SERRE'S CONJECTURE OVER IMAGINARY QUADRATIC FIELDS

By

Mehmet Haluk Şengün

A dissertation submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2008

Abstract

The connection between classical modular forms and continuous representations of the absolute Galois group of the field of rational numbers has been the focus of major research in the last thirty years. In this thesis, we investigate a similar connection over the imaginary quadratic fields. We prove a weight reduction theorem for mod p modular forms and we prove the nonexistence of absolutely irreducible level 1 mod p Galois representations of small quadratic fields for $p = 2, 3$. We list certain conjectures, including an analogue of Serre's Conjecture. We present algorithms to compute the modular forms and the Hecke action on them. Implementing the algorithms in MAGMA, we produce numerical evidence to support some of these conjectures.

Acknowledgements

I would like to start with my parents Songül and Halil Ibrahim. Without their selfless efforts on behalf of my happiness and my education, I would not be where I am today. My sisters Elif and Gülşah have always loved and supported me without boundaries. Ali Riza Abi has been a real brother to me rather than a brother-in-law. And Rosamaria Cisneros Kostic (a.k.a. Muni Muni) has been my family in the USA for the last two years. I thank my family with all my heart.

I owe so much to the mathematics family at the Bilgi University and my teacher Ali Nesin. I can only repay him for his selfless devotion to our education as mathematicians and human beings by paying it forward to future generations.

I am grateful to my adviser Nigel Boston for his support and his mentoring. He is great at tailoring his support according to the needs and characters of his students. This is why I felt very happy with him as my adviser. I will miss his humor.

I consider Fritz Grunewald as my second adviser. Without his patronage, this thesis would not exist. Over the last two years, I visited him four times, mostly with the financial help of the grant DFG-Graduiertenkolleg 1150 (Homotopy and Cohomology). I will be forever grateful for all he has done for me. I also thank Daniel Appel, Jürgen Klüners, Bertold Nöckel and Saeid Zarghani for making me feel at home at the Heinrich Heine University of Düsseldorf.

Another key figure for my research is Gabor Wiese. Every time I visited him at the University of Duisburg-Essen, I learned something new. I am thankful for his continuing support and friendship.

Seyfi Turkelli is one my best friends and our mathematical discussions and collaborations taught me a lot. I feel lucky to have such a friend. Together with Ekin Özman, they covered all my teaching duties every time I visited Germany. I am grateful to both.

I thank Yuichiro Taguchi for our discussions on the contents of Chapter 7. His crucial comments and corrections gave its final look to the chapter.

I am grateful to Avner Ash. He devoted his whole day to me when I visited him in Boston and he was a wonderful host. His work has been a guide to my research.

I also thank Farshid Hajir and Paul Gunnells for hosting me and discussing my work with me. I owe a lot to Paul Gunnells' expository articles on the cohomology of arithmetic groups.

I thank the mathematics community at the University of Wisconsin at Madison. I am grateful to Ken Ono for the support he gave me every time I approached him. Jordan Ellenberg's energy was inspiring. I thank him for sharing his insights with me.

Finally I thank all my friends in Madison. I felt at home here.

Dedication

çok sevgili annem Songül ve babam Halil Ibrahim'e ...

List of Tables

Contents

Chapter 1

Outline

A celebrated conjecture (now a theorem of Khare et al.) of Jean-Pierre Serre connects certain 2-dimensional continuous representations of the Galois group of $\mathbb{Q}$ into $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ (these are called Galois representations) with certain classical modular forms of the hyperbolic plane. In this thesis, we investigate an analogue connection between certain 2-dimensional continuous representations of the Galois group of imaginary quadratic number fields into $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ and certain automorphic forms living on the hyperbolic 3-space (called Bianchi modular forms).

In Chapter 2 we summarize the facts about discrete subgroups of $\mathbf{SL}_2(\mathbb{C})$ and their action on the hyperbolic 3-space $\mathbb{H}$. We talk about Bianchi groups $\mathbf{SL}_2(\mathcal{O}_K)$,where $\mathcal{O}_K$ is the ring of integers of an imaginary quadratic field, and define the Bianchi modular forms as classes in the cohomology of Bianchi groups. We discuss the Hecke algebra acting on this cohomology. We end the chapter with a discussion of Galois representations.

In Chapter 3 we give an overview of the classical situation that motivated our research. We discuss the classical modular forms and Serre's conjecture. Then we turn to imaginary quadratic fields and list four conjectures, well known to experts, regarding Galois representations of imaginary quadratic fields and Bianchi modular forms.

In Chapter 4 we present the statements of our theoretical results and we discuss their relevance to the conjectures we listed.

In Chapter 5 we present the numerical results that we gathered using the algorithms and programs that we developed to compute Bianchi modular forms. The numerical data, together with our theoretical results, provide supporting evidence for some of the conjectures that we listed.

In Chapters 6 and 7 we present the proofs of our theoretical results.

In Chapter 8 we explain our algorithm that we used to compute the Bianchi modular forms and the Hecke action on them.

Chapter 2

Background

2.1 The Hyperbolic 3-Space

In this section, we will discuss the the hyperbolic 3-space and the action of $\mathbf{SL}_2(\mathbb{C})$ on it. We refer the readers to the books by Elstrodt-Grunewald-Mennicke [17], Bearden [4], and Maclahlan-Reid [32] for proofs.

Three-dimensional hyperbolic space is the unique 3-dimensional connected and simply connnected Riemanninan manifold with constant sectional curvature equal to -1. Let $\mathbb{H}$ be the upper half-space of the three dimensional Euclidean space.

$$\begin{aligned}\mathbb{H} &:= \mathbb{C} \times \mathbb{R}^+ \\ &= \{(z, r) \mid z \in \mathbb{C},\ r \in \mathbb{R},\ r > 0\} \\ &= \{(x, y, r) \mid x, y, r \in \mathbb{R},\ r > 0\}\end{aligned}$$

We endow $\mathbb{H}$ with the hyperbolic metric d coming from the line element ds defined by

$$ds^2 = \frac{dx^2 + dy^2 + dr^2}{r^2}$$

and $\mathbb{H}$ becomes a model for the hyperbolic 3-space. With the metric d, the geodesics in $\mathbb{H}$ are half circles or half lines which are orthogonal to the boundary plane $\mathbb{C}$ in the Euclidean sense.

The group $\mathbf{SL}_2(\mathbb{C})$ of 2×2 complex matrices with determinant one act on $\mathbb{H}$. For $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathbf{SL}_2(\mathbb{C})$ and $(z, r) \in \mathbb{H}$, the action is given by $M \cdot (z, r) := (z^*, r^*)$ where

$$z^* = \frac{(az + b)(\bar{c}\bar{z} + \bar{d}) + a\bar{c}r^2}{|cz + d|^2 + |c|^2 r^2},$$

$$r^* = \frac{r}{|cz + d|^2 + |c|^2 r^2}.$$

This action can be given in a more compact way once quaternions are used to represent points in $\mathbb{H}$. Let $1, i, j, k$ be the standart $\mathbb{R}$-basis for Hamilton's quaternions $\mathcal{H}$. We regard $\mathbb{H}$ as a subset of $\mathcal{H}$ via $(z, r) \mapsto z + rj$. Then the action of $\mathbf{SL}_2(\mathbb{C})$ on a point $p = z + rj$ can be described as

$$M \cdot p = \frac{ap + b}{cp + d}.$$

The action can be extended to the boundary $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. If $(x : y)$ is an element of $\mathbb{P}^1(\mathbb{C})$, then

$$M \cdot (x : y) = (ax + by : cx + dy).$$

The action of $\mathbf{SL}_2(\mathbb{C})$ on $\mathbb{H}$ is doubly transitive (any pair of elements can be sent to any pair of elements) and the stabilizer of the point $j = (0, 0, 1) \in \mathbb{H}$ inside $\mathbf{SL}_2(\mathbb{C})$ is $\mathbf{SU}(2)$. This implies that, with the fact that $-I_2$ acts trivially on $\mathbb{H}$,

$$\mathbf{SL}_2(\mathbb{C})/\mathbf{SU}(2) \simeq \mathbf{PSL}_2(\mathbb{C})/\mathbf{PSU}(2) \simeq \mathbb{H}$$

In the language of Lie groups, this means that the global symmetric space of the groups $\mathbf{SL}_2$ and $\mathbf{PSL}_2$ is $\mathbb{H}$. We will discuss the situation from the perspective of automorphic forms in a later section.

We end this section by noting that $\mathbf{PSL}_2(\mathbb{C})$ is isomorphic to the group $\mathbf{Iso}^+(\mathbb{H})$ of orientation preserving isometries of $\mathbb{H}$.

2.2 Discrete Subgroups of $\mathbf{PSL}_2(\mathbb{C})$

We consider the topology on $\mathbf{SL}_2(\mathbb{C})$ that is given by the following norm

$$||M|| = \sqrt{|a|^2 + |b|^2 + |c|^2 + |d|^2}$$

for $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. A subgroup Γ of $\mathbf{PSL}_2(\mathbb{C})$ is *discrete* if its inverse image in $\mathbf{SL}_2(\mathbb{C}) \subset$ is discrete. Discrete subgroups of $\mathbf{PSL}_2(\mathbb{C})$ are also known as *Kleinian groups*.

A subgroup $\Gamma < \mathbf{Iso}^+(\mathbb{H})$ is called *discontinuous* if for every compact subset $K \subset \mathbb{H}$ we have $g \cdot K \cap K = \emptyset$ for all but finitely many $g \in \Gamma$. The following is a result of Poincare.

Theorem 2.1. *A subgroup $\Gamma < \mathbf{PSL}_2(\mathbb{C})$ is discrete if and only if it is discontinuous.*

It follows from that for a point $P \in \mathbb{H}$, its stabilizer subgroup $\Gamma_P < \Gamma$ is finite if Γ is discrete. The classification of finite subgroups of $\mathbf{PSL}_2(\mathbb{C})$ tells us that Γ_P will be cyclic, dihedral, isomorphic to the alternating groups $\mathbf{A_4}, \mathbf{A_5}$ or the symmetric group $\mathbf{S_4}$.

For the point ∞ of $\mathbb{P}^1(\mathbb{C})$, its stabilizer $\mathbf{PSL}_2(\mathbb{C})_\infty$ in $\mathbf{PSL}_2(\mathbb{C})$ is equal to the group

$$B(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; 0 \neq a, b \in \mathbb{C} \right\} / \{\pm I\}$$

which is a Borel subgroup. Given an element $\zeta \in \mathbb{P}^1(\mathbb{C})$ and a subgroup $\Gamma < \mathbf{PSL}_2(\mathbb{C})$ then we have

$$\Gamma_\zeta = \Gamma \cap M^{-1} B(\mathbb{C}) M$$

where $M \in \mathbf{PSL}_2(\mathbb{C})$ is such that $M\zeta = \infty$.

A closed subset $\mathcal{F} \subset \mathbb{H}$ is called a *fundamental domain for* $\Gamma < \mathbf{Iso}(\mathbb{H})$ if the followings are satisfied:

(1) $\mathcal{F}$ meets each Γ-orbit at least once,

(2) the interior of $\mathcal{F}$ meets each Γ-orbit at most once,

(3) the boundary of $\mathcal{F}$ has Lebesgue measure zero.

If Γ is discontinuous, then a fundamental domain $\mathcal{F}$ exists. We say that Γ is of *finite covolume* or *cofinite* if

$$\mathrm{vol}(\Gamma) = \int_{\mathcal{F}} dv < \infty$$

where $dv = \dfrac{dxdydr}{r^3}$ is the hyperbolic volume element. The covolume $\mathrm{vol}(\Gamma)$ is independent of the fundamental domain chosen. If Γ has a compact fundamental domain, then Γ is called *cocompact*.

If $\Gamma < \mathbf{PSL}_2(\mathbb{C})$ is a discrete group which acts (fixed point) freely on $\mathbb{H}$ then the quotient space $\Gamma\backslash\mathbb{H}$ inherits the structure of an orientable hyperbolic 3-manifold. Conversely, the universal cover of an orientable hyperbolic 3-manifold M will be isometric to $\mathbb{H}$ and thus the fundamental group of M will be a covering group $\Gamma < \mathbf{PSL}_2(\mathbb{C})$ that acts freely and is discrete.

Theorem 2.2. *If M is an orientable hyperbolic 3-manifold, then M is isometric to $\Gamma\backslash\mathbb{H}$ for some torsion-free discrete subgroup of $\mathbf{PSL}_2(\mathbb{C})$.*

It can be seen that Γ is cocompact if and only if $\Gamma\backslash\mathbb{H}$ is compact. Moreover, Γ is cofinite if and only if $\Gamma\backslash\mathbb{H}$ is of finite volume. This explains the prefix "co" in the above definitions.

The notion of a cusp is important for the sequel. An element $\zeta \in \mathbb{P}^1(\mathbb{C})$ is called a *cusp* of a discrete group $\Gamma < \mathbf{PSL}_2(\mathbb{C})$ if its stabilizer Γ_ζ contains a free abelian group of rank 2. We denote the set of cusps of Γ with C_Γ.

The following result provides a connection with algebraic number theory.

Theorem 2.3. *Let Γ be a discrete subgroup of $\mathbf{PSL}_2(\mathbb{C})$ which is cofinite. Then the field $\mathbb{Q}(\mathrm{tr}\Gamma)$ is a finite extension of $\mathbb{Q}$.*

Here $\mathbb{Q}(\mathrm{tr}\Gamma)$ is the field created by adjoining the traces of all preimages in $\mathbf{SL}_2(\mathbb{C})$ of elements of Γ.

2.3 Bianchi Groups

Let $d > 0$ be a square-free integer and let $\mathcal{O}_d$ denote the ring of integers of the imaginary quadratic number field $K_d = \mathbb{Q}(\sqrt{-d})$. We will drop the d when we discuss situations that cover all d's. The groups $\mathbf{PSL}_2(\mathcal{O}_d)$ are called *Bianchi groups*. Since $\mathcal{O}_d$ is discrete in $\mathbb{C}$, Bianchi groups are discrete subgroups of $\mathbf{PSL}_2(\mathbb{C})$. Using a specific fundamental domain constructed by Bianchi, one sees that Bianchi groups are cofinite but are not cocompact.

Theorem 2.4. *Every discrete subgroup of $\mathbf{PSL}_2(\mathbb{C})$ that is not cocompact is commensurable with a conjugate of some Bianchi group.*

We first discuss the properties of cusps which is a first indicator of the strong connections with arithmetic.

Proposition 2.5. *Let $\Gamma < \mathbf{PSL}_2(\mathbb{C})$ be commensurable with a Bianchi group $\mathbf{PSL}_2(\mathcal{O}_d)$, then the set of cusps $C_\Gamma = \mathbb{P}^1(K_d) \subset \mathbb{P}^1(\mathbb{C})$.*

Theorem 2.6. *The "number of cusps" of* $\mathbf{PSL}_2(\mathcal{O}_d)$ *(that is, the number of* $\mathbf{PSL}_2(\mathcal{O}_d)$*-orbits in* $\mathbb{P}^1(K_d)$*) is equal to the class number of* K_d*.*

It is effectively possible to write down a presentation for $\mathbf{PSL}_2(\mathcal{O}_d)$ from a fundamental domain. This was carried out by Bianchi, Humbert and Swan [53]. In this thesis, we will focus on the Euclidean imaginary quadratic fields K_1 and K_2. We note the following presentations that Flöge [19] produced using a 2-dimensional $\mathbf{PSL}_2(\mathcal{O})$-equivariant deformation retract of $\mathbb{H}$ that is due to Mendoza [33].

$$\mathbf{PSL}_2(\mathcal{O}_1) = \left\langle A, B, U \;\middle|\; \begin{array}{c} (AB)^3 = B^2 = AUA^{-1}U^{-1} = (BUBU^{-1})^3 = \\ (BU^2BU^{-1})^2 = (AUBAU^{-1}B)^2 = 1 \end{array} \right\rangle$$

where $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $U = \left(\begin{smallmatrix} 1 & 0 \\ i & 1 \end{smallmatrix}\right)$. Here we represent elements of $\mathbf{PSL}(\mathbb{C})$ with preimages from $\mathbf{SL}_2(\mathbb{C})$.

$$\mathbf{PSL}_2(\mathcal{O}_2) = \left\langle A, B, U \;\middle|\; (AB)^3 = B^2 = AUA^{-1}U^{-1} = (BU^2BU^{-1})^2 = 1 \right\rangle$$

where $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $U = \left(\begin{smallmatrix} 1 & 0 \\ \sqrt{-2} & 1 \end{smallmatrix}\right)$.

We now define the congruence subgroups. Given an ideal $\mathfrak{a} \subset \mathcal{O}$, the principal congruence subgroup of level $\mathfrak{a}$ is defined by

$$\Gamma(\mathfrak{a}) = \left\{ M \in \mathbf{PSL}_2(\mathcal{O}) \;\middle|\; M \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \mod \mathfrak{a} \right\}$$

A subgroup of $\mathbf{PSL}_2(\mathcal{O})$ is a *congruence subgroup* if it is contains $\Gamma(\mathfrak{a})$ for some $\mathfrak{a} \trianglelefteq \mathcal{O}$, otherwise it is a *noncongruence subgroup*. It is a well known theorem by Bass-Milnor-Serre that Bianchi groups have many noncongruence subgroups.

We end this section with a group theoretic description of $\mathbf{PSL}_2(\mathcal{O}_1)$ which is again derived from an explicit fundamental domain. Note the similarity with the fact that $\mathbf{PSL}_2(\mathbb{Z}) \simeq C_2 \star C_3$.

$$\mathbf{PSL}_2(\mathcal{O}_1) \simeq ((C_2 \times C_2) \star_{C_2} \mathbf{S_3}) \star_{(C_2 \star C_3)} (\mathbf{A_4} \star_{C_3} \mathbf{S_3})$$

where C_n is the cyclic group of order n.

2.4 Cohomology and Hecke Action

In this section we will work with $\mathbf{SL}_2$ instead of $\mathbf{PSL}_2$ for convenience. For convenience, we assume that K has class number one. This allows us to associate Hecke operators with generators of the ideals instead of the ideals themselves. We start by constructing the Hecke operators explicitly on the first cohomology group with arbitrary coefficient modules. Next, we describe the specific coefficient modules that we need.

2.4.1 Hecke Operators

Let R be a commutative ring with 1 and $\alpha = \left(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}\right)$ where π is a prime element of $\mathcal{O}$. Let $\Gamma \leq \mathrm{SL}_2(\mathcal{O})$ be a congruence subgroup of level $\mathfrak{a}$. We follow the standart notations and put $\Gamma_\alpha := \Gamma \cap \alpha^{-1}\Gamma\alpha$ and $\Gamma^\alpha := \Gamma \cap \alpha\Gamma\alpha^{-1}$.

Let V be a right $R[\mathrm{Mat}_2(\mathcal{O})_{\neq 0}]$-module where $\mathrm{Mat}_2(\mathcal{O})_{\neq 0}$ is the semi-group of 2×2 matrices of non-zero determinant with entries in $\mathcal{O}$. We define the Hecke operator T_π

on the cohomology as the composition

$$\begin{array}{ccc} H^m(\Gamma, V) & & H^m(\Gamma, V) \\ \Big\downarrow{\scriptstyle res} & & \Big\uparrow{\scriptstyle cores} \\ H^m(\Gamma_\alpha, V) & \xrightarrow{\hat{\alpha}} & H^m(\Gamma^\alpha, V) \end{array}$$

where the map $\hat{\alpha}$ is defined by

$$c \mapsto (g \mapsto c(\alpha^{-1} g \alpha) \cdot \alpha^\iota)$$

where c is a cocycle in $H^m(\Gamma_\alpha, V)$ and $\alpha^\iota = \det(\alpha)\alpha^{-1}$.

One can describe Hecke operator T_π explicitly: suppose $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{m} \gamma_i \Gamma$. Given $g \in \Gamma$ and γ_i, there is a unique $\gamma_{j(i)}$ such that $\gamma_{j(i)}^{-1} g \gamma_i \in \Gamma$. Then

$$(T_\pi c)(g) = \sum_{1 \le i \le m} c(\gamma_{j(i)}^{-1} g \gamma_i) \cdot \gamma_i^\iota$$

for all cocycles c in $H^m(\Gamma, V)$ and $g \in \Gamma$. We note that this formula agrees with the one given in [2, p.194].

For $(\pi, \mathfrak{a}) = 1$, going through the same construction with the matrix $\beta = \left(\begin{smallmatrix} \pi & 0 \\ 0 & \pi \end{smallmatrix}\right)$ instead of $\alpha = \left(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we get the Hecke operators S_π.

We define the *Hecke algebra* $\mathbf{H}$ as the (commutative) $\mathbb{Z}$-algebra generated by the T_π's and S_π's.

2.4.2 Shapiro's Lemma

For an ideal $\mathfrak{a}$ of $\mathcal{O}$, set

$$\Delta_1(\mathfrak{a}) := \{M \in \mathrm{Mat}_2(\mathcal{O})_{\neq 0} : M \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \mod \mathfrak{a}\}$$

We define the induced module $Ind(V) = Ind(\Gamma_1(\mathfrak{a}), \Gamma_1(\mathfrak{ab}), V)$ as the set of $\Gamma_1(\mathfrak{ab})$-invariant maps from $\Gamma_1(\mathfrak{a})$ to V, that is

$$Ind(V) = \{f : \Gamma_1(\mathfrak{a}) \to V \mid f(gh) = f(g) \cdot h \text{ for all } h \in \Gamma_1(\mathfrak{ab})\}.$$

Then $Ind(V)$ is a right $\Gamma_1(\mathfrak{a})$-module with the action $(f \cdot y)(x) = f(yx)$ for $x, y \in \Gamma_1(\mathfrak{a})$ and $f \in Ind(V)$.

We can extend the $\Gamma_1(\mathfrak{a})$-action on $Ind(V)$ to a right $\Delta_1(\mathfrak{a})$-action in the following way. Let $\alpha \in \Delta_1(\mathfrak{a})$ and $f \in Ind(V)$ and $x \in \Gamma_1(\mathfrak{a})$, then there are $\beta \in \Delta_1(\mathfrak{ab})$ and $y \in \Gamma_1(\mathfrak{a})$ such that $\alpha x = y\beta$ where $\Delta_1(\mathfrak{ab})$. We define

$$(f \cdot \alpha)(x) = f(y) \cdot \beta.$$

Shapiro's Lemma asserts that there is an isomorphism

$$\theta : H^m(\Gamma_1(\mathfrak{a}), Ind(V)) \to H^m(\Gamma_1(\mathfrak{ab}), V)$$

given by $f \mapsto f(I)$ for every non-homogeneous cocycle f in $H^m(\Gamma, Ind(V))$ where I denotes the identity matrix. The fact that the Hecke operators commute with the Shapiro isomorphism θ was proved in a more general setting in [2]. See also [57] for a proof in the case of $\mathrm{PSL}_2(\mathbb{Z})$ using the same construction as ours for the Hecke operators.

Proposition 2.7. *The Hecke operators commute with the Shapiro map θ.*

2.4.3 Eigenvalue Systems

A *system of eigenvalues* of $\mathbf{H}$ with values in a ring R is a set-theoretic a map $\Phi : \mathbf{H} \to R$. We say that an eigenvalue system Φ occurs in the $R\mathbf{H}$-module A if there is a nonzero element $a \in A$ such that $Ta = \Phi(T)a$ for all T in $\mathbf{H}$.

The following lemma is proved in [2, Lemma 2.1].

Lemma 2.8. *Let F be a field and V be a $F\Delta_1(\mathfrak{a})$-module which is finite dimensional over F. If an eigenvalue system $\Phi : \mathbb{H} \to F$ occurs in $H^n(\Gamma_1(\mathfrak{a}), V)$, then Φ occurs in $H^n(\Gamma_1(\mathfrak{a}), W)$ for some irreducible $F\Delta_1(\mathfrak{a})$-subquotient W of V.*

Thus it is enough to investigate the cohomology with irreducible coefficient modules if we are only interested in the eigenvalue systems.

2.4.4 The Coefficient Modules

In this section, we describe certain modules that we will use as the coefficient modules in the cohomology of Bianchi groups in the next section.

For a commutative ring R with 1, let $E_k(R)$ denote the homogeneous polynomials of degree k in two variables with coefficients in R. The set $\{X^{k-i}Y^i : 0 \leq i \leq k\}$ is an R-basis of $E_k(R)$.

We can give $E_k(\mathbb{C})$ a right $\mathbf{SL}_2(\mathcal{O})$-module structure as follows. For a polynomial $P(X,Y)$ in $E_k(K)$ and a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathbf{SL}_2(\mathcal{O})$, we set

$$\big(P \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\big)\big(X,Y\big) = P\big(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)\big) = P\big(aX + bY, cX + dY\big).$$

When λ is a prime ideal of $\mathcal{O}$, we may view $E_k(\mathbb{F}_\lambda)$, where $\mathbb{F}_\lambda$ is the residue field of λ, as an $\mathbf{SL}_2(\mathcal{O})$ module via the above formula by reducing each entry of the matrix modulo λ.

A result of Steinberg [52] says that the irreducible representations of $\mathbf{SL}_2(K)$ over $\mathbb{C}$ are of the form

$$E_{k,l}(\mathbb{C}) := E_k(\mathbb{C}) \otimes \overline{E}_l(\mathbb{C})$$

with $k, l \geq 0$ integers where the bar on the second module means that the action is

twisted with complex conjugation. Note that $-I$ acts trivially when $k+l$ is even, thus in this case the action factors through $\mathbf{PSL}_2(\mathcal{O})$.

Let ℓ be a rational prime which splits as $\lambda\bar{\lambda}$ in the ring of integers $\mathcal{O}$ of K. Note that then the residue fields of both λ and $\bar{\lambda}$ are isomorphic to $\mathbb{F}_\ell$. In this project, we are interested in the (absolutely) irreducible representations of $\mathbf{SL}_2(\mathcal{O}/(\ell)) = \mathbf{SL}_2(\mathcal{O}/\lambda) \times \mathbf{SL}_2(\mathcal{O}/\bar{\lambda})$ over $\mathbb{F}_\ell$. Results of Steinberg [52] and Brauer-Nesbitt [8] show that these are of the form

$$E_{k,l}(\mathbb{F}_\ell) := E_k(\mathbb{F}_\ell) \otimes \overline{E}_l(\mathbb{F}_\ell) \qquad 0 \leq k, l \leq \ell.$$

Here, $\mathbf{SL}_2(\mathcal{O})$ acts on the first module through reduction by λ and on the second through reduction by $\bar{\lambda}$. Note that $-I$ acts trivially when $k+l$ is even, thus in this case the action factors through $\mathbf{PSL}_2(\mathcal{O})$.

2.5 Bianchi Modular Forms

In this section, we discuss the automorphic forms on $\mathbb{H}$ that are of cohomological type.

Let K be an imaginary quadratic field of class number 1 and let $\mathcal{O}$ be its ring of integers. Let $\mathbf{G} = \mathrm{Res}_{K/\mathbb{Q}}(\mathbf{SL}_2)$ be the algebraic group over $\mathbb{Q}$ that is obtained from $\mathbf{SL}_2$ by restriction the scalars from K to $\mathbb{Q}$, see Platonov and Rapunchik [40][pg.49].

The group of real points $\mathbf{G}(\mathbb{R}) = \mathbf{SL}_2(K \otimes_{\mathbb{Q}} \mathbb{R}) = \mathbf{SL}_2(\mathbb{C})$ of $\mathbf{G}$ acts transitively on $\mathbb{H}$ as we have discussed in Section 2.1. The stabilizer $\mathbf{SU}(2)$ of $j = (0,0,1) \in \mathbb{H}$ is a maximal compact subgroup of $\mathbf{SL}_2(\mathbb{C})$. Thus the global symmetric space $\mathbf{SL}_2(\mathbb{C})/\mathbf{SU}(2)$ of $\mathbf{G}$ can be identified with $\mathbb{H}$ via the map $M \mapsto M \cdot j$.

Let Γ be a torsion-free subgroup of $\mathbf{G}(\mathbb{Z}) = \mathbf{SL}_2(\mathcal{O})$. Then the quotient $\Gamma\backslash\mathbb{H}$ is a smooth 3-manifold which is noncompact but is of finite volume. Since $\mathbb{H}$ is contractible,

$\Gamma\backslash\mathbb{H}$ is an Eilenberg-Mac Lane space for Γ. That is, $\pi_1(\Gamma\backslash\mathbb{H}) \simeq \Gamma$ and higher homotopy groups vanish. Let E be a Γ-module and let $\tilde{E}$ be the local system of coefficients induced from E. These can be defined as the bundle $\mathbb{H} \times_\Gamma E$ with discrete structure group Γ. We have

$$H^m(\Gamma, E) \simeq H^m(\Gamma\backslash\mathbb{H}; \tilde{E})$$

for all $m \in \mathbb{N}$.

In [20], Franke proves the Borel Conjecture [6] which says that the cohomology group $H^m(\Gamma, E)$ can be directly computed in terms of certain automorphic forms. Moreover, he obtains a direct sum decomposition

$$H^m(\Gamma, E) = H^m_{\text{cusp}}(\Gamma, E) \oplus H^m_{\text{Eis}}(\Gamma, E)$$

where the first summand is called the *cuspidal cohomology* and it is represented by cuspidal automorphic forms. The second summand is called the *Eisenstein cohomology* and it is constructed using Eisenstein series attached to certain cuspidal automorphic forms on lower rank groups.

The most well known example of the above decomposition is given by the theorem of Eichler and Shimura (see Theorem 3.3).

Due to Borel and Serre [7], there is a compactification $\overline{\Gamma\backslash\mathbb{H}}$ with boundary such that the inclusion $\Gamma\backslash\mathbb{H} \hookrightarrow \overline{\Gamma\backslash\mathbb{H}}$ is a homotopy equivalence. Thus after a suitable extension of the sheaf $\tilde{E}$, we have $H^m(\Gamma\backslash\mathbb{H}; \tilde{E}) = H^m(\overline{\Gamma\backslash\mathbb{H}}; \tilde{E})$.

Let $\delta(\overline{\Gamma\backslash\mathbb{H}})$ denote the boundary of $\overline{\Gamma\backslash\mathbb{H}}$. Then Harder [22, 23] shows that the kernel of the restriction map

$$H^m(\overline{\Gamma\backslash\mathbb{H}}, \tilde{E}) \longrightarrow H^m(\delta(\overline{\Gamma\backslash\mathbb{H}}), \tilde{E})$$

can be identified with the cuspidal cohomology $H^m_{\text{cusp}}(\Gamma, E)$ and the image of this map

can be identified with the Eisenstein cohomology $H^m_{\text{Eis}}(\Gamma, E)$. The cuspidal cohomology can also be algebraically described as the kernel of the restriction map in

$$0 \longrightarrow H^m_{\text{cusp}}(\Gamma, E) \longrightarrow H^m(\Gamma, E) \xrightarrow{res} \prod_{h \in C_\Gamma} H^m(\Gamma \cap \Gamma_h, E). \tag{2.1}$$

Recall that C_Γ is the set of cusps of Γ and Γ_h is the stabilizer of $h \in \mathbb{H}$ inside $\mathbf{SL}_2(\mathcal{O})$.

We note that the virtual cohomological dimension of $\mathbf{SL}_2(\mathcal{O})$ is 2, see Serre [45]. Thus for torsion-free Γ, $H^m(\Gamma, E) = \{0\}$ for all $m > 2$.

We summarize from [55] what is known about the nature of the first two cohomology groups. Recall the definition of the irreducible $\mathbf{SL}_2(K)$-modules $E_{k,l}(\mathbb{C})$ from Section 2.4.4.

- $H^m_{\text{cusp}}(\Gamma, E_{k,l}(\mathbb{C})) = \{0\}$, unless $k = l$ for $m = 1, 2$.
- $H^1_{\text{cusp}}(\Gamma, E_{k,l}(\mathbb{C})) \simeq H^2_{\text{cusp}}(\Gamma, E_{k,l}(\mathbb{C}))$
- $\dim\ H^1_{\text{Eis}}(\Gamma, E_{k,l}(\mathbb{C})) = \frac{1}{2} \dim\ H^1(\delta(\overline{\Gamma\backslash\mathbb{H}}), \tilde{E}_{k,l}(\mathbb{C}))$
- $H^2_{\text{Eis}}(\Gamma, E_{k,l}(\mathbb{C})) \simeq H^2(\delta(\overline{\Gamma\backslash\mathbb{H}}), \tilde{E}_{k,l}(\mathbb{C}))$ unless $k = l = 0$

We have seen that the cohomology groups $H^1(\Gamma, E)$ and $H^2(\Gamma, E)$ can be identified with certain automorphic forms. These automorphic forms (also known as automorphic forms of cohomological type) are what we want to call Bianchi modular forms. But as their cohomological identification is what we are going to use for computational purposes, we go ahead and call the cohomology classes themselves "Bianchi modular forms". The cuspidal automorphic forms are very important for us and the cuspidal part of H^1 and H^2 are isomorphic. So we solely focus on the first cohomology.

For an ideal $\mathfrak{a}$ of $\mathcal{O}$, we define

$$\Gamma_0(\mathfrak{a}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}) : c \equiv 0 \mod \mathfrak{a} \right\}$$

and

$$\Gamma_1(\mathfrak{a}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}) : c \equiv d-1 \equiv 0 \mod \mathfrak{a} \right\}$$

Definition 2.9. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$.*

- *A Bianchi modular form of level $\mathfrak{a}$ and weight (k,l) is a cohomology class in $H^1(\Gamma_1(\mathfrak{a}), E_{k,l}(\mathbb{C}))$. It is cuspidal if it is in the cuspidal part $H^1_{cusp}(\Gamma_1(\mathfrak{a}), E_{k,l}(\mathbb{C}))$.*
- *Similarly, we define a mod ℓ Bianchi modular form of level $\mathfrak{a}$ and weight (k,l) as a cohomology class in $H^1(\Gamma_1(\mathfrak{a}), E_{k,l}(\overline{\mathbb{F}}_\ell))$. It is cuspidal, if it is in the cuspidal part that is given algebraically by the exact sequence (2.1).*

2.6 Galois Representations

Let K be a number field and $\overline{K}$ an algebraic closure. Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be its *absolute Galois group*. We equip G_K with the profinite topology:

$$G_K = \varprojlim \mathrm{Gal}(L/K)$$

where the limit is taken over finite Galois extensions L/K.

For every finite place λ in K, we will distinguish subgroups

$$I_\lambda \leq D_\lambda \leq G_K$$

Also we will specify a class of elements $Frob_\lambda$ which give important information for almost all λ.

Let K_λ be the completion of K at a finite place λ. Fix an embedding $\overline{K} \hookrightarrow \overline{K}_\lambda$. This gives rise to an embedding $G_{K_\lambda} \hookrightarrow G_K$. We call the image of G_{K_λ} inside G_K the *decomposition subgroup* of G_K at λ. Note that a different embedding $\overline{K} \hookrightarrow \overline{K}_\lambda$ conjugates the decomposition subgroup by an element of G_K.

There is a reduction map $\pi : G_{K_\lambda} \to G_{\mathbb{F}_q}$ where $\mathbb{F}_q$ is the residue field of K_λ. This gives an exact sequence

$$1 \to I_\lambda \to G_{K_\lambda} \to G_{\mathbb{F}_q} \to 1$$

The kernel I_λ is called the *inertia subgroup* of G_K at λ.

A Frobenius element Frob_λ of G_K is a preimage of the automorphism $x \mapsto x^q$ under π. We note that this automorphism topologically generates $G_{\mathbb{F}_q}$.

An n-dimensional *Galois representation* ρ of K over a topological field F is a continuous homomorphism

$$\rho : G_K \to \mathrm{GL}_n(F)$$

If F is a field of char. ℓ , we call ρ a *mod* ℓ Galois representation of K. If F is an extension of the field $\mathbb{Q}_\ell$ of ℓ-adic numbers then ρ is called ℓ-*adic*.

A Galois representation ρ of K is said to be *unramified at a finite place* λ if $\rho(I_\lambda) = \{1\}$. In this case, every Frob_λ has the same image under ρ. Remember that a different embedding $\overline{K} \hookrightarrow \overline{K}_\lambda$ conjugates $Frob_\lambda$. Thus the image $\rho(\mathrm{Frob}_\lambda)$ is well-defined only up to conjugation but the trace and the determinant of the image are well-defined.

Chapter 3

Conjectures

In this chapter we list certain conjectures which have been considered by other authors (mainly Avner Ash and Fritz Grunewald) before. We start by a discussion of the classical case that motivates our conjectures and results.

3.1 The Classical Case

The theorems of Eichler-Shimura and Deligne [13] and the conjecture (now a theorem by Khare, Winterberger and others [28, 29]) of Serre [48] show that certain Galois representations of $\mathbb{Q}$ and certain classical modular forms are intimately related. In this section, we will briefly discuss this connection.

3.1.1 Modular Forms

Modular forms are complex analytic functions on the upper half-plane satisfying a certain kind of functional equation and growth condition.

The group $SL_2(\mathbb{Z})$ acts on the hyperbolic upper half plane $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ through linear fractional transformations:

$$\begin{pmatrix} a & b \\ & \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$

This action can be extended to the cusps $\mathbb{P}^1(\mathbb{Q})$. Note the similarity with the interaction between $\mathbf{SL}_2(\mathcal{O})$ and the hyperbolic upper half space $\mathbb{H}$, see Section 2.1.

For an integer N, let

$$\Gamma_0(N) = \{g \in \mathrm{SL}_2(\mathbb{Z}) : g \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod N\}$$

and

$$\Gamma_1(N) = \{g \in \mathrm{SL}_2(\mathbb{Z}) : g \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \bmod N\}$$

More precisely, a *holomorphic modular form* of level N and weight k (both positive integers) is a holomorphic function f on the upper half plane which satisfies:

- $f\big(\gamma \cdot z\big) = (cz+d)^k f(z) \quad$ for every $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$
- f is "holomorphic at cusps" .

The second condition roughly means that f has controlled growth towards the cusps.

Modular forms are usually presented as convergent Fourier series

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

where $q = e^{2\pi i z}$. This is possible because the matrices $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ lie in $\Gamma_1(N)$ so that $f(z+b) = f(z)$ for all integers b. A modular form is called *cuspidal* if it vanishes at the cusps. If f is cuspidal then $a_0 = 0$. We say that f is normalized if $a_1 = 1$.

The space $M_k(\Gamma_1(N))$ of modular forms of level N and weight k is finite dimensional. There is a commuting collection of operators T_m, $m \geq 1$, called Hecke operators, acting

on $M_k(\Gamma_1(N))$. These operators fix the subspace $S_k(\Gamma_1(N))$ of cuspidal forms and its complement $\mathrm{Eis}_k(\Gamma_1(N))$ so that

$$M_k(\Gamma_1(N)) = S_k(\Gamma_1(N) \oplus \mathrm{Eis}_k(\Gamma_1(N))$$

as Hecke-modules.

Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a normalized simultaneous eigenvector (an *eigenform*) for these operators. Then

$$T_m(f) = a_m f$$

It is a theorem of Shimura that if f is a normalized cuspidal eigenform, then a_n are algebraic integers and $\mathbb{Q}(a_2, ...)$ is a finite extension of $\mathbb{Q}$.

The space $M_k(\Gamma_1(N))$ admits a basis that consists of modular forms with integer coefficients. One constructs the space of mod ℓ modular forms with level N and weight k as $M_k(\Gamma_1(N), \mathbb{Z}) \otimes \overline{\mathbb{F}}_\ell$ where $M_k(\Gamma_1(N), \mathbb{Z})$ is the space of modular forms with integer coefficients.

3.1.2 Modularity and Serre's Conjecture

Given a normalized cuspidal eigenform, theorems of Deligne-Serre (weight 1), Eichler-Shimura (for weight 2) and Deligne (for weight > 2) construct ℓ-adic Galois representations of $\mathbb{Q}$ with special properties.

Theorem 3.1. *Let f be a normalized cuspidal eigenform of weight k, level N. Let $\mathcal{O}_f$ be the ring of integers of the algebraic number field K_f generated by the coefficients of f. Let ℓ be a rational prime and λ a prime of $\mathcal{O}$ over ℓ. Then there exists a Galois representation*

$$\rho_{f,\lambda} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathcal{O}_{f,\lambda})$$

where $\mathcal{O}_{f,\lambda}$ is the ring of integers of the completion of K at λ, such that for all $p \not| \ell N$

$$trace(\rho_{f,\lambda}(Frob_p)) = a_p \qquad and \qquad det(\rho_{f,\lambda}(Frob_p)) = b_p \cdot p$$

where a_p, b_p are the eigenvalues of f under the Hecke operators T_p and S_p respectively.

Serre's conjecture is in a way a converse to the above theorem. Given a $\rho_{f,\lambda}$ as above, one may reduce the image by the maximal ideal of $\mathcal{O}_{f,\lambda}$ and get a mod ℓ representation

$$\bar{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\ell^a})$$

The *weak form* of *Serre's Conjecture* says that all absolutely irreducible and odd mod ℓ Galois representations come from a normalized cuspidal eigenform in the way described above.

Here absolutely irreducible means that the representations stays irreducible when viewed as a representation into $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. A Galois representation of $\mathbb{Q}$ is odd if the determinant of the image of a complex conjugation is -1.

The *strong form* of Serre's Conjecture attaches each such mod ℓ representation $\bar{\rho}$ a level $N(\bar{\rho})$ and a weight $k(\bar{\rho})$ and says that there is a cuspidal eigenform f with this level and weight giving rise to $\bar{\rho}$.

Given a mod ℓ Galois representation, Serre defines the level $N(\bar{\rho})$ as the Artin conductor away from ℓ. More precisely,

$$N(\rho) = \prod_{p \neq (\ell)} p^{m(p)}$$

the product running over finite places p of $\mathbb{Q}$ and the exponents $m(p)$ only depend on $\rho|_{I_p}$, restriction of $\bar{\rho}$ to the inertia subgroup at p. In particular, $m(p) = 0$ if and only if $\bar{\rho}$ is unramified at p. $N(\bar{\rho})$ is well defined because $\bar{\rho}$ may ramify at only finitely many places.

To describe these exponents, let us view ρ as a homomorphism G_F into $\mathrm{Aut}(V)$ where V is a 2-dimensional vector space over $\mathbb{F}_{\ell^a}$. Then

$$m(\mathfrak{p}) = \sum_{i=0}^{\infty} \frac{1}{[G_0 : G_i]} \dim(V/V^{G_i})$$

where $G_0 = I_p$ and $G_i \subset G_0$ are the higher ramification groups at p. Here V^{G_i} stands for the subspace of V that is fixed by every element of G_i. The fact that this sum is an integer is proved in Serre [46].

The recipe of Serre for the weight $k(\rho)$ is quite involved. Since we do not need it, we skip its definition. We merely note that $k(\rho)$ only depends on $\rho|_{I_\ell}$.

3.1.3 The Big Picture

Here is the big picture for the classical situation over $\mathbb{Q}$.

Table 1: The big picture for the classical case

$\left\{ \begin{array}{c} \ell\text{-adic Galois} \\ \text{rep's of } \mathbb{Q} \end{array} \right\}$	$\xleftarrow{\text{Eichler-Shimura, Deligne}}$	$\left\{ \text{modular forms} \right\}$
$\Downarrow$		$\Updownarrow$
$\left\{ \begin{array}{c} \text{mod-}\ell \text{ Galois} \\ \text{rep's of } \mathbb{Q} \end{array} \right\}$	$\xrightarrow[\text{Serre's Conjecture}]{}$	$\left\{ \begin{array}{c} \text{mod-}\ell \\ \text{modular forms} \end{array} \right\}$

Notice that the arrows on the right hand side are two ways. This is because, for the primes $\ell \neq 2, 3$, mod ℓ modular forms all come by reduction from characteristic 0.

3.1.4 A Consequence of Serre's Conjecture

We now describe a corollary of Serre's Conjecture that we generalize later.

Let ρ be an irreducible, odd, continuous representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ that is unramified away from ℓ. Then by definition, $N(\rho) = 1$. Thus Serre's Conjecture says that there should be a cuspidal eigenform with level 1 giving rise to ρ. It is known that a suitable twist $\rho \otimes \chi^i$ of ρ should come from a level 1 cusp form of weight $\leq \ell + 1$, see [15] for a proof. Here χ is the mod ℓ cyclotomic character.

It is well known that there are no cusp forms with level 1 and weight less than 12. Thus the above mentioned Galois representations should not exist for $\ell = 2, 3, 5, 7$.

Theorem 3.2. *For $\ell = 2, 3, 5, 7$, there is no irreducible, odd Galois representation $\rho : G_{\mathbb{Q}} \to GL_2(\overline{\mathbb{F}}_\ell)$ that is unramified away from ℓ.*

For $\ell = 2$, this was proved by Tate [54]. Then Serre proved it for $\ell = 3$ [47]. Later Brueggemann [9], assuming GRH, proved it for $\ell = 5$. Moon and Taguchi [35] obtained partial results for $\ell = 7$. With the recent proof of Serre's Conjecture, all cases are proved unconditionally.

3.2 Over Imaginary Quadratic Fields

It this thesis, we are concerned with the picture where we replace $\mathbb{Q}$ with an imaginary quadratic field K. The very first question is what replaces the modular forms? An answer comes from the classical theorem of Shimura and Eichler [50, Chapter 8].

Theorem 3.3. *Let $\Gamma < \mathbf{SL}_2(\mathbb{Z})$ be a congruence subgroup preserved by the involution*

$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)$. *There is an isomorphism of Hecke modules*

$$H^1(\Gamma, E_{k-2}(\mathbb{C})) \simeq S_k(N) \oplus S_k^{anti}(N) \oplus Eis_k(N)$$

where $S_k(N), S_k^{anti}(N), Eis_k(N)$ *are the weight* k *level* N *spaces of cuspidal, anti-holomorphic cuspidal and Eisentein modular forms respectively.*

By Borel's Conjecture and Franke's proof of it (see Section 2.5), we know that the space

$$H^1(\Gamma, V_{k-2}) \simeq H^1(\Gamma\backslash\mathcal{H}^2, \widetilde{V}_{k-2})$$

can be described in terms of automorphic forms. The Eichler-Shimura theorem above tells us that the automorphic forms that appear in this description are the classical modular forms. So we decide to replace the classical modular forms with the automorphic forms that appear in the cohomology of the arithmetic quotients of (the global symmetric space in this setting) hyperbolic 3-space $\mathbb{H}$. These are the Bianchi modular forms that we discussed in Section 2.5.

Here is a comparison of the algebraic groups and the global symmetric spaces for the classical modular forms and Bianchi modular forms.

Table 2: The relevant algebraic groups

$\mathbf{G} := \mathbf{SL}_2$	$\mathbf{G} := \mathrm{Res}_{K/\mathbb{Q}}(\mathbf{SL}_2)$
$\mathbf{G}(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})$	$\mathbf{G}(\mathbb{R}) = \mathrm{SL}_2(\mathbb{C})$
$\mathbf{G}(\mathbb{Q}) = \mathrm{SL}_2(\mathbb{Q})$	$\mathbf{G}(\mathbb{Q}) = \mathrm{SL}_2(K)$
$\mathbf{G}(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})$	$\mathbf{G}(\mathbb{Z}) = \mathrm{SL}_2(\mathcal{O}_K)$
$\mathbf{G}(\mathbb{R})/\mathcal{K} \simeq \mathcal{H}^2$	$\mathbf{G}(\mathbb{R})/\mathcal{K} \simeq \mathcal{H}^3$

3.3 Conjectures

We now state the main conjectures. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with ring of integers $\mathcal{O}$. Let $\Gamma = \Gamma_1(\mathfrak{a})$ be a congruence subgroup of $\mathbf{PSL}_2(\mathcal{O})$ of level $\mathfrak{a}$ for some ideal $\mathfrak{a}$ of $\mathcal{O}$. Let $\mathbb{F}$ be a coefficient field of characteristic ℓ. If we do not want to specify the weight k, l, we just write $E(\mathbb{F})$. Recall that we have a commuting algebra of Hecke operators acting on $H^1(\Gamma, E_{k,l}(\mathbb{F}))$. An eigenform will mean a simultaneous eigenvector for the Hecke operators.

Definition 3.4. *A mod ℓ Galois representation $\rho : G_K \to GL_2(\mathbb{F})$ is modular if there is a mod ℓ Bianchi modular form v in some $H^1(\Gamma_1(\mathfrak{a}), E(\mathbb{F}))$ which is an eigenform for all Hecke operators such that*

$$tr(\rho(Frob_\lambda)) = a_\lambda \quad \text{and} \quad det(\rho(Frob_\lambda)) = b_\lambda N(\lambda)$$

for all primes $\lambda \not| \ell\mathfrak{a}$ at which ρ is unramified. Here a_λ, b_λ are the eigenvalues of v under the Hecke operators T_λ and S_λ respectively. Here $N(\lambda)$ is the norm of λ over $\mathbb{Q}$.
In this case, we say that "ρ comes from v" or that "ρ is attached to v".

Conjecture 3.5. *Every eigenform in $H^1_{cusp}(\Gamma, E_{k,l}(\mathbb{F}))$ has a Galois representation $\rho : G_K \to GL_2(\mathbb{F})$ attached to it.*

The mod ℓ eigenforms which are reductions of the torsion-free part of the integral cohomology $H^1(\Gamma, E_{k,l}(\mathcal{O}))$ are called *automorphic*. This is because the torsion-free part of the integral cohomology embeds into the complex cohomology where the automorphic forms live, see Section 2.5. Langlands' philosophy dictates that such forms should be related to Galois representations of K. In accordance, results of Taylor and others (see [56, 24, 5]) confirm that they do have attached ℓ-adic Galois representations. So our

conjecture above goes further and says that the mod ℓ eigenforms which are reductions of the *torsion* part of the integral cohomology also are related to Galois representations. Of course, these forms have nothing to do with automorphic forms and hence they are outside the scope of Langlands' philosophy. See Ash [1] for the same conjecture in the $\mathrm{GL}_n(\mathbb{Z})$ $(n > 2)$ context.

Conjecture 3.6 (The Bridge Conjecture). *An eigenvalue system attached to some non-automorphic eigenform in some $H^1(\Gamma, E(\mathbb{F}))$ also arises attached to some automoprhic eigenform in some $H^1(\Gamma', E'(\mathbb{F}))$ for some congruence subgroup $\Gamma' < \Gamma$.*

In Conjecture 3.5, we are saying that the non-automorphic mod ℓ eigenforms should give us Galois representations just like the automorphic mod ℓ eigenforms are expected to under Langlands' philosophy. Are these representations new? Conjecture 3.6 says that they are not. It says that a mod ℓ-Galois representation coming from a non-automorphic mod ℓ eigenform should also arise from an automorphic mod ℓ eigenform, of possibly higher level.

It was communicated to us by Avner Ash that the name "Bridge Conjecture" was coined by Barry Mazur.

Conjecture 3.7 (Weak Serre Conjecture). *An absolutely irreducible mod ℓ Galois representation $\rho : G_K \to GL_2(\mathbb{F})$ comes from some eigenform in some $H^1_{cusp}(\Gamma, E(\mathbb{F}))$.*

Conjecture 3.8 (Intermediate Serre Conjecture). *An absolutely irreducible mod ℓ Galois representation $\rho : G_K \to GL_2(\mathbb{F})$ of Serre conductor $N \lhd \mathcal{O}$ comes from an eigenform in $H^1_{cusp}(\Gamma_1(N), E(\mathbb{F}))$.*

This last conjecture is intermediate in the sense that we are predicting the level but

not the weights (k, l) where one can find an eigenform the Galois representation that we start with is attached to.

Chapter 4

Theoretical Results

Now we present some of our results and discuss their relevance to the conjectures above.

4.1 Weight Reduction

A result of Ash and Stevens [3] for the classical modular forms says that an eigenvalue system (mod ℓ) occuring in $M_k(\Gamma_1(N))$ with $k > 2$ also occurs, up to twist, in $M_2(\Gamma_1(N\ell))$. In particular, one sees that there are only finitely many systems of eigenvalues (mod ℓ) occurring in the infinite dimensional space $M_{\geq 2}(\Gamma_1(N))$. In joint work with Seyfi Turkelli [44], we prove an analogue in our case. The proof is presented in Chapter 6.

Theorem 4.1. *Let K be an imaginary quadratic field of class number one and $\mathcal{O}$ be its ring of integers. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ that is prime to the ideal (ℓ) where ℓ is a rational prime that is split in $\mathcal{O}$. Let Φ be a Hecke eigenvalue system occurring in $H^1(\Gamma_1(\mathfrak{a}), E)$ where E is a finite dimensional $\mathbb{F}_\ell[SL_2(\mathcal{O}/(\ell))]$-module. Then Φ occurs in $H^1(\Gamma_1(\mathfrak{a}\ell), \mathbb{F}_\ell)$.*

Notice that $E_{(0,0)}(\mathbb{F}) \simeq \mathbb{F}$ for any field $\mathbb{F}$. Basically, this theorem is saying that if we work mod ℓ, an eigenvalue system occurring in some level $\mathfrak{a}$ and weight (k, l) appears also with weight $(0, 0)$ if we raise the level to $\mathfrak{a}(\ell)$. In particular, we get the following.

Corollary 4.2. *Let K be an imaginary quadratic field of class number one and $\mathcal{O}$ be its ring of integers. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ that is prime to the ideal (ℓ) where ℓ is a rational prime that is split in $\mathcal{O}$. The set of systems of eigenvalues coming from all mod ℓ Bianchi modular forms of level $\mathfrak{a}$ is finite.*

We note that this corollary also follows from [2, Thm. 2.2].

4.2 Nonexistence of Certain Representations

The following is the main result of our paper [43] which has been accepted for publication in the Proceedings of the AMS. We give its proof in Chapter 7. We start with some terminology to simplify the statement.

Let K be a number field and p be a rational prime. We say that the pair (K, p) satisfies (†), if there is no irreducible continuous representation of G_K into $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ that is unramified away from $\{p, \infty\}$.

Theorem 4.3.

A. For $d = 6, 5, 3, 2, -1, -2, -3, -5, -6$, the pair $(\mathbb{Q}(\sqrt{d}), 2)$ satisfies (†).

B. The pair $(\mathbb{Q}(\sqrt{-3}), 3)$ satisfies (†).

This result is an analogue of Theorem 3.2. We note that part A of this theorem has been proved also by Moon-Taguchi [36]. See their recent article [37] for certain finiteness results for other quadratic fields using GRH.

In the language of Galois representations, (K, p) satisfies property (†) if there is no absolutely irreducible level 1 mod p Galois representation of K.

Corollary 4.4. *Assume that 3.8 is true. Then for the pairs (K_d, p) listed in Theorem 4.3, there should be no eigenforms in $H^1_{cusp}(\mathbf{PSL}_2(\mathcal{O}_d), E_{k,l}(\overline{F}_p))$ for any (k, l).*

We have produced computer programs to compute these cohomology spaces and the Hecke operators on them. We verified for $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-2})$ that the mod 2 cohomology spaces mentioned in the above Corollary are indeed trivial (see Section 5.1.2). This is *supporting evidence* for the Intermediate Serre Conjecture of Section 3.3.

4.2.1 Some Existence Results

Table 3: Sym(3)-extensions only ramified over 2

d	$f(x)$	ramification
-13	$x^6 + x^4 + 4x^3 + 36x^2 - 24x + 4$	only over 2
-19	$x^6 - 8x^5 + 23x^4 - 24x^3 + x^2 + 14x + 4$	only over 2
-22	$x^6 - 2x^5 + 5x^4 + 8x^3 + 47x^2 + 90x + 47$	only over 2
-37	$x^6 + 4x^5 + 23x^4 - 4x^3 + 71x^2 - 288x + 293$	only over 2
-38	$x^6 + 6x^5 + 33x^4 + 60x^3 + 89x^2 - 258x + 207$	only over 2
-46	$x^6 + 6x^5 + 21x^4 + 52x^3 + 291x^2 + 326x + 271$	unramified
-58	$x^6 + 8x^5 + 40x^4 + 60x^3 + 261x^2 + 380x + 382$	only over 2
-62	$x^6 + 6x^5 + 45x^4 + 132x^3 + 179x^2 + 246x + 423$	unramified
-74	$x^6 + 6x^5 + 41x^4 + 32x^3 + 101x^2 - 654x + 691$	only over 2
-79	$x^6 - 3x^5 + 14x^4 - 4x^3 + 40x^2 + 64x + 64$	only over 2

We also investigated the pairs $(K, 2)$ for which (†) fails, that is the pairs $(K, 2)$ for which there exist irreducible continuous representations of G_K into $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ that is unramified away from $\{2, \infty\}$. The simplest case is a $GL_2(\mathbb{F}_2) \backsimeq Sym(3)$ extension L/K that is ramified only over $\{2, \infty\}$. Using group theory with MAGMA, we have searched the number fields database of J.Klüners and G.Malle [31] for $Sym(3)$ extensions of quadratic fields with little or no ramification. In Table 4.2.1, we list some of our findings for imaginary K. In each case, L is the splitting field of the given polynomial over $\mathbb{Q}$

and the third column is ramification of finite places in L/K.

4.2.2 An Application to Elliptic Curves

We now present a straightforward corollary of our Theorem 4.3 to the theory of elliptic curves. We explain the proof in Section 7.4.

Corollary 4.5. *For $d = 5, 3, 2, -1, -2, -3, -5, -6$, there is no elliptic curve with good reduction everywhere over $\mathbb{Q}(\sqrt{d})$.*

Kagawa and Kida proved the nonexistence of elliptic curves with good reduction everywhere over many small quadratic fields , including the ones listed in this corollary (see [27, 26]). One may try to use our approach on the several other small ones quadratic fields not covered by their methods.

Chapter 5

Computational Results

To be able to investigate modularity over imaginary quadratic fields, one has to be able to effectively compute the modular forms and the Hecke action on them. In joint work with Fritz Grunewald, we produced MAGMA programs to do this task for the fields K_1 and K_2. Our code can be easily adapted to the other three Euclidean imaginary quadratic fields K_3, K_7 and K_{11}. We will report on this algorithm in Chapter 8. In this section, we present some of the results of our computations for the field K_2. In particular, we give supporting evidence to some of the conjectures we listed in Section 3.3.

The earliest calculations were done by Grunewald-Mennicke, see [16, 21]. They considered $H_1(\Gamma, \mathbb{Z})$ and $H_1(\Gamma, \mathbb{C})$. For the former, they employed an algebraic approach using the fact that $\Gamma^{ab} \simeq H_1(\Gamma, \mathbb{Z})$. For the latter, they used the modular symbols method which uses the geometry of the hyperbolic 3-space $\mathbb{H}$. Later Cremona [12] extended their methods to other imaginary quadratic fields. The only higher weight calculations have been carried out by Priplata [42] where she computed the cohomology with level 1 and weight $(2k, 0)$.

5.1 Dimension Tables

We present dimensions of various subspaces of $H^1(\Gamma, E)$ over $\mathbb{C}$ and $\mathbb{F}_2$. A very important subspace is the space of so called *plus-forms* that we define now.

Let ϵ be a generator of $\mathcal{O}^*$. Then conjugation by the element $\left(\begin{smallmatrix}\epsilon & 0\\ 0 & 1\end{smallmatrix}\right) \in \mathbf{PGL}_2(\mathcal{O})$ leaves Γ invariant and induces an involutory automorphism $\tilde{\epsilon}$ on $H^1(\Gamma, E(\mathbb{F}))$. We put

$$H^1(\Gamma, E(\mathbb{F}))^{\pm}$$

for the ± 1 eigenspaces of $\tilde{\epsilon}$. If $\mathbb{F}$ is of char. 2, we denote by $H^1(\Gamma, E(\mathbb{F}))^+$ the subspace that is invariant under $\tilde{\epsilon}$.

Remark : Note that taking $\tilde{\epsilon}$ invariants equals to working with $\mathbf{PGL}_2(\mathcal{O})$ instead of $\mathbf{PSL}_2(\mathcal{O})$. One sees by the inflation-restriction sequence that

$$H^1(\mathbf{PGL}_2(\mathcal{O}), E) \simeq H^1(\mathbf{PSL}_2(\mathcal{O}), E)^+.$$

5.1.1 Complex Cohomology

In Table 4, we give the dimensions of the cohomology group $H^1(\Gamma_0(\mathfrak{a}), E_{(k,l)}(\mathbb{C}))$ and its cuspidal part for small primes $\mathfrak{a} \triangleleft \mathcal{O}$ of residual degree 1 and weights (k, l).

The pairs in square brackets were computed with the mod ℓ cohomology. In general, the mod ℓ dimension is an upperbound for the char.0 dimension, that is $\dim H^1(\Gamma, E(\mathbb{C})) \leq \dim H^1(\Gamma, E(\mathbb{F}_\ell))$. We actually *know* that these upperbounds in Table 4 are equal to the actual complex dimensions via base change calculations and known facts about the dimension of the Eisenstein cohomology. We will not go into these here and merely use square brackets.

Table 4: Dimensions for char.0 cohomology

(k,k)	$\Gamma(1)$	$\Gamma(3)$	$\Gamma(11)$	$\Gamma(17)$	$\Gamma(19)$	$\Gamma(41)$	$\Gamma(43)$	$\Gamma(59)$	$\Gamma(67)$
0	1,0	2,0	2,0	2,0	2,0	3,1	2,0	2,0	2,0
1	1,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0	2,0
2	1,0	2,0	2,0	[2, 0]	[2, 0]	[2, 0]	[2, 0]	[2,0]	[2,0]
3	2,1	4,2	[4, 2]	[4, 2]	[4, 2]	[4, 2]	[4, 2]	[4,2]	[4,2]
4	1,0	2,0	[2, 0]	[2, 0]	[2, 0]	[2, 0]	[2, 0]	[2, 0]	[2, 0]
5	3,2	[6, 4]	[6, 4]	[6, 4]	[6, 4]	[6, 4]	[6, 4]		
6	2,1	[4, 2]	[4, 2]	[4, 2]	[4,2]	[4,2]			
7	4,3	[8, 6]	[8, 6]	[8, 6]	[8,6]				
8	2,1	[4, 2]	[4, 2]	[4, 2]					
9	5,4	[10, 8]	[10, 8]	[10,8]					
10	3,2	[6, 4]	[6,4]	[6,4]					
11	6,5	[12,10]	[12,10]	[12,10]					
12	3,2	[6,4]	[6,4]	[6,4]					
13	7,6	[14,12]	[14,12]						
14	4,3	[8,6]	[8,6]						
15	8,7	[16,14]	[16,14]						
16	4,3	[8,6]	[8,6]						
17	9,8	[18,16]							
18	5,4	[10,8]							
19	10,9								
20	5,4								

5.1.2 Mod 2 cohomology

Next we give dimensions for the mod 2 cohomology groups. Here the irreducible weights are $E_{k,l}(\mathbb{F}_2)$ with $0 \leq k, l < 2$. It is explained in Lemma 2.8 that these weights are sufficient if one is interested only in computing the eigenvalue systems. So we will consider only such weights.

In Table 5, for each level and weight, we give two pairs of integers. The first pair gives the dimensions of $H^1(\Gamma_0(\mathfrak{a}), E_{k,l}(\mathbb{F}_2))$ and $H^1_{\mathrm{cusp}}(\Gamma_0(\mathfrak{a}), E_{k,l}(\mathbb{F}_2))$ respectively. The second pair gives the dimensions of $H^1(\Gamma_0(\mathfrak{a})), E)^+$ and $H^1_{\mathrm{cusp}}(\Gamma_0(\mathfrak{a}), E_{k,l}(\mathbb{F}_2))^+$ respectively. See Sections 2.5 and 3.3 for the definitions.

Table 5: Dimensions for mod 2 cohomology

(k,l)	$\Gamma_0(1)$	$\Gamma_0(3)$	$\Gamma_0(11)$	$\Gamma_0(17)$	$\Gamma_0(19)$
(0,0)	(2,0);(2,0)	(2,0);(2,0)	(2,0);(2,0)	(4,2) ; (4,2)	(2,0);(2,0)
(1,1)	(3,0) ; (2,0)	(4,0) ; (2,0)	(4,0) ; (2,0)	(8,3) ; (5,2)	(4,0) ; (2,0)
(2,2)	(9,0) ; (6,0)	(10,0) ; (6,0)	(10,0) ; (6,0)	(18,7) ; (13,4)	(10,0) ; (6,0)
(0,2)	(4,0) ; (3,0)	(4,0) ; (3,0)	(4,0) ; (3,0)	(7,3) ; (6,2)	(4,0) ; (3,0)
(2,0)	(4,0) ; (3,0)	(4,0) ; (3,0)	(4,0) ; (3,0)	(7,3) ; (6,2)	(4,0) ; (3,0)

(k,l)	$\Gamma_0(41)$	$\Gamma_0(43)$	$\Gamma_0(59)$	$\Gamma_0(67)$	$\Gamma_0(73)$
(0,0)	(5,3) ; (5,3)	(2,0);(2,0)	(2,0);(2,0)	(4,2) ; (3,1)	(5,3) ; (4,2)
(1,1)	(11,7) ; (8,4)	(4,0) ; (2,0)	(4,0) ; (2,0)	(10,6) ; (6,2)	(9,5) ; (6,2)
(2,2)	(24,14) ; (19,7)	(10,0) ; (6,0)	(10,0) ; (6,0)	(22,12) ; (15,3)	(22,12) ; (16,4)
(0,2)	(9,5) ; (8,3)	(4,0) ; (3,0)	(4,0) ; (3,0)	(8,4) ; (6,1)	(9,5) ; (7,2)
(2,0)	(9,5) ; (8,3)	(4,0) ; (3,0)	(4,0) ; (3,0)	(8,4) ; (6,1)	(9,5) ; (7,2)

Theorem 4.3, in conjunction with the Intermediate Serre Conjecture of Section 3.3, implies that there should be no cuspidal mod 2 Bianchi eigenforms of level 1 for K_2. We see from Table 5 that this is indeed the case, that is, $H^1_{\text{cusp}}(\mathbf{PSL}_2(\mathcal{O}), E_{k,l}(\mathbb{F}_2))$ is trivial for all $0 \leq k, l \leq 2$. Thus we obtain supporting evidence for the conjecture. We made the same verification for the field K_1.

5.2 Elliptic Curves Over K

Let E be an elliptic curve over K and let ℓ be a rational prime. The absolute Galois group G_K of K acts on the group $E[\ell]$ of ℓ-torsion points of $E(\overline{K})$. The group $E[p]$ is free of rank two over $\mathbb{Z}/p\mathbb{Z}$. Thus, after fixing a basis, we get a mod ℓ Galois representation

$$\bar{\rho}_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

Let $\Delta(E)$ be the discriminant of E. It is known that for any prime λ such that $\lambda \not| \Delta(E)\ell$,

we have

$$\mathrm{tr}(\bar{\rho}_{E,\ell}(Frob_\lambda)) = N(\lambda) + 1 - \#E(\mathbb{F}_\ell) \pmod{\ell}$$

and

$$\det(\bar{\rho}_{E,\ell}(Frob_\lambda)) = N(\lambda) \pmod{\ell}$$

We made a computer search for elliptic curves E over K with the property that the norm of the its conductor is of the form $p^k\ell$ where $p = 2, 3$. In all the cases we checked where the associated mod ℓ Galois representation $\bar{\rho}_{E,p}$ was absolutely irreducible, we found an eigenform in $H^1_{\mathrm{cusp}}(\Gamma_0(\ell), E(\mathbb{F}_p))$ which numerically seemed like matching $\bar{\rho}_{E,p}$. We present one such example.

Set $\omega = \sqrt{-2}$. Let E be the elliptic curve over K given by the equation

$$E: \ y^2 = x^3 + (-3-\omega)x^2 + 2x - 4 + 2\omega.$$

Our computations with the computer algebra system MAGMA shows that the conductor of E is $(1-\omega)(3+2\omega)$. Thus the norm of the conductor is $3 \cdot 17$. Let $\Phi(x)$ be the 3-division polynomial of E. Thus the roots of $\Phi(x)$ are the x-coordinates of the 3-torsion points of $E(\overline{K})$. MAGMA tells us that the degree of the splitting field of $\Phi(x)$ over K is 24. This means that the image of $\bar{\rho}_{E,3}$ contains $\mathrm{SL}_2(\mathbb{F}_3)$ since it is the only order 24 subgroup of $\mathrm{GL}_2(\mathbb{F}_3)$. The determinants of the Frobenius elements are not always 1 mod 3, thus the image is bigger than $\mathrm{SL}_2(\mathbb{F}_3)$, thus it must be $\mathrm{GL}_2(\mathbb{F}_3)$ itself. Finally, the Serre conductor of $\bar{\rho}_{E,3}$ can be calculated to be $(3+2\omega)$.

According to the Intermediate Serre Conjecture stated in Section 3.3, there must be an eigenform in $H^1_{\mathrm{cusp}}(\Gamma_1(17), E(\mathbb{F}_3))$ that matches our representation in the sense given in Definition 3.4. We verify this using the programs we produced.

In Table 6, we give two ordered pairs of integers. The first pair gives the dimensions of $H^1(\Gamma_0(17), E_{k,l}(\mathbb{F}_3))$ and $H^1_{\text{cusp}}(\Gamma_0(17), E_{k,l}(\mathbb{F}_3))$ respectively. The second pair gives the dimensions of $H^1(\Gamma_0(17), E)^+$ and $H^1_{\text{cusp}}(\Gamma_0(17), E_{k,l}(\mathbb{F}_3))^+$ respectively.

Table 6: Dimensions for $H^1(\Gamma_0(17), E(\mathbb{F}_3))$

(k,l)	(0,0)	(1,1)	(2,2)	(3,3)
	(2,0);(0,0)	(2,0);(1,0)	(3,1);(0,0)	(8,0);(1,0)

(k,l)	(0,2)	(2,0)	(1,3)	(3,1)
	(2,0);(0,0)	(3,1);(0,0)	(4,0);(1,0)	(4,0);(1,0)

We see from Table 6, at level 17, the only cuspidal cohomology occurs at weights $(2, 2)$ and $(2, 0)$, both 1 dimensional. We compute the Hecke action on both of these spaces and find that the eigenvalues are the same for all the Hecke operators we computed. In support of the Intermediate Serre Conjecture, this eigenvalue system matches our representation $\bar{\rho}_{E,3}$. We note that both of the cuspidal spaces are inside the minus-space (see Section 5.1).

In the next table, we list the eigenvalues and the traces of the Frobenius elements for the first few primes of residue degree 1.

Table 7: Comparison of eigenvalues and traces of Frobenius elements

prime	$3+\omega$	$3-\omega$	$1+3\omega$	$1-3\omega$	$3+4\omega$	$3-4\omega$
norm	11	11	19	19	41	41
eigenvalue	2	1	0	2	1	1
trace	2	1	0	2	1	1

prime	$5+3\omega$	$5-3\omega$	$3+5\omega$	$3-5\omega$	$7+3\omega$	$7-3\omega$
norm	43	43	59	59	67	67
eigenvalue	1	1	0	2	1	0
trace	1	1	0	2	1	0

Chapter 6

Proof of the Weight Reduction Result

In this chapter, we present the proof of the weight reduction result that we announced in Theorem 4.1. We follow closely our preprint [44] that is prepared jointly with Seyfi Turkelli.

Elstrod-Grunewald-Mennicke [16] were the first investigators of the connection between mod ℓ Bianchi modular forms and mod ℓ Galois representations of imaginary quadratic fields. In his paper [18], Figueiredo considered an analogue of Serre's conjecture in this setting but he only considered mod ℓ Bianchi modular forms in cohomology spaces with trivial coefficients. Motivated by a result of Ash and Stevens [3] for the classical modular forms, he assumed that a Hecke eigenvalue system attached to a mod ℓ Bianchi modular form, after increasing the level, would be attached to another form with trivial weight.

In this paper, we prove that what Figueiredo assumed is true using the ideas of Ash and Stevens [3]. More precisely;

Theorem 6.1. *Let K be an imaginary quadratic field of class number one and $\mathcal{O}$ be its ring of integers. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}$ that is prime to the ideal (ℓ) where ℓ is a rational prime that is split in $\mathcal{O}$. Let Φ be a Hecke eigenvalue system occurring in $H^1(\Gamma_1(\mathfrak{a}), E)$ where E is a finite dimensional $\mathbb{F}_\ell[SL_2(\mathcal{O}/(\ell))]$-module. Then Φ occurs in $H^1(\Gamma_1(\mathfrak{a}\ell), \mathbb{F}_\ell)$.*

As an immediate corollary, we get

Corollary 6.2. *Mod ℓ, there are only finitely many eigenvalue systems with fixed level.*

Once and for all, fix a quadratic imaginary field K of class number one and an ideal $\mathfrak{a}$ of $\mathcal{O} = \mathcal{O}_K$. Let $\ell = \lambda\bar{\lambda}$ be a rational prime that splits in $\mathcal{O}$ which is coprime to $\mathfrak{a}$. For the rest of the paper, we use the following notation:

$$\begin{aligned}
\mathrm{Mat}_2(\mathcal{O})_{\neq 0}: &\quad 2\times 2 \text{ matrices of non-zero determinant with entries in } \mathcal{O}\\
\Gamma_0(\mathfrak{a}): &\quad \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}) : c \equiv 0 \mod \mathfrak{a} \right\}\\
\Gamma = \Gamma_1(\mathfrak{a}): &\quad \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathcal{O}) : c \equiv d-1 \equiv 0 \mod \mathfrak{a} \right\}\\
\Gamma_1: &\quad \Gamma_1(\mathfrak{a}\cdot\lambda)\\
\Gamma_2: &\quad \Gamma_1(\mathfrak{a}\cdot\lambda\bar{\lambda})\\
\Delta: &\quad \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Mat}_2(\mathcal{O})_{\neq 0} : c \equiv 0 \mod \mathfrak{a} \right\}
\end{aligned}$$

Recall that a system of eigenvalues of $\mathbb{H}$ with values in a ring R is a map of sets $\Phi : \mathbb{H} \to R$. We say that an eigenvalue system Φ occurs in the $R\mathbb{H}$-module A if there is a nonzero element $a \in A$ such that $Ta = \Phi(T)a$ for all T in $\mathbb{H}$.

The following lemma is proved in [2, Lemma 2.1].

Lemma 6.3. *Let F be a field and V be a $F\Delta$-module which is finite dimensional over F. If an eigenvalue system $\Phi : \mathbb{H} \to F$ occurs in $H^n(\Gamma, V)$, then Φ occurs in $H^n(\Gamma, W)$ for some irreducible $F\Delta$-subquotient W of V.*

Thus it is enough to investigate the cohomology with irreducible coefficient modules if we are only interested in the eigenvalue systems. In the next two sections, we discuss the irreducible $\mathbb{F}_\ell[\mathrm{SL}_2(\mathcal{O}/(\ell))]$-modules.

6.1 The Irreducible Modules

For a nonnegative integer k, let $\tilde{E}_k$ be the right representation of $\mathbf{GL}_2$ on $Sym^k(\mathbf{A}^2)$. Given a commutative a ring R, we have $E_k(R) \simeq R[x,y]_k$ where the latter is the space of homogeneous degree k polynomials in two variables over R. Note that $\{X^{k-i}Y^i : 0 \leq i \leq k\}$ is an R-basis of $E_k(R)$.

Let Δ be the semi-group of 2×2 matrices of nonzero determinant with entries in $\mathcal{O}$. We can give $E_k(\mathcal{O})$ a right Δ-module structure as follows. For a polynomial $P(X,Y)$ in $E_k(\mathcal{O})$ and a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in Δ, we set

$$\big(P \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\big)\big(X,Y\big) = P\big(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)\big) = P\big(aX+bY, cX+dY\big).$$

Δ acts on $E_k(\mathbb{F}_\ell)$ in two different ways: through reduction by λ and by $\bar{\lambda}$. In this note, we are interested in the (absolutely) irreducible representations of $SL_2(\mathcal{O}/(\ell)) = SL_2(\mathcal{O}/\lambda) \times SL_2(\mathcal{O}/\bar{\lambda})$ over $\mathbb{F}_\ell$. Results of Steinberg [52] and Brauer-Nesbitt [8] show that these are of the form

$$E_{r,s}(\mathbb{F}_\ell) := E_r(\mathbb{F}_\ell) \otimes E_s(\mathbb{F}_\ell) \quad \text{where} \quad 0 \leq r,s \leq \ell - 1.$$

Here, $SL_2(\mathcal{O})$ acts on the first module through reduction by λ and on the second through reduction by $\bar{\lambda}$.

Let I be the set of $\mathbb{F}_\ell$ valued functions on $\mathbb{F}_\ell^2$ which vanish at the origin. Again, Δ

acts on I both by reduction by λ and by $\bar{\lambda}$. The action is given by

$$(f \cdot M)(a,b) = f((a,b)M^t)$$

for $f \in I$, $(a,b) \in \mathbb{F}_\ell^2$ and $M \in \Delta$.

For each integer n, let I_n be the Δ-submodule of I consisting of homogeneous functions of degree n, that is, the collection of functions $f \in I$ such that $f((xa,xb)) = x^n f((a,b))$. The degree is well-defined modulo $\ell - 1$. A function $f \in I_n$ is determined by its values on the set $\{(1,0),...,(1,\ell-1),(0,1)\}$, which we identify with $\mathbb{P}^1(\mathbb{F}_\ell)$. Thus every I_n is $\ell + 1$ dimensional. We have the decomposition

$$I \simeq \bigoplus_{n=0}^{\ell-2} I_n.$$

We will need the following two facts, see [3][Section 3].

Lemma 6.4. *For $0 \leq r \leq \ell - 1$, there are $SL_2(\mathcal{O})$-invariant perfect pairings*

(1) $E_r \times E_r \to \mathbb{F}_\ell$

(2) $I_r \times I_{\ell-1-r} \to \mathbb{F}_\ell$

Let $0 \leq r \leq \ell - 1$. As in [3], we consider the following $SL_2(\mathcal{O})$-invariant maps. Each polynomial in E_r can be seen as a function on $\mathbb{F}_\ell^2$. This gives us a morphism $\alpha_r : E_g \to I_r$. Let $\beta_r : I_r \to E_{\ell-1-r}(r)$ be given by

$$\beta_r(f) = \sum_{(a,b)\in\mathbb{F}_\ell^2} f(a,b)(bX - aY)^{\ell-1-r}.$$

Here we mean by $E_{\ell-1-r}(r)$ the Δ-module $E_{\ell-1-r}$ where the action is twisted as

$$P \cdot M := \det(M)^r (P \cdot M)$$

Lemma 6.5. *For $0 \leq r \leq \ell - 1$, we have the following exact sequence of Δ-modules*

$$0 \longrightarrow E_r \xrightarrow{\alpha_r} I_r \xrightarrow{\beta_r} E_{\ell-1-r}(r) \longrightarrow 0$$

6.2 Proof of the Theorem

In this section, we will investigate the eigenvalue systems occurring in $H^1(\Gamma(\mathfrak{a}), E_{k,l}(\mathbb{F}_\ell))$. We first give a characterization of the induced module $Ind_{\Gamma_2}^{\Gamma}(\mathbb{F}_\ell)$.

Lemma 6.6. *There is a map $M \mapsto (1,0)M^t \mod (\ell)$ is a bijection between the right cosets $\Gamma_2\backslash\Gamma$ and the set*

$$S := \{(a,c) \in (\mathcal{O}/(\ell))^2 | < a, c >= \mathcal{O}/(\ell)\}$$

where (ℓ) is the ideal of $\mathcal{O}$ generated by ℓ.

Proof. The proof is the same as the proof of the analogue statement for $\mathrm{SL}_2(\mathbb{Z})$, see [51, p.127]. □

We identify $\mathcal{O}/(\ell) \simeq \mathcal{O}/(\lambda) \times \mathcal{O}/(\bar{\lambda})$ with $\mathbb{F}_\ell \times \mathbb{F}_\ell$. Then we can describe the set S as

$$S = (\mathbb{F}_\ell \times \mathbb{F}_\ell)^2 \backslash \{((a,0),(c,0)),((0,a'),(0,c'))\}.$$

It follows that $|S| = \ell^4 - 2\ell^2 + 1 = (\ell^2 - 1)(\ell^2 - 1)$.

Let J be the set of $\mathbb{F}_\ell$-valued functions on $(\mathbb{F}_\ell \times \mathbb{F}_\ell)^2$ that vanish outside of S. As the map in Lemma 6.6 commutes with the action of Δ, we can identify the Δ-module $Ind_{\Gamma_2}^{\Gamma}(\mathbb{F}_\ell)$ with the module J. The action of Δ on J is given by

$$(f \cdot M)(a,b) = f((a,b)M^t)$$

where M is reduced modulo (ℓ) on the right hand side. We have showed the following.

Lemma 6.7. *As Δ-modules, $Ind_{\Gamma_2}^{\Gamma}(\mathbb{F}_\ell) \simeq J$.*

Recall the definition of the Δ-modules I from Section 6.1 We now consider the Δ-module $I \otimes I$ where Δ acts on the components through reduction by λ and $\bar{\lambda}$ respectively.

Lemma 6.8. *As Δ-modules, we have $I \otimes I \simeq J$.*

Proof. Define the map $\Lambda : I \otimes I \longrightarrow J$ as

$$\varphi \otimes \psi \longmapsto \big((a,c) \mapsto \varphi(a_1,c_1)\psi(a_2,c_2)\big)$$

where $a = (a_1, a_2)$ and $c = (c_1, c_2)$. One can easily check that the image of Λ is in J. Given $M \in \Delta$, let M_1, M_2 denote its reduction modulo λ and $\bar{\lambda}$ respectively. Then a direct computation shows that

$$\begin{aligned}\Lambda\big((\varphi \otimes \psi) \cdot M\big)(a,c) &= \Lambda\big((\varphi \cdot M) \otimes (\psi \cdot M)\big)(a,c) \\ &= \varphi((a_1,c_1)M_1^t))\psi((a_2,c_2)M_2^t) = \big(\Lambda\big(\varphi \otimes \psi\big) \cdot M\big)(a,c)\end{aligned}$$

Hence Λ is Δ-invariant. Given a nonzero φ, one sees that $\Lambda(\varphi \otimes \psi) = 0$, only when $\psi = 0$. Thus Λ is injective. As they have the same cardinality, $I \otimes I$ and J are isomorphic as Δ-modules. □

Definition 6.9. *For given nonnegative integers r, s, we define the following Δ-modules where Δ acts on the components of every tensor product through reduction by λ and $\bar{\lambda}$ respectively.*

1. $E_{r,s} := E_r \otimes E_s$;
2. $I_{r,s} := I_r \otimes I_s$;
3. $U_{r,s} := [E_{\ell-1-r}(r) \otimes I_s] \oplus [I_r \otimes E_{\ell-1-s}(s)]$;
4. $V_{r,s} := E_{\ell-1-r}(r) \otimes E_{\ell-1-s}(s)$.

Recall from Section 3 that $E_{r,s}$ is an irreducible representation of $\mathrm{SL}_2(\mathcal{O}/(\ell))$ over $\mathbb{F}_\ell$ when $0 \le r, s \le \ell - 1$. We note that under the map Λ of Lemma 6.8, the submodule of functions f in J such that $f(xa, yc) = x^r y^s f(a,c)$ is isomorphic to $I_{r,s}$ as Δ-modules.

By Section 3, we have Δ-module morphisms

$$\pi : I_{r,s} \to U_{r,s} \qquad \text{defined by} \qquad \pi := [\beta_r \otimes \mathrm{id}] \oplus [\mathrm{id} \otimes \beta_s]$$

and

$$\pi' : U_{r,s} \to V_{r,s} \qquad \text{defined by} \qquad \pi' := \mathrm{id} \otimes \beta_s - \beta_r \otimes \mathrm{id}.$$

Lemma 6.10. *Let the notation be as above. Let* $0 \leq r \leq \ell - 1$ *and* $0 \leq s \leq \ell - 1$. *We have the following exact sequence* Δ*-modules:*

$$0 \longrightarrow E_{r,s} \xrightarrow{\iota} I_{r,s} \xrightarrow{\pi} U_{r,s} \xrightarrow{\pi'} V_{r,s} \longrightarrow 0 \, .$$

Proof. Note that Δ-modules in question are flat since they are also $\mathbb{F}_\ell$-vector spaces. So, by Lemma 6.5, ι is injective. One can easily see that $Im(\iota) \subseteq Ker(\pi)$ and π' is surjective. Thus, in order to complete the proof, it suffices to show that $dim(Im(\pi)) = (\ell+1)^2 - (r+1)(s+1)$; this is what we do below.

Identifying E_r with its image in I_r, we can write the decomposition $I_r = E_r \oplus E'_{\ell-1-r}$ (note that we have $E'_{\ell-1-r} \cong E_{\ell-1-r}$). Now, it is evident that $dim(\pi(E_r \otimes I_s)) = (r+1)(\ell-s)$ and that $dim(\pi(E'_{\ell-1-r} \otimes I_s)) = (\ell-r)(\ell+1)$. Elementary linear algebra shows that these images have trivial intersection and this gives us the desired dimension. $\square$

Setting $W_{r,s} := ker(\pi' : U_{r,s} \to V_{r,s})$, by Lemma 6.10, we get two short exact sequences

$$0 \longrightarrow E_{r,s} \xrightarrow{\iota} I_{r,s} \xrightarrow{\pi} W_{r,s} \longrightarrow 0 \tag{6.1}$$

and

$$0 \longrightarrow W_{r,s} \xrightarrow{i} U_{r,s} \xrightarrow{\pi'} V_{r,s} \longrightarrow 0 \, . \tag{6.2}$$

As in [3], given a prime $\alpha \in \mathcal{O}$ such that $(\alpha, \mathfrak{a}) = 1$, we define an action of the Hecke algebra $\mathbb{H}$ on the *g-fold twist* $\mathbb{F}_\ell(g)$ of the trivial Δ-module $\mathbb{F}_\ell$ by

$$T_\alpha(v) = N(\alpha)^g(N(\alpha)+1)v.$$

Note that $N(\alpha)+1$ is the index of Γ_α in Γ. Recall that $\Gamma_\alpha = \Gamma \cap \tilde{\alpha}^{-1}\Gamma\tilde{\alpha}$ where $\tilde{\alpha} = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Proposition 6.11. *For any nonnegative integers r, s, we have the following isomorphism as $\mathbb{H}$-modules:*

$$H^0(\Gamma, I_{r,s}) \cong \begin{cases} \mathbb{F}_\ell(\ell-1) & \text{if } r \equiv s \equiv 0 \pmod{\ell-1} \\ 0 & \text{otherwise} \end{cases}$$

Proof. By the discussion above, one can identify $I_{r,s}$ with the set of maps $\varphi : \mathbb{F}_\ell^2 \times \bar{\mathbb{F}}_\ell^2 \to \mathbb{F}_\ell$ satisfying

$$\varphi(x,0) = \varphi(0,y) = 0 \qquad \text{and} \qquad \varphi(cx, dy) = c^r d^s \varphi(x,y)$$

for all $x, y \in \mathbb{F}_\ell^2$ and $c, d \in \mathbb{F}_\ell$.

One can show that Γ acts transitively on $S = (\mathbb{F}_\ell \times \mathbb{F}_\ell)^2 \backslash \{((a,0),(c,0)),((0,a'),(0,c'))\}$. This implies that for any such map $\varphi \in I_{r,s}^\Gamma = H^0(\Gamma, I_{r,s})$, there exists a $c \in \mathbb{F}_\ell$ such that $\varphi(x,y) = c$ for all $(x,y) \in S$.

When $r \equiv s \equiv 0 \pmod{\ell-1}$, any given $c \in \mathbb{F}_\ell$ induces an element of $H^0(\Gamma, I_{r,s})$ as above and this implies that $H^0(\Gamma, I_{r,s}) \cong \mathbb{F}_\ell$ as $\mathbb{F}_\ell$-vector spaces. One can easily check that the action of the Hecke algebra on $\mathbb{F}_\ell$ is as prescribed above.

Suppose that $r \not\equiv 0 \pmod{\ell-1}$ or $s \not\equiv 0 \pmod{\ell-1}$. Assume $H^0(\Gamma, I_{r,s}) \neq 0$ for a contradiction. Let $\varphi \in H^0(\Gamma, I_{r,s})$ be a nonzero element. Again, by the transitivity of the action of Γ, $\varphi(x,y) = c \neq 0$ for all $(x,y) \in S$ and for some nonzero $c \in \mathbb{F}_\ell$. In particular, for all $a, b \in \mathbb{F}_\ell$ we have

$$a^r c = a^r \varphi(x,x) = \varphi(ax,x) = \varphi(x,x) = \varphi(x,bx) = b^s \varphi(x,x) = b^s c.$$

This gives a contradiction, and the vanishing of $H^0(\Gamma, I_{r,s})$.

One can check that the action of the Hecke algebra on the cohomology is as described above. □

Lemma 6.12. *Assume $0 \leq r, s \leq \ell - 1$. Then, we have (as $\mathbb{H}$-modules)*

$$H^0(\Gamma, E_{r,s}) = \begin{cases} \mathbb{F}_\ell & \text{if } r = s = 0 \\ 0 & \text{otherwise} \end{cases}$$

Proof. The claim is obvious when $(r, s) = (0, 0)$. Assume $(r, s) \neq (0, 0)$ and $(r, s) \neq (\ell - 1, \ell - 1)$. Then, the exact sequence (6.1) induces the following exact sequence

$$0 \to H^0(\Gamma, E_{r,s}) \to H^0(\Gamma, I_{r,s}).$$

By Proposition 6.11, $H^0(\Gamma, I_{r,s}) = 0$ and so is $H^0(\Gamma, E_{r,s})$.

Assume $(r, s) = (\ell - 1, \ell - 1)$. We have the isomorphism $E_{\ell-1,\ell-1} \cong (\mathcal{O}/\ell)[x, y]_{\ell-1}$. On the other hand, in [14], Dickson showed that Γ invariants of $\tilde{E}_*$ are generated by $X^\ell Y - XY^\ell$and $\sum_{i=0}^{\ell}(X^{\ell-i}Y^i)^{\ell-1}$. This implies that $H^0(\Gamma, E_{\ell-1,\ell-1}) = 0$. □

Lemma 6.13. *Let $0 \leq r, s \leq \ell - 1$. Then, we have (as $\mathbb{H}$-modules)*

$$H^0(\Gamma, U_{r,s}) = \begin{cases} \mathbb{F}_\ell(\ell-1) \oplus \mathbb{F}_\ell(\ell-1) & \text{if } (r, s) = (\ell - 1, \ell - 1) \\ \mathbb{F}_\ell(\ell-1) & \text{if } (r, s) = (0, \ell - 1) \text{ or } (\ell - 1, 0) \\ 0 & \text{otherwise} \end{cases}$$

Proof. Set $U^1 := E_{\ell-1-r}(r) \otimes I_s$ and $U^2 = I_r \otimes E_{\ell-1-s}(s)$. Then, $U_{r,s} = U^1 \oplus U^2$ and $H^0(\Gamma, U^1) \oplus H^0(\Gamma, U^2)$.

Assume (r, s) is not of $(\ell - 1, \ell - 1)$, $(0, \ell - 1)$ and $(\ell - 1, 0)$. Then, tensoring the exact sequence in Lemma 6.5 with $E_{\ell-1-r}(r)$, we get the following short exact sequence

$$0 \longrightarrow E_{\ell-1-r}(r) \otimes E_s \longrightarrow U^1 \longrightarrow V_{r,s} \longrightarrow 0\,.$$

This induces the following long exact sequence

$$0 \longrightarrow H^0(\Gamma, E_{\ell-1-r}(r) \otimes E_s) \longrightarrow H^0(\Gamma, U^1) \longrightarrow H^0(\Gamma, V_{r,s}).$$

Since $V_{r,s} \cong E_{\ell-1-r,\ell-1-s}$ as Γ-modules, by Lemma 6.12, $H^0(\Gamma, V_{r,s}) = 0$. On the other hand, by Lemma 6.12, $H^0(\Gamma, E_{\ell-1-r}(r) \otimes E_s) = 0$ and $H^0(\Gamma, U^1) = 0$. Likewise, one tensors the exact sequence in Lemma 6.5 with $E_{\ell-1-s}(s)$ and gets $H^0(\Gamma, U^2) = 0$, hence the vanishing of $H^0(\Gamma, U_{r,s})$.

Now, assume $(r, s) = (\ell - 1, 0)$. Then, by Lemma 6.12, $H^0(\Gamma, E_{\ell-1-r}(r) \otimes E_s) \cong \mathbb{F}_\ell$ and $H^0(\Gamma, V_{r,s}) = 0$. Using the exact sequence of cohomology groups above, we conclude that $H^0(\Gamma, U^1) \cong \mathbb{F}_\ell$ as vector spaces. Likewise, one gets $H^0(\Gamma, U^2) = 0$.

In case $(r, s) = (0, \ell - 1)$, one proceeds exactly as above and gets $H^0(\Gamma, U^1) = 0$ and $H^0(\Gamma, U^2) = \mathbb{F}_\ell$.

Finally assume $(r, s) = (\ell - 1, \ell - 1)$. In this case, $H^0(\Gamma, E_{\ell-1-r}(r) \otimes \bar{E}_s) = 0$ and $H^0(\Gamma, V_{r,s}) \cong \mathbb{F}_\ell$ by Lemma 6.12. One can easily see that $\pi'|_{U^1} : U^1 \to V_{r,s}$ is surjective and so $H^0(\Gamma, U^1) \cong \mathbb{F}_\ell$ as vector spaces. Exactly in the same way, one gets $H^0(\Gamma, U^2) \cong \mathbb{F}_\ell$ (as vector spaces). One checks the action of the Hecke algebra and completes the proof. □

Proposition 6.14. *Let $0 \leq r, s \leq \ell - 1$. Then, we have (as $\mathbb{H}$-modules)*

$$H^0(\Gamma, W_{r,s}) = \begin{cases} \mathbb{F}_\ell & \text{if } (r,s) = (\ell-1,\ell-1), (0,\ell-1) \text{ or } (\ell-1,0) \\ 0 & \text{otherwise} \end{cases}$$

Proof. First of all, the exact sequence (6.2) above induces the following long exact sequence of $\mathbb{H}$-modules in cohomology

$$0 \longrightarrow H^0(\Gamma, W_{r,s}) \xrightarrow{i_*} H^0(\Gamma, U_{r,s}) \xrightarrow{\pi'_*} H^0(\Gamma, V_{r,s}) \longrightarrow H^1(\Gamma, W_{r,s}) \,.$$

Assume $(r,s) = (0, \ell-1)$ or $(\ell-1, 0)$. Then, by Lemma 6.12, $H^0(\Gamma, V_{r,s}) = 0$. The proof immediately follows from Lemma 6.13.

Assume $(r,s) = (\ell-1, \ell-1)$. Then, by Lemma 6.12, $H^0(\Gamma, V_{r,s}) \cong \mathbb{F}_\ell$ and, by Lemma 6.13, $H^0(\Gamma, U_{r,s}) \cong \mathbb{F}_\ell \oplus \mathbb{F}_\ell$. Using the definition, one can easily see that π'_* is surjective and gets the desired result using the exact sequence of cohomology groups above.

Finally, assume (r,s) is not equal to one of $(0, \ell-1)$, $(\ell-1, 0)$ and $(\ell-1, \ell-1)$. Then, by Lemma 6.13, $H^0(\Gamma, U_{r,s}) = 0$ and, using the exact sequence above, we complete the proof. □

We are now ready to prove our main result:

Theorem 6.15. *Let Φ be a Hecke eigenvalue system occurring in $H^1(\Gamma, E)$ where E is a finite dimensional $\mathbb{F}_\ell[SL_2(\mathcal{O}/(\ell))]$-module. Then Φ occurs in $H^1(\Gamma_2, \mathbb{F}_\ell)$.*

Proof. Let $0 \leq r, s \leq \ell - 1$. We first claim that there exists an injection of $\mathbb{H}$-modules

$$H^1(\Gamma, E_{r,s}) \hookrightarrow H^1(\Gamma_2, \mathbb{F}_\ell).$$

Exact sequence (6.1) induces the following long exact sequence of $\mathbb{H}$-modules

$$0 \longrightarrow H^0(\Gamma, E_{r,s}) \xrightarrow{\iota_*} H^0(\Gamma, I_{r,s}) \xrightarrow{\pi'_*} H^0(\Gamma, W_{r,s}) \longrightarrow H^1(\Gamma, E_{r,s}) \longrightarrow H^1(\Gamma, I_{r,s}) \,.$$

On the other hand, by Lemma 6.7 and Lemma 6.8, $I \otimes I \cong Ind_{\Gamma_2}^{\Gamma} \mathbb{F}_\ell$, and the natural injection $I_{r,s} \hookrightarrow I \otimes I$ with Shapiro's lemma induces the following injective morphism of $\mathbb{H}-$modules

$$H^1(\Gamma, I_{r,s}) \hookrightarrow H^1(\Gamma, I \otimes I) \cong H^1(\Gamma_2, \mathbb{F}_\ell).$$

Therefore, it suffices to show that the map $H^1(\Gamma, E_{r,s}) \to H^1(\Gamma, I_{r,s})$ is injective; this is what we do below.

Assume that (r,s) is equal to one of the tuples $(0,\ell-1)$, $(\ell-1,0)$ or $(\ell-1,\ell-1)$. Then, by Lemma 6.12, $H^0(\Gamma,E_{r,s})=0$; by Lemma 6.11, $H^0(\Gamma,I_{r,s})\cong\mathbb{F}_\ell$ and, by Proposition 6.14, $H^0(\Gamma,W_{r,s})\cong\mathbb{F}_\ell$ (as vector spaces). By the definition, π'_* is surjective and thus we get the claim. Otherwise, by Proposition 6.14, $H^0(\Gamma,W_{r,s})=0$ and this completes the proof of the claim.

Now, by Lemma 6.3, we can assume that E is an absolutely irreducible $\mathbb{F}_\ell[\mathrm{SL}_2(\mathcal{O}/(\ell))]$-module. Since absolutely irreducible $\mathbb{F}_\ell[\mathrm{SL}_2(\mathcal{O}/(\ell))]$-modules are the ones $E_{r,s}$ with $0\leq r,s\leq\ell-1$, we are done. □

For congurence subgroups of $SL_2(\mathbb{Z})$, the following result is first proved by Tate-Serre for level 1 (unpublished), by Jochnowitz [25] for prime levels less than 19 and for arbitrary level by Ash-Stevens [3].

Corollary 6.16. *The set of Hecke eigenvalue systems occuring in $H^1(\Gamma_1(\mathfrak{a}),E)$ for fixed $\mathfrak{a}$ and varying E, where E is a finite dimensional $\mathbb{F}_\ell[SL_2(\mathcal{O}/(\ell))]$-module, is finite.*

It is natural to ask whether increasing the level by (ℓ) is optimal. In other words, are there eigenvalue systems with nontrivial weight that do not occur with trivial weight when the level is increased by (λ) or $(\bar{\lambda})$. Now we present an example of such an eigenvalue system.

Example 6.17. *Let $K=\mathbb{Q}(\omega)$ where $\omega=\sqrt{-2}$. Using the algorithms explained in Chapter 8, we find an eigenform v in $H^1(\Gamma_0(1),E_{10,10}(\mathbb{F}_{11}))$. The following table gives eigenvalues Φ_α of v for the first few Hecke operators T_α.*

Note that we have $11=(3+\omega)(3-\omega)$. The spaces $H^1(\Gamma_0(3+\omega),\mathbb{F}_{11})$ and $H^1(\Gamma_0(3-\omega),\mathbb{F}_{11})$ are isomorphic and they are two dimensional. Our eigenvalue system Φ does not occur in these spaces. Next, we want to examine $H^1(\Gamma_0(11),\mathbb{F}_{11})$. Our programs

Table 8: An eigenvalue system in $H^1(\Gamma_0(1), E_{10,10}(\mathbb{F}_{11}))$

α	ω	$1+\omega$	$1-\omega$	$3+2\omega$	$3-2\omega$	$1+3\omega$	$1-3\omega$	$3-4\omega$	$3-4\omega$
Φ_α	*9*	*10*	*10*	*9*	*9*	*0*	*0*	*5*	*5*

are not written for composite levels. Looking at the tables of Cremona [12], we find an eigenvector in $H1(\Gamma_0(11), \mathcal{O}_K)$ *with the following eigenvalues* Ψ_α.

Table 9: An eigenvalue system in $H^1(\Gamma_0(11), \mathbb{C})$

α	ω	$1+\omega$	$1-\omega$	$3+2\omega$	$3-2\omega$	$1+3\omega$	$1-3\omega$	$3-4\omega$	$3-4\omega$
Ψ_α	*-2*	*-1*	*-1*	*-2*	*-2*	*0*	*0*	*-6*	*-6*

Reducing these eigenvalues mod 11*, we get an eigenvalue system in* $H^1(\Gamma_0(11), \mathbb{F}_{11})$ *that matches our level 1 weight* $(10, 10)$ *eigenvalue system* Φ.

Chapter 7

Proof of the Nonexistence Result

In this chapter, we present a proof of Theorem 4.3 following very closely our paper [43].

Let K be a number field and p be a rational prime. We say that the pair (K, p) satisfies (†), if there is no irreducible continuous representation of $Gal(\overline{K}/K)$ into $GL_2(\overline{\mathbb{F}}_p)$ that is unramified away from (p, ∞).

A natural problem related to the conjectures we listed in Chapter 3 is to know which pairs (K, p) satisfy (†) and which pairs do not.

Let $\rho : Gal(\overline{K}/K) \to GL_2(\overline{\mathbb{F}}_p)$ be continuous and unramified away from $\{p, \infty\}$. Then the field L corresponding to $Ker(\rho)$ is a finite extension of K unramified away from $\{p, \infty\}$ and we get an embedding of $Gal(L/K)$ into some $GL_2(\mathbb{F}_{p^a})$. In this paper we investigate the case where K is quadratic and $p = 2, 3$.

In Section 7.1, we look at the case where $p = 2$ and the extension L/K is nonsolvable. Let $d_{K/\mathbb{Q}}$ denote the discriminant of K over $\mathbb{Q}$.

Theorem A. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field and let L/K be a nonsolvable Galois extension unramified over every odd prime whose Galois group embeds into some $GL_2(\mathbb{F}_{2^a})$. If $d = 6, 5, 3, 2, -1, -2, -3, -5, -6$ then no such L exists.*

Brueggeman [10] proved Theorem A for $d = -2, -1, 2$. In Section 7.2, we treat the case where $p = 2$ and L/K is solvable for the fields reported in Theorem A.

Theorem B. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field and let L/K be a solvable Galois extension unramified over every odd prime. Assume that there is an embedding $\rho : Gal(L/K) \hookrightarrow GL_2(\mathbb{F}_{2^a})$ for some a. If $d = 6, 5, 3, 2, -1, -2, -3, -5, -6$ then the embedding ρ is reducible.*

Putting these two theorems together, we get the following result.

Corollary. *For $d = 6, 5, 3, 2, -1, -2, -3, -5, -6$, the pair $(\mathbb{Q}(\sqrt{d}), 2)$ satisfies (†).*

In Section 7.3, we focus on $p = 3$.

Theorem C. *The pair $(\mathbb{Q}(\sqrt{-3}), 3)$ satisfies (†).*

We follow ideas of Tate [54] to prove the theorems. The proof of Theorem A is based on comparing upper and lower bounds of discriminants. Using a discriminant upper bound of Moon [34], one proves Theorem A for fields $d = 5, 3, 2, -1, -2, -3$. To also get the fields $d = 6, -5, -6$, we use part of a sharp upper bound calculation of Moon and Taguchi who studied the same problem for $p = 2$ in their article [36] which was a preprint at the time we proved this result. For Theorem B, we use class field theory and the computer algebra system MAGMA. In Section 4, we prove Theorem C by applying the methods of the first two theorems to $p = 3$. In Section 7.4, we use Theorem B to show the nonexistence of elliptic curves with good reduction everywhere over certain quadratic fields.

7.1 Nonsolvable Case, $p = 2$

We start with the discriminant upper bound of Moon [34].

Lemma 1. *Let F be a finite extension of $\mathbb{Q}_p$ with ramification index e. Suppose E/F is a finite extension with an elementary p-abelian Galois group of order p^m where $m \geq 1$. Then the different $\mathcal{D}_{E/F}$ of E/F divides $(p)^c$ where*

$$c \leq \left(1 + \frac{\alpha}{e}\right)\left(1 - \frac{1}{p^m}\right)$$

and $\alpha = \left[\frac{e}{p-1}\right] + 1$. (here $[x]$ denotes the maximal integer $\leq x$)

Observe that for $p = 2$, the above upper bound takes a simple form: $c \leq \big(2+1/e)(1-1/2^m)$.

Corollary 1. *Let F be the unramified extension of $\mathbb{Q}_2$. Let E/F be a finite Galois extension with ramification index $e2^m$ with e odd and $m \geq 1$. Assume that the Galois group G of E/F embeds into $GL_2(\mathbb{F}_{2^a})$ for some a. Then the different $\mathcal{D}_{E/F}$ of E/F divides $(2)^c$ where*

$$c \leq 3 - \frac{1}{2^{m-1}} - \frac{1}{e2^m}$$

Proof. Let E_1 (resp. E_0) be the maximal tamely ramified (resp. unramified) subextension of E/F. Normalize the valuation so that $v(2) = 1$. It is well known that $v(\mathcal{D}_{E_1/E_0}) = (e-1)/e$. As the 2-Sylow subgroups of $GL_2(\mathbb{F}_{2^a})$ are elemantary 2-abelian, so is the Galois group of the extension E/E_1. Now by Lemma 1 we have

$$v(\mathcal{D}_{E/E_1}) \leq \left(2 + \frac{1}{e}\right)\left(1 - \frac{1}{2^m}\right)$$

Combining the two differents we get

$$\begin{aligned} v(\mathcal{D}_{E/F}) &\leq \left(2 + \frac{1}{e}\right)\left(1 - \frac{1}{2^m}\right) + \left(\frac{e-1}{e}\right) \\ &\leq 3 - \frac{1}{2^{m-1}} - \frac{1}{e2^m} \end{aligned}$$

□

For ramified case, we will use the following upper bounf from [36].

Lemma 2. *Let F be a ramified quadratic extension of $\mathbb{Q}_2$. Let E/F be a finite Galois extension with ramification index $e2^m$ with e odd and $m \geq 1$. Assume that the Galois group G of E/F embeds into $GL_2(\mathbb{F}_{2^a})$ for some a. Then the different $\mathcal{D}_{E/F}$ of E/F divides $(2)^c$ where*

$$c \leq \frac{9}{4} - \frac{1}{2^{m-1}}$$

Proposition 1. *Let K be a quadratic number field and L be a finite Galois extension of K of degree n which is unramified over every odd prime with wild ramification index 2^m with $m \geq 1$. Assume $Gal(L/K)$ embeds into $GL_2(\mathbb{F}_{2^a})$ for some a. Then $|d_{L/\mathbb{Q}}| \leq |d_{K/\mathbb{Q}}|^n 2^{2cn}$ where*

(a) if 2 is ramified in K, then $c \leq \frac{9}{4} - \frac{1}{2^{m-1}}$

(b) if 2 is inert K, then $c \leq 3 - \frac{1}{2^{m-1}} - \frac{1}{e2^m}$

Proof. We take a place $\mathfrak{p}$ of K over 2 and a place $\mathfrak{q}$ of L over $\mathfrak{p}$. We complete K and L at $\mathfrak{p}$ and $\mathfrak{q}$ respectively and get an extension of local fields. We apply Corollary 1 or Lemma 2 to this local extension depending on the ramification of 2 in $K/\mathbb{Q}$. The claim follows by passing from local to global discriminant and by the fact that $d_{L/\mathbb{Q}} = (d_{K/\mathbb{Q}})^{[L:K]} \operatorname{Norm}_{K/\mathbb{Q}}(d_{L/K})$. Note that $\operatorname{Norm}_{K/\mathbb{Q}}(2) = 2^2$ in both cases. □

For lower bounds on discriminants we will use the Odlyzko-Poitou bounds [41]. Let $L/\mathbb{Q}$ be of degree m. Then

$$\gamma + \log(4\pi) - 6.860404m^{-2/3} \leq \frac{1}{m}\log(|d_{L/\mathbb{Q}}|)$$

where γ is the Euler constant.

We compare these upper and lower bounds in the nonsolvable case now. Let K be a quadratic field and let L/K be a nonsolvable Galois extension ramified only over $\{2, \infty\}$ whose Galois group G embeds into $GL_2(\mathbb{F}_{2^a})$ for some a. Let n be the degree of L/K. Note that the degree of $L/\mathbb{Q}$ is $2n$.

Assume that 2 is ramified in $K/\mathbb{Q}$. If L/K is at most tamely ramified, then $d_{L/K}$ divides $\mathfrak{p}^n$ where $\mathfrak{p}$ is a place of K over 2. Since the norm of $\mathfrak{p}$ is 2, $|d_{L/\mathbb{Q}}| \leq |d_{K/\mathbb{Q}}|^n 2^n$. Thus

$$2(\gamma + \log(4\pi) - 6.860404(2n)^{-2/3}) \leq \log|d_{K/\mathbb{Q}}| + \log 2$$

As G is nonsolvable, $n \geq 60$. For $|d_{K/\mathbb{Q}}| \leq 2^{128}$, this inequality gives a contradiction for all $n \geq 60$.

Now assume that L/K is wildly ramified with ramification index 2^m. Using Lemma 2, we have

$$2(\gamma + \log(4\pi) - 6.860404(2n)^{-2/3}) \leq \log|d_{K/\mathbb{Q}}| + 2c\log 2$$

where $c = \frac{9}{4} - \frac{1}{2^{m-1}}$.

As Tate observes in [54], we have $\frac{n}{2^{m-1}} \geq 30$ because 2^m divides n and n is divisible by at least three distinct primes as it is the order of a nonsolvable group. Now we get

$$2\left(.5772 + 2.53102 - \frac{6.860404}{2^{2/3}n^{2/3}}\right) \leq \log|d_{K/\mathbb{Q}}| + 1.386295\left(2.125 - \frac{30}{n}\right)$$

$$6.216448 - \frac{8.64356}{n^{2/3}} \leq \log|d_{K/\mathbb{Q}}| + 2.94587 - \frac{41.588}{n}$$

$$3.27057 + f(n) \leq \log |d_{K/\mathbb{Q}}|$$

where $f(x) = \frac{A - Bx^{1/3}}{x}$ with $A = 41.588$ and $B = 8.64356$. The function $f(x)$ decreases until it reaches its minimum at $x_0 = (\frac{3A}{2B})^3 \approx 375.923$ with minimum value $f_{min} = \frac{-A}{2x_0}$ and then it increases approaching 0 as x tends to infinity. So, if $\log |d_{K/\mathbb{Q}}| \leq 3.27057 + f_{min} \approx 3.21525$, the last inequality gives a contradiction for any $n \geq 60$. Thus we get $|d_{K/\mathbb{Q}}| < 24.9$, proving the claim for the fields $K = \mathbb{Q}(\sqrt{d})$ with $d = 6, 3, 2, -1, -2, -5, -6$.

Now assume that 2 is inert in $K/\mathbb{Q}$. As $e2^m$ is the order of the solvable local inertia group, its index in nonsolvable G has to be at least 3, thus $\frac{n}{e2^m} \geq 3$. Using Corollary 1, we get

$$6.216448 - \frac{8.64356}{n^{2/3}} \leq \log |d_{K/\mathbb{Q}}| + 1.386295\left(3 - \frac{30}{n} - \frac{3}{n}\right)$$

$$2.057563 + g(n) \leq \log |d_{K/\mathbb{Q}}|$$

where $g(x) = \frac{A - Bx^{1/3}}{x}$ with $A = 45.7477$ and $B = 8.64356$. The minimum value of $g(x)$ is attained at $x_0 \approx 500.385$. If $\log |d_{K/\mathbb{Q}}| \leq 2.057563 + g_{min} \approx 2.011863$, the last inequality gives a contradiction for any $n \geq 60$. Thus we get $|d_{K/\mathbb{Q}}| < 7.477$, proving the claim for the fields $K = \mathbb{Q}(\sqrt{d})$ with $d = -3, 5$.

This completes the proof Theorem A.

7.2 Solvable Case, $p = 2$

Let L/K be a solvable Galois extension with Galois group G that is ramified only over $\{2, \infty\}$. Assume that there is an embedding $\rho : G \hookrightarrow GL_2(\mathbb{F}_{2^a})$ for some a. If we show that G is a 2-group then a conjugate of the image of G will be inside the Sylow 2-subgroup $T = \{\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) |\ x \in \mathbb{F}_{2^a}\}$ of $GL_2(\mathbb{F}_{2^a})$. Thus ρ will be reducible.

Let S be a 2-Sylow subgroup of G. Then S is elementary 2-abelian as T is. Let G' be the commutator subgroup of G. To show that G is a 2-group, it is enough to show that G/G' and G'/G'' are 2-groups. If they are, then G/G'' is a 2-group and it is abelian as it is a homomorphic image of S. Indeed, $G/G'' \backsimeq SG''/G'' = S/S \cap G''$. Hence $G' = G''$. Since G is solvable, we have $G' = 1$ and thus G is a 2-group.

In the rest of this section, $K = \mathbb{Q}(\sqrt{d})$ *with* $d = 6, 5, 3, 2, -1, -2, -3, -5$ *or* -6.

Observe that 2 is either inert ($d = -3, 5$) or ramified in $K/\mathbb{Q}$. Let $\mathfrak{p}$ denote the only place of K above 2. We will prove that G/G' and G'/G'' are 2-groups.

Proposition 2. *The ray class group of* K *with modulus* $\mathfrak{p}^k\mathfrak{m}_\infty$ *is a* 2*-group for any* k *where* $\mathfrak{m}_\infty$ *is the modulus of all the real archimedean places of* K.

Proof. Let $\mathcal{O}_K$ be the ring of integers of K and U be the group of units of $\mathcal{O}_K$. Let $\mathrm{Cl}(K)$ be the ideal class group of K and let $\mathrm{Cl}(K, \mathfrak{p}^k\mathfrak{m}_\infty)$ be the ray class group of K of modulus $\mathfrak{p}^k\mathfrak{m}_\infty$ with fixed positive integer k.

We have the following exact sequence from class field theory

$$(*) \quad U \to (\mathcal{O}_K/\mathfrak{p}^k)^* \times |\mathbb{Z}/2\mathbb{Z}|^{|\mathfrak{m}_\infty|} \to \mathrm{Cl}(K, \mathfrak{p}^k\mathfrak{m}_\infty) \to \mathrm{Cl}(K) \to 1$$

It is known that the prime to 2 part of $(\mathcal{O}_K/\mathfrak{p}^k)^*$ is $\mathbb{Z}/(2^f - 1)\mathbb{Z}$ where f is the

residue degree of $\mathfrak{p}$. Thus if 2 is ramified in K, then $(\mathcal{O}_K/\mathfrak{p}^k)^*$ is a 2-group. Since the class numbers of K's are all powers of 2, the result follows in this case. If 2 is inert, there may be a non-trivial 3-part of the ray class group. Note that the 3-rank is the same for every k. For the two inert fields, we verify with MAGMA that the ray class group with modulus $(2)\mathfrak{m}_\infty$ has 3-rank zero for all d's. □

Let F be the fixed field of G'. Then F is an abelian extension of K that is ramified only over $\{2, \infty\}$ and F is contained in a ray class field of K with modulus $\mathfrak{p}^k\mathfrak{m}_\infty$ for some k. By Proposition 2, such a ray class field has degree power of 2 over K. Thus G/G' is a 2-group.

The group G'/G'' corresponds to an abelian extension of F that is only ramified over $\{2, \infty\}$ and thus is contained in a ray class field of F with modulus $(2)^k\mathfrak{m}_\infty$ for some k. Using MAGMA, we will verify for each possible F that these ray class groups are 2-groups and conclude that G'/G'' is a 2-group. First, we use the following theorem of Nakagoshi [38] to find a field A which contains all possible F's.

Theorem 1. *Let N be a number field with ramification index e and residue degree f over the rational prime p and let $\mathfrak{p}$ be a prime ideal of the ring of integers $\mathcal{O}$ of N over p. Set $e_1 = \left[\dfrac{e}{p-1}\right]$ where $[x]$ is the maximal integer $\leq x$. Let $N_\mathfrak{p}$ denote the completion of N at $\mathfrak{p}$. Then the p-rank R_n of $(\mathcal{O}/\mathfrak{p}^{n+1})^*$ is given by*

$$\begin{aligned} R_n &= \left(n - \left[\frac{n}{p}\right]\right)f, && \text{if } 0 \leq n < e + e_1 \\ R_n &= ef, && \text{if } n \geq e + e_1 \text{ and } \zeta_p \notin N_\mathfrak{p} \\ R_n &= ef + 1, && \text{if } n \geq e + e_1 \text{ and } \zeta_p \in N_\mathfrak{p} \end{aligned}$$

Combining this result with the exact sequence $(*)$, we see that the 2-ranks of ray class groups of modulus $(2)^k\mathfrak{m}_\infty$ stabilize after $k = 5$ for every quadratic field. Thus

there exists a maximal elementary 2-abelian extension A of K that is only ramified over $\{2, \infty\}$. As G/G' is elementary 2-abelian (it is a homomorphic image of S), F is a subfield of A. For every d, we list a defining polynomial of A over $\mathbb{Q}$, class number h of A and the decomposition (e, f, g) of 2 in $A/\mathbb{Q}$.

Table 10: Maximal elementary 2-abelian extensions ramified only over $\{2, \infty\}$

d	**A**	**h**	**e,f,g**
6	$x^{16} + 4x^{12} + 15x^8 + 4x^4 + 1$	1	8,2,1
5	$x^{16} - 12x^{14} + 58x^{12} - 29x^8 + 58x^4 + 12x^2 + 1$	1	8,2,1
3	$x^{16} + 4x^{14} + 56x^{12} + 36x^{10} + 542x^8 + 636x^6 + 248x^4 + 28x^2 + 1$	1	8,2,1
2	$x^{16} + 4x^{12} + 40x^{10} + 104x^8 + 112x^6 + 56x^4 + 16x^2 + 4$	1	16,1,1
-1	$x^8 + 4x^6 + 22x^4 + 4x^2 + 1$	1	8,1,1
-2	$x^8 + 4x^6 + 10x^4 - 20x^2 + 9$	1	8,1,1
-3	$x^8 - 10x^6 + 31x^4 - 6x^2 + 9$	1	4,2,1
-5	$x^8 + 32x^6 + 248x^4 + 512x^2 + 16$	1	4,2,1
-6	$x^8 + 24x^6 + 248x^4 - 288x^2 + 2704$	1	4,2,1

We compute the class numbers of all subfields of A for every d and see that they are all powers of 2.

From Table 10, we see that residue degree f of 2 in A is either 1 or 2. We also observe that each subfield of A has only one place over 2. By the exact sequence $(*)$, we see that for the subfields of A with $f = 1$, the 3-rank of its ray class group with modulus $(2)^k\mathfrak{m}_\infty$ will be 0. For the subfields of A with $f = 2$ which contain K, we check the 3-rank of their ray class groups with modulus $(2)\mathfrak{m}_\infty$ and see that it is 0 in all instances. This shows that G'/G'' is a 2-group for all the quadratic fields listed in Theorem B and thus completes the proof of Theorem B.

7.3 The Case $p = 3$

We apply Lemma 1 to the case $p = 3$ and get the following:

Proposition 3. *Let K be a quadratic field ramified over 3 and L be a finite Galois extension of K of degree n which is unramified away from $\{3, \infty\}$. Let the ramification index of L/K be $e3^m$ with $m \geq 1$ and $(e, 3) = 1$. Assume $Gal(L/K)$ embeds into some $GL_2(\mathbb{F}_{3^a})$. Then $|d_{L/\mathbb{Q}}| \leq |d_{K/\mathbb{Q}}|^n 3^{2cn}$ where*

$$c \leq 2 - \frac{1}{2 \cdot 3^{m-1}} - \frac{1}{2e \cdot 3^m}$$

Proof. Just as in the proof of Proposition 1, we look at the local differents. We suitably complete K and L over 3 to get the local extension E/F. Let E_1 (resp. E_0) be the maximal tamely ramified (resp. unramified) subextension of E/F. Normalize the valuation so that $v(3) = 1$. We have $v(\mathcal{D}_{E_1/E_0}) = (e-1)/2e$. $\mathrm{Gal}(E/E_1)$ is an elementary 3-abelian group and by Lemma 1, we see that $\mathcal{D}_{E/F}$ divides $(3)^c$ where

$$\begin{aligned} c &\leq \left(1 + \frac{\alpha}{2e}\right)\left(1 - \frac{1}{3^m}\right) + \frac{e-1}{2e} \\ &\leq \left(1 + \frac{1}{2} + \frac{1}{2e}\right)\left(1 - \frac{1}{3^m}\right) + \frac{1}{2} - \frac{1}{2e} \\ &\leq \frac{3}{2} + \frac{1}{2} - \frac{1}{2 \cdot 3^{m-1}} - \frac{1}{2e \cdot 3^m} \end{aligned}$$

We pass to the local and then to global discriminant and get the desired result. □

We follow Section 7.1 and Section 7.2 to prove Theorem C. Let L/K be an extension satisfying the hypothesis of Proposition 3. Assume that L/K is nonsolvable. Using the lower bound of Section 7.1, we get

$$6.216448 - \frac{8.64356}{n^{2/3}} \leq \log|d_{K/\mathbb{Q}}| + 2.197225\left(2 - \frac{33}{2n}\right)$$

$$1.82198 + h(n) \leq \log|d_{K/\mathbb{Q}}|$$

where $h(x) = \frac{A - Bx^{1/3}}{x}$ with $A = 41.36.254$ and $B = 8.64356$. The minimum is attained at $x_0 \approx 249.041$. For $\log|d_{K/Q}| < 1.82198 + h_{min} \approx 1.749$, the last inequality gives a contradiction for any $n \geq 60$. Thus we get $|d_{K/\mathbb{Q}}| < 5.7$, only giving $\mathbb{Q}(\sqrt{-3})$.

Now let $L/\mathbb{Q}(\sqrt{-3})$ be a solvable extension satisfying the hypothesis of Proposition 3. Let G be the Galois group of this extension. We want to show that G/G' and G'/G'' are both 3-groups following Section 3. By the exact sequence $(*)$ of Section 3, we see that any ray class group of $\mathbb{Q}(\sqrt{-3})$ with modulus $(3)^k\mathfrak{m}_\infty$ is a 3-group because the class number of $\mathbb{Q}(\sqrt{-3})$ is 1 and it has no infinite places and residue degree of 3 is one. Thus G/G' is a 3-group. Now let A be the maximal elementary 3-abelian extension of $\mathbb{Q}(\sqrt{-3})$ that is unramified over $\{3, \infty\}$. Using MAGMA, we find a defining polynomial for A over $\mathbb{Q}$: $x^{18} - 9x^{15} + 135x^{12} + 540x^9 + 2673x^6 + 1458x^3 + 729$. The decomposition of 3 in $A/\mathbb{Q}$ is $(18, 1, 1)$ which means for any subfield the residue degree of 3 is one as well. We verify that all subfields of A containing K have class number 1 and have no real infinite places. As in Section 7.2, we conclude that G'/G'' is a 3-group. This proves Theorem C.

7.4 Application to Elliptic Curves over Quadratic Fields

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Assume that E is an elliptic curve over K that has good reduction away from 2. Let G be the Galois group of the finite extension $K(E[2])/K$ where $K(E[2])$ is the extension of K obtained by adjoining coordinates of points of E that are of order 2. It is well known that there is a continuous representation

$$\rho : G \hookrightarrow GL_2(\mathbb{F}_2)$$

which is ramified away from 2. If $d = 6, 5, 3, 2, -1, -2, -3, -5, -6$ then by the proof of Theorem B, G must be a 2-group. This implies that G is either trivial or it is $\mathbb{Z}/2$. This is true only if E has a K-rational point of order 2. Thus we showed that

Proposition 4. *For $d = 6, 5, 3, 2, -1, -2, -3, -5, -6$, if E is an elliptic curve over K that has good reduction away from 2 then E has a K-rational point of order 2.*

This extends results of Pinch [39] and Kida [30].

An elliptic curve E over K is called *admissible* if the following conditions are satisified:

(1) E has good reduction everywhere over K

(2) E has a K-rational point of order 2

Comalada [11] showed that for $1 < d < 100$, there exists an admissible elliptic curve over $\mathbb{Q}(\sqrt{d})$ if and only if $d = 6, 7, 14, 22, 38, 41, 65, 77, 86$. Setzer [49] showed that for $d < 0$, there exists an admissible elliptic curve over $\mathbb{Q}(\sqrt{d})$ if and only if $d = 65d_1$ where d_1 is a square modulo 5 and modulo 13 and 65 is a square modulo d_1. Combining these two results with Proposition 4, we get

Corollary 2. *For $d = 5, 3, 2, -1, -2, -3, -5, -6$, there is no elliptic curve with good reduction everywhere over $\mathbb{Q}(\sqrt{d})$.*

Chapter 8

The Algorithm

In this chapter, we discuss the algorithm that we used to compute the cohomology groups and the Hecke operators on them. This is joint work with Fritz Grunewald. Although our algorithm works for any of the five Euclidean imaginary quadratic fields $K_1, K_2, K_3, K_7, K_{11}$, we work specifically with K_2 in this chapter and expose more details.

So set $K = K_2 = \mathbb{Q}(\sqrt{-2})$ and $\mathcal{O} = \mathcal{O}_2 = \mathbb{Z}[\sqrt{-2}]$.

8.1 Congruence Subgroups

We will only work with congruence subgroups of prime level although this is not necessary.

For a subgroup G of $PSL(2, \mathcal{O}))$ and a nonzero element α in $\mathcal{O}$, define

$$G_\alpha = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G : \alpha | c \right\} \quad \text{and} \quad G^\alpha = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G : \alpha | b \right\}$$

For every prime element π in $\mathcal{O}$, we define the congruence subgroup $\Gamma(\pi)$ of $PSL(2, \mathcal{O})$ as $PSL(2, \mathcal{O})_\pi$. We have $\Gamma(1) = PSL(2, \mathcal{O})$.

If $N(\pi) = p$, a prime integer, then $[\Gamma(1) : \Gamma(1)_\pi] = [\Gamma(1) : \Gamma(1)^\pi] = p + 1$. The set

$$R = \left\{ \left(\begin{smallmatrix} 0 & -1 \\ 1 & x \end{smallmatrix}\right) : 0 \le x \le p-1 \right\} \quad \cup \quad \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \right\}$$

is a complete set of representatives of coclasses modulo $\Gamma(1)_\pi$ and also modulo $\Gamma(1)^\pi$.

For a congruence subgroup Γ and a prime element π, one can check that

$$\Gamma_\pi = \Gamma \cap \alpha^{-1}\Gamma\alpha \quad \text{and} \quad \Gamma^\pi = \Gamma \cap \alpha\Gamma\alpha^{-1}$$

where $\alpha = \left(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Note that α, α^{-1} are not in $PSL(2,K)$ but in $PGL(2,K)$. It is easy to see that

$$\alpha^{-1}\Gamma^\pi\alpha = \Gamma_\pi$$

8.2 Computing H^1 for $\mathbf{PSL}_2(\mathcal{O})$

8.2.1 Finite Presentation

Recall that $\mathrm{PSL}_2(\mathcal{O}_2)$ has the following presentation.

$$\mathbf{PSL}_2(\mathcal{O}_2) = \left\langle A, B, U \;\middle|\; (AB)^3 = B^2 = AUA^{-1}U^{-1} = (BU^2BU^{-1})^2 = 1 \right\rangle$$

where $A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $U = \left(\begin{smallmatrix} 1 & 0 \\ \sqrt{-2} & 1 \end{smallmatrix}\right)$.

8.2.2 H^1 for $\mathbf{PSL}_2(\mathcal{O})$

Let $\Gamma = PSL_2(\mathcal{O}_K)$ and let $V = E_{k,l}(K)$. Take a cocyle $c \in H^1(\Gamma, V)$. By definition, $c : \Gamma \to V$ such that

$$c(hg) = c(h) \cdot g + c(g)$$

for all $g, h \in \Gamma$. If $g = h_1 ... h_m$, then by induction on m, we get

$$c(g) = \sum_{1 \le j \le m} c(h_j) \cdot h_1 ... h_{j-1} \tag{8.1}$$

Also,

$$c(g^{-1}) = -c(g) \cdot g^{-1} \tag{8.2}$$

Since any element g can be written as a product of A, A^{-1}, B, U, U^{-1}, a cocyle c can be determined by its values $c(A), c(B), c(U)$. So we identify a cocycle with the triple $(c(A), c(B), c(U))$ inside V^3.

Any cocyle c satisfies the equations

$$c((AB)^3) = c(B^2) = c(AUA^{-1}U^{-1}) = c((BU^2BU^{-1})^2) = c(1) = 0 \tag{8.3}$$

which are given by the relations that the generators A, B, U are satisfying.

Conversely, a function c defined on the generators A, B, U can be extended to whole Γ if it satisfies these equations. Since these equations are linear in $c(A), c(B), c(U)$, we can identify the space of cocycles $Z(\Gamma, V)$ as the null space of the system of equations (8.3). Using the identities (8.1) and (8.2) on the equations (8.3), we get the following system

- $c(B) \cdot [B + 1] = 0$
- $c(A) \cdot [B((AB)^2 + AB + 1)] + c(B) \cdot [(AB)^2 + AB + 1] = 0$
- $c(A) \cdot [A^{-1}(1 - U^{-1})] + c(U) \cdot [(A^{-1} - 1)U^{-1}] = 0$
- $c(B) \cdot [(U^{-1}BU + U)(BU^{-1}BU + 1)] + c(U) \cdot [(1 - U^{-1}BU)(BU^{-1}BU + 1)] = 0$

The subspace of coboundaries $B(\Gamma, V)$ inside the space $Z(\Gamma, V)$ of cocyles is given as the image of the linear map from V to V^3

$$v \longmapsto (v \cdot (A - 1), v \cdot (B - 1), v \cdot (U - 1))$$

Finally the quotient $Z(\Gamma, V)/B(\Gamma, V)$ gives us $H^1(\Gamma, V)$.

8.2.3 Hecke Action Revisited

Now we want the describe the action of Hecke operators on the vector space $H^1(\Gamma, V)$ that we computed in the previous section. Given a cocycle c, which is identified with the triple $(c(A), c(B), c(U))$, and a Hecke operator T, we want to describe $T(c)$, which is identified with $(T(c)(A), T(c)(B), T(c)(U))$. So the goal of this section is to describe $T(c)(A), T(c)(B)$ and $T(c)(U)$ in terms of $c(A), c(B)$ and $c(U)$.

Let π be a prime element of $\mathcal{O}$ such that $N(\pi) = p$, a rational prime. Let c be a cocyle in $H^1(\Gamma, V)$. We will compute $T_\pi(c)$. We need to compute $T_\pi(c)(A)$, $T_\pi(c)(B)$ and $T_\pi(c)(U)$. Let $\alpha = \left(\begin{smallmatrix} \pi & 0 \\ 0 & 1 \end{smallmatrix}\right)$. We fix the transversal R for Γ_π in Γ

$$\left\{R_i = \left(\begin{smallmatrix} 0 & -1 \\ 1 & x \end{smallmatrix}\right) : 0 \leq x \leq p-1\right\} \quad \cup \quad \left\{R_\infty = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$$

Then for every $g \in \Gamma$, we have

$$(T_\pi c)(g) = \sum_{1 \leq i \leq m} c(\alpha^{-1} h_i(g) \alpha) \cdot \alpha^\iota \cdot R_i^{-1}$$

where $h_i(g) = R_{\sigma_g(i)}^{-1} g R_i$ with $R_{\sigma_g(i)}$ the unique element in R such that $h_i(g) \in \Gamma^\pi$.

Thus for $g = A, B, U$, we need to describe $\sigma_g(i)$ and $h_i(g)$. This is done below.

(a) $T_\pi(c)(A)$

We have

$$\sigma_A(i) = \begin{cases} \overline{i-1} \pmod p & , 0 \leq i \leq p-1 \\ \infty & , i = \infty \end{cases}$$

This gives

$$h_i(A) = \begin{cases} I & , 1 \le i \le p-2 \\ \left(\begin{smallmatrix} 1 & -p \\ 0 & 1 \end{smallmatrix}\right) & , i = 0 \\ A & , i = \infty \end{cases}$$

Since $c(I) = 0$, the middle $p-2$ terms of $T_\pi(c)(A)$ vanish.

$$T_\pi(c)(A) = \quad c(\alpha^{-1}\ h_0(A)\ \alpha) \cdot \alpha^\iota \cdot R_0^{-1} + c(\alpha^{-1}\ h_\infty(A)\ \alpha) \cdot \alpha^\iota \cdot R_\infty^{-1}$$

Note that

$$\alpha^{-1}\ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\ \alpha = \left(\begin{smallmatrix} a & b/\pi \\ c\pi & d \end{smallmatrix}\right)$$

$$\begin{aligned} T_\pi(c)(A) &= c(\alpha^{-1}\left(\begin{smallmatrix} 1 & -p \\ 0 & 1 \end{smallmatrix}\right)\alpha) \cdot \alpha^\iota \cdot B + c(\alpha^{-1}\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\alpha) \cdot \alpha^\iota \\ &= c(\left(\begin{smallmatrix} 1 & -p/\pi \\ 0 & 1 \end{smallmatrix}\right)) \cdot \alpha^\iota \cdot B + c(\left(\begin{smallmatrix} 1 & 0 \\ \pi & 1 \end{smallmatrix}\right)) \cdot \alpha^\iota \\ &= c(\left(\begin{smallmatrix} 1 & -\bar{\pi} \\ 0 & 1 \end{smallmatrix}\right)) \cdot \alpha^\iota \cdot B + c(\left(\begin{smallmatrix} 1 & 0 \\ \pi & 1 \end{smallmatrix}\right)) \cdot \alpha^\iota \\ &= c(B\left(\begin{smallmatrix} 1 & 0 \\ \bar{\pi} & 1 \end{smallmatrix}\right)B) \cdot \alpha^\iota \cdot B + c(\left(\begin{smallmatrix} 1 & 0 \\ \pi & 1 \end{smallmatrix}\right)) \cdot \alpha^\iota \end{aligned}$$

Let $a, b \in \mathbb{Z}$ be such that $\pi = a + b\omega$. Then

$$\begin{aligned} T_\pi(c)(A) &= c(BA^aU^{-b}B) \cdot \alpha^\iota \cdot B + c(A^aU^b) \cdot \alpha^\iota \\ &= [c(B)A^aU^{-b}B + c(A^a)U^{-b}B + c(U^{-b})B + c(B)] \cdot \alpha^\iota \cdot B \\ &\quad +[c(A^a)U^b + c(U^b)] \cdot \alpha^\iota \end{aligned}$$

For an element $g \in \Gamma$,

$$c(g^n) = c(g)(g^{n-1} + ... + g^2 + g + 1)$$

Thus

$$c(g^{-n}) = -c(g^n)g^{-n} = -c(g)(g^{n-1} + ... + g^2 + g + 1)(g^{-n})$$

For abbreviation, put

$$P_M(n) = \begin{cases} M^{n-1} + ... + M^2 + M + 1 & \text{if } n > 0 \\ -(M^{n-1} + ... + M^2 + M + 1)(M^{-n}) & \text{if } n < 0 \end{cases}$$

so that $c(M^k) = c(M)P_M(k)$ for all $k \in \mathbb{Z}$ and $M \in \Gamma$.

Then we have

$$\begin{aligned} T_\pi(c)(A) &= [c(B)A^aU^{-b}B + c(A)P_A(a)U^{-b}B + c(U)P_U(-b)B + c(B)] \cdot \alpha^\iota \cdot B \\ &\quad + [c(A)P_A(a)U^b + c(U)P_U(b)] \cdot \alpha^\iota \end{aligned}$$

Putting like terms together, we get

$$\begin{aligned} T_\pi(c)(A) &= c(A)\ [P_A(a)(U^{-b}B\alpha^\iota B + U^b\alpha^\iota)] \\ &= + c(B)\ [(A^aU^{-b}B + 1)(\alpha^\iota B)] \\ &= + c(U)\ [P_U(-b)B\alpha^\iota B + P_U(b)\alpha^\iota] \end{aligned}$$

(b) $T_\pi(c)(B)$

We have

$$\sigma_B(i) = \begin{cases} \overline{-1/i} \pmod p & , 1 \le i \le p-1 \\ \infty & , i = 0 \\ 0 & , i = \infty \end{cases}$$

This gives

$$h_i(B) = \begin{cases} \begin{pmatrix} \sigma_B(i) & 1+i\sigma_B(i) \\ -1 & -i \end{pmatrix} & , 1 \le i \le p-2 \\ \\ I & , i = 0, \infty \end{cases}$$

Observe also that $R_i = A^{-i}B$ for $0 \le i \le p-1$. Thus we have

$$\begin{aligned} (T_\pi c)(B) &= \sum_{1 \le i \le p-1} c(\alpha^{-1} h_i(B)\alpha) \cdot \alpha^\iota \cdot R_i^{-1} \\ \\ &= \sum_{1 \le i \le p-1} c\left(\begin{pmatrix} \sigma_B(i) & \frac{1+i\sigma_B(i)}{\pi} \\ -\pi & -i \end{pmatrix}\right) \cdot \alpha^\iota \cdot BA^i \end{aligned}$$

We need to write those matrices in terms of A, B, U and we can do this effectively as our field is Euclidean. We describe a word decomposition algorithm to this effect in the next section.

(c) $T_\pi(c)(U)$

We have

$$\sigma_U(i) = \begin{cases} \overline{i-\omega} \pmod{\pi} & , 0 \le i \le p-1 \\ \\ \infty & , i = \infty \end{cases}$$

This gives

$$h_i(U) = \begin{cases} \begin{pmatrix} 1 & (i-\omega) - \sigma_U(i) \\ 0 & 1 \end{pmatrix} & , 0 \le i \le p-1 \\ \\ \left(\begin{smallmatrix} 1 & 0 \\ \omega & 1 \end{smallmatrix}\right) & , i = \infty \end{cases}$$

We get

$$(T_\pi c)(U) = \sum_{0\le i\le p-1} c(\begin{pmatrix} 1 & \frac{(i-\omega)-\sigma_U(i)}{\pi} \\ 0 & 1 \end{pmatrix}) \cdot \alpha^\iota \cdot BA^i + c(\left(\begin{smallmatrix} 1 & 0 \\ \omega\pi & 1 \end{smallmatrix}\right))\alpha^\iota$$

$$= \sum_{0\le i\le p-1} c(B\begin{pmatrix} 1 & 0 \\ \frac{\sigma_U(i)-(i-\omega)}{\pi} & 1 \end{pmatrix}B) \cdot \alpha^\iota \cdot BA^i + c(A^{-2b}U^a)\alpha^\iota$$

For every i, put $(\sigma_U(i) - (i-\omega))/\pi = Re(i) + Im(i)\omega$. Then

$$(T_\pi c)(U) = \sum_{0\le i\le p-1} c(BA^{Re(i)}U^{Im(i)}B) \cdot \alpha^\iota \cdot BA^i + c(A^{-2b}U^a)\alpha^\iota$$

Observe that

$$c(BA^{Re(i)}U^{Im(i)}B) = c(B)A^{Re(i)}U^{Im(i)}B + c(A^{Re(i)})U^{Im(i)}B + c(U^{Im(i)})B + c(B)$$

$$= c(A)[P_A(Re(i))U^{Im(i)}B] + c(B)[A^{Re(i)}U^{Im(i)}B + 1]$$

$$+c(U)[P_U(Im(i))B]$$

Moreover

$$c(A^{-2b}U^a) = c(A)[P_A(-2b)U^a] + c(U)[P_U(a)]$$

Hence

$$(T_\pi c)(U) = c(A)\ [\left(\sum_{0\le i\le p-1} P_A(Re(i))U^{Im(i)}B\alpha^\iota \cdot BA^i\right) + P_A(-2b)U^a\alpha^\iota]$$

$$+\ c(B)\ [\left(\sum_{0\le i\le p-1} (A^{Re(i)}U^{Im(i)}B + 1)(\alpha^\iota \cdot BA^i)\right)]$$

$$+\ c(U)\ [\left(\sum_{0\le i\le p-1} P_U(Im(i))B\alpha^\iota \cdot BA^i\right) + P_U(a)\alpha^\iota]$$

8.2.4 Word Decomposition

In this section we describe an effective algorithm to write a given element M of $\mathbf{PSL}_2(\mathcal{O})$ in terms of the generators A, B, U.

We first write M as product of lower triangular matrices.

Proposition 8.1. *Given a matrix in* $\mathbf{PSL}_2(\mathcal{O})$*, let* $M \in \mathbf{SL}_2(\mathcal{O})$ *be a preimage of* M*. There exists upper triangular matrices* $Q_1, .., Q_m$ *such that*

$$M = \pm Q_m B Q_2 .. B Q_1 \quad \text{or} \quad M = \pm B Q_m B Q_2 .. B Q_1.$$

Proof. Say $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Without loss of generality, we may assume that $N(d) > N(b)$, because if not, we can replace M with $BM = \left(\begin{smallmatrix} -c & -d \\ a & b \end{smallmatrix}\right)$.

We will proceed by induction on the norm $N(b)$ of b. If $b \neq 0$, using the Euclidean algorithm we find q and r such that

$$d = qb + r \quad , N(r) < N(b)$$

In the inductive step, set $Q = \left(\begin{smallmatrix} 1 & 0 \\ -q & 1 \end{smallmatrix}\right)$ and we take

$$M' = BQM = \left(\begin{smallmatrix} c' & -r \\ a & b \end{smallmatrix}\right)$$

Since $N(-r) < N(b)$, in a finite number of steps the top right corner will become 0, forcing the diagonal entries to be units ± 1. This gives the desired result. □

To finish the word decomposition, we need the following straighforward observation. Let $z = a + b\sqrt{-2} \in \mathcal{O}$. Then we have

$$\left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right) = A^a U^b$$

8.3 Computing H^1 for $\Gamma < \mathbf{PSL}_2(\mathcal{O})$

Let $\Gamma = \Gamma_0(\mu)$ for some element μ of $\mathcal{O}$ with rational prime norm q and $V = E_{k,l}$. To compute $H^1(\Gamma, V)$, we will not use a presentation of Γ like we did for $\mathbf{PSL}_2(\mathcal{O})$. This is feasable but very inefficient. Instead, we will use Shapiro's Lemma and express cohomology of Γ as a cohomology of $\mathbf{PSL}_2(\mathcal{O})$. More precisely, we have

$$H^1(\Gamma, V) \simeq H^1(\mathbf{PSL}_2(\mathcal{O}), \mathrm{Ind}(V))$$

where

$$Ind(V) = \{f : \mathbf{PSL}_2(\mathcal{O}) \to V \mid f(gh) = f(g) \cdot h \text{ for all } h \in \Gamma\}.$$

To compute $H^1(\mathbf{PSL}_2(\mathcal{O}), \mathrm{Ind}(V))$, we first need to describe the action of the genrators A, B, U of $\mathbf{PSL}_2(\mathcal{O})$ on the induced module $\mathrm{Ind}(V)$. We do this using another description of $\mathrm{Ind}(V)$ which is as follows.

Let $f : \mathbf{PSL}_2 \to V$ be an element of $\mathrm{Ind}(V)$. As f is Γ-invariant by definition, f is determined by its values on some (equivalently, any) transversal (that is, a set of coset representatives) of Γ in $\mathbf{PSL}_2(\mathcal{O})$. Thus, $\mathrm{Ind}(V)$ can be seen as direct sum of copies of V indexed by a transversal $\{\gamma_i\}$ of Γ in $\mathbf{PSL}_2(\mathcal{O})$. Then the action of $\mathbf{PSL}_2(\mathcal{O})$ can be dsecribed as follows. Let $g \in \mathbf{PSL}_2(\mathcal{O})$ and $v_{\gamma_i} \in \mathrm{Ind}(V)$ be an element indexed by σ_i. When $v \in V$ is indexed by γ_i, let us use v_i to denote this. We have

$$g \cdot v_i = v_{\sigma(i)} \cdot h_i(g)$$

where $g\gamma_i = \gamma_{\sigma(i)} h_i(g)$ with $h_i(g) \in \Gamma$. In other words, the element $v \in V$ which is contained in the copy indexed by γ_i goes to $v \cdot h_i(g)$ that is contained in the copy of V indexed by $\gamma_{\sigma i}$.

So we need to describe the action of A, B, U and $\alpha^\iota = \left(\begin{smallmatrix} 1 & 0 \\ 0 & \pi \end{smallmatrix}\right)$ on the induced module. This is done below.

For convenience, we choose to work with the transversal

$$\left\{R_x = \left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) : 0 \leq x \leq q-1\right\} \quad \cup \quad \left\{R_\infty = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\right\}$$

for Γ in $\mathbf{PSL}_2(\mathcal{O})$.

(a) Action of A on the induced module

We have

$$\sigma_A(i) = \begin{cases} \overline{i+1} \pmod{q} & , 0 \leq i \leq q-1 \\ \infty & , i = \infty \end{cases}$$

This gives

$$h_i(A) = \begin{cases} I & , 0 \leq i \leq q-2 \\ A^q & , i = q-1 \\ BAB & , i = \infty \end{cases}$$

(b) Action of B on the induced module

We have

$$\sigma_B(i) = \begin{cases} \overline{-1/i} \pmod{q} & , 1 \leq i \leq p-1 \\ \infty & , i = 0 \\ 0 & , i = \infty \end{cases}$$

This gives

$$h_i(B) = \begin{cases} A^{-\sigma_B(i)} B A^i & , 1 \leq i \leq q-2 \\ I & , i = 0, \infty \end{cases}$$

(c) Action of U on the induced module

We have

$$\sigma_U(i) = \begin{cases} \overline{i+\omega} \pmod{\mu} & , 0 \leq i \leq p-1 \\ \infty & , i = \infty \end{cases}$$

This gives

$$h_i(U) = \begin{cases} A^{-\sigma_U(i)} U A^i & , 0 \leq i \leq p-1 \\ BUB & , i = \infty \end{cases}$$

(d) Action of α^ι on the induced module

We have

$$\sigma_U(i) = \begin{cases} \overline{i\pi} \pmod{\mu} & , 0 \leq i \leq p-1 \\ \infty & , i = \infty \end{cases}$$

This gives

$$h_i(U) = \begin{cases} \alpha^\iota & , 0 \leq i \leq p-1 \\ \alpha & , i = \infty \end{cases}$$

Bibliography

[1] A. Ash, *Galois representations attached to mod p cohomology of $GL(n, \mathbb{Z})$*, Duke Math. J., 65 (1992), pp. 235–255.

[2] A. Ash and G. Stevens, *Cohomology of arithmetic groups and congruences between systems of hecke eigenvalues*, J. Reine Angew. Math., 365 (1986), pp. 192–220.

[3] ——, *Modular forms in characteristic l and special values of their l-functions*, Duke Math. J., 53 (1986), pp. 849–868.

[4] A. F. Beardon, *The geometry of discrete groups*, vol. 91 Corrected reprint of the 1983 original, Springer-Verlag, New York, 1995. Graduate Texts in Mathematics.

[5] T. Berger and G. Harcos, *l-adic representations associated to modular forms over imaginary quadratic fields*, Int. Math. Res. Not. IMRN, 23 (2007).

[6] A. Borel, *Regularization theorems in lie algebra cohomology. applications*, Duke Math. J., 50 (1983), pp. 605–623.

[7] A. Borel and J. P. Serre, *Corners and arithmetic groups*, Comment. Math. Helv., 48 (1973), pp. 436–491.

[8] R. Brauer and C. Nesbitt, *On the modular characters of groups*, Ann. of Math. (2), 42 (1941), pp. 556–590.

[9] S. Brueggeman, *The nonexistence of certain galois extensions unramified outside 5*, J. Number Theory, 75 (1999), pp. 47–52.

[10] ——, *The nonexistence of certain nonsolvable galois extensions of number fields of small degree*, Int. J. Number Theory, 1 (2005), pp. 155–160.

[11] S. Comalada, *Elliptic curves with trivial conductor over quadratic fields*, Pacific J. Math., 144 (1990), pp. 237–258.

[12] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math., 51 (1984), pp. 275–324.

[13] P. Deligne, *Formes modulaires et representations l-adiques*, vol. 179 of Sem. Bourbaki no.335, Lecture Notes In Mathematics, Springer-Verlag, 1971.

[14] L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Transactions of the American Mathematical Society, 12 (1911), pp. 75–98.

[15] B. Edixhoven, *The weight in serre's conjectures on modular forms*, Invent. Math., 109 (1992), pp. 563–594.

[16] J. Elstrodt, F. Grunewald, and J. Mennicke, *PSL_2 over imaginary quadratic integers*, in Arithmetic Conference (Metz, 1981), vol. 94 of Astérisque, Soc. Math. France, Paris, 1982, pp. 43–60.

[17] ——, *Groups acting on hyperbolic space*, Springer-Verlag, Berlin, 1998. Springer Monographs in Mathematics Harmonic analysis and number theory.

[18] L. M. Figueiredo, *Serre's conjecture for imaginary quadratic fields*, Compositio Math., 118 (1999), pp. 103–122.

[19] D. Floge, *Zur struktur der PSL_2 über einigen imaginär-quadratischen zahlringen*, Math. Z., 183 (1983), pp. 255–279.

[20] J. Franke, *Harmonic analysis in weighted L_2-spaces*, Ann. Sci. École Norm. Sup. (4), 31 (1998), pp. 181–279.

[21] F. Grunewald, H. Helling, and J. Mennicke, *SL_2 over complex quadratic number fields. i*, Algebra i Logika, 17 (1978), pp. 512–580, 622.

[22] G. Harder, *On the cohomology of $SL(2, \mathcal{O})$*, Lie groups and their representations (Proc. Summer School on Group Representations of the Bolyai János Math. Soc., Budapest, 1971), (1975), pp. 139–150.

[23] ——, *Eisenstein cohomology of arithmetic groups. the case GL_2*, Invent. Math., 89 (1987), pp. 37–118.

[24] M. Harris, D. Soudry, and R. Taylor, *l-adic representations associated to modular forms over imaginary quadratic fields. i. lifting to $GSp_4(\mathbb{Q})$*, Invent. Math., 112 (1993), pp. 377–411.

[25] N. Jochnowitz, *Congruences between systems of eigenvalues of modular forms*, Trans. Amer. Math. Soc., 270 (1982), pp. 269–285.

[26] T. Kagawa, *Elliptic Curves With Good Reduction Over Real Quadratic Fields*, PhD thesis, Waseda University, 1998.

[27] T. Kagawa and M. Kida, *Nonexistence of elliptic curves with good reduction everywhere over real quadratic fields*, J. Number Theory, 66 (1997), pp. 201–210.

[28] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, 2004.

[29] ——, *Serre's modularity conjecture (II)*, 2004.

[30] M. Kida, *Reduction of elliptic curves over certain real quadratic number fields*, Math. Comp., 68 (1999), pp. 1679–1685.

[31] J. Kluners and G. Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math., 4 (2001), pp. 182–196 (electronic). Accesible online http://www.math.uni-duesseldorf.de/ klueners/minimum/minimum.html.

[32] C. Maclachlan and A. W. Reid, *The arithmetic of hyperbolic 3-manifolds*, vol. 219, Springer-Verlag, New York, 2003. Graduate Texts in Mathematics.

[33] E. R. Mendoza, *Cohomology of PGL_2 over imaginary quadratic integers*, PhD thesis, Rheinische Friedrich-Wilhelms-Universität, Bonn, Bonn, 1979. Bonner Mathematische Schriften [Bonn Mathematical Publications], 128 Dissertation, 1979.

[34] H. Moon, *Finiteness results on certain mod p galois representations*, J. Number Theory, 84 (2000), pp. 156–165.

[35] H. Moon and Y. Taguchi, *Refinement of tate's discriminant bound and non-existence theorems for mod p galois representations*, Doc. Math., (2003), pp. 641–654 (electronic).

[36] ——, *The nonexistence of certain mod 2 galois representations of small quadratic fields*, 2007.

[37] ——, *On the finiteness and nonexistence of certain mod 2 galois representations of quadratic fields*, Kyungpook Math. J., 48 (2008), pp. 323–330.

[38] N. Nakagoshi, *The structure of the multiplicative group of residue classes modulo* $\mathfrak{p}^{N+1}$, Nagoya Math. J., 73 (1979), pp. 41–60.

[39] R. G. E. Pinch, *Elliptic curves with good reduction away from* 2. *ii*, Math. Proc. Cambridge Philos. Soc., 100 (1986), pp. 435–457.

[40] V. Platonov and A. Rapinchuk, *Algebraic groups and number theory*, vol. 139 Translated from the 1991 Russian original by Rachel Rowen, Academic Press Inc., Boston, MA, 1994. Pure and Applied Mathematics.

[41] G. Poitou, *Sur les petits discriminants*, in Séminaire Delange-Pisot-Poitou, 18e année: (1976/77), Théorie des nombres, Fasc. 1 (French), Secrétariat Math., Paris, 1977, pp. Exp. No. 6, 18.

[42] C. Priplata, *Cohomology and homology of* PSL_2 *over imaginary quadratic integers with general coefficients* $M_{n,m}(\mathcal{O}_K)$ *and Hecke eigenvalues*, PhD thesis, Heinrich Heine University, 2000.

[43] M. H. Sengun, *The nonexistence of certain representations of the absolute galois groups of quadratic fields*, 2007.

[44] M. H. Sengun and S. Turkelli, *Weight reduction for mod* ℓ *bianchi modular forms*, 2008.

[45] J.-P. Serre, *Le problème des groupes de congruence pour* SL_2, Ann. of Math. (2), 92 (1970), pp. 489–527.

[46] ——, *Local fields*, vol. 67 Translated from the French by Marvin Jay Greenberg, Springer-Verlag, New York, 1979. Graduate Texts in Mathematics.

[47] ——, *Œuvres. Vol. III 1972–1984*, Springer-Verlag, Berlin, 1986.

[48] ——, *Sur les représentations modulaires de degré* 2 *de Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J., 54 (1987), pp. 179–230.

[49] B. Setzer, *Elliptic curves over complex quadratic fields*, Pacific J. Math., 74 (1978), pp. 235–250.

[50] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, vol. 11, Princeton University Press, Princeton, NJ, 1994. Publications of the Mathematical Society of Japan Reprint of the 1971 original; Kano Memorial Lectures, 1.

[51] W. Stein, *Modular forms, a computational approach*, vol. 79, With an appendix by Paul E. Gunnells, American Mathematical Society, Providence, RI, 2007. Graduate Studies in Mathematics.

[52] R. Steinberg, *Tensor product theorems*, in The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986), vol. 47 of Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, RI, 1987, pp. 331–338.

[53] R. G. Swan, *Generators and relations for certain special linear groups*, Advances in Math., 6 (1971), pp. 1–77 (1971).

[54] J. Tate, *The non-existence of certain galois extensions of* $\mathbb{Q}$ *unramified outside* 2, in Arithmetic geometry (Tempe, AZ, 1993), vol. 174 of Contemp. Math., Amer. Math. Soc., Providence, RI, 1994, pp. 153–156.

[55] R. Taylor, *On Cogruences Between Modular Forms*, PhD thesis, Princeton, 1988.

[56] ——, *l-adic representations associated to modular forms over imaginary quadratic fields. II*, Invent. Math., 116 (1994), pp. 619–643.

[57] G. Wiese, *On the faithfulness of parabolic cohomology as a hecke module over a finite field*, J. Reine Angew. Math., 606 (2007), pp. 79–103.