UNIVERSITAT DE BARCELONA

ADVANCED MATHEMATICS

MASTER'S FINAL PROJECT

Fermat's Last Theorem on Totally Real Fields

Author:
Habib Ullah Abdul Parveen

Supervisor:
Lluis Diuelefet

Facultat de Matemàtiques i Informàtica

June, 28, 2023

Contents

Chapter 1

Introduction

Fermat's Last Theorem states the equation

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

has only trivial solutions, i.e $abc = 0$, for $n > 2$ and a, b, c integers. The idea of the proof is to attach the Frey Curve

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

of course we assume a, b, c are coprime integers with $a \equiv -1 \mod 4$ and $2|b$. The conductor of this curve is

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

The curve is semistable and so modular by Wile's Theorem, since the conductor is of the form $2N$ for some odd integer N, we can apply Ribet's Theorem to show there is a weight 2 newform g of level 2 such that $\bar{\rho}_g \cong \bar{\rho}_{E_{a^p,b^p,c^p}}$. This arises a contradiction, because there are no weight 2 neforms of level 2.

The first section is devoted to introduce the concepts needed to understand in more extense this proof. So, Galois representations, modular forms and Elliptics are introduced and some results stated. At the end, a more detailed proof is given.

In the second section we consider solutions over some real quadratic feilds K. We show a non-trivial solution in K gives rise to a non-trivial solution in the ring of integers $\mathcal{O}_K$. We consider the same Frey curve in hope to get a contradiction. The conductor is given by

$$\mathcal{N} = \mathfrak{m}^{s_\mathfrak{m}} \cdot \prod_{\mathfrak{P}\in S} \mathfrak{P}^{r}_{\mathfrak{P}} \cdot \prod_{q|abc, q\notin S\cup\{\mathfrak{m}\}}$$

where $\mathfrak{m}$ is an ideal that arises due to K not having class number one (so we cant consider a, b, c, coprime) and S is the set of primes above 2. The curve is semistable outside $S \cup \{\mathfrak{m}\}$. Applying a version of the Level Lowering to the representation $\bar{\rho}_{E,p}$ we conclude there exists a parallel weight 2 Hillbert newfor $\mathfrak{f}$ and level divisble only by the primes $S \cup \{\mathfrak{m}\}$. At this point we dont get a contradiction, so we will have to deviate a little from the Fermat's Last Theorem.

A simple analogy of our strategy at this point is shown when one tries to solve the Serre-Mazur-Kraus equation (that is explained in Appendix A)

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

where one gets another elliptic curve E' with 2-full torsion and potentially. Studying the images of inertia one concludes E' has potentially good reduction outside S.

There are curves with such properties and we still don't get a contradiction. But to this elliptic curve E' with full 2-torsion we can prove this comes from an $\mathcal{O}_S$-point. And studying the S-unit equation on our field K gives us a contradiction.

Chapter 2

Fermat's Last Theorem

Theorem 1 (Fermat's Last Theorem). *For an integer $n > 2$ the equation*

$$a^n + b^n = c^n \qquad a, b, c \in \mathbb{Q} \tag{2.1}$$

has only trivial solutions, i.e. $abc = 0$.

It was stated by Pierre de Fermat in 1637 and a complete proof was published in 1995 by Andrew Wiles. The proof was a work of innumberable mathematicians and needed new tools. In this chapter we introduce these objects: elliptic curves, modular forms and Galois representaion; we will mention the most notorious results, amongst others the remarkable modularity theorem. At the end of the section an idea of a proof will be presented.

2.1 Galois Representations

2.1.1 The Krull topology

Consider the rationals $\mathbb{Q}$ and an algebraic cloussure $\overline{\mathbb{Q}}$; our first step towards the definition of a Galois representation will be to endow the Galois Group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with the Krull topology.

We consider a general Galois extension M/L and its Galois group $\mathrm{Gal}(M/L)$. We define an inverse system, the objects are the Galois groups $\mathrm{Gal}(K_i/L)$ where K_i/L is a finite Galois extension such that $K_i \subset M$. The order is defined $\mathrm{Gal}(K_i/L) \leq \mathrm{Gal}(K_j/L)$ iff $K_i \subset K_j$. Finally, the maps

$$\varphi_{ij} : \mathrm{Gal}(K_j/L) \longrightarrow \mathrm{Gal}(K_i/L)$$
$$\sigma \mapsto \sigma_{|K_i}.$$

These maps are well defined because for any element $\sigma \in \mathrm{Gal}(K_j/L)$ and Galois subextension K_i/L we have $\sigma(K_i) \subset K_i$.

Let's check in fact this is an inverse system, the condition $\varphi_{ii} = \mathrm{Id}$ is trivial, and if $\varphi_{jk} \circ \varphi_{ij} = \varphi_{ik}$ for $K_i \subset K_j \subset K_k$ is also satisfied because φ_{ij} and φ_{jk} are the restriction maps.

Theorem 2. *Let M/L be a Galois extension with Galois group $Gal(M/L)$. Consider the inverse system defined above, then there is a group isomorphism*

$$\Psi : Gal(M/L) \xrightarrow{\sim} \varprojlim_{K} Gal(K/L)$$
$$\sigma \mapsto (\sigma_{|K}).$$

Proof. First of all, the map Ψ is well defined since $(\sigma_{|K}) \in \prod_K \mathrm{Gal}(K/L)$ and $\varphi_{ij}(\sigma_{|K_j}) = \sigma_{|K_i}$ for $K_i \subset K_j$. It is a group homomorphism because $(\sigma \circ \tau)_{|K} = \sigma_{|K} \circ \tau_{|K}$ (because we are dealing with Galois extensions $\tau(K) \subset K$). It remains to show its bijective.

Injective: If $\sigma \neq \mathrm{Id}$ then for some $x \in M$, $\sigma(x) \neq x$. Hence there is a finite Galois extension K/L and $x \in K$ so $\sigma_{|K} \neq \mathrm{Id}$.

Surjective: Consider any $(\sigma_K) \in \varprojlim_{K} \mathrm{Gal}(K/L)$. If $x \in K_i \cap K_j$ then $\sigma_{K_i}(x) = \sigma_{K_j}(x)$ since $K_i \cap K_j/L$ is a finite Galois extension so

$$\sigma_{K_i}(x) = \sigma_{K_i \cap K_j}(x) = \sigma_{K_j}(x).$$

Hence define $\sigma : M \to M$ by $\sigma(x) := \sigma_K(x)$ for some finite Galois extension K containing x. The map is well defined, since any element of M lives in some finite extension of L and similar arguments as before show this map is a field autormorphism and leaves K fixed. □

We endow $\mathrm{Gal}(K/L)$ with the discrete topology, the product topology on $\prod_K \mathrm{Gal}(K/L)$, and $\varprojlim_{K} \mathrm{Gal}(K/L)$ with the subspace topology; then $\mathrm{Gal}(M/L)$ inherits a topology via the map Ψ called the **Krull topology**.

Althoug the groups $\mathrm{Gal}(K/L)$ have the discrete topology but the product $\prod_K \mathrm{Gal}(K/L)$ does not have the discrete topology when the extension M/L is infinite. Certainly, a basis for the product topology is given by

$$\mathcal{B}' = \left\{ \prod_K U_K : U_K \subset \mathrm{Gal}(K/L) \text{ and } U_K \neq \mathrm{Gal}(K/L) \text{ for finitely many } K \right\}.$$

From theese expressions it follows a basis of the neighbourhoods of the identity $\mathrm{Id} \in \prod_K \mathrm{Gal}(K/L)$ is given by

$$\mathcal{B}'_{\mathrm{Id}} = \left\{ \prod_K U_K : U_K = \mathrm{Gal}(L/K) \text{ or, for finitely many } K,\, U_K = \{\mathrm{Id}\} \right\}.$$

And from the last expression, a basis of neighbourhoods for the identity $\mathrm{Id} \in \mathrm{Gal}(M/L)$ (the identity of the galois group) is given by

$$\mathcal{B}_{\mathrm{Id}} = \left\{ \mathrm{Gal}(M/K) : \text{finite Galois extension } K/L \right\}. \tag{2.2}$$

Similar reasonings prove that for $\sigma \in \mathrm{Gal}(M/L)$ a basis of neighbourhoods is given by

$$\mathcal{B}_\sigma = \sigma \cdot \mathcal{B}_{\mathrm{Id}}.$$

The last observations proves that the map $\tau \mapsto \sigma\tau$ is also an homeomorphism (it is compatible with the group structure and also with the topology). This is not a mere coincidence, because $\mathrm{Gal}(M/L)$ is a topological group, meaning:

- The multiplication map $\cdot : \mathrm{Gal}(M/L) \times \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/L)$ given by $(\sigma, \tau) \mapsto \sigma\tau$ is continuous.
- The inverse map $\mathrm{Gal}(M/L) \to \mathrm{Gal}(M/L)$ given by $\tau \mapsto \tau^{-1}$ is continuous.

In literature $\mathrm{Gal}(M/K)$ is also called a profinite group (since it arises from finite groups). There are innumberable properties that we can list: it is a compact group, every open subgroup is also closed, the group is totally disconnected, etc.

2.1.2 Galois representations

Just like we have a notion of a topological group, we say a ring A is topological if:

- The multiplication map $\cdot : A \times A \to A$ and addition $+ : A \times A \to A$ are continuous.
- The multiplication map $\mathrm{Gal}(M/L) \times \mathrm{Gal}(M/L) \to \mathrm{Gal}(M/L)$ given by $(\sigma, \tau) \mapsto \sigma\tau$ is continuous.
- The inverse map $A^* \to A^*$ is continuous.

We can identify the general lineal group $\mathrm{GL}_n(A)$ with a subset of $n \times n$ matrices with coefficients in A. Hence $\mathrm{GL}_n(A)$ inherits a topology from A^{n^2}.

Definition 1. *A **galois representation** of dimension n is a map*

$$\rho : Gal(M/K) \to GL_n(A),$$

where A is a topological ring and ρ is a group morphism and continuous.

Although the definition is quite general, we will be interested in a particular type of rings.

Definition 2. *A **coefficient ring** A is complete noetherian local ring, with finite residue field $k_A := A/m_A$, here m_A is the maximal ideal of A. And the topology is the $\mathfrak{p}$-adic.*

Definition 3. *Consider A a coefficient ring and $\rho : Gal(M/K) \to GL_n(A)$ a galois representation. The **residual representation** of ρ is*

$$\overline{\rho} : Gal(M/K) \to GL_n(k_A),$$

the composition of ρ with the reduction map $GL_n(A) \to GL_n(k_A)$.

If k denotes a finite field and $\rho_0 : Gal(M/K) \to GL_n(k)$ a galois representation, then ρ lifts to A if $k = k_A$ and $\overline{\rho} = \rho_0$.

Two liftings ρ, ρ' of ρ_0 are equivalent if ρ can be conjugated by a matrix of $GL_n(A)$ to obtain ρ'.

*A **deformation** of ρ_0 to A is an equivalence class of liftings of ρ_0 to A.*

Example 1. *Fix a prime number $p \in \mathbb{N}$ and let ord_p the valuation at p, i.e. and $ord_p(a) = m$ if $a = bp^m$ for some $p \not| b$ and we set $ord_p(0) = \infty$. We have an absolute value $|\cdot|_p := e^{-ord_p(\cdot)}$ on $\mathbb{Z}$, consequenlty a metric.*

The completion of $\mathbb{Z}$ with respect of this metric is called the p-adic numbers $\mathbb{Z}_p$. By construction they are complete, moreover it is a valuation ring, hence it is local and PID and therefore noetherian. We conclude they are a coefficient ring.

Another way of "obtaining" the ring $\mathbb{Z}_p$ is using an inverse system: the sets are $\mathbb{Z}/p^n\mathbb{Z}$ the maps $\varphi_{ij} : \mathbb{Z}/p^i\mathbb{Z} \to \mathbb{Z}/p^j\mathbb{Z}$ for $j \leq i$ is simply the restriction. Then

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p.$$

These new perspective allows us to define a Galois representation. Again, for a fixed prime $p \in \mathbb{N}$, consider the roots of the unity $\mu_n = \{\xi \in \mathbb{C} : \xi^{p^n} = 1\}$ which give rise to finite Galois extensions $\mathbb{Q}(\mu_n)/\mathbb{Q}$, the Galois group is isomorphic (not canonically) to

$$Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong \big(\mathbb{Z}/p^n\mathbb{Z}\big)^{\times}.$$

Moreover they form an inverse system with the maps $\varphi_{ij} : \mu_i \to \mu_j$ given by $\xi \mapsto \xi^{p^{i-j}}$ for $j \leq i$. To sum up, we have the commutative diagram

$$\begin{tikzcd}
\big(\mathbb{Z}/p^i\mathbb{Z}\big)^{\times} \arrow[r] \arrow[d, "\sim"] & \big(\mathbb{Z}/p^j\mathbb{Z}\big)^{\times} \arrow[d, "\sim"] \\
Gal(\mathbb{Q}(\mu_i)/\mathbb{Q}) \arrow[r] & Gal(\mathbb{Q}(\mu_j)/\mathbb{Q})
\end{tikzcd}$$

Denote by $\mu_\infty = \bigcup_{n\geq 1} \mu_n$, applying Theorem (2)

$$Gal(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \cong \varprojlim_n Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong \varprojlim_n \big(\mathbb{Z}/p^n\mathbb{Z}\big)^{\times} \cong \mathbb{Z}_p^{\times}$$

The last isomorphism is because $\varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^{\times} \subset \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$, now an element of $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is invertible iff every coordinate is invertible.

Finally, we get the the Galois representation

$$Gal(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^{\times} \cong GL_1(\mathbb{Z}_p)$$

This map is clearly a group morphism and continuous. We can extend this representation

$$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow Gal(\mathbb{Q}(\mu_\infty)/\mathbb{Q}) \to \mathbb{Z}_p$$

where the first arrow corresponds to the restriction. This is called the ***p-adic representation****.*

2.1.3 Ramifications

Fix a prime $p \in \mathbb{N}$, denote by $\overline{\mathbb{Q}}_p$ an algebraic clousre of $\mathbb{Q}_p$; it is known that the norm $|\cdot|_p$ on $\mathbb{Q}_p$ extends uniquely to every $\alpha \in \overline{\mathbb{Q}}_p$ by

$$|\alpha|_p = |N_{\mathbb{Q}_p(\alpha)/\mathbb{Q}_p}(\alpha)|^{1/[\mathbb{Q}_p(\alpha):\mathbb{Q}_p]}. \tag{2.3}$$

Denote the valuation rings $\mathcal{O}_{\overline{\mathbb{Q}}_p}$, $\mathcal{O}_{\mathbb{Q}_p}$, the maximal ideals $\mathfrak{m}_{\overline{\mathbb{Q}}_p}$, $\mathfrak{m}_{\mathbb{Q}_p}$ and the residue fields $k_{\overline{\mathbb{Q}}_p} = \mathcal{O}_{\overline{\mathbb{Q}}_p}/\mathfrak{m}_{\overline{\mathbb{Q}}_p}$, $k_{\mathbb{Q}_p} = \mathcal{O}_{\mathbb{Q}_p}/\mathfrak{m}_{\mathbb{Q}_p}$ of $\overline{\mathbb{Q}}_p$ and $\mathbb{Q}_p$ respectively.

First note that $k_{\mathbb{Q}_p} = \mathbb{F}_p$, the finite field of p elements, since $\mathcal{O}_{\mathbb{Q}_p} = \mathbb{Z}_p$ and $\mathfrak{m}_{\mathbb{Q}_p} = p\mathbb{Z}_p$. Also, $k_{\mathbb{Q}_p} \hookrightarrow k_{\overline{\mathbb{Q}}_p}$ given $\mathfrak{m}_{\mathbb{Q}_p} \subset \mathfrak{m}_{\overline{\mathbb{Q}}_p}$ and if $0 \neq \overline{x} \in k_{\mathbb{Q}_p}$ then also $0 \neq \overline{x} \in k_{\overline{\mathbb{Q}}_p}$. Moreover using the fact $k_{\overline{\mathbb{Q}}_p}/k_{\mathbb{Q}_p}$ is an algebraic extension, and $k_{\overline{\mathbb{Q}}_p}$ is algebraically closed we conlude $k_{\overline{\mathbb{Q}}_p} = \overline{\mathbb{F}}_p$.

By equation (2.3) we conclude $|\sigma(\alpha)|_p = |\alpha|_p$ for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ hence $\sigma(\mathcal{O}_{\overline{\mathbb{Q}}_p}) \subset \mathcal{O}_{\overline{\mathbb{Q}}_p}$. Hence there is a continuous map $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F})$, which turns out to be surjective.

On the other side, the identification

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p \hookrightarrow \overline{\mathbb{Q}}_p.$$

extends, not uniquely, to an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$; all other embeedings are obtained by conjugatin with an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ the field $\mathbb{Q}$ is fixed and $\sigma(\overline{\mathbb{Q}}) \subset \overline{\mathbb{Q}}$ we then have a map

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}),$$

which is continuous and is injective. To see it is continuous: it will be enough to check the preimage of neighbourhood of the identity (2.2) is open, consider $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for some finite Galois extension $K/\mathbb{Q}$, the preimage is

$\mathrm{Gal}(\overline{\mathbb{Q}}_p/K\mathbb{Q}_p)$ which is open, given $K\mathbb{Q}_p/\mathbb{Q}_p$ is a finite Galois extension. Injectivity needs more work, the idea is to use Krasner's lemma to prove $\overline{\mathbb{Q}}$ is dense inside $\overline{\mathbb{Q}}_p$.

The image $D_p \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the last identification is the **decomposition** group, defined up to conjugancy. The **inertia** group $I_p \subset D_p$ fits in the exact sequence

$$\mathrm{Id} \to I_p \to D_p \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \to \mathrm{Id}$$

Definition 4. *A Galois representation $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_n(A)$ is **unramified** at p if $I_p \subset \ker\rho$.*

2.2 Modular forms

2.2.1 First definitions

Definition 5. *The **upper half plane** is*

$$\mathcal{H} = \{a + bi \in \mathbb{C} : b > 0\}$$

The group of automorphisms of $\mathcal{H}$ is the group

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc = 1 \right\},$$

and acts on $\mathcal{H}$ via

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

We are interested in a particular subgroup of $\mathrm{SL}_2(\mathbb{R})$.

Definition 6. *The **modular group** is*

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

*The **principal congruence subgroup** of level N is*

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

*A subgroup $\Gamma \subset SL_2(\mathbb{Z})$ is a **congruence subgroup of level** N if $\Gamma(N) \subset \Gamma$.*

Definition 7. *For any* $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ *the* ***weight*** k ***operator*** *maps a function* $f : \mathcal{H} \to \mathbb{C}$ *to the function*

$$(f[\gamma]_k)(\tau) = (c\tau + d)^{-k} f(\gamma(\tau))$$

If f *is meromorphic and satisfies* $f[\gamma]_k = f$ *for every* $\gamma \in \Gamma \subset SL_2(\mathbb{Z})$, *then* f *is* ***weakly modular of weight*** k ***with respect the modular subgroup*** Γ***.***

Remark 1. *Every* $\Gamma \subset SL_2(\mathbb{Z})$ *congruence subgroup of level* N *contains a matrix that acts on* $\mathcal{H}$ *via*

$$\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \cdot \tau = \tau + h.$$

This means, every weakly modular function $f : \mathcal{H} \to \mathbb{C}$ *satisfies* $(f[\gamma]_k)(\tau) = f(\tau + h)$, *i.e. it is* $h\mathbb{Z}$ *periodic.*

Denote by $D' = \{z \in \mathbb{C} : 0 < |z| < 1\}$ *the punctured disk, and note the map* $\tau \mapsto e^{\frac{2\pi\tau}{h}}$ *transforms* $\mathcal{H}$ *into* D'. *So consider*

$$\begin{aligned} g \colon D' &\longrightarrow \mathbb{C} \\ q &\longmapsto f\left(h\frac{\log(q)}{2\pi i}\right) \end{aligned}$$

though $\log(q)$ *is determined up to* $2\pi i\mathbb{Z}$, *the function* g *is well defined because it is* $h\mathbb{Z}$ *periodic, clearly* $f(\tau) = g(q_h)$ *for* $q_h = e^{\frac{2\pi i}{\tau}}$.

If f *is holomorphic, so it is* g *and we can consider the power series*

$$f(\tau) = \sum_{i=0}^{\infty} a_i q_h^i$$

.

We say f *is holomorphic at* ∞ *if* g *extends holomorphically at* D.

Definition 8. *Let* $\Gamma \subset SL_2(\mathbb{Z})$ *be a congruence subgroup and let* k *be an integer, we say* $f : \mathcal{H} \to \mathbb{C}$ *is a* ***modular form of weight*** k ***with respect*** Γ *if:*

1. f *is holomorphic*

2. f *is weight-*k *invariant under* Γ

3. $f[\alpha]_k$ is holomorphic at ∞ for each $\alpha \in SL_2(\mathbb{Z})$

*If the Fourier coefficient $a_0 = 0$ of $f[\alpha]_k$ for all $\alpha \in SL_2(\mathbb{Z})$ then f is **cusp form** of weight-k with respect to Γ.*

The space of modular functions of weight-k with respect a congruence subgroup Γ is denoted by $\mathcal{M}_k(\Gamma)$, and the subspace of cusp form by $\mathcal{S}_k(\Gamma)$.

2.2.2 Hecke operators

The double coset operator

The group of 2-by-2 matrices with rational entries and positive determinant is denoted by $\mathrm{GL}_2^+(\mathbb{Q})$, hence $\mathrm{SL}_2(\mathbb{Z})$ is a subgroup. Given two modular subgroups Γ_1, Γ_2 and $\alpha \in \mathrm{GL}_2(\mathbb{Q})$ the **double coset** is

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}.$$

Lemma 1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let α be an element of $GL_2^+(\mathbb{Q})$. Then $\alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z})$ is again a congruence subgroup of $SL_2(\mathbb{Z})$.*

Lemma 2. *Let Γ_1 and Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$, and let α be an element of $GL_2^+(\mathbb{Q})$. Then $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$ is a subgroup of Γ_2 and the action by left multiplication by α,*

$$\Gamma_2 \longrightarrow \Gamma_1\alpha\Gamma_2 \quad \textit{given by} \quad \gamma_2 \mapsto \alpha\gamma_2,$$

induces a natural bijection from the coses space Γ_2/Γ_3 to the orbit space $\Gamma_1/\Gamma_1\alpha\Gamma_2$. In words: the set $\{\gamma_{2,j}\}_j$ is a set of coset representatives of Γ_2/Γ_3 iff $\{\beta_j\} = \{\alpha\gamma_{2,j}\}$ is a set of orbit representatives of $\Gamma_1/\Gamma_1\alpha\Gamma_2$.

We extend the definition of the weight-k operator, given $\beta \in \mathrm{GL}_2^+(\mathbb{Q})$ and a function $f : \mathcal{H} \to \mathbb{C}$ then:

$$(f[\beta]_k)(\tau) = \det(\beta)^{k-1}(c\tau + d)^{-k} f(\beta(\tau)), \tau \in \mathcal{H}$$

Definition 9. *For Γ_1 and Γ_2, congruence subgroups, and $\alpha \in GL_2^+(\mathbb{Q})$, the **weight**-$k$ $\Gamma_1\alpha\Gamma_2$ operator takes functions $f \in \mathcal{M}_k(\Gamma_1)$ to*

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum_j f[\beta_j]_k$$

where $\{\beta_j\}$ are orbit representatives, i.e. $\Gamma_1\alpha\Gamma_2 = \cup\Gamma_1\beta_j$ is a disjoint union.

To see this definition is well defined we refere to [2, Section 5.1]. We list some special cases of the double coset operator:

- If $\Gamma_2 \subset \Gamma_1$ and $\alpha = \mathrm{Id}$, the double coset is the naturial inclusion of the subspace $\mathcal{M}_k(\Gamma_1)$ in $\mathcal{M}_k(\Gamma_2)$.

- If $\alpha^{-1}\Gamma_1\alpha = \Gamma_2$, the double coset operator is the natural translation, by α, from $\mathcal{M}_k(\Gamma_1)$ to $\mathcal{M}_k(\Gamma_2)$.

- If $\Gamma_1 \subset \Gamma_2$ and $\alpha = \mathrm{Id}$, the double coset operator is the natural trace mpa that project $\mathcal{M}_k(\Gamma_1)$ onto its subspace $\mathcal{M}_k(\Gamma_2)$.

The $\langle d \rangle$ and T_p operators

Consider the congruence subgroups

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

and

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

the kernel of the map $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^*$ sending

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d$$

is $\Gamma_1(N)$, i.e. $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$. Hence any $\alpha \in \Gamma_0(N)$ acts on $f \in \mathcal{M}_k(\Gamma_1(N))$ via the double coset operator:

$$f[\Gamma_1(N)\alpha\Gamma_1(N)]_k = f[\alpha]_k,$$

and since $f[\alpha]_k = f$ for every $\alpha \in \Gamma_1(N)$, so in fact $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^*$ acts on $\mathcal{M}_k(\Gamma_1(N))$.

Definition 10 (Diamond operator)**.** *The action of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, determined by d modulo N is denoted by $\langle d \rangle$, i.e.*

$$\langle d \rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$$

given by

$$\langle d\rangle f = f[\alpha]_k, \quad \textit{for any } \alpha = \begin{bmatrix} a & b \\ c & \delta \end{bmatrix} \in \Gamma_0(N) \textit{ with } d \equiv \delta \mod N$$

.

Definition 11. *For p a prime, we define the operator*

$$T_p : \mathcal{M}(\Gamma_1(N)) \to \mathcal{M}(\Gamma_1(N))$$

given by $f \mapsto f[\Gamma_1(N)\alpha\Gamma_1(N)]_k$ *for* $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$

We generalize the last two definition multiplicatively, i.e. we desire $\langle nm\rangle = \langle n\rangle\langle m\rangle$ and $T_{nm} = T_nT_m$ if n, m are two coprime integers.

There is a case the diamond operator is not defined, precisely when (n, N), we let $\langle n\rangle$ be the zero operator.

For the other operator, for a prime power p^r we define inductively

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

,

and for $n \geq 0$ we let

$$T_n := \prod T_{p_i^{r_i}} \qquad \text{where } n = \prod p_i^{r_i}.$$

2.2.3 Newforms and oldforms

Definition 12. *Let* $\Gamma \subset SL_2(\mathbb{Z})$ *be a congruence subgroup. The Petersson inner product,*

$$\langle\rangle_\Gamma : \mathbb{S}_k(\Gamma) \times \mathbb{S}_k(\Gamma) \to \mathbb{C}$$

is given by

$$\langle f, g\rangle_\Gamma = \frac{1}{V_\Gamma}\int_{X(\Gamma)} f(\tau)\overline{g(\tau)}(Im(\tau))^k d\mu(\tau)$$

Consider M, N to integers, if $M|N$ then $\mathcal{S}_k(\Gamma_1(M)) \subset \mathcal{S}_k(\Gamma_1(N))$, but there is another way to embed $\mathcal{S}_k(\Gamma_1(M))$ into $\mathcal{S}_k(\Gamma_1(N))$: consider d any factor of N/M and let

$$\alpha_d = \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix}$$

so that $(f[\alpha_d]_k)(\tau) = d^{k-1} f(d\tau)$ for $f : \mathcal{H} \to \mathbb{C}$. This is an injective linear map that takes $\mathcal{S}_k(\Gamma_1(M))$ to $\mathcal{S}_k(\Gamma_1(N))$.

This observation alongside Peterson's inner product allows us to define oldforms and newforms of level N. For a divisor d of N consider the map

$$i_d : (\mathcal{S}_k(\Gamma_1(Nd^{-1})))^2 \to \mathcal{S}_k(\Gamma_1(N))$$

given by $(f, g) \mapsto f + g[\alpha_d]_k$.

Definition 13. *The subspace of* ***oldforms at level N*** *is*

$$\mathcal{S}_k(\Gamma_1(N))^{old} = \sum_{p|n, p \ prime} i_p((\mathcal{S}_k(\Gamma_1(Np^{-1})))^2).$$

The subspace of ***newforms at level N*** *is*

$$\mathcal{S}_k(\Gamma_1(N))^{new} = (\mathcal{S}_k(\Gamma_1(N)))^{old})^{\perp}$$

Definition 14 (Hecke algebras)**.** *For $N > 0$ an integer and $S_2(N)$ the space of weight 2 cusp forms for $\Gamma_1(N)$ we let*

$$T'(N) := \mathbb{Z}[T_\ell, \langle d \rangle End(S_2(N))$$

2.2.4 Galois representations and newforms

Choose a prime $p \in \mathbb{Z}$ and $\mathfrak{p}$ a prime of $\overline{\mathbb{Q}}$ lying over p. For $f = \sum_{n \geq 1} a_n q^n$ a weight two normalized newform of conductor N and character ϵ denote by K_f the completion at $\mathfrak{p}$ of the numberfield generated by the values of ϵ and the fourier coefficients a_n, let $\mathcal{O}_f$ be the ring of integers in K_f.

We associate to f an odd two dimensional galois representaion $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_f)$ that satisfies: for all large enough prime ℓ, the representation ρ_f is unramified at ℓ and

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_\ell)) = a_\ell \quad \text{and} \quad \det(\rho_f(\mathrm{Frob}_\ell)) = \epsilon(\ell)\ell.$$

Motivated by this correspondance we have the definition

Definition 15 (Modularity of Galois representations)**.** *A Galois representation*

$$\rho : G_{\mathbb{Q}} \to GL_2(A)$$

over a coefficient ring A is modular of there exists an integer $N > 0$ and a homomorphism $\pi : T'(N) \to A$ such that ρ is unramified outside Np and for every prime $\ell \not| pN$ we have

$$Trace(\rho(Frob_\ell)) = \pi(T_\ell) \quad and \quad det(\rho(Frob_\ell)) = \pi(\langle \ell \rangle)\ell.$$

Theorem 3 (Ribet's Theorem)**.** *Let f be a weight two newform of conductor $N\ell$ where $\ell \not| N$ is aprime. Suppose $\bar{\rho}_f$ is absolutely irreducible and that one of the following is true:*

- *either $\bar{\rho}_f$ is unramified at ℓ*
- *or $\ell = p$ and $\bar{\rho}_f$ is flat at p.*

Then there is a weight to newform g of conductor N such that $\bar{\rho}_f \cong \bar{\rho}_g$

2.3 Elliptic curves

2.3.1 Basic notions

An elliptic curve defined over a field K is a pair (E, O), where E is a smooth projective curve of genus one and O is a point of E which is algo an algebraic variety. All elliptic curves can be embedded as a smooth cubic curve in $\mathbb{P}^2_K$ given by an equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.4}$$

moreover if the characteristic of K is different from 2 or 3, the last equation can be simplified in what is called **Weiestrass form**

$$E : y^2 = x^3 + Ax + B. \tag{2.5}$$

There are two important quantities, the discriminant and the j-invariant, they are, respectively,

$$\Delta = -16(4A^3 + 27B^2) \qquad j(E) = -1728\frac{64A^3}{\Delta} = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

The condition of non-singularity is equivalent to $\Delta \neq 0$. The importance of the j-invariant is given by the theorem

Theorem 4. *Let E and E' e elliptic curves defined over an algebraically closed field K. Then E is K-isomorphic to E' if and only if $j(E) = j(E')$.*

Their group structure, also called Group Law, can be described explicitly: if we emmbed E into $\mathbb{P}^2_K$ and fix $O := [0, 1, 0]$ (the point at infinity), then for two pints $P = (x, y)$ and $P' = (x', y')$ of E

$$x(P+P') = \left(\frac{y'-y}{x'-x}\right)^2 - x - x' \qquad \text{and} \qquad x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

the additive inverse of $P = (x, y)$ is $-P = (x, -y)$.

Repeated addition of a point P gives multiplication maps,

$$[m] : E \to E, \qquad [m]P = \begin{cases} [m]P = P + ... + P & \text{if } m > 0 \\ [m]P = O & \text{if } m = 0 \\ [m]P = -P - ... - P & \text{if } m < 0 \end{cases}$$

the kernel of these maps are the m-torsion points of E

$$E[m] = \{P \in E : [m]P = O\},$$

the union of all m-torsion point is called the torsion subgroup

$$E_{tors} = \bigcup_{m \geq 1} E[m] = \{P \in E : [m]P = O \text{ for some } m \geq 1\}$$

Theorem 5. *Let E/K be an elliptic curve.*

a) If char$(K) \neq 0$ or if char$(K) = p$ with $p \nmid m$, then

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

b) If char$(K) = p > 0$, then

$$E[p^n] \cong \mathbb{Z}/p^n\mathbb{Z} \text{ or } 0.$$

Remark 2. *Fix a prime ℓ, the multiplication maps $[\ell] : E[\ell^{n+1}] \to E[\ell^n]$, $P \mapsto [\ell]P$, are clearly well defined and they form an inverse system. The inverse limit is called the Tate module and denoted by*

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

If char$(K) \neq \ell$, then applying the previous proposition we get

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

Definition 16 (Galois representations attached to elliptic curves)**.** *Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$. Since the Galois group commutes with the ℓ-multiplication map then it also naturally on the tate module $T_\ell(E)$, so we obtain a representation attached to E and the prime ℓ*

$$\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_\ell).$$

And the residual representation is denoted by $\overline{\rho}_{E,\ell} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_\ell)$.

2.3.2 Elliptic curves over finite fields

Theorem 6 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an aaliptic curve define over the finite field of q elements. Then*

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

.

Definition 17. *The* ***zeta function of an elliptic curve*** *$E/\mathbb{F}_q$ is the formal series*

$$Z(E/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \cdot \frac{T^n}{n}\right)$$

Theorem 7. *The zeta function of E is a rational function of the form*

$$Z(E/\mathbb{F}_q, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

where a is the trace of the Frobenius map $E \to E$ given by $(x, y) \mapsto (x^q, y^q)$

Theorem 8. *Two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ are isogenous over $\mathbb{F}_q$ if and only if*

$$Z(E/\mathbb{F}_q, T) = Z(E'/\mathbb{F}_q, T)$$

2.3.3 Local fields

We will make some assumptions over the field K:

- K is a complete local field, and $v : K^\times \to \mathbb{Z}$ a normalized valuation.
- R the ring of integers, i.e. $x \in R$ iff $x = 0$ or $v(x) \geq 0$.
- The maximal ideal of R is $\mathfrak{p}$, so $x \in \mathfrak{p}$ iff $x = 0$ or $v(x) > 0$.
- The residue field $k = R/\mathfrak{p}$.

A minimal Weierstrass equation for an ellitpic curve E/K is a Weierstrass equation (2.4)

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

with $a_i \in R$ and $v(\Delta)$ minimized. If $\text{char}(K) \neq 2, 3$ then E always has an equation of the type

$$y^2 = x^3 + Ax + B$$

with $A, B \in R$.

We denote by $\tilde{E}$ the reduction of E modulo $\mathfrak{p}$, i.e. the curve defined over k by the equation

$$\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6,$$

again the tilde on the a_i's denotes the reduction modulo $\mathfrak{p}$. Regarding the singularity of E we say:

- E has good (or stable) reduction if $\tilde{E}$ is non-singular.
- E has multiplicative (or semistable) reduction of $\tilde{E}$ has a node, if the tangent directions are defined over k we say it is a split, otherwise non-split.
- E has additive (or unstable) reduction if $\tilde{E}$ has a cusp.

The term semistable is also used to say the reduction is good or mullti-plicative.

2.3.4 Number fields

Let K be a number field and E/K an elliptic curve. For each prime $\mathfrak{p}$ of K denote by $K_{\mathfrak{p}}$ the completion at $\mathfrak{p}$ and consider the elliptic curve E in the local feild $K_{\mathfrak{p}}$; consider a minimal Weiestrass form in the local fields $K_{\mathfrak{p}}$ and the discriminant of this minimal equation $\Delta_{\mathfrak{p}}$. The **minimal discriminant** of E/K is the integral ideal

$$D_{E/K} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\Delta_{\mathfrak{p}})}$$

Remark 3. *If the class nomber of K is one, like the case $K = \mathbb{Q}$, there exisits a Weiestrass equation which is simultaneously minimal at all primes of K, and also the discriminant $D_{E/K}$ of this equation equals the discrimiant Δ (as ideals).*

Also, define the conductor of E/L as the ideal

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

where the exponents $f_{\mathfrak{p}}(E/K)$ are given by

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

For each prime $\mathfrak{p}$ of K, let $q_{\mathfrak{p}}$ be the norm of $\mathfrak{p}$. If E has good reduction at
$mathfrakp$, we let

$$a_{\mathfrak{p}} = q_{\mathfrak{p}} + 1 - \#\tilde{E}(k_{\mathfrak{p}}).$$

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

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

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

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

Theorem 9. *Two elliptic curves E/K and E'/K are isogenous over K if and only if $a_{\mathfrak{p}}(E) = a_{\mathfrak{p}}(E')$ almost for every $\mathfrak{p}$, i.e. excluding a set of density zero, primes of K.*

Definition 18 (Modularity)**.** *An elliptic curve $E/\mathbb{K}$ is modular if there is a weight two newform of conductor N_E and trivial character for which*

$$L(f, s) = L(E/\mathbb{Q}, s)$$

Theorem 10 (Wile's theorem)**.** *Every semistable elliptic curve over $\mathbb{Q}$ is modular.*

2.3.5 The proof od Fermat's Last Theorem

We will give a sketch of Fermat's Last Theorem, in particular

Theorem 11. *If $p \geq 5$ is prime, and $a, b, c \in \mathbb{Z}$, then $a^p + b^p + c^p = 0$ implies $abc = 0$.*

Since the theorem is known to be true when the exponent is $3, 4$ and all the other cases can be reduced to a prime exponent bigger than 3.

We will asuume a, b, c are comprime, using elemntary arithmetic properties without loss of generality we also can assume $a \equiv -1 \mod 4$ and $2|b$. Let a^p, b^p, c^p be a non-trivial solution, i.e. $abc \neq 0$, define the elliptic curve

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

The idea is to use all the tools introduced before to show such elliptic curve cannot exist. First we list some properties about E_{a^p,b^p,c^p}: it is a semistable elliptic curve with minimal discriminant

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

and conductor

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

where ℓ runs over the prime numbers divding abc.

We will denote by ρ_{a^p,b^p,c^p} the Galois representation $\rho_{E,p}$ attached to E, the following theorem crucial theorem gives ifnormation about this representation.

Theorem 12. *Let $p \geq 5$ be a prime, $a, b, c \in \mathbb{Z}$ satisfying $a^p + b^p + c^p = 0$ and $abc \neq 0$. Assume also $a \equiv -1 \mod 4$ and $2|b$. Denote by $\bar{\rho}_{a^p,b^p,c^p} = \bar{\rho}_{E,p}$; then*

a) $\overline{\rho}_{a^p,b^p,c^p}$ is absolutely irreducible;

b) $\overline{\rho}_{a^p,b^p,c^p}$ is odd;

c) $\overline{\rho}_{a^p,b^p,c^p}$ is unramified outside $2p$, flat at p, and semistable at 2.

The last big ingredient is the Ribet's Theorem.

Theorem 13 (Ribet's Theorem)**.** *Let f be a weight two newform of conductor $N\ell$ where $\ell \nmid N$ is a prime. Suppose $\bar{\rho}_f$ is absolutely irreducible and that one of the following is true:*

- *$\bar{\rho}_f$ is unramified at ℓ; or*
- *$\ell = p$ and $\bar{\rho}_f$ is flat at p.*

Then there is a weight two newform g of conductor N such that $\bar{\rho}_f \cong \bar{\rho}_g$.

By Wile's Theorem the elliptic curve E_{a^p,b^p,c^p} is modular, so 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 $\rho_{a^p,b^p,c^p} \cong \rho_{f_{a^p,b^p,c^p}}$.

Theorem (12) allows us to apply Ribet's Theorem, since the conductor of E_{a^p,b^p,c^p} is of the form $2N$ (because $2|b$ and we chose a, b, c to be comprime), then Ribet's theorem guarantees a weight two newform g of conductor 2 such that $\bar{\rho}_g \cong \bar{\rho}_{a^p,b^p,c^p}$. Since the dimension of $S_2(\Gamma_0(2))$ is equal to the genus of $X_0(2)$, which is known to be zero, we arrive to a contradiction and prove Fermat's Last Theorem.

Chapter 3

Fermat's Last Theorem over totally real fields

3.1 Hillbert forms

Let K be a totally real number field of degree m over the rational field. There are exactly m embedding of K into the real line $\mathbb{R}$, this allows us to emmbed the general linear group $GL_2(K)$ into $GL_2(\mathbb{R})^m$. We say $\gamma \in GL_2^+(\mathcal{O}_K)$ if the corresponding element is in $GL_2^+(\mathbb{R})^m$.

The group $GL_2^+(\mathcal{O}_F)$ is called the full Hillbert modular group. And for every $z = (z_1, \ldots, z_m) \in \mathcal{H}^m$ there is a group action of $GL_2^+(\mathcal{O}_F)$ give by $\gamma \cdot z = (\sigma_1(\gamma)z_1, \ldots, \sigma_m(\gamma)z_m)$.

And for a matrix $\alpha := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(R)$ define

$$j(g, z) := \frac{cz + d}{\det g^{1/2}}.$$

A Hillbert modular form of weight $(k_1, \ldots, k_m)$ is an analytic functio on $\mathcal{H}^m$ such that for every $\gamma \in GL_2^+(\mathcal{O}_F)$

$$f(\gamma z) = \prod_{j=1}^{m} j(\sigma_i(\gamma), z_i)^{k_i} f(z).$$

Note, we dont need any additional assumption about the function on the cuspids. Due to Koecher's principle.

Just like with modular forms, we can now define what a congruence modular group of level N is. We can also define what it means to be a cusp form. Introduce analogue operator of Hecker operators, the Petersson inner product. And we can also talk about newforms and oldforms. For more details see [4].

3.2 Fermat's Last Theorem over totally real fields

3.2.1 Statement of the theorems

Let K denote a totally real field, we are interested in solutions of the equation, with $p \in \mathbb{N}$ a prime,

$$x^p + y^p + z^p = 0 \quad x, y, z \in K, \tag{3.1}$$

By **asymptotic Fermat's Last Theorem** we mean that there exists a constant B_K, depending only on K, such that the equation (3.1) has only trivial solution, i.e. $xyz = 0$ for all primes $p \geq B_K$; moreover, if the constant B_K is effectively computable we will say **effective asymptotic Fermat's Last Theorem**

The main theorem we will prove in this section needs some assumptions over the field K: consider the sets

$$\begin{gathered} S = \{\mathfrak{P} : \mathfrak{P} \text{ is a prime of } K \text{ above } 2\}, \\ T = \{\mathfrak{P} \in S : f(\mathfrak{P}/2) = 1\}, \qquad U = \{\mathfrak{P} \in S : 3 \nmid v_{\mathfrak{P}}(2)\}. \end{gathered} \tag{3.2}$$

By $f(\mathfrak{P}/2)$ we mean the residual degree of $\mathfrak{P}$. We will denote by **(ES)** the assumptions made over K

$$\textbf{(ES)} \begin{cases} \text{either } [K:\mathbb{Q}] \text{ is odd;} \\ \text{or } T \neq \emptyset; \\ \text{or Conjecture 1 holds for K.} \end{cases}$$

Conjecture 1. *Let K be a totally real field. Let $\mathfrak{f}$ be a Hillbert newform of level $\mathcal{N}$ and parallel weight 2 and rational eigenvalues. Then there is an elliptic curve $E_{\mathfrak{f}}/K$ with conductor $\mathcal{N}$ having the same L-function as $\mathfrak{f}$.*

The main theorem we will prove is the following:

Theorem 14. *Let K ba a totally real field satisfying **(ES)**. Let S, T, U be as in (3.2). Write $\mathcal{O}_S^*$ for the group of S-units of K. Suppose that for every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_S^*. \tag{3.3}$$

there is

(A) either some $\mathfrak{P} \in T$ that satisfied $\max |v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}(\mu)}| \leq 4v\mathfrak{P}(2)$

(B) or some $\mathfrak{P} \in U$ that satisfies both $\max |v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}(\mu)}| \leq 4v\mathfrak{P}(2)$*, and* $v_{\mathfrak{P}}(\lambda\mu) \equiv v_{\mathfrak{P}}(2) \mod 3$.

Remark 4. *Solutions of equation (3.3) satisfying $\lambda, \mu \in \mathbb{Q}$ have the form $\lambda = \pm 2^{r_1}$ and $\mu = \pm 2^{r_2}$, in particular, all such solutions are* $(2, -1), (-1, 2), (1/2, 1/2)$, *these will be called the irrelevant solutions.*

The second main theorem to be proven is when K is a real quadratic field, we will show the effective asymptotic Fermat's Last Theorem for 5/6 of real quadratic fields holds.

More formally, the set of square free integers $\mathbb{N}_{sf} = \{d \geq 2 : d \text{ is square free }\}$ is in bijection with quadratic real feidls via $d \mapsto K = \mathbb{Q}(\sqrt{d})$, so for a subset $\mathcal{U} \subset \mathbb{N}_{sf}$ define the relative density of $\mathcal{U}$ in $\mathbb{N}_{sf}$ as

$$\delta_{rel}(\mathcal{U}) = \lim_{X \to \infty} \frac{\#\{d \in \mathcal{U} : d \leq X\}}{\#\{d \in \mathbb{N}_{sf} : d \leq X\}},$$

if the limit exists. Let

$$\begin{aligned} &\mathcal{C} = \{d \in \mathbb{N}_{sf} : \text{ the } S - \text{unit has no relevant solution in } \mathbb{Q}(\sqrt{d})\} \\ &\mathcal{D} = \{d \in \mathbb{C} : d \not\equiv 5 \mod 8\} \end{aligned} \tag{3.4}$$

And we will give also a proof of the Theorem.

Theorem 15. *Let $\mathcal{C}$ and $\mathcal{D}$ be as above. Then*

$$\delta_{rel}(\mathcal{C}) = 1, \qquad \delta_{rel}(\mathcal{D}) = 5/6. \tag{3.5}$$

If $d \in \mathcal{D}$ then the effective asymptotic Fermat's Last Theorem holds for $K = \mathbb{Q}(\sqrt{d})$. Same conclusion holds for $d \in \mathcal{C}$ if we assume Conjecture 1.

We are following the paper [7] where these theorems and others are stated and proven.

3.2.2 The main theorem

Idea of the proof

For the proof of Theorem (14) we will deviate from proof given for the classic Fermat's Last Theorem. A quick summary, for $p \geq 5$ and for a solution $a^p + b^p + c^p = 0$ with $a, b, c \in \mathbb{Q}$, after clearing out denominators we can assume $a, b, c \in \mathbb{Z}$, if moreover we elimate all common factors we can aslo assume a, b, c are coprime with $a \equiv -1 \mod 4$ and $2|b$. To this solution we attached Frey's curve given by

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

The mod p representation $\bar{\rho}_{E,p}$ is absolutely irreducible, by Wile's is modular, i.e. it arises from a weight 2 neform of level 2, and using Ribet's Theorem we concluded no such newforms exist, giving a contradiction.

Our approach for Theorem (14): first show that a solution with $a, b, c, \in K$ implies another solution living in $\mathcal{O}_K$, coprimality cannot be assumed if the class number $\mathrm{CL}(K) > 1$. However, if we fix some finite set $\mathcal{H}$ of primes of K we can ensure the solution $a, b, c \in \mathcal{O}_K$ are coprime away from $\mathcal{H}$. We will consider the same Frey curve, which will be semistable outside $S \cup \mathcal{H}$. We will apply a theorem like Ribet's Theorem, that will play the role as a level lowering (so a theorem for modularity will also be required), to $\bar{\rho}_{E,p}$ which will yield a Hilbert newform $\mathfrak{f}$ of parallel weight 2 and level disible only by the primes in $S \cup \mathcal{H}$. But such newforms may exists unlike the proof of Fermat's Last Theorem, where no newform of weight 2 and level 2 exists.

But considereing p sufficiently large we then find an elliptic curve E' with full 2-torsion and good reduction outside $S \cup \mathcal{H}$ and $\bar{\rho}_{E,p} \cong \bar{\rho}_{E',p}$, assumptions **(ES)** will be crucial in this part. We will need to study the action of Inertia groups $I_{\mathfrak{q}}$ for $q \notin S$ of the Frey curve E and finally conclude that E' has potentially good reduction away from S (we somehow eliminate the primes coming from the class group). We will relate the elliptic curve E' with the S-unit equation to prove Theorem (14)

Notation and conventions

We reserve p for exponent of the Fermat Equation, and will always denote a rational prime. Let K denote a totally real field and its integral ring by

$\mathcal{O}_K$. The class ideal $\mathfrak{a}$ of $\mathcal{O}_K$ will be denoted by $[\mathfrak{a}]$, and for three elements $a, b, c \in K$ we denote by

$$\mathcal{G}_{a,b,c} := a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K.$$

And by $[a, b, c]$ the class of $\mathcal{G}_{a,b,c}$ in the class of K.

Since every ideal class contains infinitely many prime ideal, then for ideal class $\mathfrak{c}_1, \ldots, \mathfrak{c}_h$ we can select representations $\Updownarrow_i$ such that $\mathfrak{m}_i \nmid 2$. We denote by $\mathcal{H}$ the set of our election of representatives.

Modularity

Just as we expressed before we need some results to prove the Frey curve is modular for p large enough. The following theorem from [8] lets us prove the claim.

Theorem 16. *Let K be a totally real field. Up to isomprhism over $\overline{K}$, there are at most finitely many non-modular elliptic curves E over K. Moreover, if K is real quadratic, then all elliptic curves over K are modular.*

Corollary 1. *Let K be a totally real field. There is some constant A_K depending only on K, such that for any non-trivial solution (a, b, c) of the Fermat equation with prime exponent $p > A_K$, the Frey curve E_{a^p,b^p,c^p} given by*

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

is modular.

Proof. The j-invariant of E_{a^p,b^p,c^p} is

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

where $\lambda := -\frac{b^p}{a^p}$. By Theorem (16) there are finitely many non-modular elliptic curves, up to isomorphism over $\overline{K}$, so denote by $j_1, \ldots, j_n \in K$ the different j-invariants of the classes of these non-modular elliptic curves.

Hence there are $\lambda_1, \ldots, \lambda_m \in K$, with $m \leq 6n$, such that $\lambda \neq \lambda_k$ for all $1 \leq k \leq m$ that implies E_{a^p,b^p,c^p} is modular. In the case $\lambda = \lambda_k$ for some k, then

$$\lambda_k = -(b/a)^p \quad 1 - \lambda_k = -(c/a)^p. \tag{3.6}$$

For the sake of contradiction assume there is no such constant, hence there are infinite primes such that equation (3.6) holds for some k. Since

k is bounded by m, there must some k for which (3.6) is true for infinite primes. If λ is not a root of unit, then K infinately many roots of λ_k hence it is not finite; on the other hand, since λ_k cannont be a root of unity since K is real. □

Irreducibility of mod p representations of elliptic curves

The following Theorem from [9] will be used to prove that $\bar{\rho}_{E,p}$ is irreducible, where E denotes the Frey Curve for a solution to Fermat's equation.

Theorem 17. *Let K be a Galois totally real field. There is an effective constant C_K, depending only on K, such that the following holds. If $p > C_K$ is prime, and E/K is an elliptic curve which is semistable at all $\mathfrak{q}|p$, then $\bar{\rho}_{E,p}$ is irreducible.*

Level Lowering

The following theorem is used as the Ribet step, for a proof see [7, Theorem 7].

Theorem 18 (Level Lowering)**.** *Let K be a totally real field, and E/K and elliptic curve of conductor $\mathcal{N}$. Let p be a rational prime. For a prime ideal $\mathfrak{q}$ of K denote by $\Delta_\mathfrak{q}$ the discriminant of a local minimal model for E at $\mathfrak{q}$. Let*

$$\mathcal{M}_p := \prod_{\mathfrak{q}||\mathcal{N}, p|v_\mathfrak{q}(\Delta_\mathfrak{q})} \mathfrak{q} \qquad \mathcal{N}_p := \frac{\mathcal{N}}{\mathcal{M}_p} \tag{3.7}$$

Suppose the following

(i) $p \geq 5$, the ramification index $e(\mathfrak{q}/p) < p-1$ for all $\mathfrak{q}|p$, and $\mathbb{Q}(\xi_p)^+ \not\subset K$.

(ii) E is modular

(iii) $r\bar{h}o_{E,p}$ is irreducible,

(iv) E is semistable at all $\mathfrak{q}|p$

(v) $p|v_\mathfrak{q}(\Delta_\mathfrak{q})$ for all $\mathfrak{q}|p$

Then, there is a Hillbert eigenform $\mathfrak{f}$ of parallel weight 2 that is new at level $\mathcal{N}_p$ and some prime $\bar{\omega}$ of $\mathbb{Q}_\mathfrak{f}$ such that $\bar{\omega}|p$ and $\bar{\rho}_{E,p} \equiv \bar{\rho}_{\mathfrak{f},\bar{\omega}}$.

Eichler-Shimura

The following theorem gives a partial answer to Conjecture (1)

Theorem 19 (Blasisu, Hida)**.** *Let K be a totally real field and let $\mathfrak{f}$ be a Hillbert newform of level $\mathcal{N}$ and parallel weight 2, such that $\mathbb{Q}_f = \mathbb{Q}$. Suppose that*

(a) either $[K : \mathbb{Q}]$ is odd,

(b) or there is a finite prime $\mathfrak{q}$ such that $\pi_{\mathfrak{q}}$ belongs to the discrete series, where π is the cuspidal automorphic representation of $GL_2(\mathbb{A}_K)$ attached to $\mathfrak{f}$.

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

And from this theorem we can prove the following corollary, for a proof see [7, Corollary 2.2, page 8]

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

(a) E has potentially multiplicative reduction at $\shortparallel$

(b) $p | \# \bar{\rho}_{E,p}(I_{\mathfrak{q}})$;

(c) $p \nmid (Norm_{K/\mathbb{Q}})(\mathfrak{q} \pm 1)$.

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

Frey curve

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

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

The invariants c_4, c_6, Δ, j are given by

$$c_4 = 16(u^2 - vw) = 16(v^2 - wu) = 16(w^2 - uv), \qquad (3.8)$$

$$c_6 = -32(u - v)(v - w)(w - u), \quad \Delta = 16u^2v^2w^2, \quad j = c_4^3/\Delta \qquad (3.9)$$

Lemma 3. *With the above notation, let $\mathfrak{q} \nmid 2$ be a prime and let*

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

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

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

$$v_{\mathfrak{q}}(u) = v_{\mathfrak{q}}(u) = v_{\mathfrak{q}}(w) \tag{3.10}$$

(ii) E_{min} has multiplicative reduction at $\mathfrak{q}$ if and only if s is even and the above condition (3.10) fails. In this case the minimal discriminant $\Delta_{\mathfrak{q}}$ at $\mathfrak{q}$ 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.

Lemma 4. *Let (a, b, c) be a non-trivial solution to Fermat's Equation (3.1). There is a non-trivial integral solution (a', b', c') such that the following holds*

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

(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 $[\mathcal{G}_{a,b,c}] = [\mathfrak{m}]$, so $[\mathfrak{m}] = (\xi) \cdot \mathcal{G}_{a,b,c}$ for some $\xi \in K^*$. Define a', b', c' as in (i). By definition $(a') = (\xi) \cdot (a) = \mathfrak{m} \cdot (\mathcal{G}_{a,b,c}(a))$ which is an integral ideal (since $\mathcal{G}_{a,b,c}$ devides (a)). Thus a' is in $\mathcal{O}_K$, applying the same reasoning to b and c we get $a', b', c' \in \mathcal{O}_K$.

Since

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

This proves (ii) and (iii). □

Lemma 5. *Let (a, b, c) be a non-trivial solution to the Fermat equation* (1) *with prime exponent p satisfying $\mathcal{G}_{a,b,c} = \mathfrak{m}$, where $\mathfrak{m} \in \mathcal{H}$. Write E for the Frey cure associated to the solution, and let Δ be its discriminant. Then at all $\mathfrak{q} \notin S \cup \mathfrak{m}$, the model E is minimal, semistable and satisfies $p | v_{\mathfrak{q}}(\Delta)$. Let $\mathcal{N}$ be the conductor of E, and let $\mathcal{N}_p$ be defined as before. Then*

$$\mathcal{N} = \mathfrak{m}^{s_{\mathfrak{m}}} \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r_{\mathfrak{P}}} \cdot \prod_{\mathfrak{q} | abc, \mathfrak{q} \notin S \cup \{\mathfrak{m}\}} \mathfrak{q}, \qquad \mathcal{N}_p = \mathfrak{m}^{s'_{\mathfrak{m}}} \cdot \prod_{\mathfrak{P} \in S} \mathfrak{P}^{r'_{\mathfrak{P}}}, \tag{3.11}$$

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

For the proof of this Lemma we are going to need two facts about the conductor of elliptic curves from the book Advanced Topics in the Arithmetic of Elliptic Curves. From [6, Theorem 10.4].

Theorem 20 (Lockhart-Rosen-Silverman, Brumer-Kramer)**.** *Ler $K/\mathbb{Q}_P$ be a local field with normalized valuation v_K, and let E/K be an elliptic curve. Then the expoenent of the counductor of E/K is bounded by*

$$f(E/K) \leq 2 + 3v_K(3) + 6v_K(2)$$

From [6, Theorem IV.10.2] if characteristic of the residue field of K is bigger than 3 then the exponent of the wild part is zero.

Proof. Let $\mathfrak{q}$ denote a prime of K not in S and different from $\mathfrak{m}$. If $\mathfrak{q}|abc$ then q devides only on of a, b, c, and by the expression of the invariant c_4 we see $q \nmid c_4$, i.e. the model

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

is minimal and has multiplicative reduction at $\mathfrak{q}$, and $p|v_{\mathfrak{q}}(\Delta)$. And so $q \nmid \mathcal{N}_p$.

For $\mathfrak{P} \in S$ we have the bound $r_{\mathfrak{P}} = 2 + 6v_{\mathfrak{P}}(2)$. So $r'_{\mathfrak{P}} = r_{\mathfrak{P}}$ unless E has good reduction at $\mathfrak{P}$ and $p|v_{\mathfrak{P}}(\Delta_{\mathfrak{P}})$ but in thise case $r_{\mathfrak{P}} = 1$ and $r'_{\mathfrak{P}} = 0$.

Since we choose $\mathfrak{m}$ so $m \nmid 2$ and E has full 2-torsion over K we see $\mathfrak{m}$ vanishes from the conductor. End $s_{\mathfrak{m}} = s'_{\mathfrak{m}}$ unless E has multplicative reduction at $\mathfrak{m}$ and $p|v_{\mathfrak{m}}(\Delta_{\mathfrak{m}})$ in which case $s_{\mathfrak{m}} = 0$ and so $s'_{\mathfrak{m}} = 0$. □

Images of inertia

Lemma 6. *Let E be an elliptic curve over K with j-invariant j. Let $p \geq 5$ and $\mathfrak{q} \nmid p$ be a prime of K. Then $p|\#\bar{\rho}_{E,p}(I_{\mathfrak{q}})$ if and only if E has potentially multiplicative reduction at $\mathfrak{q}$ (i.e. $v_{\mathfrak{q}}(j) < 0$ and $p \nmid v_{\mathfrak{q}}(j)$).*

Idea of the proof. Due to Krauss [11, Introduction] we know that if E has good reduction at $\mathfrak{q}$ then $\#\bar{\rho}_{E,p}|24$. For E with potentially multiplicative reduction the result if a consequence of the Tate curve theory [6, Proposition V.6.1]. □

Lemma 7. *Let $q \notin S$. Let $(a, b, c,)$ be a solution to the Fermat equation with prime exponent $p \geq 5$ such that $\mathfrak{q} \nmid p$. Let $E = E_{a,b,c}$ be the Frey curve. Then $p \nmid \#\bar{\rho}_{E,p}(I_{\mathfrak{q}})$.*

Proof. The proof uses the above lemma, also recall

$$c_4 = 16(u^2 - vw) = 16(v^2 - wu) = 16(w^2 - uv),$$
$$c_6 = -32(u-v)(v-w)(w-u), \quad \Delta = 16u^2v^2w^2, \quad j = c_4^3/\Delta.$$

If $v_\mathfrak{p}(a) = v_\mathfrak{p}(b) = v_\mathfrak{p}(c)$ then $v_\mathfrak{p}(j) < 0$ and clearly $p|v_\mathfrak{q}(j)$, so result follows from Lemma (7).

In the othcer case, the valuations at ıı ae not equal then $v_\mathfrak{q}(j) \geq 0$ and Lemma (7) still applies. □

Lemma 8. *Let E be an elliptic curve over K, and let $p \geq 3$. Let $\mathfrak{P} \in S$ and suppose E has potentially good reduction at $\mathfrak{P}$. Let Δ be the discriminant of E (not necessarily minimal at $\mathfrak{P}$). Then $3|\rho_{E,p}(I_\mathfrak{P})$ if and only if $3 \nmid v_\mathfrak{P}(\Delta)$.*

For the proof we will be using Proposition [**?**, Proposition IV.10.3],specifically we will be using the fact that for a local field K of residue field p and en elliptic curve E/K with integral j-invariant and for an integer m relatively prime to p, the elliptic curve E has good reduction over $K(E[m])$. Also we will use a result from Kraus [11, Théorème 3]

Proof. First assume $3 \nmid v_\mathfrak{P}(\Delta)$, and let L be the maximal unramiefied estension of $K_\mathfrak{P}$. By the stated proposition we know E has good reduction over $L(E[p])$, it follows the valuation is of Δ in $L(E[p])$ is divisble by 12, so $3|[L(E[p]) : L]$, and since the Galois group of $L(E[p])/L$ is isomorphic to $\bar{\rho}_{E,\rho}(I_\mathfrak{P})$ and we conclude $3|\#\bar{\rho}_{E,p}(I_\mathfrak{P})$.

The other implication follows from Kraus, where he en lists all possibilities for the Galois group of $L(E[p])/L$. In the case $3|v_\mathfrak{P}(\Delta)$ its order is $1, 2, 4$ or 8. □

Lemma 9. *Let $\mathfrak{P} \in S$. Let (a, b, c) be a solution to the Fermat equation with prime exponent $p \geq 4v_\mathfrak{P}(2)$. Let $E = E_{a^p,b^p,c^p}$ be the Frey curve, if:*

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

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

Proof. Let π denota a uniformizer for $K_{\mathfrak{P}}$, and set

$$\alpha = \pi^{-t}a, \quad \pi^{-t}b, \quad \gamma = \pi^{-t}c$$

where $t = \min\{v_{\mathfrak{P}}(a), v_{\mathfrak{P}}(b), v_{\mathfrak{P}}(c)\}$. Clearly $\alpha, \beta, \gamma \in \mathcal{O}_{\pi}$.

If the prime $\mathfrak{P} \in T$, then it's residue field is $\mathbb{F}_2$. From the equality $a^p + b^p + c^p = 0$ it follows $\alpha^p + \beta^p + \gamma^p = 0$, so there is only one of α, β, γ who is divisible by π, in other word two out of a, b, c have valuation t and the other $t + k$ with $k \geq 1$. From (3.8) we know

$$v_{\mathfrak{P}}(j) = 8v_{\mathfrak{P}}(2) - 2kp.$$

By hypothesies $p > 4v_{\mathfrak{P}}(2)$, so we conclude $v_{\mathfrak{P}}(j) < 0$ and $p \nmid v_{\mathfrak{P}}(j)$. Now (ii) follows from Lemma (6).

In the case $\mathfrak{P} \in U$. If the valuations $v_{\mathfrak{P}}(a), v_{\mathfrak{P}}(b), \mathfrak{P}(c)$ are not equal we apply the same reasoning as before. So assume all the valuations are equal, again using (3.8) we conclude

$$v_{\mathfrak{P}}(j) \geq 8v_{\mathfrak{P}}(2) > 0 \quad \text{and} \quad v_{\mathfrak{P}}(\Delta) = 4v_{\mathfrak{P}}(2) + 6tp.$$

Hence E has potentially good reducton. Since $\mathfrak{P} \in U$ we know $3 \mid v_{\mathfrak{P}}(2)$, and (ii) follows from Lemma (8). □

Level Lowering and Eichler-Shimura

Theorem 21. *Let K be a totally real field satisfying **(ES)**. There is a constant B_K depending only on K such that the following hold. Let (a, b, c) be a non-trivial to the Fermat equation with prime exponent $p \geq B_K$, and rescale $(a, b, c,)$ so that it remains integral and satisfies $\mathcal{G}_{a,b,c} = \mathfrak{m}$ for some $\mathfrak{m} \in \mathcal{H}$. Write E for the Frey curve. Then there is an Elliptic curve E' over K such that*

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

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

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

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

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

(*b*) *for* $\mathfrak{P} \in U$*, we have either* $v_{\mathfrak{P}}(j') < 0$ *or* $3 \nmid v_{\mathfrak{P}}(j')$*;*

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

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

Proof. By observing the conductor of E which we computed in Lemma (5) we conclude the elliptic curve E is semistable outside $S \cup \{\mathfrak{m}\}$. By using Corollary (1) we know that if B_K is large enough then E is modular. And by Theorem (17) the residual representation $\bar{\rho}_{E,p}$ is irreducible. Applying Level Lowering (Theorem (18)) and Lemma (5) we conclude $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\bar{\omega}}$ for a Hilbert newform $\mathfrak{f}$ of level $\mathcal{N}_p$ and some prime $\bar{\omega}|p$ of $\mathbb{Q}_{\mathfrak{f}}$ (the field generated by the Hecke eigenvalues of $\mathfrak{f}$).

Next we reduce to the case where $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$ by using Proposition (2)(1) but for Hillbert modular forms. If $\mathfrak{f}$ is not rational than there are infinitely many ℓ for which $B_\ell(\mathfrak{f}) \neq 0$ and so $p|B_\ell(f)$, hence we way enlarge B_K to assume $\mathfrak{f}$ is rational.

To show there is an elliptic curve E'/K having the same L-functions as $\mathfrak{f}$ and conductor $\mathcal{N}_p$ we make use of the assumption **(ES)**. If Conjecture 1 holds, it is trivial. And if $[K : \mathbb{Q}]$ is odd it follows from Theorem (19). And if $T \neq \emptyset$, then let $\mathfrak{P} \in T$ and apply Lemma (9) to conclude E has potentially multiplicative reduction at $\mathfrak{P}$ and $p|\#\bar{\rho}_{E,p}(I_{\mathfrak{P}})$, in this case the existence of E' is guaranteed by Corollary (2) after enlarging B_K.

If $\mathfrak{f}$ is rational but not isogenous to any another curve which corresponds to $\mathfrak{f}$ with full 2-torsion then by Proposition (2) there are infinitely many ℓ such that $B_\ell \neq 0$. So again, we may enlarge B_K to assume the form $\mathfrak{f}$ corresponds to a rational elliptic curve E' with full 2-torsion.

Since there are finitely many elliptic curves E' with full 2-torsion and good reduction outside $S \cup \{\mathfrak{m}\}$, we can enlarge B_K so that for all primes $\mathfrak{q}$, if $v_{\mathfrak{q}}(j') < 0$ then $p \nmid \#\bar{\rho}(E', p)(I_{\mathfrak{q}})$ and after applying Lemma (6) we conclude $v_{\mathfrak{q}}(j') \geq 0$, procing ($c$).

To prove (a), for $\mathfrak{P} \in U$ applyin Lemma (9) we have $p|\#\bar{\rho}_{E,p}(I_{\mathfrak{P}})$ and so $p\#\bar{\rho}_{E',p}(I_{\mathfrak{P}})$. And by Lemma (6) we have $v_{\mathfrak{P}}(j') < 0$.

For (b) let $\mathfrak{P} \in U$. If $p|\#\bar{\rho}_{E,p}$ then again $v_{\mathfrak{P}}j') < 0$. So suppose $p \nmid \bar{\rho}_{E',p}(I_{\mathfrak{P}})$ and $3|\bar{\rho}_{E',p}(I_{\mathfrak{P}})$. Using Lemma (6) we have $v_{\mathfrak{q}}(j') \geq 0$. And by Lemma (8) we have $3 \nmid v_{\mathfrak{P}}(\Delta')$, so $j' = (c_4')^3/\Delta'$ and $3 \nmid v_{\mathfrak{P}}(j')$.1

□

Proof of the main Theorem

Proof. Let K be a totally real field satisfying **(ES)**. Let B_K the constant given by theorem (21). For a prime $p > B_K$ consider the Fermat equation

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

If $a, b, c \in K$ is a non-trivial solution, i.e. $abc \neq 0$, we can rescale in such a way $a, b, c \in \mathcal{O}_K$ are integral integers and $\mathcal{G}_{a,b,c} = \mathfrak{m} \in \mathcal{H}$. As always, denote by $E := E_{a^p,b^p,c^p}$ the Frey Curve, after applying theorem (21) we obtain another elliptic curve E'/K with potentially good reduction outside S with full 2-torsion over K, so it has a model

$$E' : y^2 = (x - e_1)(x - e_2)(x - e_3), \qquad e_i \neq e_j \text{ for } 1 \leq i < j \leq 3 \tag{3.12}$$

Denote the **cross ratio** by $\lambda := \frac{e_3 - e_1}{e_2 - e_1}$ and S_3 the symmetric group of a set of three elements. The action of S_3 on $\{e_1, e_2, e_3\}$ extends to $\mathbb{P}^1_K$ via the action on the cross ratio λ; this action can be identify with the subset of $\mathrm{PGL}_2(K)$

$$\left\{ z, \frac{1}{z}, 1 - z, \frac{1}{1-z}, \frac{z}{z-1}, \frac{z-1}{z} \right\}.$$

The λ-invariants of E' are S_3-orbit of λ, they relate to the j'-invariant by

$$j' = 2^8 \cdot (\lambda^2 - \lambda + 1)^3 \cdot \lambda^{-2}(\lambda - 1)^2. \tag{3.13}$$

Also, by Theorem (21) we know the j-invariant of E' satisfies

a) for all $\mathfrak{P} \in T$: $v_{\mathbb{P}}(j') < 0$;

b) for all $\mathfrak{P} \in U$: $v_{\mathbb{P}}(j') < 0$ or $3 \nmid v_{\mathbb{P}}(j')$.

Note $j' \in \mathcal{O}_S$, since E' has potentially good reduction outside S. So by equation (3.13) we conclude $\lambda \in \mathcal{O}_S$ because it satisfies a polynomy of degree 6 with coefficients in $\mathcal{O}_S$. However $\mu := 1 - \lambda$ is also a solution to (3.13), and by the same reasoning $mu \in \mathcal{O}_S$ and so (λ, μ) is a solution to the S-unit equation. By our hypothesis on the field, it must satisfy

(A) either some $\mathfrak{P} \in T$ that satisfied $\max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}(\mu)}|\} \leq 4v\mathfrak{P}(2)$

(B) or some $\mathfrak{P} \in U$ that satisfies both $\max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}(\mu)}|\} \leq 4v\mathfrak{P}(2)$, and $v_{\mathfrak{P}}(\lambda\mu) \equiv v_{\mathfrak{P}}(2) \mod 3$.

Rewrite (3.13) as

$$j' = 2^8 \cdot (1-\lambda\mu)^3(\lambda\mu)^{-2}. \tag{3.14}$$

and let $t := \max\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\}$, and we resign by contradiction.

If it satisfies (A): For some $\mathfrak{P} \in T$ such that $t \leq 4v_{\mathfrak{P}}(2)$, if $t = 0$ then $v_{\mathfrak{P}}(j') \geq 8v_{\mathfrak{P}}(2) > 0$ which contradicts a). In the case $t > 0$, the relation $\lambda + \mu = 1$ forces three conditions, either $v_{\mathfrak{P}}(\lambda) = v_{\mathfrak{P}}(\mu) = -t$ or $v_{\mathfrak{P}}(\lambda) = 0$ and $v_{\mathfrak{P}}(\mu) = t$ or $v_{\mathfrak{P}}(\lambda) = t$ and $v_{\mathfrak{P}}(\mu) = 0$. Thus $v_{\mathfrak{P}}(\lambda\mu) = -2t \leq 0$ or $v_{\mathfrak{P}}(\lambda\mu) = t > 0$. We compute

$$v_{\mathfrak{P}}(j') = 8v_{\mathfrak{P}}(2) + 3v_{\mathfrak{P}}(1-\lambda\mu) - 2t \leq 8v_{\mathfrak{P}}(2)2 - 2t$$

hence $v_{\mathfrak{P}}(j') \geq 0$ which contradicts (a).

If it satisfies (B): There is some $\mathfrak{P} \in U$ s.t. $t \leq v_{\mathfrak{P}}(2)$ and $v_{\mathfrak{P}}(\lambda\mu) \equiv v_{\mathfrak{P}}(2) \mod 3$. By the same reasoning as in case (A) we conclude $v_{\mathfrak{P}}(j') \geq 0$, and a computation

$$v_{j'} = 8v_{\mathfrak{P}}(2) + 3v_{\mathfrak{P}}(1-\lambda\mu) - 2v_{\mathfrak{P}}(\lambda\mu),$$

since $8 \equiv 2 \mod 3$ using the last condition gives $3|v_{\mathfrak{P}}(j')$ □

3.2.3 Fermat's Last Theorem for fice sixths of Real Quadratic Fields

Recall the set of square free integers $\mathbb{N}_{sf} = \{d \geq 2 : d \text{ is square free }\}$ is in bijection with quadratic real feidls via $d \mapsto K = \mathbb{Q}(\sqrt{d})$, so for a subset $\mathcal{U} \subset \mathbb{N}_{sf}$ define the relative density of $\mathcal{U}$ in $\mathbb{N}_{sf}$ as

$$\delta_{rel}(\mathcal{U}) = \lim_{X\to\infty} \frac{\#\{d \in \mathcal{U} : d \leq X\}}{\#\{d \in \mathbb{N}_{sf} : d \leq X\}},$$

if the limit exists. And the absolute density

$$\delta(\mathcal{U}) = \lim_{X\to\infty} \frac{\#U(X)}{X}$$

Let

$$\begin{aligned} &\mathcal{C} = \{d \in \mathbb{N}_{sf} : \text{ the } S-\text{unit has no relevant solution in } \mathbb{Q}(\sqrt{d})\} \\ &\mathcal{D} = \{d \in \mathbb{C} : d \not\equiv 5 \mod 8\} \end{aligned} \tag{3.15}$$

Our goal is to prove:

Theorem 22. *Let $\mathcal{C}$ and $\mathcal{D}$ be as above. Then*

$$\delta_{rel}(\mathcal{C}) = 1, \qquad \delta_{rel}(\mathcal{D}) = 5/6. \tag{3.16}$$

If $d \in \mathcal{D}$ then the effective asymptotic Fermat's Last Theorem holds for $K = \mathbb{Q}(\sqrt{d})$. Same conclusion holds for $d \in \mathcal{C}$ if we assume Conjecture 1.

We will be using some theorem.

Theorem 23. *(see [12, page 636]) For integers r, N with N positive, let*

$$\mathbb{N}^{sf}_{r,N} = \{d \in \mathbb{N}^{sf} : d \equiv r \mod N\}.$$

Let $s = \gcd(r, N)$ and suppose that s is a squarefree. Then

$$\#\mathbb{N}^{sf}_{r,N}(X) \sim \frac{\varphi(N)}{s\varphi(N/s)\prod_{q|N}(1-q^{-2})} \cdot \frac{6}{\pi^2}X.$$

Lemma 10. *(see [7, Lemma 7.1, page 17]) Let $\mathcal{C}' = \mathbb{N}^{sf} \setminus \mathcal{C}$. Then $\delta(\mathcal{C}') = 0$.*

Proof of Theorem 22. We first show that the relative density of $\mathbb{C}$ is 1. Theorem (23) applied to $\mathbb{N}^{s,f}_{0,1} = \mathbb{N}^{sf}$ gives

$$\#\mathbb{N}^{sf} \sim \frac{6}{\pi^2}X,$$

so the relative and absolute quantity are related by

$$\delta_{rel}(\mathcal{U}) = \frac{\pi^2}{6}\delta(\mathcal{U}).$$

Applying Lemma (10) gives $\delta_{rel}(\mathcal{C}') = 0$ hence $\delta_{rel}(\mathcal{C}) = 1$.

Since any real quadratic field $\mathbb{Q}(\sqrt{d})$, for $d \in \mathcal{D}$, satisfies $T \neq 0$, i.e. assumptuon **(ES)** we need to prove only $\delta_{\mathcal{D}} = 5/6$. We apply Theorem (23) to obtain to $\mathbb{N}^{sf} \setminus \mathcal{D} = \mathbb{N}^{sf}_{5,8}$

$$\delta(\mathbb{N}^{sf}_{5,8}) = \frac{1}{8(1-2^{-2})}\frac{6}{\pi^2} = \frac{1}{\pi^2}$$

so $\delta_{rel}(\mathcal{D}) = \frac{5}{6}$. □

Appendix A

Serre-Mazur-Kraus equation

We consider the Diophantine equation, we will call it the Serre-Mazur-Kraus equation or SMK for short,

$$x^p + L^r y^p + z^p = 0 \tag{A.1}$$

for a fixed odd prime number L and $p \geq 5$ a prime number. Notice, we can assume $r < p$.

Let A, B, C be a permutation of $x^p, L^r y^p$ and z^p such that $B \equiv 0 \mod 2$ and $A \equiv -1 \mod 4$, and consider the Frey curve

$$E : Y^2 = X(X - A)(X + B). \tag{A.2}$$

We want to prove the following theorem

Theorem 24. *Let L be an odd prime that is neither a Mersenne nor a Fermat prime. There exists a constant C_L such that for any nontrivial solution (x, y, z, p) to the SMK equation we have $p \leq C_L$.*

We will attack to a solution an Elliptic curve, study it's conductor. We will use modularity and and Ribet's theorem in hope to get some contradiction. But instead of newforms of level 2 we will end up with newforms of level $2L$, we wil still be able to get a contradiction using some new tools if L is not a Mersenne or Fermat equation and p is large enough.

The minimal discriminant is given by

$$\Delta_{\text{min}} = 2^{-8} L^{2r} (xyz)^{2p}$$

and the conductor is

$$N = \prod_{q|Lxyz,\ q \text{ prime}} q.$$

Also, since L is an odd prime we see $v_L(\Delta_{\min}) \equiv 2r \not\equiv \mod p$ given $0 < r < p$, and $v_2(\Delta_{\min}) \equiv -8 \not\equiv 0 \mod p$. Those mod p, we have $L_p = 2L$. Applying Ribet's Theorem we deduce E arises modulo p frpm some newform f of level $2L$.

Lemma 11. *Assume F that F is an Elliptic curve defined over $\mathbb{Q}$ with conductor $2L$, and assume that F full 2-torsion. Then L is either a Mersenne or a Fermat prime.*

For the proof of Theorem (24) we need the following results

Propositon 1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let t be an integer such that $t||E_t(\mathbb{Q})|$ (the torsion subgroup of $E(\mathbb{Q})$). Let f be a newform of level N' with fourier coefficients c_n, let K be the totally real number field that they generate, and let ℓ be a prime number such that $\ell^2 \nmid N^2$ and $\ell \nmid N'$. Finally define*

$$S_\ell = \left\{ a \in \mathbb{Z} : -2\ell^{1/2} \le a \le 2\ell^{1/2} \text{ and } a \equiv \ell + 1 \mod t \right\},$$

$$B'_\ell(f) = \mathcal{N}_{K/\mathbb{Q}}((\ell+1)^2 - c_\ell^2) \prod_{a \in S_\ell} \mathcal{N}_{K/\mathbb{Q}}(a - c_\ell),$$

$$B_\ell = \begin{cases} \ell B'_\ell(f) & \text{if } f \text{ is not rational,} \\ B'_\ell & \text{if } f \text{ is rational} \end{cases}$$

Propositon 2. *In each of the following cases there are infinitely many ℓ for which $B_\ell(f) \neq 0$:*

1. *When f is irrational*
2. *When f is rational, t is either a prime number or is equal to 4, and for every elliptic curve isonenous to the elliptic curve corresponding to f we have $t \nmid |F_t(\mathbb{Q})|$.*
3. *If f is rational and $t = 4$ and if for every elliptic curve F isogenous to the elliptic curve corresponding to f then $F(\mathbb{Q})$ does not have full 2-torsion.*

Proof of Theorem (24). Using Ribet's theorem we found $E \sim_p f$ for a newform at level $N_p = 2L$.

If f is irrational then by Proposition (2) (1) there are infinitely many ℓ for which $B_\ell(f) \neq 0$. And by Proposition $p | B_\ell(f)$.

If f rational, because L is not either a Fermat or Mersenne prime we deduce f cannot be isogenous to form with full 2-torsion that corresponds to the elliptic curve E. And by Proposition (2) (3) there are infinitely many ℓ s.t. $B_\ell \neq 0$.

Choosing a suitable ℓ gives a bound C_L for the prime p. □

Bibliography

[1] Samuel Marks Galois representations, Harvard accesed February 2023, https://people.math.harvard.edu/~smarks/mod-forms-tutorial/mf-notes/galois-reps.pdf

[2] Fred Diamon, Jerry Shurman (2006) A First Course in Modular Forms, Springer New York, 1st ed.

[3] Gary Cornell, Joseph H. Silverman, Glenn Stevens (2000) Modular Forms and Fermat's Last Theorem, Springer New York, 1st ed.

[4] Jan Hendrik Bruinier, Gerard van der Gerr, Günter Harder, Don Zagier (2000) The 1-2-3 of Modular Forms, Springer Berlin, Heidelberg, 1st ed.

[5] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer, 1994

[6] H. Cohen (2007) Number Theory, Volume II: Analytic and Modern Tools, Springer.

[7] N. Freitas, S. Sisek (2015) The Asymptotic Fermat's Last Theorem for Five-sixths of Real Quadratic Fields, Compositio Mathematics 151, n0.8, 1395–1451. https://arxiv.org/abs/1307.3162

[8] N. Freitas, B.V. Le Hung and S. Silsek (13 Nov. 2013), Elliptic curves over real quadratic fields are modular, https://arxiv.org/abs/1310.7088

[9] N. Freitas and S. Silsek, Criterua for irreducibility of mod p representation of Frey curves

[10] D. Blasius (2004), Elliptic curves, Hillbert modular forms, and the Hodge conjecturem Contributions to automorphic forms, geometry, and number theory, 83-103, Hohns Hopkins Univ. Press

[11] A. Krauss (1998), Sur l'équation $a^3 + b^3 = c^p$, Esperimental Math. 7, 1-13.

[12] E. Landau (1909), Handuch der Lehre von der Verteilung der Primzahlen II B.G. Teubner