Title
Modularity of residually reducible Galois representations and Eisenstein ideals

Author
Yoo, Hwajong

Publication Date
2013

Peer reviewed|Thesis/dissertation

Modularity of residually reducible Galois representations and Eisenstein ideals

by

Hwajong Yoo

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Kenneth Alan Ribet, Chair
Professor Martin Olsson
Professor Terry Speed

Spring 2013

Modularity of residually reducible Galois representations and Eisenstein ideals

Abstract

Modularity of residually reducible Galois representations and Eisenstein ideals

by

Hwajong Yoo

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Kenneth Alan Ribet, Chair

The purpose of this thesis is to explain modularity of residually reducible Galois representations. More precisely, for a given reducible mod ℓ representation, we want to classify the set of newforms whose associated mod ℓ representations are isomorphic to it.

Modularity of irreducible two-dimensional mod ℓ Galois representations, which is known as Serre's modularity conjecture, has been studied for several decades. On the other hand, the same question for reducible ones has not been discussed much before.

This problem can be studied by using several methods, which mainly involve the classical theory of Jacobian varieties of modular curves and Shimura curves. We study the geometry of these curves. For instance, we prove multiplicity one theorem for Jacobian varieties for Eisenstein maximal ideals.

We summarize some known results about modularity of reducible representations and give detailed proofs due to a lack of proper references. We introduce techniques of level raising and the conjecture of congruence subgroup property of S-arithmetic groups. And we explain how these techniques shed the light on questions encountered in the thesis.

To my parents.

Contents

Acknowledgments

First of all, I would like to thank Kenneth Ribet. This thesis would not exist if not for his inspired suggestions and his constant enthusiasm for my work.

Among the excellent faculty at UC Berkeley, I would like to thank Martin Olsson and Xinyi Yuan for their invaluable advice over the years, as well as Terry Speed, for bravely serving on my dissertation committee. I would also like to thank Minhyong Kim of the University of Oxford for his encouragement and guidance, as well as Chan-ho Kim of Boston University, for providing me with examples in Chapter 4.

Finally, I would like to thank Samsung scholarship for supporting me during the course of research.

Chapter 1

Introduction

1.1 Motivation

It has been known that newforms for congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ give rise to a compatible system of ℓ-adic representations, and if the ℓ-adic representations attached to two newforms are isomorphic for some prime ℓ, then the newforms are, in fact, equal. But the corresponding statement is not true for the mod ℓ reductions of ℓ-adic representations attached to newforms, as different newforms can give rise to isomorphic mod ℓ representations which arise from reduction mod ℓ of the corresponding ℓ-adic representations. This mod ℓ reduction is well defined if we assume that it is absolutely irreducible. (If the mod ℓ representation is reducible, it is well defined after semisimplification.) This is a reflection of the fact that distinct newforms can be congruent modulo ℓ. To study the different levels from which a given modular mod ℓ representation can arise is interesting and has been discussed.

If we consider the image of the classical Hecke operators in the ring of endomorphisms of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ for some integer N, then the resulting $\mathbb{Z}$-algebra is of finite rank over $\mathbb{Z}$. We denote it by $\mathbb{T}_N$. Then to any maximal ideal $\mathfrak{m}$ of $\mathbb{T}_N$ of residue characteristic ℓ, we may attach, after the work of Eichler-Shimura, a semisimple representation :

$$\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{T}_N/\mathfrak{m}}),$$

such that it is unramified at all primes r prime to ℓN, and for such primes $\mathrm{tr}(\rho_{\mathfrak{m}}(\mathrm{Frob}_r))$ is the image of T_r in $\mathbb{T}_N/\mathfrak{m}$ and $\det(\rho_{\mathfrak{m}}(\mathrm{Frob}_r)) = r$. On viewing $\rho_{\mathfrak{m}}$ abstractly, one may try to classify all the pairs $(\mathbb{T}_M, \mathfrak{n})$, where $\mathfrak{n}$ is a new maximal ideal of $\mathbb{T}_M$, that give rise (in the above fashion) to a representation isomorphic to $\rho_{\mathfrak{m}}$. This classification has been essentially carried out in the work of several people-Mazur, Ribet, Carayol, Diamond, Taylor, and Khare when $\rho_{\mathfrak{m}}$ is absolutely irreducible.

If $\rho_{\mathfrak{m}}$ is reducible, the above classification has not been studied much until 2008. For simplicity, if we consider only newforms of weight 2 and square-free level N, there is a unique semisimple mod ℓ reducible Galois representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$$

arising from each of them. Around 2008, Ribet [3] proved that there is a newform f of level pq such that the associated mod ℓ Galois representation ρ_f is reducible if and only if p and q satisfy some conditions.

In this dissertation, we study the modularity of the above ρ which is isomorphic to $1 \oplus \chi$, in other words, classify all the pairs $(\mathbb{T}_M, \mathfrak{n})$, where $\mathfrak{n}$ is a new maximal ideal of $\mathbb{T}_M$, that give rise to a representation isomorphic to ρ. In contrast to the case when ρ is irreducible, we cannot use so called "level-raising method" directly. The reason is basically that the kernel of "the level-raising map", which is the map induced by degeneracy maps between Jacobians, is "Eisenstein".

Before studying the modularity of reducible representations, we discuss Eisenstein ideals and arithmetic of Jacobian varieties. An ideal I of $\mathbb{T}_N$ is called *Eisenstein* if $T_r - r - 1 \in I$ for almost all primes r. When N is prime, Mazur [25] studied the index of this Eisenstein ideal in $\mathbb{T}_N$. We generalize this result to the case $N = pq$ up to 2, 3 primary factors. Using this result, we can understand when there is an Eisenstein maximal ideal of certain type.

For a maximal ideal $\mathfrak{m}$ of $\mathbb{T}_N$, we study the kernel of $\mathfrak{m}$,

$$J_0(N)[\mathfrak{m}] := \{x \in J_0(N)(\overline{\mathbb{Q}}) : Tx = 0 \text{ for all } T \in \mathfrak{m}\}.$$

If $\rho_{\mathfrak{m}}$ is irreducible and N is square-free, $J_0(N)[\mathfrak{m}]$ is of dimension 2 in most cases. Even though this multiplicity one theorem has been studied long ago for the irreducible case, when $\rho_{\mathfrak{m}}$ is reducible, it was not known for composite levels. We treat $J_0(pq)[\mathfrak{m}]$ (partially) in this case.

We can treat many cases about modularity of mod ℓ reducible representations by using the study of geometry of modular and Shimura curves. For completeness, we include many proofs of known results because they have not been published yet. Furthermore, if we assume a well known conjecture about "congruence subgroup property of S-arithmetic groups", we can prove "Ihara lemma" for Jacobian of Shimura curves. By using this lemma, we can classify the pairs $(\mathbb{T}_M, \mathfrak{n})$ more concretely.

1.2 Notation

The symbols $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the ring of integers, the field of rational numbers, the field of real numbers, and the field of complex numbers, respectively. For a field $\mathbb{F}$, $\overline{\mathbb{F}}$ denotes an algebraic closure of $\mathbb{F}$.

For a prime ℓ, $\mathbb{Z}_\ell$, $\mathbb{Q}_\ell$, and $\mathbb{F}_\ell$ denote the ring of ℓ-adic integers, the field of ℓ-adic numbers, and the finite field of order ℓ, respectively.

For two integers m and n, $m \mid n$ denotes that m divides n and $m \nmid n$ denotes that m does not divide n. For a prime p, $p \parallel n$ denotes p exactly divides n, i.e., n/p is an integer and p and n/p are relatively prime.

For a ring R, $M_n(R)$ denotes the ring of $n \times n$ matrices with coefficients in R and $\mathrm{GL}_n(R)$ denotes the group of invertible matrices in $M_n(R)$. For any element $x \in M_n(R)$, $\mathrm{tr}(x)$ denotes the trace of x and $\det(x)$ denotes the determinant of x.

For two finite groups A and B, we define $A \sim B$ if the A_p, p-primary subgroup of A, is isomorphic to the B_p for all primes p but $2, 3$. In other words, we wrote $A \sim B$ if A and B are isomorphic up to 2, 3 primary factors.

For a set A, $\#A$ denotes its cardinality.

Chapter 2

Background

In the beginning of this Chapter, we recall some basic notions from the classical theory of modular forms, such as modular forms and modular curves over $\mathbb{C}$ and $\mathbb{Q}$, Hecke operators, and Eisenstein series. In the remainder of the Chapter, we discuss the notions of Shimura curves and their Jacobian varieties, which are the generalization of classical modular curves. And we study their integral models which were formulated by Deligne and Rapoport.

The main references are [13], [14], and [4].

2.1 Modular forms and modular curves

Modular curves over $\mathbb{C}$

Let

$$\mathfrak{h} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$$

be the complex upper half-plane, where $\mathrm{Im}(z)$ is the imaginary part of z. The group

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

acts by linear fractional transformations ($z \mapsto (az + b)/(cz + d)$) on $\mathfrak{h}^* := \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q})$. Any discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathfrak{h}$ in the same way.

Let $\mathrm{SL}_2(\mathbb{Z})$ be the group of two by two integer matrices of determinant one. The *principal congruence subgroup* $\Gamma(N)$ of level N is the subgroup of matrices in $\mathrm{SL}_2(\mathbb{Z})$ which reduce to the identity matrix modulo the positive integer N. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a *congruence subgroup* if it contains $\Gamma(N)$ for some N. The *level* of Γ is the smallest N for which this is true. The most important examples of congruence groups are :

1. The group $\Gamma_0(N)$ consisting of all matrices that reduce modulo N to an upper triangular matrix.

2. The group $\Gamma_1(N)$ consisting of all matrices that reduce modulo N to a matrix of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

If Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, define Y_Γ to be the quotient of $\mathfrak{h}$ by the action of Γ. One equips Y_Γ with the analytic structure coming from the projection map $\pi : \mathfrak{h} \to Y_\Gamma$. This makes Y_Γ into a connected complex analytic manifold of dimension one, i.e., a Riemann surface. If Γ is $\Gamma_0(N)$ (resp. $\Gamma_1(N)$), we will also denote Y_Γ by $Y_0(N)$(resp. $Y_1(N)$). One compactifies Y_Γ by adjoining a finite set of *cusps* which correspond to orbits of $\mathbb{P}^1(\mathbb{Q})$ under Γ. Call X_Γ the corresponding compact Riemann surface. We can, and will view X_Γ as a complex algebraic curve over $\mathbb{C}$. If Γ is $\Gamma_0(N)$ (resp. $\Gamma_1(N)$) we will also denote X_Γ by $X_0(N)$(resp. $X_1(N)$).

For details, see [14].

Modular forms over $\mathbb{C}$

Let k be an even positive integer. A *modular form* of weight k on Γ is a holomorphic function f on $\mathfrak{h}$ satisfying :

1. (Transformation property) : $f(\gamma\tau) = (c\tau + d)^k f(\tau)$, for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

2. (Behaviour at the cusps) : For all $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$, the function $(c\tau + d)^{-k} f(\gamma\tau)$ has a Fourier series expansion $\sum_{n=0}^{\infty} a_n q^{n/h}$ in fractional powers of $q = e^{2\pi i\tau}$. We call $\sum_{n=0}^{\infty} a_n q^{n/h}$ the Fourier expansion of f at the cusp $\gamma^{-1}(i\infty)$.

A modular form which satisfies the stronger property that the constant coefficient of its Fourier expansion at each cusp vanishes is called a *cusp form*. We denote by $M_k(\Gamma)$ the complex vector space of modular forms of weight k on Γ, and by $S_k(\Gamma)$ the space of cusp forms of weight k on Γ.

This dissertation is mainly concerned with modular forms of weight 2, and hence we will focus our attention on these from now on. A nice feature of the case $k = 2$ is that the cusp forms in $S_2(\Gamma)$ admit a direct geometric interpretation as holomorphic differentials on the curve X_Γ.

Lemma 2.1.1. *The map $f(\tau) \mapsto \omega_f := 2\pi i f(\tau) d\tau$ is an isomorphism between the space $S_2(\Gamma)$ and the space $\Omega^1(X_\Gamma)$ of holomorphic differentials on the curve X_Γ.*

Proof. See Theorem 3.3.1 of [14]. □

As a corollary, we find:

Corollary 2.1.2. *The space $S_2(\Gamma)$ is finite-dimensional, and its dimension is equal to the genus g of X_Γ.*

To narrow the focus of our interest, we will be mostly concerned with the cases $\Gamma = \Gamma_0(N)$ and $\Gamma_1(N)$. From now on, we suppose $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$. Because the transformation $\tau \mapsto \tau + 1$ belongs to Γ, the forms in $S_2(\Gamma)$ are periodic functions on $\mathfrak{h}$ of period 1, and hence their Fourier expansions at $i\infty$ are of the form

$$f(\tau) = \sum_{n>0} a_n q^n \ , \text{ where } q = e^{2\pi i \tau} \text{ and } a_n \in \mathbb{C}.$$

The Petersson inner product

The spaces $S_2(\Gamma)$ are equipped with a natural Hermitian inner product given by

$$< f,\ g >= \frac{i}{8\pi^2} \int_{X_\Gamma} \omega_f \wedge \bar{\omega_g} = \int_{\mathfrak{h}/\Gamma} f(\tau)\bar{g}(\tau) dx dy,$$

where $\tau = x + iy$. This is called the *Petersson inner product*.

Jacobians of modular curves over $\mathbb{C}$

Let V be the dual space

$$V = S_2(\Gamma)^\vee := \mathrm{Hom}(S_2(\Gamma), \mathbb{C}).$$

It is a complex vector space of dimension g, the genus of X_Γ. The integral homology $\Lambda = H_1(X_\Gamma, \mathbb{Z})$ maps naturally to V by sending a homology cycle c to the functional ϕ_c defined by $\phi_c(f) = \int_c \omega_f$. The image of Λ is a lattice in V, i.e., a $\mathbb{Z}$-module of rank $2g$ which is discrete. Fix a base point $\tau_0 \in \mathfrak{h}$, and define the Abel-Jacobi map $\Phi : X_\Gamma(\mathbb{C}) \to V/\Lambda$ by $\Phi(P)(f) = \int_{\tau_0}^{P} \omega_f$. Note that this is well defined, i.e., it does not depend on the choice of path on X_Γ from τ_0 to P, up to elements in Λ.

We extend the map Φ by linearity to the group $\mathrm{Div}(X_\Gamma)$ of divisors on X_Γ, and observe that the restriction of Φ to the group $\mathrm{Div}^0(X_\Gamma)$ of degree 0 divisors does not depend on the choice of base point τ_0. Moreover we have the Abel-Jacobi theorem:

Theorem 2.1.3. *The map*

$$\Phi : \mathrm{Div}^0(X_\Gamma) \to V/\Lambda$$

has a kernel consisting precisely of the group $P(X_\Gamma)$ of principal divisors on X_Γ. Hence Φ induces an isomorphism from $\mathrm{Pic}^0(X_\Gamma) := \mathrm{Div}^0(X_\Gamma)/P(X_\Gamma)$ to V/Λ.

The quotient V/Λ is a complex torus, and is equal to the group of complex points of an abelian variety. We denote this abelian variety by J_Γ, the *Jacobian variety* of X_Γ over $\mathbb{C}$. If $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$, we will also write $J_0(N)$ or $J_1(N)$ respectively for the Jacobian J_Γ.

Moduli interpretations

The points in Y_Γ can be interpreted as elliptic curves over $\mathbb{C}$ with some extra level N structure. More precisely,

1. If $\Gamma = \Gamma_0(N)$, then the Γ-orbit of $\tau \in \mathfrak{h}$ corresponds to the complex torus $E = \mathbb{C}/< 1, \tau >$ with the distinguished cyclic subgroup of order N generated by $1/N$. Hence, points on $Y_0(N)$ parametrize isomorphism classes of pairs (E, C) where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of E of order N.

2. If $\Gamma = \Gamma_1(N)$, then the Γ-orbit of $\tau \in \mathfrak{h}$ corresponds to the complex torus $E = \mathbb{C}/< 1, \tau >$ with the distinguished point of order N given by $1/N$. Hence, points on $Y_1(N)$ parametrize isomorphism classes of pairs (E, P) where E is an elliptic curve over $\mathbb{C}$ and P is a point of E of exact order N.

Modular curves over $\mathbb{Q}$

For $\Gamma = \Gamma_0(N)$ or $\Gamma_1(N)$, the modular curve X_Γ has a model over $\mathbb{Q}$. Furthermore, X_Γ has a model over $\mathbb{Z}$. The work of Igusa[20], Deligne-Rapoport[13], Drinfeld[16], and Katz-Mazur[22] uses the moduli-theoretic interpretation to describe a canonical proper model for X_Γ over Spec $\mathbb{Z}$. These models allow us to talk about the reduction of X_Γ over finite fields $\mathbb{F}_p$, for p prime. The curve X_Γ has good reduction at primes p not dividing N, with the "non-cuspidal" points of $X_{\Gamma/\mathbb{F}_p}$ corresponding to elliptic curves over $\overline{\mathbb{F}_p}$ with Γ-structure. The singular fibers at primes p dividing N can also be described precisely; an important special case is that of $\Gamma_0(N)$ with p exactly dividing N. We will discuss this model in the last section.

From now on, when we write X_Γ(resp. $X_0(N)$ or $X_1(N)$), we will mean the curve over $\mathbb{Q}$ which are the models for the complex curves defined as $\mathfrak{h}^*/\Gamma$(resp. $\mathfrak{h}^*/\Gamma_0(N)$ or $\mathfrak{h}^*/\Gamma_1(N)$).

Jacobians of modular curves over $\mathbb{Q}$

Weil's theory of the Jacobian shows that the Jacobian J_Γ defined above as complex tori also admit models over $\mathbb{Q}$. When we speak of J_Γ, $J_0(N)$, or $J_1(N)$ from now on, we will refer to these as abelian varieties defined over $\mathbb{Q}$. Thus, the points in $J_\Gamma(K)$, for any $\mathbb{Q}$-algebra K, are identified with the divisor classes on X_Γ of degree 0, defined over K.

We let $J_{\Gamma/\mathbb{Z}}$(resp.$J_0(N)_{/\mathbb{Z}}$), denote the Néron model of the Jacobian J_Γ(resp.$J_0(N)$) over Spec $\mathbb{Z}$. Using this model we define $J_{\Gamma/A}$ for arbitrary ring A. In particular we can consider $J_{\Gamma/\mathbb{F}_p}$, the reduction of the Jacobian in characteristic p, which is closely related to the reduction of the integral model of the curve X_Γ mentioned above. In particular, if p does not divide the level of Γ, then $J_{\Gamma/\mathbb{F}_p}$ can be identified with the Jacobian of $X_{\Gamma/\mathbb{F}_p}$.

2.2 Hecke operators and Hecke rings

Degeneracy maps on modular curves

Let p be a prime not dividing N. Then the points of $X_0(Np)(K)$ classify the triples (E, C, D) where E is an elliptic curve over K, C is a cyclic subgroup of E of order N, and D is a cyclic subgroup of E of order p. Similarly, the points of $X_0(N)(K)$ classify the pairs (E, C). We can consider natural maps between modular curves

$$X_0(Np) \underset{\beta_p}{\overset{\alpha_p}{\rightrightarrows}} X_0(N),$$

where $\alpha_p(E, C, D) := (E, C)$ and $\beta_p(E, C, D) := (E/D, C + D/D)$. In other words, the map α_p is "forgetting the level p structure" and the map β_p is "dividing by the level p structure".

Degeneracy maps on modular forms

Again let p be a prime not dividing N. The map α_p above (resp. β_p) also induces a map α_p (resp. β_p) between cusp forms of weight two as follows.

$$S_2(\Gamma_0(N)) \underset{\beta_p}{\overset{\alpha_p}{\rightrightarrows}} S_2(\Gamma_0(Np)),$$

where $\alpha_p(f(\tau)) = f(\tau)$ and $\beta_p(f(\tau)) = pf(p\tau)$. On its Fourier expansions, $\beta_p(\sum a_n q^n) = p\sum a_n q^{pn}$. For details, see chapter 12 of [4].

Hecke operators on modular curves and modular forms

Let p be a prime not dividing N. The above degeneracy maps induce maps between divisor groups of modular curves. More specifically, we have

$$\mathrm{Div}(X_0(N)) \underset{\beta_p^*}{\overset{\alpha_p^*}{\rightrightarrows}} \mathrm{Div}(X_0(Np)) \underset{(\beta_p)_*}{\overset{(\alpha_p)_*}{\rightrightarrows}} \mathrm{Div}(X_0(N)),$$

where

$$\alpha_p^*(E, C) = \sum_{D \subset E[p]} (E, C, D), \quad \beta_p^*(E, C) = \sum_{D \subset E[p]} (E/D, C + D/D, E[p]/D), \tag{2.1}$$

$$(\alpha_p)_*(E, C, D) = (E, C), \quad \text{and} \quad (\beta_p)_*(E, C, D) = (E/D, C + D/D). \tag{2.2}$$

In the summation of (2.1), D runs all cyclic subgroups of order p. We define T_p on $\mathrm{Div}(X_0(N))$ to be $(\alpha_p)_* \circ \beta_p^*$ or $(\beta_p)_* \circ \alpha_p^*$, in terms of divisors we have

$$T_p((E, C)) = \sum_{D \subset E[p]} (E/D, C + D/D).$$

This map induces an endomorphism of the Jacobian $J_0(N)$. We also denote it by T_p.

The above map is compatible with the action of Hecke operators on modular forms $M_2(\Gamma_0(N))$, which is (on Fourier expansions)

$$T_p(\sum a_n q^n) := \sum a_{np} q^n + p \sum a_n q^{np}.$$

For more details, see [14].

Atkin-Lehner operators and more on Hecke operators

In this section, we assume p is a prime dividing N. We will only consider modular forms of weight two and square-free level N, so assume further that $p \parallel N$, i.e., p exactly divides N. Let $M = N/p$ which is prime to p. Then we have an involution w_p on $J_0(N)$ such that

$$w_p(E, C, D) = (E/D, C + D/D, E[p]/D),$$

where E is an elliptic curve, C is a subgroup of E of order M, and D is a subgroup of order p. There is the Hecke operator T_p in $\mathrm{End}(\mathrm{Div}(J_0(N)))$ on which acts by

$$T_p(E, C, D) = \sum_{L \subset E[p]} (E/L, C + L/L, E[p]/L),$$

where L runs all subgroups of E of order p which is different from D. This operator also induces an endomorphism of $J_0(N)$, we also denote it by T_p.

Lemma 2.2.1. *As endomorphisms of $J_0(N)$, we have $T_p + w_p = \beta_p^* \circ (\alpha_p)_*$, where*

$$J_0(N) \xrightarrow{(\alpha_p)_*} J_0(M) \xrightarrow{\beta_p^*} J_0(N).$$

Proof. On the $\mathrm{Div}(J_0(N))$, $(\alpha_p)_*(E, C, D) = (E, C)$ and hence

$$\beta_p^* \circ (\alpha_p)_*(E, C, D) = \sum_{L \subset E[p]} (E/L, C + L/L, E[p]/L),$$

where L runs all subgroups of E of order p. It is equal to $(T_p + w_p)(E, C, D)$, hence they induce the same map on $J_0(N)$. □

Remark 2.2.2. Above lemma is proved in [29]

Hecke algebras

For a fixed square-free level N, we define $\mathbb{T}_N$ as follows,

$$\mathbb{T}_N := \mathbb{Z}[T_n] \text{ for all positive integers } n,$$

where the T_n are defined by the relations

$$T_{mn} = T_m T_n \quad \text{for} \quad (m,n) = 1,$$

$$T_{p^k} = T_{p^{k-1}} T_p - p T_{p^{k-2}} \quad \text{for primes } p \nmid N \quad \text{, and} \quad T_{p^k} = (T_p)^k \quad \text{for primes } p \mid N.$$

Note that the above relations only work for Hecke operators on $M_2(\Gamma_0(N))$, for more general situations, see [14]. We can consider $\mathbb{T}_N$ as a subring of $\mathrm{End}(J_0(N))$, which is finite over $\mathbb{Z}$. Therefore all maximal ideals of $\mathbb{T}_N$ are of finite index.

Remark 2.2.3. From now on, we will denote by U_p a Hecke operator T_p for primes p dividing the level.

2.3 Old and new

Old forms and new forms

We define the *old* subspace of $S_2(\Gamma_0(N))$ to be the space spanned by those functions which are of the form $g(az)$, where g is in $S_2(\Gamma_0(M))$ for some $M < N$ and aM divides N. We define the *new* subspace $S_2(\Gamma_0(N))_{\text{new}}$ of $S_2(\Gamma_0(N))$ to be the orthogonal complement of the old subspace with respect to the Petersson inner product. A normalized eigenform for all Hecke operators in the new subspace is called a *newform of level* N.

For details, see [14].

Old subvariety and new quotient

The degeneracy maps induce a map between Jacobians

$$J_0(M) \times J_0(M) \xrightarrow{\gamma_p} J_0(N),$$

where $M = N/p$ for some prime divisor p of N and $\gamma_p(a,b) = \alpha_p^*(a) + \beta_p^*(b)$ for α_p^*, β_p^* as in the previous section. The image of γ_p is called the *p-old subvariety* of $J_0(N)$ and is denoted by $J_0(N)_{p\text{-old}}$. The quotient $J_0(N)/J_0(N)_{p\text{-old}}$ is called the *p-new quotient* of $J_0(N)$ and is denoted by $J_0(N)^{p\text{-new}}$. By the autoduality of Jacobians, we have the following exact sequence,

$$0 \longrightarrow (J_0(N)^{p\text{-new}})^\vee \longrightarrow J_0(N) \longrightarrow (J_0(N)_{p\text{-old}})^\vee \longrightarrow 0.$$

We call $(J_0(N)^{p\text{-new}})^\vee$ the *p-new subvariety* of $J_0(N)$. We define the *old subvariety* of $J_0(N)$ to be the subvariety generated by the p-old subvarieties for any prime divisor p of N and

denote it by $J_0(N)_{\text{old}}$. We also define the *new subvariety* to be the connected component of the identity of the intersection of all p-new subvarieties for any prime divisor p of N and denote it by $J_0(N)_{\text{new}}$. The quotient $J_0(N)/J_0(N)_{\text{old}}$ is called the *new quotient* of $J_0(N)$ and denote it by $J_0(N)^{\text{new}}$.

New ideals

Since the map γ_p is Hecke equivariant and the action of $\mathbb{T}_N$ preserves $J_0(N)_{\text{old}}$, we define $\mathbb{T}_N^{\text{new}}$ to be the subring of $\text{End}(J_0(N)^{\text{new}})$ by the action of $\mathbb{T}_N$ on $J_0(N)^{\text{new}}$ via the projection $J_0(N) \to J_0(N)^{\text{new}}$. The ideal I of $\mathbb{T}_N$ is called *new* if it is an inverse image of some non-unit ideal of $\mathbb{T}_N^{\text{new}}$ by the projection

$$\mathbb{T}_N \to \mathbb{T}_N^{\text{new}}.$$

2.4 Galois representations attached to modular forms

Throughout this section, we fix a prime $\ell > 3$ and we only consider modular forms of weight two and $\Gamma_0(N)$ for square-free N. Assume that N is prime to ℓ.

ℓ-adic Galois representations

Let $f = \sum a_n q^n$ be a newform of level N. Let K be the field generated over $\mathbb{Q}$ by the Fourier coefficients a_n of f. Then K is a totally real number field. Let ℓ be a prime and λ be a prime of the ring of integers of K lying over ℓ. Then, by Shimura,

Theorem 2.4.1 (Shimura)**.** *There is the ℓ-adic continuous Galois representation*

$$\tilde{\rho_f} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(K_\lambda)$$

such that

1. *$\tilde{\rho_f}$ is unramified outside ℓN.*
2. *For $p \nmid \ell N$, the characteristic polynomial of $\tilde{\rho_f}(\text{Frob}_p)$ is $X^2 - a_p X + p$, where Frob_p is a Frobenius element in $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

By Ribet, $\tilde{\rho_f}$ is irreducible.
For more details, see Theorem 3.1 in [12].

Mod ℓ Galois representations

Let V be a two-dimensional K_λ vector space which gives rise to the representation $\tilde{\rho_f}$. By taking a Galois stable lattice of V and reduction modulo λ, we can associate a mod ℓ Galois representation ρ attached to f. It does depend on the choice of a lattice, but its

semisimplification does not. (See Chapter 18 of [4].) We denote ρ^{ss} by ρ_f, where ρ^{ss} is the semisimplification of ρ. If ρ_f is not irreducible, then it is the direct sum of two characters χ_1 and χ_2. Since we restrict our attention on the forms of weight two and square-free level N which is prime to ℓ, we can describe ρ_f precisely.

Proposition 2.4.2 (Ribet)**.** *ρ_f is isomorphic to $1 \oplus \chi$, where χ is the mod ℓ cyclotomic character.*

Proof. The semisimplification of ρ is the direct sum of two 1-dimensional representations. Let $\alpha, \beta : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}^\times$ be the corresponding characters, where $\mathbb{F}$ is some finite field of characteristic ℓ. As is well known, the hypothesis that N is square-free implies that the representation ρ_f is semistable outside ℓ in the sense that inertia subgroups of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for primes other than ℓ act unipotently in the representation ρ_f. It follows that α and β are unramified outside ℓ. Accordingly, each of these two characters is some power of the mod ℓ cyclotomic character

$$\chi = \chi_\ell : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\ell^\times \subset \mathbb{F}^\times.$$

If $\alpha = \chi^i$ and $\beta = \chi^j$, the two exponents i and j are determined mod $\ell - 1$ by the restrictions of α and β to an inertia group for ℓ in $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Using the results of [17], one sees easily that these exponents can only be 0 and 1(up to permutation). □

Variants

Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T} := \mathbb{T}_N$ of residue characteristic ℓ, i.e., the characteristic of $\mathbb{T}/\mathfrak{m}$ is ℓ. Then,

Proposition 2.4.3. *There is a unique semisimple representation*

$$\rho_{\mathfrak{m}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{T}/\mathfrak{m})$$

such that

1. *$\rho_{\mathfrak{m}}$ is unramified outside ℓN.*
2. *For a prime $p \nmid \ell N$, the characteristic polynomial of $\rho(\text{Frob}_p)$ is*

$$X^2 - (T_p \pmod{\mathfrak{m}})X + (p \pmod{\mathfrak{m}})$$

.

Proof. This is Proposition 5.1 of [29]. □

Let $\mathbb{F}$ be a finite field of characteristic ℓ. We define a mod ℓ representation

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{F})$$

to be *modular of level* N if the determinant of ρ is the mod ℓ cyclotomic character and if there is a homomorphism

$$\omega : \mathbb{T} \to \overline{\mathbb{F}}$$

such that

$$\mathrm{tr}(\rho(\mathrm{Frob}_p)) = \omega(T_p)$$

for almost all prime numbers p.

Given ρ as in the definition, set $\mathfrak{m} = \ker(\omega)$ and observe that ω embeds $\mathbb{T}/\mathfrak{m}$ into $\overline{\mathbb{F}}$. Since their traces and determinants coincide, their semisimplifications are isomorphic over $\overline{\mathbb{F}}$.

Remark 2.4.4. The above definition is equivalent to the existence of an eigenform f of weight two and level N whose associated mod ℓ Galois representation becomes isomorphic to ρ after embedding to $\overline{\mathbb{F}}$. Furthermore, if $\mathfrak{m}$ is new, f can be taken from $S_2(\Gamma_0(N))_{\mathrm{new}}$.

2.5 Eisenstein series and Eisenstein ideals

Eisenstein series

Let Γ be a congruence subgroup $\Gamma_0(N)$ for a square-free positive integer N. The space $M_2(\Gamma)$ of modular forms naturally decomposes into its subspace of cusp forms $S_2(\Gamma)$ and the corresponding quotient space $M_2(\Gamma)/S_2(\Gamma)$, the *Eisenstein space* $E_2(\Gamma)$. We can pick a natural basis of $E_2(\Gamma)$ which consists of eigenfunctions of all Hecke operators. The number of cusps of $X_0(N)$ is 2^t, where t is the number of distinct prime factors of N, and the dimension of $E_2(\Gamma)$ is $2^t - 1$. We define some notations for later use.

For more details, see Chapter 4 of [14].

Definition 2.5.1. We define e to be the normalized Eisenstein series of weight two and level 1,

$$e(\tau) := -\frac{1}{24} + \sum_{n=1}^{\infty} \sigma(n) q^n,$$

where $\sigma(n) = \sum_{d|n} d$ and $q = e^{2\pi i \tau}$. And we also define e_m for a positive integer m by

$$e_m(\tau) = B_m(e(\tau)) := e(m\tau) = -\frac{1}{24} + \sum_{n=1}^{\infty} \sigma(n) q^{nm},$$

where B_m sends $f(\tau)$ to $f(m\tau)$. (Thus B_p is $\frac{1}{p}\beta_p^*$ on $M_2(\Gamma)$.)

Remark 2.5.2. Note that e is not a modular form and even $e \pmod{\ell}$ is not a (mod ℓ) modular form of weight two which means it cannot be expressible as sum of mod ℓ modular forms of weight two of any level prime to ℓ. About this fact, see [25], [3], [33], or [35].

Using these functions, we can make modular forms of weight two and level N. Recall the proposition by Agashe [1],

Proposition 2.5.3. *For every prime p that divides N, suppose we are given an integer $\delta_p \in \{1, p\}$ such that $\delta_p = 1$ for at least one p. Then there is an Eisenstein series E of weight 2 on $\Gamma_0(N)$ which is an eigenfunction for all the Hecke operators such that for all primes $q \nmid N$, we have $a_q(E) = q + 1$, and for all primes $p \mid N$, we have $a_p(E) = \delta_p$.*

Corollary 2.5.4. *The above Eisenstein series form a basis for $E_2(\Gamma_0(N))$.*

Proof. Since eigenfunctions which have different eigenvalues are linearly independent, we have $2^t - 1$ Eisenstein series which are linearly independent, so they form a basis. □

Example 2.5.5. Let $N = pq$ for distinct primes p and q. We can write a basis of $E_2(\Gamma_0(N))$ explicitly. By Mazur (section 5 of Chapter II of [25]), $e - pe_p$(resp. $e - qe_q$) is a basis of $E_2(\Gamma_0(p))$(resp. $E_2(\Gamma_0(q))$). By "raising the level", we have $g_1 := (e - pe_p) - q(e_q - pe_{pq})$, $g_2 := (e - pe_p) - (e_q - pe_{pq})$, and $g_3 := (e - qe_q) - p(e_p - qe_{pq})$. For every prime $r \nmid pq$, $T_r(g_i) = (1 + r)g_i$ for $i = 1, 2, 3$. Furthermore, we have

$$U_p(g_1) = g_1 \quad \text{and} \quad U_q(g_1) = g_1,$$
$$U_p(g_2) = g_2 \quad \text{and} \quad U_q(g_2) = qg_2,$$
$$U_p(g_3) = pg_3 \quad \text{and} \quad U_q(g_3) = g_3.$$

So, g_1, g_2, and g_3 form a basis for $E_2(\Gamma_0(pq))$.

For later use, we define an *Eisenstein series of level $N = \prod_{i=1}^{t} p_i$ and type (s, t)* to be the Eisenstein series E of level N such that $U_{p_i}E = E$ for all $1 \leq i \leq s$ and $U_{p_j}E = p_jE$ for all $s < j \leq t$, where $s \leq t$ are positive integers. (The integer s should be positive because of the above proposition.)

Eisenstein ideals

Let $\mathbb{T} := \mathbb{T}_N$ for a square-free integer N as before, and let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ of residue characteristic ℓ. Then, we say that $\mathfrak{m}$ is *Eisenstein* if the Galois representation $\rho_{\mathfrak{m}}$ attached to $\mathfrak{m}$ is reducible, which is isomorphic to $1 \oplus \chi$ by Proposition 2.4.2, where χ is the mod ℓ cyclotomic character. An ideal of $\mathbb{T}$ is called *Eisenstein* if it is generated by $T_r - r - 1$ for almost all primes r. A newform $f \in S_2(\Gamma_0(N))_{\text{new}}$ is called *Eisenstein-like* (for ℓ) if the associated (mod ℓ) Galois representation ρ_f is reducible. In fact, if ρ_f is reducible, there is an Eisenstein series E such that $f \equiv E \pmod{\ell}$. We define an *Eisenstein-like newform of level $N = \prod_{i=1}^{t} p_i$ and type (s, t)*(for mod ℓ) to be the Eisenstein-like newform f of level N such that

$$U_{p_i}f = f \quad \text{and} \quad U_{p_j}f = -f,$$

for $1 \leq i \leq s$ and $s < j \leq t$.

2.6 Shimura curves and Hecke operators

Shimura curves and Jacobians

Let $D \neq 1$ be the product of even number of distinct primes and B be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant D. Let $\mathcal{O}$ be a maximal order of B. (Up to isomorphism, there is only one such order.) Then there is the Shimura curve $X_0^D(1)$ over $\mathbb{C}$ which is isomorphic to $\mathfrak{h}/\mathcal{O}^1$, where $\mathcal{O}^1$ denotes the group of (reduced) norm 1 elements in $\mathcal{O}$. (Throughout this section, all norms mean the reduced one.) For each prime p not dividing D, we fix an isomorphism of $\mathbb{Q}_p$-algebras $i_p : B_p \to M_2(\mathbb{Q}_p)$ such that $i_p(\mathcal{O}_p) = M_2(\mathbb{Z}_p)$ if $p \neq \infty$, where $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $\mathcal{O}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. For a positive square-free integer N prime to D, let $\mathcal{O}(N)$ be an Eichler order of level N. Then, the group $\Gamma_0^D(N) := \mathcal{O}(N)^1$ of norm 1 element in $\mathcal{O}(N)$ maps to the upper triangular matrices in $\mathrm{SL}_2(\mathbb{Z}_p)$ for p dividing N by i_p. This $\Gamma_0^D(N)$ also defines the Shimura curve $X_0^D(N)$ over $\mathbb{C}$ which is isomorphic to $\mathfrak{h}/\Gamma_0^D(N)$. Moreover, as the classical modular cases, this curve has moduli theoretic description and it defines an algebraic curve $X_0^D(N)$ over $\mathbb{Q}$. For more details, see [7].

Let $J_0^D(N)$ be the Jacobian variety of $X_0^D(N)$ and $J_0^D(N)_{/\mathbb{Z}}$ be the Néron model of $J_0^D(N)$ over Spec $\mathbb{Z}$. In the next section, we will discuss fibers of $J_0^D(N)_{/\mathbb{Z}}$ at primes p dividing N.

Hecke operators and Hecke rings

As in the classical case, the Hecke operator T_p acts on $J_0^D(N)$ by the following way. An element $X_0^D(N)(K)$ represents an isomorphism class of "fake elliptic curves with level N structure" over K. (For more details, see [15] or [7].) Using this moduli interpretation, we can define two natural degeneracy maps between Shimura curves,

$$X_0^D(Np) \underset{\beta_p}{\overset{\alpha_p}{\rightrightarrows}} X_0^D(N),$$

where p is a prime not dividing DN. As in the classical cases, we define T_p to be $(\alpha_p)_* \circ \beta_p^*$ for each prime p not dividing DN. We can also define the Aktin-Lehner operators w_q for primes q dividing DN. If a prime q divides N, w_q can be defined similarly as before. For a q prime dividing D, there is a unique prime ideal I_p of norm p in $\mathcal{O}$ and w_q can be defined by the map $A \to A/A[I_p]$, where A is a "fake elliptic curve with level N structure" and $A[I] := \{x \in A(\overline{\mathbb{Q}}) : Tx = 0 \text{ for all } T \in I\}$. For a prime r dividing D, T_r acts by the Atkin-Lehner operator w_r and T_q acts by $\beta_q^* \circ (\alpha_q)_* - w_q$ for a prime q dividing N, where

$$X_0^D(N) \underset{\beta_q}{\overset{\alpha_q}{\rightrightarrows}} X_0^D(N/q).$$

We denote the Hecke ring generated by all T_r(and the rule we explained in section 2.2) by $\mathbb{T}_N^D$, so $\mathbb{T}_N^D$ is a subring of $\mathrm{End}(J_0^D(N))$.

Remark 2.6.1. From now on, we will denote by U_p a Hecke operator T_p for each prime p dividing the level or discriminant.

We finish this section by recalling a famous theorem of Jacquet and Langlands.

Proposition 2.6.2 (Jacquet-Langlands correspondence)**.** *The ring $\mathbb{T}_N^D$ is isomorphic to $\mathbb{T}_{ND}^{D\text{-new}}$.*

2.7 Deligne-Rapoport models

Integral models

In their paper [13], Deligne and Rapoport studied integral models of modular curves. Buzzard extended their result to the case of Shimura curves [7]. We briefly explain their integral models of $J_0^D(N)$ when N is square-free. For easier notation, assume p does not divide ND. We study an integral model of $X_0^D(Np)$, where N is a square-free positive integer prime to D. (In this section, D might be 1, which is the modular curve case.)

Proposition 2.7.1 (Deligne-Rapoport model)**.** *The special fiber $X_0^D(Np)_{/\mathbb{F}_p}$ of $X_0^D(Np)_{/\mathbb{Z}}$ at p consists of two copies of $X_0^D(N)_{/\mathbb{F}_p}$. They meet transversally at supersingular points.*

Let S be the set of supersingular points of $X_0^D(Np)_{/\mathbb{F}_p}$. Then S is isomorphic to the set of isomorphism classes of right ideals of an Eichler order of level N of the definite quaternion algebra over $\mathbb{Q}$ of discriminant Dp. By the theory of Raynaud [19], we have special fiber $J_0^D(Np)_{/\mathbb{F}_p}$ of the Néron model $J_0^D(Np)_{/\mathbb{Z}}$. It satisfies the following exact sequence:

$$0 \longrightarrow J^0 \longrightarrow J_0^D(Np)_{/\mathbb{F}_p} \longrightarrow \Phi_p(J_0^D(Np))) \longrightarrow 0,$$

where J^0 is the identity component and $\Phi_p(J_0^D(Np))$ denotes the component group. Furthermore, we have

$$0 \longrightarrow T \longrightarrow J^0 \longrightarrow J_0^D(N)_{/\mathbb{F}_p} \times J_0^D(N)_{/\mathbb{F}_p} \longrightarrow 0,$$

where T is the torus of $J_0^D(Np)_{/\mathbb{F}_p}$. We define the character group to be $X := \mathrm{Hom}(T, \mathbb{G}_{\mathrm{m}})$, where $\mathbb{G}_{\mathrm{m}}$ is the multiplicative group scheme. Then, X is isomorphic to the group of degree 0 elements in the free abelian group $\mathbb{Z}^S$ which is generated by the elements of S. (Note that, the degree of an element in $\mathbb{Z}^S$ is the sum of its coefficients.) There is a natural pairing on $\mathbb{Z}^S$ such that

$$\text{for any } s,t \in S, \quad < s,\ t >= \frac{\#\mathrm{Aut}(s)}{2}\delta_{st} = \frac{\#\mathrm{Aut}(s)}{2} \ \text{ if } \ s = t, \ \ 0 \ \text{ otherwise.}$$

This pairing induces an injection $X \hookrightarrow \mathrm{Hom}(X, \mathbb{Z})$ and the cokernel of this injection is isomorphic to $\Phi_p(J_0^D(Np))$ by Grothendieck [19]. We called the following exact sequence "the monodromy exact sequence";

$$0 \longrightarrow X \xrightarrow{\ i\ } \mathrm{Hom}(X, \mathbb{Z}) \longrightarrow \Phi_p(J_0^D(Np)) \longrightarrow 0.$$

For more details, see [29].

Hecke actions on $J_0^D(Np)_{/\mathbb{F}_p}$

By the Proposition 3.8 of Ribet's paper [29], the Frobenius automorphism on X is equal to the operator U_p on it. Therefore, the Frobenius automorphism acts on T by pU_p. It sends $s \in S$ to some other $s' \in S$, or might fix s. For elements s, t in S the above map i sends $s - t$ to $\phi_s - \phi_t$, where

$$\phi_s(x) := \frac{\#\mathrm{Aut}(s)}{2} < s,\ x > \text{ for any } x \in S.$$

Thus in the group $\Phi := \Phi_p(J_0^D(Np))$, $\phi_s = \phi_t$ for any $s, t \in S$. Since for all $s \in S$, the elements $\frac{2}{\#\mathrm{Aut}(s)}\phi_s$ generate $\mathrm{Hom}(X, \mathbb{Z})$ and $\#\mathrm{Aut}(s)$ is 2, 4, or 6, Φ is "cyclic" and generated by ϕ_s for some $s \in S$ if we ignore 2, 3 primary factors. Using this description, we can understand Hecke actions on component groups up to 2, 3 primary factors. Let Φ^0 be the cyclic subgroup of Φ which is generated by ϕ_s for some $s \in S$. Then, Φ is an extension of some finite group which is of order $2^a \times 3^b$ by Φ_0 (Proposition 3.2 of [29]). Thus $\Phi \sim \Phi^0$.

Proposition 2.7.2. *The Hecke operator U_p acts by 1 on Φ^0 and U_q acts by 1 on Φ^0 for each prime q dividing D. Moreover U_r acts on Φ^0 by r for each prime r dividing N and T_k acts on Φ^0 by $k+1$ for each prime k not dividing DNp.*

Proof. On the Φ^0, $\phi_s = \phi_t$, so $U_p(\phi_s) = \phi_t = \phi_s$, where $t = \mathrm{Frob}(s)$. Since the set S is isomorphic to the set of isomorphism classes of right ideals on an Eichler order of level N in the definite quaternion algebra over $\mathbb{Q}$ of discriminant Dp, the set of supersingular points of $J_0^{Dp/q}(Nq)_{/\mathbb{F}_q}$ is again S. In other words, the character group of $J_0^{Dp/q}(Nq)_{/\mathbb{F}_q}$ does not depend on the choice of the prime q dividing Dp. (Hence the same is true for the component group.) Using the same description as above, we have $U_q(\phi_s) = \phi_s$ for primes q dividing D.

Since the degree of the map U_r is r for primes $r \mid N$, $U_r(\phi_s) = \sum a_i \phi_{s_i}$ and $\sum a_i = r$. Thus $U_r(\phi_s) = r\phi_s$ because $\phi_s = \phi_{s_i}$. Similarly, $T_k(\phi_s) = (k+1)\phi_s$ for primes $k \nmid NDp$. □

Using Eichler's mass formula on Eichler orders of definite quaternion algebras, we can compute the order of Φ up to 2, 3 primary factors.

Proposition 2.7.3. *Let*

$$m := \prod_{r \mid Dp}(r-1) \times \prod_{k \mid N}(k+1).$$

Then $\Phi^0 \sim \mathbb{Z}/m\mathbb{Z}$.

Proof. For any degree 0 divisor $\sum a_i s_i$, $n\phi_s(\sum a_i s_i) = 0$ if n is the order of ϕ. We decompose n as a sum $\sum n_i$ for integers n_i. Then

$$\sum_j n_j(\phi_s(\sum_i a_i s_i)) = \sum_j n_j(\phi_{s_j}(\sum_i a_i s_i)) \quad (2.3)$$

$$= \sum_j n_j a_j \frac{\#\mathrm{Aut}(s_j)}{2} = 0. \quad (2.4)$$

Thus, $n_j \frac{\#\mathrm{Aut}(s_j)}{2}$ is constant for all j since (2.4) is always true for any $\sum a_i = 0$. In other words, n_j is $\frac{c}{\#\mathrm{Aut}(s_j)}$, where c is the smallest positive integer which makes all $\frac{c}{\#\mathrm{Aut}(s_j)}$ to be integers. Note that c is a divisor of 12. Thus

$$n = \sum_{s_j \in S} \frac{1}{\#\mathrm{Aut}(s_j)}$$

up to 2, 3 primary factors.

Recall Eichler's mass formula. (For more details, see Corollary 5.2.3. of [38].)

Proposition 2.7.4 (mass formula)**.** *Let S be the set of isomorphism classes of right ideals of an Eichler order of level N in a definite quaternion algebra of discriminant Dp over a number field K. Then,*

$$\sum_{s_i \in S} \frac{\#R^\times}{\#\mathrm{Aut}(s_i)} = 2^{1-d} \times \mid \zeta_K(-1) \mid \times h_K \times \prod_{r|Dp}(r-1) \times \prod_{k|N}(k+1),$$

where ζ_K is the Dedekind zeta function, $R^\times$ is the group of units in R, the ring of integers of K, d is the degree of K over $\mathbb{Q}$, and h_K is the class number of the field K.

In our case, $K = \mathbb{Q}$, so $\mid \zeta_K(-1) \mid$ is $\frac{1}{12}$, $h_K = 1$, $d = 1$, and $\#R^\times = 2$. If we ignore 2, 3 primary factors, we get the result. □

We close this section by discussing degeneracy maps between component groups which are induced by them on Jacobians.

Proposition 2.7.5. *Let q be a prime which does not divides DNp. By the above proposition, the component groups ,$\Phi_p(J_0^D(Np))$ and $\Phi_p(J_0^D(Npq))$, are cyclic up to 2, 3 primary factors. Let $\Phi_p(J_0^D(Np))^0$(resp. $\Phi_p(J_0^D(Npq))^0$) be the cyclic subgroup of $\Phi_p(J_0^D(Np))$(resp. $\Phi_p(J_0^D(Npq))$) generated by ϕ_s(resp. ϕ_t). Then the degeneracy maps between Jacobians*

$$J_0^D(Np) \underset{\beta_q^*}{\overset{\alpha_q^*}{\rightrightarrows}} J_0^D(Npq)$$

induce the same map on $\Phi_p(J_0^D(Np))^0$

$$\Phi_p(J_0^D(Np))^0 \xrightarrow{\iota_q} \Phi_p(J_0^D(Npq))^0,$$

where $\iota_q(\phi_s) = (q+1)\phi_t$.

Proof. Since the degree of α_q^* is $q+1$, $\alpha_q^*(s) = \sum a_i t_i$ for some t_i, where $\sum a_i = q+1$. Because $\phi_{t_i} = \phi_t$ in $\Phi_p(J_0^D(Npq))$, $\iota_q(\phi_s) = \sum a_i \phi_{t_i} = (q+1)\phi_t$. The same is true for β_q^*. □

Corollary 2.7.6. *Let K (resp. C) be the kernel(resp. the cokernel) of the map γ_q,*

$$0 \longrightarrow K \longrightarrow \Phi_p(J_0^D(Np)) \times \Phi_p(J_0^D(Np)) \xrightarrow{\gamma_q} \Phi_p(J_0^D(Npq)) \longrightarrow C \longrightarrow 0,$$

where $\gamma_q(a,b) = \alpha_q^*(a) + \beta_q^*(b)$. Then, $K \sim \Phi_p(J_0^D(Np))$ and $C \sim \mathbb{Z}/2(q+1)\mathbb{Z} \sim \mathbb{Z}/(q+1)\mathbb{Z}$.

Proof. By comparing orders of two component groups $\Phi_p(J_0^D(Np))^0$ and $\Phi_p(J_0^D(Npq))^0$, ι_q is "injective" if we ignore 2, 3 primary groups. Thus the above result follows. □

Chapter 3

Eisenstein ideals and Jacobian varieties

3.1 Motivation and notation

The main problem of this dissertation is the modularity of residually reducible Galois representations, which are all isomorphic to $1 \oplus \chi$ after semisimplification if we restrict our attention on weight two modular forms for $\Gamma_0(N)$, where N is a square-free positive integer prime to ℓ.(See Proposition 2.4.2.) More specifically, for a fixed prime ℓ, we want to find the level of newforms for which one of the associated mod ℓ Galois representations is reducible. This question is slightly too coarse. Instead we will fix a "signed conductor" : we give ourselves a set of distinct prime numbers $p_i (i = 1, \ldots, t)$ and for each p_i we give ourselves a sign $\pm$. We ask whether there is a newform f of level $N = \prod_{i=1}^{t} p_i$, for which the a_{p_i}, the p_i-th Fourier coefficients of f, have the chosen signs and for which one of the associated mod ℓ representations is reducible. We can shuffle the p_i so the signs start with a string of 1's and end with a string of -1's. Let s be the number of 1's.(So, we have $0 \leq s \leq t$.)

Definition 3.1.1. By an *Eisenstein-like newform f of level $N = \prod_{i=1}^{t} p_i$ and type (s, t)*(for mod ℓ) we mean a newform $f \in S_2(\Gamma_0(N))^{\text{new}}$ such that

1. ρ_f, the semisimplification of mod ℓ representations associated to f, is $1 \oplus \chi$.
2. $U_{p_i} f = f$ for $1 \leq i \leq s$.
3. $U_{p_j} f = -f$ for $s < j \leq t$.

Remark 3.1.2. In the definition, we assume that s is not 0. We will prove this fact later.

Definition 3.1.3. Let $s \leq t$ be two non negative integers. And let $p_1, \ldots, p_t$ be distinct primes which are different from ℓ. A t-tuple $(p_1, \ldots, p_t)$ is *admissible* (for s) if there exists an Eisenstein-like newform of level $N = \prod_{i=1}^{t} p_i$ and type (s, t).

Thus our problem can be rephrased as the classification of admissible tuples. As we discussed in section 2.4, finding an Eisenstein-like newform f of level N and type (s, t) is equivalent to proving the existence of an Eisenstein maximal ideal $\mathfrak{m}$ in $\mathbb{T}_N^{\text{new}}$ such that

1. $\ell \in \mathfrak{m}$.
2. $U_{p_i} - 1 \in \mathfrak{m}$ for $1 \leq i \leq s$.
3. $U_{p_j} + 1 \in \mathfrak{m}$ for $s < j \leq t$.
4. $T_r - r - 1 \in \mathfrak{m}$ for $r \nmid N$.

We denote $\mathfrak{m}$ by $(\ell, U_{p_i} - 1, U_{p_j} + 1, T_r - r - 1)$ for primes $r \nmid N$, and call it a *new Eisenstein maximal ideal of level N and type (s, t)*.

To prove the existence of certain type of Eisenstein maximal ideals in $\mathbb{T}_N^{\text{new}}$ is the same as to find a faithful $\mathbb{T}_N^{\text{new}}$ module V such that $V[\mathfrak{m}] := \{x \in V(\overline{\mathbb{Q}}) : Tx = 0 \text{ for any } T \in \mathfrak{m}\}$ is non-zero. One of candidates for V is the Neron model of the Jacobian variety $J_0(N)^{\text{new}}$. Since $\mathbb{T}^{\text{new}}$ acts faithfully on $J_0(N)^{\text{new}}$, $J_0(N)^{\text{new}}[\mathfrak{m}]$ is not zero if $\mathfrak{m}$ is new maximal. However, the Neron model $J_0(N)^{\text{new}}_{/\mathbb{Z}}$ is hard to study, instead we try to understand $J_0^N(1)$(resp. $J_0^{N/p}(p)$) when the number of primes dividing N is even(resp. odd).

Before studying new Eisenstein maximal ideals, we will discuss Eisenstein ideals of given level and if there is an Eisenstein maximal ideal $\mathfrak{m}$ of level N, we will study the kernel of $\mathfrak{m}$, i.e, $J_0(N)[\mathfrak{m}] := \{x \in J_0(N)(\overline{\mathbb{Q}}) : Tx = 0 \text{ for all } T \in \mathfrak{m}\}$.

These study will be used in next chapter for classifying admissible tuples.

From now on we will fix a prime $\ell > 3$ and the level N will be always square-free and prime to ℓ for simplicity.

3.2 Index of Eisenstein ideals of level pq

Since we want to understand the order of sets up to 2, 3 primary factors, we define a notion for convenience.

Definition 3.2.1. We say that the order of a set S is *"roughly" n* if $\#S = n \times 2^a 3^b$ for some integer a, b.

Eisenstein ideals are generated by $T_r - r - 1$ for almost all primes r. If r divides the level N, the eigenvalue of U_r can only be 1 or r, because it satisfies $X^2 - a_r X + r = 0$. Recall the result about Eisenstein ideals of level N when N is prime.

Proposition 3.2.2 (Mazur)**.** *Let N be a prime. The ideal $I = (T_r - r - 1)$ for all primes $r \neq N$ of $\mathbb{T}_N$ is "roughly" of index $N - 1$.*

In fact, he proved that I contains $U_N - 1$ and the index is exactly the numerator of $\frac{N-1}{12}$. In this section we generalize his result to a composite level pq.

We fix two distinct primes p, q and consider Eisenstein ideals of level pq.

Eisenstein ideal of level pq and type (2,2)

Let $I = (U_p - 1, U_q - 1, T_r - r - 1)$ for primes $r \nmid pq$ be the indicated Eisenstein ideal of $\mathbb{T} := \mathbb{T}_{pq}$.

Theorem 3.2.3. *The index of I in $\mathbb{T}$ is "roughly" $(p-1)(q-1)$.*

Proof. The natural map $\mathbb{Z} \to \mathbb{T}/I$ is surjective, since, modulo I, the operators T_p are all congruent to integers. Let $F(\tau) = \sum_{n=1}^{\infty} a_n x^n$ be the formal power series, where $x = e^{2\pi i \tau}$, $a_r = r+1$ for primes r not dividing pq, $a_p = 1$, and $a_q = 1$.(For general n, a_n is defined by the rule in section 2.2.) We cannot have $\mathbb{T}/I = \mathbb{Z}$, for then F would be the Fourier expansion of a cuspidal eigenform over $\mathbb{C}$, which contradicts the Ramanujan-Petersson bounds. Therefore $\mathbb{T}/I = \mathbb{Z}/n\mathbb{Z}$ for some integer n. Let $f(\tau) = \sum_{n=1}^{\infty} (T_n \pmod I) x^n$ be a cusp form over the ring $\mathbb{Z}/n\mathbb{Z}$. Let $g_1 := e - pe_p - qe_q + pqe_{pq}$ be an Eisenstein series of level pq as in example 2.5.5. Then $f - g_1$ is a modular form over the ring $\mathbb{Z}/n\mathbb{Z}$, which has the Fourier expansion $\frac{(p-1)(q-1)}{24}$. By Mazur (see Lemma 5.3 of [25]), a non-zero constant cannot be a modular form over the ring $\mathbb{Z}/n\mathbb{Z}$ if $(n, 6) = 1$. In other words, h should be 0 modulo n up to 2, 3 primary factors, where h is the numerator of $\frac{(p-1)(q-1)}{24}$.

Since I annihilates $< C_1 >$, the cuspidal group generated by C_1, which will be introduced in next section, there is a surjection

$$\mathbb{T}/I \to \mathrm{End}(< C_1 >) \simeq \mathbb{Z}/h\mathbb{Z}.$$

Therefore n should be a multiple of h. □

Remark 3.2.4. In the proof above, we use a formal variable x. Even we consider x as a formal variable, we set it $e^{2\pi i\tau}$ for using "q-expansion principle" after modulo I. (Here since we use q as a prime number, we substitute the variable q by x.)

Therefore;

Corollary 3.2.5. *There is an Eisenstein maximal ideal $\mathfrak{m}$ such that*

1. *$\mathfrak{m}$ contains $U_p - 1$ and $U_q - 1$.*
2. *$\mathbb{T}/\mathfrak{m} = \mathbb{F}_\ell$*

if $\ell \mid (p-1)(q-1)$.

Eisenstein ideals of level pq and type $(1, 2)$

The eigenvalue of U_q should be 1 or q as we mentioned earlier. However, for newforms all eigenvalues U_q for q dividing N are ± 1. We can consider two Eisenstein ideals of this type. Let $I = (U_p - 1, U_q + 1, T_r - r - 1)$ and $J = (U_p - 1, U_q - q, T_r - r - 1)$ for primes $r \nmid pq$ be Eisenstein ideals of $\mathbb{T}$.

By the similar reason as above, the quotients $\mathbb{T}/I$ and $\mathbb{T}/J$ cannot be $\mathbb{Z}$. Thus $\mathbb{T}/I = \mathbb{Z}/m\mathbb{Z}$ and $\mathbb{T}/J = \mathbb{Z}/n\mathbb{Z}$ for some integers m, n.

Theorem 3.2.6.

1. *m is "roughly" $q + 1$.*
2. *n is "roughly" $(p - 1)(q - 1)(q + 1)$.*

Proof.

1. Let C be the cokernel of the map $\Phi_p(J_0(p)) \times \Phi_p(J_0(p)) \to \Phi_p(J_0(pq))$ which we discussed in Corollary 2.7.6. It is "roughly" of order $q + 1$. Since I annihilates C, m is a multiple of $q + 1$. Let $m = (q + 1) \times k$ for some positive integer k.

   Let $f(\tau) := \sum_{i \geq 1} (T_i \pmod I) x^i$ be a cusp form of level pq over the ring $\mathbb{Z}/(q + 1)k$, where $x = e^{2\pi i \tau}$. Consider $g_2 - f$, where g_2 is the Eisenstein series which we discussed in Example 2.5.5. This is a modular form of level pq over $\mathbb{Z}/(q + 1)k\mathbb{Z}$ whose Fourier expansion is

   $$\sum_{n \geq 1} (q + 1) a_n x^{qn},$$

   where $a_p = p + 1$ for primes $p \neq q$, $a_q = q - 1$, and $a_{q^n} = \sum_{i=0}^{n} (-1)^{(n-i)} q^i$.

   By the lemma 5.9 of [25], there is a modular form h of level p over $\mathbb{Z}/(q + 1)k\mathbb{Z}$ such that

   $$(q + 1)h(\tau) = (q + 1) \sum_{n \geq 1} a_n x^n.$$

   Since h is an eigenform of all Hecke operators T_r for primes $r \neq q$, it is an eigenform (over $\mathbb{Z}/k\mathbb{Z}$). It is an Eisenstein-like eigenform, which means $a_p = 1$ and $a_r \equiv r + 1 \pmod k$ for primes $r \neq p$. Thus,

   $$q - 1 = a_q \equiv q + 1 \pmod k,$$

   which implies that $2 \equiv 0 \pmod k$, i.e, k divides 2. Thus, m is "roughly" $q + 1$.

2. Consider the cuspidal group generated by the cusp $P_1 - P_p$, which will be introduced in next section. It is of order "roughly" $(p - 1)(q - 1)(q + 1)$ and it is annihilated by J. Therefore there is a surjection

   $$\mathbb{T}/J \to \mathrm{End}(< P_1 - P_p >) \simeq \mathbb{Z}/(p - 1)(q - 1)(q + 1)\mathbb{Z}.$$

In other words, n is a multiple of $(p-1)(q-1)(q+1)$.

Again, consider $g(\tau) := \sum_{i\geq 1}(T_i \pmod J)x^i$. Then $g_2 - g$ is a modular form of level pq over $\mathbb{Z}/n\mathbb{Z}$. Its Fourier expansion at $i\infty$ is 0. Thus it should be 0. By the result of Faltings and Jordan(Proposition 3.34 of [18]), we can calculate the constant term of the Fourier expansion of g_2 at the 0-cusp.

We shall use the same notation as Faltings and Jordan(*loc.cit.*). In our case, $\alpha = \beta = 1$, the trivial character, and $k = 2$. The Eisenstein series $e - pe_p$ is $(\alpha(p) - w_p)(e)$, so its constant term at $i\infty$ is $\alpha(p)(1-p)a_0 = \frac{p-1}{24}$ and its constant term at 0 is $b_0 := \alpha(p)(1-1/p)a_0 = \frac{1-p}{24p}$, where $a_0 = \frac{-1}{24}$ the constant term of e. Thus for

$$g_2 = (e - pe_p) - (e_q - pe_{pq}) = \frac{1}{q}(\beta(q)q - w_q)(e - pe_p),$$

its constant term at $i\infty$ is 0 and its constant term at 0 is

$$\frac{1}{q}\left(q\beta(q) - \frac{\alpha(q)}{q}\right) \times b_0 = \frac{(1-p)(q^2-1)}{24pq^2}.$$

Since g is a cusp form over $\mathbb{Z}/n\mathbb{Z}$, the constant term of $g - g_2$ at 0, which is

$$\frac{(1-p)(q^2-1)}{24pq^2},$$

should be 0 over $\mathbb{Z}/n\mathbb{Z}$ because $g - g_2$ is 0 over $\mathbb{Z}/n\mathbb{Z}$. Thus n should be "roughly" $(p-1)(q-1)(q+1)$. (The factor pq^2 on the denominator of above term occurs when we change the Fourier expansion at $i\infty$ to other cusps, such as 0. See section 4 of Chapter II of [25].)

□

Note that if we invert 2, 3, I contains $q+1, U_q+1$, hence, $U_q - q \in I$. Namely, $I \supset J$ if we invert 2, 3. Thus;

Corollary 3.2.7. *There is an Eisenstein maximal ideal $\mathfrak{m}$(resp. $\mathfrak{n}$) such that*

1. *$\mathfrak{m}$(resp. $\mathfrak{n}$) contains $U_p - 1$ and $U_q - q$(resp. $U_q + 1$).*
2. *$\mathbb{T}/\mathfrak{m} = \mathbb{F}_\ell$*

if $\ell \mid (p-1)(q-1)(q+1)$(resp. $\ell \mid q+1$).

This corollary means that the existence of a new Eisenstein maximal ideal of level pq and type $(1,2)$ implies the congruence $q \equiv -1 \pmod \ell$. We will prove the converse of this fact later.

3.3 Multiplicity one theorem for Jacobians

Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T} := \mathbb{T}_N$ of residue characteristic ℓ, i.e., $\mathbb{T}/\mathfrak{m}$ is a finite field of characteristic ℓ, and $J := J_0(N)$. Since $\mathbb{T}$ acts faithfully on J,

$$J[\mathfrak{m}] := \{x \in J(\overline{\mathbb{Q}}) : Tx = 0 \text{ for any } T \in \mathfrak{m}\}$$

is non-zero. If $\mathfrak{m}$ is not Eisenstein, then $J[\mathfrak{m}] = V^{\oplus r}$ for some integer r, where V is the Galois module which defines two-dimensional mod ℓ Galois representation $\rho_{\mathfrak{m}}$. In most cases, $r = 1$, which we call *multiplicity one theorem holds for* J.

Proposition 3.3.1. *For a non-Eisenstein maximal ideal* $\mathfrak{m}$*, multiplicity one holds if* $\ell \nmid 2N$*.*

Proof. This is Theorem 5.2.(b) of [29]. □

On the other hand, when $\mathfrak{m}$ is Eisenstein, this multiplicity one theorem was not considered much. In the Eisenstein case, multiplicity one just means "the dimension of $J[\mathfrak{m}]$ is two." Mazur proved that multiplicity one theorem holds for $J_0(N)$ when N is prime. We generalized this result to the case $N = pq$.

Let $\mathbb{T} := \mathbb{T}_{pq}$ and $J := J_0(pq)$ from now on(till next section). We have two Eisenstein ideals of certain types up to permutation. Let $\mathfrak{m} := (\ell, U_p - 1, U_q - 1, T_r - r - 1)$(resp. $\mathfrak{n} := (\ell, U_p - 1, U_q + 1, T_r - r - 1)$) for primes $r \nmid pq$ be an Eisenstein maximal ideal of type $(2, 2)$(resp. $(1, 2)$). Then we have the following theorems.

Theorem 3.3.2 (Multiplicity one theorem for type $(2, 2)$)**.** *Assume* $p \equiv 1 \pmod{\ell}$*. Then multiplicity one theorem holds for* $\mathfrak{m}$ *if one of the following conditions holds.*

1. $q \not\equiv \pm 1 \pmod{\ell}$*.*
2. $q \equiv -1 \pmod{\ell}$ *and* q *is not an* ℓ*-th power modulo* p*.*

Furthermore the Galois module $J[\mathfrak{m}]$ *is unique up to isomorphism.*

Theorem 3.3.3 (Multiplicity one theorem for type $(1, 2)$)**.** *Assume* $q \equiv -1 \pmod{\ell}$*. Then multiplicity one theorem holds for* $\mathfrak{n}$ *if one of the following conditions holds.*

1. $p \not\equiv 1 \pmod{\ell}$*.*
2. $p \equiv 1 \pmod{\ell}$ *and* $J[\mathfrak{n}]$ *is unramified at* q*.*

Furthermore the Galois module $J[\mathfrak{n}]$ *is unique up to isomorphism.*

Before proving these theorems, we introduce the general ideas to understand $J[\mathfrak{m}]$ for Eisenstein ideals $\mathfrak{m}$. By similar argument as in Mazur's paper[25], all Jordan-Hölder factors of $J[\mathfrak{m}]$ are $\mathbb{Z}/\ell\mathbb{Z}$'s and μ_ℓ's. Moreover, since we assume that ℓ is prime to $2pq$, by Mazur [2], the dimension of $H^1(X_0(pq), \Omega^1)[\mathfrak{m}]$ is at most 1. When we consider the local behaviour of $J[\mathfrak{m}]$ over $\mathbb{F}_\ell$, $\overline{\mathbb{F}_\ell}$-points of $J[\mathfrak{m}]$ maps injectively to $H^1(X_0(pq), \Omega^1)[\mathfrak{m}]$, so the étale part of

$J[\mathfrak{m}]$ over $\mathbb{F}_\ell$ is at most of dimension 1(page 119 of [25], [8]). Therefore the Jordan-Hölder factors of $J[\mathfrak{m}]$ are μ_ℓ's and (possibly) one $\mathbb{Z}/\ell\mathbb{Z}$. In our cases, $J[\mathfrak{m}]$ always contains a copy of $\mathbb{Z}/\ell\mathbb{Z}$ which comes from the cuspidal group. Let M be the quotient of $J[\mathfrak{m}]$ by $\mathbb{Z}/\ell\mathbb{Z}$. Then all Jordan-Hölder factors of M are μ_ℓ's, i.e., it is a multiplicative group. Since $\eta_r := T_r - r - 1$ annihilates $J[\mathfrak{m}]$ for almost all primes r, it annihilates M. By the theorem of constancy [25], M is a direct sum of μ_ℓ's. (We can directly follow Mazur's argument on page 126-129 of [25].) If $J[\mathfrak{m}]$ is a direct sum of $\mathbb{Z}/\ell\mathbb{Z}$ and M which is a direct sum of μ_ℓ's, it contains many μ-type subgroups of J. Here we recall the theorem of Vatsal [37].

Theorem 3.3.4 (Vatsal)**.** *Let W denote any finite $\mathbb{Q}$-rational subgroup of $J_0(N)(\overline{\mathbb{Q}})$ such that*

1. *$W \simeq \mu_n$ for some odd integer n; and*
2. *$J_0(N)$ has semistable reduction at ℓ for each prime ℓ dividing n.*

Then, W is contained in the Shimura subgroup of $J_0(N)$.

The Shimura subgroup of $J_0(N)$ is the Cartier dual of a quotient group of $(\mathbb{Z}/N\mathbb{Z})^\times$, therefore its order divides $\phi(N)$ where ϕ is the Euler function. So, if $\ell \nmid (p-1)(q-1)$, $J_0(pq)$ can't contain μ_ℓ. (Thus $J[\mathfrak{m}]$ cannot be a direct sum of $\mathbb{Z}/\ell\mathbb{Z}$ and M.) In this case, we need to understand possible extensions of μ_ℓ by $\mathbb{Z}/\ell\mathbb{Z}$. Recall the theorem of Brumer and Kramer[6].

Theorem 3.3.5 (Brumer-Kramer)**.** *Let S be a set of primes and $n(S)$ be the number of primes $p \in S$ such that $p \equiv \pm 1 \pmod{\ell}$. The group of extensions of μ_ℓ by $\mathbb{Z}/\ell\mathbb{Z}$ over $\mathbb{Z}_S := \mathbb{Z}[p^{-1} : p \in S]$, denoted by $\mathrm{Ext}_{\mathbb{Z}_S}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$, is a vector space over $\mathbb{F}_\ell$ of dimension $n(S)$. Moreover, the extensions in $\mathrm{Ext}_{\mathbb{Z}_S}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ are unramified at $r \in S$ such that $r \not\equiv \pm 1 \pmod{\ell}$.*

Thus all we need to prove multiplicity one theorems are information about Shimura subgroups and cuspidal groups.

Shimura subgroups of $J_0(pq)$

The Shimura subgroup is the kernel of the map

$$J_0(N) \to J_1(N).$$

Since the covering group of $X_1(N) \to X_0(N)$ is $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, the covering group of the maximal étale subcovering of $X_1(N) \to X_0(N)$ is a quotient of $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, which is the Cartier dual of the Shimura subgroup. When N is prime, Mazur discussed it on section 11 of Chapter II in [25]. (In general, see the paper of Ling and Oesterlé [23].) Let Σ_p(resp. Σ_q)

be the Shimura subgroup of $J_0(p)$(resp. $J_0(q)$). Then by the degeneracy map γ_q(resp. γ_p), (Σ_p, Σ_p)(resp. (Σ_q, Σ_q)) maps to the Shimura subgroup of $J_0(pq)$, where

$$\gamma_q : J_0(p) \times J_0(p) \to J_0(pq),$$

$$\gamma_p : J_0(q) \times J_0(q) \to J_0(pq).$$

And these two images generate the Shimura subgroup of $J_0(pq)$. Let Σ_1(resp. Σ_2) be the image of Σ_p(resp. Σ_q) on $J_0(pq)$. The action of Hecke operators on the Shimura subgroup is well known to be "Eisenstein", which means $\eta_r := T_r - r - 1$ annihilates it. (See [30].) Furthermore,

Lemma 3.3.6. *U_p acts by 1 on Σ_1 and by p on Σ_2. Similarly, U_q acts by q on Σ_1 and by 1 on Σ_2.*

Proof. Since γ_q is equivariant for all T_r but T_q, and $U_p - 1$ annihilates Σ_p, U_p acts by 1 on Σ_1. Let α_q and β_q be two degeneracy maps from $X_0(pq)$ to $X_0(p)$. Then α_q and β_q induce the map between Jacobians as we discussed in section 2.2.

$$J_0(pq) \underset{(\beta_q)_*}{\overset{(\alpha_q)_*}{\rightrightarrows}} J_0(p) \underset{\beta_q^*}{\overset{\alpha_q^*}{\rightrightarrows}} J_0(pq).$$

Let w_q be the Atkin-Lehner operator of $J_0(pq)$. Then $U_q + w_q = \beta_q^*(\alpha_q)_*$ by Lemma 2.2.1. Since $\Sigma_1 = (\alpha_q^* + \beta_q^*)(\Sigma_p)$ and $\beta_q^* = w_q \alpha_q^*$, w_q acts by 1 on Σ_1. Moreover $(\beta_q)_* \Sigma_1 = (\alpha_q)_* \Sigma_1$. Thus $U_q + w_q$ acts by $\beta_q^*(\alpha_q)_* = \beta_q^*(\beta_q)_* = q + 1$ on Σ_1. □

Cuspidal groups of $J_0(pq)$

Let P_1, P_p, P_q, and P_{pq} be four cusps of $X_0(pq)$ as in [26]. Then the cuspidal group of $J_0(pq)$ is the subgroup generated by cuspidal divisors. Let $C_1 = P_1 - P_p - P_q + P_{pq}$, $C_2 = P_1 - P_p$, and $C_3 = P_1 - P_q$. The order of C_1(resp. C_2, C_3) is "roughly" $(p-1)(q-1)$(resp. $(p-1)(q-1)(q+1)$, $(p-1)(p+1)(q-1)$). The action of Hecke operators on the cuspidal group is also known to be "Eisenstein". Moreover,

Lemma 3.3.7. *On C_1, U_p and U_q both act by 1. On C_2, U_p acts by 1 and U_q acts by q. Similarly, on C_3, U_p acts by p and U_q acts by 1.*

Proof. Let P_1 and P_p(resp. P_q) denote cusps of $X_0(p)$(resp. $X_0(q)$). Then, P_1, P_q(resp. P_p, P_{pq}) maps to P_1(resp. P_p) by α_q, β_q, where (as before)

$$X_0(pq) \underset{\beta_q}{\overset{\alpha_q}{\rightrightarrows}} X_0(p).$$

Furthermore, since the ramification indices of P_1 and P_q in the covering $X_0(pq) \to X_0(p)$ are 1 and q, up to permutation. Thus we have $\alpha_q^*(P_1) = P_1 + qP_q$ and $\beta_q^*(P_1) = qP_1 + P_q$. Since

$\beta_q^*(\alpha_q)_*(C_1) = \beta_q^*(0) = 0$ and w_q acts by -1 on C_1 (note that $w_q(P_1) = P_q$ and $w_q(P_p) = P_{pq}$), U_q acts by 1 on C_1. A similar computation works if we permute p and q.

Because $\beta_q^*(\alpha_q)_*(C_2) = \beta_q^*(P_1 - P_p) = qP_1 + P_q - qP_p - P_{pq}$ and $w_q(P_1 - P_p) = P_q - P_{pq}$,

$$(U_q + w_q)(P_1 - P_p) = \beta_q^*(\alpha_q)_*(P_1 - P_p) \quad (3.1)$$
$$(U_q)(C_2) + P_q - P_{pq} = q(P_1 - P_p) + P_q - P_{pq}. \quad (3.2)$$

Therefore U_q acts by q on C_2. On C_3, as before, since $(\alpha_q)_*(C_3) = 0$ and $w_q(C_3) = -C_3$, U_q acts by 1. Similar computation works if we permute p and q. □

For more details about the cuspidal groups of $J_0(pq)$, see [31], [10].

Proofs

Now we are ready to prove the theorems above.

Proof of Theorem 3.3.2. By Corollary 3.2.4, $\mathfrak{m}$ is maximal, so $J[\mathfrak{m}]$ is nontrivial. Let $T_\ell J$ be the ℓ-adic Tate module of J, i.e. $T_\ell J := \varprojlim_{\leftarrow n} J[\ell^n]$. It is of rank 2 over $\mathbb{T}_\ell := \mathbb{T} \otimes \mathbb{Z}_\ell$. Since $\mathbb{T}_\ell$ is a product of $\mathbb{T}_\mathfrak{a} := \varprojlim_{\leftarrow n} \mathbb{T}/\mathfrak{a}^n$ for all maximal ideals $\mathfrak{a}$ containing ℓ, $\mathbb{T}_\mathfrak{m}$ is a direct factor of $\mathbb{T}_\ell$. Using an idempotent $e_\mathfrak{m}$ of $\mathbb{T}_\mathfrak{m}$ in $\mathbb{T}_\ell$, $T_\mathfrak{m} J = e_\mathfrak{m} T_\ell J$ is of rank 2 over $\mathbb{T}_\mathfrak{m}$. So, $T_\mathfrak{m} J/\mathfrak{m} T_\mathfrak{m} J$ is at least of dimension 2 over $\mathbb{T}_\mathfrak{m}/\mathfrak{m}\mathbb{T}_\mathfrak{m}$. Therefore $J[\mathfrak{m}]$ is at least of dimension 2 over $\mathbb{T}/\mathfrak{m}$. (See section 7 of Chapter II of [25].) From the above discussion, if $J[\mathfrak{m}]$ contains μ_ℓ as a subgroup, q should be 1 modulo ℓ. Therefore $J[\mathfrak{m}]$ cannot contain μ_ℓ and it should contain $\mathbb{Z}/\ell\mathbb{Z}$.(We can actually make the order ℓ subgroup of the cuspidal group generated by C_1 which is annihilated by $\mathfrak{m}$.) Assume that $q \not\equiv \pm 1 \pmod{\ell}$ and $J[\mathfrak{m}]$ is of dimension bigger than 2. Then it contains W which is of dimension 3 and is an nontrivial extension of $\mu_\ell \oplus \mu_\ell$ by $\mathbb{Z}/\ell\mathbb{Z}$. Let α(resp. β) be a natural inclusion of μ_ℓ into the first(resp. second) component of $\mu_\ell \oplus \mu_\ell$,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/\ell\mathbb{Z} & \longrightarrow & W & \longrightarrow & \mu_\ell \oplus \mu_\ell & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow{\scriptstyle \alpha} \uparrow{\scriptstyle \beta} & & \\ 0 & \longrightarrow & \mathbb{Z}/\ell\mathbb{Z} & \longrightarrow & V & \longrightarrow & \mu_\ell & \longrightarrow & 0. \end{array}$$

Then $\alpha^* W$ and $\beta^* W$ are elements in $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$, where $\mathbb{Z}_{pq} := \mathbb{Z}[p^{-1}, q^{-1}]$. Since the dimension of $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is 1 if $q \not\equiv \pm 1 \pmod{\ell}$, there is $a, b \in \mathbb{F}_\ell$ such that $a\alpha^* W + b\beta^* W = 0$. In other words, W contains a two dimensional split extension of μ_ℓ by $\mathbb{Z}/\ell\mathbb{Z}$. Therefore it contains μ_ℓ, which is contradiction. So, $J[\mathfrak{m}]$ is of dimension 2. Since $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is generated by an extension which is only ramified at p, $J[\mathfrak{m}]$ is a non-zero scalar(in $\mathbb{F}_\ell$) multiple of it. As Galois modules, these are all isomorphic.

For the second case, we cannot use the above method because the dimension of $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is 2. However we can get the bound of the dimension of $J[\mathfrak{m}]$. If the dimension were greater than 3, it would contain W of dimension 4 which is an extension of ${\mu_\ell}^{\oplus 3}$ by $\mathbb{Z}/\ell\mathbb{Z}$. By the similar argument as above, we have three elements in $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$. So they are linearly

dependent, which implies W contains a split extension. This contradicts to the fact that $J[\mathfrak{m}]$ does not have μ_ℓ as a subgroup. Thus $J[\mathfrak{m}]$ is at most of dimension 3.

Consider special fiber of the Néron model of J over $\mathbb{F}_q$. By the assumption and Theorem 4.2.2.3 below, $\mathfrak{m}$ is not new, hence it is not q-new. (Otherwise there would exist an Eisenstein maximal ideal of level q which is not 1 (mod ℓ). This contradicts to Theorem 4.2.1.2.) It implies that $J[\mathfrak{m}]$ is unramified at q. The order of the component group is "roughly" $(p+1)(q-1)$ which is prime to ℓ. Thus $J[\mathfrak{m}]$ maps injectively to $J^0[\mathfrak{m}]$, where J^0 is the identity component of $J_{/\mathbb{F}_q}$. Since $\mathfrak{m}$ is not q-new, $T[\mathfrak{m}] = 0$, where T is a torus of J^0. (Note that the action of $\mathbb{T}$ on T factors through $\mathbb{T}^{q\text{-new}}$, see Theorem 3.10 of [29].) Since $J_0(p)^2[\mathfrak{m}]$ is an antidiagonal image of $J_0(p)[\mathfrak{m}_p]$ in $J_0(p)^2$, where $\mathfrak{m}_p$ is an Eisenstein maximal ideal of level p, it is of dimension 2. Thus the dimension of $J[\mathfrak{m}]$ which satisfying this exact sequence

$$0 \longrightarrow T[\mathfrak{m}] = 0 \longrightarrow J^0[\mathfrak{m}] = J[\mathfrak{m}] \longrightarrow J_0(p)^2[\mathfrak{m}]$$

is at most 2. Thus it is of dimension 2. Since $J[\mathfrak{m}]$ cannot contain μ_ℓ, it is ramified at p but unramified at q. This extension is unique up to isomorphism. □

Proof of Theorem 3.3.3. By the Corollary 3.2.6, when $q \equiv -1 \pmod{\ell}$, $\mathfrak{n}$ is maximal. For the first case, we assume further $p \not\equiv \pm 1 \pmod{\ell}$. Then the dimension of $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is 1. Again, by lemma 3.3.6, we know that $J[\mathfrak{n}]$ can't contain μ_ℓ. By similar argument as above, it follows that $J[\mathfrak{n}]$ is of dimension 2 which is only ramified at q.

When $p \equiv -1 \pmod{\ell}$, the dimension of $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is 2, so $J[\mathfrak{n}]$ is at most dimension 3. Consider $J[\mathfrak{n}]$ over $\mathbb{F}_q$. Let $J[\mathfrak{n}]^{I_q}$ be the inertia fixed part of $J[\mathfrak{n}]$, where I_q is the inertia group of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at q. It maps to $J_0(pq)_{/\mathbb{F}_q}$. By the result of section 2.7, $\Phi_q[\mathfrak{n}]$ is trivial. Moreover, since $p \not\equiv 1 \pmod{\ell}$, $J_0(p)[\mathfrak{m}_p]$ is trivial, where $\mathfrak{m}_p = (\ell, U_p - 1, T_r - r - 1)$ which is $\mathbb{T}_p$ by Mazur.(See Theorem 4.2.1.2.) Therefore $J[\mathfrak{n}]^{I_q}$ lies in a torus T. On T, Frob_q acts by qU_q, which is $-q \equiv 1 \pmod{\ell}$. So μ_ℓ can't lie in T. In other words, $J[\mathfrak{n}]^{I_q}$ is of dimension 1. Since $J[\mathfrak{n}]$ is an extension of ${\mu_\ell}^{\oplus r}$ by $\mathbb{Z}/\ell\mathbb{Z}$, $J[\mathfrak{n}]^{I_q}$ is at least of dimension r, which implies $J[\mathfrak{n}]$ is of dimension 2. Furthermore if we consider $J[\mathfrak{n}]$ over $\mathbb{F}_p$, $J[\mathfrak{n}]^{I_p}$ maps to $J_0(pq)_{/\mathbb{F}_p}$. By the result of section 2.7, $\Phi_q[\mathfrak{n}]$ is not trivial, of dimension 1 since it is "cyclic". On a torus, since $\mathfrak{n}$ is new, $T[\mathfrak{n}]$ is not trivial, which implies $J[\mathfrak{n}]^{I_p}$ is at least of dimension 2. Thus $J[\mathfrak{n}]$ is unramified at p but ramified at q. In the $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$, the class of the above extension is one dimensional, which means that $J[\mathfrak{n}]$ is unique up to isomorphism as a Galois module.

For the second case, $J[\mathfrak{n}]$ contains one μ_ℓ from the Shimura subgroup. Consider $J[\mathfrak{n}]^{I_q}$. Since the order of the component group of $J_{/\mathbb{F}_q}$ is prime to ℓ, $J[\mathfrak{n}]^{I_q}$ maps injectively to $J^0[\mathfrak{n}]$. Thus we have the following exact sequence ;

$$\begin{array}{ccccc} 0 \longrightarrow T[\mathfrak{n}] & \longrightarrow & J[\mathfrak{n}]^{I_q} & \longrightarrow & J_0(p)[\mathfrak{m}_p]^2 \\ & & \uparrow{\scriptstyle s} & \nearrow{\scriptstyle \psi} & \\ & & J_0(p)[\mathfrak{m}_p] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mu_\ell & & \end{array}$$

where $s(x) = \alpha_q^* x + \beta_q^* x$ and $\psi(x) = ((1+v)x, (1+v)x)$ for v the Vershiebung over $\mathbb{F}_q$. As before, $T[\mathfrak{n}]$ can't contain μ_ℓ. By ψ, $\mathbb{Z}/\ell\mathbb{Z}$ maps to 0, and μ_ℓ maps injectively. Thus $T[\mathfrak{n}]$ and the image of $J[\mathfrak{n}]^{I_q}$ in $J_0(p)[\mathfrak{m}_p]^2$ are both one dimensional, which implies $J[\mathfrak{n}]^{I_q}$ is of dimension 2.(Since s is injective, the image of $J[\mathfrak{n}]^{I_q}$ is equal to one of ψ.) If $J[\mathfrak{n}]$ is unramified at q, it should be of dimension 2. In this case, $J[\mathfrak{n}]$ is a direct sum of $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ. □

Remark 3.3.8. In the case when $p \not\equiv 1 \pmod{\ell}$ and $q \equiv -1 \pmod{\ell}$, $T[\mathfrak{n}]$ is of dimension 1. Since $T[\mathfrak{n}]$ is a dual of $L/\mathfrak{n}L$ where L is the character group of $J_0(pq)_{/\mathbb{F}_p}$, it is also of dimension 1 over $\mathbb{T}/\mathfrak{n}$.

3.4 Failure of multiplicity one

When $p \equiv q \equiv 1 \pmod{\ell}$, there is non trivial intersection of the old subvariety and the new subvariety of J which is annihilated by Eisenstein maximal ideals. In this case, all three different Eisenstein ideals are contained in a single maximal ideal $\mathfrak{m}$, so $J[\mathfrak{m}]$ is very complicated. Multiplicity one certainly fails in this case because $J[\mathfrak{m}]$ already contains one $\mathbb{Z}/\ell\mathbb{Z}$ from the cuspidal group and two μ_ℓ's from the Shimura subgroup. In this section, we discuss when this phenomenon occurs.

Theorem 3.4.1. *Assume $p \equiv 1 \pmod{\ell}$. And let $\mathfrak{m} := (\ell, U_p - 1, U_q - 1, T_r - r - 1)$ be an Eisenstein maximal ideal of type $(2,2)$. Then, multiplicity one fails for $\mathfrak{m}$ if*

1. *$q \equiv 1 \pmod{\ell}$ or*
2. *$q \equiv -1 \pmod{\ell}$ and $J[\mathfrak{m}]$ is ramified at q.*

Furthermore, in the first case, $J[\mathfrak{m}]$ is of dimension 4 or 5, and in the second case, it is of dimension 3 and also ramified at p.

Theorem 3.4.2. *Assume $q \equiv -1 \pmod{\ell}$. And let $\mathfrak{n} := (\ell, U_p - 1, U_q + 1, T_r - r - 1)$ be an Eisenstein maximal ideal of type $(1,2)$. Then, multiplicity one fails for $\mathfrak{n}$ if $p \equiv 1 \pmod{\ell}$ and $J[\mathfrak{n}]$ is ramified at q. Furthermore the dimension of $J[\mathfrak{n}]$ is 3 and it is unramified at p.*

The proofs of above theorems are really similar to those of the previous section.

Proof of Theorem 3.4.1. Assume $q \equiv 1 \pmod{\ell}$. By the result of Shimura subgroups on previous section, $\Sigma_1[\mathfrak{m}]$ and $\Sigma_2[\mathfrak{m}]$ are both one dimensional. Thus $J[\mathfrak{m}]$ contains two μ_ℓ's from the Shimura subgroup and one $\mathbb{Z}/\ell\mathbb{Z}$ from the cuspidal group. Since $J[\mathfrak{m}]$ is an extension of ${\mu_\ell}^{\oplus r}$ by $\mathbb{Z}/\ell\mathbb{Z}$, two μ_ℓ's are actually direct factors. By the similar reason as previous section, the dimension of $J[\mathfrak{m}]$ over $\mathbb{F}_\ell = \mathbb{T}/\mathfrak{m}$ is at most 5 because the dimension of $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is 2. On μ_ℓ which is contained in Σ_1(resp. Σ_2), $U_q + w_q$(resp. $U_p + w_p$) acts by $q+1$(resp. $p+1$) which is $\not\equiv 0 \pmod{\ell}$. Therefore these μ_ℓ's do not meet the new subvariety because on the new subvariety $U_q + w_q$ and $U_p + w_p$ act by 0. By the same argument using Tate

modules, we can prove $J_{\mathrm{new}}[\mathfrak{m}]$ is at least of dimension 2. Therefore the dimension of $J[\mathfrak{m}]$ is 4 or 5.

For the second case, $J[\mathfrak{m}]$ cannot contain μ_ℓ as a subgroup. Since the dimension of $\mathrm{Ext}_{\mathbb{Z}_{pq}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is 2, the dimension of $J[\mathfrak{m}]$ is at most 3. Consider $J[\mathfrak{m}]$ over $\mathbb{F}_q$. As we discussed in the proof of Theorem 3.3.2, $\Phi_q[\mathfrak{m}] = 0$. So $J[\mathfrak{m}]^{I_q}$ maps injectively to J^0, the identity component. Since $J[\mathfrak{m}]$ is ramified at q, $\mathfrak{m}$ should be q-new. By the similar discussion as above, we have $T[\mathfrak{m}]$ is at least of dimension 1 and the image of $J[\mathfrak{m}]^{I_q}$ on $J_0(p)^2[\mathfrak{m}]$ is at least of dimension 1. In other words, $J[\mathfrak{m}]^{I_q}$ is at least of dimension 2. Since it is ramified at q and $J[\mathfrak{m}]$ is at most of dimension 3, $J[\mathfrak{m}]^{I_q}$ should be of dimension 2 and $J[\mathfrak{m}]$ is of dimension 3. Furthermore if $J[\mathfrak{m}]$ is unramified at p, $J[\mathfrak{m}]^{I_q}$ which is 2 dimensional is unramified everywhere, i.e., it is a direct sum of μ_ℓ and $\mathbb{Z}/\ell\mathbb{Z}$, which is contradiction. Thus $J[\mathfrak{m}]$ is also ramified at p. □

Proof of Theorem 3.4.2. When $p \equiv 1 \pmod{\ell}$, as before we have $J[\mathfrak{n}]^{I_q}$ is of dimension 2. Thus it $J[\mathfrak{n}]$ is ramified at q, it should be of dimension 3. Consider $J[\mathfrak{n}]$ over $\mathbb{F}_p$. Since $\mathbb{Z}/\ell\mathbb{Z} \subset J[\mathfrak{n}]$ maps to the component group of $J_{/\mathbb{F}_p}$, we can copy Mazur's argument on page 125-126 of [25]. Thus there is an exact sequence,

$$0 \longrightarrow \mathbb{Z}/\ell\mathbb{Z} \longrightarrow J[\mathfrak{n}]^{I_p} \longrightarrow (\mu_\ell{}^{\oplus 2})^{I_p} = \mu_\ell{}^{\oplus 2} \longrightarrow 0.$$

Thus $J[\mathfrak{n}]$ is unramified at p. In this case, $T[\mathfrak{n}]$ is of dimension two, where T is a torus of $J_{/\mathbb{F}_p}$ because $J_0(q)^2[\mathfrak{n}] = 0$. (Note that there is no Eisenstein maximal ideals of level q of characteristic ℓ.) Thus the dimension of $L/\mathfrak{n}L$ is 2 where L is the character group of $J_{/\mathbb{F}_p}$ which is a $\mathbb{G}_{\mathrm{m}}$-dual of T. □

3.5 Multiplicity one theorem for Shimura curves

Let $J := J_0^{pq}(1)$ be the Jacobian of the Shimura curve $X_0^{pq}(1)$ and $\mathbb{T} := \mathbb{T}^{pq}$ be the Hecke ring in $\mathrm{End}(J)$. During this section, we will assume that $p \not\equiv 1 \pmod{\ell}$ and $q \equiv -1 \pmod{\ell}$. Then, $\mathfrak{n} := (\ell, U_p - 1, U_q + 1, T_r - r - 1)$ is not old in any way, which means $\mathfrak{n}$ cannot be q-old nor p-old. In this case we can prove multiplicity one theorem holds for $J[\mathfrak{n}]$.

Theorem 3.5.1 (Ribet)**.** *$J[\mathfrak{n}]$ is of dimension 2.*

For the proof, we need the following proposition.

Proposition 3.5.2. *$\mathbb{T}_{\mathfrak{n}}$ is Gorenstein.*

Proof. Let Y be the character group of $J_{/\mathbb{F}_p}$ which is a $\mathbb{G}_{\mathrm{m}}$-dual of the torus, then by Ribet [29], there is an exact sequence;

$$0 \longrightarrow Y \longrightarrow L \longrightarrow X \oplus X \longrightarrow 0,$$

where L is the character group of $J_0(pq)_{/\mathbb{F}_q}$ and X is the character group of $J_0(q)_{/\mathbb{F}_q}$. Since $\mathfrak{n}$ is not old, $(\mathbb{T}_{pq})_{\mathfrak{a}} \simeq \mathbb{T}_{\mathfrak{n}}$ and $X_{\mathfrak{b}} = 0$, where $\mathfrak{a}$(resp. $\mathfrak{b}$) is the image of $\mathfrak{n}$ in $\mathbb{T}_{pq}$(resp. $\mathbb{T}_q$ which should be $\mathbb{T}_q$ itself). Thus we have $Y_n \simeq L_{\mathfrak{a}}$. Since for $\mathfrak{a}$, multiplicity one theorem holds, it implies that $L_{\mathfrak{a}}$ is free of rank 1 over $(\mathbb{T}_{pq})_{\mathfrak{a}}$, i.e., $Y_{\mathfrak{n}}$ is free of rank 1 over $\mathbb{T}_{\mathfrak{n}}$. By Grothendieck [19], there is a monodromy exact sequence,

$$0 \longrightarrow Y \longrightarrow \mathrm{Hom}(Y, \mathbb{Z}) \longrightarrow \Phi \longrightarrow 0,$$

where $\Phi := \Phi_p(J_{/\mathbb{F}_p})$ is the component group of $J_{/\mathbb{F}_p}$. After tensoring with $\mathbb{Z}_\ell$ over $\mathbb{Z}$,

$$0 \longrightarrow Y \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}(Y \otimes \mathbb{Z}_\ell, \mathbb{Z}_\ell) \longrightarrow \Phi_\ell \longrightarrow 0.$$

Using an idempotent $e_{\mathfrak{n}} \in \mathbb{T}_\ell := \mathbb{T} \otimes \mathbb{Z}_\ell$, we get

$$0 \longrightarrow Y_{\mathfrak{n}} \longrightarrow \mathrm{Hom}(Y_{\mathfrak{n}}, \mathbb{Z}_\ell) \longrightarrow \Phi_{\mathfrak{n}} \longrightarrow 0.$$

By Ribet [29], there is an exact sequence,

$$0 \longrightarrow \Phi_q(J_0(q)_{/\mathbb{F}_q}) \longrightarrow (X \oplus X)/(A(X \oplus X)) \longrightarrow \Phi \longrightarrow C \longrightarrow 0,$$

where $A = \begin{pmatrix} p+1 & T_p \\ T_p & p+1 \end{pmatrix}$ and C is the cokernel of the map $\Phi_q(J_0(q)_{/\mathbb{F}_q}) \times \Phi_q(J_0(q)_{/\mathbb{F}_q}) \to \Phi_q(J_0(pq)_{/\mathbb{F}_q})$ which we discussed in section 2.7.(See Corollary 2.7.6.) Note that there is no Eisenstein maximal ideal of level q of characteristic ℓ and $C_{\mathfrak{n}} = 0$ since U_q acts by 1 on C. Thus first, second, and fourth terms vanish after localizing at $\mathfrak{n}$ (resp. $\mathfrak{b}$). In other words, $\Phi_{\mathfrak{n}} = 0$, which implies that $Y_{\mathfrak{n}} \simeq \mathrm{Hom}(Y_{\mathfrak{n}}, \mathbb{Z}_\ell)$ is self-dual. Therefore $\mathbb{T}_{\mathfrak{n}}$ is Gorenstein. □

Now we prove the theorem above.

Proof of Theorem 3.5.1. Let $J_{\mathfrak{n}} := \cup_m J[\mathfrak{n}^m]$ be the $\mathfrak{n}$-divisible group of J and let $T_{\mathfrak{n}}J$ be local factor of the Tate module of J at $\mathfrak{n}$, which is $\mathrm{Hom}(J_{\mathfrak{n}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$. Then $T_{\mathfrak{n}}J$ is free of rank 2 if and only if $J[\mathfrak{n}]$ is of dimension 2 over $\mathbb{T}/\mathfrak{n}$. Since J has purely toric reduction at p, there is an exact sequence for any $m \geq 1$ [28]:

$$0 \longrightarrow \mathrm{Hom}(Y/\ell^m Y, \mu_{\ell^m}) \longrightarrow J[\ell^n] \longrightarrow Y/\ell^m Y \longrightarrow 0.$$

By taking projective limit, we have

$$0 \longrightarrow \mathrm{Hom}(Y \otimes \mathbb{Z}_\ell, \mathbb{Z}_\ell(1)) \longrightarrow T_\ell J \longrightarrow Y \otimes \mathbb{Z}_\ell \longrightarrow 0,$$

where $\mathbb{Z}_\ell(1)$ is the Tate twist. By applying idempotent $e_{\mathfrak{n}}$, we get

$$0 \longrightarrow \mathrm{Hom}(Y_{\mathfrak{n}}, \mathbb{Z}_\ell(1)) \longrightarrow T_{\mathfrak{n}}J \longrightarrow Y_{\mathfrak{n}} \longrightarrow 0.$$

Since $Y_{\mathfrak{n}}$ is free of rank 1 over $\mathbb{T}_{\mathfrak{n}}$, $T_{\mathfrak{n}}J$ is free of rank 2 over $\mathbb{T}_{\mathfrak{n}}$. □

Remark 3.5.3. By Mazur(appendix of [36]), $\mathbb{T}_{\mathfrak{n}}$ is Gorenstein if and only if $J[\mathfrak{n}]$ is of dimension 2.

Chapter 4

Modularity of reducible representations

In this chapter, we discuss modularity of reducible mod ℓ representation $1 \oplus \chi$, more precisely, we want to classify admissible tuples for prime $\ell \geq 5$. Recall that for positive integers s, t such that $s \leq t$, a t-tuple $(p_1, \cdots, p_s, \cdots, p_t)$ is admissible (for s) if there is a mod ℓ Eisenstein-like newform $f = \sum_{n=1}^{\infty} a_n q^n$ of level $N = \prod_{i=1}^{t} p_i$ such that $a_{p_i} = 1$ for $1 \leq i \leq s$ and $a_{p_j} = -1$ for $s < j \leq t$. Since we treat only modular forms of weight two(and trivial character if it is an eigenform), $a_r \equiv 1 + r \pmod{\ell}$ for primes $r \nmid \ell N$.

From now on, fix a prime $\ell \geq 5$ and let s, t be positive integers such that $s \leq t$. (Since there is no modular forms of weight 2 and level 1, t is always positive. Moreover, we will prove s should not be 0.) We also assume that a square-free level N is prime to ℓ for simplicity.

4.1 Known results I

In this section, we study results about classification of admissible tuples before this dissertation. It started from Mazur, he proved the case for $t = 1$ in his famous paper [25]. After his work, it has not been studied much. Around 2008, Ribet generalized Mazur's result to many cases, and he could classify them completely when $t = 2$. Before handling specific cases, we consider necessary and sufficient conditions for admissibility.

Necessary conditions

Theorem 4.1.1 (Ribet)**.** *For non-negative integers $s \leq t$ assume a t-tuple $(p_1, \cdots, p_s, \cdots, p_t)$ is admissible. Then the following hold.*

1. $s \geq 1$.
2. *If $t = s$, $\ell \mid \phi(N) = \prod_{i=1}^{t} (p_i - 1)$.*

3. For $s < j \leq t$, $p_j \equiv -1 \pmod{\ell}$.

Proof. 1. When $s = 0, t = 1$, Mazur proved that a prime p is not admissible [25]. Ribet generalized his result to the case $s = 0, t = 2$ [3] and this method also works for general t. Here we prove it for $s = 0, t = 3$ by following Ribet's method. Assume (p, q, r) is admissible and f is a mod ℓ Eisenstein-like newform of type $(0, 3)$. Let $E := e - e_p - e_q - e_r + e_{pq} + e_{pr} + e_{qr} - e_{pqr}$. Then, for any Hecke operator T_k for prime k not dividing pqr, we have

$$T_k(E) = (k+1)E, \text{ and } \quad T_k(f) \equiv (k+1)f \pmod{\ell}.$$

Moreover since $p \equiv q \equiv r \equiv -1 \pmod{\ell}$ by 3, we have

$$T_p(E) \equiv T_q(E) \equiv T_r(E) \equiv -E \pmod{\ell}$$

$$T_p(f) = T_q(f) = T_r(f) = -f.$$

Thus E and f have the same Fourier expansion modulo ℓ at $i\infty$ modulo ℓ, therefore $E \equiv f \pmod{\ell}$.

Again $p \equiv -1 \pmod{\ell}$ implies that $e - pe_p \equiv e + e_p \pmod{\ell}$ is a mod ℓ Eisenstein series of level p of type $(1, 1)$. Similarly, $e + e_q$, $e + e_r$ are mod ℓ Eisenstein series. By the map B_p and B_q which are induced by the degeneracy maps, $e_p + e_{pq}$, $e_{pq} + e_{pqr}$, and $e + e_{pqr} = (e + e_p) - (e_p + e_{pq}) + (e_{pq} + e_{pqr})$ are also mod ℓ modular forms of level pqr. Since $p \equiv q \equiv r \equiv -1 \pmod{\ell}$, $F := e + e_p + e_q + e_r + e_{pq} + e_{pr} + e_{qr} + e_{pqr}$ is a mod ℓ Eisenstein series of type $(3, 3)$. Using these mod ℓ modular forms, we have $8e = F - E - 2(e + e_p) - 2(e + e_q) - 2(e + e_r) - 2(e + e_{pqr})$, a mod ℓ modular form of level pqr which is prime to ℓ. This contradicts to the fact that the "filtration" of e is $\ell + 1$ which means e cannot be a linear combination of mod ℓ modular forms of weight two of level prime to ℓ.(See Remark 2.5.2.)

2. Let f be a mod ℓ Eisenstein-like newform of type (t, t) and E be the Eisenstein series of type (t, t). Let $N = \prod_{i=1}^{t} p_i$. Then, by the definition, E is

$$e - \sum_{i=1}^{t} p_i e_{p_i} + \sum_{1 \leq i < j \leq t} p_i p_j e_{p_i p_j} + \cdots + (-1)^t N e_N.$$

So, its constant term of Fourier series is $\frac{(-1)^{t-1}}{24}\phi(N)$ that is the Fourier expansion of the mod ℓ modular form $E - f$. Therefore it should be 0 modulo ℓ by Mazur (section 5 of Chapter II of [25]).

3. Let $f = \sum a_n q^n$ be a mod ℓ Eisenstein-like newform of type (s, t). Then the semisimplification of a mod ℓ Galois representation ρ associated to f is $1 \oplus \chi$. The semisimplification of the local representation $\rho_p := \rho \mid_{\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)}$ for p dividing N is $\epsilon \oplus \epsilon\chi$ where ϵ

is an unramified quadratic character. For $s < j \leq t$, $\epsilon(\mathrm{Frob}_{p_j}) = a_{p_j} = -1$ where Frob_p is a Frobenius element of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. Therefore $p_j = \chi(\mathrm{Frob}_{p_j}) \equiv -1 \pmod{\ell}$.

□

Sufficient conditions

Theorem 4.1.2 (Ribet)**.** *For positive integers $s \leq t$ a t-tuple $(p_1, \cdots, p_s, \cdots, p_t)$ is admissible if one of the following conditions holds.*

1. *$t = s$, s is odd, and $\ell \mid \phi(N) = \prod_{i=1}^{t}(p_i - 1)$.*
2. *$t = s + 1$, s is odd, and $p_t \equiv -1 \pmod{\ell}$.*

Proof. 1. Let $p_1 = p$ and $D = \prod_{i=2}^{t} p_i$. (Since the number of prime factors of D is even, there is the Shimura curve $X_0^D(p)$.) Then $\Phi := \Phi_p(J_0^D(p))$, the component group of $J_0^D(p)_{/\mathbb{F}_p}$, is annihilated by an Eisenstein ideal $I := (U_p - 1, U_r - 1, T_k - k - 1)$ for primes $r \mid D$ and primes $k \nmid N = Dp$ in $\mathbb{T}_p^D$. Since the order of Φ is "roughly" $\phi(N)$, for $\mathfrak{m} := (I, \ell)$, $\Phi[\mathfrak{m}] \neq 0$, which means $\mathfrak{m}$ is maximal. By Ribet [29], the action of $\mathbb{T}_p^D$ on the character group X of $J_0^D(p)_{/\mathbb{F}_p}$ is p-new and we have the monodromy exact sequence,

$$0 \longrightarrow X \longrightarrow \mathrm{Hom}(X, \mathbb{Z}) \longrightarrow \Phi \longrightarrow 0.$$

Therefore the action of $\mathbb{T}_p^D$ on Φ factors through its p-new quotient, which implies $\mathfrak{m}$ is p-new. By Jacquet-Langlands correspondence, we can consider $\mathfrak{m}$ as a new maximal ideal of $\mathbb{T}_N$, in other words, there is a mod ℓ Eisenstein-like newform of level N of type (t, t).

2. Let $N = \prod_{i=1}^{t} p_i$, $D = \prod_{i=2}^{t} p_i$, $p = p_1$, and $q = p_{t+1}$. (Since the number of prime factors of D is even, there are Shimura curves $X_0^D(p)$, $X_0^D(pq)$, and $X_0^{Dpq}(1)$.) By Ribet, there are Hecke equivariant exact sequences:

$$\Phi_p(J_0^D(p)) \times \Phi_p(J_0^D(p)) \xrightarrow{g} \Phi_p(J_0^D(pq)) \longrightarrow C \longrightarrow 0$$

and

$$\Phi_q(J_0^{Dpq}(1)) \longrightarrow C \longrightarrow 0.$$

From the first one, $I := (U_p - 1, U_q - q, U_r - 1, T_s - s - 1)$ for primes $r \mid D$ and primes $s \nmid Nq$ annihilates C. By the previous discussion about Deligne-Rapoport model of the Jacobians, $\Phi_p(J_0^D(p))$ and $\Phi_p(J_0^D(pq))$ are almost cyclic groups. By Proposition 2.7.5 and the condition that $q \equiv -1 \pmod{\ell}$, $C[\mathfrak{m}] \neq 0$ where $\mathfrak{m} := (I, \ell)$. Therefore, $\mathfrak{m}$ is

maximal. From the second exact sequence, the action of Hecke operators on C factors through $\mathbb{T}^{\mathrm{new}}$, so $\mathfrak{m}$ is a new maximal ideal.

□

Here is a theorem of "level raising" which we will prove later. (See section 4.3.)

Theorem 4.1.3 (Ribet)**.** *For positive integers $s \leq t$ assume that a t-tuple $(p_1, \cdots, p_s, \cdots, p_t)$ is admissible and t is odd. Then a $t+1$-tuple $(p_1, \cdots, p_s, \cdots, p_t, p_{t+1})$ (with the same s) is admissible if and only if $p_{t+1} \equiv -1 \pmod{\ell}$.*

4.2 Known results II

In this section, we classify admissible tuples for $t \leq 2$.

The case $t = 1$

Theorem 4.2.1 (Mazur)**.** *1. For $s = 0$, (p) is not admissible.*

2. For $s = 1$, (p) is admissible if and only if $p \equiv 1 \pmod{\ell}$.

Proof. 1. This is proved by Theorem 4.1.1.1.

2. This is proved by Theorem 4.1.1.2 and Theorem 4.1.2.1.

□

The case $t = 2$

Theorem 4.2.2 (Ribet)**.** *1. For $s = 0$, a pair (p, q) is not admissible.*

2. For $s = 1$, a pair (p, q) is admissible if and only if $q \equiv -1 \pmod{\ell}$.

3. For $s = 2$, if a pair (p, q) is admissible, then $\ell \mid (p-1)(q-1)$. Assume $\ell \mid p-1$. Then, a pair (p, q) is admissible if and only if $q \equiv 1 \pmod{\ell}$ or q is an ℓ-th power modulo p.

Proof. 1. This is done by Theorem 4.1.1.1.

2. This is done by Theorem 4.1.1.3 and Theorem 4.1.2.2.

3. See section 4.3.

□

4.3 Level-raising methods

In his paper [27], Ribet studied the kernel of the map γ_p between the Jacobians of modular curves which is induced by degeneracy maps. Using this result, Ribet could find the intersection of the p-old subvariety and the p-new subvariety of the Jacobians. Diamond and Taylor generalized Ribet's results [15] and their results can be applied to level raising for irreducible modular representations. On the other hands, we cannot directly use their results to raise level of reducible modular representations. The reason is basically that the kernel of γ_p induced by degeneracy maps is "Eisenstein". We circumvent this method by using Ribet's exact sequences. We prove the known results about admissible tuples in the previous sections which can be done by this new one.

Definition

Let $\mathfrak{m}$ be a new maximal ideal of Hecke ring $\mathbb{T}_N$ of residue characteristic ℓ and let $\rho_{\mathfrak{m}}$ be the associated mod ℓ Galois representation to $\mathfrak{m}$. Assume p is prime which does not divide N. We call *level raising occurs from level N to level Np* (for given maximal ideal $\mathfrak{m}$ or Galois representation $\rho_{\mathfrak{m}}$) if there is a maximal ideal $\mathfrak{n}$ of Hecke ring $\mathbb{T}_{Np}$ such that

1. $\mathfrak{n}$ is p-new.
2. The mod ℓ representation $\rho_{\mathfrak{n}}$ associated to $\mathfrak{n}$ is isomorphic to $\rho_{\mathfrak{m}}$.

Equivalent conditions

Let $\mathbb{T} := \mathbb{T}_{Np}$. $\mathbb{T}^{p\text{-old}}$ is isomorphic to $\mathbb{T}_N$ and a maximal ideal $\mathfrak{m}$ of $\mathbb{T}_N$ can be thought as one of $\mathbb{T}^{p\text{-old}}$. By abusing notation, let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$ whose image in $\mathbb{T}^{p\text{-old}}$ is $\mathfrak{m}$. If level raising occurs for $\mathfrak{m}$, $\mathfrak{m}$ should be also p-new, in other words, the image of $\mathfrak{m}$ in $\mathbb{T}^{p\text{-new}}$ is maximal.

To detect level-raising phenomena, Ribet proved the following theorem.

Theorem 4.3.1 (Ribet)**.** *Let $J := J_0(Np)$. As before, assume Np is prime to ℓ and p does not divide N. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_N$ of residue characteristic ℓ. Then $\mathfrak{m}$ is also p-new if and only if*

$$(J_{p\text{-old}} \cap J_{p\text{-new}})[\mathfrak{m}] \neq 0.$$

Proof. Let $\Omega := J_{p\text{-old}} \cap J_{p\text{-new}}$. If $\Omega[\mathfrak{m}] \neq 0$, $J_{p\text{-new}}[\mathfrak{m}]$ is not zero, which implies $\mathfrak{m}$ is p-new.

Conversely, assume $\Omega[\mathfrak{m}] = 0$. Consider the following exact sequence;

$$0 \longrightarrow \Omega \longrightarrow J_{p\text{-old}} \times J_{p\text{-new}} \longrightarrow J \longrightarrow 0.$$

Let $e = (1, 0) \in \mathbb{T}^{p\text{-old}} \times \mathbb{T}^{p\text{-new}}$. If $e \notin \mathrm{End}(J)$, $J \ncong J_{p\text{-old}} \times J_{p\text{-new}}$. Thus $\Omega[\mathfrak{m}] = 0$, which means that $\mathfrak{m}$ is not in the support of Ω, implies $e \in \mathrm{End}(J) \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{m}}$. Moreover $e \in \mathbb{T} \otimes \mathbb{Q}$

because $\mathbb{T}^{p\text{-old}} \times \mathbb{T}^{p\text{-new}}$ is finite over $\mathbb{T}$. Thus

$$e \in (\mathbb{T} \otimes \mathbb{Q}) \cap (\mathrm{End}J \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{m}}).$$

The intersection $(\mathbb{T} \otimes \mathbb{Q}) \cap (\mathrm{End}J \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{m}})$ is equal to the localization of the saturation of $\mathbb{T}$ in $\mathrm{End}(J)$ at $\mathfrak{m}$. Since $\mathbb{T}$ is saturated in $\mathrm{End}(J)$ locally at $\mathfrak{m}$ by the Agashe, Ribet and Stein [2], $e \in \mathbb{T}_{\mathfrak{m}}$.

If $\mathfrak{m}$ is also a maximal ideal after projection $\mathbb{T} \to \mathbb{T}^{p\text{-new}}$, the injection $\mathbb{T} \hookrightarrow \mathbb{T}^{p\text{-old}} \times \mathbb{T}^{p\text{-new}}$ is not an isomorphism after localizing at $\mathfrak{m}$. Thus $e = (1, 0) \in \mathbb{T}^{p\text{-old}} \times \mathbb{T}^{p\text{-new}}$ cannot be in $\mathbb{T}_{\mathfrak{m}}$, which is contradiction. Therefore $\mathfrak{m}$ is not p-new. □

Remark 4.3.2. The theorem of Agashe, Ribet, and Stein is the following.

Theorem 4.3.3 (Agashe, Ribet, and Stein). *Let ℓ be the characteristic of $\mathbb{T}_N/\mathfrak{m}$. $\mathbb{T}_N$ is saturated in* $\mathrm{End}(J_0(N))$ *locally at $\mathfrak{m}$ if*

1. *$\ell \nmid N$, or*
2. *$\ell \| N$ and $T_\ell \equiv \pm 1 \pmod{\mathfrak{m}}$.*

In our case, the level Np is prime to ℓ, so $\mathbb{T}_{Np}$ is saturated in $\mathrm{End}(J_0(Np))$ locally at $\mathfrak{m}$.

Intersection of p-old subvariety and p-new subvariety

Let p be a prime and N be an integer which is prime to p. Let Ω be the intersection of p-old subvariety and p-new subvariety of $J_0(Np)$. By degeneracy maps, we have the following maps

$$J_0(N) \times J_0(N) \xrightarrow{\gamma_p} J_0(Np) \xrightarrow{d_p} J_0(N) \times J_0(N).$$

The composition of d_p and γ_p is the matrix

$$\delta_p := \begin{pmatrix} p+1 & T_p \\ T_p & p+1 \end{pmatrix}.$$

Let Δ be the kernel of the above composition δ_p, i.e.,

$$\Delta := J_0(N)^2[\delta_p] = \{(x, y) \in J_0(N)^2 : T_p x = (p+1)y \text{ and } (p+1)x = T_p y\}.$$

And let Σ be the kernel of γ_p. Then Δ contains Σ and is endowed with a canonical non-degenerate alternating $\mathbb{G}_{\mathrm{m}}$-valued pairing. Let $\Sigma^\perp$ be the orthogonal to Σ relative to this pairing; this subgroup of Δ contains Σ, and we have the formula

$$\Omega = \Sigma^\perp/\Sigma.$$

For more details, see [27].

If we invert 2, we can decompose Δ into eigenspaces. Let

$$\Delta^+ := \{(x,-x) \in J_0(N)^2 : x \in J_0(N)[T_p - p - 1]\}$$

and

$$\Delta^- := \{(x,x) \in J_0(N)^2 : x \in J_0(N)[T_p + p + 1]\}.$$

Then $\Delta \simeq \Delta^+ \oplus \Delta^-$ if we invert 2. Furthermore, these eigenspaces have filtration;

$$0 \subset \Sigma^+ \subset (\Sigma^\perp)^+ \subset \Delta^+$$

and

$$0 \subset \Sigma^- \subset (\Sigma^\perp)^- \subset \Delta^-.$$

Since $\Delta/\Sigma^\perp$ is the $\mathbb{G}_{\mathrm{m}}$-dual of Σ and Σ is an antidiagonal embedding of the Shimura subgroup of $J_0(N)$ by Ribet [27], $\Sigma^+ = \Sigma$ and $\Sigma^- = 0$. Thus,

$$(\Sigma^\perp)^- = \Delta^-.$$

By the map γ_p, $(\Sigma^\perp)^+$ maps to $(\Sigma^\perp)^+/\Sigma$ and $(\Sigma^\perp)^- = \Delta^-$ maps to Δ^-. $(\Sigma^\perp)^+/\Sigma$(resp. Δ^-) corresponds to the $+1$-eigenspace(resp. -1-eigenspace) of Ω of the U_p operator.

Proofs

Proof of Theorem 4.1.3. Let $p = p_1$, $M = \prod_{i=2}^{s} p_i$, $N = \prod_{j=s+1}^{t} p_j$, and $q = p_{t+1}$. (Since the number of prime factors of MN is even, there are Shimura curves $X_0^{MN}(p)$, $X_0^{MN}(pq)$, and $X_0^{pMNq}(1)$.) If a $t+1$-tuple $(p, p_2, \ldots, p_t, q)$ is admissible, then $q \equiv -1 \pmod{\ell}$ by Theorem 4.1.1.3.

Conversely, assume $q \equiv -1 \pmod{\ell}$. Since a t-tuple $(p, p_2, \ldots, p_t)$ is admissible, there is a new Eisenstein maximal ideal $\mathfrak{m}$ in $\mathbb{T}_{pMN}$ of type (s,t). In other words, $\mathfrak{m} := (\ell, U_m - 1, U_n + 1, T_k - k - 1)$ for primes $m \mid pM$, $n \mid N$, and $k \nmid pMN$ is new maximal. Let X be the character group of $J_0^{MN}(p)_{/\mathbb{F}_p}$. Then, by Ribet, there is a Hecke equivariant exact sequence

$$0 \longrightarrow X/(T_q + q + 1)X \longrightarrow \Phi_q(J_0^{pMNq}(1))$$

where $\Phi_q(J_0^{pMNq}(1))$ is the component group of $J_0^{pMNq}(1)_{/\mathbb{F}_q}$. Because $q \equiv -1 \pmod{\ell}$, $T_q + q + 1 \equiv T_q - q - 1 \pmod{\ell}$ and $T_q + q + 1 \in \mathfrak{m}$. By the Jacquet-Langlands correspondence and the fact that $\mathbb{T}_p^{MN,p\text{-new}}$ acts faithfully on X, $X/(T_q + q + 1)X[\mathfrak{m}] \neq 0$, so $\Phi_q(J_0^{pMNq}(1))[\mathfrak{n}] \neq 0$, where $\mathfrak{n} := (\ell, U_m - 1, U_n + 1, T_k - k - 1)$ for primes $m \mid pM$, $n \mid Nq$, and $k \nmid pMNq$ in $\mathbb{T}^{pMNq}$. In other words, $\mathfrak{n}$ is maximal. By the Jacquet-Langlands correspondence, $\mathfrak{n}$ is new. □

Proof of Theorem 4.2.2.3. By Theorem 4.1.1.2, first statement follows. For the second one, consider an exact sequence of Ribet,

$$0 \longrightarrow \Phi \longrightarrow X/(T_q - q - 1)X \longrightarrow \Psi^+ \longrightarrow 0,$$

where Φ is the component group of $J_0(p)_{/\mathbb{F}_p}$, X is the character group of $J_0(p)_{/\mathbb{F}_p}$, and Ψ^+ is the $+1$-eigenspace of U_q on the component group of $J_0^{pq}(1)_{/\mathbb{F}_q}$. Let I be an Eisenstein ideal of $\mathbb{T} := \mathbb{T}_p$ and $\mathfrak{m} := (I, \ell)$, in other words, $I := (U_p - 1, T_r - r - 1)$ for primes $r \nmid p$. (By Theorem 4.2.1.2, $\mathfrak{m}$ is maximal because $p \equiv 1 \pmod{\ell}$.) Since Φ is a free module of rank 1 over $\mathbb{T}/I$ and $X_{\mathfrak{m}}$ is free of rank 1 over $\mathbb{T}_{\mathfrak{m}}$ [25],

$$\#(X/IX)_{\mathfrak{m}} = \#(\mathbb{T}/I)_{\mathfrak{m}} = \#(\Phi)_{\mathfrak{m}}.$$

Therefore, if $T_q - q - 1$ is not a local generator of I at $\mathfrak{m}$,

$$\#(X/(T_q - q - 1)X)_{\mathfrak{m}} > \#(X/IX)_{\mathfrak{m}} = \#(\Phi)_{\mathfrak{m}},$$

so $\Psi^+_{\mathfrak{n}}$ is not zero, where $\mathfrak{n} := (\ell, U_p - 1, U_q - 1, T_r - r - 1)$ for primes $r \nmid pq$ in $\mathbb{T}^{pq}$. Hence, $\mathfrak{n}$ is maximal. By the Jacquet-Langlands correspondence, $\mathfrak{n}$ is new. By Mazur [25], $T_q - q - 1$ is not a local generator if and only if $q \equiv 1 \pmod{\ell}$ or q is an ℓ-th power modulo p.

Conversely, assume $T_q - q - 1$ is a local generator of I. We use the similar notations as the previous subsection. Let Ω be $J_0(pq)_{q\text{-old}} \cap J_0(pq)_{q\text{-new}}$, Δ be $J_0(pq)^2[\delta_q]$, and Σ be the kernel of γ_q. We have filtration of Δ^+;

$$0 \subset \Sigma \subset (\Sigma^{\perp})^+ \subset \Delta^+.$$

And Δ^+ is isomorphic to $J_0(p)[T_q - q - 1]$. Since $T_q - q - 1$ is a local generator of I, $(\Delta^+)_{\mathfrak{m}}$ is isomorphic to $J_0(p)[I]_{\mathfrak{m}}$. By Mazur [25], $J_0(p)[I]$ is free of rank 2 over $\mathbb{T}/I$ and Σ is free of rank 1 over $\mathbb{T}/I$. Thus the $\mathfrak{m}$-primary subgroup of $(\Sigma^{\perp})^+/\Sigma$ is 0 because $\Delta^+/(\Sigma^{\perp})^+$ is the $\mathbb{G}_{\mathrm{m}}$-dual of Σ. In other words, the $\mathfrak{m}$-primary subgroup of Ω is 0, i.e., Ω does not have support at $\mathfrak{m}$. By the Theorem 4.3.1, $\mathfrak{m}$ is not q-new. In other words, a pair (p, q) is not admissible. □

4.4 The main theorem

One of main theorems of this dissertation is the conditions of admissibility of a triple (p, q, r) for $s = 2$. Namely, the problem we want to solve is to find necessary and sufficient conditions for the existence of an Eisenstein-like newform f of level pqr such that $U_p f = f$, $U_q f = f$, and $U_r f = -f$. If a triple (p, q, r) is admissible, $r \equiv -1 \pmod{\ell}$ by Theorem 4.1.1.3.

So, assume $r \equiv -1 \pmod{\ell}$. Let $I = (U_p - 1, U_r - r, T_k - k - 1)$ for primes $k \nmid pr$ be an Eisenstein ideal of level pr. Since $r \equiv -1 \pmod{\ell}$, $\mathfrak{m} := (\ell, I)$ is new maximal by Theorem 4.2.2.2. We want to understand admissibility of a triple (p, q, r) by using level-raising method. Here is one of our main theorems.

Theorem 4.4.1. *Assume that $p \not\equiv 1 \pmod{\ell}$ and if $q \equiv 1 \pmod{\ell}$, assume p is not an ℓ-th power modulo q. Let η_q be the operator $T_q - q - 1$. Then,*

1. *a triple (p, q, r) is admissible for $s = 2$ if η_q is not a local generator of I at $\mathfrak{m}$.*

2. *Assume further that* $r \not\equiv -1 \pmod{\ell^2}$. *Then, a triple* (p,q,r) *is not admissible for* $s=2$ *if* η_q *is a local generator of* I *at* $\mathfrak{m}$.

Proof. 1. The condition that η_q is not a local generator of I at $\mathfrak{m}$ implies that $(L/\eta_q L)_{\mathfrak{m}} \neq (L/IL)_{\mathfrak{m}}$, where L is the character group of $J_0(pr)_{/\mathbb{F}_p}$. By the Ribet, there is an exact sequence,

$$0 \longrightarrow \Phi \longrightarrow L/\eta_q L \longrightarrow \Psi^+ \longrightarrow 0,$$

where $\Phi := \Phi_p(J_0(pr))$ is the component group of $J_0(pr)_{/\mathbb{F}_p}$ and Ψ^+ is the $+1$-eigenspace of the operator U_q on the component group $\Psi := \Phi_q(J_0^{pq}(r))$ of $J_0^{pq}(r)_{/\mathbb{F}_q}$. Let $\mathfrak{n}$ be the ideal of $\mathbb{T}_r^{pq}$ which is generated by ℓ,$U_p - 1$, $U_q - 1$, $U_r + 1$, and $T_k - k - 1$ for primes $k \nmid pqr$. Then, after localizing at $\mathfrak{m}$ we have

$$0 \longrightarrow \Phi_{\mathfrak{m}} \longrightarrow (L/\eta_q L)_{\mathfrak{m}} \longrightarrow (\Psi^+)_{\mathfrak{n}}.$$

If $\#(L/\eta_q L)_{\mathfrak{m}}$ is bigger than $\#\Phi_{\mathfrak{m}}$, $(\Psi^+)_{\mathfrak{n}}$ is non-zero, i.e.,$\mathfrak{n}$ is maximal. Let n be an exact power of ℓ which divides $r+1$, i.e., $\ell^n \parallel r+1$. Then, $\#(\Phi_{\mathfrak{m}}) = \ell^n$ since the order of Φ is "roughly" $(p-1)(r+1)$ and $p \not\equiv 1 \pmod{\ell}$. (Note that $\Phi_{\mathfrak{m}}$ is equal to the ℓ-primary part of Φ.) Since $L/\mathfrak{m}L$ is of dimension 1 over $\mathbb{T}/\mathfrak{m}$(see Remark 3.3.8.), $L_{\mathfrak{m}}$ is free of rank 1 over $\mathbb{T}_{\mathfrak{m}}$. The order of $\mathbb{T}_{\mathfrak{m}}/I_{\mathfrak{m}} = (\mathbb{T}/I)_{\mathfrak{m}}$ is ℓ^n, which is the largest power of ℓ which divides $(p-1)(r-1)(r+1)$ because $\ell \nmid (p-1)(r-1)$. Thus

$$\#(L/(\eta_q)L)_{\mathfrak{m}} > \#(L/IL)_{\mathfrak{m}} = \#(\mathbb{T}/I\mathbb{T})_{\mathfrak{m}} = \#(\Phi_{\mathfrak{m}})$$

since η_q is not a local generator of I at $\mathfrak{m}$. As we discussed above, this implies that $\mathfrak{n}$ is maximal. By Jacquet-Langlands correspondence, $\mathfrak{n}$ can be considered as a pq-new maximal ideal of $\mathbb{T}_{pqr}$. If it were r-old, a pair (p,q) should be admissible for $s=2$. The assumption implies that a pair (p,q) is not admissible by Theorem 4.2.2.3. Thus $\mathfrak{n}$ is genuinely new, which implies the admissibility of a triple (p,q,r) for $s=2$.

2. See Remark 5.4.1.

□

Remark 4.4.2. Examples in next section tell us that η_q is not a local generator if a pair (p,q) is admissible for $s=2$. This phenomenon can be proved by assuming a well known conjecture about congruence subgroup property for S-arithmetic groups.

4.5 Examples

When N is prime, η_q is a local generator of an Eisenstein ideal $I = (T_r - r - 1)$ for primes r not dividing N at $\mathfrak{m} := (\ell, I)$ if and only if $q \equiv 1 \pmod{\ell}$ or q is not an ℓ-th power modulo N. In contrast, when N is composite, we don't know what congruence implies local generation.

Consider the easiest case. As in Theorem 4.4.1, we assume $r \equiv -1 \pmod{\ell}$ and $p \not\equiv 1 \pmod{\ell}$. Assume further $\ell \parallel (p-1)(r+1)$, in other words, $r \not\equiv -1 \pmod{\ell^2}$. In this case $I_{\mathfrak{m}} = \mathfrak{m}$. Let $f(\tau) = \sum a_n x^n$ be an Eisenstein-like newform of level pr and type $(1,2)$ where $x = e^{2\pi i \tau}$. If $a_q \equiv q+1 \pmod{\ell^2}$, $\eta_q := T_q - q - 1 \in \mathfrak{m}^2$, so η_q is not a local generator of I at $\mathfrak{m}$.

Moreover in our examples below, all newforms are defined over $\mathbb{Q}$, i.e., $\mathbb{T}_{pr} = \mathbb{Z}$ and $\mathfrak{m} = \ell\mathbb{Z}$, which implies that η_q is not a local generator if and only if $\eta_q \in \mathfrak{m}^2$.

Admissibility of $(2, q, 19)$ for $s = 2$ when $\ell = 5$

An Eisenstein-like newform of level $pr = 38$ and type $(1,2)$ is 38.2b. Let a_n be the eigenvalue of T_n for 38.2b. Then $a_q \equiv 1 + q \pmod{25}$ when $q =$ 23, 41, 97, 101, 109, 113, 149, 151, 193, 199, 239, 241, 251, 257, 277, 347, 359, 431, and 479 for primes $q < 500$. Since only $(2, 151)$, $(2, 241)$, $(2, 251)$, and $(2, 431)$ for $s = 2$ are admissible, a triple $(2, q, 19)$ for $s = 2$ is admissible if

$$q = 23, 41, 97, 101, 109, 113, 149, 193, 199, 239, 257, 277, 347, 359, \text{ and } 479$$

for $q < 500$.

Admissibility of $(3, q, 19)$ for $s = 2$ when $\ell = 5$

An Eisenstein-like newform of level $pr = 57$ and type $(1,2)$ is 57.2b. Let b_n be the eigenvalue of T_n for 57.2b. Then $b_q \equiv 1 + q \pmod{25}$ when $q =$ 41, 97, 101, 167, 197, 251, 257, 269, 313, 349, 409, 419, 431, and 491 for primes $q < 500$. Since only $(3, 41)$, $(3, 431)$, and $(3, 491)$ for $s = 2$ are admissible, a triple $(3, q, 19)$ for $s = 2$ is admissible if

$$q = 97, 101, 167, 197, 251, 257, 269, 313, 349, 409, \text{ and } 419$$

for $q < 500$.

Admissibility of $(2, q, 29)$ for $s = 2$ when $\ell = 5$

An Eisenstein-like newform of level $pr = 58$ and type $(1,2)$ is 58.2b. Let c_n be the eigenvalue of T_n for 58.2b. Then $c_q \equiv 1 + q \pmod{25}$ when $q =$ 89, 97, 137, 151, 181, 191, 223, 241, 251, 347, 367, 401, 431, 433, and 491 for primes $q < 500$. Since only $(2, 151)$, $(2, 241)$, $(2, 251)$, and $(2, 431)$ for $s = 2$ are admissible, a triple $(2, q, 29)$ for $s = 2$ is admissible if

$$q = 89, 97, 137, 181, 191, 223, 347, 367, 401, 433, \text{ and } 491$$

for $q < 500$.

Admissibility of $(2, q, 13)$ for $s = 2$ when $\ell = 7$

An Eisenstein-like newform of level $pr = 26$ and type $(1, 2)$ is 26.2b. Let d_n be the eigenvalue of T_n for 26.2b. Then $d_q \equiv 1 + q \pmod{49}$ when $q = 43$, 101, 223, 229, 233, 269, 307, 311, and 349 for primes $q < 500$. Since a pair $(2, q)$ for $s = 2$ is not admissible for $q < 500$, a triple $(2, q, 13)$ for $s = 2$ is admissible if

$$q = 43, 101, 223, 229, 233, 269, 307, 311, \text{ and } 349$$

for $q < 500$.

Remark 4.5.1. In the last case, a pair $(2, q)$ for $s = 2$ is admissible when $q = 631$ and $q = 673$. As before,

$$d_{631} \equiv 1 + 631 \pmod{49} \text{ and } d_{691} \equiv 1 + 691 \pmod{49}.$$

Chapter 5

Congruence subgroup property

In this chapter we discuss the conjectural generalization of Ribet's result [27] to Shimura curves. In other words, we want to find the kernel of γ_r, where

$$J_0^D(1) \times J_0^D(1) \xrightarrow{\gamma_r} J_0^D(r).$$

By assuming a well known conjecture about congruence subgroup property, Ciavalla and Terracini proved the kernel of γ_r is Eisenstein [11]. However, their result was not enough to raise the level of mod ℓ modular Galois representation $1 \oplus \chi$ for $\ell > 3$. By considering the localization of quaternion algebras, we can exhibit the kernel of γ_r specifically up to 2, 3 primary factor if we assume the conjecture and this is enough for applications.

5.1 Quaternion algebras and congruence subgroups

Let B be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant $D \neq 1$. Thus D is the product of the even number of distinct primes. All maximal orders in B are conjugate; so let us fix one maximal order $\mathcal{O} \subset B$. For each prime p not dividing D, we fix an isomorphism of $\mathbb{Q}_p$-algebras $i_p : B_p \to M_2(\mathbb{Q}_p)$ such that $i_p(\mathcal{O}_p) = M_2(\mathbb{Z}_p)$ if $p \neq \infty$, where $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and $\mathcal{O}_p := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Let H_p be a quaternion algebra over $\mathbb{Q}_p$. Up to isomorphism, it is unique. Let R_p be the maximal order of H_p and $\mathfrak{m}_p$ be the maximal ideal of R_p. For each prime p dividing D, there is the unique two-sided ideal $I_p \subset \mathcal{O}$ of norm p. (In this chapter, a norm will mean a reduced one.) We fix an isomorphism of $\mathbb{Q}_p$-algebras $i_p : B_p \to H_p$ such that $i_p(\mathcal{O}_p) = R_p$ and $i_p(J_p) = \mathfrak{m}_p$ for a prime p dividing D, where $J_p := I_p \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Let $B_{\mathbb{A}}$ be the adelization of B, $B_{\mathbb{A}}^{\times}$ be the topological group of invertible elements in $B_{\mathbb{A}}$, and $B_{\mathbb{A}}^{\times,\infty}$ be the subgroup of finite ideles. For an integer N prime to D, let $K_p^0(N)$ and $K_p^1(N)$ be the subgroups of $\mathcal{O}_p^{\times}$ for a prime p not dividing D as follows,

$$K_p^0(N) := i_p^{-1}\left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{SL}_2(\mathbb{Z}_p) \middle| \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \equiv \left(\begin{array}{cc} * & * \\ 0 & * \end{array} \right) \pmod{N} \right\}$$

$$K_p^1(N) := i_p^{-1}\left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{SL}_2(\mathbb{Z}_p) \middle| \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \equiv \left(\begin{array}{cc} 1 & * \\ 0 & 1 \end{array} \right) \pmod{N} \right\}.$$

And let $V_0(N)$ and $V_1(N)$ be the subgroups of $B_{\mathbb{A}}^{\times,\infty}$ as follows,

$$V_0(N) := \prod_{p\nmid N} \mathcal{O}_p^1 \times \prod_{p|N} K_p^0(N)$$

$$V_1(N) := \prod_{p\nmid DN} \mathcal{O}_p^1 \times \prod_{p|N} K_p^1(N) \times \prod_{p|D}(1+J_p),$$

where $\mathcal{O}_p^1$ is the group of norm 1 elements in $\mathcal{O}_p^\times$ which is $i_p^{-1}(\mathrm{SL}_2(\mathbb{Z}_p))$ for a prime $p \nmid D$.

If U is an open compact subgroup of $B_{\mathbb{A}}^{\times,\infty}$, we put $\Phi(U) := \mathrm{GL}_2^+(\mathbb{R})U \cap B^\times$. Let $\Gamma_0^D(N)$ be the group of norm 1 elements in an Eichler order of level N, then $\Gamma_0^D(N) = \Phi(V_0(N))$. Define $\Gamma_1^D(N)$ by $\Phi(V_1(N))$. For a square-free integer N prime to D, the quotient $\Gamma_0^D(N)/\Gamma_1^D(N)$ is

$$\prod_{p|D} \left(\mathcal{O}_p^1/(1+J_p)\right) \times \prod_{p|N} (\mathbb{Z}/p\mathbb{Z})^\times \simeq \prod_{p|D} (\mathbb{Z}/(p+1)\mathbb{Z}) \times \prod_{p|N} (\mathbb{Z}/p\mathbb{Z})^\times.$$

For a prime r not dividing D let $\Gamma_r := (\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{r}])^1$, the group of norm 1 elements of the ring $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{r}]$. If we localize Γ_r at each prime p different from r, we have the same image as the localization of $\Gamma_0^D(1)$ at p. But the localization of Γ_r at r is isomorphic to $\mathrm{SL}_2(\mathbb{Q}_r)$ by the map i_r.

Let $U(M)$ be the subgroup of $B_{\mathbb{A}}^{\times,\infty}$ as follows,

$$U(M) := \prod_{p\nmid M} \mathcal{O}_p^1 \times \prod_{p|M}(1+M\mathcal{O}_p).$$

Now we can define congruence subgroups of Γ_r and introduce the conjecture of congruence subgroup property which is well known when $D = 1$.

Definition 5.1.1 (Congruence subgroups)**.** A subgroup of Γ_r is *a congruence subgroup* if it contains $\Phi(U(M))$ for some integer M.

Conjecture 5.1.2 (Congruence subgroup propery for Γ_r)**.** *Every subgroup of Γ_r of finite index is a congruence subgroup.*

Let Γ_r^{der} be the commutator subgroup of Γ_r, i.e. $\Gamma_r^{\mathrm{der}} = [\Gamma_r, \Gamma_r] := \{aba^{-1}b^{-1} : a, b \in \Gamma_r\}$. Then Γ_r^{der} is of finite index ([24], [21]). So it contains $\Phi(V(M))$ for some integer M if we assume congruence subgroup property for Γ_r. By the Chinese remainder theorem, we can understand Γ_r^{der} more. For each prime p dividing D, the commutator subgroup of $\mathcal{O}_p^1$ is $1+J_p$ by Riehm [32], so the image of Γ_r^{der} by the localization at p should be $1+J_p$. Therefore, Γ_r^{der}

contains $\Phi(V_1(N))$ for some integer N prime to D. For a prime $p \mid N$ and $p > 3$, we can define the map π_p by the composition $j_p \circ i_p$, where

$$\mathcal{O}_p^1 \xrightarrow{i_p} \mathrm{SL}_2(\mathbb{Z}_p) \xrightarrow{j_p} \mathrm{PSL}_2(\mathbb{Z}_p/p\mathbb{Z}_p).$$

Then the kernel of π_p contains localization of $\Phi(V_1(N))$ at p. Since the only quotients of $\mathrm{SL}_2(\mathbb{Z}_p/p^n\mathbb{Z}_p)$ are of the form $\mathrm{SL}_2(\mathbb{Z}_p/p^m\mathbb{Z}_p)$ for $m \leq n$ [5] and $\mathrm{PSL}_2(\mathbb{Z}_p/p\mathbb{Z}_p)$ is simple, the image of localization of Γ^{der} at p by π_p should be $\mathrm{PSL}_2(\mathbb{Z}_p/p\mathbb{Z}_p)$, which implies $\Gamma_r^{\mathrm{der}} = \Phi(V_1(1)_r)$ up to 2, 3 primary factors, where

$$V_1(1)_r := \prod_{p \nmid rD} \mathcal{O}_p^1 \times \prod_{p \mid D} (1 + J_p) \times \mathrm{SL}_2(\mathbb{Q}_r).$$

Therefore $\Gamma_r^{\mathrm{ab}} := \Gamma_r/\Gamma_r^{\mathrm{der}}$ is isomorphic to

$$\prod_{p \mid D} \left(\mathcal{O}_p^1/(1 + J_p)\right) \simeq \prod_{p \mid D} \left(\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times\right) \simeq \prod_{p \mid D} (\mathbb{Z}/(p+1)\mathbb{Z}) \simeq \Gamma_0^D(1)/\Gamma_1^D(1)$$

up to 2, 3 primary factors. The inverse image of Γ_r^{der} by an injection $\mathcal{O} \hookrightarrow \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{r}]$ is $\Gamma_1^D(1)$ up to 2, 3 primary factors.

5.2 Skorobogatov groups

In his paper [34], Skorobogatov introduced "Shimura coverings" of Shimura curves. For primes $p \mid D$, let $\Gamma_p^D(N)$ be the inverse image of $(1 + J_p)$ by i_p in $\Gamma_0^D(N)$. Then $\Gamma_1^D(N) = \bigcap_{p \mid D} \Gamma_p^D(N)$. Let $X_p^D(N)$ be the Shimura curve associated to $\Gamma_p^D(N)$, i.e., its complex points are isomorphic to $\mathfrak{h}/\Gamma_p^D(N)$. Then the covering map $X_p^D(N) \to X_0^D(N)$ is of degree $(p+1)/2$. By the Jordan [34], there is an unramified subcovering $X \to X_0^D(N)$ whose Galois group is $\mathbb{Z}/((p+1)/\epsilon(p))$, where $\epsilon(p)$ is 1, 2, 3, or 6.(About $\epsilon(p)$, see page 781 of [34].) Since unramifed abelian coverings of $X_0^D(N)$ correspond to subgroups of $J_0^D(N)$, we can define the Skorobogatov subgroup of Jacobians of Shimura curves.

Definition 5.2.1. The *p-Skorobogatov subgroup* Σ_p of $J_0^D(N)$ for prime p dividing D is the subgroup of $J_0^D(N)$ which corresponds to the above unramified covering X above. The *Skorobogatov subgroup* Σ of $J_0^D(N)$ is

$$\Sigma := \prod_{p \mid D} \Sigma_p.$$

These subgroups have very similar properties to the Shimura subgroups. For example,

Lemma 5.2.2. *On Σ_p, U_p acts by -1, U_q acts by 1 for primes q dividing D/p, U_r acts by r for primes r dividing N, and T_s acts by $s+1$ for primes $s \nmid DN$.*

Proof. The proof is very similar to the action of Hecke operators on Shimura subgroups. By using moduli theoretic description of $X_0^D(N)$, the complex points of X classifies (A, P) where A is a false elliptic curve with level N structure and P is a generator of $A[I_p]$. Since the level structures at other primes r dividing DN are compatible with the level structure at p, which gives rise to our covering X, w_r acts trivially on the covering group. This gives the action of U_q when q divides D/p because $U_q = w_q$. Since for primes r dividing N, $U_r + w_r = \beta_r^*(\alpha_r)_*$ by Lemma 2.2.1 and $\beta_r^* = w_r\alpha_r^*$, $U_r = w_r\alpha_r^*(\alpha_r)_* - w_r = w_r(r+1) - w_r = r$ on Σ_p. For primes $s \nmid DN$, $T_s = (\beta_s)_*\alpha_s^* = (\beta_s)_* w_s\beta_s^* = (\beta_s)_*\beta_s^* = s+1$ since the image of Skorobogatov groups by degeneracy maps lies in the Skorobogatov group and w_s acts trivially on it.

Consider U_p on Σ_p. By the pairing $< -, - >$ between $A[I_p]$ and $A[p]/A[I_p]$(about this pairing, see [7]), the map U_p sends (A, P) to $(A/A[I_p], Q)$, where $< P, Q >= \zeta_p$ for some fixed primitive p-th root of unity. For σ in the covering group, it sends (A, P) to $(A, \sigma P)$. Thus $U_p\sigma U_p^{-1} = \sigma^{-1}$, which implies U_p acts by -1 on Σ_p. □

Remark 5.2.3. It might be easier than above if you consider the actions of w_r on the group of 2×2 matrices as in Calegari and Venkatesh. See page 29 of [9].

5.3 Ihara's lemma for Shimura curves

In this section, by assuming Congruence subgroup property, up to 2, 3 primary factors, we compute the kernel of γ_r,

$$J_0^D(1) \times J_0^D(1) \xrightarrow{\gamma_r} J_0^D(r).$$

By the interpretation of Jacobians as cohomology groups, the kernel of γ_r is isomorphic to one of κ_r, where

$$H^1(X_0^D(1), \mathbb{Q}/\mathbb{Z}) \times H^1(X_0^D(1), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\kappa_r} H^1(X_0^D(r), \mathbb{Q}/\mathbb{Z}).$$

Since $H^1(X_0^D(1), \mathbb{Q}/\mathbb{Z})$ is isomorphic to a group cohomology $H^1(\Gamma_0^D(1), \mathbb{Q}/\mathbb{Z})$, we compute the kernel of κ_r by

$$H^1(\Gamma_0^D(1), \mathbb{Q}/\mathbb{Z}) \times H^1(\Gamma_0^D(1), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\kappa_r} H^1(\Gamma_0^D(r), \mathbb{Q}/\mathbb{Z}).$$

Since Γ_r is the amalgamated product of $\Gamma_0^D(1)$ and $\Gamma_0^D(1)$ over $\Gamma_0^D(r)$ ([11], [9]), by Lyndon exact sequence, we have the following exact sequence :

$$0 \longrightarrow H^1(\Gamma_r, \mathbb{Q}/\mathbb{Z}) \xrightarrow{i} H^1(\Gamma_0^D(1), \mathbb{Q}/\mathbb{Z}) \times H^1(\Gamma_0^D(1), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\kappa_r} H^1(\Gamma_0^D(r), \mathbb{Q}/\mathbb{Z}).$$

Since Γ_r acts trivially on $\mathbb{Q}/\mathbb{Z}$,

$$\begin{aligned} H^1(\Gamma_r, \mathbb{Q}/\mathbb{Z}) &= \mathrm{Hom}(\Gamma_r, \mathbb{Q}/\mathbb{Z}) && (5.1)\\ &= \mathrm{Hom}(\Gamma_r^{\mathrm{ab}}, \mathbb{Q}/\mathbb{Z}) && (5.2)\\ &\simeq \mathrm{Hom}(\Gamma_0^D(1)/\Gamma_1^D(N), \mathbb{Q}/\mathbb{Z}) && (5.3)\\ &= H^1(\Gamma_0^D(1)/\Gamma_1^D(N), \mathbb{Q}/\mathbb{Z}) && (5.4) \end{aligned}$$

There is an inflation and restriction exact sequence :

$$0 \longrightarrow H^1(\Gamma_0^D(1)/\Gamma_1^D(N), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\text{inf}} H^1(\Gamma_0^D(1), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\text{res}} H^1(\Gamma_1^D(N), \mathbb{Q}/\mathbb{Z})$$

and $H^1(\Gamma_0^D(1)/\Gamma_1^D(N), \mathbb{Q}/\mathbb{Z})$ is isomorphic to the Skorobogatov group of the Jacobian $J_0^D(1)$. Therefore $H^1(\Gamma_r, \mathbb{Q}/\mathbb{Z})$ maps into $\Sigma \times \Sigma$ by i, in other words, the kernel of γ_r is contained in $\Sigma \times \Sigma$.

Proposition 5.3.1. *The maps*

$$J_0^D(1) \underset{\beta_r}{\overset{\alpha_r}{\rightrightarrows}} J_0^D(r)$$

by the degeneracy maps are injective.

Proof. Since the covering group of $X_0^D(r)$ over $X_0^D(1)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_r)$ which is simple, there is no abelian covering between them. □

Since w_r acts as 1 on the Skorobogatov group, the kernel of γ_r is an antidiagonal embedding of Σ in $J_0^D(1) \times J_0^D(1)$ by the above proposition.

Theorem 5.3.2. *Assume congruence subgroup property holds for Γ_r. Then the kernel of $\gamma_r : J_0^D(1) \times J_0^D(1) \to J_0^D(r)$ is an antidiagonal embedding of the Skorobogatov subgroup of $J_0^D(1)$ up to 2, 3 primary factors.*

Remark 5.3.3. In their paper[24], Longo, Rotger, and Vigni discussed the kernel of γ_r, they didn't prove it though.

Remark 5.3.4. Even without congruence subgroup property for Γ_r, we can prove that the kernel of γ_r contains an antidiagonal embedding of the Skorobogatov subgroup of $J_0^D(1)$ by the same arguments as above.

5.4 Application to admissibility

Since the kernel of γ_r is an antidiagonal embedding of Skorobogatov subgroup, the intersection of r-old subvariety and r-new subvariety is

$$\Sigma^\perp/\Sigma,$$

where Σ is an antidiagonal embedding of Skorobogatov subgroup of $J_0^D(1)$ to $J_0^D(1)^2$ and $\Sigma^\perp$ is an orthogonal complement of Σ with respect to the natural pairing on $J_0^D(1)^2[\delta_r]$.(About δ_r, see section 4.3.) (The proof of this fact is exactly same as one in Ribet's paper [27].) Since w_r acts by -1 on Σ and $U_r + w_r$ acts by 0 on the r-new subvariety, U_r acts by $+1$ on Σ. Thus we have two filtrations of the kernel of the operator δ_r

$$\begin{pmatrix} r+1 & T_r \\ T_r & r+1 \end{pmatrix}$$

on $J_0^D(1) \times J_0^D(1)$ as follows.

$$0 \subset \Delta^+ = \Delta \subset (\Delta^\perp)^+ \subset J_0^D(1)[T_r - r - 1]$$

$$0 = \Delta^- \subset (\Delta^\perp)^- = J_0^D(1)[T_r + r + 1],$$

where A^+ denotes $+1$-eigenspace of U_r and A^- denotes -1-eigenspace of U_r. Thus $(\Sigma^\perp/\Sigma)^- = J_0^D(1)[T_r + r + 1]$. (Note that $J_0^D(1)[T_r - r - 1]$ maps into $J_0^D(1)^2$ by an anti-diagonal embedding and $J_0^D(1)[T_r + r + 1]$ maps into $J_0^D(1)^2$ by a diagonal embedding.)

Level raising methods II

We still fix a prime ℓ which is greater than 3. By using the results in previous sections, we can prove this theorem.

Theorem 5.4.1. *Assume congruence subgroup property holds for Γ_r and assume a t-tuple $(p_1, \dots, p_t)$ is admissible for s. Then a $t+1$-tuple $(p_1, \dots, p_t, r)$ is admissible (with the same s) if and only if $r \equiv -1 \pmod{\ell}$.*

Proof. By Theorem 4.1.1.3, if a $t+1$-tuple $(p_1, \dots, p_t, r)$ is admissible then $r \equiv -1 \pmod{\ell}$.

Conversely, assume that $r \equiv -1 \pmod{\ell}$. If t is odd, this is Theorem 4.1.3. So assume that t is even. Let $D = \prod_{i=1}^{t} p_i$. Then there is a Shimura curve $X_0^D(1)$. Since a t-tuple $(p_1, \dots, p_t)$ is admissible, there is a new Eisenstein maximal ideal of given type. Thus there is an Eisenstein maximal ideal $\mathfrak{m}$ of given type in $\mathbb{T}^D$. Since $\mathbb{T}^D$ acts faithfully on $J_0^D(1)$, $J_0^D(1)[\mathfrak{m}] \neq 0$ and $\mathfrak{m}$ contains $T_k - k - 1$ for primes k not dividing D. Since $r \equiv -1 \pmod{\ell}$ and $\mathfrak{m}$ contains ℓ, $T_r + r + 1 \equiv T_r - r - 1 \pmod{\ell}$ lies in $\mathfrak{m}$. Thus $(\Sigma^\perp/\Sigma)^- = J_0^D(1)[T_r + r + 1]$ contains $J_0^D(1)[\mathfrak{m}]$, i.e., the intersection of r-new subvariety and r-old subvariety has support at $\mathfrak{m}$. This implies that $\mathfrak{m}$ is r-new in $\mathbb{T}_r^D$. By Jacquet-Langlands correspondence, there is a new Eisenstein maximal ideal of type $(s, t+1)$ in $\mathbb{T}_{Dr}$, in other words, a $t+1$-tuple $(p_1, \dots, p_t, r)$ is admissible. □

the case $t = 3$

By combining previous results, we can classify the case $t = 3$ more specifically.

Theorem 5.4.2. *Fix a prime $\ell > 3$ and assume congruence subgroup property holds for Γ_r.*

1. *A triple (p, q, r) is admissible for $s = 3$ if and only if $\ell \mid (p-1)(q-1)(r-1)$.*
2. *A triple (p, q, r) is admissible for $s = 1$ if and only if $q \equiv r \equiv -1 \pmod{\ell}$.*
3. *A triple (p, q, r) is admissible for $s = 0$ is not admissible.*
4. *A triple (p, q, r) is admissible for $s = 2$ only if $r \equiv -1 \pmod{\ell}$.*

5. *A triple (p,q,r) is admissible for $s=2$ if a pair (p,q) is admissible for $s=2$ and $r \equiv -1 \pmod{\ell}$.*

6. *Assume a pair (p,q) is not admissible for $s=2$ and $r \equiv -1 \pmod{\ell}$. Then by shuffling p and q, we can assume $p \not\equiv 1 \pmod{\ell}$. Let $I = (U_p - 1, U_r - r, T_k - k - 1)$ for primes $k \nmid pr$ be an Eisenstein ideal of $\mathbb{T}_{pr}$. A triple (p,q,r) is admissible for $s=2$ if $\eta_q := T_q - q - 1$ is not a local generator of I at $\mathfrak{m} := (\ell, I)$.*

Proof. 1. This is by Theorem 4.1.1.2 and Theorem 4.1.2.1.

2. By Theorem 4.1.1.3, if a triple (p,q,r) is admissible for $s=1$ then $q \equiv r \equiv -1 \pmod{\ell}$.

   Conversely, assume $q \equiv r \equiv -1 \pmod{\ell}$. Then by Theorem 4.2.2.2, a pair (p,q) is admissible for $s=1$. By Theorem 5.4.1, a triple (p,q,r) is admissible for $s=1$ because $r \equiv -1 \pmod{\ell}$.

3. This is by Theorem 4.1.1.1.

4. This is by Theorem 4.1.1.3.

5. This is by Theorem 5.4.1.

6. This is by Theorem 4.4.1.

□

As we have discussed above, admissibility for triples (p,q,r) with $s=2$ is not classified by the explicit congruence. However, in some specific case, we can understand a bit more.

Theorem 5.4.3. *Assume $p \not\equiv 1 \pmod{\ell}$ and $r \equiv -1 \pmod{\ell}$. Moreover assume $r \not\equiv -1 \pmod{\ell^2}$. As before let $I = (U_p - 1, U_r - r, T_k - k - 1)$ for primes $k \nmid pr$ be an Eisenstein ideal of $\mathbb{T}_{pr}$ and $\mathfrak{m} := (\ell, I)$. Then a triple (p,q,r) is admissible for $s=2$ if and only if $\eta_q := T_q - q - 1$ is not a local generator of I at $\mathfrak{m}$.*

Proof. Only thing we have to prove is the following; If η_r is a local generator of I at $\mathfrak{m}$, then a triple (p,q,r) is not admissible. As we discussed before(e.g. Theorem 4.3.1), if $\mathfrak{n} := (\ell, U_p - 1, U_q - 1, U_r + 1, T_k - k - 1)$ is new maximal, it is also q-new. Then $(J_0^{pr}(q)_{q\text{-old}} \cap J_0^{pr}(q)_{q\text{-new}})[\mathfrak{n}] \neq 0$. (Note that $\mathfrak{n}$ is q-old since a pair (p,r) is admissible for $s=1$.) Let Σ be an antidiagonal embedding of the Skorobogatov subgroup of $J_0^{pr}(1)$ in $J_0^{pr}(1) \times J_0^{pr}(1)$. Then

$$J_0^{pr}(q)_{q\text{-old}} \cap J_0^{pr}(q)_{q\text{-new}} = \Sigma^{\perp}/\Sigma.$$

As in the proof of Theorem 4.2.2.3, there is a filtration of $J_0^{pr}(1)[\eta_q]$,

$$0 \subset \Sigma_{\mathfrak{m}} \subset \Sigma_{\mathfrak{m}}^{\perp} \subset J_0^{pr}(1)[\eta_q].$$

Since $\Sigma_{\mathfrak{m}}$ is of dimension one over $\mathbb{T}^{pr}/\mathfrak{m}$ and $J_0^{pr}(1)[\mathfrak{m}]$ is of dimension 2 by Theorem 3.5.1, if η_q is a generator of $I_{\mathfrak{m}} = \mathfrak{m}$, $(\Sigma^{\perp}/\Sigma)_{\mathfrak{m}} = 0$, in other words, $\mathfrak{m}$ is not q-new, which is contradiction. Thus a triple (p,q,r) is not admissible for $s=2$. □

Remark 5.4.4. Even without congruence subgroup property, we can prove that a triple (p, q, r) is not admissible for $s = 2$ if η_q is a local generator of I at $\mathfrak{m}$ if a pair (p, q) is not admissible for $s = 2$. The reason is that Σ, an antidiagonal embedding of the Skorobogatov subgroup, is contained in the kernel K of γ_r. (The conjecture of congruence subgroup property of Γ_r implies that K is not bigger than Σ up to 2, 3 primary factors.) Thus $(K^{\perp}/K)_{\mathfrak{m}} = 0$ by the same reason. This is proof of Theorem 4.4.1.2.

Bibliography

[1] Amod Agashe. *Rational torsion in elliptic curves and the cuspidal subgroup*. `http://www.math.fsu.edu/~agashe/math/tor1.pdf`.

[2] Amod Agashe, Kenneth A.Ribet, and William Stein. "The Manin Constant". In: *Pure and Applied Mathematics Quarterly* Volume 2 (2006), pp. 617–636.

[3] Kenneth A.Ribet. "Eisenstein primes for $J_0(pq)$". June 2008.

[4] Kenneth A.Ribet and William Stein. *Lecture note on Modular forms and Hecke operators*. `http://wstein.org/books/ribet-stein/main.pdf`. 2011.

[5] Jean Bourgain and Alex Gamburd. "Random walks and expansion in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$". In: *Comptes Rendus Mathematique* Vol. 346.Issues 11-12 (2008), pp. 619–623.

[6] Armand Brumer and Kenneth Kramer. *Paramodular abelian varieties of odd conductor*. `http://arxiv.org/pdf/1004.4699v3.pdf`.

[7] Kevin Buzzard. "Integral models of certain Shimura curves". In: *Duke Mathematical Journal* Vol. 87, No. 3 (1997), pp. 591–612.

[8] Frank Calegari and William Stein. *A Non-Gorenstein Eisenstein Descent*. `http://www.wstein.org/home/wstein/www/home/was/days/17/calegari-stein-tor.pdf`. 2008.

[9] Frank Calegari and Akshay Venkatesh. *A torsion Jacquet-Langlands correspondence*. `http://arxiv.org/pdf/1212.3847v1.pdf`.

[10] Seng-Kiat Chua and San Ling. "On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$". In: *Proceedings of the AMS* Vol. 125 (1997), pp. 2255–2263.

[11] Miriam Ciavarella and Lea Terracini. "About an analogue of Ihara's lemma for Shimura curves". In: *Funct. Approx. Comment. Math.* Vol. 5.1 (2011), pp. 23–41.

[12] Henry Darmon, Fred Diamond, and Richard Taylor. *Fermat's Last Theorem*. `http://www.math.mcgill.ca/darmon/pub/Articles/Expository/05.DDT/paper.pdf`.

[13] Pierre Deligne and Micheal Rapoport. "Les schémas de modules de courbes elliptiques". In: *Modular functions of one variable II, Lecture notes in Math.* Vol. 349 (1973), pp. 143–316.

[14] Fred Diamond and Jerry Shurman. *A first course in Modular forms*. Graduate Texts in Mathematics, Vol 228: Springer, 2005.

[15] Fred Diamond and Richard Taylor. "Non-optimal levels of mod ℓ modular representations". In: *Inventiones mathematicae* 115 (1994), pp. 435–462.

[16] Vladimir G. Drinfeld. "Elliptic modules, (Russian)". In: *Math Sbornik* 94 (1974), pp. 594–627.

[17] Bas Edixhoven. "The weight in Serre's conjectures on modular forms". In: *Inventiones mathematicae* 109 (1992), pp. 563–594.

[18] Gerd Faltings and Bruce W. Jordan. "Crystalline cohomology and $\mathrm{GL}(2,\mathbb{Q})$". In: *Israel Journal of Mathematics* 90 (1995), pp. 1–66.

[19] Alexander Grothendieck. "SGA 7 I. Expose IX." In: Lecture Notes in Math., 288: Springer-Verlag, 1972, pp. 313–523.

[20] Jun-Ichi Igusa. "Kroneckerian model of fields of elliptic modular functions". In: *American Journal of Mathematics* 81 (1959), pp. 561–577.

[21] Yasutaka Ihara. "Shimura curves over finite fields and their rational points". In: Curves over finite fields: Contemp. Math. 245, 1999, pp. 15–23.

[22] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of Elliptic curves*. Annals of Math. Studies 108: Princeton Univ. Press, Princeton, 1985.

[23] San Ling and Joseph Oesterlé. "The Shimura subgroup of $J_0(N)$". In: *Astérisque* 196 (1991), pp. 171–203.

[24] Matteo Longo, Victor Rotger, and Stefano Vigni. *Special values of L-functions and the arithmetic of Darmon points*. `http://arxiv.org/pdf/1004.3424v2.pdf`.

[25] Barry Mazur. "Modular curves and Eisenstein Ideals". In: *Publications mathématiques de l'I.H.É.S.* tome.47 (1977).

[26] Andrew Ogg. "Hyperelliptic modular curves". In: *Bull. Soc. Math. France* 102 (1974), pp. 449–462.

[27] Kenneth A. Ribet. "Congruence Relations between Modular Forms". In: *Proceeding of the International Congress of Mathematicians* 1.2 (1984), pp. 503–514.

[28] Kenneth A. Ribet. "Galois action on division points of Abelian varieties with real multiplications". In: *American Journal of mathematics* 98.3 (1976), pp. 751–804.

[29] Kenneth A. Ribet. "On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms". In: *Inventiones mathematicae* 100 (1990), pp. 431–476.

[30] Kenneth A. Ribet. "On the component groups and the Shimura subgroup of $J_0(N)$". In: *Séminaire de Thérie des Nombres de Bordeaux* 16 (1984), pp. 1–10.

[31] Kenneth A. Ribet. "The old subvariety of $J_0(pq)$". In: *Arithmetic algebraic geometry(Texel)* 89 (1989), pp. 293–307.

[32] Carl Riehm. "The norm 1 group of a $\wp$-adic division algebra". In: *American Journal of mathematics* 92.2 (1970), pp. 499–523.

[33] Jean-Pierre Serre. "Congruences et formes modulaires". In: *Séminaire Bourbaki, 24e année* Exp. No. 416 (1973), pp. 319–338.

[34] Alexei Skorobogatov. "Shimura coverings of Shimura curves and the Manin obstruction". In: *Mathematical Research Letter* 12 (2005), pp. 779–788.

[35] H.P.F. Swinnerton-Dyer. "On ℓ-adic representations and congruences for coefficients of modular forms". In: *Modular functions of one variable III, Lecture notes in Math.* Vol. 350 (1973), pp. 1–55.

[36] Jacques Tilouine. "Hecke algebras and the Gorenstein property". In: Modular forms and Fermat's last theorem(Boston, MA, 1995): Springer, New York, 1997, pp. 327–342.

[37] Vinayak Vatsal. "Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves". In: *Journal of the Institute of Mathematics of Jussieu* Vol. 4 (2005), pp. 281–316.

[38] Marie-France Vigneras. *Arithmétique des algèbres de quaternions.* Lecture Notes in Math., 800: Springer-Verlag, 1980.