

MODULAR APPROACH TO DIOPHANTINE EQUATIONS

by

Erman Işık

B.S., Mathematics, Ege University, 2015

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Mathematics
Boğaziçi University

2019

ACKNOWLEDGEMENTS

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

First and foremost, I would like to thank my thesis advisor Ekin Özman who guides and supports me preparing for my academic career. Her enthusiasm and patience encouraged me to keep going towards my study whenever I felt overwhelmed. I want to thank her for the contribution not only to the development of this thesis but also to my mathematical improvement. I feel lucky for working with her.

I would also like to express my sincere gratitude to Pınar Değirmenci for her encouragement, inspiration and love. A special thank goes to Oğuz Şavk for his friendship and motivation throughout my life.

I want to thank all the people with whom I discussed and learned about mathematics during the last three years. I am particularly grateful to Harun Kır and Emre Gungor for their numerous comments and suggestions.

I thankfully acknowledge the financial support given by TÜBİTAK project 117F045.

Finally, it would be awkward not to mention the support and encouragement I get from my family. My parents deserve a special acknowledgement for the constant support and trust.

ABSTRACT

MODULAR APPROACH TO DIOPHANTINE EQUATIONS

In this thesis, we study the modular approach to the Fermat's equation $x^p + y^p = z^p$, where x, y and z are co-prime integers, and p is a prime, and some generalizations. After reviewing and explaining how the modular approach can be used to deal with the Fermat-type equations, following the paper of Emmanuel Halberstadt and Alain Karus, we prove that there exists a dense subset of the set of prime numbers such that the equation $ax^p + by^p = cz^p$ has no non-trivial primitive solution. Here a, b, c are fixed pairwise co-prime odd integers and $p \geq 5$ is a prime. Then we show that the equation $x^4 + y^2 = z^p$ has no solutions in co-prime integers when $p \geq 211$ due to Jordan Ellenberg's article. The main idea to deal with this equation is based on the modularity of $\mathbb{Q}$ -curves and the images of Galois representations attached such curves.

This thesis was supported by TUBITAK project 117F045.

ÖZET

DIOPHANTINE DENKLEMLERE MODÜLER YAKLAŞIM

Bu tezde, aralarında asal x, y , ve z tamsayıları ve p asal olmak üzere $x^p + y^p = z^p$ Fermat denklemine ve bazı genelleştirmelerine modüler yaklaşımı çalışacağız. Modüler yaklaşımın Fermat denklemleriyle baş etmek için nasıl kullanılabileceğini özetleyip açıkladıktan sonra, Emmanuel Halberstadt and Alain Kraus'un makalesini takip ederek $ax^p + by^p = cz^p$ denkleminin aşık ve aralarında asal çözümlerinin olmadığı asal sayılar kümesinin yoğun bir altkümesi olduğunu kanıtlayacağız. Burada a, b, c aralarında asal tek sayılar ve p bir asal sayıdır. Sonrasında $x^4 + y^2 = z^p$ denkleminin $p \geq 211$ iken aralarında asal tamsayılarda bir çözümünün olmadığını Jordan Ellenberg'in makalesi aracılığıyla gösteriyoruz. Bu denklemle başa çıkmak için gerekli asıl fikir $\mathbb{Q}$ -eğrilerinin modülerliğine ve böyle eğrilere eklenmiş Galois gösterimlerinin görüntülerine dayanır.

Bu tez TÜBİTAK projesi 117F045 tarafından fonlanmıştır.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS

$a_1, \dots, a_6$	coefficients of a general Weierstrass equation,
$a_p(E)$	modified solution of E modulo p ,
$Aut(E)$	the automorphism group of the elliptic curve E ,
$D_{\mathfrak{p}}$	the decomposition subgroup of G_K corresponding to $\mathfrak{p}$,
$div(E)$	divisor group of the elliptic curve E ,
$div(f)$	divisor of a function f ,
E	an elliptic curve over K ,
$E[m]$	m -torsion subgroup of the elliptic curve E ,
$End(E)$	the endomorphism group of the elliptic curve E ,
E_q	Tate curve,
$E(K)$	group of K -rational points on the elliptic curve E/K ,
$\hat{e}$	the Weil pairing $\hat{e} : E[m] \times E[m] \rightarrow \mu_m$,
$Frob_{\mathfrak{p}}$	Frobenius element of a Galois group,
$\mathbb{F}_p$	a field of p elements,
G_K	$Gal(\overline{K}/K)$,
$\mathcal{H}$	the upper half plane,
$I_{\mathfrak{p}}$	the inertia group of G_K corresponding to $\mathfrak{p}$,
j_E	the j -invariant of the elliptic curve E ,
K_f	number field associated to the modular form f ,
K	a Galois number field,
$\overline{K}$	an algebraic closure of K ,
$\overline{K}(E)$	the function field of the elliptic curve E ,
$[m]$	multiplication-by- m map on an elliptic curve,
$M_k(\Gamma)$	the space of modular forms of weight k for Γ ,
N_E	the conductor of the elliptic curve E ,
$\mathcal{O}_K$	the ring of integers of K ,
$\mathcal{O}$	the identity element on an elliptic curve,

$ord_\ell(N)$	the value of maximal power of ℓ dividing N ,
$\mathfrak{p}$	a prime of $\mathcal{O}_K$,
$\mathbb{P}\bar{\rho}_{E,\mathfrak{p}}$	the mod $\mathfrak{p}$ projective Galois representation attached to E ,
P^σ	the action of $\sigma \in G_{\bar{K}/K}$ on the point P ,
q	abbreviation for $e^{2\pi i\tau}$,
$Res_{K/L}X$	the Weil restriction of the variety X over L
$S_k(\Gamma)$	the space of cuspforms forms of weight k for Γ ,
$S_k(\Gamma)^{new}$	the space of newforms forms of weight k for Γ ,
$S_k(\Gamma)^{old}$	the space of olforms forms of weight k for Γ ,
$SL_2(\mathbb{Z})$	the special linear group,
$T_\ell(E)$	the ℓ -adic Tate module of the elliptic curve E ,
T_n	Hecke operator, n any positive integer,
$X_0(N)$	modular curve for the congruence subgroup $\Gamma_0(N)$,
$\oplus$	group law on an elliptic curve,
$[\gamma]_k$	the weight k operator,
$\Gamma_0(N)$	congruence subgroup,
$\Gamma_1(N)$	congruence subgroup,
Δ_E	the discriminant of the elliptic curve E ,
Δ_{min}	the global minimal discriminant of the elliptic curve E ,
μ_m	the group m -th roots of unity,
$\bar{\rho}_{E,\mathfrak{p}}$	the mod $\mathfrak{p}$ Galois representation associated to E ,
$\rho_{f,\mathfrak{p}}$	the mod $\mathfrak{p}$ Galois representation associated to f ,
χ_p	the mod p cyclotomic character $G_K \rightarrow \mathbb{F}_p^*$.

1. INTRODUCTION

The main purpose of this master thesis is to study the *modular approach* to some Fermat-type Diophantine equations.

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

Theorem 1.1. (*Fermat-Wiles*) *Let $n > 2$ be an integer. Then the equation $x^n + y^n = z^n$ has no non-trivial (meaning $xyz \neq 0$) primitive (meaning $\gcd(x, y, z) = 1$) integer solutions.*

The strategy that led to the proof of FLT is called the *modular approach* and makes a remarkable use of elliptic curves, modular forms and Galois representations attached to these two objects. The *modular approach* for solving Diophantine equations typically proceeds in the following steps:

- (i) To a putative solution, associate a Frey elliptic curve E .
- (ii) Use modularity and level lowering results to show that (for a suitable prime p) the Galois representation on the p -torsion $E[p]$ is isomorphic to the mod- p representation associated to a newform f of weight 2 and small level N (for a suitable prime ideal $\mathfrak{p}$ above p of the field of coefficients of f),

$$\bar{\rho}_{E,p} \simeq \bar{\rho}_{f,\mathfrak{p}}$$

- (iii) For each of the possible newforms, show that they cannot occur, or find all possible associated solutions.

Chapter 1 is mainly devoted to cover background material necessary to the modular approach via elliptic curves over a number field K . It includes the basic definitions and theorems about elliptic curves and modular forms. Concepts like reduction of an elliptic curve at a prime, minimal discriminant and conductor are introduced.

In Chapter 2, we give some basic notions of modular forms. The idea of a modular form with respect to a congruence subgroup, Hecke operator, newform are explained. Modular forms make-up finite-dimensional vector spaces over $\mathbb{C}$. So their dimensions make sense and, for a special case, the dimension formula is introduced at the end of this chapter.

Chapter 3 focuses on the absolute Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ and Galois representations. First, we describe properties of the absolute Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ such as being a projective group. Then we introduce a general concept of Galois representations. Last two section include necessary result about Galois representations attached to elliptic curves and modular forms.

In Chapter 4, we mention the machinery to prove the Fermat's Last Theorem. Some strong theorems about irreducibility of Galois representations, modularity of elliptic curves, and Ribet's level-lowering are stated respectively. Next, we show how to combine these results to prove Fermat's Last Theorem.

Chapter 5 is concerned with the generalized version of Fermat-type equation $ax^p + by^p = cz^p$ with a, b, c are fixed pairwise co-prime odd integers. We deal with the following theorem, which the proof is based on the work of Halberstadt-Kraus:

Theorem 1.2. *There exists a dense subset of the set of prime numbers such that the equation $ax^p + by^p = cz^p$ has no non-trivial primitive solutions in integers, where a, b, c are fixed pairwise co-prime odd integers.*

In Chapter 6, we cover material about the $\mathbb{Q}$ -curves, Galois representations attached to $\mathbb{Q}$ -curves, the concept of abelian varieties of GL_2 type and Serre invariants. All the improved materials are necessary to prove the non-existence of the equation $x^4 + y^2 = z^p$ in co-prime integers. The proof is based on the work of Jordan Ellenberg.

Chapter 7 includes a survey what we have known about the generalization of Fermat-type equations. We state two tables, one of which contains unconditional results for various equations, and another includes conditional results or/and the cases for finitely many primes. We also mention the fact that the proof of some cases differ from the use of $\mathbb{Q}$ -curves or the symplectic method that we describe in Chapter 5 and Chapter 6.

2. THE HISTORY OF FERMAT'S LAST THEOREM

In 1637, Pierre de Fermat, a famous French amateur mathematician, lawyer by profession, wrote an innocuous note in his copy of *Arithmetica* by Diophantus of Alexandria:

"It can never happen that the sum of two numbers raised to n -th powers is a sum of another n -th power."

Unfortunately, his margin was too short to contain a proof...

Fermat's idea was that if $x^n + y^n = z^n$ is a relation between three integers x, y and z , and n is a fixed number greater than 2, then the only solutions to this equation must include a zero, so $xyz = 0$. Since then, this theorem has been known as Fermat's Last Theorem.

Fermat proved himself only the case when exponent n is 4. Such well-known mathematicians like Euler, Legendre, Dirichlet, Gauss and Lamé provided proofs for exponents $n = 3, 5, 7$. A technique known as *infinite descent* is used in all these proofs.

Lamé announced in 1841 a full proof of the general case of Fermat's Last Theorem. However, the proof was incorrect. His proof relied on the (incorrect) assumption that $\mathbb{Z}[\zeta_p]$, the ring of integers of $\mathbb{Q}(\zeta_p)$ with $\zeta = e^{2\pi i/p}$, forms a ring with unique factorization. Kummer showed that this assumption fails for $p = 23$. Then Kummer proceeded with an investigation of divisibility in $\mathbb{Z}[\zeta_p]$ and introduced the notation of ideal numbers, a larger group in which unique factorization was recovered. Consequently, he proved in 1857 the following theorem for Fermat's Last Theorem :

Let $K = \mathbb{Q}(\zeta_p)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ and $I(K)$ denote the set of non-zero fractional ideals, and let $P(K)$ denote the set of principal fractional ideals a normal subgroup of $I(K)$. Then the quotient $\mathcal{C}(K) := I(K)/P(K)$ is called the class group of K . Note that the class group $\mathcal{C}(K)$ is finite, and $h(K) = |\mathcal{C}(K)| = |I(K)/P(K)|$ is called the class number of K .

If the prime number p does not divide $h(K)$, we say that p is a *regular prime*.

Theorem 2.1 (Kummer). *Equation $x^p + y^p = z^p$ has no non-trivial integer solutions for regular primes.*

After Kummer's attempt, plenty of mathematicians had tried to prove the general case of Fermat's Last Theorem. However, a British mathematician Andrew Wiles reached the goal in 1995 with help of Richard Taylor.

In 1984 Gerhard Frey observed that every Fermat's solution can be linked to an elliptic curve, an algebraic object with well-defined arithmetic operation. This remark was then used by Jean-Pierre Serre and Ken Ribet to reduce the proof of Fermat's Last Theorem to the statement about modularity of elliptic curves known as the Taniyama-Shimura conjecture. In 1995 Sir Andrew Wiles showed that every semistable elliptic curves is modular and proved Fermat's Last Theorem.

3. ELLIPTIC CURVES

In this chapter, we introduce some definitions and properties about elliptic curves. The main reference for this chapter is [?].

Definition 3.1. (*Elliptic Curve*) Let K be a number field. An elliptic curve E/K is a non-singular projective curve of genus 1 with the base point $\mathcal{O}$.

We can be more precise about the base point $\mathcal{O}$. If $[X : Y : Z]$ is a point with $Z \neq 0$, then $[X : Y : Z] = [X/Z : Y/Z : 1]$. These are the “finite” points in $\mathbb{P}^2(K)$. However, if $Z = 0$ then dividing by Z should be thought of as giving ∞ in either the X or Y coordinate, and therefore the points $[X : Y : 0]$ are called the *points at infinity* in $\mathbb{P}^2(K)$. We denote the point at infinity on an elliptic curve as $\mathcal{O} = [0 : 1 : 0]$.

Definition 3.2. (*Singular Point*) Consider an affine curve C given by the equation $f(x, y) = 0$ in K^2 . Let P be a point of C . We say that $P = (x_0, y_0)$ is singular, if

$$\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0.$$

The point P is called non-singular if it is not singular. The curve C is called non-singular, if every point of C is non-singular.

The property of non-singularity guarantees that the tangent line is well-defined for each point of the curve. Indeed, the equation of the tangent line of the curve f at (a, b) is

$$\frac{\partial f}{\partial x}(a, b)(x - a) + \frac{\partial f}{\partial y}(a, b)(y - b) = 0,$$

which is well-defined when at least one derivative is non-zero.

3.1. The Weierstrass Equation of an Elliptic Curve

Every elliptic curve can be written as the locus in $\mathbb{P}^2(K)$ of a cubic equation with only one point, the base point, on the line at ∞ :

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

with $a_1, \dots, a_6 \in \overline{K}$. To ease notation, we generally write the *Weierstrass equation* for our elliptic curve using non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$,

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

always remembering that there is an extra point $\mathcal{O} = [0 : 1 : 0]$. we can simplify the equation by changing of variables :

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

with the arithmetic invariants $\Delta = -16(4A^3 + 27B^2)$ (the discriminant), $c_4 = (a_1^2 + 4a_4)^2 - 24(2a_4 + a_1 + a_3)$ and $j = -1728 \frac{(4A)^3}{\Delta}$ (the j-invariant).

Proposition 3.3. ([?] , III, Prop. 1.4)

(i) *The curve given by a Weierstrass equation satisfies:*

- (a) *It is non-singular if and only if $\Delta \neq 0$*
- (b) *It has a node if and only if $\Delta = 0$ and $c_4 \neq 0$*
- (c) *It has a cusp if and only if $\Delta = c_4 = 0$*

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

Proposition 3.4. (*[?], III, Prop. 3.1*) *Let E be an elliptic curve defined over a number field K .*

(i) *There exist functions $x, y \in K(E)$ such that the map*

$$\phi : E \rightarrow \mathbb{P}^2, \phi = [x, y, 1],$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

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

with coefficients $a_1, \dots, a_6 \in K$ and satisfying $\phi(\mathcal{O}) = [0 : 1 : 0]$. The functions x and y are called Weierstrass coordinates for the elliptic curve E .

(ii) *Every smooth cubic curve C given by a Weierstrass equation as above is an elliptic curve defined over K with base point $\mathcal{O} = [0 : 1 : 0]$.*

(iii) *Any two Weierstrass equation for E are related by a linear change of variables of the form*

$$X = u^2X' + r, Y = u^3Y' + su^2X' + t,$$

with $u \in K^*$ and $e, s, t \in K$.

3.2. The Group Law of an Elliptic Curve

Let P_1 and P_2 be two point over the elliptic curve E . Then by Bézout's theorem, there exists a third point on the curve E which is the intersection of the curve E and the straight line defined by P_1 and P_2 . Denote this point by $P_1 * P_2$. Then we clearly have $P_1 * P_2 = P_2 * P_1$.

We define the operation $\oplus$ on the set of rational points $E(K) = \{P = (x, y) \in E \mid x, y \in K\} \cup \{\mathcal{O}\}$ as follows:

$$P_1 \oplus P_2 = (P_1 * P_2) * \mathcal{O},$$

where $P_1, P_2 \in E(K)$.

This means that we first draw the straight line passing through P_1 and P_2 and we find the third intersection point $P_1 * P_2$ on E . Then we repeat the operation and draw a line between $P_1 * P_2$ and $\mathcal{O}$.

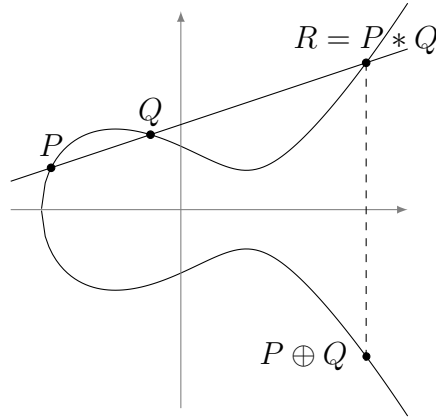


Figure 3.1. An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law.

This composition law $\oplus$ provides the set $E(\overline{K})$ with the structure of an abelian group whose identity element is $\mathcal{O}$. Moreover, the set of rational points $E(K)$ has a subgroup of this structure. The proof is quite easy, except for the associativity that needs the Riemann-Roch theorem.(see Silverman III.2 proposition 2.2).

Theorem 3.5. (*[?], III Prop. 2.1*) Consider an elliptic curve E defined by the equation

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

with $A, B \in \overline{K}$, together with the base point $\mathcal{O} = [0 : 1 : 0]$.

Consider the operation $\oplus$ on $E(\overline{K})$ defined as above. Then $(E(\overline{K}), \oplus)$ is an abelian group.

In particular we have :

- $\mathcal{O}$ is the identity element;
- $P \oplus Q = Q \oplus P$, for every $P, Q \in E(\overline{K})$;
- for every $P = (x, y) \in E(\overline{K})$ we have $P \oplus (-P) = \mathcal{O}$, with $-P = (x, -y)$.

Example 3.6. Let E be an elliptic curve over $\mathbb{Q}$ given the equation :

$$E : y^2 + y = x^3 - x$$

Let $P = (0, 0)$ and $Q = (-1, -1)$ in $E(\mathbb{Q})$. We want to find $P \oplus Q$.

The line going through P and Q is clearly $x = y$. This must meet E somewhere else.

Put $y = x$ into the equation for E :

$$\begin{aligned} x^2 + x &= x^3 - x \\ x &= 0 \text{ or } -1 \text{ or } 2 \end{aligned}$$

So we have $R = P * Q = (2, 2)$. The line $x = 2$ meet E at R and $\mathcal{O}$. Put $x = 2$ into the equation for E . Then we have $y = 2$ or -3 . Hence we have $P \oplus Q = (2, -3)$.

3.3. Isogeny and Torsion Points

Definition 3.7. (*Isogeny*) Let E and E' be two elliptic curves. An isogeny from E to E' is a morphism

$$\phi : E \rightarrow E' \text{ satisfying } \phi(\mathcal{O}) = \mathcal{O}'.$$

Definition 3.8. We say that ϕ is separable if the extension $K(E)/\phi^*(K(E'))$ is separable, where $\phi^* : K(E') \rightarrow K(E), f \mapsto f \circ \phi$.

Note that $K(E)$ is a finite extension of $\phi^*(K(E'))$, so we have

$$\deg \phi = |K(E) : \phi^*(K(E'))| < \infty.$$

Proposition 3.9. Let E and E' be two elliptic curves over K , with $\phi : E \rightarrow E'$ a non-constant isogeny. Then $\phi(E(K)) = E'(K)$, in other words ϕ is surjective.

Proof. The general statement of algebraic geometry says that an isogeny between two algebraic curve is either constant or surjective. Hence, the morphism $\phi : C_1 \rightarrow C_2$ of curves is surjective. $\square$

Example 3.10. Let E be an elliptic curve over K . Then $[m] : E \rightarrow E, P \mapsto [m]P$ is an isogeny.

Theorem 3.11. ([?], III, Thm. 4.8) An isogeny $\phi : E \rightarrow E'$ is a group homomorphism, i.e. $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$.

Corollary 3.12. ([?], III, Cor. 4.9) Let $\phi : E \rightarrow E'$ be a non-zero isogeny. Then

$$\ker \phi = \phi^{-1}(\mathcal{O})$$

is a finite group.

Theorem 3.13. ([?], III, Thm. 4.10) Let $\phi : E \rightarrow E'$ be a separable isogeny, i.e. $K(E)/\phi^*(E'K)$ is a separable extension. Then for every $Q \in E'$,

$$|\phi^{-1}(Q)| = \deg \phi.$$

Theorem 3.14. Let E be an elliptic curve and C be a finite subgroup of E . Then there are a unique elliptic curve E' and a separable isogeny $\phi : E \rightarrow E'$ such that $\ker \phi = C$.

Proof. We can get the result using Velu's formula (cf. [?], 12.3). □

Definition 3.15. (*Torsion Subgroup*) Let E be an elliptic curve over K and $m \in \mathbb{Z}$ with $m \geq 1$. The m -torsion subgroup of E , denoted by $E[m]$, is the set of points of E of order m ,

$$E[m] = \{P \in E(K) : [m]P = \mathcal{O}\}.$$

Recall that $[m]$ is an isogeny. Then we have $E[m] = \{P \in E : [m]P = \mathcal{O}\} = \ker [m]$.

Theorem 3.16. ([?], Thm. 3.2) Let E be an elliptic curve over $\overline{K}$ and let m be a positive integer with $(\text{char}(\overline{K}), m) = 1$ or $\text{char}(\overline{K}) = 0$. Then

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

Example 3.17. Let E be an elliptic curve over $\mathbb{C}$ given Weierstrass equation

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

Then we have $E[2] = \{\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)\}$.

3.4. Minimal Discriminant, Reduction Types and Conductor of an Elliptic Curve

Definition 3.18. *Let S be the set of all elliptic curves E' that are isomorphic to E over K and such that the discriminant of E' is an integer. The minimal discriminant of E is the integer Δ that attains the minimum of the set $\{|\Delta_{E'}| : E' \in S\}$. In other words, the minimal discriminant is the smallest integral discriminant (in absolute value) of an elliptic curve that is isomorphic to E over K . If E' is the model for E with minimal discriminant, we say that E' is the minimal model for E .*

Let $E/\mathbb{Q}$ be an elliptic curve with minimal model

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

with discriminant $\Delta_{\min}(E) = -16(4A^3 + 27B^2)$. Note that E defines an elliptic curve if and only if $\Delta_{\min}(E)$ is non-zero. Then we can obtain new elliptic curves over $\mathbb{F}_p$ by reducing the coefficients of E modulo p :

$$\overline{E}/\mathbb{F}_p : y^2 = x^3 + \overline{A}x + \overline{B} \subset \mathbb{P}^2(\mathbb{F}_p)$$

So $\overline{E}/\mathbb{F}_p$ defines an elliptic curve if and only if $p \nmid \Delta_{\min}(E)$

Definition 3.19. *The reduction type of E at p is called good if $\overline{E}$ is non-singular. Otherwise, we call the reduction type of $\overline{E}$ at p bad.*

If E has a node, we say that it has *multiplicative* (semistable) reduction. If E has a cusp, we say that it has *additive* (unstable) reduction.

Definition 3.20. (*Conductor*) The conductor $N = N_E$ of E is $N = \prod_{p \text{ prime}} p^{f_p}$, where

$$f_p = \begin{cases} 0 & \text{good at } p \\ 1 & \text{multip. at } p \\ 2 & \text{add. at } p \neq 2, 3 \\ 2 + \delta_p & \text{add. at } p = 2, 3 \end{cases}$$

where δ_p is defined in terms of the wild ramification of the extensions of $\mathbb{Q}_p$ by the division points of E

Note that $p \mid \Delta_{min}$ if and only if $p \mid N$, so E has good reduction at all primes not dividing N

Example 3.21. Assume that we have the elliptic curve

$$E : y^2 = x^3 + 16$$

over $\mathbb{Q}$ with $\Delta_E = -2^{12} \cdot 3^3$. Then taking $x = 4x'$ and $y = 8y' + 4$ we get the minimal form,

$$E_{min}/\mathbb{Q} : y^2 + y = x^3$$

with $\Delta_{min} = 3^3$ and $N_E = 3^3$.

4. MODULAR FORMS

In this chapter we give the necessary information about modular forms for dealing with Fermat's Last Theorem (FLT). We begin with the notions of congruence subgroup and modular form with respect to a congruence subgroup. Next we explain Hecke operators and introduce the notion of newform.

This chapter is based on [?].

4.1. The Modular Group and The Congruence Subgroups

We define the *modular group* as follows,

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

Let $\hat{\mathbb{C}}$ denote the set $\mathbb{C} \cup \{\infty\}$. Given a point $z \in \hat{\mathbb{C}}$, we define the action of $SL_2(\mathbb{Z})$ on $\hat{\mathbb{C}}$ as

$$\alpha.z = \frac{az + b}{cz + d} \text{ for all } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

This means that if $c \neq 0$, then $-d/c$ maps to ∞ and ∞ maps to a/c , if $c = 0$, then ∞ maps to itself. Note that each pair of matrices $\pm\alpha \in SL_2(\mathbb{Z})$ gives a single transformation. Hence we actually have an action of $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$ on $\hat{\mathbb{C}}$.

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

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

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 the modular group, the congruence subgroups. Given a positive integer N , the *principal modular subgroup of level N* is

$$\Gamma(N) = \left\{ \alpha = \begin{pmatrix} a_\alpha & b_\alpha \\ c_\alpha & d_\alpha \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a_\alpha & b_\alpha \\ c_\alpha & d_\alpha \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

where the matrix congruence is interpreted coefficient wise. In particular, we denote $\Gamma(1) = SL_2(\mathbb{Z})$. Observe that $\Gamma(N)$ is the kernel of the map $SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$, $\alpha \mapsto c_\alpha$ so that it is a normal subgroup of $SL_2(N)$. A subgroup Γ of $SL_2(N)$ is a *congruence subgroup* if $\Gamma(N) \subseteq \Gamma$. The main examples of congruence subgroups are

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

where $*$ means unspecified, and

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

satisfying $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$, and furthermore all these are normal subgroup inclusions.

The action of a subgroup G of $SL_2(N)$ divides $\mathcal{H}$ into equivalence classes. We say that two points $\tau_1, \tau_2 \in \mathcal{H}$ are *G-equivalent* if there exists $g \in G$ such that $g.\tau_1 = \tau_2$. Let F be a closed region in $\mathcal{H}$. We say that F is a *fundamental domain* for the subgroup G if every $\tau \in \mathcal{H}$ is G -equivalent to a point in F , but no two distinct points in the interior of F are G -equivalent. The most usual example of fundamental domain is the fundamental domain for $SL_2(N)$, which is given by

$$F = \{\tau \in \mathcal{H} : -1/2 \leq \Re(\tau) \leq 1/2 \text{ and } |\tau| \geq 1\}.$$

Let $\hat{\mathcal{H}}$ denote $\mathcal{H} \cup \{\infty\} \cup \mathbb{Q} = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$. That is, we add to $\mathcal{H}$ a point at infinity and also the rational numbers on the real axis. These points $\mathbb{P}^1(\mathbb{Q})$ are called the *cusps*. It is not difficult to see that $SL_2(\mathbb{Z})$ 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 $SL_2(\mathbb{Z})$ -equivalence class with ∞ .

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

$$N_C = \{\tau \in \mathcal{H} : \text{Im}(\tau) > C\} \cup \{\infty\}$$

for any $C > 0$. Note that under the map $\tau \mapsto q = e^{2\pi i\tau}$ 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 $\hat{H}$, 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 of the variable q having at most finitely many negative terms. That is

$$f(\tau) = \sum_{n \in \mathbb{Z}} c_n q^n,$$

where $c_n = 0$ for infinitely many $n < 0$. We say that $f(\tau)$ is holomorphic at ∞ if $c_n = 0$ for all $n < 0$, and we say that $f(\tau)$ vanishes at ∞ if $c_n = 0$ for all $n \geq 0$. More generally, if $f(\tau)$ has period N we use the map $\tau \mapsto e^{2\pi i\tau/N}$ to map $\hat{H}$ to the open unit disk.

4.2. Modular Forms

Let $f(\tau)$ 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 $f(\tau)$ satisfies the following relation

$$f(\alpha.\tau) = (c\tau + d)^k f(\tau) \text{ for all } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}), \tau \in \mathcal{H}$$

This relation will be called *modularity condition*. Note that, in particular, since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$, the modularity condition tells us that $f(\tau + 1) = f(\tau)$. This implies that it has a Fourier expansion

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

If $f(\tau)$ is holomorphic at ∞ , i.e. $c_n = 0$ for all $n < 0$, then $f(\tau)$ is called a *modular form* of weight k for $SL_2(\mathbb{Z})$. The set of such functions is denoted by $M_k(SL_2(\mathbb{Z}))$. Furthermore, if we have that $f(\tau)$ vanishes at infinity, i.e. $c_n = 0$ for all $n \leq 0$, then $f(\tau)$ is called a *cusp form* of weight k for $SL_2(\mathbb{Z})$. The set of such functions is denoted by $S_k(SL_2(\mathbb{Z}))$. For a given $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, we define the operator $[\alpha]_k$ as follows

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

Using this operator the modularity condition can be rewritten as

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

Note that if k is odd then $M_k(SL_2(\mathbb{Z})) = 0$, since, for $\alpha = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, we have $f(\tau) = f(\alpha.\tau) = -f(\tau)$, 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 $k_1 + k_2$.

We now develop the definition of modular form with respect to a congruence subgroup. Let k be an integer and Γ be a congruence subgroup of $SL_2(\mathbb{Z})$. A function $\mathcal{H} \rightarrow \mathbb{C}$ is called a modular form of weight k with respect to Γ if it satisfies

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

and some holomorphy condition described below. Each congruence subgroup Γ of $SL_2(\mathbb{Z})$ contains a translation matrix of the form

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + h$$

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

$$f(\tau) = \sum_{n \in \mathbb{Z}} c_n q_h^n,$$

where $q_h = e^{2\pi i \tau / h}$. We define such f to be *holomorphic* at ∞ if $c_n = 0$ for all $n < 0$.

Note that, unlike $SL_2(\mathbb{Z})$, the action of Γ on $\mathbb{P}^1(\mathbb{Q})$ is not transitive. Therefore, the holomorphy at ∞ condition does not imply holomorphy at all the cusps. Thus, this last condition has to be imposed. A way to express it is by saying that $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$. Note also 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 (see [?], Exercise 1.2.5).

In summary, we have the following definition.

Definition 4.1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let k be an integer. A function $f : \mathcal{H} \rightarrow \mathbb{C}$ is modular form of weight k with respect to Γ if it satisfies the following conditions:*

- (i) *f is holomorphic*
- (ii) *$f[\alpha]_k = f$ for all $\alpha \in \Gamma$*
- (iii) *$f[\alpha]_k = f$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$, i.e. f is holomorphic at the cusps.*

If in addition

- (iv) *$c_0 = 0$ in the Fourier expansion of $f[\alpha]_k$ for all $\alpha \in SL_2(\mathbb{Z})$,*

then f is said to be 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 $\Gamma_0(N)$. There are explicit formulas for computing the dimension of the spaces of modular forms. Below we just give the formula for the particular case of cusp forms of weight 2, which is of major importance in the proof of FLT.

Proposition 4.2. (*[?], Exercise 3.1.4*) *Let p be a prime. Then*

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

4.3. 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 $SL_2(\mathbb{Z})$.

Definition 4.3. *Let $N \in \mathbb{Z}^+$ and p a prime. The operator T_p is defined as*

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

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

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

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

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

Note that $T_n T_m = T_m T_n$ if $\gcd(n, m) = 1$.

Proposition 4.4. *Let $f \in M_k(\Gamma_0(N))$ have Fourier expansion*

$$f(\tau) = \sum_{m=0}^{\infty} c_m(f) q^m, \text{ where } q = e^{2\pi i \tau}.$$

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

$$(T_n f)(\tau) = \sum_{m=0}^{\infty} c_m(T_n f) q^m,$$

$$\text{where } c_m(T_n f) = \sum_{d|(n, m)} d^{k-1} c_{nm/d^2}(f).$$

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 old forms and newforms. Let us formally develop the meaning of those concepts. The most trivial way to move among levels is to observe that if $M|N$ then $S_k(\Gamma(M)) \subset S_k(\Gamma(N))$.

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 $f(d\tau) \in S_k(\Gamma_0(N))$. Note that, for $d = 1$, we get the embedding $S_k(\Gamma(M)) \subset S_k(\Gamma(N))$ again.

We say that given a modular form $f \in S_k(\Gamma_0(N))$ is an *oldform* if it is a linear combination of functions of type $g(d\tau)$ where g is a modular form of level N/M and d is a divisor of N/M . The space of oldforms is denoted by $S_k(\Gamma_0(N))^{old}$. 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 $\hat{\mathcal{H}}$ 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

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

where $z = x + iy$. This measure is invariant under the automorphism group $GL_2^+(\mathbb{R})$ of $\mathcal{H}$, meaning that $d\mu(\alpha.z) = d\mu(z)$ for all $\alpha \in GL_2^+(\mathbb{R})$ and $z \in \mathcal{H}$. Let us define, for $f, g \in S_k(\Gamma)$, a new measure,

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

The exterior form (f, g) satisfies the relations

- (i) $(f, g) = \overline{(f, g)}$,
- (ii) $(f, f) \geq 0$ and $(f, f) = 0$ implies $f = 0$,
- (iii) $(f, g)(\gamma.z) = (f, g)(z)$ for all $\gamma \in \Gamma$.

Theorem 4.5. *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 Petersson hermitian product:*

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

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

Definition 4.6. *A non-zero modular form $f \in M_k(\Gamma_0(N))$ is a Hecke form or simply an eigenform if it is an eigenvector for the Hecke operators T_n for all $n \in \mathbb{Z}^+$. The eigenform $f(\tau) = \sum_{n=0}^{\infty} c_n q^n$ is normalized if $a_1 = 1$. A newform is a normalized eigenform in $S_k(\Gamma_0(N))^{new}$.*

Theorem 4.7. *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 $n \in \mathbb{Z}^+$. Moreover, the set of newforms is an orthogonal basis of the space $S_k(\Gamma_0(N))^{new}$. Each such newform satisfies the following properties:*

- $T_n f = c_n(f) f$ for all $n \in \mathbb{Z}$. That is, its Fourier coefficients are its T_n -eigenvalues,
- The Fourier coefficients of f are algebraic integers over $\mathbb{Q}$,
- $\mathbb{Q}(\{c_n \mid n \geq 0\})$ is a number field. We denote this by K_f .

Remark 4.8. *For a fixed N , since the set of newforms is a basis for the space $S_k(\Gamma_0(N))^{new}$, there are only finitely many newforms of level N . Comparing this deduction with the dimension formula given by Proposition ??, we have, in particular, the following proposition.*

Proposition 4.9. *There are no newforms at levels 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28 and 60.*

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

- (i) $c_1 = 1$,
- (ii) $c_{p^r} = c_p c_{p^{r-1}} - p^{k-1} c_{p^{r-2}}$ for all prime p and $r \geq 2$,
- (iii) $c_{mn} = c_m c_n$ when $(m, n) = 1$.

5. ABSOLUTE GALOIS GROUP AND GALOIS REPRESENTATION

5.1. Absolute Galois Group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$

The absolute Galois group of $\mathbb{Q}$ is the Galois group $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, where $\overline{\mathbb{Q}}$ denotes an algebraic closure of $\mathbb{Q}$. Moreover, it is also the projective limit of $Gal(F/\mathbb{Q})$, where F runs all over number fields F . In order to see this fact, we need the following definition and construction. For further detail for the absolute Galois group see [?], Ch. 9.

Definition 5.1. Let $(I, \leq)$ be a directed poset and let $(A_i)_{i \in I}$ be a family of groups and suppose we have a family of homomorphisms $f_j^i : A_j \rightarrow A_i$ for all $i \leq j$ with the following properties :

- f_i^i is the identity on A_i
- $f_k^i = f_k^j \circ f_j^i$ for all $i \leq j \leq k$.

Then the pair $((A_i)_{i \in I}, (f_j^i)_{i \leq j, i, j \in I})$ is called an inverse system of groups and morphisms over I .

We define the projective limit of the inverse system $((A_i)_{i \in I}, (f_j^i)_{i \leq j, i, j \in I})$ as

$$A = \varprojlim A_i = \{a \in \prod_{i \in I} A_i \mid a_i = f_j^i(a_j) \text{ for all } i \leq j\}.$$

This same construction may be carried out if the A_i 's are sets, semigroups, topological spaces, rings, modules (over a fixed ring), algebras (over a fixed ring), etc., and the homomorphisms are the morphisms in the corresponding category. The projective limit will also belong to that category.

It is clear that $\overline{\mathbb{Q}}$ is the union of all Galois number fields. Indeed, if $\alpha \in \overline{\mathbb{Q}}$, then $\mathbb{Q}(\alpha)$ is a number field contained in $\overline{\mathbb{Q}}$ and so is its normal closure, which is Galois over $\mathbb{Q}$. Conversely, if F is a Galois number field, each of its elements is algebraic over $\mathbb{Q}$, and so lies in $\overline{\mathbb{Q}}$. Moreover, the collection

$$\{Gal(F/\mathbb{Q}) : F/\mathbb{Q} \text{ is a finite Galois extension} \}$$

is an inverse system whose maps are the ones induced by inclusions; i.e. if $K \subseteq F$ is an extension of Galois number fields we have a canonical restriction map

$$\begin{aligned} Gal(F/\mathbb{Q}) &\longrightarrow Gal(K/\mathbb{Q}) \\ \sigma &\mapsto \sigma_K := \sigma|_K \end{aligned}$$

that is surjective.

Proposition 5.2. *The absolute Galois group $G_{\mathbb{Q}}$ is isomorphic to the projective limit $\varprojlim Gal(F/\mathbb{Q})$, where F runs over all finite Galois extensions of $\mathbb{Q}$.*

Proof. Let $\sigma \in G_{\mathbb{Q}}$, and $F \subseteq \overline{\mathbb{Q}}$ be a Galois number field. Then $\sigma|_F$ lies in $Gal(F/\mathbb{Q})$, since $F/\mathbb{Q}$ is Galois. Moreover, it is clear that if $K \subseteq F$ is another Galois number field, then $\sigma|_K = (\sigma|_F)_K$. Therefore, σ defines an element of $\varprojlim Gal(F/\mathbb{Q})$.

On the other hand, let's take an element $\{\sigma\} \in \varprojlim Gal(F/\mathbb{Q})$. This comes from an element $\sigma \in G_{\mathbb{Q}}$ in an obvious way. Namely, if $\alpha \in \overline{\mathbb{Q}}$, then $\alpha \in F$ and so we get $\alpha^\sigma = \alpha^{\sigma_F}$ □

The group $G_{\mathbb{Q}}$ is then a profinite group, namely a projective limit of finite groups. Hence it carries a structure of topological group. Here we are considering the discrete topology on the finite Galois groups $\text{Gal}(F/\mathbb{Q})$ and the product topology on $G_{\mathbb{Q}}$. One can see that $G_{\mathbb{Q}}$ is compact, Hausdorff and totally disconnected; i.e. its only connected components are the points.

Remark 5.3. *For any Galois number field $F/\mathbb{Q}$ the restriction map*

$$\begin{aligned} \pi_F : G_{\mathbb{Q}} &\longrightarrow \text{Gal}(F/\mathbb{Q}) \\ \sigma &\longmapsto \sigma|_F \end{aligned}$$

is surjective. This is a general fact about projective limits of an inverse surjective systems.

Now, a system of open neighbourhoods in $G_{\mathbb{Q}}$ for $1 = 1_{G_{\mathbb{Q}}}$ is the one generated by the kernels of the projections $G_{\mathbb{Q}} \rightarrow \text{Gal}(F/\mathbb{Q})$ as F runs over all Galois number fields. Since $G_{\mathbb{Q}}$ is a topological group, it follows that the system of open neighbourhoods for any $\sigma \in G_{\mathbb{Q}}$ is generated by

$$U_{\sigma}(F) := \sigma \ker(G_{\mathbb{Q}} \rightarrow \text{Gal}(F/\mathbb{Q}))$$

as F runs over all Galois number fields.

5.2. Maximal Ideals of $\overline{\mathbb{Z}}$

Let $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ be an ideal, where $\overline{\mathbb{Z}}$ denotes the ring of integers of $\overline{\mathbb{Q}}$, and $\mathcal{O}_K \subseteq \overline{\mathbb{Z}}$ be any number ring. Since the extension $\mathcal{O}_K \subseteq \overline{\mathbb{Z}}$ is integral, the ideal $\mathfrak{p} \cap \mathcal{O}_K$ is maximal. Therefore, when $K = \mathbb{Q}$ we have $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some rational prime p . Conversely, given such a rational prime, the ideal $p\overline{\mathbb{Z}}$ is contained by Zorn's lemma in some maximal ideal $\mathfrak{p}$.

Since $\overline{\mathbb{Z}} = \bigcup_K \mathcal{O}_K$ for all number fields K , any maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ is given by $\mathfrak{p} = \bigcup_K \mathfrak{p}_K$, where $\mathfrak{p}_K = \mathfrak{p} \cap \mathcal{O}_K$ and $\mathfrak{p}_K$ are compatible, in the sense that if $K' \subseteq K$ are two number fields, then $\mathfrak{p}_K \cap K' = \mathfrak{p}_{K'}$. Conversely, every such union defines a maximal ideal of $\overline{\mathbb{Z}}$.

Remark 5.4. *One can easily see that if $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ is a maximal ideal and $p = \mathfrak{p} \cap \mathbb{Z}$, then $\overline{\mathbb{Z}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_p$. From now on we will always identify $\overline{\mathbb{Z}}/\mathfrak{p}$ with $\overline{\mathbb{F}_p}$.*

Definition 5.5. *The decomposition group of $\mathfrak{p}$ is defined as*

$$D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} : \mathfrak{p}^{\sigma} = \mathfrak{p}\}.$$

One can also see that the decomposition group $D_{\mathfrak{p}}$ is isomorphic to the projective limit $\varprojlim D_{\mathfrak{p}_F}$, where F runs over all Galois number fields, $\mathfrak{p}_F = \mathfrak{p} \cap F$ and $D_{\mathfrak{p}_F}$ is the decomposition group of $\mathfrak{p}_F$ in F .

Now the point is that if $F/\mathbb{Q}$ is a finite Galois extension, then for every rational prime p and every prime $\mathfrak{p}_F \subseteq F$ lying over p it is known (cf. [?]) that there exists an isomorphism between $D_{\mathfrak{p}_F}$ and $\text{Gal}(F_{\mathfrak{p}}/\mathbb{Q}_p)$, where $F_{\mathfrak{p}}$ denotes the completion of F with respect to the discrete valuation induced by $\mathfrak{p}_F$. This tells us that $D_{\mathfrak{p}}$ is isomorphic to $\varprojlim \text{Gal}(K/\mathbb{Q}_p)$, where K runs over all the finite extensions of $\mathbb{Q}_p$. But, again it is easy to see that

$$G_p := \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) = \varprojlim \text{Gal}(K/\mathbb{Q}_p).$$

So what we have found is that we can identify the decomposition group of any maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ with the local Galois group G_p .

Remark 5.6. (i) For another prime ideal $\mathfrak{p}' \subseteq \overline{\mathbb{Z}}$ lying over p , we have $\mathfrak{p}^\sigma = \mathfrak{p}'$ and $D_{\mathfrak{p}'} = \sigma^{-1}D_{\mathfrak{p}}\sigma$. This shows that choosing another $\mathfrak{p}$ lying over p changes the embedding $G_p \hookrightarrow G_{\mathbb{Q}}$ up to conjugation.

(ii) Each $\sigma \in D_{\mathfrak{p}}$ acts in well-defined way on the field $\overline{\mathbb{F}}_{\mathfrak{p}} = \overline{\mathbb{Z}}/\mathfrak{p}$.

$$\begin{array}{ccc} \overline{\mathbb{Z}} & \xrightarrow{\sigma} & \overline{\mathbb{Z}} \\ \pi \downarrow & & \downarrow \pi \\ \overline{\mathbb{F}}_{\mathfrak{p}} & \xrightarrow{\overline{\sigma}} & \overline{\mathbb{F}}_{\mathfrak{p}} \end{array} \quad (5.1)$$

where $(\alpha + \mathfrak{p})^{\overline{\sigma}} := \alpha^\sigma + \mathfrak{p}$. So we obtain a natural homomorphism $D_{\mathfrak{p}} \rightarrow G_{\overline{\mathbb{F}}_{\mathfrak{p}}}$. The homomorphism is actually surjective.

Definition 5.7. The inertia group of $\mathfrak{p}$, denoted by $I_{\mathfrak{p}}$, is the kernel of the map $D_{\mathfrak{p}} \rightarrow G_{\overline{\mathbb{F}}_{\mathfrak{p}}}$.

One has that $I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : x^\sigma \equiv x \pmod{\mathfrak{p}}, \forall x \in \overline{\mathbb{Z}}\}$. Again, it is easy to see that $I_{\mathfrak{p}}$ is isomorphic to $\varprojlim I_{\mathfrak{p}_F}$.

Definition 5.8. Any preimage of $\sigma_p : x \rightarrow x^p$ via the reduction map $D_{\mathfrak{p}} \rightarrow G_{\overline{\mathbb{F}}_{\mathfrak{p}}}$ is denoted by $Frob_{\mathfrak{p}}$ and is called absolute Frobenius element over p .

Clearly, $Frob_{\mathfrak{p}}$ is determined only up to $I_{\mathfrak{p}}$. Also we have that

$$Frob_{\mathfrak{p}^\sigma} = \sigma Frob_{\mathfrak{p}} \sigma^{-1}.$$

Let's now state a very important result

Theorem 5.9. (*Chebotarev Density Theorem*) *Let $K \subseteq L$ be a Galois extension of number fields, with $G = \text{Gal}(L/K)$. Let $C \subseteq G$ be a conjugacy class. Then the set*

$$S = \{\mathfrak{p} : \mathfrak{p} \subseteq \mathcal{O}_K \text{ is an unramified prime ideal of } \mathcal{O}_K \text{ s.t. } \text{Frob}_{\mathfrak{p}} \in C\}$$

has density $|C|/|G|$

Remark 5.10. *The density in the theorem is the natural density, namely if S is a set of primes of $\mathcal{O}_K$ we set*

$$d(S) := \lim_{x \rightarrow +\infty} \frac{\#\{\mathfrak{p} : \#(\mathcal{O}_K/\mathfrak{p}) \leq x, \mathfrak{p} \in S\}}{\#\{\mathfrak{p} : \#(\mathcal{O}_K/\mathfrak{p}) \leq x, \mathfrak{p} \text{ prime}\}}.$$

5.3. Galois Representation

Definition 5.11. *An n -dimensional Galois representation is a continuous homomorphism*

$$\rho : G_{\mathbb{Q}} \rightarrow GL_n(K),$$

where K is a topological field, and the topology on $GL_n(K)$ is the one induced by the inclusion $GL_n(K) \hookrightarrow K^{n^2}$.

Two representations ρ, ρ' are said to be *equivalent* if there exists $M \in GL_n(K)$ such that $\rho'(\sigma) = M^{-1}\rho(\sigma)M$ for all $\sigma \in G_{\mathbb{Q}}$

When $K = \mathbb{C}$ we speak of a complex representation, when K is an extension of $\mathbb{Q}_p$, we call ρ a *p -adic Galois representation*.

Remark Since K is chosen to be a topological field, $GL_n(K)$ turns into a topological group. If $\rho : G \rightarrow H$ is a homomorphism of topological groups, to check the continuity of ρ it is enough to check that $\rho^{-1}(V)$ is open in G for every V in a basis of open neighbourhoods of the identity 1_H .

Definition 5.12. (i) Let R be a ring and M be a left R -module. M is called *irreducible* if it does not have any left R -submodules except the zero module and M itself.

(ii) Let $c \in G_{\mathbb{Q}}$ be a complex conjugation. A Galois representation $\rho : G_{\mathbb{Q}} \rightarrow GL_n(K)$ is said to be *odd* if $\det(\rho(c)) = -1$, while is said to be *even* if $\det(\rho(c)) = 1$.

Once we have a Galois representation $\rho : G_{\mathbb{Q}} \rightarrow GL_n(K)$, a natural question is to understand $\rho(Frob_{\mathfrak{p}})$ for some prime $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$. The problem is that $Frob_{\mathfrak{p}}$ is defined only up to $I_{\mathfrak{p}}$, so the notion of $\rho(Frob_{\mathfrak{p}})$ makes sense if and only if $I_{\mathfrak{p}} \subseteq \ker \rho$. Moreover, if $p \in \mathbb{Z}$ is a prime and $\mathfrak{p}, \mathfrak{p}' \subseteq \overline{\mathbb{Z}}$ are two primes lying over p , then $I_{\mathfrak{p}}$ and $I_{\mathfrak{p}'}$ are conjugate in $G_{\mathbb{Q}}$ so that $I_{\mathfrak{p}} \subseteq \ker \rho$ if and only if $I_{\mathfrak{p}'} \subseteq \ker \rho$, since $\ker \rho$ is normal in $G_{\mathbb{Q}}$. Therefore, the following statement makes sense.

Definition 5.13. Let $p \in \mathbb{Z}$ be a prime, $\rho : G_{\mathbb{Q}} \rightarrow GL_n(K)$ be a Galois representation. We say that ρ is *unramified at p* if $I_{\mathfrak{p}} \subseteq \ker \rho$ for some $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ lying over p .

Example 5.14. Let $K = \mathbb{C}$ and $n = 1$, so that $GL_1(\mathbb{C}) = \mathbb{C}^*$. Let χ be a primitive Dirichlet character modulo $N \in \mathbb{N}$. Consider the following diagram

$$\begin{array}{ccc}
 G_{\mathbb{Q}} & & \\
 \pi_N \downarrow & & \\
 Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q}) & \xrightarrow{\cong} & (\mathbb{Z}/N\mathbb{Z})^{\times} \\
 \searrow \rho_{\chi, N} & & \swarrow \chi \\
 & \mathbb{C}^{\times} &
 \end{array} \tag{5.2}$$

where ζ_N is a primitive N -th root of unity and $\rho_{\chi, N}$ is the unique map that makes the diagram commutative. The composition $\rho_{\chi} = \rho_{\chi, N} \circ \pi_N$ yields a complex Galois

representation. In fact, the image of ρ_χ is finite and by Remark ??, the map is continuous, so it suffices to check whether $\rho_\chi^{-1}(1)$ is open. This is certainly true because $\ker \rho_{\chi,N} = \text{Gal}(\mathbb{Q}(\zeta_N)/F)$ for some Galois extension $\mathbb{Q} \subseteq F \subseteq \mathbb{Q}(\zeta_N)$ and hence $\rho_\chi^{-1}(1) = \pi_N^{-1}(\ker \rho_{\chi,N}) = \text{Gal}(F/\mathbb{Q})$, which is open in $G_\mathbb{Q}$.

Conversely, let $\rho : G_\mathbb{Q} \rightarrow \mathbb{C}^*$ be a continuous homomorphism with kernel $\text{Gal}(\overline{\mathbb{Q}}/F)$. By the Kronecker-Weber theorem, we can assume $F = \mathbb{Q}(\zeta_N)$. So we have the same commutative diagram as above, namely ρ is induced by some Dirichlet character modulo N . One can easily show that if ρ factors through $\mathbb{Q}(\zeta_N)$ and $\mathbb{Q}(\zeta_{N'})$, then it factors also through $\mathbb{Q}(\zeta_d)$, where $d = \gcd(N, N')$. Therefore, we may assume that χ is primitive. Thus, we have a one-to-one correspondence between the set of 1-dimensional complex Galois representations and primitive Dirichlet characters modulo N .

Note that the complex conjugation c restricts to the automorphism $\zeta_N \mapsto \zeta_N^{-1}$ and this shows that $\chi(c) = -1$. More generally, an absolute Frobenius element $\text{Frob}_\mathfrak{p}$ lying over a prime $p \nmid N$ maps to $p \pmod{N}$ and so $\chi(\text{Frob}_\mathfrak{p}) = \chi(p)$.

Lemma 5.15. ([?], Prop. 9.3.5) Let K be a finite extension of $\mathbb{Q}_\ell$ for some prime ℓ , let $\rho : G_\mathbb{Q} \rightarrow \text{GL}_n(K)$ be an ℓ -adic Galois representation. Then ρ is equivalent to a Galois representation $\rho' : G_\mathbb{Q} \rightarrow \text{GL}_n(\mathcal{O}_K)$, where $\mathcal{O}_K$ is the ring of integers of K .

Remark 5.16. This lemma helps us find an ideal $\mathfrak{p}$ to form a mod $\mathfrak{p}$ Galois representation (or a residual representation). Note that all mod $\mathfrak{p}$ representations arise this way. Let $\rho : G_\mathbb{Q} \rightarrow \text{GL}(V)$ be a complex or p -adic Galois representation. By the lemma above, we may choose a basis such that $\rho : G_\mathbb{Q} \rightarrow \text{GL}_d(\mathcal{O}_K)$. Let $\mathfrak{p}$ be an ideal lying above p in either $\mathbb{Z}$ or $\mathbb{Z}_p$; then $\mathcal{O}_K/\mathfrak{p}$ is an extension of $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p/p\mathbb{Z}_p \simeq \mathbb{F}_p$. So the composition

$$\bar{\rho} : G_\mathbb{Q} \rightarrow \text{GL}_d(\mathcal{O}_K) \xrightarrow{\text{mod } \mathfrak{p}} \text{GL}_d(\overline{\mathbb{F}}_p)$$

does indeed exist as a continuous Galois representation.

In order to create some natural examples such as Tate module or a p -torsion group of an elliptic curve, we need to restate the definition of Galois representation in the following equivalent way ([?], Exercise 9.3.7) :

Definition 5.17. *Let K be a topological field, and $n \in \mathbb{Z}^+$. An n - dimensional Galois representation V is an $K[G_{\mathbb{Q}}]$ -module. Namely, V is an n -dimensional K -module such that the action*

$$\begin{aligned} G_{\mathbb{Q}} \times V &\rightarrow V \\ (\sigma, v) &\mapsto v^{\sigma} \end{aligned}$$

is continuous.

Two representations V, V' are said to be equivalent if there exists a continuous $K[G_{\mathbb{Q}}]$ -module isomorphism $V \rightarrow V'$.

Proposition 5.18. *The definitions of Galois representations are compatible.*

Proof. First, let $\rho : G_{\mathbb{Q}} \rightarrow GL_n(K)$ be a Galois representation in the sense of the first definition. We can define a $K[G_{\mathbb{Q}}]$ -module structure on K^n through the map

$$\begin{aligned} G_{\mathbb{Q}} \times K^n &\rightarrow K^n \\ (\sigma, v) &\mapsto v^{\sigma} = \rho(\sigma)v \end{aligned}$$

This can be viewed as the composition of two maps

$$\begin{aligned} G_{\mathbb{Q}} \times K^n &\rightarrow GL_n(K) \times K^n \\ (\sigma, v) &\mapsto (\rho(\sigma), v) \end{aligned}$$

and

$$\begin{aligned} GL_n(K) \times K^n &\rightarrow K^n \\ (M, v) &\mapsto Mv \end{aligned}$$

The two maps are continuous, so their composition is also continuous. Therefore, we obtain a Galois representation in the sense of the second definition. Now, suppose that ρ, ρ' are two isomorphic Galois representations. Then there exists $M \in GL_n(K)$ such that $\rho(\sigma) = M^{-1}\rho'(\sigma)M$ for all $\sigma \in G_{\mathbb{Q}}$. We can define the map

$$\begin{aligned} \phi_M : K^n &\rightarrow K^n \\ v &\mapsto Mv \end{aligned}$$

which is clearly continuous. Moreover, for any $\sigma \in G_{\mathbb{Q}}$, one has

$$\phi_M(v^\sigma) = \phi_M(\rho(\sigma)v) = M\rho(\sigma)v = \rho'(\sigma)(Mv) = (Mv)^\sigma = \phi_M(v)^\sigma$$

Conversely, let V be an n -dimensional K -module which is endowed with a continuous action by $G_{\mathbb{Q}}$. Fix a basis $\mathcal{E} = \{e_1, \dots, e_n\} \subseteq V$. Then every $\sigma \in G_{\mathbb{Q}}$ induces an automorphism of V . Hence, we have a map $\rho : G_{\mathbb{Q}} \rightarrow GL_n(K)$ that is a homomorphism, since $G_{\mathbb{Q}}$ acts on V . To show that such a map is continuous, first recall that we are considering $GL_n(K) \hookrightarrow K^{n^2}$ and the topology on $GL_n(K)$ is the induced topology.

Note that to give a continuous map $\rho : G_{\mathbb{Q}} \rightarrow GL_n(K)$ is equivalent to give a continuous map $\rho : G_{\mathbb{Q}} \rightarrow K^{n^2}$ such that $\rho(G_{\mathbb{Q}}) \subseteq GL_n(K)$. Further, it is also equivalent to give n^2 continuous components of the product that make the obvious diagram commutative. Define the map

$$\begin{aligned} \rho_{ij} : G_{\mathbb{Q}} &\rightarrow K \\ \sigma &\mapsto (\rho(\sigma))_{ij} \end{aligned}$$

where $(\rho(\sigma))_{ij}$ is the (i, j) -th entry of $\rho(\sigma)$. We can see easily that $\rho_{ij}(\sigma) = \pi_j(\rho(\sigma)e_i)$, where $\pi_j : K^n \rightarrow K$ is the projection to the j -th component, which is a continuous map. Since the action of $G_{\mathbb{Q}}$ on V is continuous, ρ is continuous as composition of continuous maps.

Now let V' be a n -dimensional K -module which is isomorphic to V as $K[G_{\mathbb{Q}}]$ -module. Fix a basis $\mathcal{F} = \{f_1, \dots, f_n\} \subseteq V'$, and write M for the matrix that represents the isomorphism of V and V' in the bases $\mathcal{E}, \mathcal{F}$. Then we have

$$M(v^\sigma) = (Mv)^\sigma$$

namely, we have $M(\rho(\sigma)v) = \rho'(\sigma)(Mv)$ so that choosing $v = e_i$ for $i = 1, \dots, n$ yields $\rho(\sigma) = M^{-1}\rho'(\sigma)M$ for all $\sigma \in G_{\mathbb{Q}}$.

□

Remark 5.19. *By using this proposition, we can redefine the definition of irreducibility in matrix terms; a representation $G \rightarrow GL_d(K)$ with a field K is irreducible if and only if the matrices in the image does not share any common eigenvectors.*

Definition 5.20. (i) *Let $\rho : G_{\mathbb{Q}} \rightarrow GL_n(K)$ and $\rho' : G_{\mathbb{Q}} \rightarrow GL_m(K)$ be two Galois representations. The direct sum of ρ and ρ' is the representation given by*

$$\begin{aligned} \rho \oplus \rho' : G_{\mathbb{Q}} &\longleftrightarrow GL_{n+m}(K) \\ \sigma &\mapsto \begin{pmatrix} \rho(\sigma) & 0 \\ 0 & \rho'(\sigma) \end{pmatrix} \end{aligned}$$

(ii) *A Galois representation $\rho : G_{\mathbb{Q}} \rightarrow GL_n(K)$ is said to be semisimple if it is isomorphic to a direct sum of irreducible Galois representations.*

Lemma 5.21. *Let $\mathbb{F}$ be a finite field and let $\rho, \rho' : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F})$ be two semisimple Galois representations. If for all but finitely many primes p , where ρ, ρ' are unramified, we have $\text{Trace}(\rho(\text{Frob}_p)) = \text{Trace}(\rho'(\text{Frob}_p))$ and $\text{Det}(\rho(\text{Frob}_p)) = \text{Det}(\rho'(\text{Frob}_p))$, then ρ and ρ' are isomorphic.*

Proof. Since ρ and ρ' are continuous, it suffices to prove the statement of the lemma for $G := \text{Gal}(K/\mathbb{Q})$ where K is some finite Galois extension of $\mathbb{Q}$. Let $g \in G$. By Chebotarev density theorem we have $\sigma = \text{Frob}_p$ (modulo conjugation) for infinitely many primes p . In particular, for a prime p we have $\text{Trace}(\rho(\text{Frob}_p)) = \text{Trace}(\rho'(\text{Frob}_p))$ and $\text{Det}(\rho(\text{Frob}_p)) = \text{Det}(\rho'(\text{Frob}_p))$. So $\rho(\sigma)$ and $\rho'(\sigma)$ have the same characteristic equation. By the Brauer-Nesbitt theorem (see [?], Thm. 30.16), ρ and ρ' are isomorphic. $\square$

5.4. Galois Representations Attached to Elliptic Curves

Let E be an elliptic curve over a number field K . For every integer $n \in \mathbb{Z}$, we denote the subgroup of the n -torsion points over $\overline{\mathbb{Q}}$ by $E[n]$. $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$ module of rank 2 and the group $G_K = \text{Gal}(\overline{K}/K)$ clearly acts on $E[n]$. Indeed, if P_1, P_2 is a basis of $E[n]$, for each element $\sigma \in G_K$ we have

$$\sigma(P_1) = a_{\sigma}P_1 + b_{\sigma}P_2, \quad \sigma(P_2) = c_{\sigma}P_1 + d_{\sigma}P_2$$

If Q_1, Q_2 are arbitrary points of $E[n]$ such that

$$\begin{pmatrix} Q_1 \\ Q_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}.$$

Then by linearity we have

$$\begin{pmatrix} \sigma(Q_1) \\ \sigma(Q_2) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}.$$

Also it can easily be checked that

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

Hence, we have

Theorem 5.22. *The action of G_K on $E[n]$ defines a Galois representation*

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

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

Now fix a prime p . For all n there is a group homomorphism $E[p^{n+1}] \rightarrow E[p^n]$ given by the multiplication by p , which turns $\{E[p^n]\}_{n \in \mathbb{N}}$ into an inverse system. Since the action of G_K is compatible with the transition maps, we have $T_p(E) := \varprojlim E[p^n]$, which is called the *p -adic Tate module of E* . As $T_p(E)$ is isomorphic to $\mathbb{Z}_p$, we have ended up with a 2-dimensional p -adic Galois representation associated to E

$$\rho_{E,p} : G_K \rightarrow GL_2(\mathbb{Z}_p).$$

Theorem 5.23. (*[?], Thm. 9.4.1*) Let p be a prime and E be an elliptic curve over K with conductor N (an ideal in $\mathcal{O}_K$). The Galois representation $\rho_{E,p}$ is unramified at every prime $\lambda \nmid pN$. For any such λ , let $\mathfrak{P} \subset \overline{\mathbb{Z}}$ be any maximal ideal over λ . Then the characteristic equation of $\rho_{E,p}$ is

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

Moreover, the Galois representation $\rho_{E,p}$ is irreducible.

Theorem 5.24. (*Néron-Ogg-Shafarevich*) Let E/K be an elliptic curve and p be a prime. E has good reduction at ℓ if and only if $\rho_{E,p}$ is unramified at ℓ for some prime $p \neq \ell$ if and only if $\rho_{E,p}$ is unramified at ℓ for all primes $p \neq \ell$

5.5. Galois Representations Attached to Modular Forms

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

Theorem 5.25. (*[?], Thm 9.5.4*) Let $f \in S_k(\Gamma_0(N))$ be a normalized eigenform and $K_f = \mathbb{Q}(\{a_n\})$. 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

$$\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \rightarrow GL_2(K_{f,\mathfrak{p}}).$$

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

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

For $k = 2$ the existence of this representation is a consequence of the Eichler-Shimura theory, for which we refer to [?] or to [?], Ch.III. The Eichler-Shimura theory relates a given modular form with a 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 is $K_f = \mathbb{Q}$ this Abelian variety is an elliptic curve.

There exists a decomposition

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

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

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

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

Theorem 5.26. *Let $f \in S_k(N, \epsilon)$ be a normalized eigenform. Let ℓ be a rational prime. For each maximal ideal λ of $\mathcal{O}_{K_f}$ lying over ℓ there is an irreducible 2-dimensional Galois representation*

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

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

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

Given a newform $f \in S_2(N, \epsilon)$ we can also attach a mod ℓ representation to f . Indeed, up to similarity we may assume that the representation $\rho_{f,\lambda}$ maps to $GL_2(\mathcal{O}_{K_k,\lambda})$, hence it reduces modulo the maximal ideal to a representation

$$\bar{\rho}_{f,\lambda} : G_{\mathbb{Q}} \rightarrow GK_2(\mathcal{O}_{K_k,\lambda}/\lambda\mathcal{O}_{K_k,\lambda}) \simeq GL_2(\mathbb{F}_{l^r}).$$

6. FERMAT'S LAST THEOREM

In this chapter, we will develop some arguments and show how to combine these arguments to prove the Fermat's last theorem.

6.1. Irreducibility

Recall that a representation $\bar{\rho}_{E,p}$ is reducible if the vectors in the image $\bar{\rho}_{E,p}(G_{\mathbb{Q}})$ share some common eigenvector and that a p -isogeny $\phi : E \rightarrow E'$ is an isogeny such that the kernel of ϕ has order p . Then the existence of a p -isogeny $\phi : E \rightarrow E'$ defined over $\mathbb{Q}$ is equivalent to the associated representation $\bar{\rho}_{E,p}$ being reducible, where E is an elliptic curve defined over $\mathbb{Q}$. Note that the *mod* p Galois representation $\bar{\rho}_{E,p}$ has an action on $\text{Aut}(E[p]) \simeq GL_2(\mathbb{F}_p)$ in the following way $\bar{\rho}_{E,p}(\sigma) = \phi_{\sigma}$ for all $\sigma \in G_{\mathbb{Q}}$, where

$$\begin{aligned} \phi_{\sigma} : E[p] &\rightarrow E[p] \\ R &\mapsto \sigma(R) \end{aligned}$$

Proposition 6.1. *$E/\mathbb{Q}$ has a rational p -isogeny if and only if $\bar{\rho}_{E,p}$ is reducible.*

Proof. Suppose that E has a rational p -isogeny. Then there exist an isogeny ϕ and an elliptic curve $E'/\mathbb{Q}$ such that $\phi : E \rightarrow E'$ with $|\ker \phi| = p$. Say $\ker \phi = \langle R \rangle$ for some $R \in E[p]$. Since $\ker \phi^{\sigma} = \ker \phi$ for all $\sigma \in G_{\mathbb{Q}}$, there is an element $k_{\sigma} \in \mathbb{F}_p$ such that $\phi_{\sigma}(R) = \sigma(R) = k_{\sigma}R$ for all $\sigma \in G_{\mathbb{Q}}$. Then the matrices of the image $\bar{\rho}_{E,p}(Gal(\overline{\mathbb{Q}}/\mathbb{Q}))$ share same common eigenvector $R \in E[p]$, i.e. $\bar{\rho}_{E,p}$ is reducible.

Conversely, assume that $\bar{\rho}_{E,p}$ is reducible. Then there are elements $k_\sigma \in \mathbb{F}_p$ and $R \in E[p]$ such that $\phi_\sigma(R) = k_\sigma R$ for all $\phi_\sigma \in \bar{\rho}_{E,p}(G_\mathbb{Q})$. Thus we have $|\langle R \rangle| = p$ and $\langle R \rangle$ is $G_\mathbb{Q}$ -invariant, i.e. $\langle R \rangle^\sigma = \langle R \rangle$ for all $\sigma \in G_\mathbb{Q}$. Hence by Theorem ?? above we can construct a rational p -isogeny $\phi : E \rightarrow E'$. $\square$

Theorem 6.2 (Mazur). *Let $E/\mathbb{Q}$ be an elliptic curve with j -invariant j and let p be a rational prime. Then E does not have any p -isogenies if one of the following conditions hold:*

- (i) $p = 11$ or $p \geq 17$ and the pair (p, j) has no corresponding entry in the following table,
- (ii) E has a rational 2-torsion point, $p \geq 7$ and

$$(p, g) \neq (7, -3^3.5^3), (7, 3^3.5^3.17^3),$$

- (iii) $p \geq 5$, E is semistable and all 2-torsion points are rational,
- (iv) $p \geq 11$ and E is semistable.

Table 6.1. Pairs (p, j) corresponding to rational isogenies.

p	j
11	$-2^{15}, -11^2, -11.131^3$
17	$-17.373^3/2^{17}, -17^2.101^3/2$
19	$-2^{15}.3^3$
37	$-7.11^3, -7.137^3.2083^3$
43	$-2^{18}.3^3.5^3$
67	$-2^{15}.3^3.5^3.11^3$
163	$-2^{18}.3^3.5^3.23^3.29^3$

Remark 6.3. *Theorem ?? is mainly obtained from knowledge of rational points on modular curves. For the proof we refer to [?].*

6.2. Modularity

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

Definition 6.4. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N . Then E is said to be modular if there exists a newform f of level N such that $a_p(E) = c_p$ for all primes, where $a_p(E) = p + 1 - |\overline{E}(\mathbb{F}_p)|$*

Recall that we have stated above two theorems, Theorem ?? and Theorem ?? about Galois representations attached to elliptic curves over a number field and modular forms f with $K_f = \mathbb{Q}(\{c_n\})$. These two theorems give us very useful arithmetic information about $\overline{\rho}_{E,p}$ and $\rho_{f,p}$. Let us state them for the cases E is an elliptic curve over $\mathbb{Q}$ and $f \in S_k(\Gamma_0(N))^{new}$ with $K_f = \mathbb{Q}$.

Theorem 6.5. *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N and let ℓ, p be primes. If $\ell \nmid pN$, then the Galois representation $\overline{\rho}_{E,p}$ is unramified at ℓ and*

$$\begin{aligned} \text{Trace}(\overline{\rho}_{E,p}(\text{Frob}_\ell)) &\equiv a_\ell(E) \pmod{p} \\ \text{Det}(\overline{\rho}_{E,p}(\text{Frob}_\ell)) &\equiv \ell \pmod{p}. \end{aligned}$$

Furthermore, if $\rho' : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_p)$ is another Galois representation satisfying the conditions above, then the semi-simplifications of ρ' and $\overline{\rho}_{E,p}$ are isomorphic.

Remark 6.6. Let V be a finite-dimensional vector space over $\overline{\mathbb{Q}}_\ell$, and $\rho : G_{\mathbb{Q}} \rightarrow GL(V)$ be an ℓ -adic Galois representation. Let $0 \subset V_0 \subset V_1 \subset \dots \subset V_m = V$ be a filtration of subrepresentations, so that each V_i/V_{i-1} is an irreducible Galois representation. The semi-simplification of V is $V^{ss} := \bigoplus_{i=1}^m V_i/V_{i-1}$. For details see [?].

Theorem 6.7. Let f be a rational newform (i.e. $K_f = \mathbb{Q}$) of level N , and p be a prime. Then there exists a semisimple Galois representation

$$\rho_{f,p} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_p)$$

such that for all primes ℓ with $\ell \nmid pN$ the Galois representation $\rho_{f,p}$ is unramified at ℓ , and

$$\text{Trace}(\rho_{f,p}(\text{Frob}_\ell)) \equiv c_\ell \pmod{p}$$

$$\text{Det}(\rho_{f,p}(\text{Frob}_\ell)) \equiv \ell \pmod{p}.$$

Furthermore, if $\rho' : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_p)$ is another semisimple Galois representation satisfying the conditions above, then ρ' and $\rho_{f,p}$ are isomorphic.

Theorem 6.8 (Modularity). Let $E/\mathbb{Q}$ be an elliptic curve with conductor N . Then there exists a normalized eigenform $f = q + \sum_{n \geq 2} c_n q^n \in S_2(\Gamma_0(N))$ such that $c_n \in \mathbb{Z}$ and if $p \nmid N$ is a prime, then $a_p(E) = c_p$.

The modularity theorem of elliptic curves over $\mathbb{Q}$ can be seen as a converse of the following theorem due to Eichler-Shimura and was proven by Andrew Wiles [?] (with help of Richard Taylor) [?] for semistable elliptic curves. Christophe Breuil, Brian Conrad, Fred Diamond and Richard Taylor [?] later proved the modularity theorem for all elliptic curves over $\mathbb{Q}$.

Theorem 6.9. (*Eichler-Shimura*) Let f be newform of level N . If f is rational, then there exists an elliptic curve $E/\mathbb{Q}$ of conductor N such that $a_p(E) = c_p$ for all primes p .

Proof. See [?], Ch. 8. □

Example 6.10. Let $E : y^2 + xy + y = x^3 + x^2 - 10x - 10$. Then one can compute the arithmetic invariants of E , $\Delta_E = 3^4 \cdot 5^4$ and $N_E = 3 \cdot 5 = 15$ and, by the modularity theorem, the corresponding modular form is

$$f = q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 + q^9 - q^{10} \dots$$

where $c_2 = -1, c_3 = -1$, and $c_5 = 1$. Note that we have

$$\begin{aligned} \overline{E}(\mathbb{F}_2) &= \{\infty, (\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0})\}, \\ \overline{E}(\mathbb{F}_3) &= \{\infty, (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{2}, \overline{0})\}, \\ \overline{E}(\mathbb{F}_5) &= \{\infty, (\overline{0}, \overline{0}), (\overline{0}, \overline{4}), (\overline{4}, \overline{0}), (\overline{4}, \overline{4})\} \end{aligned}$$

Hence we have $a_2(E) = 2 + 1 - 4 = -1 = c_2$, $a_3(E) = 3 + 1 - 5 = -1 = c_3$, and $a_5(E) = 5 + 1 - 5 = 1 = c_5$, as we expect.

Definition 6.11. Let $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F})$ be a Galois representation, where $\mathbb{F}$ is a finite field of characteristic p . Suppose that ρ is irreducible, odd and $\det \rho$ is cyclotomic. Then ρ is called modular of level N if there exists a newform $f \in S_2(\Gamma_0(N))$ and a prime $\mathfrak{p}$ of $\mathcal{O}_{K_f}$ above p such that $\rho \sim \rho_{f, \mathfrak{p}}$.

Theorem 6.12 (*Modularity for Galois representations*). *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N . Then for some newform $f \in S_2(\Gamma_0(N))$ with number field $K_f = \mathbb{Q}$, we have*

$$\rho_{f,p} \sim \bar{\rho}_{E,p}$$

for all primes p .

Proof. Let E be an elliptic curve over $\mathbb{Q}$ with conductor N . By the modularity theorem, there exists a newform f of level N such that $a_p(E) = c_p$ for all primes, in particular $\mathcal{O}_{K_f} = \mathbb{Z}$. Then, by Theorem ?? and Theorem ??, we get semisimple (recall $\bar{\rho}_{E,p}$ is irreducible by Theorem ??) Galois representations $\bar{\rho}_{E,p}, \rho_{f,p} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_p)$ satisfying $\text{Trace}(\bar{\rho}_{E,p}(\text{Frob}_{\ell})) = \text{Trace}(\rho_{f,p}(\text{Frob}_{\ell}))$ and $\text{Det}(\bar{\rho}_{E,p}(\text{Frob}_{\ell})) = \text{Det}(\rho_{f,p}(\text{Frob}_{\ell}))$ for all primes $\ell \nmid pN$. Now by Lemma ??, we have that $\rho_{f,p} \sim \bar{\rho}_{E,p}$ $\square$

Remark 6.13. *There are several other equivalent versions of the modularity theorem. Above we state two versions: the first one is the more arithmetic and the other uses Galois representations.*

6.3. Level-Lowering

If f corresponds to E via Modularity theorem, then $N_f = N_E$. Sometimes it is possible, due to Ribet's work [?], to replace f by another eigenform of smaller level which has the same *mod* p representation. This section is based on [?].

Definition 6.14 (Arises mod p). Let $E/\mathbb{Q}$ be an elliptic curve and $f = q + \sum_{n \geq 2} c_n q^n$ be a newform with $K_f = \mathbb{Q}(\{c_n\})$. We say that E arises modulo p from f , if there is a prime ideal $\mathfrak{P}|p$ of $\mathcal{O}_K$ such that $a_\ell(E) \equiv c_\ell \pmod{\mathfrak{P}}$, for almost all primes ℓ , denoted by $E \sim_p f$.

Additionally, we have the following proposition to be a little more precise.

Proposition 6.15. Suppose $E \sim_p f$. Then there is some prime ideal $\mathfrak{P}|p$ of K_f such that for all primes k

- (i) if $\ell \nmid pNN'$, then $a_\ell(E) \equiv c_\ell \pmod{\mathfrak{P}}$, and
- (ii) if $\ell \nmid pN'$ and $\ell || N$, then $\ell + 1 \equiv \pm c_\ell \pmod{\mathfrak{P}}$.

Remark 6.16. Here $\ell || N$ means that ℓ divides N , but $\ell^2 \nmid N$, so one can easily deduce that E has multiplicative reduction at ℓ .

Now we can state a simplified case of Ribet's level-lowering theorem.

Theorem 6.17 (Ribet). Assume we have the following :

- $p \geq 3$
- $E/\mathbb{Q}$ is modular with N and $\Delta_{\min} = \Delta$
- $N_p = N / \prod_{\substack{\ell || N, \\ p | \text{ord}_\ell(\Delta)}} \ell$
- E does not have any p -isogenies (or $\bar{\rho}_{E,p}$ is irreducible).

Then there exists a newform of level N_p such that $E \sim_p f$.

Remark 6.18. (i) For historical reasons we keep the modularity hypothesis.

(ii) At level N_p , there may be rational and non-rational newforms and some of the non-rationals can be defined over number fields.

Example 6.19. Consider the elliptic curve

$$E : y^2 + y = x^3 + 7x - 11$$

with Cremona reference 115A1. The minimal discriminant and conductor are respectively

$$\Delta_{\min} = -5^5 \cdot 23 \quad \text{and} \quad N = 5 \cdot 23$$

The curve E has no rational isogenies. Hence we may apply Ribet's theorem for $p = 5$. Then we have

$$N_p = N / \prod_{\substack{\ell \mid N, \\ p \mid \text{ord}_\ell(\Delta)}} = \frac{5 \cdot 23}{5} = 23.$$

Hence, $E \sim_5 f$ for some newform at level $N_p = 23$. Note that there are two newforms at that level, all of which are not rational. Denote these newforms, where **lmfdb Database** labels are 23.2a.a, 23.2.c.a, by f_1 and f_2 respectively. Note that $K_{f_1} = \mathbb{Q}(\sqrt{5})$ and $K_{f_2} = \mathbb{Q}(\zeta_{22})$, and that $c_7(f_1) = 1 + \sqrt{5}$ and $c_7(f_2) = -\zeta_{22} + \zeta_{22}^2 - \zeta_{22}^3 - \zeta_{22}^5 + \zeta_{22}^6 - \zeta_{22}^7$. One can also compute that $a_7(E) = 7 + 1 - |\overline{E}(\mathbb{F}_7)| = 1$. So by Proposition ?? (i), we must have $a_7(E) \equiv c_7(f_i) \pmod{\mathfrak{P}}$ for some ideal $\mathfrak{P} \mid 5$ in $\mathcal{O}_{K_{f_i}}$ and for some $i \in \{1, 2\}$.

Note that $\mathcal{O}_{K_{f_2}} = \mathbb{Z}[\zeta_{22}]$ and one can compute (using, for example, **MAGMA**) that $5\mathcal{O}_{K_{f_2}} = \mathfrak{P}_1 \mathfrak{P}_2$ for some ideals in $\mathcal{O}_{K_{f_2}}$. We also have that

$$c_7(f_2) = -\zeta_{22} + \zeta_{22}^2 - \zeta_{22}^3 - \zeta_{22}^5 + \zeta_{22}^6 - \zeta_{22}^7 \equiv -1 - \zeta_{22} + 2\zeta_{22} \pmod{\mathfrak{P}_j}$$

for all $j = 1, 2$. Hence we get $a_7(E) \not\equiv c_7(f_2) \pmod{\mathfrak{P}_j}$ for all $j = 1, 2$. So $E \sim_p f_1$. Indeed, $\mathcal{O}_{K_{f_1}} = \mathbb{Z} \left[\frac{1 + \sqrt{5}}{2} \right]$ and $5\mathcal{O}_{K_{f_1}} = \mathfrak{P}^2$, where $\mathfrak{P} = (\sqrt{5})$. Therefore,

$$a_7(E) \equiv c_7(f_1) \pmod{\mathfrak{P}},$$

as expected.

6.4. Frey Curves and Proof of Fermat's Last Theorem

Let $A, B, C \in \mathbb{Z}$ with $A + B + C = 0$. Then the *Frey curve* is

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

with the arithmetic invariants $\Delta = 2^4(ABC)^2$, $c_4 = 16(A^2 - BC) = 16(B^2 - AC) = 16(C^2 - AB)$, and $j = c_4^3/\Delta$. The Frey curve E satisfies the following properties which are crucial to prove Fermat's last theorem ([?], Sec. 7).

- $ABC \neq 0$ implies that $\Delta \neq 0$, so $E_{A,B,C}$ is smooth.
- If $A \equiv -1 \pmod{4}$ and $B \equiv 0 \pmod{32}$, $E_{A,B,C}$ is semistable with $N = \text{rad}(ABC)$, i.e. it does not have any additive reduction.
- $\Delta_{\min}$ can be written in the form $\Delta = CD^r$, where D depends on the solution, C depends only on the equation itself.
- E has multiplicative reduction at prime ℓ dividing D , i.e. if $\ell|D$, then $\ell||N$.

Theorem 6.20. *Let $p \geq 5$. Then $x^p + y^p = z^p$ has no integer solutions with $xyz \neq 0$.*

Proof. Suppose that (a, b, c) is a solution with $abc \neq 0$ and that they are relatively prime. By replacing a, b, c if necessary, we may assume that $2|b$ and $a^p \equiv -1 \pmod{4}$. The corresponding Frey curve is

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

with $\Delta = 16(abc)^{2p}$. In order to get the minimal discriminant, we may use the Tate's algorithm (cf. Appendix ??).

The change of coordinates $x = 4X$, $y = 8Y + 4X$ yields another equation

$$Y^2 + XY = X^3 + \frac{b^p - a^p - 1}{4}X^2 - \frac{(ab)^{2p}}{16}X.$$

Hence, we have the minimal discriminant of the Frey curve and the conductor as follows

$$\Delta_{min} = 2^{-8}(abc)^{2p}, \quad \text{and } N = \prod_{\ell|abc} \ell.$$

Then we have $N_p = N / \prod_{\substack{\ell|N, \\ p|ord_\ell(\Delta)}} \ell = 2$.

Since N is square-free, E is semistable. Also we have

$$E(\mathbb{Q})[2] = \{\mathcal{O}, (0, 0), (a^p, 0), (0, -b^p)\},$$

so all 2-torsion points are rational. Thus, by Theorem ??, E does not have any p -isogenies.

Applying Theorem ??, we can conclude that there is a newform f of level $N_p = 2$ such that $E \sim_p f$, since there is no newform at this level (by Proposition ??) we get a contradiction.

□

Remark 6.21. *The tools that we have mentioned so far can be used to deal with some generalizations of Fermat-type equations. For instance, consider the equation $x^p + 2^\alpha y^p = z^p$, with $p \geq 5$ and $\alpha \geq 2$. Assume that (a, b, c) is a primitive non-trivial solution to this equation. Associate the following Frey curve*

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

Then applying the level-lowering theorem, we end up with a newform at level $N_p \in \{1, 2, 8\}$. Since there are no newforms at these levels, we get the result.

Note that for the case $\alpha = 1$, we have some non-trivial solutions $(\pm 1, 1, 1)$. But these are the only non-trivial solutions. For the proof of the case $\alpha = 1$ see [?], for the case $\alpha \geq 2$ see [?].

Since there are limited number of levels that newforms does not exists, this method have some limitations. Therefore, we need to develop some new tools or improve what we have got.

7. SYMPLECTIC METHOD

After Wiles' completion of the proof of FLT, the strategy called the *modular approach* have been strengthened and several mathematicians have achieved great success in solving other equations.

The symplectic method is due to Halberstadt and Kraus [?] and it is a way to show that, for odd pairwise coprime integers a, b, c , the generalized Fermat equation $ax^p + by^p + cz^p = 0$ has only trivial integer solutions for a dense subset of the set of prime numbers. The reason for the name is that the method is based on the symplectic behaviour of isomorphic Galois representations. An isomorphism of Galois representations on the p -torsion points of two elliptic curves is called *symplectic*, if it respects the Weil pairing.

In this chapter, first we will define *Weil pairing* and *Tate curve* based on [?] and [?]. Then we state a numerical example (the equation $x^p + 7y^p = 3z^p$) to show how modular approach can be extended to generalized Fermat equations and give the proof of the following theorem.

Theorem 7.1 (Halberstadt-Kraus (2002)). *Let a, b, c be odd pairwise coprime integers. Then there is a set of primes $\mathcal{P} = \mathcal{P}(a, b, c)$ of positive density such that if $p \in \mathcal{P}$, then the equation $ax^p + by^p + cz^p = 0$ has only trivial integer solutions.*

7.1. Weil Pairing

Let E be an elliptic curve over K with the Weierstrass form

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

Let f be a function in $\overline{K}(E) = \overline{K}[x, y]/(y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6)$. We then define the divisor group in the following way.

Definition 7.2. *The divisor group of an elliptic curve E , denoted by $\text{div}(E)$, is the free abelian group generated by the points of E . The divisor $D \in \text{div}(E)$ is a formal sum*

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

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

$$\text{div}(f) = \sum_{P \in E} \text{ord}_P(f)P.$$

Using the following theorem we may have a more practical approach to divisors.

Theorem 7.3. (*[?], III, Thm. 3.5*) *Let E be an elliptic curve, and $D = \sum n_i(P_i)$ be a divisor of E . Then D is the divisor of a function in $\overline{K}(E)^\times$ if and only if $\sum n_i = 0$ and $\sum [n_i]P_i = \mathcal{O}$.*

Note that the first sum is in integers, while the second is an addition on the curve E . In order to define the Weil pairing, we need the following example of a divisor.

Example 7.4. *Let $T \in E[m]$ and $T' \in E(\overline{K})$ be such that $mT' = T$ for some $m \in \mathbb{Z}$. By Theorem ??, there exists $g_T \in K(E)^\times$ such that*

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

is the divisor of g_T .

Note that in the example we have $g_T(X + S)^m = g_T(X)^m$ for all $S \in E[m]$ and $X \in E$. Now we can define the Weil pairing denoted by $\widehat{e}$.

Definition 7.5. *We define the Weil pairing $\widehat{e} : E[m] \times E[m] \rightarrow \mu_m$, where μ_m is the set of m -th roots of unity, by setting*

$$\widehat{e}(S, T) = \frac{g_T(X + S)}{g_T(X)},$$

where $X \in E$ is any point such that $g_T(X + S)$ and $g_T(X)$ are both well-defined and non-zero.

Theorem 7.6. (*[?], Prop. 7.4.1*) *The Weil pairing $\widehat{e}$ has the following properties.*

- *Bilinear:*

$$\widehat{e}(s_1 + s_2, T) = \widehat{e}(s_1, T)\widehat{e}(s_2, T)$$

$$\widehat{e}(S, T_1 + T_2) = \widehat{e}(S, T_1)\widehat{e}(S, T_2)$$

for all $S, S_1, S_2, T, T_1, T_2 \in E[m]$.

- *Alternating :* $\widehat{e}(T, T) = 1$, for all $T \in E[m]$.
- *Non-degenerate:* if all $S \in E[m]$, $\widehat{e}(S, T) = 1$, then $T = \mathcal{O}$.
- *Galois invariant:* $\widehat{e}(S, T)^\sigma = \widehat{e}(S^\sigma, T^\sigma)$, for all $\sigma \in \text{Gal}(\overline{K}/K)$, $S, T \in E[m]$.

We also need the following lemma and definition.

Lemma 7.7. (*[?], Pg. 30*) *Let $E/\mathbb{C}$ be an elliptic curve associated to the lattice $\Lambda = w_1\mathbb{Z} \oplus w_2\mathbb{Z}$. On*

$$E[m] = m^{-1}\Lambda/\Lambda \subset \mathbb{C}/\Lambda$$

the Weil pairing is given by the following formula

$$\widehat{e}\left(\frac{aw_1 + bw_2}{m}, \frac{cw_1 + dw_2}{m}\right) = e^{2\pi i(ad-bc)/m}.$$

Definition 7.8. Let $\Psi : E[p] \rightarrow E'[p]$ be a $G_{\mathbb{Q}}$ -module isomorphism, hence there is an element $r(\Psi) \in \mathbb{F}_p^*$ such that for all $P, Q \in E[p]$ the Weil pairing satisfies

$$\widehat{e}(\Psi(P), \Psi(Q)) = \widehat{e}(P, Q)^{r(\Psi)}.$$

We say that Ψ is a symplectic isomorphism if $r(\Psi)$ is a square modulo p .

7.2. Tate Curve

One can see that an elliptic curve defined over $\mathbb{C}$ has a parametrization $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$ via the uniformization theorem. Suppose we replace $\mathbb{C}$ by $\mathbb{Q}_p$ and endeavor to an elliptic curve $E/\mathbb{Q}_p$ by a group of the form $\mathbb{Q}_p/\Lambda$. Unfortunately, this approach immediately fails, because $\mathbb{Q}_p$ has no non-trivial lattices. In [?] Tate gave the alternative description $\mathbb{C}^*/q^{\mathbb{Z}}$ for elliptic curves over $\mathbb{C}$. Now the analogous situation over $\mathbb{Q}_p$ is much more promising, since $\mathbb{Q}_p^*$ has lots of discrete subgroups. For example, any $q \in \mathbb{Q}_p^*$ with $|q| < 1$ defines the discrete subgroup

$$q^{\mathbb{Z}} = \{q^n : n \in \mathbb{Z}\}.$$

More generally, one can work over any p -adic field K , i.e. a finite extension $K/\mathbb{Q}_p$. The Tate curve helps us characterize the ramification of a reduced representation attached an elliptic curve over a number field.

Let K be a local field with the valuation v , which we can imagine as the localization at some prime $\mathfrak{p}$ of a number field. For any $q \in K^*$ with $v(q) < 1$, 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 7.9. (*[?], V, Thm. 3.1*) *Let $q \in K^*$ with $v(q) < 1$. There is an elliptic curve E_q/K and a v -analytic isomorphism $\phi : \overline{K}^*/q^{\mathbb{Z}} \rightarrow E_q(\overline{K})$.*

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 $u \in \overline{K}^*$ and $\sigma \in G_K$. In particular, ϕ induces an isomorphism between $L^*/q^{\mathbb{Z}}$ and $E(L)$ 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,

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

It is clear from this expression that $v(j(E_q)) = -v(q) > 1$, hence a necessary condition for an elliptic curve E to be isomorphic over $\overline{K}$ to an E_q is $v(j(E)) > 1$. This condition is also sufficient, and moreover for any j such that $v(j) > 1$ there is 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

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

attached to a Weierstrass equation for E . It is straightforward to see that $\gamma(E/K)$ is well-defined as an element of K^*/K^{*2} , since for any other Weierstrass equation we have $c'_4/c'_6 = u^2 c_4/c_6$ with $u \in K^*$.

Theorem 7.10. (*Uniformization theorem*) Let E/K be an elliptic curve with $v(j(E)) > 1$ and let $\gamma(E/K)$ be defined as above.

(i) The following are equivalent.

- (a) E is isomorphic to E_q over K .
- (b) E has split multiplicative reduction.
- (c) $\gamma(E/K) = 1$.

(ii) Suppose $\gamma(E/K) \neq 1$. Note that then $L = K(\sqrt{\gamma(E/K)})$ is a quadratic extension. Let $\chi : G_K \rightarrow G_{L/K} \rightarrow \{\pm 1\}$ be the quadratic character associated to the extension L/K . Then there is an isomorphism $\psi : E \rightarrow E'$ over L such that $\psi(\sigma(P)) = \chi(\sigma)\sigma(\psi(P))$ for all $\sigma \in G_K$ and $P \in E$.

For the proof we refer to [?], V, Lem.5.2.

In the case (2), the relation between E_q and E 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

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

and, to simplify the notation say $\gamma = \gamma(E/K)$. Then $E \otimes \chi$ has an equation

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

Before giving the proof the Theorem ??, we need to prove the following two lemmas.

Lemma 7.11 (Halbestadt-Kraus). *Let E and E' be elliptic curves over $\mathbb{Q}$ with minimal discriminants Δ_E and $\Delta_{E'}$, and p be a prime such that $E[p]$ and $E'[p]$ are isomorphic as $G_{\mathbb{Q}}$ -modules. Suppose that E and E' have multiplicative reduction at $\ell \neq p$ such that $p \nmid \text{ord}_{\ell}(\Delta_E), \text{ord}_{\ell}(\Delta_{E'})$. Then we have*

- (i) $p \nmid \text{ord}_{\ell}(\Delta_{E'})$,
- (ii) The following statements are equivalent:
 - (a) the isomorphism between the $G_{\mathbb{Q}}$ -modules is symplectic,
 - (b) $\text{ord}_{\ell}(\Delta_E)/\text{ord}_{\ell}(\Delta_{E'})$ is a square modulo p .

Proof. Let L denote the maximal unramified extension $\mathbb{Q}^{un}$ of the local field $\mathbb{Q}_{\ell}$. Both E and E' have multiplicative reduction at ℓ , so their j -invariants are not integers in L . We deduce from Theorem ?? that E is uniformized over $\bar{L}$ by the Tate curve for some $q \in L$ where q has valuation $a = -\text{ord}_{\ell}(j_E) = \text{ord}_{\ell}(\Delta_E)$. The same is true for E' with a q' in L of valuation $a' = \text{ord}_{\ell}(\Delta_{E'})$. The isomorphism between $E[p]$ and $E'[p]$ as $G_{\mathbb{Q}}$ -modules and the uniformizations provide a $\text{Gal}(\bar{L}/L) = G_L$ -module isomorphism Ψ between $E[p]$ of $\bar{L}^*/q^{\mathbb{Z}}$ and $E'[p]$ of $\bar{L}^*/q'^{\mathbb{Z}}$.

Now we look at how G_L and Ψ act on a basis of $E[p]$ using [?], Prop 6.1. We choose and fix an embedding $L \hookrightarrow \mathbb{C}$. Since L contains a p -th root of unity, we can choose and fix a primitive root of unity ζ_p such that ζ_p is mapped to $e^{2\pi i/p}$ under the embedding. We can also fix $\gamma \in \bar{L}$, a p -th root of q . Then $\{\zeta_p q^{\mathbb{Z}}, \gamma q^{\mathbb{Z}}\}$ forms a basis for $E[p]$. If G_L acts transitively in the p -th conjugates $\{\zeta_p^j \mid 1 \leq j < p\}$, then there exists a $\sigma \in G_L$ such that $\sigma(\gamma) = \zeta_p \gamma$. The corresponding matrix to σ is

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

since G_L fixes $\zeta_p \in L$. So G_L acts transitively on $E[p]$ if and only if $\gamma \in L$, i.e. $p \mid a = \text{ord}_\ell(q) = \text{ord}_\ell(\Delta_E)$. The same holds for $E'[p]$ and a' . Hence, since $p \nmid \text{ord}_\ell(\Delta_E)$ and the Galois modules are isomorphic, it follows that $p \nmid \text{ord}_\ell(\Delta_{E'})$, which concludes the proof of (i).

Now we will look at how Ψ acts on the basis. Since $p \nmid aa'$, there exist $n, m \in \mathbb{Z}$ such that $a' = na + mp$. Since $\text{ord}_\ell(q') = a'$, and $\text{ord}_\ell(q^n \ell^{mp}) = na + mp$, we have that $q'/q^n \ell^{mp}$ is a unit in L , so $\text{ord}_\ell(q'/q^n \ell^{mp}) = 1$. Therefore, it has a p -th root $\alpha \in L$. Now we set $\gamma' = \gamma^n \ell^{mp} \alpha$. Then

$$\gamma'^p = \gamma^{np} \ell^{mp} \alpha^p = q^n \ell^{mp} q' / q^n \ell^{mp} = q'.$$

So γ' is a p -th root of q' . Hence, $\{\zeta_p q'^{\mathbb{Z}}, \gamma' q'^{\mathbb{Z}}\}$ is a basis for $E'[p]$. Note that since Ψ is compatible with G_L , we have, for all $g \in G_L$

$$\Psi(\zeta_p q^{\mathbb{Z}})^g = \Psi((\zeta_p q^{\mathbb{Z}})^g) = \Psi(\zeta_p q^{\mathbb{Z}}).$$

Therefore, the matrix of Ψ with respect to the basis $\{\zeta_p q^{\mathbb{Z}}, \gamma q^{\mathbb{Z}}\}$ is upper triangular, say $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Also note that $\sigma(\gamma') = \sigma(\gamma)\sigma(\ell^m \alpha) = \zeta_p^n \gamma^n \ell^m \alpha = \zeta_p^n \gamma'$, as $\ell^m \alpha \in L$. Thus, compatibility between Ψ and σ can be written in matrix terms:

$$\begin{pmatrix} a & a+b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b+nd \\ 0 & d \end{pmatrix}.$$

So we can deduce that $a = nd$.

Now we look at the Weil pairing. Recall that it is a bilinear alternating satisfying the following identities on $E[p]$ and $E'[p]$ respectively, since γ, ζ_p correspond to $w_1/p, w_2/p$ in the embedding $L \hookrightarrow \mathbb{C}$, $\widehat{e}(\gamma q^{\mathbb{Z}}, \zeta_p q^{\mathbb{Z}}) = \zeta_p = \widehat{e}'(\gamma q'^{\mathbb{Z}}, \zeta_p q'^{\mathbb{Z}})$.

Suppose now that Ψ is symplectic. Then

$$\begin{aligned}\zeta_p = \widehat{e}(\gamma q^{\mathbb{Z}}, \zeta_p q^{\mathbb{Z}}) &= \widehat{e}'(\Psi(\gamma q^{\mathbb{Z}}), \Psi(\zeta_p q^{\mathbb{Z}})) \\ &= \widehat{e}'(\zeta_p^b \gamma^d q^{\mathbb{Z}}, \zeta_p^a q^{\mathbb{Z}}).\end{aligned}$$

Now by properties of Weil pairing we have

$$\widehat{e}'(\zeta_p^b \gamma^d q^{\mathbb{Z}}, \zeta_p^a q^{\mathbb{Z}}) = \widehat{e}'(\gamma q^{\mathbb{Z}}, \zeta_p q^{\mathbb{Z}})^{ad} = \zeta_p^{ad}.$$

Thus $\zeta_p = \zeta_p^{ad}$, so $ad \equiv 1 \pmod{p}$. Since $a = nd$, it follows that $nd^2 \equiv 1 \pmod{p}$, which tells us that n is a square modulo p . Now $\text{ord}_\ell(\Delta_{E'}) = a' = na + mp$. So $\text{ord}_\ell(\Delta_{E'})$ is a square modulo p if and only if $\text{ord}_\ell(\Delta_E)$ is a square modulo p . Hence their quotient is a square modulo p .

Coversely, if $n = \text{ord}_\ell(\Delta_{E'})/\text{ord}_\ell(\Delta_E)$ is square modulo p , then there exists an $r \in \mathbb{Z}$ such that $r^2 nd^2 \equiv 1 \pmod{p}$. So Ψ^r is a symplectic isomorphism due to the following equalities

$$\begin{aligned}\widehat{e}'(\Psi^r(\gamma q^{\mathbb{Z}}), \Psi^r(\zeta_p q^{\mathbb{Z}})) &= \widehat{e}'(\zeta_p^w \gamma^{rd} q^{\mathbb{Z}}, \zeta_p^{ra} q^{\mathbb{Z}}) \\ &= \zeta_p^{adr^2} = \zeta_p^{nd^2 r^2} = \zeta_p,\end{aligned}$$

where $w \in \mathbb{Z}$. Since $\zeta_p = \widehat{e}(\gamma q^{\mathbb{Z}}, \zeta_p q^{\mathbb{Z}})$, we have

$$\widehat{e}(\gamma q^{\mathbb{Z}}, \zeta_p q^{\mathbb{Z}}) = \widehat{e}'(\Psi^r(\gamma q^{\mathbb{Z}}), \Psi^r(\zeta_p q^{\mathbb{Z}})).$$

□

Lemma 7.12. *Let $a, n \geq 1$ be positive integers with $(a, n) = 1$. Then the set $\mathcal{Q} = \{p \mid p \text{ is a prime } p \equiv a \pmod{n}\}$ has positive density.*

Proof. Let ζ_n be a primitive n^{th} root of unity, $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta_n)$. Since L/K is a cyclotomic Galois extension, $\text{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^*$, where the isomorphism is identified by an element $a \in (\mathbb{Z}/n\mathbb{Z})^*$ and the unique automorphism of L/K that maps ζ_n^k to ζ_n^{ak} for all k .

If $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ lying over p such that $\sigma \in \text{Gal}(L/K)$ satisfies $\sigma(\alpha) = \alpha^{\text{Norm}(p\mathbb{Z})} \pmod{\mathfrak{P}}$, we must have $\sigma(\zeta_n^k) = \zeta_n^{pk} \pmod{\mathfrak{P}}$ for all k . So long as $p \nmid n$, the ideal $p\mathbb{Z}$ does not ramify in L , so $\left[\frac{L/K}{p\mathbb{Z}}\right] = \bar{p} \in \text{Gal}(L/K)$, where $\bar{p}$ is the class of p modulo n . Thus, $\left[\frac{L/K}{p\mathbb{Z}}\right] = a$ if and only if $p \equiv a \pmod{n}$. By Chebotarev Density theorem this set has positive density.

□

Theorem 7.13. *Let $p \geq 5$ be a prime. Then there is a set of primes $\mathcal{P}$ that has positive density such that if $p \in \mathcal{P}$, then the equation*

$$x^p + 7y^p + 3z^p = 0$$

has no non-trivial integer solutions.

Proof. Assume that (x, y, z) is a non-trivial solution of the equation. Without loss of generality we may assume that

$$x^p \equiv -1 \pmod{4} \text{ and } 2 \text{ divides } 7y^p.$$

Then our associated Frey curve is

$$E : Y^2 = X(X - x^p)(X + 7y^p)$$

where the minimal discriminant is $\Delta_E = \Delta_{\min}(E) = 2^{-8}21^2(xyz)^{2p}$ and the conductor is $N = \prod_{\substack{\ell \mid 21xyz, \\ \ell \text{ prime}}} \ell$. So we have $N_p = N / \prod_{\substack{\ell \mid N, \\ p \mid \text{ord}_\ell(\Delta_E)}} \ell = 42$.

Since N is squarefree, E is semistable. Also note that all 2-torsion points are rational. Thus by Theorem ??, E does not have any p -isogenies. Hence by Theorem ??, $E \sim_p f$ for some newform f of weight 2 of level 42.

There is only one such newform over $\mathbb{Q}$ and it has integer coefficients. So Eichler-Shimura theory provides an elliptic curve E' over $\mathbb{Q}$ of conductor 42 with the Weierstrass equation

$$E' : y^2 + xy + y = x^3 + x^2 - 4x + 5,$$

where $\Delta_{E'} = -2^8 \cdot 3^2 \cdot 7$. So $E \sim_p E'$. Using Lemma ??, we get

- $\ell = 2$

$$\frac{\text{ord}_2(\Delta_E)}{\text{ord}_2(\Delta_{E'})} \equiv \frac{-8}{8} \equiv -1 \pmod{p}$$

So -1 must be a square $\pmod{p}$, i.e. $p \equiv 1 \pmod{4}$.

- $\ell_2 = 7$

$$\frac{\text{ord}_7(\Delta_E)}{\text{ord}_7(\Delta_{E'})} \equiv 2 \pmod{p}$$

So 2 also is a square *mod* p . Hence $p \equiv 1 \pmod{8}$.

Thus, if $p \not\equiv 1 \pmod{8}$, the equation does not have non-trivial integer solutions. $\square$

7.3. Proof of Theorem ??

The proof is the generalization of the proof of Theorem ?? above. Let (x, y, z) be a non-trivial integer solution to the equation $ax^p + by^p + cz^p = 0$. Without loss of generality we may assume that

$$ax^p \equiv -1 \pmod{4} \text{ and } 2 \text{ divides } by^p.$$

Then the associated Frey curve is

$$E : Y^2 = X(X - ax^p)(x + by^p),$$

where $\Delta_E = 16(ABC)^2$ where $A = ax^p$, $B = by^p$ and $C = cz^p$. Using the results in Appendix ??, we get

$$\Delta_{\min}(E) = 2^{-8}(ABC)^2, N = N_E = \prod_{\substack{\ell \text{ prime,} \\ \ell | ABC}} \ell.$$

Thus we have

$$N_p = N / \prod_{\substack{\ell | N, \\ p | \text{ord}_\ell(\Delta_{\min}(E))}} \ell = 2 \prod_{\substack{\ell \text{ prime,} \\ \ell | abc}} \ell.$$

Since the conductor N of E is square-free, the elliptic curve E is semistable. If we choose $p \geq 5$, since $|E(\mathbb{Q})[2]| = 4$, E does not have any p -isogenies, by Theorem ??.

By Theorem ??, there exists a newform $f = q + \sum_{n \geq 2} c_n(E)q^n$ of weight 2 on $\Gamma_0(N_p)$ and a prime ideal $\mathfrak{P}|p$ of $K_f = \mathbb{Q}(c_2, \dots)$ such that

- (i) $c_\ell \equiv a_\ell(E) \pmod{\mathfrak{P}}$ if $\ell \nmid pN_E$
- (ii) $c_\ell \equiv \pm(\ell + 1) \pmod{\mathfrak{P}}$ if $\ell | N_E$ and $\ell \nmid pN_p$.

Note that at level N_p there may be rational or non-rational newforms. Therefore, we must first reduce to the case where the modular form f has coefficients in $\mathbb{Z}$.

The Hasse bound gives $|a_\ell(E)| \leq 2\sqrt{\ell}$, while Weil-Deligne's bound shows that $|\sigma(c_\ell)| \leq 2\sqrt{\ell}$ for each real embedding σ of K_f .

In any case p is bounded by a number depending only on a, b, c . Therefore, choosing large enough p we can make sure that f has integer coefficients. Thus by Eichler-Schimura theorem $f \sim_p E'$ for some elliptic curve $E'/\mathbb{Q}$ with conductor N_p . Hence we have two elliptic curves E and E' over $\mathbb{Q}$ such that $E \sim_p E'$.

Since, up to isogeny, there are only finitely many elliptic curves over $\mathbb{Q}$ of conductor N_p , say $E_1, \dots, E_h$, the elliptic curve E' arises modulo p from one of $\{E_1, \dots, E_h\}$, say $E' = E_j$. Now we apply the Lemma ?? to the pair (E, E_j) . Note that we do not know whether E and E_j are symplectically isomorphic or not. But in both cases we get the following result. We choose ℓ_1 dividing odd integer abc and $\ell_2 = 2$. If p is large enough, p does not divide $\text{ord}_{\ell_1}(\Delta_E), \text{ord}_2(\Delta_E), \text{ord}_{\ell_1}(\Delta_{E_j}), \text{ord}_2(\Delta_{E_j})$. Then

$$\frac{\text{ord}_{\ell_1}(\Delta_E)}{\text{ord}_{\ell_1}(\Delta_{E_j})} \pmod{p} \text{ and } \frac{\text{ord}_2(\Delta_E)}{\text{ord}_2(\Delta_{E_j})} \pmod{p}$$

is a square modulo p , since both terms are simultaneously square or non-square. Hence,

$$\frac{ord_{\ell_1}(\Delta_E)ord_2(\Delta_E)}{ord_{\ell_1}(\Delta_{E_j})ord_2(\Delta_{E_j})} = \frac{2ord_{\ell_1}(abc)(-8 + 2pord_2(xyz))}{ord_{\ell_1}(\Delta_{E_j})ord_2(\Delta_{E_j})}$$

is a square modulo p . So symplectic criterion implies that

$$n_j = -ord_{\ell_1}(abc)ord_{\ell_1}(\Delta_{E_j})ord_2(\Delta_{E_j})$$

has to be a square modulo p .

Hence if p is large enough satisfying the condition

$$\left(\frac{n_j}{p}\right) = -1, \text{ for all } j = 1, \dots, h$$

the equation $ax^p + by^p + cz^p = 0$ has no non-trivial integer solutions. Now we need to show that there exists a dense subset of the set of prime numbers for which the following two conditions hold

- (i) -1 is a non-square modulo p
- (ii) each prime divisor of n_j is a square modulo p .

The first condition is equivalent to requiring that $p \equiv 3 \pmod{4}$. The second one is equivalent to saying that for ever prime q dividing n_j we have $\left(\frac{q}{p}\right) = 1$ If $p = 2$, then this condition is equivalent to requiring that $p \equiv \pm 1 \pmod{8}$.

Since $p \equiv 3 \pmod{4}$ we need $p \equiv -1 \pmod{8}$. If q is odd then $\left(\frac{q}{p}\right) = 1$ is equivalent to

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod{4} \\ -1 & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

Now define a_p as in the following

$$\left(\frac{a_p}{q}\right) = \begin{cases} 1 & \text{if } q \equiv 1 \pmod{4} \\ -1 & \text{if } q \equiv 3 \pmod{4}. \end{cases}$$

Hence, if the following equivalence relation holds

$$p \equiv \begin{cases} -1 & \pmod{8} \\ a_p & \pmod{q} \text{ for all odd primes } q \mid \prod_j n_j \end{cases}$$

then $\left(\frac{n_j}{p}\right) = -1$. Now define $M = 8 \prod_{q \mid \prod_j n_j} q$, then there exists an integer k such that

$$k \equiv \begin{cases} -1 & \pmod{8} \\ a_p & \pmod{q} \text{ for all odd primes } q \mid \prod_j n_j. \end{cases}$$

So if a prime $p \equiv k \pmod{M}$, then there is no non-trivial solution to the equation $ax^p + by^p = cz^p$. By Lemma ??, this set has positive density. $\square$

8. THE EQUATION $x^4 + y^2 = z^p$ and $\mathbb{Q}$ -CURVES

In this chapter, our main motivation is to show how $\mathbb{Q}$ -curves can be useful to treat the generalized Diophantine equations. We will give a brief overview of the concepts about $\mathbb{Q}$ -curves and Galois representations attached to $\mathbb{Q}$ -curve that we need to prove the following theorem due to Jordan Ellenberg [?].

Theorem 8.1. *Let $p \geq 211$ be a prime. Then the equation*

$$x^4 + y^2 = z^p \tag{8.1}$$

does not have any non-trivial primitive solutions in integers.

Let (A, B, C) be a solution to the equation. If A, B and C are relatively prime we call such solution *primitive*. If $ABC \neq 0$, we call (A, B, C) is non-trivial.

Suppose that (A, B, C) is a primitive non-trivial solution to the equation ???. We attach to (A, B, C) a Frey curve E given the following Weierstrass equation

$$E : y^2 = x^3 + 2(1+i)Ax^2 + (B+iA^2)x,$$

where the arithmetic invariants $c_4 = 80iA^2 - 48B$ and $\Delta_E = -64i(A^2 + iB)(A^2 - iB)^2 = -64iC^p(A^2 - iB)$. This Frey curve was first discussed by Darmon in [?] to examine the equation $x^4 + y^4 = z^p$.

Note that if (A, B, C) is a solution to the equation $x^4 + y^2 = z^p$, then so is $(A, -B, C)$. Therefore, without loss of generality we may assume that $B \equiv 0, 2, 3 \pmod{4}$.

Proposition 8.2. *The elliptic curve $E/\mathbb{Q}(i)$ has either good or multiplicative reduction at primes away from 2, and has multiplicative reduction at an odd prime $\mathfrak{p}$ of $\mathbb{Q}(i)$ precisely when $\mathfrak{p}$ divides C .*

Proof. Since $(A, B) = 1$, $c_4 = 80iA^2 - 48B$ and $\Delta_E = -64i(A^2 + iB)(A^2 - iB)^2 = -64iC^p(A^2 - iB)$, we have the result by [?], VII, Prop.5.1. $\square$

Write σ for the non-trivial element of $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. Then the map

$$\mu_\sigma: (x, y) \mapsto \left(\frac{-1}{2x} ((ix^2 - A^2 - iB) - (i+1)Ax), \frac{1}{4x^2} ((i+1)x^2y + ((i-1)A^2 - (i+1)B)y) \right)$$

is a 2-isogeny from E^σ to E (see Appendix ??). Therefore, we can say that $E/\mathbb{Q}(i)$ is a $\mathbb{Q}$ -curve of degree 2 in terms of the following definition.

8.1. $\mathbb{Q}$ -curves and Their Galois Representations

Definition 8.3. *Let E be an elliptic curve over $\overline{\mathbb{Q}}$. We say that E is a $\mathbb{Q}$ -curve if for every $\sigma \in G_{\mathbb{Q}}$ there is an isogeny $\mu_\sigma: E^\sigma \rightarrow E$. We say that a $\mathbb{Q}$ -curve E is completely defined over a number field K if all the conjugates of E and the isogenies between them are defined over K .*

Remark 8.4. *This notion was originally defined and studied for a CM-elliptic curve in [?] and [?], but was extended by Ribet in [?] to the non-CM case using different methods. Throughout this thesis, it will be understood that all $\mathbb{Q}$ -curves are elliptic curves without complex multiplication.*

Let p be a rational prime, and define

$$\phi_{E,p} : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}_2(\mathbb{Z}_p)$$

to be the representation of $\text{Gal}(\overline{K}/K)$ on the p -adic Tate module $T_p(E)$ of E , where we have fixed an isomorphism $T_p(E) \simeq \mathbb{Z}_p$. In the following proposition we describe an extension of $\phi_{E,p}$ to a representation of the whole group $G_{\mathbb{Q}}$.

Proposition 8.5. *([?], Prop. 2.3) There exists a representation*

$$\rho_{E,p} : G_{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}_p^* \text{GL}_2(\mathbb{Q}_p)$$

such that $\mathbb{P}\rho_{E,p}|_{\text{Gal}(\overline{K}/K)} \simeq \mathbb{P}\phi_{E,p}$. This representation is odd, continuous, and ramified at only finitely many primes. In particular, $\rho_{E,p}|_{\text{Gal}(\overline{K}/K)}$ and $\phi_{E,p}$ differ by the continuous character $\alpha : \text{Gal}(\overline{K}/K) \rightarrow \overline{\mathbb{Q}}^*$ such that $c_E(g, h) = \alpha(g)\alpha(h)\alpha(gh)^{-1}$, where $c_E \in H^2(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathbb{Q}^*)$

Remark 8.6. *(i) $\mathbb{P}\rho$ denotes the projectivization of ρ . For further details see Appendix ??.*

Using this proposition, we can also define a projective mod p Galois representation

$$\mathbb{P}\overline{\rho}_{E,p} : G_{\mathbb{Q}} \rightarrow \text{PGL}_2(\mathbb{F}_p)$$

associated to any $\mathbb{Q}$ -curve.

(ii) We need the fact that the representation $\rho_{E,p}$ can also be viewed as the p -adic Galois representation of a certain abelian variety over $\mathbb{Q}$.

8.2. Weil Restriction

In this section we will give a brief description of the definition of Weil restriction and its relation with $\mathbb{Q}$ -curves.

Definition 8.7. (*Weil restriction*) Let L/K be any finite extension of fields, and X be any algebraic variety over L . The Weil restriction is a functor that produces another variety $\text{Res}_{L/K}X$ defined over K such that the K -rational points of $\text{Res}_{L/K}X$ are the L -rational points of X .

Note that the Weil restriction is unique up to isomorphism if it exists.

Example 8.8. Let E be an elliptic curve defined over $\mathbb{Q}(i)$ with the Weierstrass equation

$$E : y^2 = x^3 + i.$$

If we want to find $E(\mathbb{Q}(i))$, we are looking for the solutions of

$$(c + di)^2 = (a + bi)^3 + i,$$

where $y = c + di$ and $x = a + bi$ are in $\mathbb{Q}(i)$. So we have the following equations

$$a^3 - 3ab^2 - c^2 + d^2 = 0$$

$$2cd + 3a^2b + b^3 - 1 = 0.$$

Hence, $\text{Res}_{\mathbb{Q}(i)/\mathbb{Q}}E$ is the abelian variety defined over $\mathbb{Q}$ given by the equations above.

The relation between $\mathbb{Q}$ -curves and Weil restrictions arises in the following way; the Weil restriction contains the curve as a product.

Theorem 8.9. (*[?], Sec.6*) Let E/F be $\mathbb{Q}$ -curve over a number field F and let $A = \text{Res}_{F/\mathbb{Q}} E$ be the Weil restriction. Then A has the following properties

$$A(\mathbb{Q}) \simeq E(F) \text{ and } A(F) \simeq \prod_{\sigma \in \text{Gal}(F/\mathbb{Q})} E^\sigma(F),$$

where E^σ is the Galois conjugate of E through $\sigma \in \text{Gal}(F/\mathbb{Q})$.

8.3. Abelian Variety of GL_2 -type

Let A be a d -dimensional Abelian variety over $\mathbb{Q}$. We say that A is GL_2 -type if there is a field K of degree $d = \dim A$ such that $K \hookrightarrow \text{End}_{\mathbb{Q}} A \otimes_{\mathbb{Z}} \mathbb{Q}$.

Example 8.10. Every elliptic curve $E/\mathbb{Q}$ is an Abelian variety of GL_2 -type. Recall that $\dim E = 1$, so trivially $\mathbb{Q} \hookrightarrow \text{End}_{\mathbb{Q}} E \otimes_{\mathbb{Z}} \mathbb{Q}$. Note that the endomorphism ring may be strictly larger. For instance, consider the elliptic curve over $\mathbb{Q}$

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

Then we have $\text{End}(E) = \mathbb{Z}[i]$, so $\text{End}_{\mathbb{Q}} E \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(i)$. In fact, this $\mathbb{Q}$ -vector space is strictly larger than $\mathbb{Q}$ if and only if E has complex multiplication (For details see *[?], Ch.II*).

Canonical non-trivial examples of Abelian varieties of GL_2 -type are given by $\mathbb{Q}$ -curves.

Let $F/\mathbb{Q}$ be a Galois extension and E/F be an elliptic curve with the isogenies $\mu_\sigma : E^\sigma \rightarrow E$ for each $\sigma \in \text{Gal}(F/\mathbb{Q})$. Recall that the Abelian variety $A = \text{Res}_{F/\mathbb{Q}} E$ is defined over $\mathbb{Q}$ of dimension $d = [F : \mathbb{Q}]$ with the properties

$$A(\mathbb{Q}) \simeq E(F) \text{ and } A(F) \simeq \prod_{\sigma \in \text{Gal}(F/\mathbb{Q})} E^\sigma(F).$$

If $m_\sigma = \deg(\mu_\sigma)$ are the degrees of each isogeny, then the composite $\mu_\sigma \circ \mu_\sigma^\sigma : E \rightarrow E$ is the multiplication by $\pm m_\sigma$ map. Hence, $\text{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ contains the field $K = \mathbb{Q}(\dots, \sqrt{\pm m_\sigma}, \dots)$ and $d = [K : \mathbb{Q}]$. That is, A is an Abelian variety over $\mathbb{Q}$ of GL_2 -type.

Example 8.11. Let $F = \mathbb{Q}(\sqrt{5})$ and consider the elliptic curve

$$E : y^2 = x^3 + (5 - \sqrt{5})x^2 + \sqrt{5}x.$$

E is indeed a $\mathbb{Q}$ -curve (see Appendix ??).

Since $\text{Gal}(F/\mathbb{Q})$ has only two elements, one can show that $m_\sigma = 1, 2$ depending on whether $\sigma : \sqrt{5} \mapsto \pm\sqrt{5}$. In the former case, we have $E^\sigma \simeq E$, whereas in the latter case $\mu_\sigma : E \rightarrow E^\sigma$ satisfies $\mu_\sigma \circ \mu_\sigma^\sigma = [-2]$; therefore, $K = \mathbb{Q}(\sqrt{-2})$. This means that $d = [F : \mathbb{Q}] = [K : \mathbb{Q}] = 2$. So $A = \text{Res}_{F/\mathbb{Q}} E$ is an Abelian variety of GL_2 -type.

In general, we have the following lemma for $\mathbb{Q}$ -curves over quadratic number fields.

Lemma 8.12. ([?], Lem. 4.4) Let E be a $\mathbb{Q}$ -curve over a quadratic field F , furnished with the isogeny $\mu_\sigma : E^\sigma \rightarrow E$. Assume that μ_σ is defined over F and of degree prime p . Let $\widehat{\mu}_\sigma$ be the dual isogeny of μ_σ . Then we have

$$K = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } \mu_\sigma^\sigma = \widehat{\mu}_\sigma \\ \mathbb{Q}(\sqrt{-p}) & \text{if } \mu_\sigma^\sigma = -\widehat{\mu}_\sigma. \end{cases}$$

We can construct the 2-dimensional Galois representation associated to an Abelian variety of GL_2 -type A in the following way (cf. [?]) :

Let A be of dimension d and p be a rational prime. Note that $T_p(A) = \varprojlim A[p^n]$ is the p -adic Tate module and $V_p(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a $2d$ -dimensional $\mathbb{Q}$ vector space. By assumption, there exists a field $K \hookrightarrow \text{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ of degree d over $\mathbb{Q}$. Choose an ideal $\mathfrak{p}$ in K lying over $p \in \mathbb{Q}$ and consider the localization $K_{\mathfrak{p}}$ so that $V_p(A)$ is a $K_{\mathfrak{p}}$ -vector space of dimension 2. So, we have the $\mathfrak{p}$ -adic Tate module

$$T_{\mathfrak{p}}(A) = \varprojlim A[\mathfrak{p}^n]$$

along with the vector space $V_{\mathfrak{p}}(A) = T_{\mathfrak{p}}(A) \otimes K_{\mathfrak{p}}$. Since $G_{\mathbb{Q}}$ has a natural action on $V_{\mathfrak{p}}(A)$, we have the 2-dimensional Galois representation

$$\rho_{A,\mathfrak{p}} : G_{\mathbb{Q}} \rightarrow GL(V_{\mathfrak{p}}(A)).$$

Now it follows from [?], Prop. 2.10 that $\rho_{E,\mathfrak{p}} \simeq \rho_{A,\mathfrak{p}}$, where $\rho_{E,\mathfrak{p}}$ the Galois representation attached to E .

Remark 8.13. *By Remark ??, there is closed relation between p -adic Galois representations and mod p Galois representations. Due to this fact and the Lemma ?? from now on we will consider the mod p Galois representations of the objects given above.*

8.4. Serre's Invariants

In this section, our goal is to introduce the Serre invariants associated to a Galois representation. For details and the definition in complete generality see [?]. Fix an odd irreducible continuous 2-dimensional mod p Galois representation

$$\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL(V) \simeq GL_2(\overline{\mathbb{F}}_p).$$

Definition 8.14. An irreducible representation $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_{\ell})$ is modular of type (N, k, ϵ) if there exists a newform $f \in S_k(N, \epsilon)$ and a maximal ideal $\lambda \subset \mathcal{O}_{K_f}$ lying over ℓ such that $\bar{\rho}_{f, \lambda} \sim \bar{\rho}$.

First, we introduce briefly the definition of $N(\bar{\rho})$, which measures the minimal level of the modular forms giving rise to the given $\bar{\rho}$. Indeed, given a 2-dimensional Galois representation $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_p)$ we can think of it given by the action of $G_{\mathbb{Q}}$ in a two dimensional $\overline{\mathbb{F}}_p$ vector space V . Let $\ell \neq p$ be a prime number and choose an extension to $\overline{\mathbb{Q}}$ of ℓ -adic valuation on $\mathbb{Q}$. Let $G_0 \supset G_1 \supset \dots \supset G_i \supset \dots$ be the sequence of ramification subgroups corresponding to that valuation (see [?], Chap. IV) and let V_i be the subspace of V fixed by the action of G_i . Moreover, define also

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

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

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

We want to emphasize that $p \nmid N(\bar{\rho})$ by construction. In the rest of this thesis, when we talk about the conductor of a mod p representation $\bar{\rho}$, we will be always considering it outside of p .

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

Lemma 8.15. ([?], Pg. 186-191) Let E/K be an elliptic curve and put $\bar{\rho} := \bar{\rho}_{E,p}$.

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

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

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

- (ii) If E/K has multiplicative reduction at $\mathfrak{p}$ and $p|v_{\mathfrak{p}}(\Delta_E)$, then $\bar{\rho}$ is finite at $\mathfrak{p}$.
 (iii) If $\mathfrak{p}$ is of good reduction for E/K then $\bar{\rho}$ is finite at $\mathfrak{p}$.

Lemma ?? help us reduce the level through the following theorem (see [?]).

Theorem 8.16. Let $p \geq 3$ be a prime. Assume that $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_{p^r})$ is irreducible over $\mathbb{F}_{p^r}$ and is modular of type $(N, 2, 1)$. If ρ is finite at p then ρ is modular of type $(N(\rho), 2, 1)$.

Now we mention the character $\epsilon(\bar{\rho})$ and the weight k , in particular, $k \pmod{p-1}$. Associated to $\bar{\rho}$ we have the character

$$\det \bar{\rho} : G_{\mathbb{Q}} \rightarrow \mathbb{F}_p^*.$$

Since $\bar{\rho}$ is continuous, the image of $\det \bar{\rho}$ is a finite subgroup of $\mathbb{F}_p^*$. One can show ([?], Chap. VII) that the character $\det \bar{\rho}$ has conductor dividing $pN(\bar{\rho})$ and therefore

may be interpreted as a character

$$(\mathbb{Z}/pN(\bar{\rho})\mathbb{Z})^\times \rightarrow \overline{\mathbb{F}}_p^*.$$

Since $p \nmid N(\bar{\rho})$, there is a canonical isomorphism

$$(\mathbb{Z}/pN(\bar{\rho})\mathbb{Z})^\times \simeq (\mathbb{Z}/N(\bar{\rho})\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times,$$

and we define the character $\epsilon(\bar{\rho})$ to be the restriction of $\det \bar{\rho}$ to $(\mathbb{Z}/N(\bar{\rho})\mathbb{Z})^\times$. Furthermore, since the character group $\text{Hom}((\mathbb{Z}/p\mathbb{Z})^\times, \overline{\mathbb{F}}_p^*)$ is cyclic group of order $p-1$, generated by the cyclotomic character χ , the restriction of $\det \bar{\rho}$ to $(\mathbb{Z}/p\mathbb{Z})^\times$ is of the form χ^h for some $h \in \mathbb{Z}/(p-1)\mathbb{Z}$. We define $k(\bar{\rho}) \pmod{p-1}$ to be $h+1$. For the precise definition of the integer $k(\bar{\rho})$ see [?], Chap. 2. To determine the Serre weight of $\bar{\rho}_{E,p}$ precisely, we give the following two propositions :

The integer k depends only on the restriction of $\bar{\rho}$ to the decomposition group at p (in fact, to the inertia group). Therefore, consider the local Galois representation

$$\bar{\rho}_p : G_p \rightarrow GL_2(\overline{\mathbb{F}}_p),$$

where $G_p = \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Proposition 8.17. ([?], Prop. 2) *One has $\det \bar{\rho}_p|_{I_p} = \chi^{k-1}$, where I_p is the inertia group.*

Proposition 8.18. (*[?], Prop. 4*) *We have $k = 2$ if and only if the following two conditions hold:*

- (i) $\det \bar{\rho}_p|_{I_p} = \chi$
- (ii) $\bar{\rho}_p$ is finite at p .

Note that the condition $\det \bar{\rho}_p|_{I_p} = \chi$ is equivalent to $k \equiv 2 \pmod{p-1}$.

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

Conjecture 8.19. (*Serre*) *Let $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\bar{\mathbb{F}}_p)$ be odd and irreducible. The $\bar{\rho}$ is modular of type $(N(\bar{\rho}), k(\bar{\rho}), \epsilon(\bar{\rho}))$.*

Theorem 8.20. (*Khare-Wintenberger*) *Serre's conjecture holds.*

Proof. For the proof we refer to [?] and [?]. □

8.5. Back to our Frey Curve

Recall that we attached the Frey curve to the equation $A^4 + B^2 = C^p$

$$E : y^2 = x^3 + 2(1+i)Ax^2 + (B+iA^2)x.$$

We define a projective mod p Galois representation

$$\mathbb{P}\bar{\rho}_{E,p} : G_{\mathbb{Q}} \rightarrow PGL_2(\mathbb{F}_p)$$

associated to the Frey curve $E/\mathbb{Q}(i)$. Since E is a $\mathbb{Q}$ -curve, the Abelian variety $A = \text{Res}_{\mathbb{Q}(i)/\mathbb{Q}} E$ is of GL_2 -type, and by Appendix ?? we have that $\hat{\mu}_\sigma = \mu_\sigma^\sigma$, so Lemma ?? implies that $\mathbb{Q}(\sqrt{2}) \hookrightarrow \text{End}(A) \otimes \mathbb{Q}$. Let $\mathfrak{p}|p$ be a prime of $\mathbb{Z}[\sqrt{2}]$. Then we can attach the mod p Galois representation

$$\bar{\rho}_{E,\mathfrak{p}} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_p)$$

to the Abelian variety A . Note that, as we discussed above, the lifting of $\mathbb{P}\bar{\rho}_{E,p}$, as notation suggests, is the representation $\bar{\rho}_{E,\mathfrak{p}}$, and that $\bar{\rho}_{E,\mathfrak{p}}|_{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))}$ is precisely the Galois representation of $E[p]$. What we want to show is to prove that $\mathbb{P}\bar{\rho}_{E,p}$ is irreducible.

Lemma 8.21. *There exists a rational prime ℓ greater than 3 which divides C .*

Proof. If both A and B were odd, then C^p would be congruent to 2 modulo 4, which is not possible. So C must be odd. Furthermore, C cannot be divisible by 3, since $A^4 + B^2 = 0$ has no nonzero solutions over $\mathbb{F}_3$. Finally, since (A, B, C) is a non-trivial solution to the equation, $C \neq 1$. So there exists a prime ℓ greater than 3 dividing C . $\square$

Note that E has multiplicative reduction at primes of $\mathbb{Q}(i)$ over ℓ by Proposition ??.

Proposition 8.22. (*[?], Prop. 3.2*) *Let K be a quadratic field, and E/K be a $\mathbb{Q}$ -curve of square-free degree d . Suppose $\mathbb{P}\bar{\rho}_{E,p}$ is reducible for $p = 11$ or $p > 13$ with $(p, d) = 1$. Then E has potentially good reduction at all primes of K of characteristic greater than 3.*

Proposition ?? and the conclusion of Lemma ?? implies that $\bar{\rho}_{E,\mathfrak{p}}$ is irreducible. Since it is odd and irreducible, $\bar{\rho}_{E,\mathfrak{p}}$ is modular of type (N, k, ϵ) , where $k = k(\bar{\rho}_{E,\mathfrak{p}})$ and $\epsilon = \epsilon(\bar{\rho}_{E,\mathfrak{p}})$ are Serre invariants. If we can show that ϵ is trivial and that $k = 2$, then, by Theorem ??, we have

$$\bar{\rho}_{E,\mathfrak{p}} \simeq \bar{\rho}_{f,p}$$

for some newform f of level $N(\bar{\rho}_{E,\mathfrak{p}})$. Hence, our next goal is to compute the Serre invariants.

Proposition 8.23. *We have $k \equiv 2 \pmod{p-1}$. Moreover, $k = 2$.*

Proof. Let $\bar{\rho}_p$ denote the local representation obtained by $\bar{\rho}_{E,\mathfrak{p}}|_{G_p}$, where $G_p = \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. Recall that

$$\det \bar{\rho}_p|_{I_p} = \chi^{k-1},$$

where χ is the p^{th} cyclotomic character. Since $\det \bar{\rho}_{E,\mathfrak{p}} = \chi$, we have $\det \bar{\rho}_p|_{I_p} = \chi$. As χ is of order $p-1$, we have $k \equiv 2 \pmod{p-1}$. Furthermore, since $E/\mathbb{Q}(i)$ has multiplicative reduction at $\mathfrak{p}$ over p , and $p|v_{\mathfrak{p}}(\Delta_E)$, $\bar{\rho}_{E,\mathfrak{p}}$ is finite at $\mathfrak{p}$. Thus, by Proposition ?? $k = 2$. $\square$

Proposition 8.24. *The character $\epsilon = \epsilon(\bar{\rho}_{E,\mathfrak{p}})$ is trivial.*

Proof. By Deligne's work we have $\det \bar{\rho}_{f,p} = \epsilon \chi^{k-1}$. Since $\det \bar{\rho}_{E,\mathfrak{p}}$ is cyclotomic and $k \equiv 2 \pmod{p-1}$, we have $\epsilon \chi = \chi$. Hence ϵ is trivial. $\square$

Using Tate curve, we can prove the following result about the ramification of the reduced Galois representation associated to an elliptic curve.

Theorem 8.25. (*[?], Thm. 1.1.14*) *Let K be a number field and E/K an elliptic curve. Let λ be a prime of K where E has multiplicative reduction and let $p \geq 3$ be a rational prime such that $\lambda \nmid p$. Suppose that $p \mid v_\lambda(j(E))$. Then the reduced representation $\bar{\rho}_{E,p}$ is unramified at λ .*

Corollary 8.26. *The conductor $N = N(\bar{\rho}_{E,p})$ is a power of 2.*

Proof. By Theorem ??, $\bar{\rho}_{E,p}|_{\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(i))}$ is unramified away from 2. Hence, by the criterion of Néron-Ogg Shafarevich (Theorem ??), the conductor N is a power of 2. $\square$

Proposition 8.27.

$$N = \begin{cases} 32 & \text{if } A \text{ is even} \\ 256 & \text{otherwise.} \end{cases}$$

Proof. Since N is a power of 2, it suffices to follow Tate's algorithm for prime $\pi = i + 1$ above 2. For details see (*[?], Prop. 4.5*). $\square$

We have now established that $\bar{\rho}_{E,p}$ is isomorphic to $\bar{\rho}_{f,p}$, where f is newform of weight 2 and level 32 or 256. Using `lmfdb-The L-functions and Modular Forms Database` and the Eichler-Schimura theory, one can see that all associated elliptic curves have complex multiplication by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$ and the images of Galois representations attached to these elliptic curves are in the normalizer of a Cartan subgroup for $p \geq 2$. Hence, the image of $\mathbb{P}\bar{\rho}_{E,p}$ is the normalizer of a Cartan subgroup in $PGL_2(\mathbb{F}_p)$ (for definitions and classification of maximal subgroups of $PGL_2(\mathbb{F}_p)$ see Appendix ??).

Suppose the image of $\mathbb{P}\bar{\rho}_{E,p}$ lies in the normalizer of a split Cartan subgroup. Then it follows from [?] Prop. 3.4 that E has good reduction away from 6. But this contradicts Proposition ?? . We conclude that the image of $\mathbb{P}\bar{\rho}_{E,p}$ must be the normalizer of a non-split Cartan subgroup. Now this fact will be used to bound p .

Proposition 8.28. (*[?], Prop. 4.6*) *Let $C/\mathbb{Q}(i)$ be a $\mathbb{Q}$ -curve of degree 2, and suppose $\mathbb{P}\bar{\rho}_{C,p}$ has image contained in the normalizer of a non-split Cartan subgroup of $PGL_2(\mathbb{F}_p)$, for some $p \geq 211$. Then C has potentially good reduction for all primes of $\mathbb{Q}(i)$.*

We have shown that if (A, B, C) is a solution to the equation $x^4 + y^2 = z^p$, then $\mathbb{P}\bar{\rho}_{E,p}$ has an image the normalizer of a non-split Cartan subgroup of $PGL_2(\mathbb{F}_p)$. Proposition ?? shows that E has potentially good reduction at all primes of $\mathbb{Q}(i)$, but this contradicts to Proposition ?? . Hence, there is no such solution.

8.6. Points on Quadratic Twists of $X_0(N)$

Let $N = p_1 \dots p_r$ be a positive, square-free integer. The modular curve $Y_0(N)$ is a moduli space of tuples (E, C) , where E is an elliptic curve and C is a cyclic subgroup of order N in $E[N]$. Namely, every points of $Y_0(N)$ correspond to , up to isomorphism, a tuple (E, C) . Equivalently, any point of $Y_0(N)$ corresponds to (E, ϕ) , where ϕ is a cyclic N -isogeny of E . A projective smooth curve $X_0(N)$ is obtained by adding 2^r cusps to $Y_0(N)$. Note that all the cusps are $\mathbb{Q}$ -rational.

The Atkin-Lehner involution ω_N of $Y_0(N)$ sends (E, C) to the pair $(E/C, E[N]/C)$. The action of the rational map ω_N extends to $X_0(N)$ and freely permutes the cusps.

Let d be a square-free integer, $K := \mathbb{Q}(\sqrt{d})$, and σ be the generator of $Gal(K/\mathbb{Q})$. The twist $X^d(N)$ of $X_0(N)$ is obtained by Galois descent from $X_0(N)/K$ (for more details about the process see [?], p 102). It is a smooth curve over $\mathbb{Q}$, isomorphic to $X_0(N)$ over K but not over $\mathbb{Q}$. This means that $\mathbb{Q}$ -rational points of $X^d(N)$ are

precisely identified with the K -rational points of $X_0(N)$ fixed by $\sigma \circ \omega_N$. We are interested in such points. This because, like $X_0(N)$, the twisted curve $X^d(N)$ is a parameter space. A class of elliptic curves that are quadratic $\mathbb{Q}$ -curves of degree N correspond to $\mathbb{Q}$ -rational points on some $X^d(N)$. Therefore, if $X^d(N)(\mathbb{Q})$ is empty then there are no such quadratic $\mathbb{Q}$ -curves of degree N .

In this section we will prove the following theorem (see [?]) in order to show that our Frey curve exists. For general proof see [?].

Theorem 8.29. *(Shih) For $N = 2, 3, 7$, the two fixed points of ω_N in $X_0(N)$ are $\mathbb{Q}$ -rational.*

Hence, these points stay rational in $X^d(N)$ for any $\mathbb{Q}(\sqrt{d})$.

8.6.1. Complex Multiplication

Recall that every elliptic curve E over $\mathbb{C}$ is isomorphic to $\mathbb{C}/\Lambda$, where $\Lambda \subset \mathbb{C}$ is a lattice; that is there exist $\tau \in \mathcal{H}$ with $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$. The isomorphism of complex analytic manifolds $E \simeq \mathbb{C}/\Lambda$ is not only a diffeomorphism between an algebraic curve and a torus, but also is a group isomorphism.

For further information and proofs see [?] for an algebro-geometric viewpoint, and [?] and [?] for a more analytic perspective.

Theorem 8.30. *A $\mathbb{C}$ -isomorphism of elliptic curves $\mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$ is induced by multiplication by some $\lambda \in \mathbb{C}^*$ such that $\lambda\Lambda_1 = \Lambda_2$.*

Given a model E as a lattice $E \simeq \mathbb{C}/\Lambda$, we see that

$$\text{End}(E) \simeq \{\lambda \in \mathbb{C} : \lambda\Lambda \subset \Lambda\} \subset \mathbb{C}.$$

We can actually fully classify $\text{End}(E)$ for elliptic curves $E/\mathbb{C}$, as captured in the following theorem:

Theorem 8.31. *Let $E/\mathbb{C}$ be an elliptic curve. Then exactly one of the following is true:*

- (i) $\text{End}(E) \simeq \mathbb{Z}$
- (ii) $\text{End}(E) \simeq \mathcal{O}$, where $\mathcal{O}$ is isomorphic to an order in some imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$.

Note that an *order* $\mathcal{O}$ of a degree n number field $K/\mathbb{Q}$ is a finitely generated free $\mathbb{Z}$ -subalgebra of rank n .

We have a special name for elliptic curves satisfying (ii) in the theorem above.

Definition 8.32. *An elliptic curve $E/\mathbb{C}$ is said to have complex multiplication if*

$$\mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(E) \simeq \mathbb{Q}(\sqrt{-d})$$

for some discriminant d of an imaginary quadratic field (in other words, $\mathbb{Q} \otimes_{\mathbb{Z}} \text{End}(E)$ is isomorphic to an imaginary quadratic field when embedded into $\mathbb{C}$).

Recall that given an elliptic curve E with the Weierstrass equation

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

the discriminant and j -invariant are

$$\Delta_E = -16(4A^3 + 27B^2), \quad j_E = -1728 \frac{(4A)^3}{\Delta}.$$

Now we state the integrality of j_E for CM elliptic curves and its relation with class group. Note that K is a quadratic number field with ring of integers $\mathcal{O}_K$.

Theorem 8.33. *Let $E/\mathbb{C}$ be an elliptic curve with complex multiplication. Then j_E is an algebraic integer.*

Now define the following sets:

$$\begin{aligned}\mathcal{E}(\mathcal{O}) &= \{ \text{elliptic curves } E/\mathbb{C} \text{ with } \text{End}(E) \simeq \mathcal{O} \} / \sim \\ &= \{ \text{lattices } \Lambda \text{ with } \text{End}(E_\Lambda) \simeq \mathcal{O} \} / \text{homothety}\end{aligned}$$

$$\begin{aligned}\mathcal{C}(\mathcal{O}) &= \text{ideal class group of } \mathcal{O} \\ &= \frac{\{\text{non-zero fractional ideals of } K\}}{\{\text{non-zero principal ideals of } K\}}\end{aligned}$$

Theorem 8.34. *Let E be an elliptic curve representing an isomorphism class in $\mathcal{E}(\mathcal{O}_K)$.*

- (i) $K(j_E)$ is the Hilbert class field of K .
- (ii) $|\mathbb{Q}(j_E) : \mathbb{Q}| = |K(j_E) : K| = h_K$, where $h_K = |\mathcal{C}(\mathcal{O}_K)| = |\text{Gal}(K(j_E)/K)|$ is the class number of K .
- (iii) Let $E_1, \dots, E_{h_K}$ be a complete set of representatives for $\mathcal{E}(\mathcal{O}_K)$. Then $j_{E_1}, \dots, j_{E_{h_K}}$ is a complete set of $\text{Gal}(\overline{K}/K)$ conjugates for j_E .

8.6.2. Points in moduli space $Y_0(N)$

Recall that the Atkin-Lehner involution ω_N sends the point (E, C) to $(E/C, E[N]/C)$, where E is an elliptic curve and C is a cyclic subgroup of $E[N]$ of order N . Now we study the fixed points of the action of the involution ω_N on the moduli space $Y_0(N)$. In this section we study the points (E, C) of $Y_0(N)$ such that $(E, C) \sim (E/C, E[N]/C)$, i.e. the fixed points of $Y_0(N)$ under the action of the involution ω_N .

Note that $(E, C) \sim (E/C, E[N]/C)$ means that there exists an isogeny $\phi : E \rightarrow E/C$ such that $\phi(C) = E[N]/C$.

Let (E, C) represent such a class, where $E = \mathbb{C}/L$ with $L = \mathbb{Z} \oplus \tau\mathbb{Z}$ and $C = \langle \bar{g} \rangle \leq E[N]$. Consequently, $C = L + g\mathbb{Z}/L$. Then we have that

$$E/C \simeq \frac{\mathbb{C}/L}{L + g\mathbb{Z}/L} \simeq \mathbb{C}/L + g\mathbb{Z} = \mathbb{C}/L',$$

where $L' = L + g\mathbb{Z} = \mathbb{Z} + \tau\mathbb{Z} + g\mathbb{Z}$. Hence we have that $\mathbb{C}/L \simeq \mathbb{C}/L'$ if and only if there exists $\lambda \in \mathbb{C}$ such that $\lambda L = L'$.

Let ϕ be defined in the following way

$$\begin{aligned} \phi : \mathbb{C}/L &\longrightarrow \mathbb{C}/L' \\ \bar{z} &\mapsto \widehat{\lambda z}. \end{aligned}$$

Then we have

$$\phi(C) = \phi\left(\frac{L + g\mathbb{Z}}{L}\right) = \lambda \frac{L + g\mathbb{Z}}{L} = \frac{L' + \lambda g\mathbb{Z}}{L'}.$$

Since $E[N] = \frac{1}{N}L/L$, we have

$$E[N]/C = \frac{\frac{1}{N}L/L}{L + g\mathbb{Z}/L} \simeq \frac{1}{N}L/L'.$$

So we obtain that $\phi(C) = E[N]/C$ if and only if $L' + g\mathbb{Z} = \frac{1}{N}L$, which is equivalent to saying that $\lambda L' = \lambda^2 L = \frac{1}{N}L$. Hence, we have $\phi(C) = E[N]/C$ if and only if $N\lambda^2 L = L$.

Now we have enough tools to prove Theorem ??.

Proof of Theorem ??. Let $\mathcal{O}$ be an order of class number 1 in a quadratic number field, and $E_{\mathcal{O}} = \mathbb{C}/\mathcal{O}$ be an elliptic curve with endomorphism ring $\mathcal{O}$. Assume that the unique prime ramified in the field is N , and that $\mathcal{O}$ contains an element π with $\pi\bar{\pi} = N$. This is indeed possible for $N = 2, 3, 7$.

N	$\mathcal{O}$	π
2	$\mathbb{Z}[i]$	$1 + i$
	$\mathbb{Z}[\sqrt{-2}]$	$\sqrt{-2}$
3	$\mathbb{Z}\left[\frac{1 + \sqrt{-3}}{2}\right]$	$\sqrt{-3}$
	$\mathbb{Z}[\sqrt{-3}]$	$\sqrt{-3}$
7	$\mathbb{Z}\left[\frac{1 + \sqrt{-7}}{2}\right]$	$\sqrt{-7}$
	$\mathbb{Z}[\sqrt{-7}]$	$\sqrt{-7}$

To show that the pair $(E_{\mathcal{O}}, \pi)$ is a rational point of $X_0(N)$ fixed by ω_N , we need to find $\lambda \in \mathbb{C}$ satisfying the conditions mentioned above. For instance, let $\mathcal{O} = \mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$, $E_{\mathcal{O}} = \mathbb{C}/\mathcal{O}$, and $\pi = 1 + i$. Then $\ker \pi = C = \langle \frac{1}{1+i} + \mathcal{O} \rangle$ is a cyclic subgroup of $E_{\mathcal{O}}[2]$ of order 2, i.e. $g = \frac{1}{1+i}$. Then $L' = \mathcal{O} + \frac{1}{1+i}\mathbb{Z}$.

Firstly, we claim $\mathbb{C}/\mathcal{O} \simeq \mathbb{C}/L'$. To show that we need to find $\lambda \in \mathbb{C}$ such that $\lambda\mathcal{O} = L'$. By taking $\lambda = \frac{1}{1-i}$ we get the result. Since $2\lambda^2 = \frac{2}{(1-i)^2} = \frac{(1+i)(1-i)}{(1-i)^2} = \frac{1+i}{1-i} = i \in \mathcal{O}$, the pair $(E_{\mathcal{O}}, \pi)$ is fixed by ω_2 . Moreover, as the class number of $\mathcal{O}$ is 1, $(E_{\mathcal{O}}, \pi)$ is a rational point in $X_0(2)$ by Theorem ??.

To find another rational point for $X_0(2)$ fixed by ω_2 , consider the following

$$N = 2, \mathcal{O} = \mathbb{Z}[\sqrt{-2}], E_{\mathcal{O}} = \mathbb{C}/\mathcal{O}, \pi = \sqrt{-2}.$$

Let $C = \ker \pi = \langle \bar{g} \rangle$ be a cyclic group of order 2. Then $\bar{g} = 1/\sqrt{-2} + \mathcal{O}$ and $L' = \mathcal{O} + \frac{1}{\sqrt{-2}}\mathbb{Z}$. By taking $\lambda = \sqrt{-2}/2$ one can easily show that $(E_{\mathcal{O}}, C) \sim (E_{\mathcal{O}}/C, E_{\mathcal{O}}[2]/C)$ and that $(E_{\mathcal{O}}, C)$ is a rational point of $X_0(2)$.

9. A BRIEF SURVEY OF WHAT WE KNOW

Even before Wiles announced his proof, various generalizations of Fermat's Last Theorem had already been considered, which is of the shape

$$Ax^p + By^q = Cz^r, \quad (9.1)$$

for fixed integers A, B and C . We call (p, q, r) the *signature* of the equation ???. The behaviour of primitive solutions depends fundamentally upon the size of the quantity

$$\sigma(p, q, r) = \frac{1}{p} + \frac{1}{q} + \frac{1}{r},$$

in particular, whether $\sigma(p, q, r) > 1$, $\sigma(p, q, r) < 1$ or $\sigma(p, q, r) = 1$. We will focus on the case $\sigma(p, q, r) < 1$, for other cases we refer to [?]. In this case, we know that, for a fixed signature (p, q, r) the number of solutions in integers to equation ??? is at most finite:

Theorem 9.1. (*Darmon-Granville [?]*) *If A, B, C, p, q and r are fixed positive integers with*

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1,$$

then the equation

$$Ax^p + By^q = Cz^r$$

has at most finitely many solutions in co-prime non-zero integers x, y and z .

It is worth to mention that the argument used in the proof is ineffective in the meaning that it does not give us an algorithm to find all possible solutions since it depends on the Falting's theorem [?]. In the following tables, we list all known (as of 2018) cases where Equation ?? has been solved in integers. The first table contains all unconditional results for infinitely many primes. In the second one, we give all conditional results, which we denote them by * and/or for finitely many signature (p, q, r) . For example, in [?], the equation $x^2 + y^{2p} = z^5$ has no solutions if $p \equiv 1 \pmod{4}$.

Table 9.1. The infinite family of the equations with signature (p, q, r) without additional conditions.

(p, q, r)	reference(s)
$(n, n, n), n \geq 3$	Wiles, Taylor-Wiles
$(n, n, k), n \geq 4, k \in \{2, 3\}$	Darmon-Merel, Poonen
$(2n, 2n, 5), n \geq 2$	Bennett
$(2, 4, n), n \geq 4$	Ellenberg, Bennett-Ellenberg-Ng, Bruin
$(2, 6, n), n \geq 3$	Bennett-Chen, Bruin
$(2, n, 4), n \geq 4$	Bennett-Skinner, Bruin
$(2, n, 6), n \geq 3$	Bennett-Chen-Dahmen-Yazdani
$(3j, 3k, n), j, k \geq 2, n \geq 3$	immediate from Kraus
$(3, 3, 2n), n \geq 2$	Bennett-Chen-Dahmen-Yazdani
$(3, 6, n), n \geq 2$	Bennett-Chen-Dahmen-Yazdani
$(2, 2n, k), k \in \{9, 10, 15\}, n \geq 2$	Bennett-Chen-Dahmen-Yazdani
$(4, 2n, 3),$	Bennett-Chen-Dahmen-Yazdani
$(2j, 2k, n), j, k \geq 5 \text{ prime}, n \in \{3, 5, 7, 11, 13\}$	Anni-Siksek
$(13, 13, n), n \geq 17 \text{ or } n = 11$	Dieulefait-Freitas, Freitas-Samir
$(5, 5, n), n \geq 13$	Billerey-Dieulefait

Table 9.2. The equations with signature (p, q, r) of finite family or with additional conditions.

(p, q, r)	reference(s)
$(3, 3, n)^*$	Chen-Siksek, Kraus, Bruin, Dahmen
$(2, 2n, 3)^*$	Chen, Dahmen, Siksek
$(2n, 2n, 5)^* \ n \geq 2$	Bennett
$(2, 2n, 5)^*$	Chen
$(2m, 2n, 3)^*$	Bennett-Chen-Dahmen-Yazdani
$(2, 4n, 3)^*$	Bennett-Chen-Dahmen-Yazdani
$(3, 3n, 2)^*$	Bennett-Chen-Dahmen-Yazdani
$(2, 3, n), n \in \{6, 7, 8, 9, 10, 15\}$	Poonen-Schaefer-Stoll, Bruin, Zureick-Brown, Siksek, Siksek-Stoll
$(3, 4, 5)$	Siksek-Stoll
$(5, 5, 7), (7, 7, 5)$	Dahmen-Siksek
$(n, n, r)^*, r \geq 5$ regular prime	Billerey-Chen-Dieulefait-Freitas

Remark 9.2. (i) In some signatures the equation also has coefficients. For instance, in [?] the equation $x^5 + y^5 = 3z^p$ is solved. But in the tables we did not mention the coefficients.

(ii) The modular approach not only contains treating to equations via $\mathbb{Q}$ -curves, but it also includes some other approaches, which we have not set in this thesis, such as the program of Darmon-Granville [?].

(iii) Due to works of Derickx-Najman-Siksek [?] and Freitas-Le Hung-Siksek [?], we know the modularity of elliptic curves over quadratic and real cubic number fields. This forces us to consider Diophantine equations where coefficients and unknowns lie in a number field. Under certain assumptions of modularity, irreducibility and level-lowering, we get some results on the equation

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

asymptotically, which we refer the reader to [?], [?] for the case $A = B = C = 1$, and [?], [?] for a general result.

10. CONCLUSIONS

In this thesis, we summarize a technique called modular approach to treat some Fermat-type Diophantine equations. This technique is powerful enough to deal with many cases of generalized Fermat equations such as $x^4 + y^2 = z^p$. Curiously, one may ask whether this approach is enough to create an algorithm to solve all kind of ternary Diophantine equations. Unfortunately, the answer is no. For instance, it has not been known how to attach a Frey curve to an equation algorithmically. In addition, to understand K -rational points of a modular curve which parametrizes elliptic curves of various kinds is another issue. Therefore, one can deduce that the study of solutions of Diophantine equations is directly related to other aspects of mathematics.

On the other hand, many mathematicians have been trying to improve the methods they have or develop new ones to overcome the problems encountered. The results hold big promises for further substantial progress on the generalized Fermat equations. For example, for (p, q, r) Darmon constructs some Frey-Hellegouarch abelian varieties of GL_2 type over a totally real field and established modularity in the sense that they correspond to Hilbert modular forms. So one may ask:

- (i) Are there other geometric objects that are somehow modular?
- (ii) If so, can these be used as an alternative to tackle generalized Fermat equations?

Moreover, there are other advanced techniques, such as modularity of elliptic curves over real quadratic and real cubic fields, to treat Diophantine equations. Therefore, there is still hope to solve such equations for infinitely many cases.

APPENDIX A: RECIPES FOR SIGNATURE (p,p,p)

The following results are referred to [?]. Fix integers A, B , and C and consider the equation

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

where $p \geq 5$ is a prime. We may assume that Ax, By , and Cz are pairwise co-prime. Without loss of generality we also may assume that $By^p \equiv 0 \pmod{2}$ and that $Ax^p \equiv -1 \pmod{4}$. The Frey curve is given by the following Weierstrass equation

$$Y^2 = X(X - Ax^p)(X + By^p).$$

Its minimal discriminant is given by $\Delta_{min} = \begin{cases} 2^4 R^2 (xyz)^{2p} & \text{if } 16 \nmid By^p \\ 2^{-8} R^2 (xyz)^{2p} & \text{if } 16 \mid By^p \end{cases}$ where $R = ABC$ and the conductor N is given by $N = 2^\alpha \text{rad}_2(Rxyz)$, with

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

Theorem A.1. (*A. Kraus*) Under the above assumptions we have, $E \sim_p f$ for some newform f of level $N_p = 2^\beta \text{rad}_2(R)$, where

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

Note that $\text{rad}_q(M) = \prod_{\substack{p|M, \\ p \neq q \text{ prime}}} p$.

APPENDIX B: MAXIMAL SUBGROUPS OF $PGL_2(\mathbb{F}_p)$

Let V be vector space over a field K . Then obviously V has an action by scalars, namely multiplication. These transformations, denoted by $Z(V)$, form a normal subgroup of the group of linear transformations $GL(V)$. We can always express $Z(V) = K^\times \cdot id$ in terms of the identity transformation $id : V \rightarrow V$. For instance, assume that $V = \mathbb{F}_p$. Then we have

$$Z(V) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{F}_p^\times \right\}.$$

So we define the projective linear group as the quotient group $PGL(V) = GL(V)/Z(V)$ with the natural projection $\pi : GL(V) \twoheadrightarrow PGL(V)$. For each Galois representation $\rho : G_{\mathbb{Q}} \rightarrow GL(V)$, the composition $\rho \circ \pi$

$$\mathbb{P}\rho : G_{\mathbb{Q}} \xrightarrow{\rho} GL(V) \xrightarrow{\pi} PGL(V)$$

is known as the projectivization of the representation ρ .

Definition B.1. Let $\mathbb{P}\rho : G_{\mathbb{Q}} \rightarrow PGL(V)$ be a projective Galois representation. A lifting of $\mathbb{P}\rho$ is a Galois representation $\rho : G_{\mathbb{Q}} \rightarrow GL(V)$ such that the following diagram

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\rho} & GL(V) \\ & \searrow \mathbb{P}\rho & \downarrow \pi \\ & & PGL(V) \end{array}$$

commutes.

Hence, it is natural to ask that if we have a projective Galois representation $\mathbb{P}\rho$, does there exist a lifting ρ ? The answer is yes, but it involves Galois cohomology.

Now we focus on the subgroups of $PGL_2(\mathbb{F}_p)$.

Definition B.2. *A Borel subgroup is a subgroup of $GL_2(\mathbb{F}_p)$ of the form (up to conjugation)*

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

A split Cartan subgroup is a subgroup of $GL_2(\mathbb{F}_p)$ of the form (up to conjugation)

$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}.$$

Let $\epsilon \in \mathbb{F}_p^\times$ be a non-square element. Then, a non-split Cartan subgroup is a subgroup of the form

$$\left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_p, a^2 - \epsilon b^2 \neq 0 \right\}.$$

The following theorem is due to Serre [?], and classifies the maximal subgroups of $GL_2(\mathbb{F}_p)$.

Theorem B.3. (*Maximal subgroups of $GL_2(\mathbb{F}_p)$*) Let G be a subgroup of $GL_2(\mathbb{F}_p)$, let H denote the image of G in $PGL_2(\mathbb{F}_p)$. Then one of the following holds:

- (i) G has order prime to p and either;
 - (a) H is cyclic and G is contained in a Cartan subgroup of $GL_2(\mathbb{F}_p)$,
 - (b) H is dihedral and G is contained in the normalizer of a Cartan subgroup C of $GL_2(\mathbb{F}_p)$ but not in C ,
 - (c) H is isomorphic to A_4, S_4 or A_5 and we call G exceptional;
- (ii) G has order divisible by p and either
 - (a) G is contained in a Borel subgroup,
 - (b) G contains $SL_2(\mathbb{F}_p)$.

APPENDIX C: MAGMA SCRIPT

The following **MAGMA** script gives us the isogeny μ_σ and its dual isogeny $\widehat{\mu}_\sigma$ mentioned in Chapter ?? and Section ??.

```

> K<Ip>:=QuadraticField(-1);
> S<X>:=PolynomialRing(K);
> I:=K!Ip;
> R:=PolynomialRing(K,2);
> F<a,b>:=FieldOfFractions(R);

/* Frey curve for  $a^4 + b^2 = c^p$ . */
> E:=EllipticCurve([0,2*(1+I)*a,0,b+I*(a^2),0]);

/* Conjugate curve */
> Ec:=EllipticCurve([0,2*(1-I)*a,0,b-I*(a^2),0]);

/* There is a point P2 of order 2 on Ec. */
> f2:=DivisionPolynomial(Ec,2);
> f2l:=Factorization(f2);
> P2:=f2l[1][1];

/* Find using Velu the elliptic curve  $E2 = E/P2$ . */
> E2,phi2:=IsogenyFromKernel(Ec,P2);

/* E2 and E are isomorphic over  $K = Q(I)$  */
> IsIsomorphic(E2,E);
true

> M:=Isomorphism(E2,E);

```

```

/* the isogeny from Ec to E*/
> N:=phi2*M;
> N;
Elliptic curve isogeny from: CrvEll: Ec to CrvEll: E
taking (x : y : 1) to ((-1/2*Ip*x^2 + (-Ip - 1)*a*x
- 1/2*a^2 - 1/2*Ip*b) / x :
(1/4*(Ip + 1)*x^2*y + (1/4*(Ip - 1)*a^2
+ 1/4*(-Ip - 1)*b)*y) / x^2 : 1)

> DualIsogeny(N);
Elliptic curve isogeny from: CrvEll: E to CrvEll: Ec
taking (x : y : 1) to ((1/2*Ip*x^2 + (Ip - 1)*a*x - 1/2*a^2
+ 1/2*Ip*b) / x :
(1/4*(-Ip + 1)*x^2*y + (1/4*(-Ip - 1)*a^2 + 1/4*(Ip -
1)*b)*y) / x^2 : 1)

```

We can show that the elliptic curve $E : y^2 = x^3 + (5 - \sqrt{5})x^2 + \sqrt{5}x$ described in Example ?? is a $\mathbb{Q}$ -curve over $\mathbb{Q}(\sqrt{5}, \sqrt{-2})$ due to the following MAGMA script.

```

> R<x> := PolynomialRing(Integers());
> f := x^2 - 5;
> K<I> := NumberField(f);
> S<X>:=PolynomialRing(K);

> R:=PolynomialRing(K,2);
> L<z>:=ext<K|X^2+2>;
> I:=L!I;
> P:=PolynomialRing(L,2);

> E:=EllipticCurve([0,5-I,0,I,0]);

```

```

/* Conjugate curve */
> Ec:=EllipticCurve([0,5+I,0,-I,0]);

/* There is a point P2 of order 2 on Ec. */
> f2:=DivisionPolynomial(Ec,2);
> f2l:=Factorization(f2);
> P2:=f2l[1][1];

/* Find using Velu the elliptic curve E2 = E/P2. */
> E2,phi2:=IsogenyFromKernel(Ec,P2);
> IsIsomorphic(E2,E);
True

```

APPENDIX D: TATE'S ALGORITHM

Two elliptic curves with different parameters may be isomorphic over $\mathbb{Q}$. Such an isomorphism must be given by transformations $x = u^2x' + r, y = u^3y' + su^2x' + t$, where $u \in \mathbb{Q}^*, r, s, t \in \mathbb{Q}$. Let $E/\mathbb{Q}$ be an elliptic curve with the Weierstrass equation $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$. Using the same quantities, the parameters of the new model are given by

$$\begin{aligned} ua'_1 &= a_1 + 2s, u^2a'_2 = a_2 - sa_1 + 3r - s^2 \\ u^3a'_3 &= a_3 + ra_1 + 2t \\ u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\ u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - 2sa_1 \\ u^{12}\Delta' &= \Delta \\ u^4c'_4 &= c_4, u^6c'_6 = c_6 \end{aligned}$$

Using these formulas, we may now assume that the coefficients of E are integers. We know that every isomorphism class of elliptic curves has the minimal model, i.e. such elliptic curve has the minimal discriminant. But this existence does not guarantee how to compute the minimal discriminant. The following algorithms are due to Tate and they help us compute the coefficients of the minimal model and the conductor of the elliptic curve.

Note that to compute the invariants of the following examples we will follow the steps of the algorithms in [?].

Let $E/\mathbb{Q}$ be an elliptic curve with the Weierstrass equation $y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$, where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. We may also define quantities

$$\begin{aligned} b_2 &= a_1^2 + 4a_4, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta \end{aligned}$$

Also recall that the *conductor* N_E of $E_{\min}$ is $N_E = \prod_p p^{f_p}$, where

$$f_p = \begin{cases} 0 & \text{good at } p \\ 1 & \text{multip. at } p \\ 2 & \text{add. at } p \neq 2, 3 \\ 2 + \delta_p & \text{add. at } p = 2, 3 \end{cases}$$

Remark D.1. • In [?], Algorithm 7.5.1 is for primes $p \geq 3$, Algorithm 7.5.2 is for primes $p = 2, 3$ and Algorithm 7.5.3 computes the minimal model and the conductor for given elliptic curve using the outputs of Algorithm 7.5.1 and Algorithm 7.5.2.

- In the following calculation, $(*)$ refers to the step in the related algorithm.

Let $a^p + b^p + c^p = 0$, where $p \geq 5$, $a, b, c \in \mathbb{Z}$ pairwise coprime and $abc \neq 0$. Recall that our associated Frey Curve is

$$E : y^2 = x(x - a^p)(x + b^p) = x^3 + (b^p - a^p)x^2 - (ab)^p x$$

So our quantities are

$$\begin{aligned} a_1 &= 0, a_2 = b^p - a^p, a_3 = a_6 = 0, a_4 = -a^p b^p \\ b_2 &= 4(b^p - a^p), b_4 = -2a^p b^p, b_6 = 0, b_8 = -(ab)^{2p} \\ c_4 &= 16(c^{2p} - (ab)^p), c_6 = 16(a^p - b^p)(4a^{2p} + (ab)^p + 4b^{2p}) \\ \Delta &= 2^4(abc)^{2p}, j = \frac{2^8(c^{2p} - (ab)^p)}{(abc)^{2p}} \end{aligned}$$

- For all primes not dividing Δ , we have $f_p = 0$. Now we have three cases.
- Assume that ℓ is a prime that divides Δ , i.e. divides abc , and $\ell \neq 2, 3$.

- (1) Since $v_\ell(j) = -2p < 0$, set $k = v_\ell(\Delta) + v_\ell(j) = 0$
- (2) Since $k = 0 < 12$, set $u = 1, r = s = t = 0$,
- (3) Since $v_\ell(j) = -2p < 0$, set $v = 2p$. Since $k = 0$, set $f = 1, u = 1$,
 $r = s = t = 0$.

Thus, we get $f_\ell = 1, u_\ell = 1, r = s = t = 0$ for all primes $\ell \neq 2, 3$ dividing Δ .

- Assume that $\ell = 3$. If ℓ does not divide Δ , we have $f_3 = 0$. So assume now that ℓ divides Δ .

(1) Set $u = 1, r = s = t = 0$ and $v = v_3(\Delta) = 2p$,

(3) We have $b_2 = 4(b^p - a^p)$. If 3 divides c , then $3 \nmid b_2$, and we get $f_3 = 1$.

If 3 divides ab , then 3 divides either a or b . In either case we get $3 \nmid b_2$.

Thus, we have $f_3 = 1, u = 1, r = s = t = 0$.

So we get $f_3 = 1, u_3 = 1$ and $r_3 = s_3 = t_3 = 0$.

- Suppose that $\ell = 2$.

(1) Set $u = 1, r = s = t = 0$ and $v = v_2(\Delta) = 2p + 4, v_2(j) = 2p - 8$,

(4) Since $\ell = 2$, set $u = 1, r_1 = t_1 = 0, s_1 = 1$. Change coordinates using parameters $1, 0, 1, 0$. Then we have $a_1 = 2, a_2 = b^p - a^p - 1, a_3 = 0$,

$a_4 = -(ab)^p, a_6 = 0$ and $r = t = 0, s = 1$,

(15) Change coordinates using parameters $2, 0, 0, 0$. Then we have $a_1 = 1$,

$a_2 = \frac{b^p - a^p - 1}{2^2}, a_3 = 0, a_4 = -(ab)^p/2^4, a_6 = 0$ and $u = 2, r = t = 0$,

$s = 1, v = 2p - 8, b_2 = 1 + 4\left(\frac{b^p - a^p - 1}{4}\right) = b^p - a^p$,

(3) Since $2 \nmid b_2 = b^p - a^p$, we set $f = 1$

(22) Set $f = 1, u = 2, r = t = 0, s = 1$.

Hence we have $f_3 = 1, u_3 = 2, r_3 = t_3 = 0$ and $s_3 = 1$.

Now we can compute the minimal model and the conductor using *algorithm* 7.5.3.

(1) Set $N = 1, u = 1, r = s = t = 0, D = 2^4(abc)^{2p}$

(3) For all odd prime divisors of D , we have $N_E = \prod_{\ell|D, \text{oddprime}} \ell, u = 1,$

$r = s = t = 0$. Set $D = 2^{2p+4},$

(3) Since $\ell = 2$, we have $f_2 = 1, u = 2, r = t = 0, s = 1$. Set $D = 1,$

(2) Set $N_E = \prod_{\ell|abc, \text{prime}} \ell, u = 2, r = t = 0, s = 1.$

Using outputs of *algorithm 7.5.3*, we can compute the coefficients of the minimal model :

$$a_1 = 1, a_2 = \frac{b^p - a^p - 1}{2^2}, a_3 = 0, a_4 = \frac{-(ab)^p}{2^4}, a_6 = 0$$

So we have

$$E_{min} : y^2 + xy = x^3 + \frac{b^p - a^p - 1}{2^2} - \frac{(ab)^p}{2^4}x$$

with $\Delta_{min}2^{-8}(abc)^{2p}$ and $N_E = \prod_{\ell|abc} \ell.$