e_i}.$$

An *oldform* is a Hilbert modular form $f \in S_2(\Gamma_0(\mathfrak{N}))$ coming from a lower level in the same sense as for modular forms. That is, f is a linear combination of functions of type $g(dz)$ where g is a Hilbert form of level $\mathfrak{M} \mid \mathfrak{N}$ and d is a generator of $\mathfrak{N}/\mathfrak{M}$. The subspace of oldforms is denoted $S_2(\Gamma_0(\mathfrak{N}))^{\text{old}}$.

Define the differential form on $\mathcal{H}^2$ given by

$$d\mu = \frac{dx_1 dy_1}{y_1^2}\frac{dx_2 dy_2}{y_2^2}.$$

It is invariant under the action of $\mathrm{SL}_2(\mathbb{R})^2$. Let $f, g \in S_2(\Gamma_0(\mathfrak{N}))$ and let $D_{\Gamma_0(\mathfrak{N})}$ be a fundamental domain for $\Gamma_0(\mathfrak{N})$. Then we define the *Petersson inner product* as

$$(f, g) = \int_{D_{\Gamma_0(\mathfrak{N})}} f(z)\overline{g(z)}(y_1 y_2)^2 d\mu.$$

The space of newforms $S_2(\Gamma_0(\mathfrak{N}))^{\text{new}}$ is the orthogonal complement of the space of oldforms. A *newform* is a normalized (i.e. $a_{(1)} = 1$) eigenform for all the Hecke operators which belongs to $S_2(\Gamma_0(\mathfrak{N}))^{\text{new}}$. If f is a newform then $T_{\mathfrak{n}}f = a_{\mathfrak{n}}f$.

If $f \in S_2(\Gamma_0(\mathfrak{N}))$ is a normalized eigenform its eigenvalues are algebraic integers and moreover the field $\mathbb{Q}(\{a_{\mathfrak{n}}\}) \coloneqq K_f$ generated by all its Fourier coefficients is a finite extension of $\mathbb{Q}$. We may attach to it an L-function

$$L(f, s) = \sum_{\mathfrak{n}} \frac{a_{\mathfrak{n}}}{N(\mathfrak{n})^s}$$

and $\mathfrak{l}$-adic Galois representations

$$\rho_{f,\mathfrak{l}} \colon G_K \longrightarrow \mathrm{GL}_2(K_{f,\mathfrak{l}})$$

for primes $\mathfrak{l} \in \mathcal{O}_K$, which are unramified away from $\mathfrak{l}\mathfrak{N}$ and furthermore

$$\mathrm{Tr}(\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})) = a_{\mathfrak{p}}(f) \quad \text{and} \quad \det(\rho_{f,\mathfrak{l}}(\mathrm{Frob}_{\mathfrak{p}})) = N(\mathfrak{p}).$$

Chapter 4

Fermat's Last Theorem

In this chapter we will make use of the tools provided in the previous chapters for studying the asymptotic Fermat's Last Theorem. We begin by sketching the proof of the classical FLT, this will serve as an inspiration for the study of the asymptotic FLT, which will be proved next.

4.1 Fermat's Last Theorem

Assume that $p \geq 5$, and suppose that

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

with a, b, c coprime integers, is a non-trivial solution to the Fermat equation. Observe that exactly one of them must be even. By changing the order and the sign of a, b and c we may assume that $a \equiv -1 \pmod 4$ and $2 \mid b$. Attach to the triple an elliptic curve

$$E_{a^p,b^p,c^p} : y^2 = x(x - a^p)(x - b^p), \tag{4.1}$$

known as the *Frey curve* associated to a^p, b^p, c^p. By the coprimality of a, b and c we have that E_{a^p,b^p,c^p} is semistable, and hence its conductor can be expressed as

$$N_{a^p,b^p,c^p} = \prod_{\ell \mid abc} \ell.$$

Let us compute its minimal discriminant. The discriminant and c_4-invariant of E_{a^p,b^p,c^p} are given by

$$\begin{aligned} \Delta &= 16(abc)^{2p}, \\ c_4 &= 16(a^{2p} - (bc)^p). \end{aligned}$$

Clearly $v_l(c_4) = 0$ for all primes $l \neq 2$, so that the equation (4.1) is minimal at all these primes. However $v_2(c_4) = 4$, hence (4.1) may not be minimal at 2. Indeed the change of coordinates

$$x = 4x', \quad y = 8y' + 4x'$$

yields another equation

$$y^2 + xy = x^3 + \frac{b^p - a^p - 1}{4}x^2 - \frac{(ab)^{2p}}{16}x. \tag{4.2}$$

By our assumptions on a and b the coefficients of this equations belong to $\mathbb{Z}$, and by Section 2.1, eq. 2.3, $v_2(c_4') = 0$ and $v_2(\Delta') = v_2(\Delta) - 12 = 2p - 8$. In particular equation (4.2) is minimal at 2. All this put together yields that the minimal discriminant of the Frey curve is

$$\Delta_{a^p,b^p,c^p} = 2^{-8}(abc)^{2p}.$$

Denote by ρ_{a^p,b^p,c^p} the p-adic Galois representation attached to E_{a^p,b^p,c^p}. By Theorem 2.13 we have that ρ_{a^p,b^p,c^p} is unramified outside pN. Moreover, recall that, by Theorem 2.16 we have that $\bar{\rho}_{a^p,b^p,c^p}$ is unramified at $l \neq p$ if and only if $p \mid v_l(\Delta_{a^p,b^p,c^p})$ and flat at p if and only if $p \mid v_p(\Delta_{a^p,b^p,c^p})$. Thus in our case $\bar{\rho}_{a^p,b^p,c^p}$ is unramified outside $2p$ and flat at p. Moreover, Mazur proved in [16] and [17] the following result about irreducibility of residual representations attached to semistable elliptic curves.

Theorem 4.1. *Let $E/\mathbb{Q}$ be a semistable elliptic curve. Then $\bar{\rho}_{E,\ell}$ is absolutely irreducible for $\ell > 7$. Moreover if E has full 2-torsion over $\mathbb{Q}$ then $\bar{\rho}_{E,\ell}$ is absolutely irreducible for all $\ell > 3$.*

Definition 4.2. We say that an elliptic curve $E/\mathbb{Q}$ is *modular* if there is a weight two newform f of level N_E for which

$$L(E, s) = L(f, s).$$

In particular this implies that $\rho_{E,p} \sim \rho_{f,p}$ at every prime.

Theorem 4.3 (Wiles)**.** *Every semistable elliptic curve over $\mathbb{Q}$ is modular.*

Since the Frey curve E_{a^p,b^p,c^p} is semistable this implies that there is a weight two newform f_{a^p,b^p,c^p} of conductor N_{a^p,b^p,c^p} associated to E_{a^p,b^p,c^p}. In particular, we have $\rho_{a^p,b^p,c^p} \sim \rho_{f_{a^p,b^p,c^p}}$. We know that $\bar{\rho}_{a^p,b^p,c^p}$ is absolutely irreducible, unramified outside $2p$ and flat at p, hence so is $\rho_{f_{a^p,b^p,c^p}}$. The final step is to apply Ribet's level lowering theorem.

Theorem 4.4 (Ribet)**.** *Let f be a weight two newform of level $N\ell$ where $\ell \nmid N$ is a prime. Suppose $\bar{\rho}_{f,p}$ is absolutely irreducible and that one of the following is true:*

- *$\ell \neq p$ and $\bar{\rho}_{f,p}$ is unramified at ℓ, or*
- *$\ell = p$ and $\bar{\rho}_{f,p}$ is flat at p.*

Then there is a weight 2 newform g of level N such that $\bar{\rho}_{g,p} \simeq \bar{\rho}_{f,p}$.

Applying Ribet's theorem we conclude that there is a weight two newform g of conductor 2 such that $\rho_g \cong \rho_{a^p,b^p,c^p}$. But by Proposition 3.2 the dimension of $S_2(\Gamma_0(2))$ is 0. Thus we reach contradiction, and Fermat's Last Theorem is proved.

4.2 Fermat's Last Theorem for Real Quadratic Fields

Recall that real quadratic fields are those of the form $K = \mathbb{Q}(\sqrt{d})$ with d a positive squarefree integer. We define the following sets once and for all,

$$S = \{\mathfrak{P} \colon \mathfrak{P} \text{ prime above } 2\},$$
$$T = \{\mathfrak{P} \in S \colon f(\mathfrak{P}/2) = 1\},$$

where $f(\mathfrak{P}/2)$ stands for the residual degree. Note that since K is quadratic the only possibilities for the decomposition of 2 in K are

$$2 \text{ is } \begin{cases} \text{inert} & \text{if } d \equiv 5 \pmod 8 \Longrightarrow S = \{\mathfrak{P}\}, T = \emptyset, \\ \text{split} & \text{if } d \equiv 1 \pmod 8 \Longrightarrow S = T = \{\mathfrak{P}_1, \mathfrak{P}_2\}, \\ \text{ramified} & \text{if } d \equiv 2, 3 \pmod 4 \Longrightarrow S = T = \{\mathfrak{P}\}. \end{cases}$$

First of all, let us see why the strategy followed to prove FLT fails when dealing with the Fermat equation over extensions of $\mathbb{Q}$. Let $K/\mathbb{Q}$ be a real quadratic field and $\mathcal{O}_K$ its ring of integers. Suppose $a^p + b^p + c^p = 0$ with $a, b, c \in K$, $abc \neq 0$ and $p \geq 5$ prime. We can scale them so that they belong to the ring of integers $\mathcal{O}_K$. If the class number of K is greater than 1 then we can not assume coprimality of a, b and c. However we can take a finite set $\mathcal{H}$ of representatives of the class group and assume coprimality outside $\mathcal{H}$. In this case the Frey curve E_{a^p,b^p,c^p} defined as in the classical case is semistable outside $S \cup \mathcal{H}$. Applying level lowering yields a Hilbert newform of parallel weight 2 and level divisible only by primes in $S \cup \mathcal{H}$, but in general there are newforms at these levels. Hence we do not reach a contradiction as we did in the classical case.

To go further we must somehow get rid of the bad primes coming from the class group. To achieve this we study, for $\mathfrak{P} \in T$, the action of $I_{\mathfrak{P}}$ in $E_{a^p,b^p,c^p}[p]$. This allows us to find another elliptic curve E' such that $\bar{\rho}_{a^p,b^p,c^p} \sim \bar{\rho}_{E',p}$ and with better properties, namely, potentially good reduction away from S and full 2-torsion over K. These properties, along with the study of the the action of $I_{\mathfrak{q}}$ in $E_{a^p,b^p,c^p}[p]$ for $\mathfrak{q} \notin S$, permits us to relate the j-invariant of E' with the S-unit equation over K. Since we can explicitly solve the S-unit equation for all real quadratic K, we will reach a contradiction for some of them.

Before starting with these computations, we give some strong results necessary to prove the asymptotic Fermat's Last Theorem. More precisely, we state the modularity theorem for real quadratic fields, level-lowering theorem for Hilbert modular forms, irreducibility of reduced representations attached to elliptic curves, and a version of Eichler-Shimura for Hilbert modular forms.

Theorem 4.5. *Let K be a real quadratic field. Then all elliptic curves over K are modular.*

This modularity theorem was proved by Freitas, Le Hung and Siksek in [11]. We need also the following irreducibility theorem, derived in [12].

Theorem 4.6. *Let K be a real quadratic field. There is an effective constant C_K, depending only on K, such that, if $p > C_K$ is a prime, and E is an elliptic curve over K semistable at all $\mathfrak{q} \mid p$, then $\bar{\rho}_{E,p}$ is irreducible.*

For the level-lowering theorem we refer to main article by Freitas and Siksek we are following, [10].

Theorem 4.7. *Let K be a real quadratic field and E/K and elliptic curve of conductor $\mathfrak{N}$. Let p be a rational prime. For a prime ideal $\mathfrak{q}$ of K denote by $\Delta_\mathfrak{q}$ the minimal discriminant of E at $\mathfrak{q}$. Let*

$$\mathfrak{M}_p \coloneqq \prod_{\substack{\mathfrak{q} \| \mathfrak{N} \\ p \mid v_\mathfrak{q}(\Delta_\mathfrak{q})}} \mathfrak{q}, \quad \mathfrak{N}_p = \frac{\mathfrak{N}}{\mathfrak{M}_p}.$$

Suppose that

(i) $\bar{\rho}_{E,p}$ is irreducible,

(ii) E is semistable at all $\mathfrak{q} \mid p$,

(iii) $p \mid v_\mathfrak{q}(\Delta_\mathfrak{q})$ for all $\mathfrak{q} \mid p$.

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

Finally, we need the following version of Eichler-Shimura, in order to attach an elliptic curve to a given Hilbert modular form with rational eigenvalues. This result is proved in [7, Theorem 7.7].

Theorem 4.8. *Let K be a real quadratic field and let f be a Hilbert new form over K of level $\mathfrak{N}$ and parallel weight 2 such that $\mathbb{Q}_f = \mathbb{Q}$. Suppose that there is a prime ideal $\mathfrak{q}$ of K such that $v_\mathfrak{q}(\mathfrak{N}) = 1$. Then there is an elliptic curve E_f/K of conductor $\mathfrak{N}$ with the same L-function as f.*

Corollary 4.9. *Let E be an elliptic curve over a real quadratic field K and p an odd prime. Suppose $\bar{\rho}_{E,p}$ is irreducible, and $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,p}$ for some Hilbert newform over K of parallel weight 2 with $\mathbb{Q}_f = \mathbb{Q}$. Let $\mathfrak{q} \nmid p$ a prime of K such that*

(i) E has potentially good reduction at $\mathfrak{q}$,

(ii) $p \mid \#\bar{\rho}_{E,p}(I_\mathfrak{q})$,

(iii) $p \nmid (N(\mathfrak{q}) \pm 1)$.

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

Proof. Consider the usual invariants c_4 and c_6 attached to E and $\gamma = -c_4/c_6$ as in Section 2.5. Let χ be the quadratic character associated to $K(\sqrt{\gamma})/K$. By what we saw in Section 2.5 the quadratic twist $E \otimes \chi$ has split multiplicative reduction at $\mathfrak{q}$. Consider $g = f \otimes \chi$. Then since χ is quadratic and $\mathbb{Q}_f = \mathbb{Q}$ we have that $\mathbb{Q}_g = \mathbb{Q}$.

Suppose g is new at level $\mathfrak{N}_g$. Then it is enough to prove that $v_\mathfrak{q}(\mathfrak{N}_g) = 1$. In fact in this case by the previous theorem there is an elliptic curve E_g having the same L-function as g, but recall that the twist by a quadratic character acts in the same way on elliptic curves and on modular forms, so that L-functions of $f = g \otimes \chi$ and $E_f := E_g \otimes \chi$ are also the same.

In order to prove $v_\mathfrak{q}(\mathfrak{N}_g) = 1$ we look at the equivalence $\bar{\rho}_{E\otimes\chi,p} \sim \bar{\rho}_{g,\mathfrak{p}}$. Let $\mathfrak{N}$ be their optimal level. Then since $E \otimes \chi$ has multiplicative reduction at $\mathfrak{q}$ then $v_\mathfrak{q}(\mathfrak{N}) = 0$ or 1. Since χ is a quadratic character and $\bar{\rho}_{E\otimes\chi,p} = \bar{\rho}_{E,p} \otimes \chi$ then since $p \mid \bar{\rho}_{E,p}$ we have that $p \mid \bar{\rho}_{E\otimes\chi,p}$. Hence $v_\mathfrak{q}(\mathfrak{N}) \neq 0$ and so $v_\mathfrak{q}(\mathfrak{N}) = 1$. Now, by [13, Theorem 1.5] we have that $v_\mathfrak{q}(\mathfrak{N}) = v_\mathfrak{q}(\mathfrak{N}_g)$ except possibly when $v_\mathfrak{q}(\mathfrak{N}) = 0$ and $v_\mathfrak{q}(\mathfrak{N}_g) = 1$ or when $N_{K/\mathbb{Q}}(\mathfrak{q}) = \pm 1 \pmod{p}$. The former is impossible since $v_\mathfrak{q}(\mathfrak{N}) = 1$ and the latter is impossible by hypothesis (c). Therefore $v_\mathfrak{q}(\mathfrak{N}_g) = 1$. □

Conductor of the Frey curve

In this section we minimize the primes of bad reduction of the Frey curve and compute its conductor.

Let $u, v, w \in \mathcal{O}_K$ such that $uvw \neq 0$ and $u + v + w = 0$ and let

$$E\colon y^2 = x(x-u)(x+v).$$

Lemma 4.10. *Let $\mathfrak{q} \nmid 2$ be a prime and let*

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

Denote by E_{min} a local minimal model of E at $\mathfrak{q}$. Then

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

$$v_\mathfrak{q}(u) = v_\mathfrak{q}(v) = v_\mathfrak{q}(w).$$

(ii) E_{min} has multiplicative reduction at $\mathfrak{q}$ if and only if s is even and the valuations above are not all equal. In this case the minimal discriminant satisfies

$$v_\mathfrak{q}(\Delta_\mathfrak{q}) = 2v_\mathfrak{q}(u) + 2v_\mathfrak{q}(v) + 2v_\mathfrak{q}(w) - 6s.$$

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

Proof. Let π be a uniformizer of $K_\mathfrak{q}$. Suppose first that s is even and $v_\mathfrak{q}(u) = v_\mathfrak{q}(v) = v_\mathfrak{q}(w) = s$. Then the change of coordinates $y = \pi^{3s/2}y'$ and $x = \pi^s x'$ yields

an equation with $v_\mathfrak{q}(\Delta) = 0$, and hence this equation is minimal and has good reduction at $\mathfrak{q}$.

If s is even and $v_\mathfrak{q}(u) < v_\mathfrak{q}(v)$ (say) then necessarily $s = v_\mathfrak{q}(u) = v_\mathfrak{q}(w)$. Thus the same change of coordinates yields an equation with $v_\mathfrak{q}(\Delta) > 0$ and $v_\mathfrak{q}(c_4) = 0$, and hence this equation is minimal and has multiplicative reduction at $\mathfrak{q}$.

Finally, if s is odd we apply the change of coordinates $y = \pi^{3(s-1)/2}y'$ and $x = \pi^{s-1}x'$. Then if $v_\mathfrak{q}(u) = v_\mathfrak{q}(v) = v_\mathfrak{q}(w)$ the equation we get has $v_\mathfrak{q}(\Delta) = 6$ and $v_\mathfrak{q}(c_4) > 0$. Otherwise the equation has $v_\mathfrak{q}(\Delta) > 0$ and $v_\mathfrak{q}(c_4) = 2$. Thus in both cases the equation is minimal and has additive reduction at $\mathfrak{q}$.

□

Let (a, b, c) be a non-trivial solution to the Fermat equation. Let $\mathcal{G}_{a,b,c}$ be the ideal $a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K$. By the previous lemma an odd prime not dividing $\mathcal{G}_{a,b,c}$ is a prime of good or multiplicative reduction for $E_{a,b,c}$ and does not appear in the final level $\mathfrak{N}_p$. However, a prime dividing $\mathcal{G}_{a,b,c}$ exactly once is an additive prime, and does appear in $\mathfrak{N}_p$. Thus in order to control $\mathfrak{N}_p$ we must to control $\mathcal{G}_{a,b,c}$. The following lemma achieves this.

Lemma 4.11. *Let (a, b, c) a non-trivial solution to the Fermat equation. There is a non-trivial integral solution (a', b', c') to the Fermat equation such that*

(i) For some $\eta \in K^*$, we have $a' = \eta a$, $b' = \eta b$, $c' = \eta c$,

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

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

Proof. Let $\mathfrak{m} \in \mathcal{H}$ satisfy $[\mathcal{G}_{a,b,c}] = [\mathfrak{m}]$, where $[\,\cdot\,]$ stands for the class in the class group. Therefore there is a $\eta \in K^*$ such that $\mathfrak{m} = (\eta) \cdot \mathcal{G}_{a,b,c}$. Define a', b' and c' as in (i). Observe that $(a') = (\eta) \cdot (a) = \mathfrak{m}\mathcal{G}_{a,b,c}^{-1} \cdot (a)$, which is an integral ideal, since by its definition $\mathcal{G}_{a,b,c}$ divide (a). Similarly for (b') and (c'). Finally we have

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

□

Lemma 4.12. *Let Let (a, b, c) a non-trivial solution to the Fermat equation with prime exponent p satisfying $\mathcal{G}_{a,b,c} = \mathfrak{m} \in \mathcal{H}$. Write E for the Frey curve, and let Δ be its discriminant. Then, at all $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$, the model E is minimal, semistable and satisfies $p \mid v_\mathfrak{q}(\Delta)$. Let $\mathfrak{N}$ be the conductor of E, and let $\mathfrak{N}_p$ as defined in Theorem 4.7. Then*

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

where $0 \le r'_\mathfrak{P} \le r_\mathfrak{P} \le 2 + 6v_\mathfrak{P}(2)$ and $0 \le s'_\mathfrak{m} \le s'_\mathfrak{m} \le s_\mathfrak{m} \le 2$.

Proof. Let $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$ be a prime such that $\mathfrak{q} \mid abc$. Then we have that $\mathfrak{q}$ divides exactly one of a, b and c, since otherwise we would have $\mathfrak{q} \mid \mathcal{G}_{a,b,c}$ and hence $\mathfrak{q} = \mathfrak{m}$, contradicting the hypothesis. This implies that $v_{\mathfrak{q}}(c_4) = 0$, so that $\mathfrak{q}$ is a prime of multiplicative reduction. It is clear that $p \mid v_{\mathfrak{q}}(\Delta)$, and therefore $\mathfrak{q} \nmid \mathfrak{N}_p$.

Let $\mathfrak{P} \in S$. Then by [19, Theorem IV.10.4] we have that $v_{\mathfrak{P}}(\mathfrak{N}) \leq 2 + v_{\mathfrak{P}}(2)$. Note that $r'_{\mathfrak{P}} = r_{\mathfrak{P}}$ unless E has multiplicative reduction at $\mathfrak{P}$ and $p \mid v_{\mathfrak{P}}(\Delta_{\mathfrak{P}})$, in which case $r_{\mathfrak{P}} = 1$ and $r'_{\mathfrak{P}} = 0$. Finally, for $s_{\mathfrak{m}}$, recall that $\mathfrak{m} \nmid 2$. Since E has full 2-torsion by Proposition 2.10 we have that $s_{\mathfrak{m}} \leq 2$, and as before $s_{\mathfrak{m}} = s'_{\mathfrak{m}}$ unless E has multiplicative reduction at $\mathfrak{m}$ and $\mid v_{\mathfrak{m}}(\Delta_{\mathfrak{m}})$, in which case $s_{\mathfrak{m}} = 1$ and $s'_{\mathfrak{m}} = 0$. □

Images of inertia

As mentioned in the beginning of the section, we need some results about the images of the inertia subgroups at all primes. The first lemma shows that for all primes $\mathfrak{q} \nmid 2$ then $p \nmid \#\bar{\rho}_{E,p}(I_{\mathfrak{q}})$, while the second one shows that for primes $\mathfrak{P} \mid 2$ with residual degree 1 we have $p \mid \#\bar{\rho}_{E,p}(I_{\mathfrak{P}})$.

Lemma 4.13. *Let $\mathfrak{q} \notin S$ be a prime of K. Let (a, b, c) a non-trivial solution to the Fermat equation with prime exponent $p \geq 5$ such that $\mathfrak{q} \nmid p$. Let E be the Frey curve. Then $p \nmid \#\bar{\rho}_{E,p}(I_{\mathfrak{q}})$.*

Proof. By Theorem 2.16 and Proposition 2.18 if $p \geq 5$ then $p \mid \#\rho_{E,p}(I_{\mathfrak{q}})$ if and only if $v_{\mathfrak{q}}(j) < 0$ and $p \nmid v_{\mathfrak{q}}(j)$. Recall that $j = c_4^3/\Delta$. If a, b, c have distinct valuations at $\mathfrak{q}$ then $v_{\mathfrak{q}}(j) < 0$ and $p \mid v_{\mathfrak{q}}(j)$. Otherwise $v_{\mathfrak{q}}(j) \geq 0$. In either case it follows that $p \nmid \#\bar{\rho}_{E,p}(I_{\mathfrak{q}})$.

□

Lemma 4.14. *Let $\mathfrak{P} \in S$. Let (a, b, c) a non-trivial solution to the Fermat equation with prime exponent $p > 4v_{\mathfrak{P}}(2)$. Let $E = E_{a,b,c}$ be the Frey curve. If $\mathfrak{P} \in T$ then E has potentially multiplicative reduction at $\mathfrak{P}$ and $p \mid \#\bar{\rho}_{E,p}(I_{\mathfrak{P}})$.*

Proof. Let $\mathfrak{P}$ be a uniformizer for $K_{\mathfrak{P}}$. Let

$$t = \min\{v_{\mathfrak{P}}(a), v_{\mathfrak{P}}(b), v_{\mathfrak{P}}(c)\}$$

and $\alpha = \pi^{-t}a$, $\beta = \pi^{-t}b$ and $\gamma = \pi^{-t}c$. Note that $\alpha, \beta, \gamma \in \mathcal{O}_K$. Since the residue field of $\mathfrak{P}$ is $\mathbb{F}_2$ the equation $\alpha^p + \beta^p + \gamma^p = 0$ tells us that exactly one of them is divisible by π. Thus $v_{\mathfrak{P}}(a), v_{\mathfrak{P}}(b), v_{\mathfrak{P}}(c)$ are not all equal, and hence two of them must be equal to t and the other one equal to $t + k$ with $k \geq 1$. By the definition of j we thus get $v_{\mathfrak{P}}(j) = 8v_{\mathfrak{P}}(2) - 2kp$. As $p > 4v_{\mathfrak{P}}(2)$, we see that $v_{\mathfrak{P}}(j) < 0$ and $p \nmid v_{\mathfrak{P}}(j)$. Therefore by Theorem 2.16 $p \mid \#\bar{\rho}_{E,p}(I_{\mathfrak{P}})$. □

The curve E'

We combine now the lemmas in the two last subsections with the theorems at the beginning of this section for finding another elliptic curve with better properties than the Frey curve E and equivalent reduced Galois representation mod p. However, first of all we need the following result, which will allow us to assume that the coefficient field of certain modular form is the rational numbers, in order to be within the hypothesis of Corollary 4.9. Although it holds in totally real fields, we are going to prove it, for simplicity, over $\mathbb{Q}$.

Theorem 4.15. *Let E/K be an elliptic curve of conductor N and f a modular newform of level N' and weight 2 such that $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{w}}$ for some prime p and prime ideal $\mathfrak{w} \mid p$ in $\mathbb{Q}_f$. Let $\ell \in \mathbb{Q}$ be a prime such that $\ell^2 \nmid N$ and $\ell \nmid pN'$. Denote by $t = \#E_{tors}(\mathbb{Q})$. Define*

$$S_\ell = \left\{ a \in \mathbb{Z} \colon \ -2\sqrt{\ell} \leq a \leq 2\sqrt{\ell} \text{ and } a \equiv \ell \pmod{t} \right\},$$
$$B_\ell = \ell N_{\mathbb{Q}_f/\mathbb{Q}}((\ell+1)^2 - c_\ell^2) \prod_{a \in S_\ell} N_{\mathbb{Q}_f/\mathbb{Q}}(a - c_\ell),$$

where c_ℓ are the Fourier coefficients of f. Then $p \mid B_\ell$.

Proof. Note that if ℓ is of good reduction, or what is the same $\ell \nmid N$, then t divides $\#E(\mathbb{F}_\ell) = \ell + 1 - a_\ell$, so that $a_\ell \equiv \ell + 1 \pmod{t}$. This follows from the fact that for primes ℓ of good reduction there is an injective homomorphism $\phi \colon E_{\text{tors}}(\mathbb{Q}) \to E(\mathbb{F}_\ell)$ (see for example [18, Ch.VII]).

If $\ell = p$ the first term of B_ℓ ensures us that $p \mid B_\ell$. Assume thus that $\ell \nmid p$. If $\ell \nmid pN$, then the hypothesis $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{w}}$ implies that $a_\ell \equiv c_\ell \pmod{\mathfrak{w}}$, so that $p \mid N_{\mathbb{Q}_f/\mathbb{Q}}(a_\ell - c_\ell)$. Otherwise $\ell \mid\mid N$, and by [4, Theorem 15.2.2] this implies that $p \mid N_{\mathbb{Q}_f/\mathbb{Q}}((\ell+1)^2 - c_\ell^2)$. Since by Hasse's theorem

$$-2\sqrt{\ell} \leq a_\ell \leq 2\sqrt{\ell},$$

and since in the first case ℓ is of good reduction we have that $a_\ell \in S$. Therefore $p \mid B_\ell$.

□

In order for this result to be useful we have to see whether there is a prime ℓ as in the theorem such that $B_\ell \neq 0$. If $\mathbb{Q}_f \neq \mathbb{Q}$ then there is infinitely many non-rational c_ℓ, so for all those ℓ clearly $B_\ell \neq 0$. Also, by [4, Proposition 15.4.2], there exists an ℓ which satisfies $B_\ell \neq 0$ if $4 \mid t$ and for every elliptic curve F/K isogenous to E then $F(K)$ does not have full 2-torsion.

Theorem 4.16. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with $d \not\equiv 1 \pmod{4}$. There is a constant B_K depending only on K such that the following hold. Let (a, b, c) a non-trivial solution to the Fermat equation with prime exponent $p > B_K$, and assume $\mathcal{G}_{a,b,c} = \mathfrak{m} \in \mathcal{H}$. Let E be the Frey curve. Then there is an elliptic curve E' over K such that*

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

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

(iii) $\bar{\rho}_{E,p} \sim \bar{\rho}_{E',p}$.

Moreover, if we call j' the j-invariant of E'. Then

(a) for $\mathfrak{P} \in T$, we have $v_{\mathfrak{P}}(j') < 0$,

(b) for $\mathfrak{q} \notin S$, we have $v_{\mathfrak{q}}(j') \geq 0$.

In particular, E' has potentially good reduction at outside S.

Proof. By Lemma 4.12 E is semistable away from $S \cup \{\mathfrak{m}\}$. Theorem 4.5 tells us that all elliptic curves over real quadratic fields are modular, therefore E is modular. By Theorem 4.6 we can take a constant B_K such that $\bar{\rho}_{E,p}$ is irreducible. Now, applying Theorem 4.8 we see that $\bar{\rho}_{E,p} \sim \bar{\rho}_{f,\mathfrak{w}}$ for a Hilbert newform f of level $\mathfrak{N}_p$ and some prime $\mathfrak{w} \mid p$ of $\mathbb{Q}_f$. Recall that $\mathfrak{N}_p = \mathfrak{m}^{s'} \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r'_{\mathfrak{P}}}$, as in Lemma 4.12.

By the previous theorem we can reduce to the case $\mathbb{Q}_f = \mathbb{Q}$, after enlarging B_K by an effective amount. Since we have assumed $d \not\equiv 1 \pmod 4$ then there is only one prime $\mathfrak{P}$ above 2 and furthermore $\mathfrak{P} \in T$. Thus, by Lemma 4.14 E has potentially multiplicative reduction at $\mathfrak{P}$ and $p \mid \#\bar{\rho}_{E,p}(I_{\mathfrak{P}})$. If we enlarge B_K so that $p \nmid (N(\mathfrak{P}) \pm 1)$ then by Corollary 4.9 there is an elliptic curve E'/K having the same L-function as f. By the discussion above, after enlarging B_K and possibly replacing E' by an isogenous curve we may assume that E' has full 2-torsion.

It remains to prove (a) and (b). Recall that by Theorem 2.9 there are finitely many elliptic curves E' with full 2-torsion and good reduction outside $S \cup \{m\}$. Therefore we may assume, after possibly enlarging B_K, that for all primes $\mathfrak{q}$, if $v_{\mathfrak{q}}(j') < 0$ then $p \nmid v_{\mathfrak{q}}(j')$. We know from Lemma 4.13 that for $\mathfrak{q} \notin S$, $p \nmid \#\bar{\rho}_{E,p}(I_{\mathfrak{q}})$, hence $p \nmid \#\bar{\rho}_{E',p}(I_{\mathfrak{q}})$. By Lemma 4.13 this implies that $v_{\mathfrak{q}}(j') \geq 0$.

Finally, as mentioned before we have that $p \mid \bar{\rho}_{E,p}(I_{\mathfrak{P}})$ for $\mathfrak{P} \in T$, therefore $p \mid \bar{\rho}_{E',p}(I_{\mathfrak{P}})$. By Theorem 2.16 we have that $v_{\mathfrak{P}}(j') < 0$.

□

The S-unit equation

In the previous section we have found a particular elliptic curve E' related to a solution the Fermat equation. Relating the j-invariant of E' with the S-unit equation in K allows us to derive a condition which if satisfied by K implies that the asymptotic Fermat's Last Theorem holds in K.

Recall that the ring of *S-integers* of K, which already appeared in Section 2.4, is

$$\mathcal{O}_S = \{a \in K : v_{\mathfrak{q}}(a) \geq 0 \text{ for all } \mathfrak{q} \notin S\}.$$

Here S denotes the set of primes above 2, as before. The *S-unit equation* is

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

Note that the S-unit equation has precisely 3 solutions in $\mathbb{Q} \cap \mathcal{O}_S^*$, namely

$$(\lambda, \mu) = (2, -1), (-1, 2), (1/2, 1/2).$$

These solutions will be called *irrelevant*, while any other solution will be called *relevant*.

Theorem 4.17. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with $d \not\equiv 1 \pmod 4$. Suppose that for every solution (λ, μ) to the S-unit equation*

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

the prime $\mathfrak{P} \in T$ above 2 satisfies $\max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leq 4v_{\mathfrak{P}}(2)$. Then the asymptotic Fermat's Last Theorem holds over K.

Proof. Take B_K as in Theorem 4.16, and let (a, b, c) be a non-trivial solution to the Fermat equation with prime exponent $p > B_K$. By Lemma 4.11 we can rescale (a, b, c) such that they remain integral and $\mathcal{G}_{a,b,c} = \mathfrak{m}$ for some $\mathfrak{m} \in \mathcal{H}$. Recall that since $d \not\equiv 1 \pmod 4$ then $S = T = \{\mathfrak{P}\}$. Now Theorem 4.16 yields an elliptic curve E'/K with full 2-torsion and potentially good reduction outside $\mathfrak{P}$ (i.e. $v_{\mathfrak{q}}(j') \geq 0$ for all $\mathfrak{q} \neq \mathfrak{P}$). Moreover $v_{\mathfrak{P}}(j') < 0$. As a consequence $j' \in \mathcal{O}_S$.

Recall from Section 2.1 that the j-invariant can be written as

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

for some $\lambda \in K$. Moreover j' is invariant under any of the six combinations

$$\left\{ \lambda, \frac{1}{\lambda}, 1 - \lambda, \frac{1}{1 - \lambda}, \frac{\lambda}{\lambda - 1}, \frac{\lambda - 1}{\lambda} \right\}. \tag{4.3}$$

The equation for j' shows that λ satisfies a polynomial equation with coefficients in $\mathcal{O}_S$, and therefore $\lambda \in \mathcal{O}_S$. In the same way, all six combinations above belong to $\mathcal{O}_K$. In particular $1/\lambda, \mu \coloneqq 1 - \lambda$ and $1/\mu$ belong to $\mathcal{O}_S$, so that both $\lambda, \mu \in \mathcal{O}_S^*$, and hence (λ, μ) is a solution to the S-unit equation.

We rewrite the j' as

$$j' = 2^8 \frac{(1 - \lambda\mu)^3}{(\lambda\mu)^2}$$

and denote $t \coloneqq \max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\}$. By our assumption $t \leq 4v_{\mathfrak{P}}(2)$. If $t = 0$ then $v_{\mathfrak{P}}(j') \geq 8v_{\mathfrak{P}}(2) > 0$, which is a contradiction. If $t > 0$, then the relation $\lambda + \mu = 1$ implies that either $v_{\mathfrak{P}}(\lambda) = v_{\mathfrak{P}}(\mu) = -t$, $v_{\mathfrak{P}}(\lambda) = 0$ and $v_{\mathfrak{P}}(\mu) = t$ or $v_{\mathfrak{P}}(\lambda) = t$ and $v_{\mathfrak{P}}(\mu) = 0$. Thus $v_{\mathfrak{P}}(\lambda\mu) = -2t < 0$ or $v_{\mathfrak{P}}(\lambda\mu) = t > 0$. In either case $v_{\mathfrak{P}}(j') = 8v_{\mathfrak{P}}(2) - 2t \geq 0$, which is again a contradiction. □

The final step is to understand the solutions the S-unit equation for real quadratic fields, in order to give a explicit description of the d's such that $\mathbb{Q}(\sqrt{d})$ satisfy the asymptotic Fermat's Last Theorem. We will say that two solutions to

the S-unit equation are *equivalent* if they are related to each other by a transformation as in (4.3). Note that the three relevant solutions $(2,-1),(-1,2),(1/2,1/2)$ form a single set of equivalent solutions.

It is straightforward to see that given two equivalent solutions (λ,μ) and (λ',μ') then

$$\max\{|v_{\mathfrak{P}}(\lambda)|,|v_{\mathfrak{P}}(\mu)|\}\leq 4v_{\mathfrak{P}}(2)\Longleftrightarrow \max\{|v_{\mathfrak{P}}(\lambda')|,|v_{\mathfrak{P}}(\mu')|\}\leq 4v_{\mathfrak{P}}(2).$$

Let us check for example the case $\lambda'=1/\lambda$. Clearly $|v_{\mathfrak{P}}(\lambda)|=|v_{\mathfrak{P}}(\lambda')|$. Now, $\mu'=(\lambda-1)/\lambda$, so that if $v_{\mathfrak{P}}(\lambda)>0$ then $v_{\mathfrak{P}}(\mu')=-v_{\mathfrak{P}}(\lambda)$, if $v_{\mathfrak{P}}(\lambda)<0$ then $v_{\mathfrak{P}}(\mu')=0$ and if $v_{\mathfrak{P}}(\lambda)=0$ then $v_{\mathfrak{P}}(\mu')=v_{\mathfrak{P}}(\mu)$. In all three cases we get the desired result.

Finally, since K is quadratic there is only one or two primes above 2, and this implies that in any equivalence class of solutions there is a representative which lies in $\mathcal{O}_K$, or what is the same, there is a solution (λ,μ) such that $v_{\mathfrak{P}}(\lambda),v_{\mathfrak{P}}(\mu)\geq 0$ for all $\mathfrak{P}\in S$.

Lemma 4.18. *Let $K=\mathbb{Q}(\sqrt{2})$ with $d\geq 2$ squarefree. Up to equivalence every relevant solution to the S unit equation (λ,μ) has the form*

$$\lambda=\frac{\eta_1 2^{r_1}-\eta_2 2^{r_2}+1+v\sqrt{d}}{2},\qquad \mu=\frac{\eta_2 2^{r_2}-\eta_1 2^{r_1}+1-v\sqrt{d}}{2},\tag{4.4}$$

where

$$\eta_1=\pm 1,\qquad \eta_2=\pm 1,\qquad r_1\geq r_2\geq 0,\qquad v\in\mathbb{Z},\qquad v\neq 0\tag{4.5}$$

are related by

$$(\eta_1 2^{r_1}-\eta_2 2^{r_2}+1)^2-\eta_1 2^{r_2+2}=dv^2,\tag{4.6}$$
$$(\eta_2 2^{r_2}-\eta_1 2^{r_1}+1)^2-\eta_1 2^{r_1+2}=dv^2.\tag{4.7}$$

Moreover, if $d\not\equiv 1 \pmod 8$ then we can take $r_2=0$.

Note that (4.6) and (4.7) are equivalent.

Proof. Let us first see that (λ,μ) defined as above are indeed relevant solutions. It is clear from (4.4) that λ and μ belong to $\mathcal{O}_S\setminus\mathbb{Q}^*$ and that they satisfy $\lambda+\mu=1$. Moreover, by (4.6) and (4.7) the norms of λ and μ are $\eta_1 2^{r_1}$ and $\eta_2 2^{r_2}$ respectively, so that $\lambda,\mu\in\mathcal{O}_S^*$. Thus (λ,μ) is a relevant solution.

Conversely, assume (λ,μ) is a relevant solution. By the discussion above we may suppose that $(\lambda,\mu)\in\mathcal{O}_K$. Denote by $x\mapsto\bar{x}$ conjugation in K. Then

$$\lambda\bar{\lambda}=\eta_1 2^{r_1},\qquad \mu\bar{\mu}=\eta_2 2^{r_2},$$

with $\eta_1=\pm 1$, $\eta_2=\pm 1$ and since $\lambda,\mu\in\mathcal{O}_K$ then $r_1,r_2\geq 0$. We may suppose by switching λ and μ that $r_1\geq r_2\geq 0$. Note that if $d\not\equiv 1 \pmod 8$ then S consists of 1 element and therefore the relation $\lambda+\mu=1$ forces $r_2=0$. Write

$$\lambda+\bar{\lambda}=\lambda\bar{\lambda}-(1-\lambda)(1-\bar{\lambda})+1=\lambda\bar{\lambda}-\mu\bar{\mu}+1=\eta_1 2^{r_1}-\eta_2 2^{r_2}+1.$$

In the same way, $\lambda - \bar{\lambda} = v\sqrt{d}$ for some $v \in \mathbb{Z}$. Expressing λ as $\lambda = \frac{1}{2}((\lambda + \bar{\lambda}) + (\lambda - \bar{\lambda}))$ gives the result in (4.4). The expression for μ comes from $\mu = 1 - \lambda$, equation (4.6) derive from the identity $(\lambda + \bar{\lambda})^2 - (\lambda - \bar{\lambda})^2 = 4\lambda\bar{\lambda}$ and similarly with (4.7) and μ. □

d	relevant solutions of the S-unit equation up to equivalence
$d = 2$	$(\sqrt{2}, 1-\sqrt{2})$, $(-16+12\sqrt{2}, 17-12\sqrt{2})$, $(4+2\sqrt{2}, -3+2\sqrt{2})$, $(-2+2\sqrt{2}, 3-2\sqrt{2})$
$d = 3$	$(2+\sqrt{3}, -1-\sqrt{3})$, $(8+4\sqrt{3}, -7-4\sqrt{3})$
$d = 5$	$((1+\sqrt{5})/2, (1-\sqrt{5})/2)$, $(-8, +4\sqrt{5}, 9-4\sqrt{5})$, $(-1+\sqrt{5}, 2-\sqrt{5})$
$d = 6$	$(-4+2\sqrt{6}, 5-2\sqrt{6})$
$d \equiv 3 \pmod 8$, $d \neq 3$	none
$d \equiv 5 \pmod 8$, $d \neq 5$	none
$d \equiv 7 \pmod 8$	$(2^{2s+1} + 2^{s+1}w\sqrt{d}, 1 - 2^{2s+1} - 2^{s+1}w\sqrt{d})$ such that $4^s - 1 = dw^2$, $s \geq 2$ and $w \neq 0$
$d \equiv 2 \pmod{16}$, $d \neq 2$	$(-2^{2s} + 2^s w\sqrt{d}, 1 + 2^{2s} - 2^s w\sqrt{d})$ such that $4^s + 1 = dw^2$, $s \geq 2$ and $w \neq 0$
$d \equiv 6 \pmod{16}$, $d \neq 6$	none
$d \equiv 10 \pmod{16}$	none
$d \equiv 14 \pmod{16}$	$(2^{2s} + 2^s w\sqrt{d}, 1 - 2^{2s} - 2^s w\sqrt{d})$ such that $4^s - 2 = dw^2$, $s \geq 2$ and $w \neq 0$

Table 4.1: Relevant solutions of the S-unit equation for $d \geq 2$ squarefree, $d \not\equiv 1 \pmod 8$.

Lemma 4.19. *Let $d \not\equiv 1 \pmod 8$ be squarefree ≥ 2. The relevant solutions to the S-unit equation, up to equivalence, are as given in Table 4.1.*

Proof. Since $d \not\equiv 1 \pmod 8$ we assume $r_2 = 0$. Values $0 \leq r_1 \leq 5$ combined with $\eta_1 = \pm 1$ and $\eta_2 = \pm 1$ give the solutions Table 4.1 for $d = 2, 3, 5, 6$ and the solution $(16 - 4\sqrt{14}, -15 + 4\sqrt{14})$, which is included under $d \equiv 14$ in Table 4.1. Therefore we suppose that $r_1 \geq 6$. If $\eta_2 = -1$ then equation (4.7) gives $2^{2r_1} + 4 = dv^2$. Since $r_1 \geq 6$ this implies that $4 \equiv dv^2 \pmod 8$. However a square mod 8 can only be 0, 1 or 4, and as d is squarefree we have that necessarily $d \equiv 1 \pmod 8$, which is a contradiction.

Thus assume $\eta_2 = 1$. Now equation (4.6) yields

$$2^{r_1+2}(2^{r_1-2} - \eta_1) = dv^2.$$

Note that if d is odd then r_1 is even, since in this case 2^{r_1+2} is the greatest power of 2 which divides v^2. Moreover, if d is even, since it is squarefree the greatest power

of 2 dividing v^2 is 2^{r_1+1}, so that r_1 must be *odd*. Suppose first that d is odd, and so $r_1 = 2s+2$ and $v = 2^{s+2}w$ for some non-zero integer w. Note that since $r_1 \geq 6$ then $s \geq 2$. Dividing by 2^{s+2} we get $4^s - \eta_1 = dw^2$. As $\eta = \pm 1$ this equation has no solution if $d \equiv 3$ or $5 \pmod 8$. This completes the proof in these two cases. If $d \equiv 7 \pmod 8$ reduction of the equation modulo 8 shows that $\eta = 1$. This gives the solution in Table 4.1 for $d \equiv 7 \pmod 8$.

Suppose that d is even, and so $r_1 = 2s+1$ and $v = 2^{s+1}w$ for some non-zero integer w, and $s \geq 2$. Then $2^{2s-1} - \eta = (d/2)w^2$. As before this gives a contradiction when $d \equiv 6$ or $10 \pmod 8$, and thus proving these cases, including $d = 6$ (recall that the solution for $d = 6$ was for $r_1 < 6$). Finally for $d \equiv 2$ or $14 \pmod 8$ then $\eta_1 = -1, 1$ respectively, leading to the solutions of Table 4.1. However it is easy to see that $\eta_1 = -1$ neither gives a solution for $d = 2$ since $2^{2s-1} + 1 = w^2$ implies that $(w+1)(w-1) = 2^{2s-1}$, which is impossible.

□

Theorem 4.20. *Let $d \geq 2$ be squarefree, satisfying one of the following*

(i) $d \equiv 3 \pmod 8$.

(ii) $d \equiv 6$ *or* $10 \pmod{16}$.

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

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

Then the asymptotic Fermat's Last Theorem holds in $K = \mathbb{Q}(\sqrt{d})$.

Proof. Since in all cases $d \not\equiv 1 \pmod 4$ we have that $S = T = \{\mathfrak{P}\}$. We have to verify that for all such d all the solutions to the S-unit equation over $K = \mathbb{Q}(\sqrt{2})$ satisfy

$$\max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\} \leq 4v_{\mathfrak{P}}(2), \tag{4.8}$$

and then apply Theorem 4.17 to conclude that the asymptotic Fermat's Last Theorem holds. In fact, by what we saw above, we only have to check (4.8) for one representative of each equivalence class of solutions. The irrelevant solutions and the particular solutions for $d = 2, 3, 6$ listed in Table 4.1 satisfy it.

For $d \equiv 3 \pmod 8$ or $d \equiv 6$ or $10 \pmod{16}$ there are no further solutions, so cases (i) and (ii) are proved.

Suppose $d \equiv 2 \pmod{16}$ and $d \neq 2$. Then there is no relevant solutions unless there are $s \geq 2$ and $w \neq 0$ such that $4^s + 2 = dw^2$. If $q \mid d$ is an odd prime, then $2^{2s} \equiv -2 \pmod q$, which implies that $q \equiv 1$ or $3 \pmod 8$.

Finally id $d \equiv 14 \pmod{16}$ there are no relevant solutions unless there are $s \geq 2$ and $w \neq 0$ such that $4^s - 2 = dw^2$. Now if $q \mid d$ is an odd prime, then $2^{2s} \equiv 2 \pmod q$, which implies that $q \equiv 1$ or $7 \pmod 8$.

□

Bibliography

[1] Berger, L., Böckle, G., Dembélé, L., Dimitrov, M., Dokchitser, T., Voight, J., *Elliptic Curves, Hilbert Modular Forms and Galois Deformations*, Advanced Courses in Mathematics - CRM Barcelona, Birkhaüser, 2013.

[2] Bourbaki, N., *Algebra*, Elements of Mathematics, Hermann, Paris, 1958.

[3] Bruinier, J. H., van der Geer, Harder, G., Zagier, D., *The 1-2-3 of Modular Forms*, Universitext, Springer, 2008.

[4] Cohen, H., *Number Theory, Volume II: Analytic and Modern Tools*, GTM 240, Springer, 2007.

[5] Curtis, C. W., Reiner, I.,*Representation Theory of Finite Groups and Associative Algebras*, Wiley Interscience, New York,1962.

[6] Cornell, G., Silverman J. H., Stevens, G., *Modular Forms and Fermat's Last Theorem*, Springer-Verlag, 1997.

[7] Darmon, H., *Rational Points on Modular Elliptic curves*, CBMS 101, AMS,2004.

[8] Diamond, F., Shurman, J., *A First Course in Modular Forms*, GTM 228, Springer, 2005.

[9] Deligne, P., *Formes modulaires et représentation ℓ-adiques*, Sém. Bourbaki, 1968/69, Exposé 355. Lect. Notes in Math. 179 (1971), 139-172.

[10] Freitas, N., Siksek, S., *The Asymptotic Fermat's Last Theorem for Five-sixths of Real Quadratic Fields*, `arXiv:1307.3162`, 16 July 2014.

[11] Freitas, N., Le Hung, B. V., Siksek, S., *Elliptic curves over real quadratic fields ar modular,* `arXiv:1310.7088`, 13 November 2013.

[12] Freitas, N., Siksek, S., *Criteria for irreducibility of mod p representations of Frey curves*, `arXiv:1309.4748`, 18 September 2013.

[13] Jarvis, F., *Level lowering for modular forms mod ℓ over totally real fields*, Math. Ann. 313 (1999), no. 1, 141-160.

[14] Koblitz, N., *Introduction to Elliptic Curves and Modular Forms*, GTM 97, Springer-Verlag, 1984.

[15] Kraus, A., *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. 69 (1990) no. 4, 353-385.

[16] Mazur, B.,*Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33 - 186.

[17] Mazur, B.,*Rational assignees of prime degree*, Inventiones Math. 44 (1978), 129-162.

[18] Silverman, J. H.,*The Arithmtic of Elliptic Curves*, GTM 106, Springer, 1986.

[19] Silverman, J. H.,*Advanced Topics in the Arithmtic of Elliptic Curves*, GTM 151, Springer, 1994.