國立交通大學

應用數學系

碩士論文

伽羅瓦表現與模型式

Galois Representations and Modular Forms

研 究 生：黃彥璋

指導老師：楊一帆　教授

中華民國九十九年七月

伽羅瓦表現與模型式
Galois Represetations and Modular Forms

研究生：黃彥璋　　Student：Yan-Jhang Huang

指導教授：楊一帆　教授　　Advisor：Professor Yi-Fan Yang

國立交通大學
應用數學系
碩士論文

A Thesis
Submitted to Department of Applied Mathematics
College of Science
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of
Master
in
Applied Mathematics
June 2010

Hsinchu, Taiwan, Republic of China

中華民國九十九年七月

伽羅瓦表現與模型式

學生：黃彥璋　　　　　　　　　　　　指導老師：楊一帆 教授

國立交通大學應用數學系(研究所)碩士班

摘　　　要

我們想要探討的問題，是如何去尋找一個簡單的方法來討論一個特別的函數x^4-2在模掉一個質數p之後解的個數。這是一個跟Hecke L-函數、伽羅瓦群、群的表現有關的應用問題。

更進一步來說，我們可利用這個多項式解空間的伽羅瓦表現來找出一個weight為12，level為256的cusp form。

Galois Representations and Modular Forms

Student：Yan-Jhang Huang Advisor：Professor Yi-Fan Yang

Department of Applied Mathematics

National Chiao Tung University

Degree of Master

ABSTRACT

The problem we want to discuss in this thesis is trying to find a simple description "How the polynomial splits modulo a prime p for a special polynomial x^4-2." This is an application of Hecke L-function, the Galois theorem and the group representation. We will try to connect them by some well-known knowledge, and use them to solve the problem in our discussion.

Moreover, we will use the Galois representation of the splitting filed of the polynomial x^4-2 to construct a cusp form of weight 1 with level 256.

誌　謝

首先，在我完成我的碩士論文之後，最要感謝的是我的指導教授楊一帆老師。感謝他帶我走入這個研究領域，並且給予我許多的學習機會。也引導我走向更高深、更有趣的數學殿堂。

另外我也要感謝潘戍衍老師以及王千真老師在百忙之中抽空擔任我的口試委員。

接著我要感謝涂芳婷學姊與林家銘同學。在我研究各方面問題遇上瓶頸時，他們兩位總是能夠提供我所需要的協助。

最後，我要感謝我的家人，因為有你們的栽培，我才能夠順利完成學業。

黃彥璋
謹誌于交通大學
2010年7月

目錄

Chapter 1

Introduction

In 2003, *Jean-Pierre Serre* gave a paper *"On A Theorem Of Jordan"*, which interests us. The paper has a part which is talking about the number of roots for a given polynomial f in $\mathbb{Z}/p\mathbb{Z}$. Let $N_p(f)$ denotes the number of zeros of f in $\mathbb{Z}/p\mathbb{Z}$. In the paper, Serre gave three special examples, all of them has form $f(x) = x^n - x - 1$ for $n = 2, 3, 4$. He related the $N_p(f)$ to the coefficients of theta series.

1.1 Examples From Serre's Paper

In this section, we talk about the special case of $f(x) = x^n - x - 1$ for $n = 2, 3, 4$, and we relate the numbers $N_p(f)$ to the coefficients of theta series.

1.1.1 Case $n = 2$: $x^2 - x - 1$

The discriminant of $f = x^2 - x - 1$ is 5. The polynomial f has a double root modulo 5, hence $N_5(f) = 1$. For $p \neq 5$, we have

$$N_p(f) = \begin{cases} 2, & \text{if } p \equiv \pm 1 \mod 5 \\ 0, & \text{if } p \equiv \pm 2 \mod 5. \end{cases}$$

If one defines a power series $F(q) = \sum_{n=0}^{\infty} a_n q^n$ by

$$\begin{aligned} F &= \frac{q - q^2 - q^3 + q^4}{1 - q^5} = q - q^2 - q^3 + q^4 + q^6 - q^7 - q^8 + \cdots \\ &= \sum_{n=1}^{\infty} \left(\frac{n}{5}\right) q^n, \end{aligned}$$

the above formula can be restated as

$$N_p(f) = a_p + 1 \text{ for all primes } p,$$

where a_p is the p-th term coefficient in the L-function

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \left(1 - \left(\frac{p}{5}\right) p^{-s}\right)^{-1},$$

which is analytic continued to the complex plane.

1.1.2 Case $n = 3$: $x^3 - x - 1$

The discriminant of $f = x^3 - x - 1$ is -23. The polynomial f has a double root and a simple root mod 23, hence $N_{23}(f) = 2$. For $p \neq 23$, one has,

$$N_p(f) = \begin{cases} 0 \text{ or } 3, & \text{if } (\frac{p}{23}) = 1 \\ 1, & \text{if } (\frac{p}{23}) = -1. \end{cases}$$

Moreover, in the ambiguous case where $(\frac{p}{23}) = 1$, p can be written either as $x^2 + xy + 6y^2$ or as $2x^2 + xy + 3y^2$ with $x, y \in \mathbb{Z}$; in the first case, one has $N_p(f) = 3$; in the second case, one has $N_p(f) = 0$. (The smallest p of the form $x^2 + xy + 6y^2$ is $59 = 5^2 + 5 \times 2 + 6 \times 2^2$, hence $N_{59}(f) = 3$.)

Let us define a power series $F = \sum_{n=0}^{\infty} a_n q^n$ by the formula

$$\begin{aligned} F &= q \prod_{k=1}^{\infty} (1 - q^k)(1 - q^{23k}) \\ &= \frac{1}{2} \left(\sum_{x,y \in \mathbb{Z}} q^{x^2+xy+6y^2} - \sum_{x,y \in \mathbb{Z}} q^{2x^2+xy+3y^2} \right) \\ &= q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + \cdots . \end{aligned}$$

This is a modular form of weight 1 on $\Gamma_0(23)$ with character $\left(\frac{-23}{n}\right)$. The formula for $N_p(f)$ given above can be reformulated as,

$$N_p(f) = a_p + 1 \text{ for all primes } p.$$

Note that the coefficients of F are *multiplicative*, one has $a_{mm'} = a_m a_{m'}$ if m and m' are relatively prime. And the associated Dirichlet series is

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p} \left(1 - \frac{a_p}{p^s} + \left(\frac{p}{23}\right) \frac{1}{p^{2s}} \right)^{-1} .$$

(This equation comes from [6].)

1.1.3 Case $n = 4$: $x^4 - x - 1$

The discriminant of $f(x) = x^4 - x - 1$ is -283. The polynomial f has two simple roots and a double root modulo 283, hence $N_{283}(f) = 3$. If $p \neq 283$, one has,

$$N_p(f) = \begin{cases} 0 \text{ or } 4, & \text{if } p \text{ can be written as } x^2 + xy + 71y^2 \\ 1, & \text{if } p \text{ can be written as } 7x^2 + 5xy + 11y^2 \\ 0 \text{ or } 2 & \text{if } (\frac{p}{283}) = -1. \end{cases}$$

A complete determination of $N_p(f)$ can be obtained via a newform of weight 1 and level 283 as follows

$$\begin{aligned} F &= \sum_{n=1}^{\infty} a_n q^n \\ &= q + \sqrt{-2}q^2 - \sqrt{-2}q^3 - q^4 - \sqrt{-2}q^5 + 2q^6 - q^7 - q^9 + 2q^{10} + q^{11} + \cdots . \end{aligned}$$

One has,

$$N_p(f) = 1 + a_p^2 - (\frac{p}{283}) \text{ for all primes } p \neq 283.$$

1.1.4 A Small Table Of $N_p(f)$ for $f = x^n - x - 1$

In the end of this section, we give a small table of $N_p(f)$ for $f(x) = x^n - x - 1,\ n = 2, 3, 4.$

p	$n = 2$	$n = 3$	$n = 4$
2	0	0	0
3	0	0	0
5	1	1	0
7	0	1	1
11	2	1	1
13	0	0	1
17	0	1	2
19	2	1	0
23	0	2	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
59	2	3	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
83	0	1	4

1.2 Abstract

The problem we want to discuss in this thesis is trying to find a simple description "How the polynomial splits modulo a prime p for a special polynomial $x^4 - 2$." This is an application of Hecke L-function, the Galois theorem and the group representation. We will try to connect them by some well-known knowledge,and use them to solve the problem in our discussion.

In the further chapters, we will introduce some background, and explain the detail of the example for $f(x) = x^3 - x - 1$, and in the last chapter, we will pick a special polynomial to be our main subject "$f(x) = x^4 - 2$". Whose spliting field is $L = \mathbb{Q}(\sqrt[4]{2}, i)$, and the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to D_4. And for this case, we try to construct a weight 1 cusp form, says that if the cusp form be written as a Fourier expansion, then the coefficients of prime terms are just the same as the prime terms of an Artin L-function associated with the Galois group $\mathrm{Gal}(L/\mathbb{Q})$.

Chapter 2

Basic Knowledge

2.1 Number Fields

Let K be a number field, and L be a Galois extension of K. Let $\mathcal{O}_L, \mathcal{O}_K$ denote the ring of integers in L, K respectively. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ lying over $\mathfrak{p}$.

Definition 2.1.1. The *decomposition group* of $\mathfrak{P}$ is

$$D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{GAL}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

and the *inertia group* of $\mathfrak{P}$ is

$$E(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in \mathrm{GAL}(L/K) : \sigma(\alpha) \equiv \alpha \mod \mathfrak{P}\} \ \forall \alpha \in \mathcal{O}_L.$$

Theorem 2.1.2 ([7])**.** *Let L be a Galois extension of K, a prime $\mathfrak{p}$ is ramified in L if and only if $\mathfrak{p}$ divides the discriminant of L.*

And for the prime is unramified in L, there is a special proposition for them.

Proposition 2.1.3 ([7])**.** *Let L be a Galois extension of K, $\mathfrak{p}$ be an unramified prime lies under $\mathfrak{P}$ in L. Then there exists a unique automorphism $\sigma \in \mathrm{Gal}(L/K)$ such that*

$$\sigma(a) \equiv a^{N(\mathfrak{p})} \mod \mathfrak{P}$$

for all $a \in \mathcal{O}_L$.

We give a definition and a notation for this special automorphism.

Definition 2.1.4. The special element σ is called to be the *Frobenius automorphism* of $\mathfrak{P}$ over $\mathfrak{p}$. Obviously, we have $\mathrm{Frob}(\mathfrak{P}|\mathfrak{p}) \in D(\mathfrak{P}|\mathfrak{p})$. We denote it by $\mathrm{Frob}(\mathfrak{P}|\mathfrak{p})$.

Proposition 2.1.5 ([7])**.** *Assume that L is a Galois extension of K and $\mathfrak{p}$ is unramified in L, Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be two primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Suppose that $\sigma \in \mathrm{Gal}(L/K)$ maps $\mathfrak{P}_1$ to $\mathfrak{P}_2$. Then we have*

$$\mathrm{Frob}(\mathfrak{P}_1|\mathfrak{p}) = \sigma \mathrm{Frob}(\mathfrak{P}_2|\mathfrak{p})\sigma^{-1}.$$

From the above proposition, if $\mathrm{Gal}(L/K)$ is abelian, then the Frobenius automorphism depends only on $\mathfrak{p}$. In this case, the Frobenius automorphism σ will satisfy

$$\sigma(a) \equiv a^{N(\mathfrak{p})} \mod \mathfrak{p}\mathcal{O}_L$$

for all $a \in \mathcal{O}_L$. Thus, the proposition lead to the following definition.

Definition 2.1.6. Assume that $\mathrm{Gal}(L/K)$ is abelian. For a prime $\mathfrak{p}$ in K unramified in L, define the *Artin symbol* by

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{Frob}(\mathfrak{P}|\mathfrak{p})$$

where $\mathfrak{P}$ is any prime in L lying over $\mathfrak{p}$. Let $\mathfrak{I}_{L/K}$ denote he multiplicative group of fractional ideals generated by primes of K unramified in L. Then the *Artin map* $\mathrm{Frob}_{L/K} : \mathfrak{I}_{L/K} \rightarrow \mathrm{Gal}(L/K)$ is the group homomorphism defind by

$$\mathrm{Frob}_{L/K}(\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_k^{e_k}) = \prod_{i=1}^{k} \left(\frac{L/K}{\mathfrak{p}_i}\right)^{e_i}$$

where $\mathfrak{p}_i$ are primes of K unramified in L and e_i are integers.

Proposition 2.1.7 ([7])**.** *Each automorphism σ of L in $D(\mathfrak{P}|\mathfrak{p})$ induces an automorphism $\overline{\sigma} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}$ of the field $\mathcal{O}_L/\mathfrak{P}$ that fixes $\mathbb{Z}/p\mathbb{Z}$ pointwise and if we let $\gamma : \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P}$ be the canonical homomorphism $\gamma(\alpha) = \alpha + \mathfrak{P}$, then $\overline{\sigma} \circ \gamma = \gamma \circ \sigma$. Since $\sigma \in D(\mathfrak{P}|\mathfrak{p})$, the property $\sigma(\mathfrak{P}) = \mathfrak{P}$ implies $\overline{\sigma}$ is defined by $\overline{\sigma}(a + \mathfrak{P}) = \sigma(a) + \mathfrak{P}\ \forall a \in \mathcal{O}_L$.*

More precisely, in the Proposition 2.1.7 we say that $\overline{\sigma}$ fixes $\mathbb{Z}/p\mathbb{Z}$ pointwise means there exists an embedding $i : \mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_L/\mathfrak{P}$, defined by $i(a + p\mathbb{Z}) = a + \mathfrak{P}$, such that $\alpha + \mathfrak{P}$ contained in the image of i.

2.2 Representations, Characters And Artin L-functions

In our discussion, *L-function* plays an important role. Before we discuss L-functions, we need to introduce *representations* and *characters*.

Definition 2.2.1. Let V be a vector space over a field $\mathbb{F}$ and $GL(V)$ be the group of isomorphisms of V onto itself. A *representation* of a group G in V is a group homomorphism ρ from G to $GL(V)$. The dimension of V is called the *degree* of ρ.

Now, Let $\mathbb{F}$ be a field and G be a finite group. Consider the set

$$\mathbb{F}G = \left\{ \sum_{g \in G} c_g g : c_g \in \mathbb{F} \right\}$$

of all formal linear combinations $\sum c_g g$ with all but finitely many c_g equal to 0. With the obvious addition and scalar multiplication, it becomes a vector space over $\mathbb{F}$. Then the algebraic structure $\mathbb{F}G$ given above is the *group algebra* of G over $\mathbb{F}$.

From the above definition, we can define the module as follows.

Definition 2.2.2. Let G be a group and V be a vector space over a field $\mathbb{F}$. Then V is a *module* over the group algebra $\mathbb{F}G$ or simply an $\mathbb{F}G$*-module* if there is a group action of G on V such that the group action respects the linearity of the vector spaces.

And we say a vector subspace W of V is an $\mathbb{F}G$*-submodule* if $gw \in W$ for all $g \in G$ and all $w \in W$.

Next, we will introduce *restrictions* and *induced representation.*

If H is a subgroup of a finite group G, then the restriction of an representation of G to H is automatically a representation of H. Conversely, given a representation of H, there are many ways to construct representations of G.

Definition 2.2.3. Let H be a subgroup of a finite group G, and V be an $\mathbb{F}G$-module. The $\mathbb{F}H$-module V, obtained by restricting the action on V of G to H, is the restriction of V to H, and is denoted by $\mathrm{Res}_H^G V$ or simply $\mathrm{Res}V$ if it is clear which groups are involved. Equivalently, if $\rho : G \to GL(V)$ is a representation of G, then $\rho_H : H \to GL(V)$ defined by $\rho_H(h) = \rho(h)$, $\forall\, h \in H$ is the *restriction* of ρ to H.

Next, let U be an $\mathbb{F}H$-submodule of $\mathbb{F}H$. The action of G on U can be taken just as the ordinary multiplication. Then the $\mathbb{F}G$-module $(\mathbb{F}G)U = \{ru : r \in \mathbb{F}G, u \in U\}$ is the *induced module* of U, and we denote it by $\mathrm{Ind}_H^G U$ or simply $\mathrm{Ind}U$. The representation associated to $\mathrm{Ind}U$ is the *induced representation.*

Definition 2.2.4. Let G be a finite group, and V be a vector space over $\mathbb{C}$. Given a representation $\rho : G \to GL(V)$, the function $\chi : G \to \mathbb{C}$ defined by $\chi(g) = trace(\rho)$ is called the *character* of the representation ρ. Similarly we have the definition of restriction, denote by $\mathrm{Res}\chi$, and *induced character*, denoted by $\mathrm{Ind}\chi$.

Now, we can define the *Artin L-function* associated to a representation.

Definition 2.2.5. Let G be the Galois group of the Galois extension L/K, and ρ be a representation of G over $\overline{\mathbb{Q}}$. Then we define *Artin L-function* as follows.

$$L(s, \chi) \;=\; \prod_p \frac{1}{\det(I - \rho(\mathrm{Frob}(p))p^{-s})} \;=\; \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

where χ is the character of the representation ρ.

Proposition 2.2.6 ([1]). *Let L/K be a Galois extension of number field. then the following equalities were only up to a finite number of Euler factor.*

1. *If χ_1 and χ_2 are characters of* $\mathrm{Gal}(L/K)$, *then*
$$L(s, \chi_1 + \chi_2, L/K) = L(s, \chi_1, L/K) \times L(s, \chi_2, L/K)$$
2. *Let M be an intermediate subfield and $H = \mathrm{Gal}(L/M) < \mathrm{Gal}(L/K)$. If χ is a character of H, then*
$$L(s, \mathrm{Ind}\chi, L/K) = L(s, \chi, L/M)$$

Theorem 2.2.7 ([3]). *Let G be a finite group. Then for each character χ of G, there exist integers n_i and subgroups H_i of G that are either abelian groups or p-groups such that*

$$\chi = \sum n_i \mathrm{Ind}\psi_i,$$

where ψ_i are characters of H_i.

Next, we want to talk about *Hecke L-function*, before that, we need more background as follows.

2.3 Adeles And Ideles

Definition 2.3.1. A field K is a *global field* if K is a number field or a function field of one variable over a finite field. And a *local field* is a locally compact topological field with respect to a non-discrete topology.

It is easy to see, that a local field arises naturally as completions of a global field.

Definition 2.3.2. Let K be a global field and consider the set of all embeddings of K into local fields L such that the image of K is dense in L. Two such embeddings $i : K \to L$ and $i' : K \to L'$ are said to be equivalent if there exists a continuous isomorphism $f : L \to L'$ such that $i' = f \circ i$. An equivalence class is called a *place* of K.

A place is denoted by v, and the corresponding embedding and local field are denoted by i_v and K_v, respectively.

If K is a number field, we say a place of K is *infinite* if it is either a real embedding or a pair of complex-conjugate embeddings. And a place of K is called to be *finite* if it is non-Archimedean place.

Definition 2.3.3. Let K be a global field. For each finite place v, consider a locally compact space K_v and its *valuation ring* R_v. Then the restricted product

$$\mathbb{A}_K = \left\{ (x_v) \in \prod_{v \in V} K_v \ : \ x_v \in \ R_v \textit{ for all but finitely many finite places} \right\}$$

is the *adele ring* of K, and the elements of $\mathbb{A}_K$ are called *adeles*.

Let K be a global field. For each finite place v, consider a locally compact space K_v^* and its *unit group* R_v^*. Then the restricted product

$$\mathbb{I}_K = \left\{ (x_v) \in \prod_{v \in V} K_v^* \ : \ x_v \in \ R_v^* \textit{ for all but finitely many finite places} \right\}$$

is the *idele group* of K, and the elements of $\mathbb{I}_K$ are called *ideles*.

Now, we consider the subgroup $\mathbb{I}_K^1$ of $\mathbb{I}_K$,where

$$\mathbb{I}_K^1 = \{x \in \mathbb{I}_K : \|x\| = 1\}$$

contains all the elements of *modulus* 1. In different situation modulus have several definitions. Here we define modulus $|| \cdot ||$ as

$$||x|| = \begin{cases} |x|, & \textit{if } K = \mathbb{R} \\ x_1^2 + x_2^2, & \textit{if } K = \mathbb{C} \text{ and } x = x_1 + ix_2 \\ q^{-n}, & \textit{if } K \textit{ is non-Archimedean and } x \in \pi^n R^* \end{cases}$$

where the non-Archimedean might be $\mathbb{Q}_p$, p is a prime, or $\mathbb{F}_q[[T]]$ of formoal Laurent series, $q = p^k$ is a prime power. And, we called the factor group $\mathbb{I}_K/K^*$ the *idele class group*. For example, if $K = \mathbb{Q}$, we have $\mathbb{I}_{\mathbb{Q}}/\mathbb{Q}^* \cong \mathbb{R}^+ \times \mathbb{I}_{\mathbb{Q}}^1/\mathbb{Q}^*$

2.4 Hecke Characters

Definition 2.4.1. Let K be a number field. A *Hecke character* or a *Grössencharakter* is a character of the idele class group $\mathbb{I}_K/K^*$.

Definition 2.4.2. Let χ be a Hecke character on $\mathbb{I}_K/K^*$. Define a formal product

$$\mathfrak{m}(\chi) = \prod_v v^{n_v}$$

1. $n_v = 1$, if v is a real place and $\chi_v(-1) = -1$.
2. $n_v = 0$, if v is a complex place or if v is a real place and $\chi_v(-1) = 1$.
3. $n_v = 0$, if $\chi_v(x_v) = 1$ for all $x_v \in R_v^*$.
4. $n_v = e_v$, else, where e_v is the smallest positive integer such that $1 + \pi_v^{e_v} R_v$ is contained in the kernel of χ_v and $\pi_v \in \mathbb{I}_K/K^*$.

The formal product $\mathfrak{m}(\chi)$ is called the *modulus* of the Hecke character.

Definition 2.4.3. Let K be a number filed and χ be a Hecke character. Then we define the associated *Hecke* L*-function* by

$$L(s,\chi) = \prod_{v \text{ is finite}:\chi_v(R_v^*)=1} \frac{1}{1-\chi_v(\pi_v)N(v)^{-s}}$$

A Hecke character is also a generalisation of a *Dirichlet character*, introduced by *Erich Hecke* to construct a class of *L-functions* larger than *Dirichlet L-functions*, and a natural setting for the *Dedekind zeta-functions* and certain others which have functional equations analogous to that of the *Riemann zeta-function.*

For each Hecke L-function, we can give the following functional equation.

Theorem 2.4.4 ([8])**.** *Let χ be a Hecke character on $\mathbb{I}_K/K^*$ and $L(s,\chi)$ be its Hecke L-function. Let r_1^+ be the number of real places v with $\chi_v(-1) = 1$ and r_1^- be the number of real places v with $\chi_v(-1) = -1$. Let r_2 be the number of complex places. Set*

$$Z_{\mathbb{R}}^+(s) = \pi^{-s/2}\Gamma(s/2),\ Z_{\mathbb{R}}^-(s) = \pi^{-(s+1)/2}\Gamma((s+1)/2),\ Z_{\mathbb{C}}(s) = (2\pi)^{1-s}\Gamma(s),$$

and

$$Z_K(s,\chi) = (d_K d_\chi)^{s/2} Z_{\mathbb{R}}^+(s)^{r_1^+} Z_{\mathbb{R}}^-(s)^{r_1^-} Z_{\mathbb{C}}^{r_2} L(s,\chi)$$

where d_K is the absolute value of the discriminant of K. Then $Z_K(s)$ has an analytic continuation to the whole complex plane, except for two simple poles at $s = 0$ and $s = 1$ in the case χ is trivial on $\mathbb{I}_K/K^*$. Moreover it satisfies the functional equation

$$Z_K(s,\chi) = (-i)^{r_1^-} \frac{\tau(\chi)}{d_K^{1/2}} Z_K(1-s,\chi^{-1})$$

where $\tau(\chi)$ is the Gaussian sum associated to χ.

At last, we come back to the Artin L-function. From the definition of an Artin L-function, it is not clear whether it has an analytic continuation to the whole complex plane. But after we introduce the Hecke L-function, and by Proposition 2.2.6, Theorem 2.6.4. We see that every Artin L-function can be written as a product of finitely many Hecke L-functions. And the products is taken over all places including the archimedean ones. So Artin L-function can be meromorphic continued to the whole plane.

2.5 Modular Forms

Definition 2.5.1. We called $SL(2,\mathbb{Z})$ or its subgroup of finite index a *modular group*.

Now, we give $SL(2,\mathbb{Z})$ a group action on upper half-plane $\mathbb{H} = \{\tau = x+iy : x \in \mathbb{R}, y > 0\}$ by the *linear fractional transformation*

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}\ , \text{ for } \tau \in \mathbb{H},\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}).$$

The linear fractional transformations are rigid motions of the hyperplane, and they move points in distinct ways. And an element $\gamma \in SL(2,\mathbb{Z})$ has fixed points, then we give definitions of those γ and fixed points as follows.

Definition 2.5.2. An element $\gamma \in SL(2,\mathbb{Z})$ is *parabolic* if it has one fixed point, *hyperbolic* if it has two distinct fixed points on $\mathbb{P}^1(\mathbb{R})$, *elliptic* if it has a pair of conjugate complex numbers as fixed points. A point in $\mathbb{P}^1(\mathbb{Q})$ fixed by a parabolic element is called a *cusp*, and a point in the upper half-plane fixed by an elliptic element is called an *elliptic point*.

Now, we change our objective to those subgroups of $SL(2,\mathbb{Z})$ with finite index.

Definition 2.5.3. Let Γ be a discrete subgroup of $SL(2,\mathbb{Z})$. If Γ contains the subgroup

$$\Gamma(N) = \left\{ \gamma \in SL(2,\mathbb{Z}) : \gamma \equiv \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

for some positive integer N, then Γ is a *congruence subgroup*. The smallest such positive integer N is the *level* of Γ. The group $\Gamma(N)$ is called the *principal congruence subgroup* of level N.

The following congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) : c \equiv 0 \mod N \right\}$$

is also called the *Hecke congruence subgroups*.

Since they are subgroups of $SL(2,\mathbb{Z})$, we want to ask what indices of them in $SL(2,\mathbb{Z})$ are.

Theorem 2.5.4 ([8]).

$$[SL(2,\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right),$$

$$[\Gamma_0(N) : \Gamma(N)] = N \times \phi(N)$$

where ϕ is the Euler function.

Now, we try to discuss how many inequivalent elliptic points and cusps are there in $\Gamma_0(N)$,

Theorem 2.5.5 ([8]). *For $N \geqslant 2$, we have,*

1. *The number of inequivalent elliptic points of $\Gamma_0(N)$ of order 2*

$$v_2(\Gamma_0(N)) = \begin{cases} 0, & \text{if } 4|N \\ \prod_{p|N} (1 + \left(\frac{-1}{p}\right)), & \text{if } 4 \nmid N. \end{cases}$$

2. *The number of inequivalent elliptic points of* $\Gamma_0(N)$ *of order* 3

$$v_3(\Gamma_0(N)) = \begin{cases} 0, & \text{if } 9|N \\ \prod\limits_{p|N}(1+\left(\frac{-3}{p}\right)), & \text{if } 9 \nmid N. \end{cases}$$

3. *The number of inequivalent cusps of* $\Gamma_0(N)$

$$v_\infty = \sum_{0<d|N} \phi((d, N/d))$$

where $(\frac{\cdot}{p})$ *is the Legendre symbol and* ϕ *is the Euler function.*

And for each modular group Γ we give a theorem to calculate the *genus* g as follows.

Theorem 2.5.6 ([8])**.** *Let* Γ *is a modular group, and the index* $[SL(2,\mathbb{Z}):\Gamma] = m$*. Let* v_2, v_3, v_∞ *be the number of inequivalent elliptic point of order 2, order 3, and cusps, respectively. Then the genus* g *of* Γ *is given by the formula:*

$$g = 1 + \frac{m}{12} - \frac{v_2}{4} - \frac{v_3}{3} - \frac{v_\infty}{2}.$$

Definition 2.5.7. A function f is said to be a *modular form* of *weight* k on Γ if it satisfies the following conditions,

1. f is holomorphic in the upper half-place $\mathbb{H}$.

2. $f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$ for every $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in the modular group Γ.

3. f is holomorphic at every cusps.

Moreover, if f vanishes at every cusp, then the function f is a *cusp form* of weight k. And for convenience, let $\mathcal{M}_k(\Gamma)$ denotes the space which contains all modular forms of wright k on Γ, and $\mathcal{S}_k(\Gamma)$ denote the space which contains all cusp forms of weight k with respect to Γ.

If a modular form f be written as a Fourier expansion and a_n be the Fourier coefficients, then we put

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

$L(s, f)$ converges absolutely and uniformly for $\Re(s) > 1+k/2$, then we called $L(s, f)$ the L-function associated with f.

For each L-function associated with a modular form f we also have a functional equation as follow.

Theorem 2.5.8 ([8])**.** *For* $N > 0$ *be the level of the modular form* f*, we let*

$$\Lambda_N(s, f) = \left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s) L(s, f),$$

then the following functional equation will hold

$$\Lambda_N(s, f) = \Lambda_N(k-s, g)$$

where k *is the weight of* f*, and* $g(z) = (-i\sqrt{N}z)^{-k} f(-1/Nz)$*.*

Now, we are going to define the divisor of a holomorphic in $\mathbb{H}$.

Definition 2.5.9. For a nonzero holomorphic function f, we define the *divisor* of f by

$$div(f) = \sum_{a} v_a(f)a$$

where a runs over all elliptic points and cusps, and $v_a(f)$ denotes the order of f at a.

Then for the divisor of holomorphic in $\mathbb{H}$, we define the degree of the divisor as follows theorem.

Theorem 2.5.10 ([8])**.** *Let k be an odd integer. Assume -1 is not contained in a modular group Γ. For a nonzero element f, f is an meromorphic form of weight k with respect to Γ, then we have,*

$$deg(div(f)) = k(g-1) + \frac{k}{2}\sum_{\mathrm{a}}(1 - \frac{1}{e_{\mathrm{a}}})$$

where $\mathrm{a} \in \Gamma\backslash\mathbb{H}^*$*,* e_{a} *is the ramification index of* a*,* g *is genus of* f*.*

2.6 Hecke Operators

Now, we try to introduce Hecke operator. Let G be a group, and Γ and Γ' are two subgroups of G. We say that Γ and Γ' are *commensurable* if

$$[\Gamma : \Gamma \cap \Gamma'] < \infty \text{ and } [\Gamma' : \Gamma \cap \Gamma'] < \infty.$$

Definition 2.6.1. For $N \in \mathbb{N}$, if $\alpha \in GL^+(2, \mathbb{Z})$, and $\Gamma_0(N)$ and $\alpha^{-1}\Gamma_0(N)\alpha$ are commensurable. The double coset $\Gamma_0(N)\alpha\Gamma_0(N)$ is a finite union of right coset,

$$\Gamma_0(N)\alpha\Gamma_0(N) = \bigcup_{i=1}^{h} \Gamma_0(N)\alpha_i,$$

where $\alpha_i \in GL^+(2, \mathbb{Z})$, $h = \left[\Gamma_0(N) : \Gamma_0(N) \bigcap \alpha^{-1}\Gamma_0(N)\alpha\right]$ Then we define a linear operator $[\Gamma_0(N)\alpha\Gamma_0(N)]$ on all $f \in \mathcal{M}_k(\Gamma_0(N))$ by

$$f|\left[\Gamma_0(N)\alpha\Gamma_0(N)\right]_k = \sum f|\alpha_i.$$

Then we call the linear operator $[\Gamma_0(N)\alpha\Gamma_0(N)]$ as a *Hecke operator*.

Definition 2.6.2. For each divisor d of N, let i_d be the map

$$i_d : (\mathcal{S}_k(\Gamma_0(Nd^{-1})) \times (\mathcal{S}_k(\Gamma_0(Nd^{-1}))) \to \mathcal{S}_k(\Gamma_0(N))$$

given by

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

The subspace of *oldforms at level* N is

$$\mathcal{S}_k(\Gamma_0(N))^{\text{old}} = \sum_{p|N \text{ p is prime}} i_p(\mathcal{S}_k(\Gamma_0(Np^{-1})) \times \mathcal{S}_k(\Gamma_0(Np^{-1})))$$

and the subspace of *newforms at level* N is the orthogonal complement with respect to the Petersson inner product,

$$\mathcal{S}_k(\Gamma_0(N))^{\text{new}} = (\mathcal{S}_k(\Gamma_0(N))^{\text{old}})^{\perp}$$

Definition 2.6.3. We say a nonzero $f \in \mathcal{M}_k(\Gamma_0(N))$ is an *Hecke eigenform* if it is an eigenform for Hecke operators. And we say the eigenform $f = \sum_{n=0}^{\infty} a_n q^n$ is *normalized* if $a_1 = 1$. Moreover a *newform* is a normalized eigenform in $\mathcal{S}_k(\Gamma_0(N))^{\text{new}}$.

Then, for a normalized eigenform f, there is a theorem such that $L(s, f)$ has an Euler product expansion.

Theorem 2.6.4 ([6])**.** *Let $f = \sum_{n=0}^{\infty} a_n q^n$, $q = e^{2\pi i \tau}$ be a modular form with a character χ. The following are equivalent.*

1. *f is a normalized eigenform.*
2. *$L(s, f)$ has an Euler product expansion*

$$L(s, f) = \prod_p (1 - a_p p^{-s} + \chi(p) p^{k-1-2s})^{-1},$$

where the product is taken over all primes, k is the weight of f.

Chapter 3

The Detail Of Serre's Examples

In this chapter, we will use some basic knowledge that we introduced in Chapter 2 to explain Serre's example $f(x) = x^3 - x - 1$.

First, we give some precise result corresponding to the table we gave in Chapter 1. Using Maple, we can easily check that

$$f(x) = x^3 - x - 1 \equiv \begin{cases} x^3 + x + 1 \quad \text{mod } 2 \\ (x^2 + 2x + 3)(x - 2) \quad \text{mod } 5 \\ (x - 10)^2(x - 3) \quad \text{mod } 23 \\ (x - 4)(x - 13)(x - 42) \quad \text{mod } 59 \\ \quad\quad \vdots \end{cases}$$

For convenience, follows primes appear in this chapter do not equal to 23.

3.1 Use Cyclic Group To Determine $N_p(f)$

In this section, we try to determine $N_p(f)$ in algebraic number theory. We give the following theorem to help us determine $N_p(f)$ from the order of $\mathrm{Frob}(\mathfrak{P}|p)$.

Theorem 3.1.1. *Let L be the splitting field of $f(x) = x^3 - x - 1$ over $\mathbb{Q}$, and the Galois group* $\mathrm{Gal}(L/\mathbb{Q})$ *is identified with S_3. If*

1. $\mathrm{Frob}(\mathfrak{P}|p) = e$, *then* $N_p(f) = 3$.
2. $\mathrm{Frob}(\mathfrak{P}|p) \in \{(12)\}$, *then* $N_p(f) = 1$.
3. $\mathrm{Frob}(\mathfrak{P}|p) \in \{(123)\}$, *then* $N_p(f) = 0$.

where the permutation (123) *means that the* $\mathrm{Frob}(\mathfrak{P}|p)$ *acts three roots in L transitively. Similarly, if* $\mathrm{Frob}(\mathfrak{P}|p) \in \{(12)\}$, *then we say* $\mathrm{Frob}(\mathfrak{P}|p)$ *has order 2 and fixes a root in L.*

Proof. Assume that f has three distinct roots, names α_1, α_2, α_3 in L.

Note that $\mathrm{Frob}(\mathfrak{P}|p) \in D(\mathfrak{P}|p)$, then by Proposition 2.1.7, then for all $a \in \mathcal{O}_L$ we have an automorphism

$$\overline{\mathrm{Frob}(\mathfrak{P}|p)} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P} \text{ is defined by } \overline{\mathrm{Frob}(\mathfrak{P}|p)}(a + \mathfrak{P}) = \mathrm{Frob}(\mathfrak{P}|p)(a) + \mathfrak{P}.$$

And a canonical homomorphism

$$\gamma : \mathcal{O}_L \to \mathcal{O}_L/\mathfrak{P} \text{ is defined by } \gamma(a) = a + \mathfrak{P}.$$

Such that $\overline{\text{Frob}(\mathfrak{P}|p)} \circ \gamma = \gamma \circ \text{Frob}(\mathfrak{P}|p)$, and $\overline{\text{Frob}(\mathfrak{P}|p)}$ fixes $\mathbb{Z}/p\mathbb{Z}$ pointwise.

If $\text{Frob}(\mathfrak{P}|p) = e$, that says $\text{Frob}(\mathfrak{P}|p)$ fixes α_1, α_2, α_3. We have $\text{Frob}(\mathfrak{P}|p)(\alpha_i) = \alpha_i$ for $i = 1, 2, 3$. Then

$$\overline{\text{Frob}(\mathfrak{P}|p)}(\gamma(\alpha_i)) = \overline{\text{Frob}(\mathfrak{P}|p)}(\alpha_i + \mathfrak{P}) = \text{Frob}(\mathfrak{P}|p)(\alpha_i) + \mathfrak{P} = \alpha_i + \mathfrak{P},$$

so we have $\overline{\text{Frob}(\mathfrak{P}|p)}$ fixes $\alpha_i + \mathfrak{P}$, that means there is an embedding $i : \mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_L/\mathfrak{P}$ is defined by $i(a + p\mathbb{Z}) = a + \mathfrak{P}$ for all $a \in \mathbb{Z}$. And $\alpha_i + \mathfrak{P}$ is contained in the image of i. Thus, there exist an element $a_i \in \mathbb{Z}$ such that $i(a_i + p\mathbb{Z}) = \alpha_i + \mathfrak{P}$.

Now, we will claim that $a_i + \mathfrak{P}$ are roots of f in $\mathbb{Z}/p\mathbb{Z}$. Consider the norm of $f(a_i + \mathfrak{P})$, easy to check that will be divided by p for $i = 1, 2, 3$. Thus, if $\text{Frob}(\mathfrak{P}|p) = e$, then $N_p(f) = 3$.

We can show the other two cases by the same argument. □

3.2 Relation Between $N_p(f)$ And Legendre Symbols

From above section, we know the relation between $N_p(f)$ and the order of Frobenius automorphism. Now we can use that to describe the Serre's example precisely.

For $p \neq 23$, one has,

$$N_p(f) = \begin{cases} 0 \text{ or } 3 & \text{if } \left(\frac{p}{23}\right) = 1 \\ 1 & \text{if } \left(\frac{p}{23}\right) = -1. \end{cases}$$

Assume $\left(\frac{p}{23}\right) = -1$. Consider that $\mathbb{Q}(\sqrt{-23}) \subset L$, and $\left(\frac{p}{23}\right) = -1$ says that p is inert in $\mathbb{Q}(\sqrt{-23})$, so $\text{Frob}(\mathfrak{P}|p)$ has order 2. Thus, $N_p(f) = 1$.

For $\left(\frac{p}{23}\right) = 1$, in Serre's article, we have that p can be written either as $x^2 + xy + 6y^2$ or $2x^2 + xy + 3y^2$ with $x, y \in \mathbb{Z}$, in the first case, one has $N_p(f) = 3$, another case, $N_p(f) = 0$. Now, we give a Theorem to describe this statement completely.

Theorem 3.2.1 ([5]). *Let m be an integer, $m \equiv 1 \mod 4$. Then there is a monic irreducible polynomial $f_m(x) \in \mathbb{Z}[x]$ of degree $h(m)$ (Where $h(m)$ denotes the ideal class number of $K = \mathbb{Q}(\sqrt{m})$.) such that if an odd prime p divides neither n nor the discriminant of $f_m(x)$, then*

$$p = x^2 + xy + \frac{1 - d_K}{4} y^2$$
$$\Leftrightarrow \quad \left(\frac{d_K}{p}\right) = 1 \text{ and } f_m(x) \equiv 0 \mod p \text{ has a integer solution.}$$

Where, d_K is the discriminant of $\mathbb{Q}(\sqrt{m})$. Furthermore, $f_m(x)$ may be taken to be the minimal polynomial of a real algebraic integer α for which $L = K(\alpha)$ is the Hilbert class field. And $f_m(x)$ is said to be the Hilber class polynomial.

In Theorem 3.2.1, fortuitously, the Hilbert class polynomial is same as $f(x) = x^3 - x - 1$. Since the field L is a cubic cyclic extension of the quadratic field $K = \mathbb{Q}(\sqrt{-23})$, it is unramified, and since $h(-23) = 3$. So L is the Hilbert class field of K.

That is why if p can be written as $x^2 + xy + 6y^2$ then $N_p(f) = 3$. The other case, if $p = 2x^2 + xy + 3y^2$ for some $x, y \in \mathbb{Z}$, since the prime is not inert in $\mathbb{Q}(\sqrt{-23})$, and it will not satisfy Theorem 3.2.1, so in this case $N_p(f) = 0$.

Chapter 4

Main Results

Theorem 4.0.2. *Let $N_p(f)$ denotes the number of roots for a given polynomial $f(x) = x^4 - 2$ in $\mathbb{Z}/p\mathbb{Z}$. Then we have $N_p(f) = a_p + 1 + \left(\frac{2}{p}\right)$, where a_p is the Fourier coefficient of prime terms in a cusp form of weight 1 on $\Gamma_0(256)$. The cusp form we find is*

$$\begin{aligned} F(\tau) &= \frac{1}{2}\left(\sum_{m,n\in\mathbb{Z}} q^{m^2+64n^2} - \sum_{m,n\in\mathbb{Z}} q^{4m^2+4mn+17n^2}\right) \\ &= q + q^9 - 2q^{17} - q^{25} - 2q^{41} + q^{49} + 2q^{73} + \cdots \end{aligned}$$

4.1 Galois Group Of f Is Isomorphic To D_4

Now, we claim that the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ of the polynomial $f(x) = x^4 - 2$ is isomorphic to D_4. The simplest way to describe the Galois group of f is write down all the automorphisms of $\mathbb{Q}(\sqrt[4]{2}, i)$.

$$\begin{array}{rlrl}
\mathrm{id} : & \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto i \end{cases} & \tau : & \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{cases} \\
\sigma : & \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2}i \\ i \mapsto i \end{cases} & \sigma\tau : & \begin{cases} \sqrt[4]{2} \mapsto \sqrt[4]{2}i \\ i \mapsto -i \end{cases} \\
\sigma^2 : & \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2} \\ i \mapsto i \end{cases} & \sigma^2\tau : & \begin{cases} \sqrt[4]{2}- \mapsto \sqrt[4]{2} \\ i \mapsto -i \end{cases} \\
\sigma^3 : & \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2}i \\ i \mapsto i \end{cases} & \sigma^3\tau : & \begin{cases} \sqrt[4]{2} \mapsto -\sqrt[4]{2}i \\ i \mapsto -i. \end{cases}
\end{array}$$

It is easy to check that our statement is true. For the Dihedral group of order 8, we give the following character table.

	e	σ^2	$\{\tau, \sigma^2\tau\}$	$\{\sigma, \sigma^3\}$	$\{\sigma\tau, \sigma^3\tau\}$
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

4.2 $N_p(f)$ Is A Class Function Of Frobenius

Similarly, the discriminant of $f(x) = x^4 - 2$ is -2048, thus the only prime p of $\mathbb{Z}$ ramified in $\mathbb{Q}(\sqrt[4]{2}, i)$ is 2. We consider the case $p = 2$ specially. An easy compution gives $x^4 - 2 \equiv x^4 \mod 2$. Thus, $N_2(f) = 1$.

After that, we will start to compute another $N_p(f)$ for $p \neq 2$. There is a Theorem just like Theorem 3.1.1.

The following theorem gives the notation in D_4 as permutations, but we use the notations σ, τ to denote the mapping in D_4. There is a question. How to connect two kinds symbol? Since σ acts on $\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}$, $-\sqrt[4]{2}i$ transitively, then we note that $\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}$, $-\sqrt[4]{2}i$ as 1, 2, 3, 4, respectively. So σ corresponds to (1234), and the others have following relations.

$$\begin{aligned}
\{\sigma\tau, \sigma^3\tau\} &\quad \text{corresponds to} \quad \{(12)(34)\}, \\
\{\tau, \sigma^2\tau\} &\quad \text{corresponds to} \quad \{(12)\}, \\
\{\sigma, \sigma^3\} &\quad \text{corresponds to} \quad \{(1234)\}, \\
\sigma^2 &\quad \text{corresponds to} \quad (13)(24), \\
e &\quad \text{corresponds to} \quad e.
\end{aligned}$$

So we can give a theorem as follows.

Theorem 4.2.1. *Let L be the splitting field of $f(x) = x^4 - 2$, and the Galois group* $\mathrm{Gal}(L/\mathbb{Q})$ *is isomorphic to D_4. If*

1. $\mathrm{Frob}(\mathfrak{P}|p) = e$*, then* $N_p(f) = 4$
2. $\mathrm{Frob}(\mathfrak{P}|p) = (13)(24)$*, then* $N_p(f) = 0$
3. $\mathrm{Frob}(\mathfrak{P}|p) \in \{(1234)\}$*, then* $N_p(f) = 0$
4. $\mathrm{Frob}(\mathfrak{P}|p) \in \{(12)\}$*, then* $N_p(f) = 2$
5. $\mathrm{Frob}(\mathfrak{P}|p) \in \{(12)(34)\}$*, then* $N_p(f) = 0$

Proof. Use same argument as Theorem 3.1.1. □

Now we try to connect $N_p(f)$ and $\mathrm{Frob}(\mathfrak{P}|p)$. Before that, we need to determine that what conjugacy classes are those $\mathrm{Frob}(\mathfrak{P}|p)$ contained in D_4.

Lemma 4.2.2. *For the prime*

1. $p \equiv 3 \mod 8$*,* $\mathrm{Frob}(\mathfrak{P}|p) \in \{\sigma\tau, \sigma^3\tau\}$.

2. $p \equiv 5 \mod 8$, $\mathrm{Frob}(\mathfrak{P}|p) \in \{\sigma, \sigma^3\}$.

3. $p \equiv 7 \mod 8$, $\mathrm{Frob}(\mathfrak{P}|p) \in \{\tau, \sigma^2\tau\}$.

Before we prove this Lemma, we need two lemmas.

Lemma 4.2.3 ([7])**.**

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

Lemma 4.2.4 ([7])**.**

$$\left(\frac{2}{p}\right) \equiv \begin{cases} 1 & \textit{if } p \equiv \pm 1 \mod 8 \\ -1 & \textit{if } p \equiv \pm 3 \mod 8. \end{cases}$$

Now, we can start our proof.

Proof of Lemma 4.2.2. For $p \equiv 3 \mod 8$, assume that p splits as $\mathfrak{P}_1, \cdots, \mathfrak{P}_k$ in $\mathbb{Q}(\sqrt[4]{2}, i)$. Then the Frobenius automorphism of $\mathfrak{P}$ over p, $\mathrm{Frob}(\mathfrak{P}|p)$ will satisfy following equation.

$$\mathrm{Frob}(\mathfrak{P}|p)(\sqrt[4]{2}) \equiv (\sqrt[4]{2})^{N(p)} \mod \mathfrak{P},$$

$$\mathrm{Frob}(\mathfrak{P}|p)(i) \equiv i^{N(p)} \mod \mathfrak{P}.$$

First, we consider how $\mathrm{Frob}(\mathfrak{P}|p)$ acts on i, from the above equation, we have

$$\mathrm{Frob}(\mathfrak{P}|p)(i) \equiv i^{8k+3} \mod \mathfrak{P}, \text{ for some } k \in \mathbb{Z},$$

It is easy to check that $\mathrm{Frob}(\mathfrak{P}|p)$ sends i to $-i$.

Next, we observe that how $\mathrm{Frob}(\mathfrak{P}|p)$ acts on $\sqrt[4]{2}$. Similarly, since $\mathrm{Frob}(\mathfrak{P}|p) \in \mathrm{Gal}(L/\mathbb{Q})$, so it sends $\sqrt[4]{2}$ to its conjugate element $\sqrt[4]{2}$, $\sqrt[4]{2}i$, $-\sqrt[4]{2}$, $-\sqrt[4]{2}i$, so we let ϵ be the fourth root of unity such that $\mathrm{Frob}(\mathfrak{P}|p)(\sqrt[4]{2}) = \epsilon\sqrt[4]{2}$. Then, we can rewrite the equation as follows,

$$\begin{aligned} \epsilon \cdot \sqrt[4]{2} &\equiv (\sqrt[4]{2})^p \mod \mathfrak{P}, \text{ where } \epsilon \in \{\pm 1, \ \pm i\}. \\ \text{thus,} \quad \epsilon &\equiv 2^{(p-1)/4} \mod \mathfrak{P}, \end{aligned}$$

Since $p \equiv 3 \mod 8$, by Lemma 4.2.3 and Lemma 4.2.4, we have,

$$-1 \equiv \left(\frac{2}{p}\right) \equiv 2^{(p-1)/2} \mod p.$$

Thus, we know that $p|(2^{(p-1/2)} + 1)$ so $\mathfrak{P}|(2^{(p-1)/2} + 1)$. Then we have,

$$\begin{aligned} 2^{(p-1)/2} &\equiv -1 \mod \mathfrak{P}, \\ \text{thus,} \quad 2^{(p-1)/4} &\equiv \pm i \mod \mathfrak{P}. \end{aligned}$$

Finially, we conclude that $\epsilon \equiv \pm i \mod \mathfrak{P}$. That says $\mathrm{Frob}(\mathfrak{P}|p)(\sqrt[4]{2}) = \pm\sqrt[4]{2}i$. Thus,we have that for $p \equiv 3 \mod 8, \mathrm{Frob}(\mathfrak{P}|p) \in \{\sigma\tau, \sigma^3\tau\}$.

Next, for $p \equiv 5 \mod 8$ and $p \equiv 7 \mod 8$, we can give the proof by same argument as the case $p \equiv 3 \mod 8$. □

So, for the prime p not congruence to 1 modulo 8, we have known that $N_p(f)$ precisely. How about the prime p congruence to 1 modulo 8? Unfortunately, we can not decide what conjugacy classes will contain the $\mathrm{Frob}(\mathfrak{P}|p)$ precisely by Lemma 4.2.2. But, we have another way to determine the $\mathrm{Frob}(\mathfrak{P}|p)$ case by case.

Now, we compute an example $p = 3$ with another algorithm, we using the norm of p to determine the $\mathrm{Frob}(\mathfrak{P}|p)$.

Example 4.2.5. We consider the prime $p = 3$ in $\mathbb{Z}$. Although, we do not know how the prime ideal (3) splits in $\mathbb{Q}(\sqrt[4]{2}, i)$. But, without lost of generality, we can assume that (3) splits as $\mathfrak{P}_1\mathfrak{P}_2 ... \mathfrak{P}_k$ in $\mathbb{Q}(\sqrt[4]{2}, i)$. And that no matter which $\mathfrak{P}$ we pick, the $\mathrm{Frob}(\mathfrak{P}|3)$ will satisfy

$$\mathrm{Frob}(\mathfrak{P}|3)(\sqrt[4]{2}) \equiv (\sqrt[4]{2})^3 \mod \mathfrak{P}$$

$$\text{and } \mathrm{Frob}(\mathfrak{P}|3)(i) \equiv (i)^3 \mod \mathfrak{P}.$$

Since $\mathrm{Frob}(\mathfrak{P}|3) \in \mathrm{Gal}(L/\mathbb{Q})$, then there also exist a fourth root of unity ϵ such that $\mathrm{Frob}(\mathfrak{P}|3)(\sqrt[4]{2}) = \epsilon(\sqrt[4]{2})$. Then, we just need to determine that $\epsilon = \pm 1$ or $\pm\, i$ precisely.

From above two equations we have, $\epsilon\sqrt[4]{2} \equiv (\sqrt[4]{2})^3 \mod \mathfrak{P}$ (ie. $\epsilon \equiv \sqrt{2} \mod \mathfrak{P}$). and we know that $\mathfrak{P}|(3)$, so $N^L_{\mathbb{Q}}(\sqrt{2} - \epsilon)$ must dividing by 3. So ϵ has to be $\pm i$. Thus we can make sure that $\mathrm{Frob}(\mathfrak{P}|3)$ sends $\sqrt[4]{2}$ to $\pm\sqrt[4]{2}i$.

Next, we want to know that, how $\mathrm{Frob}(\mathfrak{P}|3)$ acts on i. By the same argument, we have $\mathrm{Frob}(\mathfrak{P}|3)(i) \equiv i^3 \mod \mathfrak{P}$. Again, from above equation, and we have $\mathrm{Frob}(\mathfrak{P}|3)(i) = \pm i$ since it contained in the Galois group. Obviously, it has to be $-i$.

Thus, we have

$$\mathrm{Frob}(\mathfrak{P}|3) : \begin{cases} \sqrt[4]{2} \mapsto \pm\sqrt[4]{2}i \\ i \mapsto -i. \end{cases}$$

Then

$$\mathrm{Frob}(\mathfrak{P}|3) \in \left\{\sigma\tau, \sigma^3\tau\right\}.$$

Now we have another algorithm, and we know that really works. So we can try to determine the Frobenius automorphism of $\mathfrak{P}$ over $p \equiv 1 \mod 8$.

Example 4.2.6. For $p = 17$, we also assume that (17) splits as $\mathfrak{P}_1\mathfrak{P}_2 ... \mathfrak{P}_k$ in $\mathbb{Q}(\sqrt[4]{2}, i)$. Then the $\mathrm{Frob}(\mathfrak{P}|17)$ will satisfy that

$$\mathrm{Frob}(\mathfrak{P}|17)(i) \equiv i^{17} \mod \mathfrak{P}.$$

Easy to check that $\mathrm{Frob}(\mathfrak{P}|p)(i) = i$. We also have

$$\mathrm{Frob}(\mathfrak{P}|17)(\sqrt[4]{2}) \equiv (\sqrt[4]{2})^{17} \mod \mathfrak{P},$$

as above, there exist a fourth root of unity ϵ such that $\mathrm{Frob}(\mathfrak{P}|17)(\sqrt[4]{2}) = \epsilon\sqrt[4]{2}$. Then we rewrite the equation as

$$\epsilon\sqrt[4]{2} \equiv (\sqrt[4]{2})^{17} \mod \mathfrak{P}.$$

Obviously, $\epsilon = -1$, that says $\mathrm{Frob}(\mathfrak{P}|p)(\sqrt[4]{2}) = -\sqrt[4]{2}$. Thus, $\mathrm{Frob}(\mathfrak{P}|p) = \sigma^2$.

Using the above algorithm we can determine that, for $p = 17,\ 41,\ 73$, the $\mathrm{Frob}(\mathfrak{P}|p)$ are $\sigma^2,\ \sigma^2,\ e$ respectively. Although, this way looks like very inefficient, but it can determine all kinds of prime.

Now, we want to find the relation between $N_p(f)$ and a_p. Note $a_p = \chi_5(\mathrm{Frob}(\mathfrak{P}|p))$, then we have

$$a_p = \begin{cases} 2, & \text{if } \mathrm{Frob}(\mathfrak{P}|p) = e \\ -2, & \text{if } \mathrm{Frob}(\mathfrak{P}|p) = \sigma^2 \\ 0, & \text{else.} \end{cases}$$

From $\mathrm{Frob}(\mathfrak{P}|p) = e$, we have $N_p(f) = a_p + 2$. And $\mathrm{Frob}(\mathfrak{P}|p) = \sigma^2$ tells us $N_p(f) = a_p + 2$. Similarly $\mathrm{Frob}(\mathfrak{P}|p) \in \{\tau, \sigma^2\tau\}$ gives $N_p(f) = a_p + 2$. Then we have

$$\begin{aligned} N_p(f) &= a_p + 1 + \left(\frac{2}{p}\right) \\ &= \chi_5(\mathrm{Frob}(\mathfrak{P}|p)) + \chi_1(\mathrm{Frob}(\mathfrak{P}|p)) + \chi_3(\mathrm{Frob}(\mathfrak{P}|p)). \end{aligned}$$

That is our first result.

4.3 Construct A Cusp Form

We start from the Artin L-function,

$$L(s,\chi_5) = \prod_{\mathrm{Frob}(p)=e} \frac{1}{(1-p^{-s})^2} \times \prod_{\mathrm{Frob}(p)=\sigma^2} \frac{1}{(1+p^{-s})^2} \times \prod_{\mathrm{Frob}(p)\in\{\tau,\tau\sigma^2\}} \frac{1}{(1-p^{-2s})} \times$$

$$\prod_{\mathrm{Frob}(p)\in\{\sigma,\sigma^3\}} \frac{1}{(1+p^{-2s})} \times \prod_{\mathrm{Frob}(p)\in\{\tau\sigma,\tau\sigma^3\}} \frac{1}{(1-p^{-2s})} \times \prod_{p \textit{ is ramified}} * = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Those ramified primes are not particularly important in our consideration. Thus, by the Proposition 2.2.6 and Theorem 2.6.4. We have

$$L(s,\chi_5) \;=\; L(s, \mathrm{Ind}\psi, L/\mathbb{Q}) \;=\; L(s,\psi,L/K)$$

where K is $\mathbb{Q}(i)$, $\chi_5 = \mathrm{Ind}\psi$, and ψ should be a Hecke character corresponding to $\mathbb{Q}(i)$. The Hecke character ψ gives values as following table.

$\mathrm{Frob}(p)$	e	σ	σ^2	σ^3
$\psi(p)$	1	i	-1	$-i$

Now, we try to find a modular form F such that $L(s,F) = L(s,\psi)$. So F should be written as $\sum_{n=1}^{\infty} a_n q^n$, where $q = e^{2\pi i\tau}$, that says F is a cusp form. Next, we try to explain that why the cusp form F with weight 1 of level 256.

From Theorem 2.5.8, the Dirichlet series associated with F, $L(s,F)$ will satisfy the functional equation

$$\left(\frac{2\pi}{\sqrt{N}}\right)^{-s} \Gamma(s)L(s,F) = \left(\frac{2\pi}{\sqrt{N}}\right)^{-(k-s)} \Gamma(k-s)L(k-s,G) \tag{4.1}$$

where k and N are the weight and level of F. And from Theorem 2.4.4, the Hecke L-function $L(s,\psi)$ will satisfy the functional equation

$$\left(\frac{2\pi}{\sqrt{d_K d_\psi}}\right)^{-s} \Gamma(s)L(s,\psi) = \epsilon \left(\frac{2\pi}{\sqrt{d_K d_\psi}}\right)^{-(1-s)} \Gamma(1-s)L(1-s,\psi^{-1}). \tag{4.2}$$

where ϵ is a root of unity and d_K is the discriminant of K takes absolute value, d_ψ is the norm of modulus of ψ. Remember that, our goal is finding a modular form F such that $L(s,F) = L(s,\psi)$. Compare (4.1) and (4.2) we have weight $k = 1$ and level $N = d_K \times d_\psi$.

In the Hecke L-function $L(s,\psi,L/K)$, ψ is a Hecke character of modulus $(1+i)^k$, since the only prime ramifies in $\mathcal{O}_L$ is 2. And ψ takes values $\pm i$, so we have a property, that $(\mathbb{Z}[i]/\mathfrak{m})^*$ has a non-unit element of order 4. Apply the definition of modulus, in this case $\mathfrak{m} = (1+i)^k$ for some $k \in \mathbb{N}$.

Note that, if k=1, then $|(\mathbb{Z}[i]/\mathfrak{m})^*| = 1$.
If k=2, then $|(\mathbb{Z}[i]/\mathfrak{m})^*| = 2$. *ie.* $(\mathbb{Z}[i]/\mathfrak{m})^* \cong \mathbb{Z}_2$
If k=3, then $|(\mathbb{Z}[i]/\mathfrak{m})^*| = 4$. *ie.* $(\mathbb{Z}[i]/\mathfrak{m})^* \cong \mathbb{Z}_4$
If k=4, then $|(\mathbb{Z}[i]/\mathfrak{m})^*| = 8$. *ie.* $(\mathbb{Z}[i]/\mathfrak{m})^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2$
If k=5, then $|(\mathbb{Z}[i]/\mathfrak{m})^*| = 16$. *ie.* $(\mathbb{Z}[i]/\mathfrak{m})^* \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
If k=6, then $|(\mathbb{Z}[i]/\mathfrak{m})^*| = 32$. *ie.* $(\mathbb{Z}[i]/\mathfrak{m})^* \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$
so the modulus $\mathfrak{m}$ is $(1+i)^6$

Thus, we can conclude that the level of cusp form here is 256.

Now, we know the level of cusp form is 256, then we can use the algorithm in [5], there are four primitive quadratic forms

$$m^2 + 64n^2,\ 5m^2 \pm 2mn + 13n^2,\ 4m^2 + 4mn + 17n^2$$

might be a part of the exponent of cusp form.

Consider the series

$$a\sum_{m,n\in\mathbb{Z}} q^{m^2+64n^2} + b\sum_{m,n\in\mathbb{Z}} q^{5m^2+2mn+13n^2}$$
$$+c\sum_{m,n\in\mathbb{Z}} q^{5m^2-2mn+13n^2} + d\sum_{m,n\in\mathbb{Z}} q^{4m^2+4mn+17n^2}$$

for some $a, b, c, d \in \mathbb{Q}$, where $q = e^{2\pi i\tau}$. And the expansion of each series are

$$\sum_{m,n\in\mathbb{Z}} q^{m^2+64n^2} = 1 + 2q + 2q^4 + 2q^9 + \cdots$$

$$\sum_{m,n\in\mathbb{Z}} q^{5m^2+2mn+13n^2} = 1 + 2q^5 + 2q^{13} + 2q^{16} + 4q^{20} + 2q^{29} + 2q^{37} + \cdots$$

$$\sum_{m,n\in\mathbb{Z}} q^{4m^2+4mn+17n^2} = 1 + 2q^4 + 2q^{16} + 4q^{17} + 4q^{25} + 2q^{36} + 4q^{41} + \cdots$$

Now, we consider a modular form,

$$\begin{aligned} F(\tau) &= \frac{1}{2}\left(\sum_{m,n\in\mathbb{Z}} q^{m^2+64n^2} - \sum_{m,n\in\mathbb{Z}} q^{4m^2+4mn+17n^2}\right) \\ &= q + q^9 - 2q^{17} - q^{25} - 2q^{41} + q^{49} + 2q^{73} + \cdots \end{aligned}$$

Fortunately, for the first 73 terms, the coefficients of prime terms are just equal to a_p for each prime p.

But, how can we make sure that every terms after 73 are also equal? In fact, we only need to check the degree of divisor terms. Since the degree of divisor means the summation of orders of cusps, elliptic points (here, we only have cusps), so the order of $i\infty$ is equal or less then the degree of divisor.

In our discussion, the notation a in the Theorem 2.5.10 are just cusps, thus, 1/a are all zeros, then the summation in the degree of divisor is just the number of inequivalent cusps. Using Theorem 2.5.5, we know that there has 24 inequivalent cusps. And we use Theorem 2.5.6 to compute the genus of F. Before that, we need Theorem 2.5.4 to evaluate the index $m = 384$, and by Theorem 2.5.5 we have $v_2 = 0, v_3 = 0, v_\infty = 24$. Thus the genus g equals 21.

Now, from Theorem 2.5.10 we can compute the degree of divisor of F is 32. So we only need to compare first 32 terms. We compare first 73 terms already, then we can make sure the cusp form's Fourier coefficients are equal to a_p for every prime terms.

Moreover, since a_n are Hecke eigenvalues and from the functional equation we have F has level 256. Thus, F is a newform. Then the Theorem 2.6.4 can help us to write $L(s, F)$ as an Euler product.

$$L(s,F) = \prod_p \left(1 - a_p p^{-s} + \left(\frac{-2}{p}\right) p^{-2s}\right)^{-1}.$$

Bibliography

[1] Emil Artin. *Zur Theorie de L-Reihen mit algemenien Gruppencharakteren*, Abh. Math. Sem. Univ Hamburg 8, 1930.

[2] Apostol, Tom M. *Modular Functions and Dirichlet Series in Number Theory*, Second edition. Graduate Texts in Mathematics, 41. Springer-Verlag, New York, 1990.

[3] Brauer, Richard, *On Artin's L-series with general group character*, Ann. of Math. (2) 48, 1947.

[4] Collins, M. J. *Representations and characters of finite groups*, Cambridge Studies in Advanced Mathematics, 22. Cambridge University Press, Cambridge, 1990.

[5] Cox, David A. *Primes of the form* $x^2 + ny^2$, Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[6] Diamond, Fred; Shurman, Jerry. *A first Course in Modular Forms*, Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005.

[7] Marcus, Daniel A. *Number Fields*, Universitext. Springer-Verlag, New York-Heidelberg, 1977.

[8] Miyake Toshitsune. *Modular Forms*, Translated from the Japanese by Yoshitaka Maeda. Springer-Verlag, Berlin, 1989

[9] Serre, Jean-Pierre. *On A Theorem Of Jordan*, Bull. Amer. Math. Soc. (N.S.) 40 (2003), no. 4, 429–440