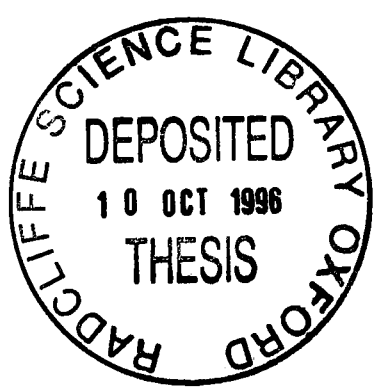
The Jacobian of Modular Curves Associated to Cartan Subgroups

Imin Chen
Exeter College, Oxford.
Hiliary Term, 1996.



A thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at the University of Oxford.

The Jacobians of Modular Curves Associated to Cartan Subgroups

Imin Chen
Exeter College, Oxford.
Hiliary Term, 1996.

A thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy at the University of Oxford.

Abstract

The mod p representation associated to an elliptic curve is called split/non-split dihedral if its image lies in the normaliser of a split/non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Let $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$ denote the modular curves which classify elliptic curves with dihedral split and non-split mod p representation, respectively. We call such curves (split/non-split) *Cartan modular curves.* It is well known that $X^+_{\text{split}}(p)$ is isomorphic to the curve $X^+_0(p^2)$. On the other hand, the curve $X^+_{\text{non-split}}(p)$ is distinctly different from any of the classical modular curves. Despite this apparent disparity, it is shown in this thesis that the jacobian of $X^+_{\text{non-split}}(p)$ is isogenous to the new part of the jacobian of $X^+_0(p^2)$.

The method of proof uses the Selberg trace formula. An explicit formula for the trace of Hecke operators is derived for both split and non-split Cartan modular curves. Comparing these two trace formulae, one obtains a trace relation, which in combination with the Eichler-Shimura relations allows us to conclude that the L-series of the two abelian varieties in question are the same, up to finitely many L-factors. The result then follows by Faltings' isogeny theorem.

Acknowledgements

The experience of my studies at Oxford owes a large part of its substance to many people. In particular, I would like to thank my supervisor Prof. B.J. Birch for his guidance during the past three years. It is due to his generous capacity that I have been fortunate enough to explore this wonderful world of number theory. Special thanks also goes to Prof. N. Yui, whose generous attention has been a source of inspiration and encouragement since my undergraduate days. It has been my fortune to have come to know D.L. Reed, Dr. C. Gasbarri, Dr. H. Goto, Dr. P. Guha, O. Bultel, Y. Hong, S. Galbraith, P. Bending, J. Wilson, who as fellow students or visitors at one time or another have enriched my time here.

I am grateful to Prof. S.J. Edixhoven for explaining to me his approach to the work discussed in this thesis and to Dr. A. Jarvis for his generous time and patience on the numerous occasions I have sought his help during the writing of this thesis. Also, I would like to thank Prof. D.B. Zagier for bringing to my attention the references in [Gro80] and [Lig77].

To all of my friends and family who have shared in their experience with me these past three years, I wish to thank them for their support and friendship.

I wish to express my gratitude to the Association of Commonwealth Universities and NSERC who have made my studies here possible through their generous support.

Contents

Chapter 1

Introduction

Let E be an elliptic curve defined over a number field K. The galois group $\mathrm{Gal}(\overline{K}|K)$ acts on the $\overline{K}$-points of E. In particular, this action leaves stable the p-torsion points of E, denoted $E[p]$. Hence, one obtains a representation $\rho_{E,p} : \mathrm{Gal}(\overline{K}|K) \to \mathrm{Aut}(E[p]) \cong GL_2(\mathbb{F}_p)$, called the mod p representation of E.

Let p be an odd prime. It is known from the theory of complex multiplication that the mod p representation of an elliptic curve over $\mathbb{Q}$ with complex multiplication has image lying in the normaliser of a (split/non-split) Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, if it is irreducible. Such a mod p representation is called (split/non-split) *dihedral*. Conversely, one may ask whether these are the only elliptic curves over $\mathbb{Q}$ with dihedral mod p representation (see [Ser72], section 4.3).

There exist modular curves $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$ defined over $\mathbb{Q}$ which classify elliptic curves with split and non-split dihedral mod p representation in the sense that the $\mathbb{Q}$-rational points of $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$ correspond to elliptic curves over $\mathbb{Q}$ with split and non-split dihedral mod p representation [DR72]. The above question can therefore be rephrased by asking whether the non-cuspidal $\mathbb{Q}$-rational points on the modular curves $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$ arise only from elliptic curves over $\mathbb{Q}$ with complex multiplication.

If genus of $X^+_{\text{split}}(p)$ or $X^+_{\text{non-split}}(p)$ is zero, then it has infinitely many $\mathbb{Q}$-rational points. Thus, the question has a negative answer in this situation, which occurs for $p = 3, 5, 7$. Only $X^+_{\text{non-split}}(p)$ achieves genus one and this occurs for $p = 11$. It can be shown that $X^+_{\text{non-split}}(11)$ is the elliptic curve 121E in [BK72] and that its Mordell-Weil group has rank one. Thus, there are infinitely many elliptic curves over $\mathbb{Q}$ with non-split dihedral mod 11 representation. For all other values of p, $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$ have genus greater than one so there are only finitely many elliptic curves over $\mathbb{Q}$ with dihedral mod p representation by Faltings' Theorem. Hence, in these cases it is plausible that the non-cuspidal rational points arise only from elliptic curves over $\mathbb{Q}$ with complex multiplication, although it may be possible for some exceptions for occur for small values of p. Indeed, in [Ser72], it is asked whether this is the case for $p \geq 19$.

Because of the isomorphism $X^+_{\text{split}}(p) \cong X^+_0(p^2)$, the methods of [Maz77] [Maz78] can be used to tackle this problem in the split case. In [Mom84], some progress has been made in this direction. However, Mazur states in [Maz77] that the non-split case does not seem to be approchable by known methods. In an effort to understand $X^+_{\text{non-split}}(p)$, we prove the following Theorem:

Theorem 1 *The jacobian of $X^+_{non\text{-}split}(p)$ is isogenous to the new part of the jacobian of $X^+_0(p^2)$.*

The method of proof uses the Selberg trace formula. We calculate an explicit formula for the trace of Hecke operators acting on the space of weight two cusp forms of $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$. Subsequently, we obtain the following trace identity:

Theorem 2 *For n prime to p,*

$$tr(T_n \mid S_2(\Gamma^+_{non\text{-}split}(p))) = tr(T_n \mid S_2(\Gamma^+_0(p^2))^{new}) \tag{1.1}$$

By the Eichler-Shimura congruence relations, one sees that the L-series of $J(X^+_{\text{non-split}}(p))$ and $J(X^+_0(p^2))^{\text{new}}$ are the same except possibly for the L-factor at p. Thus, $J(X^+_{\text{non-split}}(p))$ and $J(X^+_0(p^2))^{\text{new}}$ are isogenous by Faltings' isogeny Theorem [Fal86].

The technique of making the Selberg trace formula explicit for Hecke operators is well-known for the unit group of an Eichler order of level N with character χ in an indefinite quaternion algebra over $\mathbb{Q}$ [Hij74]. Two new aspects are involved in deriving an explicit trace formula for $\Gamma^+_{\text{split}}(p) \cong \Gamma^+_0(p^2)$ and $\Gamma^+_{\text{non-split}}(p)$. Firstly, these two Fuchsian groups do not arise as the unit group of an order in an indefinite quaternion algebra, but rather as a normaliser extension of a unit group. This introduces some minor adjustment terms in the usual calculation of the trace formula for unit groups. Secondly, the order arising in the non-split case does not resemble an Eichler order. As a result, the method for obtaining the quantities $c^+_p(\alpha, \mathfrak{r})$ is more complicated in the non-split case.

The trace relation originates from an observation of Birch [Bir94], following genus calculations in [Che94], that the genus of $X^+_{\text{non-split}}(p)$ is precisely the genus of $X^+_{\text{split}}(p)$ less the genus of $X_0(p)$. Subsequent computations by the author using modular symbols confirmed that the action of Hecke operators on the space of weight two cusp forms in each case was the same for some small primes. It has also come to the recent attention of the author that there are references in the literature to the modular curve $X^+_{\text{non-split}}(p)$. Gross in [Gro80] p. 66 quotes [Lig77] and states that Ligozat observes the isogeny in Theorem 1. Also, Darmon in [Dar93] states that Elkies observes a variant of the isogeny in question.

Edixhoven [Edi95] has recently given an alternate and more enlightening proof of the isogeny in Theorem 1 based on the representation theory of $\mathrm{GL}_2(\mathbb{F}_p)$. His method and some of its consequences will be discussed in the concluding chapter.

The curves $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$ also classify those elliptic curves which Wiles stated in his original Cambridge lectures to be the first class of elliptic curves which he proved to be modular, referred to as the CM-case. The subsequent paper [Wil95] however (due to certain technical difficulties), only deals with the *ordinary* CM-case, which excludes those elliptic curves classified by $X^+_{\text{non-split}}(p)$.

Finally, there has been some recent interest in $X^+_{\text{non-split}}(p)$ due to its appearance in the application of the Shimura-Taniyama-Weil conjecture to variants of the Fermat equation. In particular, knowledge about the $\mathbb{Q}$-rational points on $X^+_{\text{non-split}}(p)$ would strengthen the results obtained in [Dar93] [Rib80].

1.1 Modular curves associated to Cartan subgroups

For an odd prime p, we define in this section a class of modular curves associated to Cartan subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, as smooth projective curves over $\mathbb{C}$.

For $\lambda \in \mathbb{F}_p$, let θ_λ be the following matrix in $M_2(\mathbb{F}_p)$:

$$\theta_\lambda = \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}. \tag{1.2}$$

We define $H_\lambda(p)$ to be the subgroup $\mathbb{F}_p[\theta_\lambda]^\times = (\mathbb{F}_p + \mathbb{F}_p\theta_\lambda)^\times$ of $\mathrm{GL}_2(\mathbb{F}_p)$. It is easily seen that two subgroups $H_\lambda(p)$ and $H_{\lambda'}(p)$ are conjugate if and only if $\left(\frac{\lambda}{p}\right) = \left(\frac{\lambda'}{p}\right)$. With this in mind, we make the following definition:

Definition 1.1.1 *A subgroup of $GL_2(\mathbb{F}_p)$ which is in the conjugacy class of $H_\lambda(p)$ is called a non-split Cartan subgroup, a unitriangular subgroup, a split Cartan subgroup, accordingly as $\left(\frac{\lambda}{p}\right) = -1, 0, 1$.*

The normalisers of the above subgroups can be described in the following way:

Lemma 1.1.1 *Let $H^+_\lambda(p)$ denote the normaliser of $H_\lambda(p)$. Then*

$$H^+_\lambda(p) = \begin{cases} H_\lambda(p) \coprod \omega H_\lambda(p) & \text{if } \left(\frac{\lambda}{p}\right) = -1 \\ \coprod_{d \in \mathbb{F}_p^\times} \omega_d H_\lambda(p) & \text{if } \left(\frac{\lambda}{p}\right) = 0 \\ H_\lambda(p) \coprod \omega H_\lambda(p) & \text{if } \left(\frac{\lambda}{p}\right) = 1. \end{cases}$$

where

$$\omega = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\omega_d = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}.$$

A subgroup in the conjugacy class of $H^+_\lambda(p)$ is called the normaliser of a non-split Cartan subgroup, a Borel subgroup, the normaliser of a split Cartan subgroup, accordingly as $\left(\frac{\lambda}{p}\right) = -1, 0, 1$. It is a well-known fact that these three types of subgroups give all the non-exceptional proper maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ (see section 2 of [Ser72]).

It is sometimes convenient to use the following more canonical descriptions of the subgroups $H^+_\lambda(p)$:

i. (the normaliser of a non-split Cartan subgroup)

$$N'_\lambda(p) = \left\{ \begin{pmatrix} \alpha & \beta \\ \lambda\beta & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & \beta \\ -\lambda\beta & -\alpha \end{pmatrix} \mid (\alpha,\beta) \not\equiv (0,0), \left(\frac{\lambda}{p}\right) = -1 \right\}$$

There is really no natural choice for λ unless $p \equiv -1 \pmod 4$, in which case we set $\lambda = -1$. In most contexts, the choice of λ does not matter and we use the notation $N'(p)$ to refer to $N'_\lambda(p)$ with some choice of quadratic non-residue λ.

ii. (a Borel subgroup)

$$B(p) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}$$

iii. (the normaliser of a split Cartan subgroup)

$$N(p) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \begin{pmatrix} 0 & a \\ d & 0 \end{pmatrix} \mid a, d \in \mathbb{F}_p^\times \right\}$$

From above, we also get canonical descriptions $T'_\lambda(p)$, $U(p)$, $T(p)$ of non-split Cartan, unipotent, split Cartan subgroups.

Suppose H is a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Let $\Gamma_H(p)$ be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which reduces modulo p to $H \cap \mathrm{SL}_2(\mathbb{F}_p)$. The compact Riemann surface $X_H(p) = \Gamma_H(p)\backslash\mathfrak{H}^*$ is a smooth projective curve over $\mathbb{C}$.

Our case of interest is when H is the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. We note that if H and H' are conjugate subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$, then $X_H(p)$ is isomorphic to $X_{H'}(p)$ as curves over $\mathbb{C}$. Hence, the isomorphism class of $X_H(p)$ only depends on the conjugacy class of H in $\mathrm{GL}_2(\mathbb{F}_p)$. However, to fix things, we prefer to use a particular choice of subgroups in the definition below:

$$\Gamma^+_{\text{non-split},\lambda}(p) = \Gamma_{N'_\lambda(p)}(p) \tag{1.3}$$

$$X^+_{\text{non-split},\lambda}(p) = \Gamma^+_{\text{non-split},\lambda}(p)\backslash\mathfrak{H}^* \tag{1.4}$$

$$\Gamma^+_{\text{split}}(p) = \Gamma_{N(p)}(p) \tag{1.5}$$

$$X^+_{\text{split}}(p) = \Gamma^+_{\text{split}}(p)\backslash\mathfrak{H}^*. \tag{1.6}$$

We call $X^+_{\text{non-split},\lambda}(p)$ and $X^+_{\text{split}}(p)$ *Cartan modular curves.*

For later reference, we also make the following definitions:

$$\Gamma_{\text{non-split},\lambda}(p) = \Gamma_{T'_\lambda(p)}(p) \tag{1.7}$$
$$X_{\text{non-split},\lambda}(p) = \Gamma_{\text{non-split},\lambda}(p)\backslash\mathfrak{H}^* \tag{1.8}$$

$$\Gamma_{\text{split}}(p) = \Gamma_{T(p)}(p) \tag{1.9}$$
$$X_{\text{split}}(p) = \Gamma_{\text{split}}(p)\backslash\mathfrak{H}^* \tag{1.10}$$

$$\Gamma_0(p) = \Gamma_{B(p)}(p) \tag{1.11}$$
$$X_0(p) = \Gamma_0(p)\backslash\mathfrak{H}^* \tag{1.12}$$

The choice of quadratic non-residue λ in 1.3, 1.7 above will often be omitted in contexts where it does not matter.

The genus of $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$ can calculated either using classical methods [Che94] or the trace formula (see section 5.2) as

$$g^+_{\text{split}}(p) = \frac{1}{24}(p^2 - 8p + 11 - 4\left(\frac{-3}{p}\right)) \tag{1.13}$$
$$g^+_{\text{non-split}}(p) = \frac{1}{24}(p^2 - 10p + 23 + 6\left(\frac{-1}{p}\right) + 4\left(\frac{-3}{p}\right)). \tag{1.14}$$

Also, in [BT92] a table for the genera of $X^+_{\text{non-split}}(p)$ and $X^+_{\text{split}}(p)$ are given for $p \leq 349$.

Using the Riemann-Hurwitz formula, it can be shown that there is no covering map from $X^+_{\text{split}}(p)$ to $X^+_{\text{non-split}}(p)$ for large enough primes p. Hence, the homomorphism of jacobians which we are considering does not seem be given in a straightforward way.

1.2 Moduli spaces of elliptic curves

The purpose of this section is to discuss the existence of a $\mathbb{Q}$-model for the smooth projective curves over $\mathbb{C}$, $X^+_{\text{non-split}}(p)$ and $X^+_{\text{split}}(p)$, and to give a modular interpretation of the K-rational points of this $\mathbb{Q}$-model. With this aim in mind, we briefly review some formalism regarding moduli problems and the general representability results of Drinfeld.

Some formalism

A geometric point of a scheme X is a morphism $\text{Spec}(\Omega) \to X$ where Ω is an algebraically-closed field. Given an S-scheme X/S and a geometric point $\text{Spec}(\Omega)/S$ of S, the fibre product $X \times_S \text{Spec}(\Omega)$ is called a geometric fibre.

Definition 1.2.1 *An S-scheme E/S together with an S-section of E/S is called an elliptic curve if:*

i. The structure morphism $E \to S$ is proper and smooth.

ii. The geometric fibres of E/S are connected (necessarily smooth) curves of genus one.

Let $\mathcal{C}$ be a subcategory of (Sch). We denote by $(Ell)/\mathcal{C}$ the category of elliptic curves in $\mathcal{C}$ defined over variable base schemes in $\mathcal{C}$ whose morphisms are pull-back squares in $\mathcal{C}$. Although we discuss moduli problems for elliptic curves in $\mathcal{C} = (Sch)$, the formalism extends equally well other choices of $\mathcal{C}$ (for instance, $\mathcal{C} = (Var/\mathbb{C})$ or $\mathcal{C} = (Sch/S)$ where S is a fixed scheme). By convention, we set $(Ell) = (Ell)/(Sch)$ and $(Ell)/(Sch/S) = (Ell)/S$.

Definition 1.2.2 *A moduli problem $\mathcal{P}$ for (Ell) is a contravariant functor $(Ell) \to (Sets)$.*

Definition 1.2.3 *Let $\mathcal{P}$ be a moduli problem for (Ell). The contravariant functor*

$$\begin{aligned} &\mathcal{M}_{\mathcal{P}} : (Sch) \to (Sets) \\ &\quad S \mapsto \textit{isomorphism classes of } (E/S, \phi) \textit{ where } \phi \in \mathcal{P}(E/S). \end{aligned}$$

is called the moduli space associated to $\mathcal{P}$.

Definition 1.2.4 *A moduli problem $\mathcal{P}$ is rigid if for each E/S and $\phi \in \mathcal{P}(E/S)$ there are no automorphisms of E/S which fix ϕ.*

The functor $\mathcal{P}$ is representable if and only if the functor $\mathcal{M}_{\mathcal{P}}$ is representable and $\mathcal{P}$ is rigid. Indeed, if $\mathcal{P}$ is representable by $\mathbb{E}/\mathbb{M}$, then $\mathbb{M}$ represents $\mathcal{M}_{\mathcal{P}}$ and it is easily seen from the universal property of pull-back squares that $\mathcal{P}$ is rigid. On the other hand, if $\mathbb{M}$ represents $\mathcal{M}_{\mathcal{P}}$, then the elliptic curve $\mathbb{E}/\mathbb{M}$ which is associated to the identity of $\mathcal{M}_{\mathcal{P}}(\mathbb{M}) = \mathrm{Hom}_{(Sch)}(\mathbb{M}, \mathbb{M})$ represents $\mathcal{P}$, where rigidity of $\mathcal{P}$ ensures that the desired isomorphism of functors is injective.

Definition 1.2.5 *Let $\mathcal{P}$ be a rigid moduli problem on (Ell). A scheme $\mathbb{M}$ is called a fine moduli scheme for $\mathcal{P}$ if it represents the moduli space $\mathcal{M}_{\mathcal{P}}$.*

There is a weaker definition of fine moduli scheme given in [Mum94] which excludes the rigidity condition. The example of $Y(N)/\{\pm 1\}$ discussed in the next section gives an example where these two notions differ.

Often a fine moduli scheme for $\mathcal{P}$ does not exist and one has to consider the next best approximation:

Definition 1.2.6 *Let $\mathcal{P}$ be a moduli problem on (Ell). A pair $(\mathbb{M}, \alpha)$ consisting of a scheme $\mathbb{M}$ and a natural transformation of functors $\alpha : \mathcal{M}_{\mathcal{P}}(\cdot) \to Hom(\cdot, \mathbb{M})$ is called a coarse moduli scheme for $\mathcal{P}$ if:*

i. The natural transformation α is bijective on algebraically-closed fields Ω.

ii. If $(\mathbb{M}', \alpha')$ is another such pair and α' satisfies the above property, then α' factors through α uniquely.

So a coarse moduli scheme for $\mathcal{P}$ is a scheme $\mathbb{M}$ which represents the moduli space $\mathcal{M}_{\mathcal{P}}$ on algebraically-closed fields Ω and which is universal with respect to this property. Of course, every fine moduli scheme is a coarse moduli scheme.

Level N-structures

Let E/S be an elliptic curve. Given a section $t \in E[N](S)$ and an integer m, we note that $m \cdot t$ is only dependent on the congruence class of m in $\mathbb{Z}/N\mathbb{Z}$. Also, given a section $t \in E[N](S)$, its image $t(S)$ can be considered as a Cartier divisor on E.

A Drinfeld basis over S for $E[N]$ is then a pair of sections $\phi_1, \phi_2 \in E[N](S)$ which satisfy

$$\sum_{a,b \in \mathbb{Z}/N\mathbb{Z}} a \cdot \phi_1(S) + b \cdot \phi_2(S) = E[N] \tag{1.15}$$

as Cartier divisors of $E[N]$.

Let $\mu^*(N)$ be the group scheme $\mathbb{Z}[X]/(\Phi_N(X))$, where $\Phi_N(X)$ is the N-th cyclotomic polynomial.

There are two moduli problems which can be formed using the notion of a Drinfeld basis:

$$\mathcal{E}(N) : (Ell) \to (Sets) \tag{1.16}$$

$$E/S \mapsto \text{ the set of Drinfeld bases over } S \text{ for } E[N]$$

$$\mathcal{E}^{can}(N) : (Ell)/\mu^*(N) \to (Sets) \tag{1.17}$$

$$E/S/\mu^*(N) \mapsto \text{ the set of Drinfeld bases } \phi \text{ over } S \text{ for } E[N] \tag{1.18}$$

such that the Weil pairing $e_N(\phi)$ is the structure morphism of $S/\mu^*(N)$

We denote by $\mathcal{Y}(N)$ and $\mathcal{Y}^{can}(N)$, the moduli spaces associated to $\mathcal{E}(N)$ and $\mathcal{E}^{can}(N)$. The Weil pairing e_N gives a natural transformation of functors $e_N : \mathcal{Y}(N) \to \mu^*(N)$ by sending an isomorphism class $(E/S, \phi)$ to $e_N(\phi) \in \mu^*(N)(S)$.

Theorem 1.2.1 *(Drinfeld) For $N \geq 3$, there exists a fine moduli scheme $Y(N)$ for $\mathcal{E}(N)$. The characteristic zero geometric fibres of $Y(N)/Spec(\mathbb{Z})$ are smooth curves.*

Corollary 1.2.1 *Let $Y(N)$ be the fine moduli scheme given in Theorem 1.2.1.*

i. The Weil pairing e_N gives $Y(N)$ the structure of a $\mu^*(N)$-scheme.

ii. $Y(N)/\mu^*(N)$ is a fine moduli scheme for $\mathcal{E}^{can}(N)$.

iii. The characteristic zero geometric fibres of $Y(N)/\mu^*(N)$ are smooth connected curves.

For a discussion of these results, see sections 6, 7 of [MW84] and chapters 4, 5, 9 of [KM85].

The $\mu^*(N)$-scheme $Y(N)/\mu^*(N)$ given above represents the functor $\mathcal{Y}^{can}(N)$ on $(Sch/\mu^*(N))$. Its Spec($\mathbb{C}$)-fibres can be interpreted as follows: Let σ : Spec($\mathbb{C}$) $\to$ $\mu^*(N)$ be a morphism (such a morphism is given by a choice of embedding $\mathbb{Z}[X]/(\Phi_N(X)) \cong \mathbb{Z}[\zeta] \to \mathbb{C}$ and hence a specific choice of primitive N-th root of unity). The pull-back of $Y(N)/\mu^*(N)$ along σ gives a smooth connected curve in $(Sch/\mathbb{C})$, which we denote by $Y(N)_\sigma$/Spec($\mathbb{C}$). The curve $Y(N)_\sigma$/Spec($\mathbb{C}$) is seen to represent the functor $\mathcal{Y}^{can}_\sigma(N)$ which assigns to a scheme $S \in (Sch/\mathbb{C})$, the isomorphism classes of $(E/S, \phi)$ such that $e_N(\phi) \in \mu^*(N)(S)$ is the structure morphism of S/Spec($\mathbb{C}$) composed with σ. For instance, if $S = \mathbb{C}$, then $\mathcal{Y}^{can}_\sigma(N)(S)$ gives the isomorphism classes of $(E/\text{Spec}(\mathbb{C}), \phi)$ such that $e_N(\phi)$ is the primitive N-th root of unity determined by the morphism σ.

Level H-structures

Associated to a subgroup H of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ are the following two moduli problems:

$$\mathcal{E}_H(N) : (Ell) \to (Sets) \tag{1.19}$$
$$E/S \mapsto \text{ the set of Drinfeld bases over } S \text{ for } E[N]/H$$
$$\mathcal{E}^{can}_H(N) : (Ell)/\mu^*_H(N) \to (Sets) \tag{1.20}$$
$$E/S/\mu^*_H(N) \mapsto \text{ the set of Drinfeld bases } \phi \text{ over } S \text{ for } E[N]/H \text{ such that } e_N(\phi) \text{ is the structure morphism of } S/\mu^*_H(N)$$

where

i. a Drinfeld basis ϕ over S for $E[N]/H$ consists of the data (t_i, ϕ_i) where

   (a) $t_i : T_i \to S$ is an étale morphism

   (b) ϕ_i is a Drinfeld basis over T_i for $(E \times_S T_i)[N]$

   (c) $\phi_i = \phi_j$ when considered as Drinfeld bases over $T_i \times_S T_j$ for $(E \times_S (T_i \times_S T_j))[N]$

   (d) $S = \cup_i t_i(T_i)$

   and we identify two Drinfeld bases ϕ and ϕ' over S for $E[N]/H$ if and only if for each $T_i \times_S T'_j$ we have étale morphisms $u_{k,i,j} : U_{k,i,j} \to T_i \times_S T'_j$ such that

   (a) $\phi_i = h_{k,i,j}\phi'_j$ for some $h_{k,i,j} \in H$ when considered as Drinfeld bases over $U_{k,i,j}$ for $(E \times_S U_{k,i,j})[N]$

   (b) $T_i \times_S T'_j = \cup u_{k,i,j}(U_{k,i,j})$

(in fancier language, a Drinfeld basis over S for $E[N]/H$ is a Drinfeld basis for $E[N]$ locally for the étale topology and we identify two Drinfeld bases ϕ and ϕ' if and only if locally for the étale topology we have $\phi = h\phi'$ for $h \in H$)

ii. $\mu_H^*(N)$ is the quotient of $\mu^*(N)$ by H where the action of H on $\mu^*(N)$ is given by the determinant map.

For a discussion of level H-structures, see [DR72], Chapter 4, section 3. Since $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on the isomorphism classes of $(E/S, \phi)$ where $\phi \in \mathcal{E}(N)(E/S)$, we also obtain an action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the functor $\mathcal{Y}(N)$ and hence on the fine moduli scheme $Y(N)$ given by Theorem 1.2.1. By the properties of the Weil pairing e_N, the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $Y(N)$ and $\mu^*(N)$ are compatible with the structure morphism of $Y(N)/\mu^*(N)$.

Corollary 1.2.2 *Let $Y(N)$ be the fine moduli scheme given in Theorem 1.2.1 and suppose H is a subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$.*

i. The quotient scheme $Y_H(N) = Y(N)/H$ exists and is a coarse moduli scheme for $\mathcal{E}_H(N)$.

ii. The characteristic zero geometric fibres of $Y_H(N)/Spec(\mathbb{Z})$ are smooth curves.

Corollary 1.2.3 *Let $Y_H(N)$ be the coarse moduli scheme given in Corollary 1.2.2.*

i. The Weil pairing e_N gives $Y_H(N)$ the structure of a $\mu_H^*(N)$-scheme.

ii. $Y_H(N)/\mu_H^*(N)$ is a coarse moduli scheme for $\mathcal{E}_H^{can}(N)$.

iii. The characteristic zero geometric fibres of $Y_H(N)/\mu_H^*(N)$ are smooth connected curves.

For a discussion of these results, see sections 6, 7 of [MW84] and chapters 7, 8 of [KM85].

Using the fact that $Y_H(N)/\mu_H^*(N)$ is a coarse moduli scheme for $\mathcal{E}_H^{can}(N)$, one can interpret the $\mathrm{Spec}(\mathbb{C})$-fibres of $Y_H(N)/\mu_H^*(N)$ to a certain extent. Let $\sigma_H : \mathrm{Spec}(\mathbb{C}) \to \mu_H^*(N)$ be a morphism. The pull-back of $Y_H(N)/\mu_H^*(N)$ along σ_H gives a smooth connected curve in $(Sch/\mathbb{C})$, which we denote by $Y_H(N)_{\sigma_H}/\mathrm{Spec}(\mathbb{C})$. The $\mathrm{Spec}(\mathbb{C})$-points of $Y_H(N)_{\sigma_H}/\mathrm{Spec}(\mathbb{C})$ correspond to isomorphism classes $(E/\mathbb{C}, \phi)$, where ϕ is an H-equivalence class of bases for $E[N]$ and $e_N(\phi)$ is the H-equivalence class of primitive N-th roots of unity determined by the morphism σ_H.

Let $I = \pm 1$. The moduli spaces $\mathcal{Y}_I(N)$ and $\mathcal{Y}(N)$ are isomorphic because $(E/S, \phi) \cong (E/S, -\phi)$ by the -1 automorphism of E/S. Thus, $\mathcal{E}_I(N)$ is a moduli problem whose associated moduli space $\mathcal{Y}_I(N)$ is representable but is not rigid.

Representability in $(Var/\mathbb{C})$

One can be completely concrete so as to work with $(Var/\mathbb{C})$ instead of (Sch) and $(Ell)/(Var/\mathbb{C})$ instead of (Ell). In doing so, we can relate the scheme $Y(N)$ with the classical complex analytic description. This will be done in the following way: We show that the disconnected modular curve $Z(N) = (\Gamma(N)\backslash\mathfrak{H}) \times \mu^*(N)(\mathbb{C})$ is a *coarse moduli* $\mathbb{C}$*-variety* for the functor $\mathcal{E}(N)$ in the sense that the conditions of 1.2.6 are satisfied, but we only require that α be a bijection on the field $\mathbb{C}$. If $Y(N)/\mathrm{Spec}(\mathbb{C})$ is the $\mathrm{Spec}(\mathbb{C})$-fibre of $Y(N)/\mathrm{Spec}(\mathbb{Z})$, then $Y(N)/\mathrm{Spec}(\mathbb{C})$ is a coarse moduli scheme for $\mathcal{E}(N)$ on $(Ell)/(Var/\mathbb{C})$. By the universal property of $Z(N)$, there exists a morphism $\beta : Z(N) \to Y(N)/\mathrm{Spec}(\mathbb{C})$ which is seen to be bijective on $\mathbb{C}$. Since we are working in $(Var/\mathbb{C})$, this implies that β is an isomorphism.

Let first us consider the case of $\mathcal{P}(1)$. This moduli problem assigns to an elliptic curve E/S a fixed one element set. Thus, $\mathcal{M}(1)$ is the functor which assigns to a variety S, the isomorphism classes of elliptic curves E/S.

Classically, one constructs $\Gamma(1)\backslash\mathfrak{H}^*$ as a compact Riemann surface which then inherits the structure of a unique smooth projective curve in $(Var/\mathbb{C})$, which in this case is isomorphic to the projective line by the classical j-function. The open Riemann surface $Z(1) = \Gamma(1)\backslash\mathfrak{H}$ is then isomorphic to the affine line $\mathrm{Spec}(\mathbb{C}[j])$. To show that $Z(1)$ is a coarse moduli scheme for $\mathcal{P}(1)$ by hand, we need to address the following points.

First of all, one requires a natural transformation of functors $\alpha : \mathcal{M}(\cdot) \to \mathrm{Hom}(\cdot, Z(1))$. This amounts to assigning to an isomorphism class of E/S, a morphism $\alpha(E/S) : S \to Z(1)$. This assignment must be natural in the sense that if $\sigma : S' \to S$ and E'/S' is the pull-back of E/S along σ, then we have $\alpha(E'/S') = \alpha(E/S) \circ \sigma$.

The main point in constructing α is the ability to obtain a Weierstrass model for any E/S. By a Weierstrass model for E/S, we mean an open cover $S = \cup_\lambda U_\lambda$ such that

i. $U_\lambda = \mathrm{Spec}(R_\lambda)$ where R_λ

ii. $E\mid_{U_\lambda}/U_\lambda \cong \mathrm{Spec}(R_\lambda[X,Y]/(Y^2 - (4X^3 - g_{2,\lambda}X - g_{3,\lambda})))/\mathrm{Spec}(R_\lambda)$ for some $g_{2,\lambda}, g_{3,\lambda} \in R_\lambda$

The desired morphism from S to $Z(1) = \mathrm{Spec}(\mathbb{C}[j])$ is then given by the expression of the j-invariant in terms of the coefficients $g_{2,\lambda}, g_{3,\lambda} \in R_\lambda$. That is, we define a morphism on $j : S \to \mathrm{Spec}(\mathbb{C}[j])$ by defining it on the open sets $j_\lambda : U_\lambda = \mathrm{Spec}(R_\lambda) \to \mathrm{Spec}(\mathbb{C}[j])$, which amounts to defining a $\mathbb{C}$-algebra homomorphism $j_\lambda : \mathbb{C}[j] \to R_\lambda$ and hence expressing j in terms of elements in R_λ. The particular expression we take is nothing but $j = g_{2,\lambda}^3/(g_{2,\lambda}^3 - 27g_{3,\lambda}^2)$. Note that the discriminant $\Delta = g_{2,\lambda}^3 - 27g_{3,\lambda}^2$ is invertible in R_λ since $E\mid_{U_\lambda}$ is an elliptic curve over $U_\lambda = \mathrm{Spec}(R_\lambda)$. One can check that this defines a morphism $j : S \to \mathrm{Spec}(\mathbb{C}[j])$ and that this association gives us the desired natural transformation α.

Now, by construction of $Z(1)$,

$$\alpha(\mathrm{Spec}(\mathbb{C})) : \mathcal{M}(1)(\mathrm{Spec}(\mathbb{C})) \to \mathrm{Hom}(\mathrm{Spec}(\mathbb{C}), Z(1))$$

is bijective (see section 1.2 for more details). We have therefore obtained a pair $(Z(1), \alpha)$ which satisfies the first property of 1.2.6 for $\Omega = \mathbb{C}$. We now need to check that $Z(1)$ is universal with respect to this property. One way to do this would be to construct an elliptic curve $E/Z(1)$ whose fibre at a $\mathbb{C}$-point of $Z(1)$ is in the isomorphism class of elliptic curves it is supposed to represent. Then, if $(\mathbb{M}', \alpha')$ is another pair which satisfies the first property of 1.2.6 for $\Omega = \mathbb{C}$, one obtains a morphism $\alpha'(E/Z(1)) : Z(1) \to \mathbb{M}'$, and hence a natural transformation of functors $\beta : \mathrm{Hom}(\cdot, Z(1)) \to \mathrm{Hom}(\cdot, \mathbb{M}')$. The property of the fibres of $E/Z(1)$ allow us to deduce that $\alpha' = \beta \circ \alpha$ on $\mathbb{C}$. Since we are working in $(Var/\mathbb{C})$, this implies that $\alpha' = \beta \circ \alpha$ on all of $(Var/\mathbb{C})$ and that β is uniquely determined.

The problem is therefore reduced to finding a family $E/Z(1)$ as above. One can certainly come close to writing down such a family:

$$E/Z(1) : \mathrm{Spec}(\mathbb{C}[j][X,Y]/(Y^2 - (X^3 - 27\frac{j}{j-1728}X + 54\frac{j}{j-1728})) \quad (1.21)$$

However, $E/Z(1)$ is not an elliptic curve since for $j = 0, 1728$ the fibres are not elliptic curves. Moreover, it is not possible to write down an elliptic curve $E/Z(1)$ with the required property: any such elliptic curve is a twist of the one given above, but by inspection of the Weierstrass equations for the twists of the above family one sees that it is not possible to twist the above family so that its fibres are elliptic curves for all j-invariants.

We can remedy this problem in the following way. Let G be a finite group which acts on $S \in (Var/\mathbb{C})$ in such a way that the quotient $q : S \to S/G$ exists and the inverse image of a $\mathbb{C}$-point in S/G is the G-orbit of a $\mathbb{C}$-point in S. Suppose that $S/G \cong Z(1)$ and that we have an elliptic curve E/S with the property that two $\mathbb{C}$-fibres E_s and E_t are isomorphic if and only if the two $\mathbb{C}$-points s and t of S lie in the same G-orbit. Also, if s is a $\mathbb{C}$-point of S, then E_s is in isomorphism class of elliptic curves represented by the point $q(s) \in Z(1)$.

Now suppose $(\mathbb{M}', \alpha')$ is another pair satisfying the first property of 1.2.6 for $\Omega = \mathbb{C}$. If we have all of the above, then using α', we obtain a morphism $\alpha'(E/S) : S \to \mathbb{M}'$. Moreover, it is clear that this morphism is G-equivariant so by the universal property of quotients, we see that $\alpha(E/S)$ factors through a unique morphism $\beta : Z(1) \to \mathbb{M}'$. One can then check that the existence of β gives $(Z(1), \alpha)$ the desired universal property.

Thus, it remains to show such a E/S exists. We take

$$S = \mathrm{Spec}(\mathbb{C}[j, j^{1/3}, (j-1728)^{1/2}]) \quad (1.22)$$

which is easily seen to be isomorphic to the elliptic curve $\mathrm{Spec}(\mathbb{C}[T,U]/(U^2 - (T^3 - 1728))$ (i.e. make the substitutions $T^3 = j$, $U^2 = (j - 1728)$). There is an action of $\{\pm 1, \pm\zeta_3, \pm\zeta_3^{-1}\}$ on S such that $S/G \cong \mathrm{Spec}(\mathbb{C}[j])$ exists and the inverse image of a $\mathbb{C}$-point is the G-orbit of a $\mathbb{C}$-point.

We define E/S to be

$$E/S : \mathrm{Spec}(\mathbb{C}[T,U,X,Y]/(Y^2-(X^3-27TX+54U), U^2-(T^3-1728))) \tag{1.23}$$

It is not hard to check that E/S has the desired properties. For instance, E has j-invariant equal to $T^3 = j$. Thus, $Z(1)$ is a coarse moduli $\mathbb{C}$-variety for $\mathcal{P}(1)$.

One can imagine a similar argument to show that $Z(N) = (\Gamma(N)\backslash\mathfrak{H}) \times \mu^*(N)(\mathbb{C})$ is a coarse moduli scheme for $\mathcal{E}(N)$, again working in $(Var/\mathbb{C})$ and $(Ell)/(Var/\mathbb{C})$. Let $Y^2 = 4X^3 - g_2X - g_3$ be an elliptic curve over S and let $\phi : \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \cong E[N]$ be a basis over S for $E[N]$. For $a \in \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, we define the Fricke invariants as:

$$f_a^{\phi} = \frac{g_2g_3}{\Delta} \cdot (\text{ X-coordinate of } \phi(a)) \tag{1.24}$$

$$f_a^{2,\phi} = \frac{g_2^2}{\Delta} \cdot (\text{ X-coordinate of } \phi(a))^2 \tag{1.25}$$

$$f_a^{3,\phi} = \frac{g_3}{\Delta} \cdot (\text{ X-coordinate of } \phi(a))^3. \tag{1.26}$$

Note that

$$f_a^{2,\phi} = \frac{1}{4^3(j-1728)}(f_a^{\phi})^2 \tag{1.27}$$

$$f_a^{3,\phi} = \frac{1}{48^3 j(j-1728)}(f_a^{\phi})^3. \tag{1.28}$$

It is a fact that the function field of $X(N)$ is $\mathbb{C}(j(\tau), f_a(\tau))$ where $j(\tau)$ and $f_a(\tau)$ are the invariants of the elliptic curve $E_\tau = \mathbb{C}/ < 1, \tau >$ with ϕ taken to be the basis $(1/N, \tau/N)$ (see Proposition 6.9 in [Shi71]). The coordinate ring of the affine curve $Y(N)$ is the subalgebra $\mathbb{C}[j(\tau), f_a(\tau)]$ of $\mathbb{C}(j(\tau), f_a(\tau))$. Thus, given $(E/S, \phi)$, we can define a morphism $S \to Y(N)$ in a way similar by using the invariants j, f_a^{ϕ}. In case that $Aut(E/S) = \mu_4, \mu_6$, we use the Fricke invariants $f_a^{2,\phi}, f_a^{3,\phi}$, respectively.

As a result of the above discussion, we obtain:

Lemma 1.2.1 *Let $Y(N)$ be the fine moduli scheme given in Theorem 1.2.1. The Spec($\mathbb{C}$)-fibre of $Y(N)/Spec(\mathbb{Z})$ is isomorphic to $(\Gamma(N)\backslash\mathfrak{H}) \times \mu^*(N)(\mathbb{C})$.*

Lemma 1.2.2 *Let $Y(N)/\mu^*(N)$ be the fine moduli scheme given in Corollary 1.2.1. The Spec($\mathbb{C}$)-fibre of $Y(N)/\mu^*(N)$ along a morphism σ : Spec($\mathbb{C}$) $\to \mu^*(N)$ is isomorphic to $\Gamma(N)\backslash\mathfrak{H}$.*

Lemma 1.2.3 *Suppose $H \subset GL_2(\mathbb{Z}/N\mathbb{Z})$. Let $Y_H(N)$ be the coarse moduli scheme given in Corollary 1.2.2. The Spec($\mathbb{C}$)-fibre of $Y_H(N)/Spec(\mathbb{Z})$ is isomorphic to $(\Gamma_H(N)\backslash\mathfrak{H}) \times \mu_H^*(N)(\mathbb{C})$.*

Lemma 1.2.4 *Suppose $H \subset GL_2(\mathbb{Z}/N\mathbb{Z})$. Let $Y_H(N)/\mu_H^*(N)$ be the coarse moduli scheme given in Corollary 1.2.3. The Spec($\mathbb{C}$)-fibre of $Y_H(N)/\mu_H^*(N)$ along a morphism σ_H : Spec($\mathbb{C}$) $\to \mu_H^*(N)$ is isomorphic to $\Gamma_H(N)\backslash\mathfrak{H}$.*

$\mathbb{C}$-points of $Y(N)$

In this section, we consider the disconnected modular curve $Z(N) = (\Gamma(N)\backslash\mathfrak{H})\times \mu^*(N)(\mathbb{C})$ and the natural transformation of functors $\alpha : \mathcal{Y}(N)(\cdot) \to \mathrm{Hom}(\cdot, Z(N))$ which gives it the structure of a coarse moduli scheme for $\mathcal{E}(N)$. Again, we work in $(Var/\mathbb{C})$ and $(Ell)/(Var/\mathbb{C})$. We show that α is bijective on the field $\mathbb{C}$.

Given $(E/\mathbb{C}, \phi)$, we can represent it in the form $(\mathbb{C}/ < \omega_1, \omega_2 >, (\omega_1, \omega_2)P)$ where $< \omega_1, \omega_2 >= \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is a lattice in $\mathbb{C}$ and P is a matrix in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We can make this representation a bit more canonical by choosing a basis so that $P = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$. Furthermore, the pair $(\mathbb{C}/ < \omega_1, \omega_2 >, (\omega_1/N, d \cdot \omega_2/N)) \cong (\mathbb{C}/ < 1, \tau >, (1/N, d \cdot \tau/N))$ where $\tau \in H$.

It is not hard to check that two pairs $(\mathbb{C}/ < 1, \tau >, (1/N, d \cdot \tau/N))$ and $(\mathbb{C}/ < 1, \tau' >, (1/N, d' \cdot \tau'/N))$ are isomorphic if and only if τ and τ' are equivalent under a transformation in $\Gamma(N)$ and $d = d' \in (\mathbb{Z}/N\mathbb{Z})^\times \cong \mu^*(N)(\mathbb{C})$.

Thus, given an isomorphism class $(E/\mathbb{C}, \phi) \in \mathcal{Y}(N)(\mathbb{C})$, we can associate to it a point on $Z(N)$, namely, write the isomorphism class $(E/\mathbb{C}, \phi)$ in the form $(\mathbb{C}/ < 1, \tau >, (1/N, d \cdot \tau/N))$ and send it to the point $(\tau, \exp^{2\pi i d/N}) \in Z(N)(\mathbb{C})$. By the remarks above, this defines a bijection between $\mathcal{Y}(N)(\mathbb{C})$ to $Z(N)(\mathbb{C})$. This is precisely the association given by the functor α. Therefore, α is bijective on the field $\mathbb{C}$.

K-points of $Y_H(N)$

Suppose $H \subset \mathrm{GL}(\mathbb{Z}/N\mathbb{Z})$ is a subgroup containing ± 1 and $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$. Let $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ be the $\mathrm{Spec}(\mathbb{Q})$-fibre of $Y_H(N)/\mathrm{Spec}(\mathbb{Z})$. The $\mathrm{Spec}(\mathbb{C})$-fibre of $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ is isomorphic to the smooth connected curve $\Gamma_H(N)\backslash\mathfrak{H}$ by Lemma 1.2.3. Thus, $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ provides a $\mathbb{Q}$-model for the curve $\Gamma_H(N)\backslash\mathfrak{H}$.

We wish to interpret the K-points of $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ where K is a field extension of $\mathbb{Q}$. We know that $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ is a coarse moduli scheme for $\mathcal{E}_H(N)$, considered as a functor on $(Ell)/\mathbb{Q}$. Therefore, the set $\mathcal{Y}_H(N)(\mathrm{Spec}(K))$ consists of the isomorphism classes of pairs $(E/K, [\phi]_H)$ where $\phi \in \mathcal{E}_H(N)(\mathrm{Spec}(K))$ (note: ϕ is defined over K!). Let $\sigma : \mathrm{Spec}(\mathbb{C}) \to \mathrm{Spec}(K)$ be a morphism. Consider the following diagram in $(Sch/\mathbb{Q})$:

$$\begin{array}{ccc} \mathcal{Y}_H(N)(\mathrm{Spec}(K)) & \xrightarrow{\alpha} & \mathrm{Hom}(\mathrm{Spec}(K), Y_H(N)) \\ \sigma\downarrow & & \sigma\downarrow \\ \mathcal{Y}_H(N)(\mathrm{Spec}(\overline{K})) & \xrightarrow{\alpha} & \mathrm{Hom}(\mathrm{Spec}(\overline{K}), Y_H(N)) \end{array} \tag{1.29}$$

We note that α on the bottom is a bijection as $Y_H(N)$ is a coarse moduli scheme for $\mathcal{E}_H(N)$. Also, since $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ is a $\mathbb{Q}$-model for its $\mathrm{Spec}(\overline{K})$-fibre, we see that $\sigma : \mathrm{Hom}(\mathrm{Spec}(K), Y_H(N)) \to \mathrm{Hom}(\mathrm{Spec}(\overline{K}), Y_H(N))$ is an injective map. Thus, we see that two pairs $(E/K, [\phi]_H)$ and $(E'/K, [\phi']_H)$ when

considered as K-points of $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ under α are equivalent if and only if they are isomorphic over $\overline{K}$. Thus, this is the sense in which $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ fails to represent $\mathcal{Y}_H(N)$ on $(Sch/\mathbb{Q})$.

On the other hand, $\alpha(\mathrm{Spec}(K))$ is surjective so given a K-rational point P of $Y_H(N)$, there is exists a pair $(E,[\phi]_H) \in \mathcal{Y}_H(N)(\mathrm{Spec}(K))$ to which it corresponds, [DR72], Chapter 6, section 5, Proposition 3.2. The main idea of the proof is to consider the pair $(E,[\phi]_H) \in \mathcal{Y}_H(N)(\mathrm{Spec}(\overline{K}))$ which corresponds to the point P. One can construct an obstruction class associated to this pair in $H^2(\mathrm{Gal}(\overline{K} \mid K), \mathrm{Aut}_{\overline{K}}(E,[\phi]_H))$ which is trivial if and only if $(E,[\phi]_H)$ can be defined over K, [Gir71], section 7.3. The argument in [DR72] then shows the cohomology group above is trivial.

The surjectivity of $\alpha(\mathrm{Spec}(K))$ can also be seen in a more bare-handed approach. As before, a K-rational point P of $Y_H(N)$ corresponds uniquely to a $\overline{K}$-isomorphism class $(E,[\phi]_H) \in \mathcal{Y}_H(N)(\mathrm{Spec}(\overline{K}))$. Since P maps to a K-rational point of $Y(1)$, we see that the j-invariant of E is K-rational. Therefore, by a suitable $\overline{K}$-isomorphism, we may assume that E is defined over K. The actions of $\mathrm{Gal}(\overline{K} \mid K)$ on $\mathcal{Y}_H(N)(\mathrm{Spec}(\overline{K}))$ and $Y_H(N)(\mathrm{Spec}(\overline{K}))$ are compatible with the morphism $\alpha(\mathrm{Spec}(\overline{K}))$. Therefore, since P corresponds to a K-rational point of $Y_H(N)(\mathrm{Spec}(\overline{K}))$, we see for all $\sigma \in \mathrm{Gal}(\overline{K} \mid K)$ that $[\phi]_H^\sigma = [\zeta][\phi]_H$ where $[\cdot] : \mu_n/\nu \to \mathrm{Aut}_{\overline{K}}(E)$, $\zeta \in \mu_n/\nu$, and ν is the intersection of H and the image of $\mathrm{Aut}(E)$ in $\mathrm{Aut}(E[N])$. Hence, we obtain a representation $\rho : \mathrm{Gal}(\overline{K} \mid K) \to \mu_n/\nu$. Since $\pm 1 \in H$, ν contains at least ± 1. For simplicity, let us consider the case $n = 4$. If ρ is trivial, then $(E,[\phi]_H)$ is already defined over K, otherwise $\nu = \{\pm 1\}$ and ρ is surjective to $\mu_4/\{\pm 1\}$. Let $\psi : E \to E_D$ be the isomorphism defined over $\overline{K}$ from E/K to a twist E_D/K. One can easily check that

$$\psi(\phi)^\sigma = [\zeta_\sigma]\psi(\phi^\sigma) = [\zeta_\sigma][\rho(\sigma)]\psi(\phi) \tag{1.30}$$

for $\sigma \in \mathrm{Gal}(\overline{K} \mid K)$ where ζ_σ is the 1-cocycle associated to the twist E_D. Let $L = K(\sqrt{D_0})$ be the quadratic extension associated to ρ. If we consider the particular twist $D = D_0$, it is easy to see that $[\zeta_\sigma][\rho(\sigma)] = \pm 1$. Hence, the twisted pair $(E_D/K,[\psi(\phi)]_H)$ is defined over K.

The description of the K-points of $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ above can be reinterpreted in terms of galois representations. A K-point of $Y_H(N)/\mathrm{Spec}(\mathbb{Q})$ is a pair $(E/K,[\phi]_H)$. Since it is defined over K, we see that for all $\sigma \in \mathrm{Gal}(\overline{K} \mid K)$, $(E/K,[\phi]_H)^\sigma = (E/K,[\phi]_H)$. The condition $[\phi]_H^\sigma = [\phi]_H$ means that the $\mathrm{Gal}(\overline{K} \mid K)$ representation on $E[N]$ lies in the subgroup $H \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Finally, we note the following curious phenomenon. Consider the following two subgroups:

$$I = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \tag{1.31}$$

$$D = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & * \end{pmatrix} \right\}. \tag{1.32}$$

The Spec($\mathbb{C}$)-fibre of $Y_I(N)/\mathrm{Spec}(\mathbb{Z})$ and $Y_D(N)/\mathrm{Spec}(\mathbb{Z})$ are, respectively:

$$Y_I(N)/\mathrm{Spec}(\mathbb{C}) \cong (\Gamma_I(N)\backslash\mathfrak{H}) \times \mu^*(N)(\mathbb{C}) \tag{1.33}$$
$$Y_D(N)/\mathrm{Spec}(\mathbb{C}) \cong (\Gamma_D(N)\backslash\mathfrak{H}). \tag{1.34}$$

We note that $\Gamma_D = \Gamma_I$ so that $Y_I(N)$ consists of $\phi(N)$ copies of $Y_D(N)/\mathrm{Spec}(\mathbb{C})$. Since $Y_D(N)/\mathrm{Spec}(\mathbb{C})$ has a $\mathbb{Q}$-model, it follows that $Y_I(N)/\mathrm{Spec}(\mathbb{C})$ also has a $\mathbb{Q}$-model, even though it is most naturally defined over $\mathbb{Q}(\zeta_N)$.

Compactifications

It will be convenient to consider compactifications $X(N)$, $X_H(N)$, $X(N)/\mu^*(N)$, $X_H(N)/\mu_H^*(N)$ of the modular curves $Y(N)$, $Y_H(N)$, $Y(N)/\mu^*(N)$, $Y_H(N)/\mu_H^*(N)$. One can describe the extra points in the compactification as corresponding to Néron polygons with level structure up to a certain equivalence relation [DR72], but we content ourselves with noting that the Spec($\mathbb{C}$)-fibres of $X(N)$, $X_H(N)$, $X(N)/\mu^*(N)$, $X_H(N)/\mu_H^*(N)$ are smooth projective curves over $\mathbb{C}$ given by

$$X(N) : (\Gamma(N)\backslash\mathfrak{H}^*) \times \mu^*(N)(\mathbb{C}) \tag{1.35}$$
$$X_H(N) : (\Gamma_H(N)\backslash\mathfrak{H}^*) \times \mu_H^*(N)(\mathbb{C}) \tag{1.36}$$
$$X(N)/\mu^*(N) : \Gamma(N)\backslash\mathfrak{H}^* \tag{1.37}$$
$$X_H(N)/\mu_H^*(N) : \Gamma_H(N)\backslash\mathfrak{H}^* \tag{1.38}$$

where $\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$.

1.3 Complex multiplication points

The general philosophy behind the study of rational points of $X_H(N)$ is that for large N, the only non-cuspidal rational points of $X_H(N)$ should arise from complex multiplication curves. In this section, we discuss how elliptic curves with complex multiplication give rise to rational points on the curves $X_H(p)$ where p is a prime.

Proposition 1.3.1 *Let E be an elliptic curve defined over L with complex multiplication by a maximal order $\mathfrak{r}$ in K. Then the Gal($\overline{L}|L$) representation on $E[p]$ has image lying in:*

$$\begin{cases} \textit{the normaliser of a non-split Cartan subgroup} & \textit{if } p \textit{ is inert in } \mathfrak{r} \\ \textit{a Borel subgroup} & \textit{if } p \textit{ is ramified in } \mathfrak{r} \\ \textit{the normaliser of a split Cartan subgroup} & \textit{if } p \textit{ is split in } \mathfrak{r} \end{cases}$$

Proof. Let $M = L \cdot K$ and let $\mathrm{End}(E) = \mathfrak{r}$ be an order in K. Since the action of galois commutes with the action of $\mathfrak{r}$ on $E[p]$, we see that $E[p]$ can be considered as a $(\mathfrak{r}/p\mathfrak{r})[\mathrm{Gal}(\overline{M}|M)]$-module. Since $E[p]$ is a free rank one $\mathfrak{r}/p\mathfrak{r}$-module, the image of the mod p representation of $\mathrm{Gal}(\overline{M}|M)$ lies in $(\mathfrak{r}/p\mathfrak{r})^\times$.

However, $(\mathfrak{r}/p\mathfrak{r})^\times \cong (\mathbb{F}_{p^2})^\times, (\mathbb{F}_p[\epsilon])^\times, (\mathbb{F}_p{}^2)^\times$ depending on whether p is inert, ramified, split in $\mathfrak{r}$. It follows that the image of the mod p representation of $\mathrm{Gal}(\overline{M}|M)$ lies in a non-split Cartan, unitriangular, split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Therefore, the image of the mod p representation of $\mathrm{Gal}(\overline{L}|L)$ lies in the normaliser of these subgroups. □

Consider the case of H a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. The modular curve $X_H(p)$ is then the modular curve $X_0(p)$. From the general philosophy alluded to above, for p large enough the non-cuspidal $\mathbb{Q}$-rational points of $X_0(p)$ should only arise from complex multiplication curves over $\mathbb{Q}$. However, there are only finitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ with complex multiplication and in order for such a curve to give rise to a $\mathbb{Q}$-rational point of $X_0(p)$, p must be ramified in the CM-fields of these curves. This restricts p to a finite number of primes which divide the discriminants of the CM-fields involved. Hence, in this case, we see that for p large enough, there should not be any non-cuspidal $\mathbb{Q}$-rational points on $X_0(p)$. Indeed, this should be the case once p is larger than the largest discriminant of a CM-field of an elliptic curve over $\mathbb{Q}$, that is, $p > 163$. This is the famous result of Mazur [Maz78].

On the other hand, if H is the normaliser of a (split/non-split) Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, then an elliptic curve defined over $\mathbb{Q}$ with complex multiplication in K will give rise to a $\mathbb{Q}$-rational point of $X_H(p)$ if p is split/inert in K. Thus, in this case, $X_H(p)$ will in general have some non-cuspidal $\mathbb{Q}$-rational points arising from complex multiplication curves, though by the general philosophy, these should be the only ones for p large enough. Momose has made obtained some results using methods of Mazur in the split case [Mom84]. A related result of Serre [Ser72] states for a *fixed* elliptic curve over $\mathbb{Q}$, its mod p galois representation has image $\mathrm{GL}_2(\mathbb{F}_p)$ for p larger than some bound which is dependent on the elliptic curve. This bound can be made explicit [MW93].

There exists a class of modular curves which have more refined modular interpretations, called "twisted modular curves" in [Maz77]. Given a mod p representation ρ, it is possible to associate to a certain $\overline{\mathbb{Q}}$-twist $X_\rho(p)$ of $X_D(p)$ such that the $\mathbb{Q}$-points of this twisted modular curve correspond to the $\mathbb{Q}$-isomorphism classes of elliptic curves E over $\mathbb{Q}$ such that $\rho_{E,p} \cong \rho$. In particular, let S be the set of elliptic curves over $\mathbb{Q}$ which have complex multiplication in K where p is inert. The $\mathbb{Q}$-points of the twisted modular curves $X_{\rho_{E,p}}$ where $E \in S$ give all elliptic curves over $\mathbb{Q}$ with mod p representation isomorphic to a (non-split) complex multiplication mod p representation. If the general philosophy about the $\mathbb{Q}$-points of $X^+_{\text{non-split}}(p)$ is to be believed, then for p large enough, the only $\mathbb{Q}$-point on $X_{\rho_{E,p}}$ should arise from E itself. A more detailed description of this class of twisted modular curves is described in [SR95]. They are used in the final stages to Wiles' proof of Fermat's Last Theorem to deal with the case of reducible mod 3 representations.

1.4 Double coset operators on Fuchsian groups

Let Γ be a Fuchsian group of the first kind. Then $X_\Gamma = \Gamma\backslash\mathfrak{H}^*$ is a compact Riemann surface. Associated to Γ is its vector space of weight k cusp forms $S_k(\Gamma)$. In this section, we will describe some natural linear operators on $S_k(\Gamma)$ which we call double coset operators. We will also interpret these operators geometrically in case of $k = 2$.

Action on $S_k(\Gamma)$

To define a double coset operator on $S_k(\Gamma)$, we start with a double coset $\Gamma\delta\Gamma$ where $\delta \in \mathrm{GL}_2(\mathbb{R})^+$. From the Lemma below, we see that if δ lies in the commensurator $\tilde{\Gamma}$ of Γ (i.e. those elements in $\mathrm{GL}_2(\mathbb{R})^+$ which conjugate Γ to a group which is commensurable with Γ), the double coset $\Gamma\delta\Gamma$ can be decomposed into a finite union of cosets $\cup_{\lambda\in\Lambda}\Gamma\delta\lambda$. We define the linear operator $\Theta_k(\Gamma\delta\Gamma)$ as:

$$\Theta_k(\Gamma\delta\Gamma) : S_k(\Gamma) \to S_k(\Gamma) \tag{1.39}$$

$$f \mapsto \det(\delta)^{k/2-1}\sum_{\lambda\in\Lambda} f\mid_{\delta\lambda} \tag{1.40}$$

It is easily checked that $\Theta_k(\Gamma\delta\Gamma)$ sends $S_k(\Gamma)$ to itself and is thus a linear operator on the vector space $S_k(\Gamma)$(see Proposition 3.37 in [Shi71]). We call the linear operator $\Theta_k(\Gamma\delta\Gamma)$ *a double coset operator.* The definition of $\Theta_k(\Gamma\delta\Gamma)$ does not depend on the choice of Λ by invariance of $f \in S_k(\Gamma)$ by Γ.

Lemma 1.4.1 *Let $\delta \in GL_2(\mathbb{R})^+$ and let Γ be a Fuchsian group. The following are equivalent:*

i. $\Gamma\delta\Gamma = \cup_{\lambda\in\Lambda}\Gamma\delta\lambda$ *where* $\Lambda \subset \Gamma$ *and the cosets* $\Gamma\delta\lambda$ *are all distinct.*

ii. Λ *forms a complete set of inequivalent representatives for* $(\Gamma \cap \delta^{-1}\Gamma\delta)\backslash\Gamma$.

Proof. Note firstly that $\lambda, \lambda' \in \Gamma$, $\Gamma\delta\lambda = \Gamma\delta\lambda'$ if and only if $(\Gamma \cap \delta^{-1}\Gamma)\delta\lambda = (\Gamma \cap \delta^{-1}\Gamma\delta)\lambda'$.

Suppose that $\Gamma = \cup_{\lambda\in\Lambda}(\Gamma \cap \delta^{-1}\Gamma\delta)\lambda$. Multiplying on the left by $\Gamma\delta$ we obtain $\Gamma\delta\Gamma = \cup_{\lambda\in\Lambda}(\Gamma\delta\Gamma \cap \Gamma\delta)\lambda = \cup_{\lambda\in\Lambda}\Gamma\delta\lambda$. By the opening remark, all these cosets are distinct.

Suppose that $\Gamma\delta\Gamma = \cup_{\lambda\in\Lambda}\Gamma\delta\lambda$ where $\Lambda \subset \Gamma$ and the cosets $\Gamma\delta\lambda$ are all distinct. By the opening remark, Λ forms an inequivalent set of representatives for $\Gamma \cap \delta^{-1}\Gamma\delta\backslash\Gamma$. On the other hand, for any $\lambda \in \Gamma$, $\Gamma\delta\lambda$ occurs in $\Gamma\delta\Gamma$ so that Λ forms a complete set of inequivalent representatives. □

Define $\mathcal{T}(\Gamma)$ to be the free $\mathbb{Z}$-module generated by the set of double cosets $\Gamma\delta\Gamma$ where $\delta \in \tilde{\Gamma}$. One can define a multiplication on $\mathcal{T}(\Gamma)$ by extending $\mathbb{Z}$-linearly the following rule:

$$\Gamma\delta\Gamma \cdot \Gamma\delta'\Gamma = \sum_{\alpha\in\Upsilon}\Gamma\alpha\delta'\Gamma$$

where $\Gamma\delta\Gamma = \cup_{\alpha\in\Upsilon}\Gamma\alpha$. The resulting multiplication is well-defined, associative, and $\mathbb{Z}$-linear so that $\mathcal{T}(\Gamma)$ becomes a $\mathbb{Z}$-algebra (see section 3.1 in [Shi71]).

The map which sends $\Gamma\delta\Gamma$ to $\Theta_k(\Gamma\delta\Gamma)$ defines a representation Θ_k of the $\mathbb{Z}$-algebra $\mathcal{T}(\Gamma)$ to the $\mathbb{Z}$-algebra $\mathrm{End}(S_k(\Gamma))$. We will often abuse notation and not make this representation explicit.

The map which sends $\Gamma\delta\Gamma$ to the integer $|\Gamma \cap \delta^{-1}\Gamma\delta\backslash\Gamma|$ defines a representation $\deg : \mathcal{T}(\Gamma) \to \mathbb{Z}$.

Action on $S_2(\Gamma)$

The action of double coset operators on $S_2(\Gamma)$ can be interpreted as endomorphisms of $J(X_\Gamma)$, essentially because $S_2(\Gamma)$ is the cotangent space to the complex torus associated to $J(X_\Gamma)$.

Let $\delta \in \tilde{\Gamma}$. The map $z \mapsto \delta^{-1}(z)$ induces a morphism w_δ from $X_{\delta\Gamma\delta^{-1}\cap\Gamma}$ to $X_{\Gamma\cap\delta^{-1}\Gamma\delta}$. Hence, we have the following diagram:

$$\begin{array}{ccc} X_{\delta\Gamma\delta^{-1}\cap\Gamma} & \xrightarrow{w_\delta} & X_{\Gamma\cap\delta^{-1}\Gamma\delta} \\ {\scriptstyle\pi_1}\downarrow & & {\scriptstyle\pi_2}\downarrow \\ X & & X \end{array} \tag{1.41}$$

Define T_δ as the endomorphism of $\mathrm{Div}(X_\Gamma)$ given by $\pi_{1*}w_\delta{}^*\pi_2{}^*$. The fact the w_δ is a morphism means that T_δ factors to an endomorphism $\Theta_k(T_\delta)$ of $J(X_\Gamma)$.

The following Lemmas are easily verified:

Lemma 1.4.2 *Let Λ be a complete set of inequivalent representatives for $(\Gamma \cap \delta^{-1}\Gamma\delta)\backslash\Gamma$. The endomorphism T_δ of $Div(X_\Gamma)$ is explicitly given by:*

$$T_\delta(\Gamma z) = \sum_{\lambda\in\Lambda} \Gamma\delta\lambda z. \tag{1.42}$$

Lemma 1.4.3 *Let $\gamma_1, \gamma_2 \in \Gamma$. Then $T_\delta = T_{\gamma_1\delta\gamma_2}$ as endomorphisms of $Div(X_\Gamma)$.*

Given a double coset $\Gamma\delta\Gamma$, one can associate to it a well-defined endomorphism $T_{\Gamma\delta\Gamma}$ of $\mathrm{Div}(X_\Gamma)$ by Lemma 1.4.3. The endomorphism $\Theta_2(T_{\Gamma\delta\Gamma})$ of $J(X_\Gamma)$ it induces coincides with the endomorphism $\Theta_2(\Gamma\delta\Gamma)$ of $S_2(\Gamma)$ defined in the previous section under the identification of $S_2(\Gamma)$ with the cotangent space of $J(X_\Gamma)$.

More generally, suppose that Γ_1 and Γ_2 are commensurable so that they both have the same commensurator. In weight $k = 2$, the double coset operator $\Theta_k(\Gamma_1\delta\Gamma_2)$ can be interpreted as a divisorial correspondence from X_{Γ_1} to X_{Γ_2}. Such a correspondence is called a modular correspondence and induces a homomorphism from $J(X_{\Gamma_1})$ to $J(X_{\Gamma_2})$. Formally, all homomorphisms of jacobians arise from a divisorial correspondence. One may ask whether the isogeny under investigation is given by a linear combination of modular correspondences. Recent work by Edixhoven (to be discussed in the conclusion) has answered this in the affirmative.

1.5 Arithmetic congruence groups

In this section, we define a certain class of Fuchsian groups of the first kind called *arithmetic congruence groups* and discuss the notion of a Hecke operator on them. This class of Fuchsian groups is derived from *indefinite* quaternion algebras over $\mathbb{Q}$ and includes the groups $\Gamma^+_{\text{split}}(p)$ and $\Gamma^+_{\text{non-split}}(p)$ for which we are interested in obtaining an explicit trace formula.

Quaternion algebras, orders, unit groups

A central simple algebra B of dimension four over $\mathbb{Q}$ is called a quaternion algebra over $\mathbb{Q}$. On B, there is an anti-automorphism of order 2 ($x \mapsto \bar{x}$) as well multiplicative and additive maps to $\mathbb{Q}$, called the reduced norm ($x \mapsto \mathbf{n}(x)$) and reduced trace ($x \mapsto \mathbf{t}(x)$), respectively. Similarly, one can consider quaternion algebras over an arbitrary field F, but we restrict our attention to the cases of $F = \mathbb{Q}$, and the completion $F = \mathbb{Q}_v$ of $\mathbb{Q}$ at a place v.

By Wedderburn's Theorem, a quaternion algebra B over field F is isomorphic to $M_2(F)$ or a division quaternion algebra. With this in mind, we say that a quaternion algebra B over $\mathbb{Q}$ is *split* or *ramified* at a place v of $\mathbb{Q}$ if B_v is isomorphic to $M_2(\mathbb{Q}_v)$ or a division algebra over $\mathbb{Q}_v$, respectively. It is a fact that B is ramified at a finite number of even places v and one defines the discriminant of B to be the product of p_v where v runs through the places where B ramifies.

Let B be a quaternion algebra over $\mathbb{Q}$. Unlike fields over $\mathbb{Q}$, the set of integral elements of B does not form ring. As a replacement, one considers $\mathbb{Z}$-modules of rank 4 which are subrings of B. Such an object is called an order of B. Any order of B is contained in a maximal order, though this may not be unique. There is a similar notion of orders in quaternion algebras over $\mathbb{Q}_v$, where v is finite place. For $v = \infty$, we set by convention $\mathbb{Z}_\infty = \mathbb{Q}_\infty$ so that orders in B_∞ are just B_∞ itself.

Lemma 1.5.1 *Let R be an order in a quaternion algebra B over $\mathbb{Q}$. The units of R are given by*

$$R^\times = \{x \in R \mid \mathbf{n}(x) \in \mathbb{Z}^\times\} \tag{1.43}$$

Proof. This follows from the fact that $x \mapsto \bar{x}$ preserves orders. □

Let $R^{\times,+}$ be the elements in $R^\times$ with positive reduced norm. By the above Lemma, $R^{\times,+}$ consists of the elements in R of reduced norm one. We call this group *the unit group of R* (not to be confused with the units of R). The unit group of R will often be denoted it by Γ_R.

Adelisation of quaternion algebras

It is useful to analyse quaternion algebras B over $\mathbb{Q}$ by considering the local quaternion algebras $B_v = B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ for each place v of $\mathbb{Q}$. Indeed, one knows that $B_v \cong M_2(\mathbb{Q}_v)$ for all but a finite number of even places v of $\mathbb{Q}$.

Given an order R in B, its localisations $R_v = R \otimes_{\mathbb{Z}} \mathbb{Z}_v$ are orders in B_v. The correspondence between orders R and collections of local orders $\{R_v\}$ is characterised by the following two Lemmas:

Lemma 1.5.2 *Let R and R' be orders in a quaternion algebra B over $\mathbb{Q}$. Then $R_v = R'_v$ for all but a finite number of places.*

Proof. Since R and R' are both $\mathbb{Z}$-modules of rank 4, $R \cap R'$ is of finite index in R and R'. For places v not dividing $[R : R \cap R']$ and $[R' : R \cap R']$, we have $R_v = R'_v$. □

Lemma 1.5.3 *Suppose B is a quaternion algebra over $\mathbb{Q}$. Let $\{R_v\}$ be a collection of local orders R_v where v runs through all places of $\mathbb{Q}$. If there exists an order R' such that $R'_v = R_v$ for all but a finite number of places v, then there exists an unique order R whose localisation at v is R_v for all places v.*

Proof. Refer to Lemma 5.2.4(3) in [Miy89]. □

Consider the example of $B = M_2(\mathbb{Q})$. It is easily checked that $M_2(\mathbb{Z})$ is an order in B. Since $M_2(\mathbb{Z})_v = M_2(\mathbb{Z}_v)$ for all places v of $\mathbb{Q}$, we see that if R is an order in B, then $R_v = M_2(\mathbb{Z}_v)$ for all but a finite number of places v. Conversely, if $\{R_v\}$ is a collection of local orders such that $R_v = M_2(\mathbb{Z}_v)$ for all but a finite number of places v, then there exists an order R whose localisation at a place v is R_v for all places v.

In general, we have:

Corollary 1.5.1 *Let B be a quaternion algebra over $\mathbb{Q}$ and let R be an order in B. Then R_v is a maximal order in B_v for all but a finite number of places v.*

Proof. Maximal orders in B exist, so the result follows from Lemma 1.5.2. □

Lemma 1.5.4 *Let B_v be a quaternion algebra over $\mathbb{Q}_v$ where v is a finite place.*

i. If B_v is split, then all maximal orders of B_v are conjugate to $M_2(\mathbb{Z}_v)$.

ii. If B_v is ramified, then there is a unique maximal order S_v of B_v.

Proof. If B_v is split, then $B_v \cong M_2(\mathbb{Q}_v)$. Any order R_v lies in $\mathrm{End}(\Lambda)$ where Λ is a lattice in $\mathbb{Q}_v^2$. Thus, by a suitable change of basis (which is uniquely determined up to conjugation by $\mathrm{GL}_2(\mathbb{Z}_v)$), we may assume $\mathrm{End}(\Lambda) = M_2(\mathbb{Z}_v)$.

If B_v is ramified, then B_v is a division algebra. The unique maximal order of B_v is given by

$$S_v = \{x \in B_v \mid \mathbf{n}(x) \in \mathbb{Z}_v\}.$$

□

The adelisation $B_{\mathbb{A}}$ of a quaternion algebra B over $\mathbb{Q}$ is an object which allows us to analyse B locally in a way which reflects the properties in listed in the Lemmas above. It is defined as the restricted topological product of the B_v's with respect to the open subrings R_v, where R is an order in B. The resulting topological ring does not depend on the choice of R (essentially because of Lemma 1.5.2). Similarly, the adelisation $B_{\mathbb{A}}^{\times}$ of $B^{\times}$ is the restricted product of $B_v^{\times}$ with respect to the subgroups $R_v^{\times}$, where again the resulting topological group does not depend on the choice of R. Note that one can embed B into $B_{\mathbb{A}}$ using the diagonal map. Also, it is sometimes useful to consider the adelisation of $B_{\mathbb{A}}$, $B_{\mathbb{A}}^{\times}$ over finite places only, denoted $B_{\mathbb{A}}^0$, $B_{\mathbb{A}}^{\times,0}$, respectively, and we will often use the decompositions, $B_{\mathbb{A}} = B_\infty \times B_{\mathbb{A}}^0$ and $B_{\mathbb{A}}^{\times} = B_\infty^{\times} \times B_{\mathbb{A}}^{\times,0}$ to distinguish between the cases of finite and infinite places.

Using adelisations, Lemmas 1.5.2 and 1.5.3 can be summarised as

Lemma 1.5.5 *Given an order R in B, the product of local orders $R_{\mathbb{A}} = B_\infty \times \prod_{v \neq \infty} R_v$ is contained in $B_{\mathbb{A}}$. Conversely, given a product of orders $R_{\mathbb{A}} = B_\infty \times \prod_{v \neq \infty} R_v$ which is contained in $B_{\mathbb{A}}$, $R = R_{\mathbb{A}} \cap B$ is an order of B.*

Arithmetic congruence groups

Definition 1.5.1 *A quaternion algebra B over $\mathbb{Q}$ is called indefinite or definite if B_∞ is isormorphic to $M_2(\mathbb{Q}_\infty)$ or a division algebra over $\mathbb{Q}_\infty$, respectively.*

Definition 1.5.2 *Let B be an indefinite quaternion algebra over $\mathbb{Q}$. Let $\Gamma_{\mathbb{A}}^0$ be an open compact subgroup of $B_{\mathbb{A}}^{\times,0}$ and let $\Gamma = B^{\times} \cap (B_\infty^{\times,+} \times \Gamma_{\mathbb{A}}^0)$. We call Γ an arithmetic congruence group.*

Remark 1.5.1 *We note that it is possible for an arithmetic congruence group Γ to arise from different open compact subgroups of $B_{\mathbb{A}}^{\times,0}$. However, it will usually be clear from the context which open compact subgroup we are taking, so we will suppress this dependence.*

Lemma 1.5.6 *Let B be an indefinite quaternion algebra over $\mathbb{Q}$ and suppose Γ is an arithmetic congruence group in $B^{\times}$. Then there exist orders $R \subset S$ in B satisfying*

$$\Gamma_R \subset \Gamma \subset \Gamma_S.$$

Proof. (For the proof, we will use the Lemmas below describing the open compact subgroups of $B_{\mathbb{A}}^{\times,0}$.)

Since Γ is an arithmetic congruence group, $\Gamma = B^{\times} \cap (B_\infty^{\times,+} \times \Gamma_{\mathbb{A}}^0)$ for some open compact subgroup of $B_{\mathbb{A}}^{\times,0}$. By Lemma 1.5.9, there exists a finite set of finite places P such that $\Gamma_v = R_v'$ for $v \notin P$ and Γ_v is an compact open subgroup of $B_v^{\times}$ for $v \in P$, where R_v' denotes the localisation at v of an order R'. Since Γ_v is an compact open subgroup of $B_v^{\times}$ for $v \in P$, by Lemma 1.5.7 and 1.5.8, there exist orders R_v'' and S_v'' such that $R_v''^{\times} \subset \Gamma_v \subset S_v''^{\times}$. Let S

be the order such that $S_v = R'_v$ for $v \notin P$ and $S_v = S''_v$ for $v \in P$. Let R be the order such that $R_v = R'_v$ for $v \notin P$ and $R_v = R''_v$ for $v \in P$. Then $\Gamma_R \subset \Gamma = B^\times \cap (B_\infty^{\times,+} \times \Gamma_{\mathbb{A}}^0) \subset \Gamma_S$ so that Γ is an arithmetic congruence group. □

Lemma 1.5.7 *Suppose v is a finite place of $\mathbb{Q}$. Then Γ_v is a compact subgroup of $B_v^\times$ if and only if*

i. (B_v split) Γ_v can be conjugated to lie in $GL_2(\mathbb{Z}_v)$ as a closed subgroup.

ii. (B_v ramified) Γ_v lies in $S_v^\times$ as a closed subgroup, where S_v is the unique maximal order of B_v.

Proof. Suppose B_v is split. Let Λ be a lattice in $\mathbb{Q}_v^2$. By compactness and the fact that $\mathrm{Aut}(\Lambda)$ is an open subgroup of $B_v^\times$, we see that Γ_v and $\mathrm{Aut}(\Lambda)$ are commensurable. Thus, we can form a Γ_v-invariant lattice Λ' so that Γ_v is contained in $\mathrm{Aut}(\Lambda')$, which is conjugate to $\mathrm{GL}_2(\mathbb{Z}_v)$.

Suppose B_v is ramified. We note that $\det(\Gamma_v) \subset \mathbb{Z}_p^\times$ since Γ_v is compact and $\det : B_v^\times \to \mathbb{Q}_v^\times$ is continuous. By the description of the maximal order S_v in B_v given in the proof of Lemma 1.5.4, we see that $\Gamma_v \subset S_v$. Therefore, $\Gamma_v \subset S_v^\times$.

For the converse, we note that $\mathrm{GL}_2(\mathbb{Z}_v)$ and $S_v^\times$ are compact subgroups of $B_v^\times$ in each respective case. □

Lemma 1.5.8 *Suppose that v is a finite place of $\mathbb{Q}$. Then Γ_v is an open subgroup of $B_v^\times$ if and only if Γ_v contains $R_v^\times$ for some order R_v in B_v*

Proof. We simply note that a basis for the topology on $B_v^\times$ is given by $\{x \cdot R_v^\times \mid x \in B_v^\times\}$ where R_v is *any* order in B_v. □

Lemma 1.5.9 *$\Gamma_{\mathbb{A}}^0$ is an open compact subgroup of $B_{\mathbb{A}}^{\times,0}$ if and only if*

$$\Gamma_{\mathbb{A}}^0 = \prod_{v \in P} \Gamma_v \times \prod_{v \notin P} R_v^\times \tag{1.44}$$

where P is a finite set of finite places, R_v denotes the localisation at v of an order R, and Γ_v is a open compact subgroup of $B_v^\times$.

Proof. A basis for the topology on $B_{\mathbb{A}}^{\times,0}$ is given by

$$U(P) = \prod_{v \in P} U_v^\times \times \prod_{v \notin P} R_v^\times \tag{1.45}$$

where P runs through finite sets of finite places, $U_v^\times$ is an open subgroup of $B_v^\times$, and R_v denotes the localisation at v of an order R.

Since $\Gamma_{\mathbb{A}}^0$ is an open set, it is a union of basis sets $U(P)$ as above. By compactness, it is in fact a finite union of such sets. The result then follows by noting that Γ_v is a compact open subgroup of $B_v^\times$ for all finite places v. □

If B is an indefinite quaternion algebra over $\mathbb{Q}$ then $\phi : B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$ for some isomorphism ϕ. Under the isomorphism ϕ, B can be viewed as a subalgebra of $M_2(\mathbb{R})$. In this way an arithmetic congruence group Γ of $B^\times$ can be identified with a Fuchsian group of the first kind: The group Γ is by Lemma 1.5.6 a subgroup of a unit group of finite index. Since unit groups of orders in *indefinite* quaternion algebras are well-known to be Fuchsian groups of the first kind (see Theorem 5.2.13 in [Miy89]), it follows that Γ is a Fuchsian group of the first kind.

Definition 1.5.3 *Let Γ be an arithmetic congruence group. Let P be the set of finite places v such that $\Gamma_v \neq S_v^\times$ where S_v is a maximal order in B_v. By Lemma 1.5.9 and Lemma 1.5.1, P is a finite set. We define the level of Γ to be $N = \prod_{v \in P} v$.*

Lemma 1.5.10 *Let Γ be an arithmetic congruence group of level N. Then there exist orders $R \subset S$ such that $\Gamma_R \subset \Gamma \subset \Gamma_S$ and $R_v = S_v$ is maximal in B_v if and only if $v \mid N$.*

Proof. Let $R \subset S$ be a choice of orders such that $\Gamma_R \subset \Gamma \subset \Gamma_S$. By Lemma 1.5.2 and 1.5.1, there exists a finite set of finite places P such that for $v \notin P$, $R_v = S_v$ is maximal in B_v. If $v \in P$ is such that $\Gamma_v = {S'_v}^\times$, where S'_v is a maximal order in B_v, then we modify R and S so that $R_v = S_v = S'_v$. The resulting R and S has the desired property. □

For later reference, we quote the important

Theorem 1.5.1 *(Strong approximation) Let B be an indefinite quaternion algebra over $\mathbb{Q}$ and let $\Gamma_{\mathbb{A}}^0$ be an open compact subgroup of $B_{\mathbb{A}}^{\times,0}$ such that $\mathbf{n}(\Gamma_v) = \mathbb{Z}_v^\times$ for all finite places v. Then*

$$B_{\mathbb{A}}^\times = B^\times \cdot (B_\infty^{\times,+} \times \prod_{v \neq \infty} \Gamma_v). \tag{1.46}$$

Proof. The proof of Theorem 5.2.11 in [Miy89] for $\Gamma_{\mathbb{A}}^0 = R_{\mathbb{A}}^{\times,0}$ also works for a general compact open subgroup. □

Definition 1.5.4 *A strong arithmetic congruence group Γ is an arithmetic congruence group such that $\mathbf{n}(\Gamma_v) = \mathbb{Z}_v^\times$ for all finite places v.*

Some examples

Let us give some examples of (strong) arithmetic congruence groups:

i. Let B be an indefinite quaternion algebra and suppose R is an order in B. Then $\Gamma_{\mathbb{A}}^0 = \prod_{v \neq \infty} R_v^\times$ is an open compact subgroup of $B_{\mathbb{A}}^{\times,0}$ so that $\Gamma = B^\times \cap B_\infty^{\times,+} \times \Gamma_{\mathbb{A}}^0$ is an arithmetic congruence group of $B^\times$. In fact, by Lemma 1.5.1, Γ is the unit group Γ_R of R.

ii. Let $B = M_2(\mathbb{Q})$. Consider the following subset of $M_2(\mathbb{Z})$:

$$R_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod{p} \right\}.$$

It is easily checked that $R = R_0(p)$ is an order in B. The unit group $\Gamma = \Gamma_R$ is an arithmetic congruence group of level p.

iii. Let $B = M_2(\mathbb{Q})$ and set $R = R(1) = M_2(\mathbb{Z})$. The unit group $\Gamma = \Gamma_R$ is an arithmetic congruence group of level 1.

iv. Let $B = M_2(\mathbb{Q})$ and consider the following subset of $M_2(\mathbb{Z})$:

$$R_{\text{non-split},\lambda}(p) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid a \equiv d \pmod{p}, c \equiv \lambda b \equiv 0 \pmod{p} \}$$

where $\left(\frac{\lambda}{p}\right) = -1$. The set $R_{\text{non-split},\lambda}(p)$ is an order in B: It is clear $R_{\text{non-split},\lambda}(p)$ is a subring of B so the only point to check is that it is a $\mathbb{Z}$-module of rank 4. For this, we note that

$$R_{\text{non-split},\lambda}(p) = \mathbb{Z} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 & 1 \\ \overline{\lambda} & 0 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 & p \\ 0 & 0 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 & 0 \\ 0 & p \end{pmatrix}$$

where $\overline{\lambda}$ is any element of $\mathbb{Z}$ such that $\overline{\lambda} \equiv \lambda \pmod{p}$.

The unit group Γ_R is an arithmetic congruence group of level p and is in fact the group $\Gamma_{\text{non-split},\lambda}(p)$ given in section 1.1.

Let $\Gamma^0_{\mathbb{A}} = \prod_{v \neq \infty} R_v^\times \cup \omega R_v^\times$ where $\omega = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then $\Gamma^0_{\mathbb{A}}$ is an open compact subgroup of $B^0_{\mathbb{A}}$ so that $\Gamma = B^\times \cap B_\infty^{\times,+} \times \Gamma^0_{\mathbb{A}}$ is an arithmetic congruence group of level p which is in fact the group $\Gamma^+_{\text{non-split},\lambda}(p)$ given in section 1.1.

v. Let $B = M_2(\mathbb{Q})$ and consider the following subset of $M_2(\mathbb{Z})$:

$$R_{\text{split}}(p) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid b \equiv c \equiv 0 \pmod{p} \}$$

The set $R_{\text{split}}(p)$ is an order in B: It is clear $R_\lambda(p)$ is a subring of B so the only point to check is that it is a $\mathbb{Z}$-module of rank 4. For this, we note that

$$R_{\text{split}}(p) = \mathbb{Z} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 & p \\ 0 & 0 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 & 0 \\ p & 0 \end{pmatrix} \oplus \mathbb{Z} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

The unit group Γ_R is an arithmetic congruence group of level p and is in fact the group $\Gamma_{\text{split}}(p)$ given in section 1.1.

Let $\Gamma^0_{\mathbb{A}} = \prod_{v \neq \infty} R_v^\times \cup \omega R_v^\times$ where $\omega = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then $\Gamma^0_{\mathbb{A}}$ is an open compact subgroup of $B^0_{\mathbb{A}}$ so that $\Gamma = B^\times \cap B_\infty^{\times,+} \times \Gamma^0_{\mathbb{A}}$ is an arithmetic congruence group of level p which is in fact the group $\Gamma^+_{\text{split}}(p)$ given in section 1.1.

Hecke operators

In this section, we define Hecke operators on strong arithmetic congruence groups.

Lemma 1.5.11 *Let B be an indefinite quaternion algebra over $\mathbb{Q}$ and let Γ be an arithmetic congruence group in $B^\times$. The commensurator of Γ contains $B^\times$.*

Proof. A proof can be seen from the special case given in Lemma 3.10 of [Shi71]. □

Thus, for $\delta \in B^\times$, the double coset $\Gamma\delta\Gamma$ defines a double coset operator $\Theta_k(\Gamma\delta\Gamma)$ on $S_k(\Gamma)$.

Let B be an indefinite quaternion algebra over $\mathbb{Q}$ with discriminant D and let Γ be a strong arithmetic congruence group in $B^\times$ with level N.

Let $l \mid m$ be two positive integers such that $(lm, DN) = 1$. Write $l = \prod_{v\in Q} v^{e_v}$ and $m = \prod_{v\in Q} v^{f_v}$ where $e_v \leq f_v \neq 0$. For $v \in Q$, we see that $\Gamma_v = S_v$ where S_v is a maximal order in $B_v \cong M_2(\mathbb{Q}_v)$. By Lemma 1.5.4, $S_v = \alpha_v^{-1} M_2(\mathbb{Z}_v)\alpha_v$ for some $\alpha_v \in \mathrm{GL}_2(\mathbb{Q}_v)$, which is unique up to multiplication on the left by $\mathrm{GL}_2(\mathbb{Z}_v)$.

Define $(\delta_v)_v \in B_{\mathbb{A}}^\times$ as follows:

$$\delta_v = 1 \qquad \text{for } v \notin Q$$
$$\delta_v = \alpha_v \begin{pmatrix} v^{e_v} & 0 \\ 0 & v^{f_v} \end{pmatrix} \alpha_v^{-1} \qquad \text{for } v \in Q.$$

By Theorem 1.5.1, there exists an element $\delta \in B^\times$ such that $(\delta_v)_v = (\delta)_v \cdot \gamma$ where $\gamma \in B_\infty^{\times,+}$. Define $T_{l,m}$ to be the double coset $\Gamma\delta\Gamma$. This double coset is well-defined and does not depend on the choice of α_v nor δ. Furthermore, for n a positive integer such that $(n, DN) = 1$, we define the n-th Hecke operator to be the formal sum $T_n = \sum_{l|m>0, lm=n} T_{l,m}$.

Let R, S be orders such that $\Gamma_R \subset \Gamma \subset \Gamma_S$ and $R_v = S_v$ is maximal in B_v if and only if $v \nmid N$ (see Lemma 1.5.10). We note that the δ given by strong approximation above is such that $\delta \in \cup_{\omega\in\Omega} \omega R$, where $\Gamma = \cup_{\omega\in\Omega} \omega\Gamma_R$.

Remark 1.5.2 *Since δ can be taken to lie in R, we see that $T_{l,m} = \Gamma\delta\Gamma$ is contained in S_n, the elements in S with reduced norm $n = lm$. Similarly, T_n is contained in S_n.*

The following two Lemmas are easily deduced from their classical counterparts.

Lemma 1.5.12 *For m, n, p prime to DN, the Hecke operators satisfy the following relations:*

$$T_{mn} = T_m T_n \text{ for } (m,n) = 1$$
$$T_p T_{p^e} = T_{p^{e+1}} + pT_{p,p}T_{p^{e-1}}$$

Proof. c.f. Lemma 4.5.7. in [Miy89]. □

Lemma 1.5.13 *For $n = \prod_{p|n} p^{e_p}$ prime to DN,*

$$deg(T_n) = \prod_{p|n} \frac{1 - p^{e_p+1}}{1 - p}.$$

Proof. One uses the relations given above and an inductive argument. □

We call the subalgebra $\mathbb{T}(\Gamma) = \mathbb{Z}[T_n \mid (n, N) = 1] \subset \mathcal{T}(\Gamma)$ a *Hecke algebra.* It has a representation Θ_k into $\mathrm{End}(S_k(\Gamma))$.

Chapter 2

The Trace formula for Hecke operators

The Selberg trace formula is a general formula from analysis which gives, under suitable hypotheses, the trace of an linear operator acting on a Hilbert space.

Let Γ be a Fuchsian group of the first kind. For $k > 2$, the vector space of cusp forms $S_k(\Gamma)$ together with the Petersson inner product is a finite-dimensional Hilbert space (see Theorems 2.1.5 and section 6.3 of [Miy89]). There are natural linear operators $\Gamma\delta\Gamma$ which act on $S_k(\Gamma)$ (see section 1.4). The Selberg trace formula can be used to calculate the traces of these operators and in this particular context, it reads:

Theorem 2.0.2 *Let Γ be a Fuchsian group of the first kind and let $\Gamma\delta\Gamma$ be a double coset operator. Then*

$$tr(\Gamma\delta\Gamma \mid S_k(\Gamma)) = |Z(\Gamma)|^{-1} \int_{\Gamma\backslash\mathfrak{H}} \sum_{\alpha\in\Gamma\delta\Gamma} \kappa(z;\alpha) dv(z) \tag{2.1}$$

where

$$\begin{aligned} Z(\Gamma) &= \text{ center of } \Gamma \\ \kappa(z;\alpha) &= det(\alpha)^{k-1} K_k(\alpha z, z) j(\alpha, z)^{-k} \Im(z)^k \\ K_k(z_1, z_2) &= \frac{k-1}{4\pi} \left(\frac{z_1 - \bar{z}_2}{2i} \right)^{-k} \end{aligned}$$

Proof. See the proof of Theorem 6.4.2 in [Miy89]. □

For $k = 2$, there are some complications in convergence of the sum $\sum_{\alpha\in\Gamma\delta\Gamma} \kappa(z,\alpha)$ which add an extra term $\deg(\Gamma\delta\Gamma)$ to the trace formula above. Refer to [Eic57] [Eic72] for a treatment of this case and the case $k > 2$ above which uses the slightly different viewpoint of generalised abelian integrals.

The above formula for the trace of $\Gamma\delta\Gamma$ can be simplified by an integral calculation so it involves only sums. We shall content ourselves with quoting

some standard sources for this part as they are valid for quite general Fuchsian group of the first kind.

If Γ is a strong arithmetic congruence group rather than an arbitrary Fuchsian group of the first kind, then there is a distinguished class of linear operators T_n on $S_k(\Gamma)$ called Hecke operators (see section 1.5). By an algebraic calculation, the above trace formula can be put into an explicit form which is in principle calculable. We will illustrate this algebraic calculation for a certain class of strong arithmetic congruence groups. The calculation is a modification of the one done in section 6.5 in [Miy89] for unit groups of orders in quaternion algebras over $\mathbb{Q}$.

2.1 Integral calculation for Fuchsian groups of the first kind

Theorem 2.1.1 *Let Γ be a Fuchsian group of the first kind and let $\Gamma\delta\Gamma$ be a double coset operator. Suppose that $\Gamma\delta\Gamma$ satisfies the following condition:*

Condition 2.1.1
There is an element $g \in GL_2(\mathbb{R})$ with $det(g) = -1$ such that $g^{-1}\Gamma\delta\Gamma g \subset \Gamma\delta\Gamma$.

Then the Selberg trace formula for $\Gamma\delta\Gamma$ on $S_k(\Gamma)$ can be simplified to the following form:

$$tr(\Gamma\delta\Gamma \mid S_k(\Gamma)) = t^{\Sigma} + \delta(k) \tag{2.2}$$

$$t^{\Sigma} = -\lim_{s\to 0^+} \sum_{\alpha\in\Gamma\delta\Gamma//\Gamma} k(\alpha)l(\alpha) \tag{2.3}$$

$$\delta(k) = \begin{cases} deg(\Gamma\delta\Gamma) & if\ k = 2 \\ 0 & otherwise \end{cases} \tag{2.4}$$

$$k(\alpha) = \begin{cases} \frac{k-1}{4\pi} v(\Gamma\backslash\mathfrak{H}) sgn(\alpha)^k det(\alpha)^{k/2-1} & if\ \alpha \in \Gamma\delta\Gamma^o \\ \frac{\eta_\alpha^{k-1} - \zeta_\alpha^{k-1}}{\eta_\alpha - \zeta_\alpha} & if\ \alpha \in \Gamma\delta\Gamma^e \\ sgn(\zeta_\alpha)^k \frac{min(|\zeta_\alpha|,|\eta_\alpha|)^{k-1}}{|\zeta_\alpha - \eta_\alpha|} & if\ \alpha \in \Gamma\delta\Gamma^{h,c} \\ \frac{s}{4} sgn(\zeta_\alpha)^k det(\alpha)^{k/2-1} & if\ \alpha \in \Gamma\delta\Gamma^{p,c} \end{cases} \tag{2.5}$$

$$l(\alpha) = \begin{cases} 1/|Z(\Gamma)| & if\ \alpha \in \Gamma\delta\Gamma^o \\ 1/2\,|\Gamma(\alpha)| & if\ \alpha \in \Gamma\delta\Gamma^e \\ 1/|Z(\Gamma)| & if\ \alpha \in \Gamma\delta\Gamma^{h,c} \\ 1/|Z(\Gamma)|\,|m(\alpha)|^{s+1} & if\ \alpha \in \Gamma\delta\Gamma^{p,c} \end{cases} \tag{2.6}$$

where

$$\begin{aligned}
\Gamma\delta\Gamma//\Gamma &= \text{elements of } \Gamma\delta\Gamma \text{ up to conjugation by } \Gamma \\
\Gamma\delta\Gamma^{o} &= \text{scalar elements of } \Gamma\delta\Gamma \\
\Gamma\delta\Gamma^{e} &= \text{elliptic elements of } \Gamma\delta\Gamma \\
\Gamma\delta\Gamma^{h,c} &= \text{hyperbolic cuspidal elements of } \Gamma\delta\Gamma \\
\Gamma\delta\Gamma^{p,c} &= \text{parabolic cuspidal elements of } \Gamma\delta\Gamma \\
v(\Gamma\backslash\mathfrak{H}) &= \text{volume of } \Gamma\backslash\mathfrak{H} \\
\zeta_\alpha, \eta_\alpha &= \text{eigenvalues of } \alpha \text{ in any order and not necessarily distinct} \\
\operatorname{sgn}(\alpha) &= \operatorname{sgn}(\zeta_\alpha) \text{ (this is well-defined if } \alpha \text{ is not elliptic)} \\
\Gamma(\alpha) &= \text{those elements in } \Gamma \text{ which centralise } \alpha \\
m(\alpha) &= \text{a number which depends on } \alpha//\Gamma \text{ to be explained below}
\end{aligned}$$

Proof. Refer to Theorem 6.4.10 in [Miy89] for a detailed derivation in the case $k > 2$. For $k = 2$, see the statement in [Miy89] and [Hij74]. A proof can be found in [Sai71], who in turn cites [Eic57] for a derivation in the case which pertains to us. Also, [Miy89] refers to [Ish73] for an alternative proof from [Eic57] based on a certain limiting process. □

There is also a version of the above Theorem in the case that $\Gamma\delta\Gamma$ does not satisfy condition 2.1.1. See Theorem 6.4.9 in [Miy89].

We now explain in more detail the various components and terms involved in the above trace formula:

First of all, we recall the definitions of scalar, elliptic, hyperbolic, parabolic, cuspidal elements of $\mathrm{GL}_2(\mathbb{R})^+$.

Lemma 2.1.1 *Let $\mathbb{Q} \subset k \subset \mathbb{R}$ be a field. Then the $GL_2(k)$-conjugacy classes of elements in $M_2(k)$ are represented uniquely by elements of the following type.*

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \quad \text{where } \lambda \in k \qquad \textit{(scalar)}$$

$$\begin{pmatrix} 0 & 1 \\ -n & t \end{pmatrix} \quad \text{where } t^2 - 4n < 0 \quad \textit{(elliptic)}$$

$$\begin{pmatrix} 0 & 1 \\ -n & t \end{pmatrix} \quad \text{where } t^2 - 4n > 0 \quad \textit{(hyperbolic)}$$

$$\begin{pmatrix} 0 & 1 \\ -n & t \end{pmatrix} \quad \text{where } t^2 - 4n = 0 \quad \textit{(parabolic)}$$

Proof. This follows from the Frobenius normal form for $M_2(k)$. See p. 347 of [Coh82]. □

Corollary 2.1.1 *Elements $g \in GL_2(\mathbb{R})^+$ can be classified according to their*

action on $\mathfrak{H}$ as follows:

scalar	*if g fixes all points in $\mathbb{C} \cup \{\infty\}$*
elliptic	*if g has two fixed points, one in $\mathfrak{H}$ and the other in $\bar{\mathfrak{H}}$*
hyperbolic	*if g has two fixed points in $\mathbb{R} \cup \{\infty\}$*
parabolic	*if g has one fixed point in $\mathbb{R} \cup \{\infty\}$*

Proof. Let $k = \mathbb{R}$ in Lemma 2.1.1. □

Definition 2.1.1 *An element $g \in GL_2(\mathbb{R})^+$ is called cuspidal (with respect to Γ) if at least one of its fixed points is a cusp of Γ.*

For instance, if Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, then the cusps of Γ are precisely $\mathbb{Q} \cup \{\infty\}$. Thus, an element of $\mathrm{GL}_2(\mathbb{R})^+$ is cuspidal with respect to Γ if one of its fixed points lies in $\mathbb{Q} \cup \{\infty\}$. On the other hand, if Γ is the unit group of an order in an indefinite quaternion algebra over $\mathbb{Q}$ which is a division algebra, then Γ has no cusps and there are no elements of $\mathrm{GL}_2(\mathbb{R})^+$ which are cuspidal with respect to Γ.

Lemma 2.1.2

$$GL_2(\mathbb{R})^+_\infty = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad > 0 \right\}$$

$$GL_2(\mathbb{R})^{+,p}_\infty = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a \neq 0 \right\}$$

$$GL_2(\mathbb{R})^+_{\infty,0} = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid ad > 0 \right\}$$

$$GL_2(\mathbb{R})^+_i = \mathbb{R}^\times \cdot SO_2(\mathbb{R})$$

Proof. See Lemma 1.3.2 in [Miy89]. □

Lemma 2.1.3 *Suppose that α is elliptic/parabolic so that it has a unique fixed point z in $\mathfrak{H} \cup \mathbb{R} \cup \{\infty\}$. The group $\Gamma(\alpha)$ is precisely the group of elements Γ_z.*

Proof. Suppose $\gamma \in \Gamma$ centralises α. Then γ is also elliptic/parabolic and has the same fixed point z in $\mathfrak{H} \cup \mathbb{R}$.

Suppose $\gamma \in \Gamma_z$. Then both γ and α lie in the subgroup of elements in $\mathrm{GL}_2(\mathbb{R})^+_z$ which are elliptic/parabolic. This subgroup is abelian by Lemma 2.1.2 so that γ and α commute with each other and γ lies in $\Gamma(\alpha)$. □

We explain the term $m(\alpha)$ arising in the case of α parabolic. Let z be the unique fixed point of α in $\mathbb{R}$. By Lemma 2.1.3, $\Gamma(\alpha) = \Gamma_z$. Let $\sigma \in \mathrm{SL}_2(\mathbb{R})$ such that $\sigma(z) = \infty$. Then

$$\begin{aligned} \sigma\Gamma(\alpha)\sigma^{-1} &= \sigma\Gamma_z\sigma^{-1} \\ &= \Gamma_\infty \\ &= Z(\Gamma) \cdot \left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle \end{aligned}$$

for some $h > 0$ and

$$\sigma\alpha\sigma^{-1} = \begin{pmatrix} \zeta & \tau \\ 0 & \zeta \end{pmatrix}$$

for some ζ, τ. We define

$$m(\alpha) = \frac{\tau/\zeta}{h}.$$

Thus, the quantity $m(\alpha)$ measures the power of the translation $z \mapsto z+h$ which α represents. Note that the definition of $m(\alpha)$ is independent of the choice of σ since σ is determined up to multiplication on the left by matrices of the form

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \tag{2.7}$$

and the expression defining $m(\alpha)$ does not change when σ is multiplied on the left by such a matrix.

Lemma 2.1.4 *Let α and β be elements of $GL_2(\mathbb{R})^+$.*

i. If α and β are $GL_2(\mathbb{R})$-conjugate, then they are of the same type (i.e. elliptic, hyperbolic, parabolic).

ii. If α and β are $GL_2(\mathbb{R})^-$-conjugate and elliptic/parabolic, then they are not $GL_2(\mathbb{R})^+$-conjugate.

iii. If α and β are $GL_2(\mathbb{R})^-$-conjugate and hyperbolic, then they are also $GL_2(\mathbb{R})^+$-conjugate.

Proof. See Lemma 1.3.5 in [Miy89]. □

We note that $k(\alpha)$ only depends on the $\mathrm{GL}_2(\mathbb{R})$-conjugacy class of α as it is only determined by the type of α and its characteristic polynomial (see Lemma 2.1.4 above). As for $l(\alpha)$, we have the following Lemma:

Lemma 2.1.5 *Let α and β be elements of $GL_2(\mathbb{R})^+$. Suppose there exists a $\sigma \in GL_2(\mathbb{R})$ such that $\alpha = \sigma^{-1}\beta\sigma$ and $\Gamma(\alpha) = \sigma^{-1}\Gamma(\beta)\sigma$. Then $l(\alpha) = l(\beta)$.*

Proof. The only non-trivial case to check is when α is parabolic where it follows directly from the definition of the quantity $m(\alpha)$. □

In particular, if α and β are Γ-conjugate, then $l(\alpha) = l(\beta)$ so the quantity $l(\alpha)$ only depends on the Γ-conjugacy class of α as suggested by the trace formula.

We can decompose the set $\Gamma\delta\Gamma//\Gamma$ into four parts, $\Gamma\delta\Gamma^o//\Gamma$, $\Gamma\delta\Gamma^e//\Gamma$, $\Gamma\delta\Gamma^{h,c}//\Gamma$, $\Gamma\delta\Gamma^{p,c}//\Gamma$ and correspondingly we have $t^\Sigma = t^o + t^e + t^{h,c} + t^{p,c}$. The sets $\Gamma\delta\Gamma^o//\Gamma$, $\Gamma\delta\Gamma^e//\Gamma$, $\Gamma\delta\Gamma^{h,c}//\Gamma$ are finite whereas the set $\Gamma\delta\Gamma^{p,c}//\Gamma$ is infinite (see section 2.2). Thus, the limit above is really needed only for the term $t^{p,c}$ and it is in this case that the quantity $l(\alpha)$ depends on s.

We will be mainly interested in the case $k = 2$. Here, the trace formula reads:

$$\mathrm{tr}(\Gamma\delta\Gamma \mid S_2(X_\Gamma)) = t^\Sigma + \deg(\Gamma\delta\Gamma) \tag{2.8}$$

$$t^\Sigma = -\lim_{s\to 0^+} \sum_{\alpha\in\Gamma\delta\Gamma//\Gamma} k(\alpha)l(\alpha) \tag{2.9}$$

$$k(\alpha) = \begin{cases} \frac{1}{4\pi}v(\Gamma\backslash\mathfrak{H}) & \text{if } \alpha \in \Gamma\delta\Gamma^o \\ 1 & \text{if } \alpha \in \Gamma\delta\Gamma^e \\ \frac{\min(|\zeta_\alpha|,|\eta_\alpha|)}{|\zeta_\alpha-\eta_\alpha|} & \text{if } \alpha \in \Gamma\delta\Gamma^{h,c} \\ \frac{s}{4} & \text{if } \alpha \in \Gamma\delta\Gamma^{p,c} \end{cases} \tag{2.10}$$

$$l(\alpha) = \begin{cases} 1/|Z(\Gamma)| & \text{if } \alpha \in \Gamma\delta\Gamma^o \\ 1/2\,|\Gamma(\alpha)| & \text{if } \alpha \in \Gamma\delta\Gamma^e \\ 1/|Z(\Gamma)| & \text{if } \alpha \in \Gamma\delta\Gamma^{h,c} \\ 1/|Z(\Gamma)|\,|m(\alpha)|^{s+1} & \text{if } \alpha \in \Gamma\delta\Gamma^{p,c} \end{cases} \tag{2.11}$$

2.2 Algebraic calculation for arithmetic congruence groups

In this section, we consider the trace formula in Theorem 2.1.1 for Hecke operators T_n on strong arithmetic congruence groups Γ. The trace formula in Theorem 2.1.1 is stated for a double coset operator. However, the Hecke operator T_n for a strong arithmetic congruence group Γ is a sum of the double coset operators $T_{l,m}$ so by the additivity of the trace formula, we can simply replace the double coset $\Gamma\delta\Gamma$ in the trace formula by $T_n = \cup_{l|m>0,lm=n}\Gamma\delta_{l,m}\Gamma$. We will perform an algebraic calculation to make this trace formula for T_n explicitly calculable for strong arithmetic congruence groups Γ which satisfy

Condition 2.2.1
There exist orders R, S such that $\Gamma_R \subset \Gamma \subset \Gamma_S$ and $\Gamma \subset N(R) = \{\delta \in B^\times \mid \delta^{-1}R\delta = R\}$.

Some facts about orders

We first recall some facts about quadratic algebras (i.e. an algebra of dimension 2 over a field) and orders in quadratic algebras.

Lemma 2.2.1 *Let K be a quadratic algebra over $\mathbb{Q}$. Then K is isomorphic to one of the following:*

$$K = \begin{cases} \textit{an imaginary quadratic field} \\ \mathbb{Q}\times\mathbb{Q} \\ \textit{a real quadratic field} \\ \mathbb{Q}[\epsilon] \textit{ where } \epsilon^2 = 0 \end{cases}$$

Proof. If $\alpha \in K - \mathbb{Q}$, then $K = \mathbb{Q}[\alpha]$. The different types of minimal polynomials of α which can arise correspond to the different types of quadratic algebras which occur. □

Corollary 2.2.1 *Let B be an indefinite quaternion algebra over $\mathbb{Q}$ which we consider as being embedded in $M_2(\mathbb{R})$ under some fixed isomorphism $\phi : B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R})$. Let $\alpha \in B$ be a non-scalar with characteristic polynomial $X^2 - tX + n$. Set $D = t^2 - 4n$. Then $K = \mathbb{Q}[\alpha]$ is a quadratic algebra over $\mathbb{Q}$ of the following type:*

$$K = \begin{cases} \text{an imaginary quadratic field} & \text{if } \alpha \text{ is elliptic} \\ \mathbb{Q} \times \mathbb{Q} & \text{if } \alpha \text{ is hyperbolic and } D \text{ is a square in } \mathbb{Q} \\ \text{a real quadratic field} & \text{if } \alpha \text{ is hyperbolic and } D \text{ is not a square in } \mathbb{Q} \\ \mathbb{Q}[\epsilon] \text{ where } \epsilon^2 = 0 & \text{if } \alpha \text{ is parabolic} \end{cases}$$

where the terms scalar, elliptic, hyperbolic, and parabolic refer to the type of α considered as an element of $M_2(\mathbb{R})$ (see Lemma 2.1.1).

Lemma 2.2.2 *Let K be a quadratic algebra over $\mathbb{Q}$.*

i. If K is not $\mathbb{Q}[\epsilon]$, then the ring of integers of K is an order. This order contains all orders of K and is called the maximal order of K. It is given by

$$\mathfrak{r}_K = \begin{cases} \mathcal{O}_K & \text{if } \alpha \text{ is elliptic} \\ \mathbb{Z} \times \mathbb{Z} & \text{if } \alpha \text{ is rational hyperbolic} \\ \mathcal{O}_K & \text{if } \alpha \text{ is irrational hyperbolic} \end{cases}$$

ii. If $K = \mathbb{Q}[\epsilon]$, then the ring of integers is given by $\mathbb{Z} + \mathbb{Q}\epsilon$ (which is not a finitely-generated $\mathbb{Z}$-module).

Proof. The case of $K \neq \mathbb{Q}[\epsilon]$ is well-known. For $K = \mathbb{Q}[\epsilon]$, the result is easily verified. □

Lemma 2.2.3 *Let K be a quadratic algebra over $\mathbb{Q}$.*

i. If K is not $\mathbb{Q}[\epsilon]$, then every order in K is given by $\mathbb{Z} + f\mathfrak{r}_K$, where f is a positive integer.

ii. If K is $\mathbb{Q}[\epsilon]$, then every order in K is given by $\mathbb{Z} + \mathbb{Z}f\epsilon$, where f is a positive rational number.

Proof. The proof of Lemma 6.6.1 in [Miy89] works for $\mathbb{Q}$ in place of $\mathbb{Q}_p$. □

The number f is uniquely determines the order and is called the conductor of the order. If K is not $\mathbb{Q}[\epsilon]$, then for an order $\mathfrak{r}$ in K, the conductor of $\mathfrak{r}$ is equal to the index $[\mathfrak{r}_K : \mathfrak{r}]$.

Finally, we quote the following Lemma for later reference.

Lemma 2.2.4 *Let B be a quaternion algebra over $\mathbb{Q}$ and suppose $\alpha \in B - \mathbb{Q}$. The elements in B which commute with α are given by the elements in $\mathbb{Q}[\alpha]$.*

Proof. See Lemma 5.2.2(3) in [Miy89]. □

The trace formula in terms of B

We now follow the algebraic calculation given in [Miy89] with some modifications to obtain an explicit formula for the traces of Hecke for the class of strong arithmetic congruence groups which satisfy condition 2.2.1. To make explicit the assumptions used in this algebraic calculation, we list them below.

Condition 2.2.2

i. *B is an indefinite quaternion algebra over $\mathbb{Q}$ with discriminant D which we regard as being contained in $M_2(\mathbb{R})$.*

ii. *Γ is a strong arithmetic congruence group of level N' in $B^\times$.*

iii. *N is a multiple of N'*

iv. *$R \subset S$ are orders of B such that $\Gamma_R \subset \Gamma \subset \Gamma_S$ and $R_v = S_v$ is maximal in B_v if and only if $v \nmid N'$ (see Lemma 1.5.10).*

v. *M is a positive integer such that $M \cdot S \subset R$ (note: $N \mid M$)*

vi. $\Gamma \subset N(R) = \{\delta \in B^\times \mid \delta^{-1} R \delta = R\}$

vii. *n is prime to DN*

We allow N to be larger than the level of Γ so that we can write down a common trace formula in chapter 3 for $\Gamma^+_{\text{non-split}}(p)$, $\Gamma^+_{\text{split}}(p)$, $\Gamma_0(p)$, $\Gamma(1)$, even though the levels differ.

In section 2.1, a formula for the trace of $\Gamma\delta\Gamma$, and hence T_n, was given. We now wish to make this formula more explicit. Consider the term

$$t^\Sigma = \lim_{s \to 0^+} \sum_{\alpha \in T_n // \Gamma} k(\alpha) l(\alpha).$$

Since $k(\alpha)$ is invariant under conjugation by $B^\times$, we have

$$\begin{aligned} \sum_{\alpha \in T_n // \Gamma} k(\alpha) l(\alpha) &= \sum_{\alpha \in T_n // B^\times} k(\alpha) \sum_{\beta \in (T_n \cap C(\alpha)) // \Gamma} l(\beta) \\ &= \sum_{\alpha \in S_n // B^\times} k(\alpha) \sum_{\beta \in (T_n \cap C(\alpha)) // \Gamma} l(\beta) \end{aligned}$$

where

$$C(\alpha) = \{\delta \alpha \delta^{-1} \mid \delta \in B^\times\}. \tag{2.12}$$

Let S_n denote the elements in S with reduce norm n. By remark 1.5.2, $T_n \subset S_n$. We can replace T_n by S_n in the outer sum since if $\alpha \in S_n$ but is not $B^\times$-conjugate to an element in T_n, then $T_n \cap C(\alpha) = \emptyset$ anyways.

Consider

$$C(\alpha, \mathfrak{r}) = \left\{ \delta\alpha\delta^{-1} \mid \delta \in B^\times, \mathbb{Q}[\alpha] \cap \delta^{-1} R \delta = \mathfrak{r} \right\}. \tag{2.13}$$

Since $\mathbb{Q}[\alpha] \cap \delta^{-1}R\delta$ is an order in $\mathbb{Q}[\alpha]$ for any $\delta \in B^\times$, we have that $C(\alpha) = \bigcup_{\mathfrak{r}} C(\alpha, \mathfrak{r})$. Moreover, if $\beta \in C(\alpha, \mathfrak{r})$ and $\beta \in C(\alpha, \mathfrak{r}')$, then $\mathfrak{r} = \mathfrak{r}'$ so the union is disjoint. Also, $C(\alpha, \mathfrak{r})$ is closed under conjugation by Γ because of the hypothesis $\Gamma \subset N(R)$ in 2.2.2.

Lemma 2.2.5 *If $\mathfrak{r} \not\supset \mathbb{Z}[M\alpha]$, then $T_n \cap C(\alpha, \mathfrak{r}) = \emptyset$.*

Proof. Suppose that $\beta \in T_n \cap C(\alpha, \mathfrak{r}) \neq \emptyset$. Since $T_n \subset S$, we have that $\beta \in S$ so by the defining property of M, $M\beta \in R$. Thus, we have $M\beta \in \delta\mathfrak{r}\delta^{-1}$ and hence $M\alpha \in \mathfrak{r}$. Therefore, $\mathfrak{r} \supset \mathbb{Z}[M\alpha]$. □

Lemma 2.2.6 *If $\mathfrak{r} \not\supset \mathbb{Z}[\alpha]$, then $(T_n \cap R) \cap C(\alpha, \mathfrak{r}) = \emptyset$.*

Proof. Suppose that $\beta \in (T_n \cap R) \cap C(\alpha, \mathfrak{r}) \neq \emptyset$. Then $\beta \in \delta\mathfrak{r}\delta^{-1}$ and hence $\alpha \in \mathfrak{r}$. Therefore, $\mathfrak{r} \supset \mathbb{Z}[\alpha]$. □

Thus, it suffices to consider only those orders $\mathfrak{r} \supset \mathbb{Z}[M\alpha]$ in the inner sum of 2.2.1. If $l(\beta)$ only depends on $\mathfrak{r}$ and not on the particular $\beta \in T_n \cap C(\alpha, \mathfrak{r})$, then the sum can be rewritten as:

$$\sum_{\alpha \in S_n//B^\times} k(\alpha) \sum_{\beta \in (T_n \cap C(\alpha))//\Gamma} l(\beta)$$
$$= \sum_{\alpha \in S_n//B^\times} k(\alpha) \sum_{\mathfrak{r} \supset \mathbb{Z}[M\alpha]} l(\mathfrak{r}) \cdot |(T_n \cap C(\alpha, \mathfrak{r}))//\Gamma| . \tag{2.14}$$

Lemma 2.2.7 *Let Γ be an arithmetic congruence group. If β and β' are elements of $T_n \cap C(\alpha, \mathfrak{r})$, then $l(\beta) = l(\beta')$.*

Proof. The strategy is to show that there is an element σ of $B^\times$ which conjugates $\Gamma(\beta)$ to $\Gamma(\beta')$ and β to β' so we can apply Lemma 2.1.5.

Write $\Gamma = \cup_{\omega \in \Omega} \omega \Gamma_R$ where Ω is a complete set of inequivalent representatives for Γ/Γ_R. Then

$$\Gamma(\beta) = \mathbb{Q}[\beta] \cap \Gamma$$
$$= \cup_{\omega \in \Omega} \mathbb{Q}[\beta] \cap \omega\Gamma_R$$

since one knows that the elements in B which commute with β are precisely the elements in $\mathbb{Q}[\beta]$ (see Lemma 2.2.4).

Next, note that $l(\beta)$ does not depend β if α is hyperbolic so from here on we assume that α is either elliptic or parabolic. In these two cases, we see that every element in $\mathbb{Q}[\beta]$ has non-negative norm. Therefore,

$$\begin{aligned}\Gamma(\beta) &= \cup_{\omega\in\Omega}\mathbb{Q}[\beta]\cap\omega\Gamma_R \\ &= \cup_{\omega\in\Omega}\mathbb{Q}[\beta]\cap\omega R^\times\end{aligned}$$

Consider the set $\mathfrak{a} = \mathbb{Q}[\beta]\cap\omega R$ for a fixed $\omega\in\Omega$. We can assume without loss of generality that $\mathfrak{a}$ is not contained in $\delta\mathfrak{r}\delta^{-1}$. Now, as $\mathbb{Q}[\beta]\cap R = \delta\mathfrak{r}\delta^{-1}$, $\mathfrak{a}$ is a $\delta\mathfrak{r}\delta^{-1}$-module. Moreover, $\mathfrak{a}' = M\cdot\mathfrak{a}$ is an ideal of $\delta\mathfrak{r}\delta^{-1}$. Since M is invertible in $\mathbb{Q}[\beta]$, we see that $\mathfrak{a} = \frac{1}{M}\mathfrak{a}'$. Thus, $\mathfrak{a}\cap\mathbb{Q}$ is a fractional ideal of $\mathbb{Q}$ which means that it is the $\mathbb{Z}$-module generated by a rational number $\frac{m}{M}$ where $(m,M) = 1$. One knows that the denominators of this fractional ideal has denominators in M exactly because $\mathfrak{a}$ is not contained in $\delta\mathfrak{r}\delta^{-1}$ whereas $M\cdot\mathfrak{a}$ is.

Let $x\in\mathfrak{a}$. The reduced norm $\mathbf{n}(x)$ lies in fractional ideal $\mathfrak{a}\cap\mathbb{Q} = \left(\frac{m}{M}\right)$ since conjugation preserves $\mathfrak{a}$. The only way $\mathbf{n}(x)$ can be ±1 is if $m = \pm1$. This cannot happen because it would imply that ±1 lies in $R\cap\omega R$, a contradiction as this would mean that ω lies in $R^\times$, contrary to our assumption that $\mathfrak{a}\not\subset\delta\mathfrak{r}\delta^{-1}$. Since there are no elements in $\mathfrak{a}$ with unital reduced norm, it follows that $\mathbb{Q}[\beta]\cap\omega R^\times$ is empty. Therefore, $\Gamma(\beta)$ is in fact just $\delta\mathfrak{r}^\times\delta^{-1}$. Therefore, we see that given β and β', then $\sigma = \delta^{-1}\delta'$ conjugates $\Gamma(\beta)$ to $\Gamma(\beta')$ and β to β'. Therefore, by Lemma 2.1.5, $l(\beta) = l(\beta')$. □

Remark 2.2.1 *The main point of Lemma 2.2.7 is that $\mathbb{Q}[\beta]\cap\Gamma$ is no larger than $\mathbb{Q}[\beta]\cap R^\times = \delta\mathfrak{r}^\times\delta^{-1}$. However, if we consider this locally at $v\mid N$, one finds that $\mathbb{Q}_v[\beta]\cap\Gamma_v$ may be larger than $\mathbb{Q}_v[\beta]\cap R_v^\times$ (see Lemma 3.1.3).*

If $\alpha\in T_n^{p,c}//B^\times$, then there are infinitely-many orders $\mathfrak{r}$ containing $\mathbb{Z}[N\alpha]$ so the set $T_n^{p,c}//\Gamma$ is infinite. On the other hand, there are only finitely many $\alpha\in T_n^e//B^\times, T_n^{h,c}//B^\times$, and there are only finitely-many orders $\mathfrak{r}$ containing $\mathbb{Z}[M\alpha]$ in this case so that $T_n^e//\Gamma$ and $T_n^{h,c}//\Gamma$ are all finite. For more details, see section 3.7.

Since an arithmetic congruence group satisfies condition 2.1.1, we have therefore shown

Proposition 2.2.1 *Under the hypotheses and definitions of 2.2.2 and Theorem 2.1 we have*

$$\begin{aligned}tr(T_n\mid S_k(\Gamma)) &= t^\Sigma + \delta(k)\\ t^\Sigma &= \sum_{\alpha\in S_n//B^\times} k(\alpha)\sum_{\mathfrak{r}\supset\mathbb{Z}[M\alpha]} l(\mathfrak{r})\cdot|(T_n\cap C(\alpha,\mathfrak{r}))//\Gamma|\,.\end{aligned}$$

The trace formula in terms of $B_{\mathbb{A}}$

In this section, we work in the same situation outlined in 2.2.2. We now localise the calculation and express the trace formula in terms of the adelisation $B_{\mathbb{A}}$ of

B. If $\alpha \in S_n$ and $\mathfrak{r}$ is an order in $\mathbb{Q}[\alpha]$, we let

$$\mathfrak{r}_v = \mathfrak{r} \otimes_{\mathbb{Z}} \mathbb{Z}_v \tag{2.15}$$
$$\mathfrak{r}_{\mathbb{A}} = \mathfrak{r} \otimes_{\mathbb{Z}} \mathbb{Z}_{\mathbb{A}} \tag{2.16}$$
$$C_v(\alpha) = \left\{\delta\alpha\delta^{-1} \mid \delta \in B_v^{\times}\right\} \tag{2.17}$$
$$C_{\mathbb{A}}(\alpha) = \left\{\delta\alpha\delta^{-1} \mid \delta \in B_{\mathbb{A}}^{\times}\right\} \tag{2.18}$$
$$C_v(\alpha, \mathfrak{r}) = \left\{\delta\alpha\delta^{-1} \mid \delta \in B_v^{\times}, \mathbb{Q}_v[\alpha] \cap \delta^{-1} R_v \delta = \mathfrak{r}_v\right\} \tag{2.19}$$
$$C_{\mathbb{A}}(\alpha, \mathfrak{r}) = \left\{\delta\alpha\delta^{-1} \mid \delta \in B_{\mathbb{A}}^{\times}, \mathbb{Q}_{\mathbb{A}}[\alpha] \cap \delta^{-1} R_{\mathbb{A}} \delta = \mathfrak{r}_{\mathbb{A}}\right\} \tag{2.20}$$

where by convention we set $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$. We also define

$$\Gamma_{\mathbb{A}} = B_\infty^{\times,+} \times \Gamma_{\mathbb{A}}^0. \tag{2.21}$$

Lemma 2.2.8 *i. The map*

$$\theta : C(\alpha)//\Gamma \longrightarrow C_{\mathbb{A}}(\alpha)//\Gamma_{\mathbb{A}}$$

arising from the natural inclusion $\iota : C(\alpha) \to C_{\mathbb{A}}(\alpha)$ is surjective.

ii. For any $g \in C_{\mathbb{A}}(\alpha, \mathfrak{r})$, $|\theta^{-1}(g//\Gamma_{\mathbb{A}})| = h^+(\mathfrak{r})$ where

$$\begin{aligned} g//\Gamma_{\mathbb{A}} &= \textit{ the orbit of } g \textit{ under conjugation by } \Gamma_{\mathbb{A}} \\ h^+(\mathfrak{r}) &= h(\mathfrak{r})/w(\mathfrak{r}) \\ h(\mathfrak{r}) &= \left|\mathbb{Q}_{\mathbb{A}}[\alpha]^{\times}/\mathfrak{r}_{\mathbb{A}}^{\times,+} \cdot \mathbb{Q}[\alpha]\right| \\ w(\mathfrak{r}) &= \textit{ a quantity to be explained below.} \end{aligned}$$

Proof. We will use the notation $\cdot//\Gamma$ or $\cdot//\Gamma_{\mathbb{A}}$ to denote the orbit of $\cdot$ under conjugation by Γ or $\Gamma_{\mathbb{A}}$, respectively. The proof of this Lemma is based on Lemma 6.5.2 of [Miy89].

Let g be an element of $C_{\mathbb{A}}(\alpha)$. Then $g = h\alpha h^{-1}$ for some $h \in B_{\mathbb{A}}^{\times}$. Strong approximation holds for $\Gamma_{\mathbb{A}}^0$ by the hypotheses 2.2.2 on Γ so we can write $h = \gamma\delta$ where $\gamma \in \Gamma_{\mathbb{A}}$ and $\delta \in B^{\times}$. Hence $\theta(\delta\alpha\delta^{-1}//\Gamma) = g//\Gamma_{\mathbb{A}}$ so θ is indeed surjective.

Let g be an element of $C_{\mathbb{A}}(\alpha, \mathfrak{r})$. Then $g = h\alpha h^{-1}$ for some $h \in B_{\mathbb{A}}^{\times}$ where $\mathbb{Q}_{\mathbb{A}}[\alpha] \cap h^{-1} R_{\mathbb{A}} h = \mathfrak{r}_{\mathbb{A}}$. Now,

$$\begin{aligned} \xi\alpha\xi^{-1}//\Gamma_{\mathbb{A}} = g//\Gamma_{\mathbb{A}} &\iff \xi\alpha\xi^{-1} = \gamma h\alpha h^{-1}\gamma^{-1} \text{ for some } \gamma \in \Gamma_{\mathbb{A}} \\ &\iff \xi^{-1}\gamma h\alpha h^{-1}\gamma^{-1}\xi = \alpha \text{ for some } \gamma \in \Gamma_{\mathbb{A}} \\ &\iff \xi \in (\Gamma_{\mathbb{A}} h \mathbb{Q}[\alpha]^{\times}) \cap B^{\times} \end{aligned}$$

where the last equivalence uses the fact that the centraliser of α is $\mathbb{Q}_{\mathbb{A}}[\alpha]^{\times}$ (see Lemma 2.2.4). Thus, we have

$$\iota^{-1}(g//\Gamma_{\mathbb{A}}) = \{\xi\alpha\xi^{-1} \mid \xi \in (\Gamma_{\mathbb{A}} h \mathbb{Q}_{\mathbb{A}}[\alpha]^{\times}) \cap B^{\times}\}.$$

Similarly,

$$\begin{aligned} &\xi\alpha\xi^{-1}//\Gamma = \eta\alpha\eta^{-1}//\Gamma \\ \iff\ &\Gamma\xi\mathbb{Q}[\alpha]^\times = \Gamma\eta\mathbb{Q}[\alpha]^\times. \end{aligned}$$

Hence, we see that

$$\theta^{-1}(g//\Gamma_{\mathbb{A}}) = \Gamma\backslash(\Gamma_{\mathbb{A}}h\mathbb{Q}_{\mathbb{A}}[\alpha]^\times)\cap B^\times/\mathbb{Q}[\alpha]^\times.$$

Write $h = \gamma\delta$ by strong approximation, where $\gamma \in \Gamma_{\mathbb{A}}$ and $\delta \in B^\times$. Then we see that

$$\begin{aligned} \theta^{-1}(g//\Gamma_{\mathbb{A}}) &= \Gamma\backslash(\Gamma_{\mathbb{A}}\delta\mathbb{Q}_{\mathbb{A}}[\alpha]^\times)\cap B^\times/\mathbb{Q}[\alpha]^\times \\ &= \Gamma\backslash(\Gamma_{\mathbb{A}}\cdot\mathbb{Q}_{\mathbb{A}}[\delta\alpha\delta^{-1}]^\times)\cap B^\times/\mathbb{Q}[\delta\alpha\delta^{-1}]^\times. \end{aligned}$$

The last equation can be seen by writing an element $\xi \in \Gamma_{\mathbb{A}}\delta\mathbb{Q}_{\mathbb{A}}[\alpha]^\times = \Gamma_{\mathbb{A}}\mathbb{Q}_{\mathbb{A}}[\delta\alpha\delta^{-1}]^\times\delta$ as $\xi = \xi'\delta$. We then see that $\xi'(\delta\alpha\delta^{-1})\xi'^{-1}//\Gamma = \eta'(\delta\alpha\delta^{-1})\eta'^{-1}//\Gamma$ if and only if $\Gamma\xi'\mathbb{Q}_{\mathbb{A}}[\delta\alpha\delta^{-1}]^\times = \Gamma\eta'\mathbb{Q}_{\mathbb{A}}[\delta\alpha\delta^{-1}]^\times$.

Let $E = \mathbb{Q}_{\mathbb{A}}[\delta\alpha\delta^{-1}]^\times$. If $x \in E$, then by strong approximation there exists $\gamma \in \Gamma_{\mathbb{A}}$ such that $\gamma x \in (\Gamma_{\mathbb{A}}\cdot E)\cap B^\times$. On the other hand, suppose that $x_1, x_2 \in \mathbb{Q}_{\mathbb{A}}[\delta\alpha\delta^{-1}]^\times$ and $\gamma_1, \gamma_2 \in \Gamma_{\mathbb{A}}$. Then

$$\Gamma\gamma_1x_1E\cap B^\times = \Gamma\gamma_2x_2E\cap B^\times \iff x_1x_2^{-1} \in (E\cap\Gamma_{\mathbb{A}})\cdot(E\cap B^\times).$$

Hence, we see that

$$\begin{aligned} \theta^{-1}(g//\Gamma_{\mathbb{A}}) &= E/(E\cap\Gamma_{\mathbb{A}})\cdot(E\cap B^\times) \\ &= \mathbb{Q}_{\mathbb{A}}[\delta\alpha\delta^{-1}]^\times/(\mathbb{Q}_{\mathbb{A}}[\delta\alpha\delta^{-1}]\cap\Gamma_{\mathbb{A}})\cdot\mathbb{Q}[\delta\alpha\delta^{-1}]^\times \\ &= \mathbb{Q}_{\mathbb{A}}[\alpha]^\times/(\mathbb{Q}_{\mathbb{A}}[\alpha]\cap\delta^{-1}\Gamma_{\mathbb{A}}\delta)\cdot\mathbb{Q}[\alpha]^\times. \end{aligned}$$

Because $g \in C_{\mathbb{A}}(\alpha, \mathfrak{r})$, we see that $\mathbb{Q}_{\mathbb{A}}[\alpha]\cap\delta^{-1}R_{\mathbb{A}}\delta = \mathfrak{r}$ so that $\mathbb{Q}_{\mathbb{A}}[\alpha]\cap\delta^{-1}R_{\mathbb{A}}^{\times,+}\delta = \mathfrak{r}_{\mathbb{A}}^{\times,+}$. Hence, $|\theta^{-1}(g)| = h^+(\mathfrak{r}) = h(\mathfrak{r})/w(\mathfrak{r})$ where

$$w(\mathfrak{r}) = [\mathbb{Q}_{\mathbb{A}}[\alpha]\cap\delta^{-1}\Gamma_{\mathbb{A}}\delta : \mathfrak{r}_{\mathbb{A}}^{\times,+}]. \tag{2.22}$$

Remark that $w(\mathfrak{r})$ does not depend on the choice of δ above as δ is determined up to $\Gamma_{\mathbb{A}}\cap B^\times = \Gamma$ and Γ normalises $\Gamma_{\mathbb{A}}$.

At finite v not dividing N, $\Gamma_v = R_v^\times$ so that $\mathbb{Q}_v[\alpha]\cap\delta^{-1}\Gamma_v\delta = \mathfrak{r}_v^\times$. At $v = \infty$, $\mathbb{Q}_\infty[\alpha]\cap\delta^{-1}B_\infty^{\times,+}\delta = \mathfrak{r}_\infty^{\times,+}$. At v dividing N, $\mathbb{Q}_v[\alpha]\cap\delta^{-1}\Gamma_v\delta$ contains $\mathfrak{r}_v^\times$ with index at most $[\Gamma_v : R_v^\times]$. Thus,

$$w(\mathfrak{r}) = \prod_{v|N}[\mathbb{Q}_v[\alpha]\cap\delta^{-1}\Gamma_v\delta : \mathfrak{r}_v^\times] \le \prod_{v|N}[\Gamma_v : R_v^\times]. \tag{2.23}$$

□

Lemma 2.2.9 *Let S be a subset of $B^\times$ which is invariant under conjugation by Γ. Let $S_{\mathbb{A}}$ be a subset of $B_{\mathbb{A}}^\times$ invariant under conjugation by $\Gamma_{\mathbb{A}}$ and satisfying $S_{\mathbb{A}} \cap B^\times = S$. The natural map*

$$\theta : (S \cap C(\alpha))//\Gamma \longrightarrow (S_{\mathbb{A}} \cap C_{\mathbb{A}}(\alpha))//\Gamma_{\mathbb{A}}$$

is surjective and $|\theta^{-1}(g)| = h^+(\mathfrak{r})$ for any $g \in (S_{\mathbb{A}} \cap C_{\mathbb{A}}(\alpha, \mathfrak{r}))//\Gamma_{\mathbb{A}}$.

Proof. Let $g \in (S_{\mathbb{A}} \cap C_{\mathbb{A}}(\alpha)//\Gamma_{\mathbb{A}}$. By Lemma 2.2.8, there exists an $g' \in C(\alpha)$ such that $g' = \gamma^{-1} g \gamma$ where $\gamma \in \Gamma_{\mathbb{A}}$. However, any such g' lies in $S_{\mathbb{A}} \cap B^\times$ so $g' \in S \cap C(\alpha)$. Hence, θ is surjective.

Suppose in addition g lies in $(S_{\mathbb{A}} \cap C_{\mathbb{A}}(\alpha, \mathfrak{r}))//\Gamma_{\mathbb{A}}$. Any element in $C(\alpha)//\Gamma$ which maps to g under θ must in fact lie in S, so that $\theta^{-1}(g)$ has all $h^+(\mathfrak{r})$ possible elements. □

Since $S = T_n \cap C(\alpha, \mathfrak{r})$ and $S_{\mathbb{A}} = (T_n)_{\mathbb{A}} \cap C_{\mathbb{A}}(\alpha, \mathfrak{r})$ satisfy the hypotheses of Lemma 2.2.9, we see that

$$\begin{aligned} |(T_n \cap C(\alpha, \mathfrak{r}))//\Gamma| &= h^+(\mathfrak{r}) \cdot |((T_n)_{\mathbb{A}} \cap C_{\mathbb{A}}(\alpha, \mathfrak{r}))//\Gamma_{\mathbb{A}}| \\ &= h^+(\mathfrak{r}) \cdot \prod_v |((T_n)_v \cap C_v(\alpha, \mathfrak{r}))//\Gamma_v| \,. \end{aligned}$$

Therefore, the desired sum is finally simplified to

$$\sum_{\alpha \in S_n//\Gamma} k(\alpha) l(\alpha) = \sum_{\alpha \in S_n//B^\times} k(\alpha) \sum_{\mathfrak{r} \supset \mathbb{Z}[M\alpha]} l(\mathfrak{r}) h^+(\mathfrak{r}) \cdot \prod_v |((T_n)_v \cap C_v(\alpha, \mathfrak{r}))//\Gamma_v| \quad (2.24)$$

and we obtain

Proposition 2.2.2 *Under the hypotheses and definitions of 2.2.2 and Theorem 2.1, we have*

$$tr(T_n \mid S_k(\Gamma)) = t^\Sigma + \delta(k)$$

$$t^\Sigma = \sum_{\alpha \in S_n//B^\times} k(\alpha) \sum_{\mathfrak{r} \supset \mathbb{Z}[M\alpha]} l(\mathfrak{r}) h^+(\mathfrak{r}) \cdot \prod_v |((T_n)_v \cap C_v(\alpha, \mathfrak{r}))//\Gamma_v| \,.$$

Chapter 3

Calculation for Cartan modular curves

3.1 Overview

In this chapter, we calculate an explicit trace formula for Hecke operators $T = T_n$ on $\Gamma = \Gamma^+_{\text{non-split},\lambda}(p), \Gamma^+_{\text{split}}(p)$. According to the algebraic calculation given in section 2.2, an explicit determination of the trace formula for Γ in the form of 2.2.2 amounts to a calculation of

$$c_v^+(\alpha, \mathfrak{r}) = |(T_v \cap C_v(\alpha, \mathfrak{r}))//\Gamma_v|$$

for each place v.

Hijikata's results in [Hij74] give explicit representatives for this set in the case when $\Gamma = \Gamma_0(p)$. In fact, he considers $\Gamma = \Gamma_0(N)$ together with a character χ of $(\mathbb{Z}/N\mathbb{Z})^\times$. We modify his calculation to the case $\Gamma = \Gamma^+_{\text{non-split},\lambda}(p), \Gamma^+_{\text{split}}(p)$. The method is based on Miyake's [Miy89] detailed exposition of Hijikata's work.

To fix notation for the rest of the chapter, let

i. p be an odd prime

ii. $B = M_2(\mathbb{Q})$

iii. $\Gamma = \Gamma^+_{\text{non-split},\lambda}(p), \Gamma^+_{\text{split}}(p), \Gamma_0(p), \Gamma(1)$

iv. $R = R_{\text{non-split},\lambda}(p), R_{\text{split}}(p), R_0(p), R(1)$

v. $S = M_2(\mathbb{Z})$

vi. $T = T_n$ where n is prime to p

vii. $c_v(\alpha, \mathfrak{r}) = |(T_v \cap C_v(\alpha, \mathfrak{r}))//R_v^\times|$

viii. $c_v^+(\alpha, \mathfrak{r}) = |(T_v \cap C_v(\alpha, \mathfrak{r}))//\Gamma_v|$.

From the discussion in section 1.5, we see that the hypotheses of 2.2.2 are satisfied so that the form of the trace formula given in 2.2.2 is valid for Γ. In the context above, $N' = N = M = p$ for $\Gamma^+_{\text{non-split},\lambda}(p)$, $\Gamma^+_{\text{split}}(p)$, $\Gamma_0(p)$, and $N' = 1 \mid N = M = p$ for $\Gamma(1)$.

Lemma 3.1.1 *Suppose $v \neq p$. Then*

$$c_v^+(\alpha, \mathfrak{r}) = \begin{cases} v \neq \infty & 1 \\ v = \infty & \begin{cases} \alpha \text{ elliptic} & 2 \\ \alpha \text{ hyperbolic} & 1 \\ \alpha \text{ parabolic} & 2 \end{cases} \end{cases}$$

Proof. For $v \nmid p\infty$, $\Gamma_v = R_v$ is conjugate to the maximal order $M_2(\mathbb{Z}_v)$ so by Theorem 6.6.7 of [Miy89], $c_v^+(\alpha, \mathfrak{r}) = 1$. For $v = \infty$, see calculation (6.6.1) in [Miy89]. □

Thus, the distinguishing factor in the trace formula for Γ is $c_p^+(\alpha, \mathfrak{r})$ whose determination will be the goal of this chapter.

Let $T_o = T \cap R$ and $T_\omega = T \cap \omega R$ so that $T = T_o \amalg T_\omega$ (because n is prime to p).

Lemma 3.1.2 *If $T_p \cap C_p(\alpha, \mathfrak{r}) \neq \emptyset$, then exactly one of $(T_o)_p \cap C_p(\alpha, \mathfrak{r})$, $(T_\omega)_p \cap C_p(\alpha, \mathfrak{r})$ is non-empty. If the former holds, then $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$. If the latter holds, then $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$.*

Proof. Suppose that $\beta \in T_p \cap C_p(\alpha, \mathfrak{r}) \neq \emptyset$. Then $\beta = \delta\alpha\delta^{-1}$ for some $\delta \in B^\times$ where $\mathbb{Q}_p[\beta] \cap R_p = \delta\mathfrak{r}_p\delta^{-1}$. Now, $\beta \in R_p$ if and only if $\alpha \in \mathfrak{r}_p$. Hence, either $(T_o)_p \cap C_p(\alpha, \mathfrak{r})$ is non-empty and $\alpha \in \mathfrak{r}_p$, or $(T_\omega)_p \cap C_p(\alpha, \mathfrak{r})$ is non-empty and $\alpha \notin \mathfrak{r}_p$.

Suppose we are in the latter case. We always have that $p\alpha \in R_p$ so that $p\alpha \in \mathfrak{r}_p$. Since there are no orders between $\mathbb{Z}_p[\alpha]$ and $\mathbb{Z}_p[p\alpha]$, we have $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$. □

As we would like to make a comparison between the traces of $X^+_{\text{split}}(p)$ and $X^+_{\text{non-split}}(p)$, the trace formulae should at this stage at least have the same form. In order for this to be true, the quantity $h^+(\mathfrak{r})$ should be the same irrespective of whether we are in the split or non-split case.

Lemma 3.1.3 *Suppose $\Gamma = \Gamma^+_{non\text{-}split,\lambda}(p), \Gamma^+_{split}(p)$. Let $\alpha \in S_n$ and $\mathfrak{r}$ be an order in $\mathbb{Q}[\alpha]$. If $T_p \cap C_p(\alpha, \mathfrak{r}) \neq \emptyset$ then*

$$h^+(\mathfrak{r}) = \begin{cases} h(\mathfrak{r}) & \text{if } \mathfrak{r}_p \supset \mathbb{Z}_p[\alpha] \\ h(\mathfrak{r})/2 & \text{if } \mathfrak{r}_p = \mathbb{Z}_p[p\alpha]. \end{cases} \tag{3.1}$$

Proof. Let $\beta \in T_p \cap C_p(\alpha, \mathfrak{r})$ so that $\beta = \delta\alpha\delta^{-1}$ and $\mathbb{Q}_p[\alpha] \cap \delta^{-1}R_p\delta = \mathfrak{r}_p$ for some $\delta \in B^\times$. Recall the situation in Lemma 2.2.8: If we let g in the Lemma to be β, then the δ above corresponds to a choice of δ in the Lemma. Therefore, it suffices to show that $[\mathbb{Q}_p[\alpha] \cap \delta^{-1}\Gamma_p\delta : \mathbb{Q}_p[\alpha] \cap \delta^{-1}R_p^\times\delta] = 1, 2$ accordingly as $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$, $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$.

Suppose $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$. The proof of Lemma 3.1.2 shows that $\beta \in R_p$ so that $\mathbb{Q}_p[\beta] \cap \omega R_p \supset pR_p$. As $\Gamma_p = R_p^\times \amalg \omega R_p^\times$, it follows that $\mathbb{Q}_p[\beta] \cap \Gamma_p = \mathbb{Q}_p[\beta] \cap R_p^\times$ so $w(\mathfrak{r}) = 1$.

Suppose $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$. The proof of Lemma 3.1.2 shows that $\beta \in (T_\omega)_p \cap C_p(\alpha, \mathfrak{r})$. Therefore, $\beta \in \mathbb{Q}_p[\beta] \cap \Gamma_p$ but $\beta \notin \mathbb{Q}_p[\beta] \cap R_p^\times$. Hence, $w(\mathfrak{r}) = 2$. □

3.2 Standard elements in $C_p(\alpha, \mathfrak{r})$

In order to determine the size of

$$(T_p \cap C_p(\alpha, \mathfrak{r}))//\Gamma_p$$

we first define some standard elements in $C_p(\alpha, \mathfrak{r})$. It will turn out that these standard elements will be sufficient to form a complete set of representatives.

First define

$$D_p(t, n, \rho) = \{g \in (\mathbb{Z}_p + p^\rho R_p) - (\mathbb{Z}_p + p^{\rho+1}R_p) \mid t(g) = t, n(g) = n, \tag{3.2}$$
$$g \text{ and } \alpha \text{ are of the same type (i.e. scalar, elliptic, hyperbolic, parabolic)}\}. \tag{3.3}$$

Lemma 3.2.1 *Suppose that* $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$ *and* $[\mathfrak{r}_p : \mathbb{Z}_p[\alpha]] = p^\rho$. *Then*

$$g \in C_p(\alpha, \mathfrak{r}) \iff g \in D_p(t(\alpha), n(\alpha), \rho)$$

Proof. (See Lemma 6.6.3 in [Miy89].) First note that

$$\begin{aligned} &g \in C_p(\alpha, \mathfrak{r}) \\ &\quad\iff g = \delta\alpha\delta^{-1} \text{ for some } \delta \in B^\times \text{ and } \mathbb{Q}_p[g] \cap R_p = \delta\mathfrak{r}_p\delta^{-1}. \end{aligned}$$

Now,

$$\begin{aligned} \mathbb{Q}_p[g] \cap R_p = \delta\mathfrak{r}_p\delta^{-1} &\iff [\mathbb{Q}_p[g] \cap R_p : \mathbb{Z}_p[g]] = p^\rho \\ &\iff \mathbb{Z}_p[g] = \mathbb{Z}_p + p^\rho\mathbb{Q}_p[g] \cap R_p \\ &\iff g \in \mathbb{Z}_p + p^\rho R_p \text{ and } g \notin \mathbb{Z}_p + p^{\rho+1}R_p. \end{aligned}$$

As $g = \delta\alpha\delta^{-1}$ for some $\delta \in B^\times$ if and only if $t(g) = t(\alpha)$ and $n(g) = n(\alpha)$ and both g and α are of the same type, we obtain the desired result. □

Corollary 3.2.1 *Suppose that* $\mathfrak{r}_p \supset \mathbb{Z}_p[p\alpha]$ *and* $[\mathfrak{r}_p : \mathbb{Z}_p[p\alpha]] = p^\rho$. *Then*

$$g \in C_p(\alpha, \mathfrak{r}) \iff p \cdot g \in D_p(p \cdot t(\alpha), p^2 \cdot n(\alpha), \rho)$$

Proof.

$$\begin{aligned} & g \in C_p(\alpha, \mathfrak{r}) \\ & \iff p \cdot g \in C_p(p\alpha, \mathfrak{r}) \\ & \iff p \cdot g \in D_p(p \cdot t(\alpha), p^2 \cdot n(\alpha), \rho) \end{aligned}$$

where the last equivalence follows from Lemma 3.2.1 as applied to $p\alpha$. □

Hence, to determine elements in $C_p(\alpha, \mathfrak{r})$, it suffices to determine elements in $D_p(t, n, \rho)$. Let

$$g_{\xi,u} = \xi + p^\rho \begin{pmatrix} 0 & u \\ \bar{n}(\xi)/u & \bar{t}(\xi) \end{pmatrix} \tag{3.4}$$

where

$$\bar{n}(\xi) = -f(\xi)/p^{2\rho} \tag{3.5}$$
$$\bar{t}(\xi) = (t - 2\xi)/p^\rho \tag{3.6}$$

where $f(x) = x^2 - tx + n$. By construction, the element $g_{\xi,u}$ has the same norm n and trace t. Hence, provided the matrix

$$r_{\xi,u} = \begin{pmatrix} 0 & u \\ \bar{n}(\xi)/u & \bar{t}(\xi) \end{pmatrix} \tag{3.7}$$

lies in R_p but not in pR_p, the element $g_{\xi,u}$ will lie in $D_p(t, n, \rho)$. Thus, one can construct some standard elements $g_{\xi,u}$ in $C_p(\alpha, \mathfrak{r})$ by Lemma 3.2.1.

3.3 Counting Lemmas

We give some technical Lemmas which will be used in the following two sections. It may be useful to refer to them during some of the calculations to follow.

Lemma 3.3.1 *Let $f(x) = x^2 - tx + n \in \mathbb{Z}_p[x]$ and suppose $\xi \in \mathbb{Z}_p$ satisfies $f(\xi) \equiv 0 \pmod{p^\epsilon}$. Then*

$$t - 2\xi \equiv 0 \pmod{p^{\lceil \epsilon/2 \rceil}} \iff \Delta(f) \equiv 0 \pmod{p^\epsilon}. \tag{3.8}$$

Proof. This follows from the fact that $\Delta(f) \equiv (t - 2\xi)^2 \pmod{p^\epsilon}$. □

Lemma 3.3.2 *Let $f(x) = x^2 - tx + n \in \mathbb{Z}_p[x]$. Suppose that $\Delta(f) = p^\delta d$ where $p \nmid d$. The number of solutions to $f(x) \equiv 0 \pmod{p^\epsilon}$ modulo p^ν is given by*

$$r_p(\nu, \delta, \epsilon, d) = \begin{cases} \delta \geq \epsilon & p^{\nu - \lceil \epsilon/2 \rceil} \\ \delta < \epsilon & \begin{cases} \delta \text{ odd} & 0 \\ \delta \text{ even} & \left[\frac{d}{p^{\epsilon-\delta}}\right] p^{\nu-(\epsilon-\delta/2)} \end{cases} \end{cases} \tag{3.9}$$

where $\left[\frac{d}{p^e}\right]$ denotes the number of solutions to $x^2 \equiv d \pmod{p^e}$ and the expressions $p^{\nu-\lceil \epsilon/2 \rceil}$, $p^{\nu-(\epsilon-\delta/2)}$ are defined to be 1 when $\nu - (\epsilon - \delta/2) < 0$, $\nu - \lceil \epsilon/2 \rceil$.

Proof. This is a routine calculation. □

Lemma 3.3.3 *Assume p is an odd prime. Let $r(\alpha,\beta) = \left|\left\{x \in \mathbb{F}_p \mid \left(\frac{\alpha x^2-\beta}{p}\right) = 1\right\}\right|$ where $\alpha \neq 0$. Then*

$$r(\alpha,\beta) = \begin{cases} \left(\frac{\alpha}{p}\right) = 1 & \begin{cases} (p-1)/2 & \text{if } \left(\frac{\beta}{p}\right) = -1 \\ p-1 & \text{if } \left(\frac{\beta}{p}\right) = 0 \\ (p-3)/2 & \text{if } \left(\frac{\beta}{p}\right) = 1 \end{cases} \\ \left(\frac{\alpha}{p}\right) = -1 & \begin{cases} (p-1)/2 & \text{if } \left(\frac{\beta}{p}\right) = -1 \\ 0 & \text{if } \left(\frac{\beta}{p}\right) = 0 \\ (p+1)/2 & \text{if } \left(\frac{\beta}{p}\right) = 1 \end{cases} \end{cases}$$

Proof. This is a routine calculation. □

Lemma 3.3.4 *Assume p is an odd prime. Let $f_\epsilon(x) = a_\epsilon x^2 + b_\epsilon x + c_\epsilon \in \mathbb{F}_p[x]$ and suppose $\Delta(f_\epsilon) = \alpha\epsilon^2 - \beta$ where $\alpha \neq 0$. The total number of distinct roots of $f_\epsilon(x)$ as ϵ varies through $\mathbb{F}_p$ is*

$$2 \cdot r(\alpha,\beta) + \left[\frac{\alpha\beta}{p}\right]$$

where $r(\alpha,\beta)$, $\left[\frac{d}{p^e}\right]$ are as in Lemma 3.3.2, Lemma 3.3.3, respectively.

Proof. This is a routine calculation. □

3.4 The case of non-split Cartan

Assume now that $R = R_{\text{non-split},\lambda}(p)$ and $\Gamma = \Gamma^+_{\text{non-split},\lambda}(p)$. If $g_{\xi,u}$ satisfies the following conditions

$$\begin{aligned} u &= p^\delta w \\ \delta &= 0,1 \\ 0 < w &< p \\ \bar{n}(\xi) &\equiv \lambda u^2 \pmod{p^{1+\delta}} \\ \bar{t}(\xi) &\equiv 0 \pmod{p} \\ \bar{n}(\xi) &\not\equiv \lambda u^2 \pmod{p^{2+\delta}} \text{ or } \bar{t}(\xi) \not\equiv 0 \pmod{p^2} \end{aligned} \tag{3.10}$$

then the $r_{\xi,u}$ of the previous section will lie in R_p but not in pR_p so $g_{\xi,u}$ will lie in $D_p(t,n,\rho)$. The following Lemma shows that the set of elements $g_{\xi,u}$ satisfying condition 3.10 forms a complete set of representatives for $D_p(t,n,\rho)//R_p^\times$.

Lemma 3.4.1 *Let $g \in D_p(t,n,\rho)$. Then g is $R_p^\times$-conjugate to an element $g_{\xi,u}$ for some ξ, u satisfying 3.10.*

Proof. Suppose that $g \in D_p(t, n, \rho)$ and write

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Now, $g \in \mathbb{Z}_p + p^\rho R_p$ and $g \notin \mathbb{Z}_p + p^{\rho+1} R_p$ so g satisfies all of the following conditions

$$\begin{aligned} b &\equiv 0 \pmod{p^\rho} \\ c &\equiv 0 \pmod{p^\rho} \\ a - d &\equiv 0 \pmod{p^{\rho+1}} \\ (c - \lambda b)/p^\rho &\equiv 0 \pmod{p} \end{aligned}$$

and at least one of the following conditions

$$\begin{aligned} b &\not\equiv 0 \pmod{p^{\rho+1}} \\ c &\not\equiv 0 \pmod{p^{\rho+1}} \\ a - d &\not\equiv 0 \pmod{p^{\rho+2}} \\ (c - \lambda b)/p^{\rho+1} &\not\equiv 0 \pmod{p} \end{aligned}$$

First suppose that $b \not\equiv 0 \pmod{p^{\rho+2}}$. Rewrite g into the following form:

$$\begin{aligned} g &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ &= aI + \begin{pmatrix} 0 & b \\ c & d-a \end{pmatrix} \\ &= aI + p^\rho \begin{pmatrix} 0 & b' \\ c' & (d-a)/p^\rho \end{pmatrix} \end{aligned}$$

where $b' = b/p^\rho$ and $c' = c/p^\rho$. Put $b' = p^\delta b''$ so that $b'' \in \mathbb{Z}_p^\times$. Note that $0 \le \delta \le 1$. Since $b'' = u + kp^\nu = u(1 + \frac{k}{u}p^\nu)$ for some $0 < u < p$, the following matrix

$$h = \begin{pmatrix} 1 & 0 \\ 0 & (1 + \frac{k}{u}p^\nu)^{-1} \end{pmatrix}$$

lies in $R_p^\times$. Conjugating g by this matrix allows us to assume $b' = p^\delta b''$ where $0 < b'' < p$ so that b' is among the finite set of possibilities listed in condition 3.10. On the other hand,

$$\begin{aligned} f(a) &= a^2 - ta + n \\ &= a^2 - (a+d)a + (ad - bc) \\ &= -bc. \end{aligned}$$

Therefore, $\bar{n}(a)/b' = c'$ and $\bar{t}(a) = (t-2a)/p^\rho = (d-a)/p^\rho$. Hence, $h^{-1}gh = g_{a,b'}$ where a, b' satisfy 3.10.

Suppose that $c \not\equiv 0 \pmod{p^{\rho+2}}$. Conjugating g by the matrix

$$\begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix} \in R_p^\times$$

replaces the entry b by c/λ so we can revert to the previous case.

Now, assume that $b \equiv c \equiv 0 \pmod{p^{\rho+2}}$ but $a - d \not\equiv 0 \pmod{p^{\rho+2}}$. Conjugating g by the matrix

$$\begin{pmatrix} 1 & 1 \\ \lambda & 1 \end{pmatrix} \in R_p^\times$$

replaces the entry b by $\frac{1}{1-\lambda}(a-d+b-c) \not\equiv 0 \pmod{p^{\rho+2}}$ so we can again revert to the first case.

The case $b \equiv c \equiv (a-d) \equiv 0 \pmod{p^{\rho+2}}$ and $(c - \lambda b)/p^{\rho+1} \not\equiv 0 \pmod{p}$ cannot happen for the former conditions imply $(c - \lambda b)/p^{\rho+1} \equiv 0 \pmod{p}$. □

Having established that the elements $g_{\xi,u}$ form a complete set representatives for $D_p(t,n,\rho)//R_p^\times$, the next step is to determine when two $g_{\xi,u}$'s are $R_p^\times$-conjugate. The answer is given in the next three Lemmas.

Lemma 3.4.2 *The elements $g_{\xi,u}$ and $g_{\xi',u'}$ are $R_p^\times$-conjugate only if $u \equiv u' \pmod{p}$ and $(\xi' - \xi)/p^\rho \equiv 0 \pmod{p}$*

Proof. The elements $g_{\xi,u}$ and $g_{\xi',u'}$ are conjugate if and only if $r_{\xi,u}$ and $r_{\xi',u'} + (\xi' - \xi)/p^\rho I$ are conjugate. Note however that any $R_p^\times$-conjugate of $r_{\xi,u}$ is congruent to $r_{\xi,u}$ modulo p. This follows from the fact an element of R_p is fixed modulo p by conjugation by an element of $R_p^\times$. Hence, we have that $u' \equiv u \pmod{p}$ and $(\xi' - \xi)/p^\rho \equiv 0 \pmod{p}$ as required. □

Lemma 3.4.3 *If u, u' are prime to p, then $g_{\xi,u}$ and $g_{\xi',u'}$ are $R_p^\times$-conjugate if and only if $u = u'$ and $(\xi' - \xi)/p^\rho \equiv 0 \pmod{p}$.*

Proof. Necessity was proven in the Lemma 3.4.2. Suppose $u = u'$ and $(\xi' - \xi)/p^\rho \equiv 0 \pmod{p}$. Consider the matrix

$$\begin{pmatrix} 1 & 0 \\ (\xi' - \xi)/p^\rho u & 1 \end{pmatrix} \in R_p^\times.$$

A routine calculation shows this matrix conjugates $g_{\xi,u}$ to $g_{\xi',u'}$. □

Lemma 3.4.4 *The elements $g_{\xi,pw}$ and $g_{\xi',pw'}$ are $R_p^\times$-conjugate if and only if*

$$\Delta(\epsilon) = (\bar{n}(\xi')/p^2 + \lambda w'^2)^2 + 4\lambda w'^2(\epsilon^2 + \epsilon\bar{t}(\xi')/p - \bar{n}(\xi')/p^2)$$

is a square modulo p, where $\epsilon = (\xi' - \xi)/p^{\rho+1}$. If particular, if $\epsilon \equiv 0 \pmod{p}$, then $g_{\xi,pw}$ and $g_{\xi',pw'}$ are $R_p^\times$-conjugate.

Proof. Let $u = pw, u' = pw'$. We compute those $h \in B^\times$ which centralise $g_{\xi',u'}$. Remark that h centralises $g_{\xi',u'}$ if and only if it centralises the matrix

$$r_{\xi',u'} = \begin{pmatrix} 0 & u' \\ \bar{n}(\xi')/u' & \bar{t}(\xi') \end{pmatrix}.$$

Writing

$$h = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we obtain the following four equations from the condition $hr_{\xi',u'} = r_{\xi',u'}h$.

$$\begin{aligned} b\bar{n}(\xi')/u' &= cu' \\ au' + b\bar{t}(\xi') &= du' \\ d\bar{n}(\xi')/u' &= a\bar{n}(\xi')/u' + c\bar{t}(\xi') \\ cu' + d\bar{t}(\xi') &= b\bar{n}(\xi')/u' + d\bar{t}(\xi') \end{aligned}$$

A simple calculation then shows that h has the form

$$h = \begin{pmatrix} a & b \\ b\bar{n}(\xi')/u'^2 & a + b\bar{t}(\xi')/u' \end{pmatrix}.$$

The matrix

$$\begin{pmatrix} 1 & 0 \\ (\xi' - \xi)/p^\rho u & 1 \end{pmatrix}$$

conjugates $g_{\xi,u}$ to $g_{\xi',u}$, and the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & u'/u \end{pmatrix}$$

conjugates $g_{\xi',u}$ to $g_{\xi',u'}$. Thus, the general element in $B^\times$ which conjugates $g_{\xi,u}$ to $g_{\xi',u'}$ has the form

$$c(a,b) = \begin{pmatrix} 1 & 0 \\ (\xi' - \xi)u'/p^\rho u & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & u'/u \end{pmatrix} \begin{pmatrix} a & b \\ b\bar{n}(\xi')/u'^2 & a + b\bar{t}(\xi')/u' \end{pmatrix} = \begin{pmatrix} a & b \\ a(\xi' - \xi)/p^\rho u + b\bar{n}(\xi')/uu' & au'/u + b(\xi' - \xi)/p^\rho u + b\bar{t}(\xi')/u \end{pmatrix}.$$

The elements $g_{\xi,u}$ and $g_{\xi',u'}$ are $R_p^\times$-conjugate if and only if there exist a, b such that the matrix $c(a,b)$ lies in $R_p^\times$. The matrix $c(a,b)$ lies in $R_p^\times$ if and only if $a, b \in \mathbb{Z}_p$ and the following system of two equations holds:

$$a(u'/u - 1) + b((\xi' - \xi)/p^\rho u + \bar{t}(\xi')/u) \equiv 0 \pmod{p} \tag{3.11}$$

$$a(\xi' - \xi)/p^\rho u + b(\bar{n}(\xi')/uu' - \lambda) \equiv 0 \pmod{p} \tag{3.12}$$

There exists a non-trivial solution to this system if and only if the determinant of the above linear system is zero. This determinant is easily calculated as:

$$\Xi = w'^{-1}w^{-2} \cdot \{(w'-w)(\bar{n}(\xi')/p^2 - \lambda w w') - \epsilon(\epsilon + \bar{t}(\xi')/p)w'\} \tag{3.13}$$

where $\epsilon = (\xi' - \xi)/p^{\rho+1}$. The equation $\Xi \equiv 0 \pmod{p}$ is a quadratic equation in the variable w with discriminant

$$\Delta(\epsilon) = (\bar{n}(\xi')/p^2 + \lambda w'^2)^2 + 4\lambda w'^2(\epsilon^2 + \epsilon\bar{t}(\xi')/p - \bar{n}(\xi')/p^2) \tag{3.14}$$

Thus, $g_{\xi,u}$ and $g_{\xi',u'}$ are $R_p^\times$-conjugate if and only if Δ is a square modulo p. □

We are now ready to compute the quantities $c_p(\alpha,\mathfrak{r})[X^+_{\text{non-split},\lambda}(p)]$ and $c_p^+(\alpha,\mathfrak{r})[X^+_{\text{non-split},\lambda}(p)]$.

Proposition 3.4.1 *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$. Put $[\mathfrak{r}_p : \mathbb{Z}_p[\alpha]] = p^\rho$, $D = \Delta(\alpha)$, $d = D/p^{2\rho}$, $\mu = ord_p(d)$. Then*

$$c_p(\alpha,\mathfrak{r})[X^+_{non\text{-}split,\lambda}(p)] = \begin{cases} \mu < 2 & \begin{cases} 2 & if\ \left(\frac{d}{p}\right) = -1 \\ 0 & if\ \left(\frac{d}{p}\right) = 0 \\ 0 & if\ \left(\frac{d}{p}\right) = 1 \end{cases} \\ \mu \geq 2 & \begin{cases} p-2 & if\ \left(\frac{d/p^2}{p}\right) = -1 \\ p-1 & if\ \left(\frac{d/p^2}{p}\right) = 0 \\ p & if\ \left(\frac{d/p^2}{p}\right) = 1. \end{cases} \end{cases}$$

Proof. In this case, we have $T_p \cap C_p(\alpha,\mathfrak{r}) = (T_o)_p \cap C_p(\alpha,\mathfrak{r}) = C_p(\alpha,\mathfrak{r})$ by Lemma 3.1.2. Hence, we will determine the size of $C_p(\alpha,\mathfrak{r})//R_p^\times$. By Lemma 3.4.1 and Lemma 3.2.1, the elements $g_{\xi,u}$ satisfying condition 3.10 give a complete set of representatives for $C_p(\alpha,\mathfrak{r})//R_p^\times$.

Recall condition 3.10 and note the following two equivalences:

$$\bar{n}(\xi)/u \equiv \lambda u \pmod{p} \tag{3.15}$$

$$\iff f(\xi) = \xi^2 - t\xi + (n + p^{2\rho}\lambda u^2) \equiv 0 \pmod{p^{2\rho+1+\delta}} \tag{3.16}$$

$$\bar{t}(\xi) \equiv 0 \pmod{p} \iff t - 2\xi \equiv 0 \pmod{p^{\rho+1}} \tag{3.17}$$

where $\delta = v_p(u) = 0, 1$. If ξ, u satisfy these conditions, then by Lemma 3.3.1, $D \equiv p^{2\rho}\lambda u^2 \pmod{p^{2\rho+1+\delta}}$ and hence $d \equiv \lambda u^2 \pmod{p^{1+\delta}}$.

Assume that $\mu < 2$. If there exist ξ, u satisfying condition 3.10 with $v_p(u) = 1$, then $D \equiv 0 \pmod{p^{2\rho+2}}$ and hence $d \equiv 0 \pmod{p^2}$. Since $\mu < 2$, we deduce there are no elements $g_{\xi,u}$ with $v_p(u) = 1$ in this case. If $\left(\frac{d}{p}\right) = -1$, then there are two u's prime to p such that $d \equiv \lambda u^2 \pmod{p}$. Moreover, since the discriminant of the polynomial $f(x)$ in condition 3.15 is equal to $D - p^{2\rho}\lambda u^2 \equiv 0 \pmod{p^{2\rho+1}}$, there is precisely one root $\xi \in \mathbb{Z}_p$ modulo $p^{\rho+1}$ of $f(x)$ for each u by Lemma 3.3.2. Hence, by Lemma 3.4.3, $c_p(\alpha,\mathfrak{r}_p) = 2$. If $\left(\frac{d}{p}\right) = 0, 1$, then

$c_p(\alpha, \mathfrak{r}_p) = 0$ as there are no u's prime to p such that $d \equiv \lambda u^2 \pmod{p}$ in these two cases.

Suppose $\mu \geq 2$. If there exist ξ, u satisfying condition 3.10 with $v_p(u) = 0$, then $D \equiv p^{2\rho}\lambda u^2 \pmod{p^{2\rho+1}}$ and hence $d \equiv \lambda u^2 \pmod{p}$. This implies that d is prime to p, a contradiction. Hence, there are no $g_{\xi,u}$'s with u prime to p in this case and we can assume that $u = pw$ where w is prime to p. Note when $v_p(u) = 1$, the conditions 3.15 and 3.17 on ξ are independent of w. There are p values of ξ modulo $p^{\rho+2}$ satisfying these two conditions for each w by Lemma 3.3.2. Hence, a priori there are $p(p-1)$ distinct $g_{\xi,pw}$'s by Lemma 3.4.4. However, some of these $g_{\xi,u}$'s are $R_p^\times$-conjugate and some of them may lie in $\mathbb{Z}_p + p^{\rho+1}R_p$ (refer to condition 3.10).

Let us first fix a $g_{\xi',pw'}$ satisfying all the conditions of 3.10. We shall count the number of distinct elements $g_{\xi,pw}$ in the orbit of $g_{\xi',pw'}$ under conjugation by $R_p^\times$. According to Lemma 3.4.4, $g_{\xi,pw}$ is R_p-conjugate to $g_{\xi',pw'}$ if and only if $\Delta(\epsilon)$ is a square modulo p where $\epsilon = (\xi' - \xi)/p^{\rho+1}$. Note that $\Delta(\epsilon)$ has the form $\alpha\epsilon^2 - \beta$ where

$$\begin{aligned}
\alpha &= 4\lambda w'^2 \\
\beta &= 16\lambda w'^2(\lambda w'^2 \bar{t}(\xi')^2/p^2 - (\bar{n}(\xi')/p^2 - \lambda w'^2)^2) \\
\epsilon' &= \epsilon + \bar{t}(\xi')/p.
\end{aligned}$$

Observe that $\beta \not\equiv 0 \pmod{p}$ unless $\bar{t}(\xi')/p \equiv 0 \pmod{p}$ and $\bar{n}(\xi')/p^2 \equiv \lambda w'^2 \pmod{p}$. This cannot happen as $g_{\xi',pw'}$ was assumed to satisfy the conditions of 3.10.

As ϵ varies through $\mathbb{F}_p$, the total number of roots to $\Xi \equiv 0 \pmod{p}$ is $p+1$ by Lemma 3.3.4. We must be careful however to eliminate any pairs (ξ, w) with $w = 0$ since these are excluded by condition 3.10. Looking back on the conjugation relation 3.13, we see this will occur if and only if

$$\epsilon^2 + \epsilon\bar{t}(\xi')/p - \bar{n}(\xi')/p^2 \equiv 0 \pmod{p}.$$

This equation has a solution if and only if

$$(\bar{t}(\xi')^2 + 4\bar{n}(\xi'))/p^2 = (t^2 - 4n)/p^{2\rho+2} = D/p^{2\rho+2} = d/p^2$$

is a square modulo p. When $\left(\frac{d/p^2}{p}\right) = -1, 0, 1$, the number of (ξ, w) with $w = 0$ is therefore 0,1,2, respectively, and hence the orbit size is $p+1$,p,$p-1$, respectively.

We now consider the question of determining those $g_{\xi,pw}$ which lie in $\mathbb{Z}_p + p^{\rho+1}R_p$ (and hence do not satisfy all the conditions of 3.10). This amounts to counting the number of $g_{\xi,u}$ with u prime to p and $[\mathfrak{r}_p : \mathbb{Z}_p[\alpha]] = p^{\rho+1}$. Recalling the calculation done for the case $\mu < 2$, we see there are 2 or 0 such $g_{\xi,pw}$'s depending on whether $\left(\frac{D/p^{2\rho+2}}{p}\right) = \left(\frac{d/p^2}{p}\right) = -1$, or 0,1.

We now have enough information to compute $c_p(\alpha, \mathfrak{r})$. If $\left(\frac{d/p^2}{p}\right) = -1$, then there are $p(p-1) - 2 = p^2 - p - 2$ $g_{\xi,pw}$'s satisfying condition 3.10. The orbit under conjugation by $R_p^\times$ of any particular element has size $p+1$. Hence, there

are $p-2$ conjugacy classes of elements. If $\left(\frac{d/p^2}{p}\right) = 0$ or 1, then there $p(p-1)$ $g_{\xi,pw}$'s satisfying condition 3.10. If the former case occurs, then the orbit size is p and hence there are $p-1$ conjugacy classes. If the latter case occurs, then the orbit size is $p-1$, and there are p conjugacy classes. □

Proposition 3.4.2 *With the same hypotheses as in Lemma 3.4.1, we have*

$$c_p^+(\alpha,\mathfrak{r})[X^+_{non\text{-}split,\lambda}(p)] = \begin{cases} \mu < 2 & \begin{cases} 1 & if \left(\frac{d}{p}\right) = -1 \\ 0 & if \left(\frac{d}{p}\right) = 0 \\ 0 & if \left(\frac{d}{p}\right) = 1 \end{cases} \\ \mu \geq 2 & \begin{cases} \frac{p-1}{2} & if \left(\frac{d/p^2}{p}\right) = -1 \\ \frac{p-1}{2} & if \left(\frac{d/p^2}{p}\right) = 0 \\ \frac{p+1}{2} & if \left(\frac{d/p^2}{p}\right) = 1. \end{cases} \end{cases}$$

Proof. The involution ω acts on $(T_p \cap C_p(\alpha,\mathfrak{r}))//R_p^\times$. To determine the size of $(T_p \cap C_p(\alpha,\mathfrak{r}))//\Gamma_p$ it suffices to count the fixed points of this action. In the case $\mu < 2$, the involution ω does not fix any $g_{\xi,u}$'s, so $c_p^+(\alpha,\mathfrak{r}) = c_p(\alpha,\mathfrak{r})/2$.

Suppose $\mu \geq 2$. As in the previous Lemma, the standard representatives $g_{\xi,u}$ for $C_p(\alpha,\mathfrak{r})//R_p^\times$ in this case satisfy $u = pw$ where $w = 1,\ldots,p-1$. From the proof of 3.4.4, we see that $g_{\xi,pw}$ and $\omega g_{\xi,pw}\omega^{-1}$ are $R_p^\times$-conjugate if and only if $\Xi \equiv 0 \pmod p$. This is equivalent to

$$\bar{n}(\xi')/p^2 + \lambda w'^2 \equiv 0 \pmod p. \tag{3.18}$$

For each fixed w', the condition 3.18 is a quadratic equation in ξ'. As w' varies through $\mathbb{F}_p$, we see by Lemma 3.3.4 that the total number of roots to this quadratic equation is $p+1$ if $\left(\frac{d/p^2}{p}\right) = \pm 1$, and 0 otherwise. Now, $w' = 0$ causes 3.18 to be soluble if and only if $\left(\frac{d/p^2}{p}\right) = 1$. Therefore, as w' varies through $\mathbb{F}_p^\times$, the total number of roots to this quadratic equation is $p+1,0,p-1$, accordingly as $\left(\frac{d/p^2}{p}\right) = -1,0,1$.

We note that any two $g_{\xi,pw}$ satisfying 3.18 are $R_p^\times$-conjugate. Hence, there is one fixed point if $\left(\frac{d/p^2}{p}\right) = \pm 1$ and none otherwise. Thus, for $\left(\frac{d/p^2}{p}\right) = -1$, $c_p^+(\alpha,\mathfrak{r}) = \frac{p-2-1}{2} + 1 = \frac{p-1}{2}$. For $\left(\frac{d/p^2}{p}\right) = 0$, $c_p^+(\alpha,\mathfrak{r}) = \frac{p-1}{2}$. For $\left(\frac{d/p^2}{p}\right) = 1$, $c_p^+(\alpha,\mathfrak{r}) = \frac{p-1}{2} + 1 = \frac{p+1}{2}$. □

From Lemma 3.2.1, a determination of $T_p \cap C_p(\alpha,\mathfrak{r})//R_p^\times$ in the case of $\mathfrak{r} = \mathbb{Z}_p[p\alpha]$ therefore reduces to a determination of those elements $g_{\xi,u} \in D_p(p \cdot t(\alpha), p^2 \cdot n(\alpha), 0)$ which satisfy $g_{\xi,u}/p \in (T_\omega)_p$, up to $R_p^\times$-conjugacy.

Proposition 3.4.3 *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$. Put $d = \Delta(\alpha)$. Then*

$$c_p^+(\alpha,\mathfrak{r})[X^+_{non\text{-}split,\lambda}(p)] = c_p(\alpha,\mathfrak{r})[X^+_{non\text{-}split,\lambda}(p)] = \begin{cases} t \not\equiv 0 \pmod p & 0 \\ t \equiv 0 \pmod p & \begin{cases} 1 & \text{if } \left(\frac{d}{p}\right) = -1 \\ 0 & \text{if } \left(\frac{d}{p}\right) = 0 \\ 1 & \text{if } \left(\frac{d}{p}\right) = 1. \end{cases} \end{cases}$$

Proof. In this case, $T_p \cap C_p(\alpha,\mathfrak{r}) = (T_\omega)_p \cap C_p(\alpha,\mathfrak{r})$ by Lemma 3.1.2. By Lemma 3.2.1, $g \in C_p(\alpha,\mathfrak{r})$ if and only if $p \cdot g \in D_p(p \cdot t(\alpha), p^2 \cdot n(\alpha), 0)$.

Suppose $g_{\xi,u} \in D_p(p \cdot t(\alpha), p^2 \cdot n(\alpha), 0)$. By the argument given in the beginning of Lemma 3.4.1, it follows that $d \equiv \lambda u^2 \pmod p$. As $\mu \geq 2$, u cannot be prime to p and hence $u = pw$ for $w = 1, \ldots, p-1$.

We now count the number of $g_{\xi,pw}$ (up to $\xi \pmod{p^{\rho+2}}$) such that $g_{\xi,pw}/p \in (T_\omega)_p$.

Note that

$$g_{\xi,pw}/p = \begin{pmatrix} \xi/p & w \\ \bar{n}(\xi)/p^2 w & \xi/p + \bar{t}(\xi)/p \end{pmatrix}$$

For $g_{\xi,pw}/p$ to lie in $(T_\omega)_p$, we must have

$$\begin{aligned} t &\equiv 0 \pmod p \\ \xi^2 - pt\xi + p^2 n - p^2\lambda w^2 &\equiv 0 \pmod{p^3} \end{aligned}$$

As w varies through $\mathbb{F}_p^\times$, the total number of roots ξ to the quadratic equation above is $p+1, 0, p-1$ accordingly as $\left(\frac{d}{p}\right) = -1, 0, 1$. Thus, there is one $g_{\xi,pw}/p \in (T_\omega)_p$ up to $R_p^\times$-conjugacy if $\left(\frac{d}{p}\right) = \pm 1$ and 0 otherwise (as the orbit size of $g_{\xi,pw}$ under conjugation by $R_p^\times$ is precisely $p+1$,0,$p-1$ accordingly as $\left(\frac{d}{p}\right) = -1, 0, 1$.

As there is at most one element in $T_p \cap C_p(\alpha,\mathfrak{r})//R_p^\times$, we see that

$$c_p^+(\alpha,\mathfrak{r}) = c_p(\alpha,\mathfrak{r}).$$

□

3.5 The case of split Cartan

Since $X_{\text{split}}(p) \cong X_0(p^2)$, one can attempt to derive an explicit trace formula for $X^+_{\text{split}}(p) \cong X_0^+(p^2)$ in terms of the known formulae for $X_0(p^2)$. However, we shall directly calculate an explicit trace formula for $X^+_{\text{split}}(p)$. This approach has the advantage of putting $X^+_{\text{split}}(p)$ on a more equal footing with $X^+_{\text{non-split}}(p)$ so that the trace formulae can be more transparently compared. In addition, since $X^+_{\text{split}}(p)$ covers $X(1)$ whereas $X_0^+(p^2)$ does not, the calculation is of a more standard nature.

Assume now that $R = R_{\text{split}}(p)$ and $\Gamma = \Gamma^{+}_{\text{split}}(p)$. If ξ satisfies the following conditions,

$$\begin{aligned} f_\alpha(\xi) &\equiv 0 \pmod{p^{2\rho+2}} \\ t - 2\xi &\equiv 0 \pmod{p^\rho}, \end{aligned} \tag{3.19}$$

then the element $g_\xi = g_{\xi,p}$ defined by

$$g_{\xi,p} = \xi + p^\rho \begin{pmatrix} 0 & p \\ \bar{n}(\xi)/p & \bar{t}(\xi) \end{pmatrix}$$

will lie in $D_p(t, n, \rho)$.

Lemma 3.5.1 *Let $g \in D_p(t, n, \rho)$. Then g is Γ_p-conjugate to an element g_ξ satisfying 3.19.*

Proof. Suppose that $g \in D_p(t, n, \rho)$ and write

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Now, $g \in \mathbb{Z}_p + p^\rho R_p$ and $g \notin \mathbb{Z}_p + p^{\rho+1} R_p$ so g satisfies all of the following conditions

$$\begin{aligned} b &\equiv 0 \pmod{p^{\rho+1}} \\ c &\equiv 0 \pmod{p^{\rho+1}} \\ a - d &\equiv 0 \pmod{p^\rho} \end{aligned}$$

and at least one of the following conditions

$$\begin{aligned} b &\not\equiv 0 \pmod{p^{\rho+2}} \\ c &\not\equiv 0 \pmod{p^{\rho+2}} \\ a - d &\not\equiv 0 \pmod{p^{\rho+1}} \end{aligned}$$

First suppose that $b \not\equiv 0 \pmod{p^{\rho+2}}$. By a modification of the argument in Lemma 3.4.1, we see that g is $R_p^\times$-conjugate to some g_ξ satisfying condition 3.19.

Suppose that $c \not\equiv 0 \pmod{p^{\rho+2}}$. Conjugating g by $\omega \in \Gamma_p$ replaces the entry b by c so we can revert to the previous case.

Now, assume that $b \equiv c \equiv 0 \pmod{p^{\rho+2}}$ but $a - d \not\equiv 0 \pmod{p^{\rho+1}}$. Conjugating g by the matrix

$$\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix} \in R_p^\times$$

replaces the entry b by $p(a-d)+b-p^2c \not\equiv 0 \pmod{p^{\rho+2}}$ so we can again revert to the first case. □

Thus, the elements g_ξ and $\omega g_\xi \omega^{-1}$ satisfying condition 3.19 form a complete set of representatives for $D_p(t,n,\rho)//R_p^\times$.

We also note that an element $g \in D_p(t,n,\rho)$ is $R_p^\times$-conjugate to an element g_ξ for some ξ satisfying 3.19 if and only if $b \not\equiv 0 \pmod{p^{\rho+2}}$ or $a-d \not\equiv 0 \pmod{p^{\rho+1}}$ as it is only in the -case when $c \not\equiv 0 \pmod{p^{\rho+2}}$ that we need to conjugate by an element of Γ_p. We therefore obtain the following two Lemmas:

Lemma 3.5.2 *Elements g_ξ and $g_{\xi'}$ are $R_p^\times$-conjugate if and only if $\xi \equiv \xi' \pmod{p^{\rho+2}}$.*

Lemma 3.5.3 *Elements g_ξ and $\omega g_{\xi'} \omega^{-1}$ are $R_p^\times$-conjugate if and only if*

$$f_\alpha(\xi') \not\equiv 0 \pmod{p^{2\rho+3}} \text{ or } t - 2\xi' \not\equiv 0 \pmod{p^{\rho+1}}$$
$$\text{and } \xi \equiv t - \xi' \pmod{p^{\rho+2}}$$

We are now ready to compute the quantitites $c_p(\alpha,\mathfrak{r})[X^+_{\text{split}}(p)]$ and $c_p^+(\alpha,\mathfrak{r})[X^+_{\text{split}}(p)]$.

Proposition 3.5.1 *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$. Put $[\mathfrak{r}_p : \mathbb{Z}_p[\alpha]] = p^\rho$, $D = \Delta(\alpha)$, $d = D/p^{2\rho}$, $\mu = ord_p(d)$. Then*

$$c_p(\alpha,\mathfrak{r})[X^+_{split}(p)] = \begin{cases} \mu < 2 & \begin{cases} 0 & \text{if } \left(\frac{d}{p}\right) = -1 \\ 0 & \text{if } \left(\frac{d}{p}\right) = 0 \\ 2 & \text{if } \left(\frac{d}{p}\right) = 1 \end{cases} \\ \mu \geq 2 & \begin{cases} p & \text{if } \left(\frac{d/p^2}{p}\right) = -1 \\ p+1 & \text{if } \left(\frac{d/p^2}{p}\right) = 0 \\ p+2 & \text{if } \left(\frac{d/p^2}{p}\right) = 1. \end{cases} \end{cases}$$

Proof. In this case, we have $T_p \cap C_p(\alpha,\mathfrak{r}) = (T_o)_p \cap C_p(\alpha,\mathfrak{r}) = C_p(\alpha,\mathfrak{r})$ by Lemma 3.1.2. Hence, we will determine the size of $C_p(\alpha,\mathfrak{r})//R_p^\times$.

If $\mu < 2$, then by Lemma 3.3.2 the number of ξ modulo $p^{\rho+2}$ satisfying condition 3.19 is 0,0,2, accordingly as $\left(\frac{d}{p}\right) = -1,0,1$. An element $\omega g_\xi \omega^{-1}$ is not $R_p^\times$-conjugate to some $g_{\xi'}$ if and only if

$$\begin{aligned} f_\alpha(\xi) &\equiv 0 \pmod{p^{2\rho+3}} \\ t - 2\xi &\equiv 0 \pmod{p^{\rho+1}} \end{aligned} \tag{3.20}$$

by Lemma 3.5.3. There are no such ξ by Lemma 3.3.2 so that $c_p(\alpha,\mathfrak{r}) = 0,0,2$ accordingly as $\left(\frac{d}{p}\right) = -1,0,1$.

Suppose $\mu \geq 2$. The number of ξ modulo $p^{\rho+2}$ satisfying condition 3.19 is p. The number of ξ modulo $p^{\rho+2}$ which satisfy 3.20 is 0,1,2, acccordingly as $\left(\frac{d/p^2}{p}\right) = -1,0,1$. Thus, $c_p(\alpha,\mathfrak{r}) = p, p+1, p+2$ accordingly as $\left(\frac{d/p^2}{p}\right) = -1,0,1$. □

Proposition 3.5.2 *With the same hypthotheses as in Lemma 3.5.1, we have*

$$c_p^+(\alpha,\mathfrak{r})[X^+_{split}(p)] = \begin{cases} \mu \le 1 & \begin{cases} 0 & \text{if } \left(\frac{d}{p}\right) = -1 \\ 0 & \text{if } \left(\frac{d}{p}\right) = 0 \\ 1 & \text{if } \left(\frac{d}{p}\right) = 1 \end{cases} \\ \mu > 1 & \begin{cases} \frac{p+1}{2} & \text{if } \left(\frac{d/p^2}{p}\right) = -1 \\ \frac{p+1}{2} & \text{if } \left(\frac{d/p^2}{p}\right) = 0 \\ \frac{p+3}{2} & \text{if } \left(\frac{d/p^2}{p}\right) = 1. \end{cases} \end{cases}$$

Proof. The involution ω acts on $(T_p \cap C_p(\alpha,\mathfrak{r}))//R_p^\times$ so to determine the size of $(T_p \cap C_p(\alpha,\mathfrak{r}))//\Gamma_p$ it suffices to count the fixed points of this action.

Now, $\omega g_\xi \omega^{-1}$ is $R_p^\times$-conjugate to g_ξ by Lemma 3.20 if and only if

$$\begin{aligned} f_\alpha(\xi) &\not\equiv 0 \pmod{p^{2\rho+3}} \\ t - 2\xi &\equiv 0 \pmod{p^{\rho+2}}. \end{aligned}$$

If $\mu < 2$, then there are no ξ's which satisfy

$$\begin{aligned} f_\alpha(\xi) &\not\equiv 0 \pmod{p^{2\rho+3}} \\ t - 2\xi &\equiv 0 \pmod{p^{\rho+2}} \end{aligned} \tag{3.21}$$

Hence, there are no fixed points in this case, and $c_p^+(\alpha,\mathfrak{r}) = c_p(\alpha,\mathfrak{r})/2$.

If $\mu = 2$, then there is one ξ modulo $p^{\rho+2}$ which satisfies 3.21. If $\mu \ge 3$, then there is one ξ modulo $p^{\rho+2}$ which satisfies

$$\begin{aligned} f_\alpha(\xi) &\equiv 0 \pmod{p^{2\rho+3}} \\ t - 2\xi &\equiv 0 \pmod{p^{\rho+2}} \end{aligned} \tag{3.22}$$

Hence, there is one fixed point if $\mu = 2$ and none otherwise. Therefore, for $\left(\frac{d/p^2}{p}\right) = -1$, $c_p^+(\alpha,\mathfrak{r}) = \frac{p-1}{2} + 2 = \frac{p+1}{2}$. For $\left(\frac{d/p^2}{p}\right) = 0$, $c_p^+(\alpha,\mathfrak{r}) = \frac{p+1}{2}$. For $\left(\frac{d/p^2}{p}\right) = 1$, $c_p^+(\alpha,\mathfrak{r}) = \frac{p+2-1}{2} + 1 = \frac{p+3}{2}$ □

Proposition 3.5.3 *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$. Put $d = \Delta(\alpha)$. Then*

$$c_p^+(\alpha,\mathfrak{r})[X^+_{split}(p)] = c_p(\alpha,\mathfrak{r})[X^+_{split}(p)] = \begin{cases} t \not\equiv 0 \pmod{p} & 0 \\ t \equiv 0 \pmod{p} & \begin{cases} 1 & \text{if } \left(\frac{d}{p}\right) = -1 \\ 0 & \text{if } \left(\frac{d}{p}\right) = 0 \\ 1 & \text{if } \left(\frac{d}{p}\right) = 1. \end{cases} \end{cases}$$

Proof. In this case, $T_p \cap C_p(\alpha,\mathfrak{r}) = (T_\omega)_p \cap C_p(\alpha,\mathfrak{r})$ by Lemma 3.1.2. By Lemma 3.2.1, $g \in C_p(\alpha,\mathfrak{r})$ if and only if $p \cdot g \in D_p(p \cdot t(\alpha), p^2 \cdot n(\alpha), 0)$.

Suppose $g_\xi \in D_p(p \cdot t(\alpha), p^2 \cdot n(\alpha), 0)$. We count the number of g_ξ (up to $\xi \pmod{p^2}$) such that $g_\xi/p \in (T_\omega)_p$. Note that

$$g_\xi/p = \begin{pmatrix} \xi/p & 1 \\ \bar{n}(\xi)/p^2 & \xi/p + \bar{t}(\xi)/p \end{pmatrix}$$

For g_ξ/p to lie in $(T_\omega)_p$, we must have additionally

$$t \equiv 0 \pmod{p} \tag{3.23}$$
$$\xi \equiv 0 \pmod{p^2}. \tag{3.24}$$

There is one ξ modulo p^2 satisfying these conditions. As $t \equiv 0 \pmod{p}$, $\left(\frac{d}{p}\right) \neq 0$. Furthermore, there are no ξ's which satisfy

$$f_\alpha(\xi) \equiv 0 \pmod{p^{2\rho+3}}$$
$$t - 2\xi \equiv 0 \pmod{p^{\rho+2}}.$$

so all $\omega g_\xi \omega^{-1}$'s are $R_p^\times$-conjugate to the element g_ξ above. □

3.6 The case of Borel

From the table on p. 266 of [Miy89], the local invariants $c_p^+(\alpha, \mathfrak{r})$ for $\Gamma = \Gamma_0(p), \Gamma(1)$ can be obtained as:

Proposition 3.6.1 *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$. Put $[\mathfrak{r}_p : \mathbb{Z}_p[\alpha]] = p^\rho$, $D = \Delta(\alpha)$, $d = D/p^{2\rho}$, $\mu = ord_p(d)$. Then*

$$c_p^+(\alpha, \mathfrak{r})[X_0(p)] = \begin{cases} \mu \leq 1 & \begin{cases} 0 & \text{if } \left(\frac{d}{p}\right) = -1 \\ 1 & \text{if } \left(\frac{d}{p}\right) = 0 \\ 2 & \text{if } \left(\frac{d}{p}\right) = 1 \end{cases} \\ \mu > 1 & \begin{cases} 2 & \text{if } \left(\frac{d/p^2}{p}\right) = -1 \\ 2 & \text{if } \left(\frac{d/p^2}{p}\right) = 0 \\ 2 & \text{if } \left(\frac{d/p^2}{p}\right) = 1. \end{cases} \end{cases}$$

Proposition 3.6.2 *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$. Then*

$$c_p^+(\alpha, \mathfrak{r})[X_0(p)] = 0.$$

Proposition 3.6.3 *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$. Then*

$$c_p^+(\alpha, \mathfrak{r})[X(1)] = 1.$$

Proposition 3.6.4 *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$. Then*

$$c_p^+(\alpha, \mathfrak{r})[X(1)] = 0.$$

3.7 Explicit form of the trace formula

Following [Miy89] section 6.8, we give an numerically computable form of the trace formula in situation being considered in this chapter for weight $k = 2$.

We make more explicit the main term t^{Σ} of the trace formula in the form of 2.2.2:

$$t^{\Sigma} = -\lim_{s\to 0^+} \sum_{\alpha\in S_n//B^{\times}} k(\alpha) \sum_{\mathfrak{r}\supset\mathbb{Z}[M\alpha]} l(\mathfrak{r})h^+(\mathfrak{r}) \cdot \prod_v c_v^+(\alpha,\mathfrak{r}). \quad (3.25)$$

By Lemma 2.1.1, a complete set of representatives for $S_n//B^{\times}$ excluding scalars is given by the matrices

$$\begin{pmatrix} 0 & 1 \\ -n & t \end{pmatrix}$$

where $t \in \mathbb{Z}$. By construction, $t(\alpha) = t$ and $n(\alpha) = n$. Now, α is elliptic, hyperbolic-cuspidal, parabolic-cuspidal accordingly as $\Delta(\alpha) = t^2 - 4n$ is negative, a positive square, a positive non-square, zero. We now consider the inner sum according to the four cases above. Note that $c_{\infty}^+(\alpha,\mathfrak{r}) = 2, 1, 2$ accordingly as $\alpha \in T^e, T^{h,c}, T^{p,c}$ and $c_v^+(\alpha,\mathfrak{r}) = 1$ for $v \nmid M\infty$ (see Lemma 3.1.1).

If α is scalar, then n is necessarily a square and α must be

$$\alpha = \pm\begin{pmatrix} \sqrt{n} & 0 \\ 0 & \sqrt{n} \end{pmatrix}.$$

Now,

$$k(\alpha) = \frac{1}{4\pi} v(\Gamma\backslash\mathfrak{H}^*)$$
$$l(\alpha) = 1/\left|Z(\Gamma)\right|$$

so that

$$t^0 = \frac{1}{4\pi} v(\Gamma\backslash\mathfrak{H}^*). \quad (3.26)$$

Note that $T_n^0//\Gamma$ is easy to calculate directly so that it is not necessary to break it up any further as in the other cases.

If α is elliptic, then $K = \mathbb{Q}[\alpha]$ is an imaginary quadratic field. Write $t^2 - 4n = m^2 d_K$ so that $[\mathfrak{r}_K : \mathfrak{r}] = m$. The inner summation is over orders $\mathfrak{r}$ in K such that $\mathfrak{r}_K \supset \mathfrak{r} \supset \mathbb{Z}[M\alpha]$, or in other words, orders $\mathfrak{r}_f$ with conductor f dividing mM. Now,

$$k(\alpha) = 1$$
$$l(\mathfrak{r}_f) = 1/2\left|\mathfrak{r}_f^{\times}\right|$$

so that we have

$$t^e = -\sum_{t\in\mathbb{Z},t^2-4n=m^2 d_K,d_K<0} k(\alpha)\sum_{f|mM} l(\mathfrak{r}_f)h^+(\mathfrak{r}_f)\cdot 2\prod_{v|M} c_v^+(\alpha,\mathfrak{r}_f)$$
$$= \sum_{t\in\mathbb{Z},t^2-4n=m^2 d_K,d_K<0}\sum_{f|mM}\frac{h^+(\mathfrak{r}_f)}{|\mathfrak{r}_f^\times|}\cdot\prod_{v|M} c_v^+(\alpha,\mathfrak{r}_f). \quad (3.27)$$

If α is rational hyperbolic, then $K=\mathbb{Q}\times\mathbb{Q}$ is a product of two fields. Write $t^2-4n=m^2$ so that $[\mathfrak{r}_K:\mathfrak{r}]=m$. The inner sum is then over orders $\mathfrak{r}_f$ with conductor f dividing mM. Now,

$$k(\alpha)=\frac{\min(|\zeta_\alpha|,|\eta_\alpha|)}{|\zeta_\alpha-\eta_\alpha|}$$
$$h(\mathfrak{r}_f)=\phi(f)$$
$$l(\mathfrak{r}_f)=1/|Z(\Gamma)|$$

so that we have

$$t^h = -\sum_{t\in\mathbb{Z},t^2-4n=m^2} k(\alpha)\sum_{f|mM} l(\mathfrak{r}_f)h^+(\mathfrak{r}_f)\cdot\prod_{v|M} c_v^+(\alpha,\mathfrak{r}_f)$$
$$= \sum_{t\in\mathbb{Z},t^2-4n=m^2}\frac{\min(|\zeta_\alpha|,|\eta_\alpha|)}{|\zeta_\alpha-\eta_\alpha|}\sum_{f|mM}\frac{h^+(\mathfrak{r}_f)}{|Z(\Gamma)|}\cdot\prod_{v|M} c_v^+(\alpha,\mathfrak{r}_f). \quad (3.28)$$

If α is parabolic, let η be the unique eigenvalue of α so that $t=2\eta$ and $n=\eta^2$. Then $K=\mathbb{Q}[\alpha]=\mathbb{Q}[\epsilon]$ where $\epsilon=\alpha-\eta$ satisfies $\epsilon^2=0$. If $\mathfrak{r}=\mathbb{Z}[M\epsilon]$, then by Propositions 3.4.3, 3.5.3 and the fact that $(n,M)=1$, we see that $c_v^+(\alpha,\mathfrak{r})=0$ for $v\mid M$. Hence, in the inner sum, it suffices to sum over orders in K containing $\mathbb{Z}[\alpha]$. An order in K containing $\mathbb{Z}[\alpha]=\mathbb{Z}[\epsilon]$ is of the form $\mathfrak{r}^l=\mathbb{Z}+\frac{1}{l}\mathbb{Z}\epsilon$ where l is a positive integer. Now, $k(\alpha)=\frac{s}{4}$, $h^+(\mathfrak{r}^l)=h(\mathfrak{r}^l)=1$ and a routine calculation shows that $l(\mathfrak{r}^l)=\frac{(|\eta|/l)^{s+1}}{|Z(\Gamma)|}$. Therefore we have

$$t^p = -\lim_{s\to 0^+}\sum_{t\in\mathbb{Z},t^2-4n=0} k(\alpha)\sum_{l=1}^{\infty} l(\mathfrak{r}^l)h^+(\mathfrak{r}^l)\cdot 2\prod_{v|M} c_v^+(\alpha,\mathfrak{r}^l)$$
$$= -\lim_{s\to 0^+}\sum_{t\in\mathbb{Z},t^2-4n=0}\frac{s}{4}\frac{|\eta|^{s+1}}{|Z(\Gamma)|}\sum_{l=1}^{\infty}\frac{1}{l^{s+1}}\prod_{v|M}\cdot 2c_v^+(\alpha,\mathfrak{r}^l)$$
$$= -\lim_{s\to 0^+}\sum_{t\in\mathbb{Z},t^2-4n=0}\frac{s}{2}\frac{|\eta|^{s+1}}{|Z(\Gamma)|}\times\prod_{p\nmid M}(1-p^{-(s+1)})^{-1}\times\prod_{p|M}\sum_{\rho=0}^{\infty}\frac{1}{p^{\rho(s+1)}}c_p^+(\alpha,\mathfrak{r}^{p^\rho}) \quad (3.29)$$

For the subgroups under consideration, $c_p^+(\alpha,\mathfrak{r}^{p^\rho})$ does not depend on ρ in the case of α parabolic: if α is parabolic, the quantity μ is effectively equal to ∞ no matter what ρ is, so that $c_p^+(\alpha,\mathfrak{r}^{p^\rho})$ is a fixed value as it takes on a fixed value

once $\mu \geq 3$ (refer to Propositions 3.4.2, 3.5.2). Thus, the above expression is equal to

$$\begin{aligned} t^p &= -\lim_{s\to 0^+} \sum_{t\in\mathbb{Z}, t^2-4n=0} \frac{s}{2}\frac{|\eta|^{s+1}}{|Z(\Gamma)|}\zeta(s+1) \times \prod_{v|M} c_v^+(\alpha, \mathbb{Z}[\epsilon]) \\ &= \sum_{t\in\mathbb{Z}, t^2-4n=0} \frac{1}{2}\frac{|\eta|}{|Z(\Gamma)|} \times \prod_{v|M} c_v^+(\alpha, \mathbb{Z}[\epsilon]) \\ &= \frac{|\eta|}{|Z(\Gamma)|} \times \prod_{v|M} c_v^+(\alpha, \mathbb{Z}[\epsilon]). \quad (3.30) \end{aligned}$$

Chapter 4

The Jacobians of Cartan modular curves

In this chapter, the main result of this thesis is deduced from the trace calculations of the previous chapter. The main idea of the proof is consider the two abelian varieties $J(X^+_{\text{non-split}}(p))$ and $J(X_0^+(p^2))^{\text{new}}$ defined over $\mathbb{Q}$ and the Hecke algebra $\mathbb{T} = \mathbb{Z}[T_n \mid (n,p) = 1]$. The $\mathbb{T}$-modules $S_2(\Gamma^+_{\text{non-split}}(p))$ and $S_2(\Gamma_0^+(p^2))^{\text{new}}$ are semi-simple and have the same traces by Theorem 2. Thus, they are isomorphic $\mathbb{T}$-modules. By Eichler-Shimura, it follows that the L-series of the two abelian varieties above are the same, up to finitely-many L-factors. Faltings' isogeny Theorem then implies that the two abelian varieties in question are isogenous over $\mathbb{Q}$.

4.1 The new part of $J(X_0^+(p^2))$

Consider the decomposition

$$S_2(\Gamma_0(p^2)) = S_2(\Gamma_0(p^2)^{\text{new}} \oplus S_2(\Gamma_0(p^2))^{\text{old}} \tag{4.1}$$

where $S_2(\Gamma_0(p^2))^{\text{old}}$ is the vector space generated by the two inclusions of $S_2(\Gamma_0(p))$ into $S_2(\Gamma_0(p^2))$. The decomposition above is defined via the Petersson inner product and is stable under the action of Hecke. There is thus a corresponding decomposition of the jacobian $J(X_0(p^2))$ into a new and an old part which is stable under the action of Hecke. From Atkin-Lehner theory [AL70], there is a basis for $S_2(\Gamma_0(p^2))^{\text{new}}$ which consists of eigenforms for all Hecke operators. Furthermore, there is a basis for $S_2(\Gamma_0(p^2))^{\text{old}}$ which consists of eigenforms for T_q and W_p such that the eigenvalue for W_p is 1 for half of forms in the basis and -1 for the other half, and the eigenvalues for T_q correspond to their eigenvalues as eigenforms on $S_2(\Gamma_0(p))$. Explicitly, if $\{f_1(z) \dots f_g(z)\}$ is a basis for $S_2(\Gamma_0(p))$, where g is the genus of $X_0(p)$ and the $f_i(z)$ are eigenforms for all T_q, then $\{f_1(z) \pm f_1 \mid_{R_p} (z), \dots, f_g(z) \pm f_g \mid_{R_p} (z)\}$ is a basis for $S_2(\Gamma_0(p^2))^{\text{old}}$ with the required property, where $R_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. The sign in

$f_i(z) \pm f_i|_{R_p}(z)$ determines its eigenvalue for the operator W_p. Refer to Lemma 26 in [AL70] and the comments thereafter for more details.

The old part of the $J(X_0^+(p^2))$ therefore consists of one copy of $S_2(\Gamma_0(p))$ so we have

Lemma 4.1.1

$$tr(T_n \mid S_2(\Gamma_0^+(p^2))^{new}) = tr(T_n \mid S_2(\Gamma_0^+(p^2))) - tr(T_n \mid S_2(\Gamma_0(p))).$$

4.2 Comparison of trace formulae

The following table summarises the calculations done in chapter 3. Refer to the hypotheses of Propositions 3.4.2, 3.5.2, 3.4.3, 3.5.3 for further explanation of the terms used in the table.

			$\Gamma^+_{\text{non-split}}(p)$	$\Gamma^+_{\text{split}}(p)$	$\Gamma_0(p)$	$\Gamma(1)$
$\mathfrak{r}_p \supset \mathbb{Z}_p[\alpha]$	$\mu < 2$	$\left(\frac{d}{p}\right) = -1$	1	0	0	1
		$\left(\frac{d}{p}\right) = 0$	0	0	1	1
		$\left(\frac{d}{p}\right) = 1$	0	1	2	1
	$\mu \geq 2$	$\left(\frac{d/p^2}{p}\right) = -1$	$\frac{p-1}{2}$	$\frac{p+1}{2}$	2	1
		$\left(\frac{d/p^2}{p}\right) = 0$	$\frac{p-1}{2}$	$\frac{p+1}{2}$	2	1
		$\left(\frac{d/p^2}{p}\right) = 1$	$\frac{p+1}{2}$	$\frac{p+3}{2}$	2	1
$\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$	$t \not\equiv 0 \pmod p$		0	0	0	0
	$t \equiv 0 \pmod p$	$\left(\frac{d}{p}\right) = -1$	1	1	0	0
		$\left(\frac{d}{p}\right) = 0$	0	0	0	0
		$\left(\frac{d}{p}\right) = 1$	1	1	0	0

Table 4.1: Calculation of $c_p^+(\alpha, \mathfrak{r})$ for $X^+_{\text{non-split}}(p)$, $X^+_{\text{split}}(p)$, $X_0(p)$, $X(1)$

By inspection of the table, we obtain

$$c_p^+(\alpha,\mathfrak{r})[X^+_{\text{non-split}}(p)] - (c_p^+(\alpha,\mathfrak{r})[X^+_{\text{split}}(p)] - c_p^+(\alpha,\mathfrak{r})[X_0(p)]) = c_p^+(\alpha,\mathfrak{r})[X(1)]. \tag{4.2}$$

so that

$$t^{(\cdot)}[X^+_{\text{non-split}}(p)] - (t^{(\cdot)}[X^+_{\text{split}}(p)] - t^{(\cdot)}[X_0(p)]) = t^{(\cdot)}[X(1)] \tag{4.3}$$

where $(\cdot) = (e), (h,c), (p,c)$.

From the discussion in section 3.7,

$$t^o[X_\Gamma] = \frac{1}{4\pi} v(\Gamma\backslash\mathfrak{H}^*) \tag{4.4}$$

Therefore, using the fact that

$$v(\Gamma\backslash\mathfrak{H}^*) = \frac{1}{3\pi}[\Gamma(1) : \Gamma] \tag{4.5}$$

and $[\Gamma(1):\Gamma] = p(p-1)/2, p(p+1)/2, p+1, 1$ for $\Gamma = \Gamma^+_{\text{non-split}}(p), \Gamma^+_{\text{split}}(p), \Gamma_0(p), \Gamma(1)$, we see that

$$t^o[X^+_{\text{non-split}}(p)] - (t^o[X^+_{\text{split}}(p)] - t^o[X_0(p)]) = t^o[X(1)]. \tag{4.6}$$

Thus,

$$t^\Sigma[X^+_{\text{non-split}}(p)] - (t^\Sigma[X^+_{\text{split}}(p)] - t^\Sigma[X_0(p)]) = t^\Sigma[X(1)] \tag{4.7}$$

so that

$$\begin{aligned} &\text{tr}(T_n \mid S_2(\Gamma^+_{\text{non-split}}(p))) - (\text{tr}(T_n \mid S_2(\Gamma^+_{\text{split}}(p))) - \text{tr}(T_n \mid S_2(\Gamma_0(p)))) &(4.8)\\ &= \text{tr}(T_n \mid S_2(\Gamma(1))) = 0 &(4.9)\end{aligned}$$

for all n prime to p. By Lemma 4.1.1 and the fact that $X^+_0(p^2) \cong X^+_{\text{split}}(p)$, we obtain

Theorem 2 *For all n prime to p,*

$$tr(T_n \mid S_2(\Gamma^+_{non\text{-}split}(p))) = tr(T_n \mid S_2(\Gamma^+_0(p^2))^{new}).$$

4.3 The Eichler-Shimura relations

Let Γ be a strong arithmetic congruence group in $B^\times = \text{GL}_2(\mathbb{Q})$ of level N. Consider the modular curve X_Γ. The modular curve X_Γ has a proper smooth model over $\mathbb{Z}[1/N]$ so the reduction $\overline{X_\Gamma}/\mathbb{F}_q$ of X_Γ modulo q gives a smooth curve over $\mathbb{F}_q$ for $q \nmid N$ (see [Igu68] or [KM85]). Similarly, $J(X_\Gamma)$ has a proper smooth model over $\mathbb{Z}[1/N]$ so the reduction $\overline{J_\Gamma}/\mathbb{F}_q$ of $J(X_\Gamma)$ modulo q gives an abelian variety over $\mathbb{F}_q$ for $q \nmid N$. The Hecke operator T_q can be considered as an endomorphism of $J(X_\Gamma)$ which can be reduced mod q to give an endomorphism $\overline{T}_q$ of $\overline{J(X_\Gamma)}/\mathbb{F}_q$.

Theorem 4.3.1 *(Eichler-Shimura) Let Γ be a strong arithmetic congruence group in $B^\times = GL_2(\mathbb{Q})$ of level N. Let X_Γ be the corresponding modular curve over $\mathbb{Z}[1/N]$. For $q \nmid N$, we have*

$$\overline{T}_q = F_q + V_q < q > \text{ as endomorphisms of } \overline{J(X_\Gamma)}/\mathbb{F}_q$$

where F_q and V_q are the Frobenius and Vershiebung endomorphisms on $\overline{J(X_\Gamma)}$, and $< q >$ is the endomorphism of $\overline{J(X_\Gamma)}$ induced by letting the matrix $\begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z})$ act on X_Γ.

Proof. See Theorem 7.9 in [Shi71]. □

If Γ_p contains all scalars for $p \mid N$, then the diamond operators act trivially. We will assume this is the case in the sequel as $\Gamma^+_{\text{non-split}}(p), \Gamma^+_{\text{split}}(p), \Gamma_0(p), \Gamma(1)$ all have this property.

For an abelian variety A defined over $\mathbb{Q}$, the L-factor at a prime q is defined to be

$$L_q(A, X) = \det(1 - F_q X \mid T_l(A))^{-1} \tag{4.10}$$

where $X = q^{-s}$ and l is any prime. The Eichler-Shimura congruence relation allows one to express the L-factor of $J = J(X_\Gamma)$ at a prime $q \nmid N$ in terms of the action of the Hecke operator T_q on $S_2(\Gamma)$ [BSD72]. We briefly recall this process:

Suppose $q \neq l$. From the identity $F_q V_q = V_q F_q = q$, we see that

$$\begin{aligned}
\det(1 - \overline{T}_q X + qX^2 \mid T_l(\overline{J})) &= \det(1 - F_q X \mid T_l(\overline{J})) \cdot \det(1 - V_q X \mid T_l(\overline{J})) \\
&= \det(1 - F_q X \mid T_l(\overline{J}))^2 \\
&= \det(1 - F_q X \mid T_l(J))^2 \text{ (since } l \neq q) \\
&= L_q(A, X)^2
\end{aligned}$$

where the equality $\det(1 - F_q X \mid T_l(\overline{J})) = \det(1 - V_q X \mid T_l(\overline{J}))$ follows from a calculation in [Wei48].

On the other hand,

$$\begin{aligned}
\det(1 - \overline{T}_q X + qX^2 \mid T_l(\overline{J})) &= \det(1 - T_q X + qX^2 \mid T_l(J)) \text{ (since } l \neq q) \\
&= \det(1 - T_q X + qX^2 \mid H^{1,+}(J, \mathbb{C}) \oplus H^{1,-}(J, \mathbb{C})) \\
&= \det(1 - T_q X + qX^2 \mid H^{1,+}(J, \mathbb{C}))^2
\end{aligned}$$

where we use the fact that the l-adic cohomology is isomorphic to two copies of the complex cohomology (Hodge decomposition). Since $H^{1,+}(J, \mathbb{C}) = H^0(J, \Omega^1(J)) = H^0(X_\Gamma, \Omega^1(X_\Gamma)) = S_2(\Gamma)$, the L-factor at q for J is therefore

$$L_q(J, X) = \det(1 - T_q X + qX^2 \mid S_2(\Gamma)). \tag{4.11}$$

Thus, by choosing $l \mid N$ in the above argument, we see that the action of the Hecke algebra $\mathbb{T} = \mathbb{Z}[T_n \mid (n, N) = 1]$ on $S_2(X_\Gamma)$ determines the L-factors of $J(X_\Gamma)$ at primes $q \nmid N$.

What has been said above also applies to any quotient of $J(X_\Gamma)$ which is stable under the action of Hecke by replacing $S_2(\Gamma)$ by a suitable subspace. For instance, the L-factors of $J(X_0^+(p^2))^{\text{new}}$ at primes $q \neq p$ are determined by the action of the Hecke algebra $\mathbb{T} = \mathbb{Z}[T_n \mid (n, p) = 1]$ on $S_2(\Gamma_0^+(p^2))^{\text{new}}$.

4.4 The Jacobian of $X^+_{non-split}(p)$

Consider the Hecke algebra $\mathbb{T} = \mathbb{T}(\Gamma^+_{\text{non-split}}(p)) \cong \mathbb{T}(\Gamma_0^+(p^2)) = \mathbb{Z}[T_n \mid (n, p) = 1]$. The $\mathbb{T}$-modules $S_2(\Gamma^+_{\text{non-split}}(p))$ and $S_2(\Gamma_0^+(p^2))^{\text{new}}$ are semi-simple as there is a basis for $S_2(\Gamma^+_{\text{non-split}}(p))$ and $S_2(\Gamma_0^+(p^2))^{\text{new}}$ consisting of eigenforms for $\mathbb{T}$.

Lemma 4.4.1 *Let M be a finite-dimensional vector space over $\mathbb{C}$. Suppose we have a representation of a ring R*

$$\rho : R \to End(M)$$

which gives M the structure of a semi-simple R-module.

Then the character χ of ρ

$$\begin{aligned} \chi : R &\to \mathbb{C} \\ r &\mapsto tr(\rho(r)) \end{aligned}$$

determines the representation ρ up to isomorphism.

Proof. This is a well-known principle. □

Since the two semi-simple $\mathbb{T}$-modules $S_2(\Gamma^+_{\text{non-split}}(p))$ and $S_2(\Gamma^+_0(p^2))^{\text{new}}$ have the same characters by Theorem 2, they are isomorphic $\mathbb{T}$-modules by the above Lemma. By the discussion in the previous section, we then see that the L-factors of $J(X^+_{\text{non-split}}(p))$ and $J(X^+_0(p^2))^{\text{new}}$ are the same for all $q \neq p$. Therefore, by Faltings' isogeny Theorem [Fal86], the two abelian varieties above are isogenous over $\mathbb{Q}$.

Theorem 1 *The jacobian of $X^+_{non\text{-}split}(p)$ is isogenous to the new part of the jacobian of $X^+_0(p^2)$.*

4.5 A trace relation in higher weights

The quantities $c^+_p(\alpha, \mathfrak{r})$ do not depend on the weight of the space of cusp forms on which the Hecke operators act. Hence, a similar trace relation holds for the space of cusp forms of higher weight:

$$\begin{aligned} &\text{tr}(T_n \mid S_k(\Gamma^+_{\text{non-split}}(p))) - \text{tr}(T_n \mid S_k(\Gamma(1)) \\ &= \text{tr}(T_n \mid S_k(\Gamma^+_{\text{split}}(p))) - \text{tr}(T_n \mid S_2(\Gamma_0(p)) \end{aligned} \tag{4.12}$$

for all n prime to p. In general, $S_k(\Gamma(1))$ is non-zero for higher weights so the trace relation now asserts that the trace on $S_k(\Gamma^+_{\text{non-split}}(p))$ excluding level 1 old forms is the same as the trace on $S_k(\Gamma^+_{\text{split}}(p))$ excluding level p old forms. It would be interesting to interpret this trace relation geometrically, especially in terms of Edixhoven's setting [Edi95].

Mazur's approach to studying the rational points on $X_0(p)$, a certain quotient of $J_0(p)$ called the Eisenstein quotient was used. An essential property of this quotient is that it is non-trivial and has finite Mordell-Weil group. The isogeny between $J(X^+_{\text{non-split}}(p))$ and $J(X^+_0(p^2))^{\text{new}}$ shows that such behaviour does not occur in the non-split case, at least conjecturally: $J(X^+_0(p^2))^{\text{new}}$ decomposes up to isogeny into a product of simple abelian varieties defined over $\mathbb{Q}$ whose L-series have negative ϵ-factors. Thus, standard conjectures predict

that each factor has positive rank and $J(X^+_{\text{non-split}}(p))$ does not have any non-trivial quotients with finite Mordell-Weil group. Thus, one cannot even begin to apply Mazur's approach. Notice in the case of $X^+_{\text{split}}(p)$, one can get around this because of the old part in $X_0^+(p^2) \cong X^+_{\text{split}}(p)$. Indeed, Mazur describes a surjective map from $J(X^+_{\text{split}}(p))$ to $J_0^-(p)$ which Momose exploits in his study of rational points on $X^+_{\text{split}}(p)$.

If one descends to $X_0(p)$ to study the points on $X^+_{\text{split}}(p)$, the trace relation above suggests that one should descend to $X(1)$ to study the points on $X^+_{\text{non-split}}(p)$. However, in order to get something non-trivial from $X(1)$, one has to consider cusp forms of higher weight whose geometry less well-understood.

Chapter 5

Examples

5.1 Cartan modular curves of genus ≤ 1

The Cartan modular curves $X^+_{\text{non-split}}(p)$ and $X^+_{\text{split}}(p)$ have genus zero precisely when $p = 3, 5, 7$, and in each case a $\mathbb{Q}$-rational point exists on the curve.

Suppose $X = \Gamma\backslash\mathfrak{H}^*$ is a genus zero Cartan modular curve as above. The existence of a $\mathbb{Q}$-rational point on X means that the function field of X is of the form $\mathbb{Q}(t)$. The function t is called a *hauptmodul* of X.

Since X is a finite cover of $X(1)$, the function field $\mathbb{Q}(t)$ is a finite extension of $\mathbb{Q}(j)$. This implies that there is a relation of the form

$$j = \frac{P(t)}{Q(t)} \tag{5.1}$$

where $P(x)$, $Q(x)$ are polynomials in $\mathbb{Q}[x]$. As entertainment for the reader, these relations will be computed explicitly in the spirit of Fricke and Klein, though details will only be provided in the non-split case since the calculation in the split case is of a more standard nature [Bir72].

The hauptmodul t is unique up to a $\mathbb{Q}$-Mobius transformation. Hence, it is necessary to normalise it uniquely before attempting to find its relation with j. This can be done in a number of ways: one can, for instance, specify its value on three distinct points, or its value on two distinct points and the leading coefficient of its q-expansion. Whatever the method of normalising t, one is still left with the following problem: only certain normalisations of t are allowed. An arbitrary normalisation of t will in general give a hauptmodul for X over $\mathbb{C}$: it will generate the function field of the curve over $\mathbb{C}$, but it will not in general generate the function field of the curve over $\mathbb{Q}$. Hence, although j would still be a rational function of such a t, the coefficients of this rational function would in general lie in $\mathbb{C}$. To get a proper normalisation, one needs to know more about the desired hauptmodul t.

Lemma 5.1.1 *Let $\mathfrak{F}(p)$ be the modular function of level p and suppose H is a subgroup of $GL_2(\mathbb{F}_p)/\{\pm 1\} = Gal(\mathfrak{F}(p)|\mathbb{Q}(j))$. Let $\mathfrak{F}_H(p)$ be the fixed field of H*

and suppose t_H be a primitive element for the extension $\mathfrak{F}_H(p)|\mathbb{Q}(j)$. Consider the group

$$D = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix} \mid d \in \mathbb{F}_p^\times \right\} \tag{5.2}$$

Then the field generated by the coefficients of the q-expansion of t_H is the subfield of $\mathbb{Q}(\zeta_p)$ given by the fixed field of the group $det(D \cap H) \subset \mathbb{F}_p^\times = Gal(\mathbb{Q}(\zeta_p)|\mathbb{Q})$.

Proof. A matrix of the form $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ acts as $d \in \mathbb{F}_p^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ on the q-coefficients of t_H. This follows from $\mathfrak{F}(p)$ being generated over $\mathbb{Q}(j)$ by the Fricke functions f_a and that the action of such a matrix on a Fricke function f_a is as described by inspection of the q-expansion of f_a. Note that the q-coefficients of t_H lie in $\mathbb{Q}(\zeta_p)$ so this makes sense. Such a matrix therefore fixes the field of q-coefficients of t_H if and only if it lies in H. □

Remark 5.1.1 *Although j and f_a have convergent q-expansions, the general element in $\mathbb{Q}(j, f_a)$ will not. Even so, the description of the action of matrices in D on elements in $\mathbb{Q}(j, f_a)$ still holds.*

Corollary 5.1.1 *Let t be a hauptmodul for a genus zero Cartan modular curve over $\mathbb{Q}$. The field generated by the coefficients of the q-expansion of t is $\mathbb{Q}$, $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ in the split, non-split case, respectively.*

Lemma 5.1.2 *Suppose that $j = \lambda \frac{P(t)}{Q(t)}$ where t is a hauptmodul for a genus zero subgroup Γ of $\Gamma(1)$, $P(x)$ and $Q(x)$ are monic polynomials in $\mathbb{Q}[x]$, and $\lambda \in \mathbb{Q}$. Let K denote the field generated by the coefficients of the q-expansion of t. If $deg(P) = deg(Q)$, then $K = \mathbb{Q}(a_0)$ where a_0 is a root of $Q(x)$. Otherwise, $K = \mathbb{Q}(\lambda^{\frac{1}{h}})$ where h is the width of the cusp ∞.*

Proof. Let $\mu = [\Gamma(1) : \Gamma]$. If $t = a_{-1}q^{-1} + a_0 + a_1 q + a_2 q^2 + \ldots$ where $a_{-1} \neq 0$, then $deg(P) = \mu$ and $deg(Q) = \mu - h$. Substituting the q-expansions of t and j into the equation $jQ(t) = \lambda P(t)$, and equating powers of q, we see that $a_{-1} = 1/\lambda^{\frac{1}{h}}$ and a_n is a polynomial with $\mathbb{Q}$-coefficients in $a_{-1}, a_0, \ldots, a_{n-1}$ for $n \geq 0$. Hence, $K = \mathbb{Q}(\lambda^{\frac{1}{h}})$.

If $t = a_0 + a_1 q + a_2 q^2 + \ldots$ where $a_0 \neq 0$, then $deg(P) = deg(Q) = \mu$. Again, by substituting the q-expansions of t and j into the equation $jQ(t) = \lambda P(t)$, we see that a_0 is a root of $Q(x)$ and $a_n \in \mathbb{Q}(a_0, \ldots, a_{n-1})$ for $n \geq 0$. Therefore, $K = \mathbb{Q}(a_0)$ where a_0 is a root of $Q(x)$.

If $t = a_1 q + a_2 q^2 + \ldots$, then $deg(Q) = \mu$ and $deg(P) = \mu - h$. By the substitution $t \to 1/t$, we can reduce to the first case. □

Corollary 5.1.2 *The coefficients of the q-expansion of t lie in $\mathbb{Q}$ if and only if t has a normalisation with $t(\infty) = \infty$ and λ is an h-th power.*

Proof. Suppose that $j = \lambda\frac{P(t)}{Q(t)}$ where $deg(P) = deg(Q)$. Since the coefficients of the q-expansion of t lie in $\mathbb{Q}$, $Q(x)$ must have a root a in $\mathbb{Q}$ by the proof of Lemma 5.1.2. By the substitution $t \to 1/(t-a)$, a normalisation with $t(\infty) = \infty$ is obtained. If on the other hand $deg(P) = \mu - h$ and $deg(Q) = \mu$, the substitution $t \to 1/t$ gives the desired normalisation.

Conversely, suppose t has a normalisation with $t(\infty) = \infty$ and λ is an h-th power. By Lemma 5.1.2, the q-coefficients of t lie in $\mathbb{Q}$. □

The above Corollary provides a starting point for finding the correct normalisation. By Lemma 5.1.1, the field of q-coefficients of t in the non-split case is precisely $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$, which is strictly larger than $\mathbb{Q}$ for $p = 5, 7$. Hence, in these two cases, t does not have a normalisation with $t(\infty) = \infty$. Indeed, the covering relation

$$j = \lambda\frac{P(t)}{Q(t)} \tag{5.3}$$

must have the property $deg(P) = deg(Q)$ where each root of $Q(x)$ generates the field $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$. Any two primitive elements of the extension $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)|\mathbb{Q}$ differ by a $\mathbb{Q}$-Mobius transformation if $p = 5, 7$ (since the degree of the extension is ≤ 3). Now, $X^+_{\text{non-split}}(p)$ has 2, 3 cusps respectively when $p = 5$, 7, so $Q(x)$ is a 5^{th}, 7^{th} power of some degree 2, 3 polynomial. Because of the above remark, a suitable $\mathbb{Q}$-Mobius transformation allows us to assume that these two polynomials are $x^2 + x + 1$, $x^3 + x^2 - 2x - 1$, respectively.

One can now find a suitable normalisation (keeping in mind the restrictions and deductions outlined above) for t. From the fundamental domain of Γ, one can deduce how the finite cover $X \to X(1)$ branches. This in turn allows us to set up a system of non-linear equations which determine the desired covering relation between j and t. The method described works in principle, but the system of equations which one must solve is usually too large to be done even on a computer. Hence, in practice one must try to reduce the size of resulting system of equations any which way one can. To reduce the number of variables, one should always try to choose a normalization which places a known value at a branched point. Also, if the covering factors through an intermediate curve, then one can compute the relation in two steps, keeping in mind the intermediate hauptmodul may have to be normalised in two different ways to obtain the smallest system of equations for each of the two covering relations in the factorisation.

The non-split case: For $p = 3$, the direct approach works. For $p = 5$, we use the factorisation $X_{\text{non-split}}(5) \to X_{A_4}(5) \to X(1)$ and the covering $X_{\text{non-split}}(5) \to X^+_{\text{non-split}}(5)$. For $p = 7$, we use the factorisation $X^+_{\text{non-split}}(7) \to$

$X_{S_4}(7) \to X(1)$. The relations obtained are

$$j = n_3^3 \tag{5.4}$$

$$j = 5^4 \frac{(2n_5+1)(n_5+1)^3(6n_5^2+21n_5+19)^3}{(n_5^2+n_5-1)^5} \tag{5.5}$$

$$j = \frac{((4n_7^2+5n_7+2)(n_7^2+3n_7+4)(n_7^2+10n_7+4)(3n_7+1))^3}{(n_7^3+n_7^2-2n_7-1)^7} \tag{5.6}$$

where n_3, n_5, n_7 are the hauptmoduln of $X^+_{\text{non-split}}(p)$ for $p = 3, 5, 7$, respectively. One can verify these covering maps independently. To check they are correct over $\mathbb{C}$, it suffices to verify that the covering relation factors in a way which corresponds to how the points i, ρ, ∞ branch. To check they are correct over $\mathbb{Q}$, we can proceed as follows: Let $m_p(\tau)$ be a hauptmodul for $X^+_{\text{non-split}}(p)$ over $\mathbb{Q}$. If we can find three points $\tau_1, \tau_2, \tau_3 \in \mathfrak{H}^*$ such that both m_p and n_p take on three distinct $\mathbb{Q}$-values, then it would follow that m_p and n_p are related by a $\mathbb{Q}$-mobius transformation, and hence n_p is also a hauptmodul for $X^+_{\text{non-split}}(p)$ over $\mathbb{Q}$. By the modular interpretation of $X^+_{\text{non-split}}(p)$, it is easy to find such τ from CM-points. It is then a matter to check the corresponding value of n_p is rational. For instance, consider $p = 7$. For τ_1, τ_2, τ_3 corresponding to elliptic curves over $\mathbb{Q}$ with CM by $-8, -11, -16$, respectively, one obtains a $\mathbb{Q}$-point on $X^+_{\text{non-split}}(7)$ and hence m_7 takes on $\mathbb{Q}$-values for these τ. The j-invariants of these curves are known to be $20^3, -32^3, 66^3$. If one substitutes these values of j into the covering relation above and solves for the corresponding values of n_7, one obtains at least one $\mathbb{Q}$-value for n_7 in each case. Therefore, by the above discussion, n_7 is also a hauptmodul for $X^+_{\text{non-split}}(7)$ over $\mathbb{Q}$.

The split case:

$$j = \frac{((s_3-9)(s_3+3))^3}{s_3^3} \tag{5.7}$$

$$j = \frac{((s_5^2-5)(s_5^2+5s_5+10)(s_5+5))^3}{(s_5^2+5s_5+5)^5} \tag{5.8}$$

$$j = \frac{((s_7^2-5s_7+8)(s_7^2-5s_7+1)(s_7^4-5s_7^3+8s_7^2-7s_7+7)(s_7+1))^3 s_7}{(s_7^3-4s_7^2+3s_7+1)^7} \tag{5.9}$$

where s_3, s_5, s_7 are the hauptmoduln of $X^+_{\text{split}}(p)$ in the case of $p = 3, 5, 7$, respectively.

The modular curves $X_{\text{split}}(p)$ and $X_{\text{non-split}}(p)$ have genus zero precisely when $p = 3, 5$. However, these genus zero curves may still lack $\mathbb{Q}$-points. Hence, the function field of these genus zero curves are generated by a hauptmodul only after some finite extension of $\mathbb{Q}$. For instance, consider the case of $X_{\text{non-split}}(3)$. One model for its function field is $\mathbb{Q}(n_3, f)$ where n_3 and f satisfy $f^2 + n_3^2 + 12n_3 + 144 = 0$. Notice this defines a non-singular conic which does not have a rational point. Moreover, f is not a hauptmodul for the curve. On the other hand, over $\mathbb{Q}(i)$, the curve has a rational point and hence has a hauptmodul t

whose covering relation is of the form

$$n_3 = -6\frac{t^2 + (1+3i)t + (1+\frac{3}{2}i)}{t^2+t+1}. \tag{5.10}$$

Note the following curious phenomenon. The curves $X^+_{\text{split}}(3)$ and $X_{\text{non-split}}(3)$ are isomorphic over $\overline{\mathbb{Q}}$ since they have the same fundamental domains. However, they are not $\mathbb{Q}$-isomorphic. Hence, to distinguish between these two curves, one must pick out the correct $\mathbb{Q}$-model in a $\overline{\mathbb{Q}}$-isomorphism class of curves. This does not occur for larger p as the values of genus then begin to differ.

Modular curves associated to Cartan subgroups have genus one in only three cases: $X_{\text{non-split}}(7)$, $X_{\text{split}}(7)$, $X^+_{\text{non-split}}(11)$. Using the degree 2 cover

$$X_{\text{non-split}}(7) \to X^+_{\text{non-split}}(7) \tag{5.11}$$

one can identify the elliptic curve $X_{\text{non-split}}(7)$ as 49B in the tables of [BK72]. Clearly, $X_{\text{split}}(7)$ is the strong Weil curve 49A, so that these curves are 2-isogenous.

Given this description of $X_{\text{non-split}}(7)$, one can go a bit further. The invariant differential can be expressed in terms of explicit functions on the original curve so that one can compute its q-expansion. This differential should correspond up to a scaling factor to the newform on $X_{\text{non-split}}(7)$. Below are the first 13 terms of its q-expansion after rescaling so $a_1 = 1$

$$a_1 = 1 \tag{5.12}$$
$$a_2 = -(\zeta + 1) \tag{5.13}$$
$$a_3 = 0 \tag{5.14}$$
$$a_4 = -\zeta \tag{5.15}$$
$$a_5 = 0 \tag{5.16}$$
$$a_6 = 0 \tag{5.17}$$
$$a_7 = 0 \tag{5.18}$$
$$a_8 = -3 \tag{5.19}$$
$$a_9 = 3(\zeta + 1) \tag{5.20}$$
$$a_{10} = 0 \tag{5.21}$$
$$a_{11} = 4\zeta \tag{5.22}$$
$$a_{12} = 0 \tag{5.23}$$
$$a_{13} = 0 \tag{5.24}$$

where ζ is a root of $x^3 + x^2 - 2x - 1$. The original coefficient a_1 obtained from the computation was

$$a_1 = .639524003844966302873925622 89i \tag{5.25}$$

so the analogue of Manin's constant in the case of $X^+_{\text{non-split}}(p)$ is not one.

One can try to compute the equations for $X^+_{\text{non-split}}(11)$ and $X^+_{\text{split}}(11)$ in the spirit of Fricke and Klein. However, we note that the cycloidal 11 subgroup only contains the normaliser of a split Cartan subgroup (because A_5 does not have an element of order 6!). Thus, it would be difficult to compute an equation since there are no intermediate curves in the non-split case. Although one may try to compute the curve from scratch in the split case, we already know what it must be from the known tables, namely, the strong Weil curve 121D. The elliptic curve $X^+_{\text{non-split}}(11)$ has been identified as lying in the isogeny class of 121D by computing the first few terms of its L-series using modular symbols as well as the trace formula, so $X^+_{\text{non-split}}(11)$ is the 11-isogenous curve 121E (as they cannot be $\mathbb{Q}$-isomorphic and there are only two curves in this isogeny class).

5.2 A sample calculation of the trace formula

To illustrate the explicit trace formula in 3.7, the trace of T_1 and T_2 will be calculated by hand for $X^+_{\text{non-split}}(p)$. In fact, we have implemented the trace formula on computer for both $X^+_{\text{non-split}}(p)$ and $X^+_{\text{split}}(p)$. The traces obtained for $X^+_{\text{split}}(p)$ have agreed with tables [BK72] for various n and p.

The trace of T_1

We calculate the terms t^o, t^e, $t^{h,c}$, $t^{p,c}$ in the trace formula for T_1 on $\Gamma = \Gamma^+_{\text{non-split}}(p)$.

$$t^o = \frac{1}{4\pi} v(\Gamma\backslash\mathfrak{H}) = \frac{1}{12}[\Gamma(1):\Gamma] = \frac{1}{24}p(p-1) \tag{5.26}$$

$$\begin{aligned} -t^e &= \sum_{t\in\mathbb{Z}, t^2-4=m^2 d_K, d_K<0} \sum_{f|pm} \frac{h^+(\mathfrak{r}_{f^2 d_K})}{\left|\mathfrak{r}^\times_{f^2 d_K}\right|} \cdot c_p^+(\alpha, \mathfrak{r}_{f^2 d_K}) \\ &= \frac{h^+(\mathfrak{r}_{-4})}{|\mathfrak{r}_{-4}|} \cdot c_p^+(\alpha, \mathfrak{r}_{-4}) + \frac{h^+(\mathfrak{r}_{-p^2\cdot 4})}{|\mathfrak{r}_{-p^2\cdot 4}|} \cdot c_p^+(\alpha, \mathfrak{r}_{-p^2\cdot 4}) + 2\frac{h^+(\mathfrak{r}_{-3})}{|\mathfrak{r}_{-3}|} \cdot c_p^+(\alpha, \mathfrak{r}_{-3}) \\ &= \frac{1}{4}\frac{1-\left(\frac{-4}{p}\right)}{2} + \frac{1}{8}(p - \left(\frac{-4}{p}\right)) + \frac{2}{6}\frac{1-\left(\frac{-3}{p}\right)}{2} \\ &= \frac{1}{24}(3p - 6\left(\frac{-4}{p}\right) - 4\left(\frac{-3}{p}\right) + 7) \end{aligned} \tag{5.27}$$

$$t^{h,c} = 0 \tag{5.28}$$

$$-t^{p,c} = \frac{p-1}{4} \tag{5.29}$$

Therefore, $\mathrm{tr}(T_1) = t_0 + t_1^e + t_1^h + t_1^p + \sigma(1)$ is

$$g^+_{\text{non-split}}(p) = \frac{1}{24}(p^2 - 10p + 23 + 6\left(\frac{-1}{p}\right) + 4\left(\frac{-3}{p}\right)). \tag{5.30}$$

Note we have made simplications which make the above formula incorrect for $p = 2, 3$.

A similar calculation for $\Gamma = \Gamma^+_{\text{split}}(p)$ yields

$$g^+_{\text{split}}(p) = \frac{1}{24}(p^2 - 8p + 11 - 4\left(\frac{-3}{p}\right)) \tag{5.31}$$

where $p \neq 2, 3$.

The trace of T_2

We calculate the terms t^o, t^e, $t^{h,c}$, $t^{p,c}$ in the trace formula for T_2 on $\Gamma = \Gamma^+_{\text{non-split}}(p)$. Since 2 is not a square, $t^o = t^{p,c} = 0$, so it is only necessary to calculate the terms t^e and $t^{h,c}$:

$$\begin{aligned} -t^e &= \sum_{t\in\mathbb{Z}, t^2-8=m^2 d_K, d_K<0} \sum_{f|pm} \frac{h^+(\mathfrak{r}_{f^2 d_K})}{\left|\mathfrak{r}^\times_{f^2 d_K}\right|} \cdot c_p^+(\alpha, \mathfrak{r}_{f^2 d_K}) \\ &= \frac{h^+(\mathfrak{r}_{-8})}{|\mathfrak{r}_{-8}|} \cdot c_p^+(\alpha, \mathfrak{r}_{-8}) + \frac{h^+(\mathfrak{r}_{-p^2\cdot 8})}{|\mathfrak{r}_{-p^2\cdot 8}|} \cdot c_p^+(\alpha, \mathfrak{r}_{-p^2\cdot 8}) + 2\frac{h^+(\mathfrak{r}_{-7})}{|\mathfrak{r}_{-7}|} \cdot c_p^+(\alpha, \mathfrak{r}_{-7}) \\ &\qquad + 2\frac{h^+(\mathfrak{r}_{-4})}{|\mathfrak{r}_{-4}|} \cdot c_p^+(\alpha, \mathfrak{r}_{-4}) \\ &= \frac{1}{2}\frac{1 - \left(\frac{-8}{p}\right)}{2} + \frac{1}{4}(p - \left(\frac{-8}{p}\right)) + \frac{2}{2}\frac{1 - \left(\frac{-7}{p}\right)}{2} + \frac{2}{4}\frac{1 - \left(\frac{-4}{p}\right)}{2} \\ &= \frac{1}{4}(p - 2\left(\frac{-8}{p}\right) - 2\left(\frac{-7}{p}\right) - \left(\frac{-4}{p}\right) + 4) \end{aligned} \tag{5.32}$$

$$t^{h,c} = 0 \tag{5.33}$$

Therefore, $\mathrm{tr}(T_2) = t^e + \sigma(2)$ is

$$\mathrm{tr}(T_2 \mid S_2(\Gamma^+_{\text{non-split}}(p))) = \frac{1}{4}(-p + 2\left(\frac{-2}{p}\right) + 2\left(\frac{-7}{p}\right) + \left(\frac{-1}{p}\right) + 8). \tag{5.34}$$

Note we have made simplications which make the above formula incorrect for $p = 2, 3, 7$.

A similar calculation for $\Gamma = \Gamma^+_{\text{split}}(p)$ yields

$$\mathrm{tr}(T_2 \mid S_2(\Gamma^+_{\text{split}}(p))) = \frac{1}{4}(-p - 2\left(\frac{-7}{p}\right) - \left(\frac{-1}{p}\right) + 4) \tag{5.35}$$

for $p \neq 2, 3, 7$.

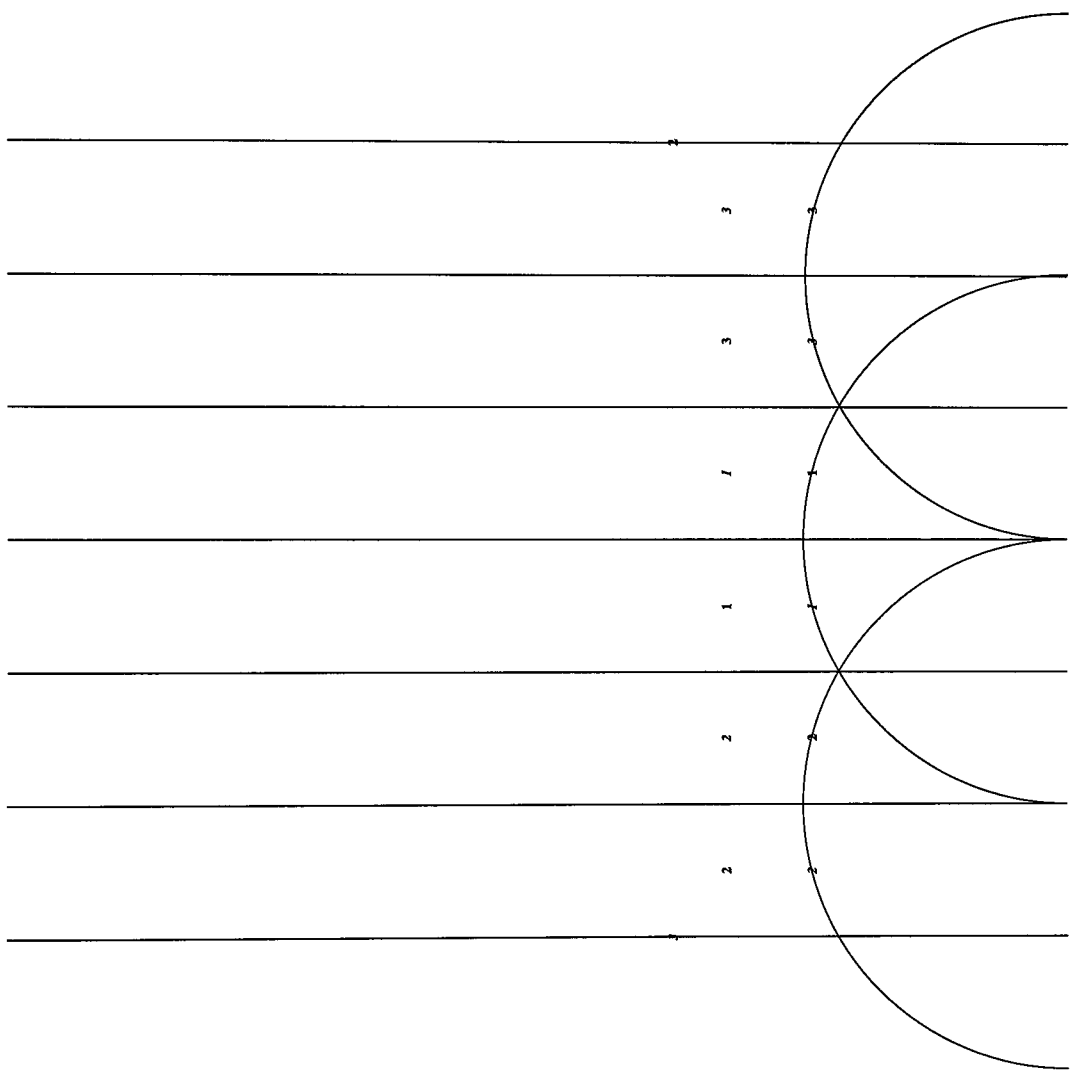


Figure 5.1: Fundamental domain for $X^{+}_{\text{non-split}}(3)$

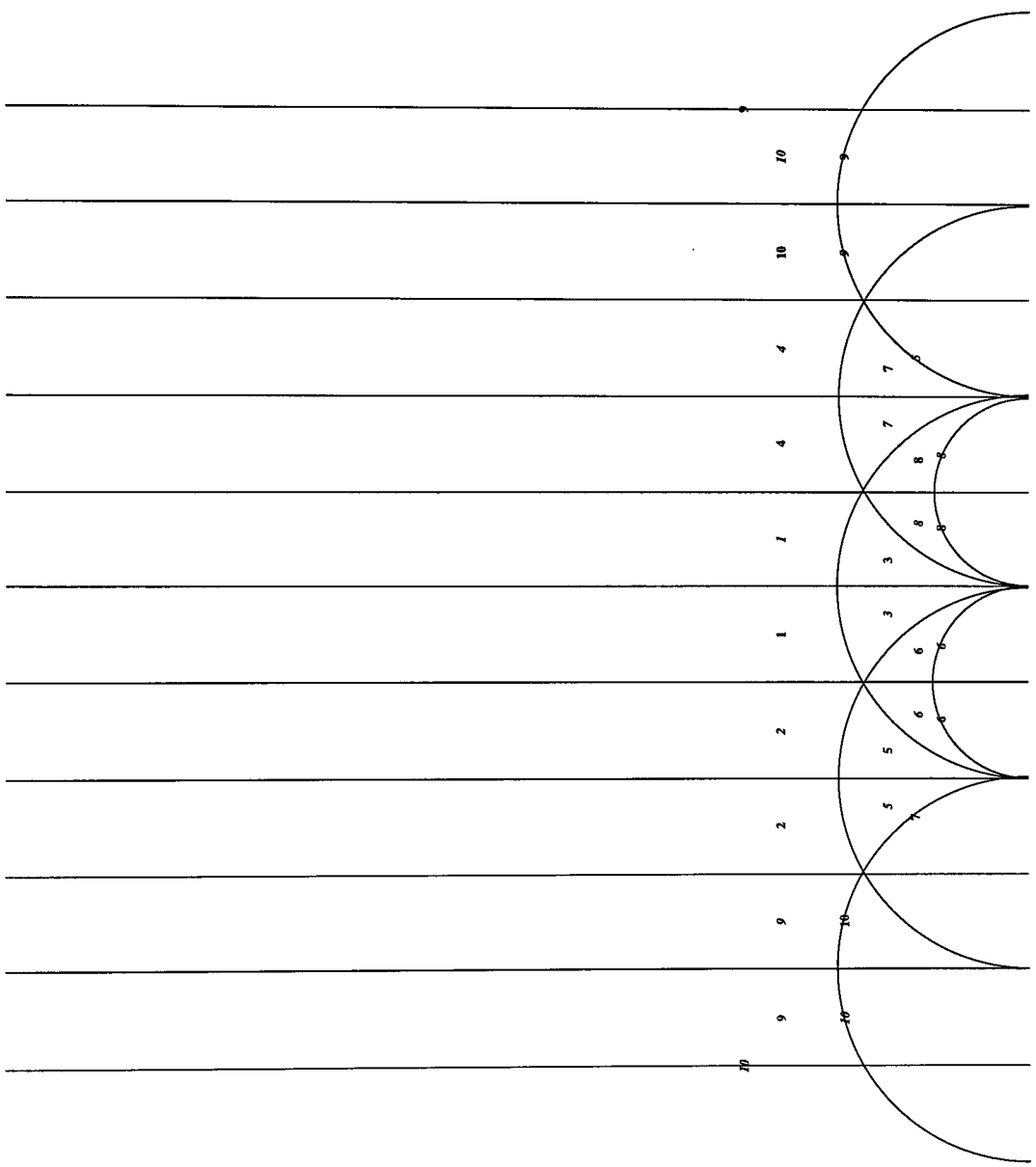


Figure 5.2: Fundamental domain for $X^{+}_{\text{non-split}}(5)$

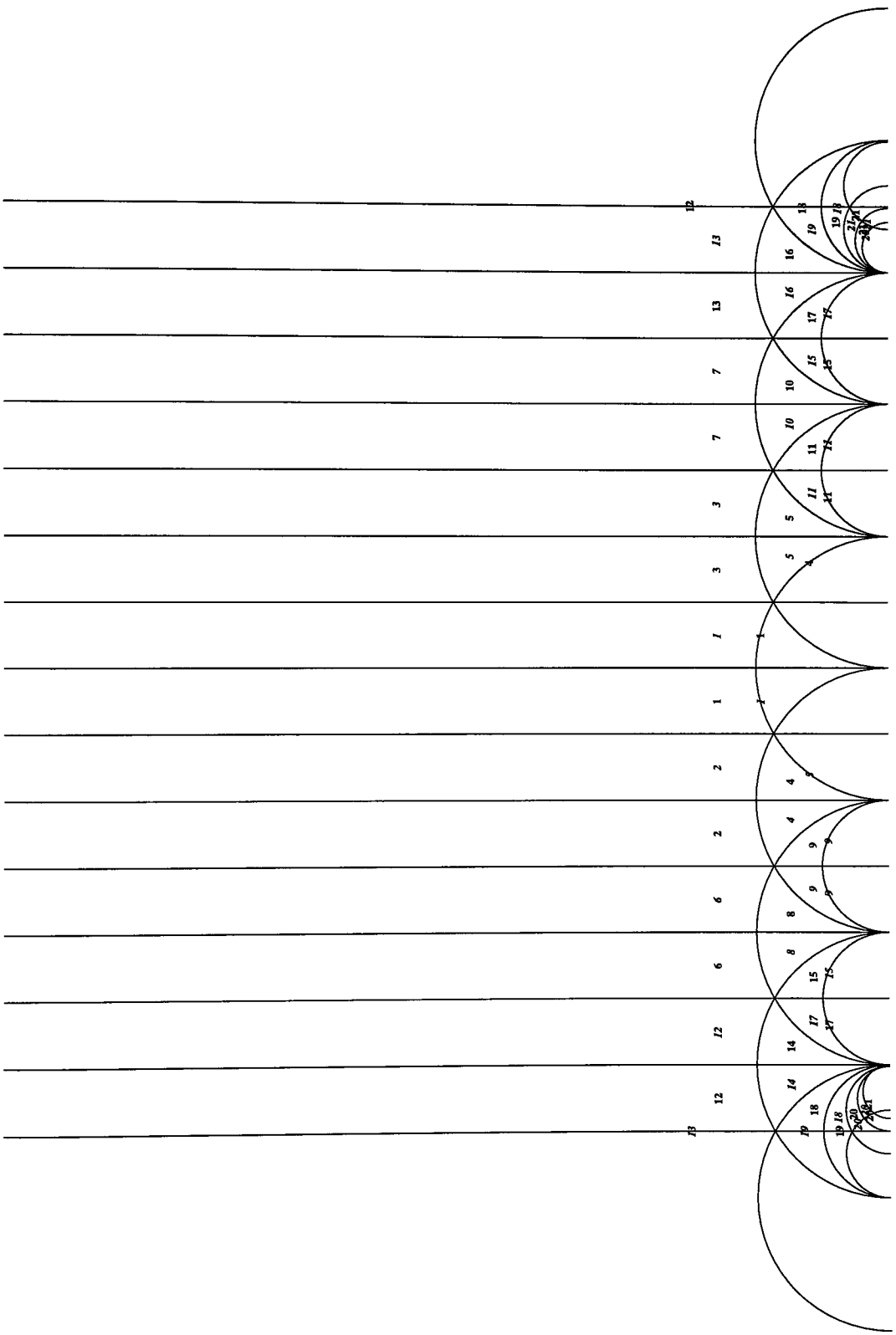


Figure 5.3: Fundamental domain for $X^{+}_{\text{non-split}}(7)$

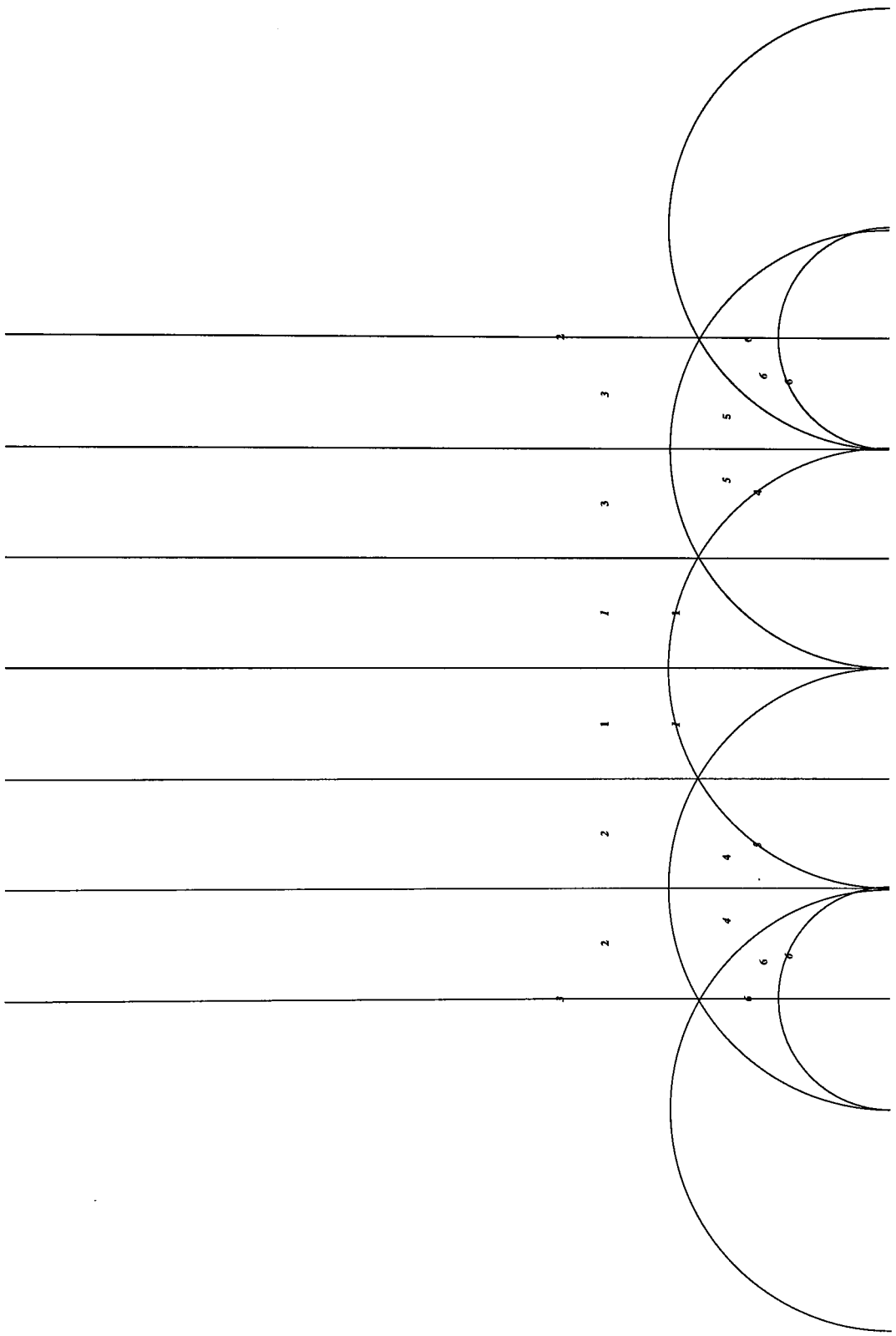


Figure 5.4: Fundamental domain for $X_{\text{non-split}}(3)$ and $X^{+}_{\text{split}}(3)$

Chapter 6

Conclusion

6.1 Edixhoven's work

The proof given in this thesis of Theorem 1 does not exhibit the isogeny between $J(X^+_{\text{non-split}}(p))$ and $J(X_0^+(p^2))^{\text{new}}$ in a concrete way. A description of Hecke actions on the reduction of the modular curves involved [Edi89] may yield a more geometric explanation [Edi94] of the phenomenon. Recently however, Edixhoven [Edi95] following up [Edi94] has given a more enlightening proof of the results in this thesis which is based on the representation theory of $\mathrm{GL}_2(\mathbb{F}_p)$. His proof in principle gives the isogeny in question explicitly, though it would still be interesting to pursue this in more detail.

The starting point for his proof is the fact that $X(p)$ covers both $X^+_{\text{non-split}}(p)$ and $X^+_{\text{split}}(p)$ and has an action of $G = \mathrm{GL}_2(\mathbb{F}_p)$. We work in the category of abelian varieties defined over $\mathbb{Q}$ up to isogeny. For two isogeny classes $\widetilde{A}, \widetilde{B}$ we let $\mathrm{Hom}(\widetilde{A}, \widetilde{B}) = \mathrm{Hom}(A, B) \otimes \mathbb{Q}$. If e is an idempotent in $\mathrm{End}(\widetilde{A})$, then e has a kernel and image by Poincaré reducibility and we have $\widetilde{A} \sim \ker(e) \times \mathrm{im}(e)$. In this category, each object is naturally a $\mathbb{Q}$-module.

By the G-action on $J(X(p))$, one obtains a representation

$$\rho : G \to \mathrm{Aut}(\widetilde{J(X(p))}). \tag{6.1}$$

This yields a representation of the associated group algebra $\mathbb{Q}[G]$

$$\rho : \mathbb{Q}[G] \to \mathrm{End}(\widetilde{J(X(p))}). \tag{6.2}$$

By the representation ρ, idempotents in $\mathbb{Q}[G]$ give a product decomposition of $\widetilde{J(X(p))}$. For instance, if H is a subgroup of G, then the element

$$\mathrm{pr}_H = \frac{1}{|H|} \sum_{h \in H} h \tag{6.3}$$

is an idempotent in $\mathbb{Q}[G]$. One sees that $\widetilde{J(X(p))}$ decomposes into $\ker(\rho(\mathrm{pr}_H)) \times \mathrm{im}(\rho(\mathrm{pr}_H)) \sim \widetilde{J'} \times \widetilde{J(X_H(p))}$, where $J(X_H(p))$ is the jacobian of $X_H(p)$ and

J' is the complementary abelian variety given by Poincaré reducibility. In particular, $\rho(\mathrm{pr}_G)$ has trivial image since $J(X_G(p)) = J(X(1)) = 0$. Thus, the representation ρ factors through $\overline{\mathbb{Q}[G]} = \mathbb{Q}[G]/(\mathrm{pr}_G)$. Consequently, if $H \cdot H' = G$, then the element $\overline{\mathrm{pr}_H} + \overline{\mathrm{pr}_{H'}}$ is also an idempotent in $\overline{\mathbb{Q}[G]}$. Also, note that two idempotents in $\overline{\mathbb{Q}[G]}$ which are $\overline{\mathbb{Q}[G]}^\times$-conjugate have isomorphic kernels and hence give the same product decomposition of $\widetilde{J(X(p))}$.

The key point in Edixhoven's proof is to show that $\overline{\mathrm{pr}_{N'}} + \overline{\mathrm{pr}_B}$ is $\overline{\mathbb{Q}[G]}^\times$-conjugate to $\overline{\mathrm{pr}_N}$. These two elements are idempotents in $\overline{\mathbb{Q}[G]}$ so the relation above induces a $\mathbb{Q}$-isogeny

$$\widetilde{J(X^+_{\text{non-split}}(p))} \times \widetilde{J(X_0(p))} \sim_{\mathbb{Q}} \widetilde{J(X^+_{\text{split}}(p))}. \tag{6.4}$$

The method for proving that the two idempotents above are $\overline{\mathbb{Q}[G]}^\times$-conjugate is to show they have the same rank (i.e. their images are of the same dimension) in every irreducible factor. This is done using the character table of $G = \mathrm{GL}_2(\mathbb{F}_p)$ and a case by case verification. In each irreducible factor, two idempotents of the same rank are conjugate, so we obtain the desired result.

One can interpret Edixhoven's argument in terms of modular forms. To do this, we work in the category of abelian varieties defined over $\mathbb{C}$ up to isogeny. Consider fibre $X(p)_\sigma/\mathrm{Spec}(\mathbb{C})$ of $X(p)/\mu(p)$ along a morphism $\sigma : \mathrm{Spec}(\mathbb{C}) \to \mu(p)$. The finite cover $X(p)_\sigma | X(1)$ has galois group $\mathrm{SL}_2(\mathbb{F}_p)/\{\pm 1\}$. Applying Edixhoven's argument to $G = \mathrm{SL}_2(\mathbb{F}_p)$, the idempotent $\overline{\mathrm{pr}_{SN'}} + \overline{\mathrm{pr}_{SB}}$ is $\overline{\mathbb{Q}[G]}^\times$-conjugate to the idempotent $\overline{\mathrm{pr}_{SN}}$, where SH denotes group $H \cap \mathrm{SL}_2(\mathbb{F}_p)$.

Let $\sum_{g\in G} \alpha_g \cdot g \in \mathbb{Q}[G] \to \overline{\mathbb{Q}[G]}$ be an element which conjugates $\overline{\mathrm{pr}_{SN'}} + \overline{\mathrm{pr}_{SB}}$ to $\overline{\mathrm{pr}_{SN}}$. The isogeny $\phi : J(X_{SN'}(p)_\sigma) \times J(X_{SB}(p)_\sigma) \to J(X_{SN}(p)_\sigma)$ is then explicitly descibed as

$$(z_1, z_2) \mapsto \sum_{g\in G} \alpha_g \cdot g(\iota_1(z_1) + \iota_2(z_2)) \tag{6.5}$$

where $\iota_1 : J(X_{SN'}(p)_\sigma) \to J(X(p)_\sigma)$, $\iota_2 : J(X_{SB}(p)_\sigma) \to J(X(p)_\sigma)$.

Let $\Gamma_1 = \Gamma^+_{\text{non-split}}(p)$ and $\Gamma_2 = \Gamma^+_{\text{split}}(p)$. For an element $g \in G$, let $\overline{g}$ be an element in $\mathrm{SL}_2(\mathbb{Z})$ which reduces mod p to g. The double coset $\Gamma_1 \overline{g} \Gamma_2$ induces a homomorphism from $J(X^+_{\text{non-split}}(p))$ to $J(X^+_{\text{split}}(p))$. In terms of the diagram below, this homomorphism corresponds to the correspondence $T_{\overline{g}} = \pi_{1*} w_{\overline{g}}{}^* \pi_2{}^*$ (see section 1.4).

$$\begin{array}{ccc} X_{\Gamma_2 \cap \overline{g}\Gamma_1\overline{g}^{-1}} & \xrightarrow{w_{\overline{g}}} & X_{\overline{g}^{-1}\Gamma_2\overline{g}\cap\Gamma_1} \\ {\scriptstyle \pi_1}\downarrow & & {\scriptstyle \pi_2}\downarrow \\ X_{\Gamma_2} & & X_{\Gamma_1} \end{array} \tag{6.6}$$

Note that

$$X_{\Gamma_1} \cong_{\mathbb{C}} X_{SN'}(p)_\sigma \tag{6.7}$$
$$X_{\Gamma_2} \cong_{\mathbb{C}} X_{SN}(p)_\sigma \tag{6.8}$$
$$X_{\Gamma_2 \cap \overline{g}\Gamma_1\overline{g}^{-1}} \cong_{\mathbb{C}} X_{\overline{g}^{-1}\Gamma_2\overline{g}\cap\Gamma_1} \tag{6.9}$$
$$\cong_{\mathbb{C}} X(p)_\sigma \tag{6.10}$$

and the map

$$w_{\overline{g}} : X(p)_\sigma \to X(p)_\sigma \tag{6.11}$$
$$z \mapsto \overline{g}^{-1}z \tag{6.12}$$

corresponds to reducing $\overline{g}^{-1}$ modulo p to an element in G and then letting it act on $X(p)_\sigma$.

Consider the injection $\iota : J(X_{SN'}(p)_\sigma) \to J(X_{SN'}(p)_\sigma) \times J(X_{SB}(p)_\sigma)$. By the above discussion, the homomorphism $f \circ \iota : J(X_{SN'}(p)_\sigma) \to J(X_{SN}(p)_\sigma)$ is seen to be the modular correspondence:

$$\sum_{g\in G} \alpha_g \cdot \Gamma_1\overline{g}\Gamma_2. \tag{6.13}$$

In other words, the modular correspondence above moves a modular form on $X^+_{\text{non-split}}(p) \cong_{\mathbb{C}} X_{SN'}(p)_\sigma$ to a modular form on $X^+_{\text{split}}(p) \cong_{\mathbb{C}} X_{SN}(p)_\sigma$ corresponding to the isogeny in question. The image consists precisely of the new forms on $X^+_{\text{split}}(p)$. Similarly, one has a homomorphism in the opposite direction which is surjective and has kernel precisely the old forms on $X^+_{\text{non-split}}(p)$. If f is a newform on $X^+_{\text{split}}(p)$ and if one knew how to obtain the q-coefficients of f at the various cusps of $X^+_{\text{split}}(p)$, then it would be possible to obtain the q-coefficients of the corresponding newform on $X^+_{\text{non-split}}(p)$, provided one knew the element u. This would in principle give the correspondence between the fourier coefficients and eigenvalues of an eigenform on $X^+_{\text{non-split}}(p)$, though the relationship will not be as transparent as in the $\Gamma_0(N)$ case.

6.2 Relation to Shimura curves

One may also ask what other non-trivial relations exist between the jacobians of arithmetic congruence groups. A more mysterious relationship exists in the following case: Let $\Gamma_{p,q}$ be the unit group of a maximal order in the quaternion algebra over $\mathbb{Q}$ which is ramified at precisely two finite primes $p \neq q$. The curve $X_{p,q} = \Gamma_{p,q}\backslash\mathfrak{H}$ has the modular interpretation of classifying abelian surfaces with endomorphism ring containing the order defining $\Gamma_{p,q}$. These Shimura curves do not have cusps and are hence already compact. It is shown in [Shi65] using the trace formula that the zeta function of the new part of the jacobian of $X_0(pq)$ is the same as the zeta function of the jacobian of the curve $X_{p,q}$, so that the corresponding abelian varieties are isogenous by [Rib80].

The Shimura curve $X_{p,q}$ figures in many important guises. On one hand, the isogeny described can be thought of as an example of a geometric realisation of the Langlands' functoriality conjecture. Briefly, this conjecture relates automorphic forms on two different semi-simple reductive algebraic groups G, G': given a L-homomorphism $\rho : G^L \to G'^L$ between the (galois form) L-groups of G and G', one can move an automorphic form from G to G'. In the case of $G = D^\times$ (D a quaternion algebra) and $G' = \mathrm{GL}_2$, the so called Jacquet-Langlands' correspondence characterises the forms on GL_2 which arise from forms on $D^\times$. In our case of interest, this correspondence sends an eigenform on Γ to a eigenform on $\Gamma_0(pq)$ (with the same eigenvalues of Hecke). Furthermore, the forms which actually arise in this manner are the new forms on $\Gamma_0(pq)$. The curve $X_{p,q}$ is also used in Ribet's proof [Rib90] of Shimura-Taniyama-Weil implies Fermat's Last Theorem: to show that a mod l representation ρ which is apriori modular of level Mp is really modular of level M if p is a prime dividing N exactly and ρ is finite at p, one needs to pass to modular forms on this Shimura curve. One already knows by a result of Mazur [Maz85] that if $p \not\equiv 1 \pmod{l}$, then this is true (so without loss of generality we may assume that N is prime to l). The idea is to reduce to this case: Ribet shows that ρ is modular of level Mpq for a suitable auxilliary prime $q \not\equiv 1 \pmod{l}$. Then, using the relationship between modular forms on $\Gamma_0(Mpq)$ and suitable analogue $\Gamma_{p,q}(M)$ of the Shimura curve described above (one needs to add in level M-structure), he shows that ρ is modular of level Mq. This follows from the mysterious Drinfeld switch: in passing from $\Gamma_0(Mpq)$ to $\Gamma_{p,q}(M)$, the primes p and q appear to be switched so that the Hecke action on certain character groups of $J_0(Mpq)$ mod q are equivalent to those of $J_{p,q}(M)$ mod p and vice versa. However, since $q \not\equiv 1 \pmod{l}$, the result of Mazur shows that ρ is modular of level M.

Although the trace formula calculation for $X_{p,q}$ seems to be easier than the one for $X^+_{\text{non-split}}(p)$, this isogeny appears to be more mysterious in the following sense. According to a result of Takeuchi [Tak77], two arithmetic Fuchsian groups Γ_1 and Γ_2 arising from orders in quaternion algebras Q_1 and Q_2 are commensurable if and only if there is an isomorphism between Q_1 and Q_2 satisfying some additional technical conditions. Since $\Gamma_{p,q}$ and $\Gamma_0(pq)$ arise from non-isomorphic quaternion algebras, they are therefore not commensurable. Thus, unlike $X^+_{\text{non-split}}(p)$ and $X^+_{\text{split}}(p)$ which are covered by $X(p)$ finitely, the obvious candidate for a finite cover of $X_{p,q}$ and $X_0(pq)$, namely $\Gamma \cap \Gamma_0(pq)\backslash\mathfrak{H}^*$ does not work. With regard to this, we make the following remark. Formally, a homomorphism of jacobians $\phi : J(C_1) \to J(C_2)$ is induced by the correspondence given by a divisor D on $C_2 \times C_1$. Thus, if a non-trivial homomorphism ϕ exists, a finite cover of both C_1 and C_2 exists. Indeed, if the genus of $X_0(pq)$ is greater than one, then by the classification of Riemann surfaces, we see that it has a model $\Gamma\backslash\mathfrak{H}$ where Γ is a Fuchsian group of the first kind with no elliptic nor parabolic elements. This Fuchsian group Γ is unique up to conjugation by $\mathrm{SL}_2(\mathbb{R})$. By introducing level structures, it is possible to find a subgroup $\Gamma_{p,q}(N)$ of $\Gamma_{p,q}$ which has no elliptic elements (it already lacks parabolic elements). It would seem that a finite cover of $X_{p,q}$ and $X_0(pq)$ is then $\Gamma \cap \Gamma_{p,q}(N)\backslash\mathfrak{H}$. If one

could describe Γ more concretely, it may be possible to generalise Edixhoven's construction to this setting.

6.3 Final remarks

The identification of the jacobian of $X^+_{\text{non-split}}(p)$ up to isogeny as the new part of the jacobian of $X^+_{\text{split}}(p)$ still leaves open several questions and avenues of exploration. One may ask what the kernel of this (minimal) isogeny is.

We have been mainly interested in $X^+_{\text{non-split}}(p)$, but our calculations also show a similar result for the jacobian of $X_{\text{non-split}}(p)$, namely, that it is isogenous to the new part of the jacobian of $X_{\text{split}}(p)$. This follows from the fact that

$$c_p^+(\alpha, \mathfrak{r})[X_{\text{non-split}}(p)] = c_p(\alpha, \mathfrak{r})[X^+_{\text{non-split}}(p)] \tag{6.14}$$

$$c_p^+(\alpha, \mathfrak{r})[X_{\text{split}}(p)] = c_p(\alpha, \mathfrak{r})[X^+_{\text{split}}(p)]. \tag{6.15}$$

This result could have been proved with less effort as $\Gamma = \Gamma_{\text{non-split}}(p), \Gamma_{\text{split}}(p)$ is the unit group of an order in $M_2(\mathbb{Q})$ so the modifications of the trace formula for normaliser extensions of unit groups in 2.2.2 are not necessary. Also, implicit in our calculations is an explicit trace formula for $X_0^+(p^2)$.

The modular curve $X^+_{\text{non-split}}(p)$ does not seem to possess a Hecke operator at p. It would be interesting to investigate this further as well as look into the possibility of a twisting operator [AL70] for $X^+_{\text{non-split}}(p)$.

Finally, one would hope that this description of the jacobian of $X^+_{\text{non-split}}(p)$ will help in the determination of its non-cuspidal rational points. Unfortunately, the relation of jacobians implies that something very different is going on for non-split Cartan modular curves. Indeed, since their jacobians are isogenous to the new part of the jacobians of $X_0^+(p^2)$, their jacobians conjecturally do not have any non-trivial quotients with finite Mordell-Weil group.

Bibliography

[AL70] A.O.L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Mathematische Annalen*, 185:134–160, 1970.

[Bir72] B. Birch. Some calculations of modular relations. In W. Kuyk, editor, *Modular Functions of One Variable I*, number 320 in Lecture Notes in Mathematics, pages 175–186. Springer-Verlag, 1972.

[Bir94] B.J. Birch. Private communication, 1994.

[BK72] B.J. Birch and W. Kuyk, editors. *Modular Functions of One Variable IV*, number 476 in Lecture Notes in Mathematics. Springer-Verlag, 1972.

[BSD72] B.J. Birch and H.P.F. Swinnerton-Dyer. Elliptic curves and modular functions. In B.J. Birch and W. Kuyk, editors, *Modular Functions of One Variable IV*, number 476 in Lecture Notes in Mathematics, pages 2–32. Springer-Verlag, 1972.

[BT92] P. Bayer and T. Travesa, editors. *Corbes Modulars: Taules*, Notes del Seminari Teoria de Nombres, Barcelona, 1992.

[Che94] I. Chen. Personal notes, 1994.

[Coh82] P.M. Cohn. *Algebra.* John Wiley & Sons, 1982.

[Dar93] H. Darmon. The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$. *International Mathematics Research Notices*, pages 263–273, 1993.

[DR72] P. Deligne and M. Rappoport. Les schémas de modules de courbes elliptiques. In P. Deligne and W. Kuyk, editors, *Modular Functions of One Variable II*, number 349 in Lecture Notes in Mathematics, pages 143–316. Springer-Verlag, 1972.

[Edi89] S.J. Edixhoven. *Stable models of modular curves and applications.* PhD thesis, University of Utrecht, 1989.

[Edi94] S.J. Edixhoven. Private communication with B.J. Birch, 1994.

[Edi95] S.J. Edixhoven. On a result of Imin Chen. Preprint, 1995.

[Eic57] M. Eichler. Eine verallgemeinerung der abelschen integrale. *Mathematische Zeitschrift*, 67:267–298, 1957.

[Eic72] M. Eichler. The basis problem for modular forms and the traces of Hecke operators. In *Modular Functions of One Variable I*, number 320 in Lecture Notes in Mathematics, pages 75–152. Springer-Verlag, 1972.

[Fal86] G. Faltings. Finiteness theorems for abelian varieties. In G. Cornell and J. Silverman, editors, *Arithmetic Geometry*. Springer-Verlag, 1986.

[Gir71] J. Giraud. *Cohomologie non abélienne*. Springer-Verlag, 1971.

[Gro80] B. Gross. *Arithmetic on Elliptic Curves with Complex Multiplication*. Number 776 in Lecture Notes in Mathematics. Springer-Verlag, 1980.

[Hij74] H. Hijikata. Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$. *Journal of the Mathematical Society of Japan*, 26(1):57–82, 1974.

[Igu68] J. Igusa. On the algebraic theory of elliptic modular functions. *Journal of the Mathematical Society of Japan*, 20:96–106, 1968.

[Ish73] H. Ishikawa. On the trace formula for Hecke operators. *Journal of the Faculty of Science of the University of Tokyo*, 20:217–238, 1973.

[KM85] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985.

[Lig77] G. Ligozat. Courbes modulaires de niveau 11. In J.P. Serre and D.B. Zagier, editors, *Modular Functions of One Variable V*, number 601 in Lecture Notes in Mathematics, pages 149–237. Springer-Verlag, 1977.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *I.H.E.S. Publications Mathématiques*, 47:33–186, 1977.

[Maz78] B. Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978.

[Maz85] B. Mazur. Letter to J-F. Mestre, 16 August 1985.

[Miy89] T. Miyake. *Modular Forms*. Springer-Verlag, 1989.

[Mom84] F. Momose. Rational points on the modular curves $X_{\text{split}}(p)$. *Compositio Mathematica*, 52:115–137, 1984.

[Mum94] Mumford D., Fogarty J., and Kirwan F. *Geometric Invariant Theory*. Number 34 in A Series of Modern surveys in Mathematics. Springer-Verlag, 3 edition, 1994.

[MW84] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbb{Q}$. *Inventiones Mathematicae*, 76:179–330, 1984.

[MW93] D.W. Masser and G. Wüstholz. Galois properties of division fields of elliptic curves. *Bulletin of the London Mathematical Society*, 25:247–254, 1993.

[Rib80] K. Ribet. Sur les variétés abéliennes à multiplications réelles. *Comptes Rendus de l'Académie des Sciences de Paris*, 291:121–123, 1980. Série A.

[Rib90] K. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ arising from modular forms. *Inventiones mathematicae*, 100:431–476, 1990.

[Sai71] H. Saito. On Eichler's trace formula. *Journal of the Mathematical Society of Japan*, 24(2):333–340, 1971.

[Ser72] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15:259–331, 1972.

[Shi65] H. Shimizu. On zeta functions of quaternion algebras. *Annals of Mathematics*, 81:166–193, 1965.

[Shi71] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Iwanami Shoten, Publishers and Princeton University Press, 1971.

[SR95] A. Silverberg and K. Rubin. Mod p representations of elliptic curves. In J. Coates and S.T. Yau, editors, *Elliptic Curves, Modular Forms, and Fermat's Last Theorem*, volume I of *Series in Number Theory*, pages 148–161. International Press, 1995.

[Tak77] K. Takeuchi. Commensurability classes of arithmetic triangle groups. *Journal of the Faculty of Science of the University of Tokyo*, 24(1):201–212, 1977.

[Wei48] A. Weil. *Variétés abéliennes et courbes algébrique.* Number 1064 in Actualités Scientifiques et Industrielles. Hermann & Associés Editeurs, 1948.

[Wil95] A. Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995.