THE JACOBIANS OF NON-SPLIT CARTAN MODULAR CURVES

IMIN CHEN

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 or non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, if it is irreducible. Such a mod p representation is called split or non-split *dihedral*, respectively. Conversely, one may ask whether these are the only elliptic curves over $\mathbb{Q}$ with dihedral mod p representation (see [25], 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 dihedral and non-split dihedral mod p representation, respectively, 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 dihedral and non-split dihedral mod p representation, respectively [7]. 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 the genus of $X^+_{\text{split}}(p)$ or $X^+_{\text{non-split}}(p)$ is zero, then it has infinitely many $\mathbb{Q}$-rational points. Thus, this question has a negative answer in case of genus zero, 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 [3] and that its Mordell-Weil group has rank one. Thus, there are infinitely many elliptic curves over $\mathbb{Q}$, non-isomorphic over $\overline{\mathbb{Q}}$, 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 to occur for small values of p. Indeed, in [25], 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 [18] [19] can be used to tackle this problem in the split case. In [21], some progress has been made in this direction. However, Mazur states in [18] that the non-split case does not seem to be approachable 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 $X^+_0(p^2)$.*

Date: 6 July 1996.

1991 *Mathematics Subject Classification.* Primary 11G18; Secondary 11F72.

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,*

$$tr(T_n \mid S_2(\Gamma^+_{non\text{-}split}(p))) = tr(T_n \mid S_2(\Gamma^+_0(p^2))^{new}) \tag{1}$$

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 [11].

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 $\mathbb{Q}$ [13]. 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 following genus calculations by the author, 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 recently come to the attention of the author that there are references in the literature to the modular curve $X^+_{\text{non-split}}(p)$. Gross in [12] p. 66 quotes [17] and states that Ligozat observes the isogeny in Theorem 1. Also, Darmon in [6] states that Elkies observes a variant of the isogeny in question.

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 [28] 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 [6] [23].

2. Acknowledgements

I would like to thank my supervisor Prof. B.J. Birch for bringing this problem to my attention and for many useful discussions during the development of this paper. Also, I would like to thank Dr. D.L. Reed for pointing out the phenomenon described in [22].

3. 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 $M_2(\mathbb{F}_p)$:

$$\theta_\lambda = \begin{pmatrix} 0 & 1 \\ \lambda & 0 \end{pmatrix}. \tag{2}$$

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 3.1. *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 or a split Cartan subgroup, accordingly as $\left(\frac{\lambda}{p}\right) = -1, 0$ or 1.*

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

Lemma 3.2. *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 or the normaliser of a split Cartan subgroup, accordingly as $\left(\frac{\lambda}{p}\right) = -1, 0$ or 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 [25]).

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 a curve 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:

$$\Gamma^+_{\text{non-split},\lambda}(p) = \Gamma_{N'_\lambda(p)}(p) \tag{3}$$

$$X^+_{\text{non-split},\lambda}(p) = \Gamma^+_{\text{non-split},\lambda}(p)\backslash\mathfrak{H}^* \tag{4}$$

$$\Gamma^+_{\text{split}}(p) = \Gamma_{N(p)}(p) \tag{5}$$

$$X^+_{\text{split}}(p) = \Gamma^+_{\text{split}}(p)\backslash\mathfrak{H}^*. \tag{6}$$

We call $X^+_{\text{non-split},\lambda}(p)$ and $X^+_{\text{split}}(p)$ *Cartan modular curves*. The choice of quadratic non-residue λ in (3) 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, using either classical methods or the trace formula, to be

$$g^+_{\text{split}}(p) = \frac{1}{24}(p^2 - 8p + 11 - 4\left(\frac{-3}{p}\right)) \tag{7}$$

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

Also, in [2] 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 to be given in a straightforward way.

4. 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.

Definition 4.1. *Let B be an indefinite quaternion algebra over $\mathbb{Q}$. Suppose $\Gamma^0_{\mathbb{A}}$ is an open compact subgroup of $B^{\times,0}_{\mathbb{A}}$, the finite ideles of B. Let $\Gamma = B^\times \cap (B^{\times,+}_\infty \times \Gamma^0_{\mathbb{A}})$. We call Γ an arithmetic congruence group.*

Remark 4.2. *We note that it is possible for an arithmetic congruence group Γ to arise from different open compact subgroups of $B^{\times,0}_{\mathbb{A}}$. However, it will usually be clear from the context which open compact subgroup we are taking, so we will suppress this dependence.*

Lemma 4.3. *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. This follows from a description of the open compact subgroups of $B^{\times,0}_{\mathbb{A}}$. □

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 4.3 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 [20]), it follows that Γ is a Fuchsian group of the first kind.

Definition 4.4. *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. We define the level of Γ to be $N = \prod_{v\in P} v$ (this is well-defined as P is a finite set).*

Lemma 4.5. *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 $v \mid N$.*

For later reference, we quote the important

Theorem 4.6. *(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*

$$B_{\mathbb{A}}^\times = B^\times \cdot (B_\infty^{\times,+} \times \prod_{v\neq\infty} \Gamma_v). \tag{9}$$

Proof. The proof of Theorem 5.2.11 in [20] for $\Gamma_{\mathbb{A}}^0 = R_{\mathbb{A}}^{\times,0}$ also works for a general compact open subgroup. □

Definition 4.7. *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.*

4.1. **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, Γ is the unit group Γ_R of R (as the units of R have norm ± 1).

(ii) 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 that $R_{\text{non-split},\lambda}(p)$ 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 3.

Let $\Gamma_{\mathbb{A}}^0 = \prod_{v\neq\infty} R_v^\times \cup \omega R_v^\times$ where $\omega = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Then $\Gamma_{\mathbb{A}}^0$ is an open compact subgroup of $B_{\mathbb{A}}^0$ so that $\Gamma = B^\times \cap B_\infty^{\times,+} \times \Gamma_{\mathbb{A}}^0$ is an arithmetic congruence group of level p which is in fact the group $\Gamma_{\text{non-split},\lambda}^+(p)$ given in section 3.

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

Lemma 4.8. *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 [27]. □

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 $\Gamma_v = S_v^\times$ where S_v is a maximal order in $B_v \cong M_2(\mathbb{Q}_v)$. Now, $S_v = \alpha_v^{-1} M_2(\mathbb{Z}_v)\alpha_v$ 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:

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

By Theorem 4.6, 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 4.5). 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 4.9. *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.*

5. 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 [20]). There are natural linear operators $\Gamma\delta\Gamma$ which act on $S_k(\Gamma)$. The Selberg trace formula can be used to calculate the traces of these operators and in this particular context, it reads:

Theorem 5.1. *Let Γ be a Fuchsian group of the first kind and let $\Gamma\delta\Gamma$ be a double coset operator. Then*

$$tr(\Gamma\delta\Gamma \mid S_k(\Gamma)) = |Z(\Gamma)|^{-1} \int_{\Gamma\backslash\mathfrak{H}} \sum_{\alpha\in\Gamma\delta\Gamma} \kappa(z;\alpha) dv(z) \tag{10}$$

where

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

Proof. See the proof of Theorem 6.4.2 in [20]. □

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 [9] [10] 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 4). 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 [20] for unit groups of orders in quaternion algebras over $\mathbb{Q}$.

5.1. **Integral calculation for Fuchsian groups of the first kind.**

Theorem 5.2. *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 5.3. *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:

$$tr(\Gamma\delta\Gamma \mid S_k(\Gamma)) = t^{\Sigma} + \delta(k) \tag{11}$$

$$t^{\Sigma} = -\lim_{s\to 0^+} \sum_{\alpha\in\Gamma\delta\Gamma//\Gamma} k(\alpha)l(\alpha) \tag{12}$$

$$\delta(k) = \begin{cases} deg(\Gamma\delta\Gamma) & \text{if } k = 2 \\ 0 & \text{otherwise} \end{cases} \tag{13}$$

$$k(\alpha) = \begin{cases} \frac{k-1}{4\pi} v(\Gamma\backslash\mathfrak{H}) sgn(\alpha)^k det(\alpha)^{k/2-1} & \text{if } \alpha \in \Gamma\delta\Gamma^o \\ \frac{\eta_\alpha^{k-1} - \zeta_\alpha^{k-1}}{\eta_\alpha - \zeta_\alpha} & \text{if } \alpha \in \Gamma\delta\Gamma^e \\ sgn(\zeta_\alpha)^k \frac{min(|\zeta_\alpha|,|\eta_\alpha|)^{k-1}}{|\zeta_\alpha - \eta_\alpha|} & \text{if } \alpha \in \Gamma\delta\Gamma^{h,c} \\ \frac{s}{4} sgn(\zeta_\alpha)^k det(\alpha)^{k/2-1} & \text{if } \alpha \in \Gamma\delta\Gamma^{p,c} \end{cases} \tag{14}$$

$$l(\alpha) = \begin{cases} 1/|Z(\Gamma)| & \text{if } \alpha \in \Gamma\delta\Gamma^o \\ 1/2\,|\Gamma(\alpha)| & \text{if } \alpha \in \Gamma\delta\Gamma^e \\ 1/|Z(\Gamma)| & \text{if } \alpha \in \Gamma\delta\Gamma^{h,c} \\ 1/|Z(\Gamma)|\,|m(\alpha)|^{s+1} & \text{if } \alpha \in \Gamma\delta\Gamma^{p,c} \end{cases} \tag{15}$$

where

$$\begin{aligned} \Gamma\delta\Gamma//\Gamma &= \text{elements of } \Gamma\delta\Gamma \text{ up to conjugation by } \Gamma \\ \Gamma\delta\Gamma^o &= \text{scalar elements of } \Gamma\delta\Gamma \\ \Gamma\delta\Gamma^e &= \text{elliptic elements of } \Gamma\delta\Gamma \\ \Gamma\delta\Gamma^{h,c} &= \text{hyperbolic cuspidal elements of } \Gamma\delta\Gamma \\ \Gamma\delta\Gamma^{p,c} &= \text{parabolic cuspidal elements of } \Gamma\delta\Gamma \\ v(\Gamma\backslash\mathfrak{H}) &= \text{volume of } \Gamma\backslash\mathfrak{H} \end{aligned}$$

$$\begin{aligned}\zeta_\alpha, \eta_\alpha &= \text{eigenvalues of } \alpha \text{ in any order and not necessarily distinct}\\ \operatorname{sgn}(\alpha) &= \operatorname{sgn}(\zeta_\alpha) \text{ (this is well-defined if } \alpha \text{ is not elliptic)}\\ \Gamma(\alpha) &= \text{those elements in } \Gamma \text{ which centralise } \alpha\\ m(\alpha) &= \text{a number which depends on } \alpha//\Gamma \text{ to be explained below}\end{aligned}$$

Proof. Refer to Theorem 6.4.10 in [20] for a detailed derivation in the case $k > 2$. For $k = 2$, see the statement in [20] and [13]. A proof can be found in [24], who in turn cites [9] for a derivation in the case which pertains to us. Also, [20] refers to [15] for an alternative proof from [9] based on a certain limiting process. □

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

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

$$\begin{pmatrix}0 & 1\\ -n & t\end{pmatrix} \textit{ where } t, n \in k \textit{ (non-scalar)}$$

Proof. This follows from the Frobenius normal form for $M_2(k)$. See p. 347 of [5]. □

Let g be an element of $\mathrm{GL}_2(\mathbb{R})^+$. We say that g is scalar or non-scalar according to its type as an element of $M_2(\mathbb{R})$ as given by the above lemma. Furthermore, if g is non-scalar, we say g is elliptic, parabolic, hyperbolic if $t^2 - 4n$ is negative, zero, positive, respectively.

Definition 5.5. *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 5.6. *Suppose that α is elliptic or 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 or 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 or parabolic. This subgroup is abelian 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 5.6, $\Gamma(\alpha) = \Gamma_z$. Let $\sigma \in \mathrm{SL}_2(\mathbb{R})$ be 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

$$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \tag{16}$$

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

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. As for $l(\alpha)$, we have the following Lemma.

Lemma 5.7. *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 5.2). 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:

$$\mathrm{tr}(\Gamma\delta\Gamma \mid S_2(X_\Gamma)) = t^\Sigma + \deg(\Gamma\delta\Gamma) \tag{17}$$

$$t^\Sigma = -\lim_{s\to 0^+} \sum_{\alpha \in \Gamma\delta\Gamma//\Gamma} k(\alpha)l(\alpha) \tag{18}$$

$$k(\alpha) = \begin{cases} \frac{1}{4\pi} v(\Gamma\backslash\mathfrak{H}) & \text{if } \alpha \in \Gamma\delta\Gamma^o \\ 1 & \text{if } \alpha \in \Gamma\delta\Gamma^e \\ \frac{\min(|\zeta_\alpha|, |\eta_\alpha|)}{|\zeta_\alpha - \eta_\alpha|} & \text{if } \alpha \in \Gamma\delta\Gamma^{h,c} \\ \frac{s}{4} & \text{if } \alpha \in \Gamma\delta\Gamma^{p,c} \end{cases} \tag{19}$$

$$l(\alpha) = \begin{cases} 1/|Z(\Gamma)| & \text{if } \alpha \in \Gamma\delta\Gamma^o \\ 1/2\,|\Gamma(\alpha)| & \text{if } \alpha \in \Gamma\delta\Gamma^e \\ 1/|Z(\Gamma)| & \text{if } \alpha \in \Gamma\delta\Gamma^{h,c} \\ 1/|Z(\Gamma)|\,|m(\alpha)|^{s+1} & \text{if } \alpha \in \Gamma\delta\Gamma^{p,c} \end{cases} \tag{20}$$

5.2. **Algebraic calculation for arithmetic congruence groups.** In this section, we consider the trace formula in Theorem 5.2 for Hecke operators T_n on strong arithmetic congruence groups Γ. The trace formula in Theorem 5.2 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 5.8. *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 5.9. *Let K be a quadratic algebra over $\mathbb{Q}$. Then K is isomorphic to one of the following:*

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

Corollary 5.10. *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 5.4).

Lemma 5.11. *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).*

Lemma 5.12. *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 [20] 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 5.13. *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 [20]. □

The trace formula in terms of B. We now follow the algebraic calculation given in [20] with some modifications to obtain an explicit formula for the traces of Hecke operators for the class of strong arithmetic congruence groups which satisfy condition (5.8). To make explicit the assumptions used in this algebraic calculation, we list them below.

Condition 5.14. (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 4.5).*
(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 section 6 for $\Gamma^+_{\text{non-split}}(p)$, $\Gamma^+_{\text{split}}(p)$, $\Gamma_0(p)$, $\Gamma(1)$, even though the levels differ.

In section 5.1, 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

$$C(\alpha) = \{\delta \alpha \delta^{-1} \mid \delta \in B^\times\}. \tag{21}$$

Let S_n denote the elements in S with reduce norm n. By remark 4.9, $T_n \subset S_n$. 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

$$C(\alpha, \mathfrak{r}) = \left\{\delta \alpha \delta^{-1} \mid \delta \in B^\times, \mathbb{Q}[\alpha] \cap \delta^{-1} R \delta = \mathfrak{r}\right\}. \tag{22}$$

Since $\mathbb{Q}[\alpha] \cap \delta^{-1} R \delta$ is an order in $\mathbb{Q}[\alpha]$ for any $\delta \in B^\times$, we have $C(\alpha) = \bigcup_{\mathfrak{r}} C(\alpha, \mathfrak{r})$. 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 (5.14).

Lemma 5.15. *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 $\beta \in S$ 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 5.16. *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 (5.19). 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:

$$\sum_{\alpha \in S_n//B^\times} k(\alpha) \sum_{\beta \in (T_n \cap C(\alpha))//\Gamma} l(\beta) = \sum_{\alpha \in S_n//B^\times} k(\alpha) \sum_{\mathfrak{r} \supset \mathbb{Z}[M\alpha]} l(\mathfrak{r}) \cdot |(T_n \cap C(\alpha, \mathfrak{r}))//\Gamma| \,. \tag{23}$$

Lemma 5.17. *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 5.7.

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

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

since one knows that the elements in B which commute with β are precisely the elements in $\mathbb{Q}[\beta]$ (see Lemma 5.13).

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 the 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 $m = \pm 1$. 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 5.7, $l(\beta) = l(\beta')$. □

Remark 5.18. *The main point of Lemma 5.17 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 6.3).*

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 6.6.

Since an arithmetic congruence group satisfies condition (5.3), we have therefore shown

Proposition 5.19. *Under the hypotheses and definitions of* (5.14) *and Theorem 5.1 we have*

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

The trace formula in terms of $B_{\mathbb{A}}$. In this section, we work in the same situation outlined in (5.14). 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

$$\mathfrak{r}_v = \mathfrak{r} \otimes_{\mathbb{Z}} \mathbb{Z}_v \tag{24}$$

$$C_v(\alpha) = \left\{\delta\alpha\delta^{-1} \mid \delta \in B_v^{\times}\right\} \tag{25}$$

$$C_v(\alpha, \mathfrak{r}) = \left\{\delta\alpha\delta^{-1} \mid \delta \in B_v^{\times}, \mathbb{Q}_v[\alpha] \cap \delta^{-1} R_v \delta = \mathfrak{r}_v\right\} \tag{26}$$

where by convention we set $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$ and correspondingly with v replaced by $\mathbb{A}$. We also define

$$\Gamma_{\mathbb{A}} = B_{\infty}^{\times,+} \times \Gamma_{\mathbb{A}}^0. \tag{27}$$

Lemma 5.20. (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 $g \in C_{\mathbb{A}}(\alpha, \mathfrak{r})$, $\left|\theta^{-1}(g//\Gamma_{\mathbb{A}})\right| = h^+(\mathfrak{r})$ where*

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

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 [20].

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 (5.14) 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 5.13). 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

$$\Gamma\gamma_1 x_1 E \cap B^\times = \Gamma\gamma_2 x_2 E \cap B^\times \iff x_1 x_2^{-1} \in (E \cap \Gamma_{\mathbb{A}}) \cdot (E \cap B^\times).$$

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, $\left|\theta^{-1}(g)\right| = h^+(\mathfrak{r}) = h(\mathfrak{r})/w(\mathfrak{r})$ where

$$w(\mathfrak{r}) = [\mathbb{Q}_{\mathbb{A}}[\alpha] \cap \delta^{-1}\Gamma_{\mathbb{A}}\delta : \mathfrak{r}_{\mathbb{A}}^{\times,+}]. \tag{28}$$

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,

$$w(\mathfrak{r}) = \prod_{v|N} [\mathbb{Q}_v[\alpha] \cap \delta^{-1}\Gamma_v\delta : \mathfrak{r}_v^\times] \leq \prod_{v|N} [\Gamma_v : R_v^\times]. \tag{29}$$

□

Lemma 5.21. *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 $\left|\theta^{-1}(g)\right| = h^+(\mathfrak{r})$ 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 5.20, there exists a $g' \in C(\alpha)$ 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 that 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 (see proof of previous lemma). □

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 5.21, 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

$$\sum_{\alpha\in S_n//\Gamma} k(\alpha)l(\alpha) = \sum_{\alpha\in S_n//B^\times} k(\alpha) \sum_{\mathfrak{r}\supset\mathbb{Z}[M\alpha]} l(\mathfrak{r})h^+(\mathfrak{r}) \cdot \prod_v |((T_n)_v \cap C_v(\alpha,\mathfrak{r}))//\Gamma_v| \tag{30}$$

and we obtain

Proposition 5.22. *Under the hypotheses and definitions of* (5.14) *and Theorem 5.1, we have*

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

6. Calculation for Cartan modular curves

In this section, we calculate an explicit trace formula for Hecke operators $T = T_n$ on $\Gamma = \Gamma^+_{\text{non-split},\lambda}(p)$ and $\Gamma^+_{\text{split}}(p)$. According to the algebraic calculation given in section 5.2, an explicit determination of the trace formula for Γ in the form of (5.22) 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 [13] 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 adapt his calculation to the cases $\Gamma = \Gamma^+_{\text{non-split},\lambda}(p)$ and $\Gamma = \Gamma^+_{\text{split}}(p)$. The method is based on Miyake's [20] detailed exposition of Hijikata's work.

To fix notation for the rest of the section, let

(i) p be an odd prime
(ii) $B = M_2(\mathbb{Q})$
(iii) $\Gamma = \Gamma^+_{\text{non-split},\lambda}(p), \Gamma^+_{\text{split}}(p), \Gamma_0(p)$ or $\Gamma(1)$
(iv) $R = R_{\text{non-split},\lambda}(p), R_{\text{split}}(p), R_0(p)$ or $R(1)$
(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 4.1, we see that the hypotheses of (5.14) are satisfied so that the form of the trace formula given in (5.22) is valid for Γ. In the context above, $N' = N = M = p$ for $\Gamma^+_{\text{non-split},\lambda}(p)$, $\Gamma^+_{\text{split}}(p)$ or $\Gamma_0(p)$, and $N' = 1$ divides $N = M = p$ for $\Gamma(1)$.

Lemma 6.1. *Suppose $v \neq p$. Then*

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

Proof. For $v \neq p, \infty$, $\Gamma_v = R_v$ is conjugate to the maximal order $M_2(\mathbb{Z}_v)$ so by Theorem 6.6.7 of [20], $c_v^+(\alpha,\mathfrak{r}) = 1$. For $v = \infty$, see calculation (6.6.1) in [20]. □

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

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

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 compare 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 6.3. *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*

$$h^+(\mathfrak{r}) = \begin{cases} h(\mathfrak{r}) & \text{if } \mathfrak{r}_p \supset \mathbb{Z}_p[\alpha] \\ h(\mathfrak{r})/2 & \text{if } \mathfrak{r}_p = \mathbb{Z}_p[p\alpha]. \end{cases} \tag{31}$$

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 5.20. If in that lemma, we take $g = \beta$, then the δ above corresponds to a choice of δ in its proof. Therefore, it suffices to show that $[\mathbb{Q}_p[\alpha] \cap \delta^{-1}\Gamma_p\delta : \mathbb{Q}_p[\alpha] \cap \delta^{-1}R_p^\times\delta] = 1, 2$ according 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 6.2 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 6.2 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, $w(\mathfrak{r}) = 2$. □

6.1. **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 form a complete set of representatives.

First define

(32)

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

Lemma 6.4. *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 [20].) 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 6.5. *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. We have

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

where the last equivalence follows from Lemma 6.4 as applied to $p\alpha$. □

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

$$g_{\xi,u} = \xi + p^\rho \begin{pmatrix} 0 & u \\ \bar{n}(\xi)/u & \bar{t}(\xi) \end{pmatrix} \tag{33}$$

where

$$\bar{n}(\xi) = -f(\xi)/p^{2\rho} \tag{34}$$

$$\bar{t}(\xi) = (t - 2\xi)/p^\rho \tag{35}$$

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

$$r_{\xi,u} = \begin{pmatrix} 0 & u \\ \bar{n}(\xi)/u & \bar{t}(\xi) \end{pmatrix} \tag{36}$$

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 6.4.

6.2. **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 the calculations to follow.

Lemma 6.6. *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*

$$t - 2\xi \equiv 0 \pmod{p^{\lceil \epsilon/2 \rceil}} \iff \Delta(f) \equiv 0 \pmod{p^\epsilon}. \tag{37}$$

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

Lemma 6.7. *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 of* $f(x) \equiv 0 \pmod{p^\epsilon}$ *modulo* p^ν *is given by*

$$r_p(\nu, \delta, \epsilon, d) = \begin{cases} p^{\nu - \lceil \epsilon/2 \rceil} & \delta \geq \epsilon \\ 0 & \delta < \epsilon \text{ and } \delta \text{ odd} \\ \left[\frac{d}{p^{\epsilon-\delta}}\right] p^{\nu-(\epsilon-\delta/2)} & \delta < \epsilon \text{ and } \delta \text{ even} \end{cases} \tag{38}$$

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 6.8. *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*

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

Proof. This is a routine calculation. □

Lemma 6.9. *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 $\left[\frac{d}{p^e}\right]$ and $r(\alpha,\beta)$ are as in Lemma 6.7, Lemma 6.8, respectively.

Proof. This is a routine calculation. □

6.3. **The case of non-split Cartan modular curves.** 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

$$\begin{aligned} u &= p^\delta w \\ \delta &= 0, 1 \\ 0 < w &< p \\ \bar{n}(\xi) &\equiv \lambda u^2 \pmod{p^{1+\delta}} \\ \bar{t}(\xi) &\equiv 0 \pmod{p} \\ \bar{n}(\xi) &\not\equiv \lambda u^2 \pmod{p^{2+\delta}} \text{ or } \bar{t}(\xi) \not\equiv 0 \pmod{p^2} \end{aligned} \tag{39}$$

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 (39) forms a complete set of representatives for $D_p(t,n,\rho)//R_p^\times$.

Lemma 6.10. *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* (39).

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

$$b \not\equiv 0 \pmod{p^{\rho+1}} \tag{40}$$

$$c \not\equiv 0 \pmod{p^{\rho+1}} \tag{41}$$

$$a - d \not\equiv 0 \pmod{p^{\rho+2}} \tag{42}$$

$$(c - \lambda b)/p^{\rho+1} \not\equiv 0 \pmod{p} \tag{43}$$

First suppose that $b \not\equiv 0 \pmod{p^{\rho+2}}$. Rewrite g in 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 $0 \leq \delta \leq 1$. Since $b'' = u + kp^{\nu} = u(1 + \frac{k}{u}p^{\nu})$ for some $0 < u < p$, the 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 (39). 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 (39).

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 $(c - \lambda b)/p^{\rho+1} \not\equiv 0 \pmod{p}$ does not occur for the former conditions (40)–(42) imply $(c - \lambda b)/p^{\rho+1} \equiv 0 \pmod{p}$. □

Having established that the elements $g_{\xi,u}$ form a complete set of 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 6.11. *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 6.12. *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 Lemma 6.11. 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 that this matrix conjugates $g_{\xi,u}$ to $g_{\xi',u'}$. □

Lemma 6.13. *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:

$$a(u'/u - 1) + b((\xi'-\xi)/p^\rho u + \bar{t}(\xi')/u) \equiv 0 \pmod{p} \tag{44}$$

$$a(\xi'-\xi)/p^\rho u + b(\bar{n}(\xi')/uu' - \lambda) \equiv 0 \pmod{p} \tag{45}$$

There exists a non-trivial solution to the system (44), (45) if and only if the determinant of the above linear system is zero. This determinant is easily calculated to be

$$\Xi = {w'}^{-1} w^{-2} \cdot \left\{ (w'-w)(\bar{n}(\xi')/p^2 - \lambda w w') - \epsilon(\epsilon + \bar{t}(\xi')/p) w' \right\} \tag{46}$$

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

$$\Delta(\epsilon) = (\bar{n}(\xi')/p^2 + \lambda {w'}^2)^2 + 4\lambda {w'}^2(\epsilon^2 + \epsilon\bar{t}(\xi')/p - \bar{n}(\xi')/p^2) \tag{47}$$

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 6.14. *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*

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

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 6.2. Hence, we will determine the size of $C_p(\alpha,\mathfrak{r})//R_p^\times$. By Lemma 6.10 and Lemma 6.4, the elements $g_{\xi,u}$ satisfying condition (39) give a complete set of representatives for $C_p(\alpha,\mathfrak{r})//R_p^\times$.

Recall condition (39) and note the following two equivalences

$$\bar{n}(\xi)/u \equiv \lambda u \pmod{p} \iff f(\xi) = \xi^2 - t\xi + (n + p^{2\rho}\lambda u^2) \equiv 0 \pmod{p^{2\rho+1+\delta}} \tag{48}$$

$$\bar{t}(\xi) \equiv 0 \pmod{p} \iff t - 2\xi \equiv 0 \pmod{p^{\rho+1}} \tag{49}$$

where $\delta = v_p(u) = 0, 1$. If ξ, u satisfy these conditions, then by Lemma 6.6, $D \equiv p^{2\rho}\lambda u^2 \pmod{p^{2\rho+1+\delta}}$ and hence $d \equiv \lambda u^2 \pmod{p^{1+\delta}}$.

Assume that $\mu < 2$. If there exist ξ, u satisfying condition (39) 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 (48) 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 6.7. Hence, by Lemma 6.12, $c_p(\alpha, \mathfrak{r}_p) = 2$. If $\left(\frac{d}{p}\right) = 0$ or 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 (39) 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 (48) and (49) 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 6.7. Hence, a priori there are $p(p-1)$ distinct $g_{\xi,pw}$'s by Lemma 6.13. 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 (39)).

Let us first fix a $g_{\xi',pw'}$ satisfying all parts of conditions (39). 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 6.13, $g_{\xi,pw}$ 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 condition (39).

As ϵ varies through $\mathbb{F}_p$, the total number of roots of $\Xi \equiv 0 \pmod{p}$ is $p+1$ by Lemma 6.9. We must be careful however to eliminate any pairs (ξ, w) with $w = 0$ since these are excluded by condition (39). Looking back on the conjugation relation (46), 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 $\left(\frac{d/p^2}{p}\right) = -1, 0$ or 1, the number of (ξ, w) with $w = 0$ is therefore 0,1 or 2, respectively, and hence the orbit size is $p+1$,p or $p-1$, 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 (39)). 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 for the case $\mu < 2$, we see there are 2 such $g_{\xi,pw}$'s if $\left(\frac{D/p^{2\rho+2}}{p}\right) = \left(\frac{d/p^2}{p}\right) = -1$ and none otherwise.

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 (39). 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 (39). 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 6.15. *With the same hypotheses as in Lemma 6.14, we have*

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

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 $g_{\xi,u}$ of $C_p(\alpha,\mathfrak{r})//R_p^\times$ in this case satisfy $u=pw$ where $w=1,\dots,p-1$. From the proof of (6.13), 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

$$\bar{n}(\xi')/p^2 + \lambda {w'}^2 \equiv 0 \pmod p. \tag{50}$$

For each fixed w', condition (50) is a quadratic equation in ξ'. As w' varies through $\mathbb{F}_p$, we see by Lemma 6.9 that the total number of roots of this quadratic equation is $p+1$ if $\left(\frac{d/p^2}{p}\right)=\pm 1$ and 0 otherwise. Now, $w'=0$ causes (50) 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 of this quadratic equation is $p+1$,0 or $p-1$, according as $\left(\frac{d/p^2}{p}\right)=-1,0$ or 1.

We note that any two $g_{\xi,pw}$ satisfying (50) 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 6.5, a determination of $T_p \cap C_p(\alpha,\mathfrak{r})//R_p^\times$ in the case where $\mathfrak{r} = \mathbb{Z}_p[p\alpha]$ 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 6.16. *Let $\alpha\in S_n$. Assume that $\mathfrak{r}_p=\mathbb{Z}_p[p\alpha]$. Put $d=\Delta(\alpha)$. Then*

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

Proof. In this case, $T_p\cap C_p(\alpha,\mathfrak{r}) = (T_\omega)_p \cap C_p(\alpha,\mathfrak{r})$ by Lemma 6.2. By Lemma 6.5, $g\in C_p(\alpha,\mathfrak{r})$ 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 at the beginning of Lemma 6.14, 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 $w=1,\dots,p-1$.

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 of the quadratic equation above is $p+1, 0$ or $p-1$ accordingly as $\left(\frac{d}{p}\right) = -1, 0$ or 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 or $p-1$ according as $\left(\frac{d}{p}\right) = -1, 0$ or 1.

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

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

□

6.4. **The case of split Cartan modular curves.** 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,

$$\begin{aligned} f_\alpha(\xi) &\equiv 0 \pmod{p^{2\rho+2}} \\ t - 2\xi &\equiv 0 \pmod{p^\rho}, \end{aligned} \tag{51}$$

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 6.17. *Let $g \in D_p(t, n, \rho)$. Then g is Γ_p-conjugate to an element g_ξ satisfying* (51).

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 6.10, we see that g is $R_p^\times$-conjugate to some g_ξ satisfying (51).

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 (51) 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 (51) 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 $c \not\equiv 0 \pmod{p^{\rho+2}}$ that we need to conjugate by an element of Γ_p. We therefore obtain the following two lemmas.

Lemma 6.18. *Elements g_ξ and $g_{\xi'}$ are $R_p^\times$-conjugate if and only if $\xi \equiv \xi' \pmod{p^{\rho+2}}$.*

Lemma 6.19. *Elements g_ξ and $\omega g_{\xi'} \omega^{-1}$ are $R_p^\times$-conjugate if and only if*

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

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 6.20. *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*

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

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 6.2. We will determine the size of $C_p(\alpha,\mathfrak{r})//R_p^\times$.

If $\mu < 2$, then by Lemma 6.7 the number of ξ modulo $p^{\rho+2}$ satisfying condition (51) is 0,0 or 2, according as $\left(\frac{d}{p}\right) = -1, 0$ or 1. An element $\omega g_\xi \omega^{-1}$ is not $R_p^\times$-conjugate to some $g_{\xi'}$ if and only if

$$\begin{aligned} f_\alpha(\xi) &\equiv 0 \pmod{p^{2\rho+3}} \\ t-2\xi &\equiv 0 \pmod{p^{\rho+1}} \end{aligned} \tag{52}$$

by Lemma 6.19. There are no such ξ by Lemma 6.7 so that $c_p(\alpha,\mathfrak{r}) = 0, 0$ or 2 according as $\left(\frac{d}{p}\right) = -1, 0$ or 1.

Suppose $\mu \geq 2$. The number of ξ modulo $p^{\rho+2}$ satisfying (51) is p. The number of ξ modulo $p^{\rho+2}$ which satisfy (52) is 0,1 or 2, acccordingly as $\left(\frac{d/p^2}{p}\right) = -1, 0$ or 1. Thus, $c_p(\alpha,\mathfrak{r}) = p, p+1$ or $p+2$ according as $\left(\frac{d/p^2}{p}\right) = -1, 0$ or 1. □

Proposition 6.21. *With the same hypthotheses as in Lemma 6.20, we have*

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

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 52 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

$$\begin{aligned} f_\alpha(\xi) &\not\equiv 0 \pmod{p^{2\rho+3}} \\ t-2\xi &\equiv 0 \pmod{p^{\rho+2}} \end{aligned}. \tag{53}$$

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 (53). If $\mu\geq 3$, then there is one ξ modulo $p^{\rho+2}$ which satisfies

$$\begin{aligned} f_\alpha(\xi) &\equiv 0 \pmod{p^{2\rho+3}} \\ t-2\xi &\equiv 0 \pmod{p^{\rho+2}} \end{aligned}. \tag{54}$$

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

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

Proof. In this case, $T_p\cap C_p(\alpha,\mathfrak{r}) = (T_\omega)_p \cap C_p(\alpha,\mathfrak{r})$ by Lemma 6.2. By Lemma 6.5, $g\in C_p(\alpha,\mathfrak{r})$ 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

$$t\equiv 0 \pmod p \tag{55}$$

$$\xi\equiv 0 \pmod{p^2}. \tag{56}$$

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. □

6.5. **The case of Borel modular curves.** From the table on p. 266 of [20], the local invariants $c_p^+(\alpha, \mathfrak{r})$ for $\Gamma = \Gamma_0(p), \Gamma(1)$ are obtained by the following.

Proposition 6.23. *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*

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

Proposition 6.24. *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 6.25. *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 6.26. *Let $\alpha \in S_n$. Assume that $\mathfrak{r}_p = \mathbb{Z}_p[p\alpha]$. Then*

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

6.6. **Explicit form of the trace formula.** Following [20] section 6.8, we give an numerically computable form of the trace formula in the situation being considered in this section for weight $k = 2$.

We make more explicit the main term t^Σ of the trace formula in the form of (5.22):

$$t^\Sigma = -\lim_{s \to 0^+} \sum_{\alpha \in S_n // B^\times} k(\alpha) \sum_{\mathfrak{r} \supset \mathbb{Z}[M\alpha]} l(\mathfrak{r}) h^+(\mathfrak{r}) \cdot \prod_v c_v^+(\alpha, \mathfrak{r}). \tag{57}$$

By Lemma 5.4, 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 or parabolic-cuspidal accordingly as $\Delta(\alpha) = t^2 - 4n$ is negative, a positive square, a positive non-square or zero. We now consider the inner sum according to the four cases above. Note that $c_\infty^+(\alpha, \mathfrak{r}) = 2, 1$ or 2 accordingly as $\alpha \in T^e, T^{h,c}$, or $T^{p,c}$ and $c_v^+(\alpha, \mathfrak{r}) = 1$ if $v \nmid M$ and $v \neq \infty$ (see Lemma 6.1).

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

$$t^0 = \frac{1}{4\pi} v(\Gamma \backslash \mathfrak{H}^*). \tag{58}$$

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

$$\begin{aligned} t^e &= - \sum_{t \in \mathbb{Z}, t^2 - 4n = m^2 d_K, d_K < 0} k(\alpha) \sum_{f | mM} l(\mathfrak{r}_f) h^+(\mathfrak{r}_f) \cdot 2 \prod_{v | M} c_v^+(\alpha, \mathfrak{r}_f) \\ &= \sum_{t \in \mathbb{Z}, t^2 - 4n = m^2 d_K, d_K < 0} \sum_{f | mM} \frac{h^+(\mathfrak{r}_f)}{\left|\mathfrak{r}_f^\times\right|} \cdot \prod_{v | M} c_v^+(\alpha, \mathfrak{r}_f). \end{aligned} \tag{59}$$

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,

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

so that we have

$$\begin{aligned} t^h &= - \sum_{t \in \mathbb{Z}, t^2 - 4n = m^2} k(\alpha) \sum_{f | mM} l(\mathfrak{r}_f) h^+(\mathfrak{r}_f) \cdot \prod_{v | M} c_v^+(\alpha, \mathfrak{r}_f) \\ &= \sum_{t \in \mathbb{Z}, t^2 - 4n = m^2} \frac{\min(\left|\zeta_\alpha\right|, \left|\eta_\alpha\right|)}{\left|\zeta_\alpha - \eta_\alpha\right|} \sum_{f | mM} \frac{h^+(\mathfrak{r}_f)}{\left|Z(\Gamma)\right|} \cdot \prod_{v | M} c_v^+(\alpha, \mathfrak{r}_f). \end{aligned} \tag{60}$$

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 6.16, 6.22 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

$$t^p = -\lim_{s\to 0^+} \sum_{t\in\mathbb{Z}, t^2-4n=0} k(\alpha) \sum_{l=1}^{\infty} l(\mathfrak{r}^l) h^+(\mathfrak{r}^l) \cdot 2 \prod_{v|M} c_v^+(\alpha, \mathfrak{r}^l) \tag{61}$$

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

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

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 6.15, 6.21). Thus, the above expression is equal to

$$t^p = -\lim_{s\to 0^+} \sum_{t\in\mathbb{Z}, t^2-4n=0} \frac{s}{2} \frac{|\eta|^{s+1}}{|Z(\Gamma)|} \zeta(s+1) \times \prod_{v|M} c_v^+(\alpha, \mathbb{Z}[\epsilon]) \tag{62}$$

$$= \sum_{t\in\mathbb{Z}, t^2-4n=0} \frac{1}{2} \frac{|\eta|}{|Z(\Gamma)|} \times \prod_{v|M} c_v^+(\alpha, \mathbb{Z}[\epsilon])$$

$$= \frac{|\eta|}{|Z(\Gamma)|} \times \prod_{v|M} c_v^+(\alpha, \mathbb{Z}[\epsilon]).$$

7. The Jacobians of Cartan modular curves

In this section, the main result of this paper is deduced from the trace calculations of the previous section. 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 $\mathbb{Q}$.

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

Consider the decomposition

$$S_2(\Gamma_0(p^2)) = S_2(\Gamma_0(p^2)^{\text{new}} \oplus S_2(\Gamma_0(p^2))^{\text{old}} \tag{63}$$

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 [1], 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 $f_i(z) \pm f_i \mid_{R_p} (z)$ determines its eigenvalue for the operator W_p. Refer to Lemma 26 in [1] 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 7.1.

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

7.2. **Comparison of trace formulae.** The following table summarises the calculations done in section 6. Refer to the hypotheses of Propositions 6.15, 6.21, 6.16, 6.22 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 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

(64)
$$c_p^+(\alpha,\mathfrak{r})[X^+_{\text{non-split}}(p)] - (c_p^+(\alpha,\mathfrak{r})[X^+_{\text{split}}(p)] - c_p^+(\alpha,\mathfrak{r})[X_0(p)]) = c_p^+(\alpha,\mathfrak{r})[X(1)].$$

so that

$$t^{(\cdot)}[X^+_{\text{non-split}}(p)] - (t^{(\cdot)}[X^+_{\text{split}}(p)] - t^{(\cdot)}[X_0(p)]) = t^{(\cdot)}[X(1)] \tag{65}$$

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

From the discussion in section 6.6,

$$t^o[X_\Gamma] = \frac{1}{4\pi} v(\Gamma\backslash\mathfrak{H}^*) \tag{66}$$

Therefore, using the fact that

$$v(\Gamma\backslash\mathfrak{H}^*) = \frac{1}{3\pi}[\Gamma(1):\Gamma] \tag{67}$$

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

$$t^o[X^+_{\text{non-split}}(p)] - (t^o[X^+_{\text{split}}(p)] - t^o[X_0(p)]) = t^o[X(1)]. \tag{68}$$

Thus,

$$t^\Sigma[X^+_{\text{non-split}}(p)] - (t^\Sigma[X^+_{\text{split}}(p)] - t^\Sigma[X_0(p)]) = t^\Sigma[X(1)] \tag{69}$$

so that

$$\text{tr}(T_n \mid S_2(\Gamma^+_{\text{non-split}}(p))) - (\text{tr}(T_n \mid S_2(\Gamma^+_{\text{split}}(p))) - \text{tr}(T_n \mid S_2(\Gamma_0(p)))) \tag{70}$$

$$= \text{tr}(T_n \mid S_2(\Gamma(1))) = 0 \tag{71}$$

for all n prime to p. By Lemma 7.1 and the fact that $X_0^+(p^2) \cong X^+_{\text{split}}(p)$, we obtain

Theorem 2. *For all n prime to p,*

$$tr(T_n \mid S_2(\Gamma^+_{non\text{-}split}(p))) = tr(T_n \mid S_2(\Gamma_0^+(p^2))^{new}).$$

7.3. **The Eichler-Shimura relations.** Let Γ be a strong arithmetic congruence group in $B^\times = \mathrm{GL}_2(\mathbb{Q})$ 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 [14] or [16]). 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 7.2. *(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 [27]. □

If Γ_v contains all scalars for $v \mid N$, 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

$$L_q(A, X) = \det(1 - F_q X \mid T_l(A))^{-1} \tag{72}$$

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 $S_2(\Gamma)$ [4]:

$$L_q(J, X) = \det(1 - T_q X + qX^2 \mid S_2(\Gamma)). \tag{73}$$

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 $S_2(\Gamma_0^+(p^2))^{\text{new}}$.

7.4. **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 $\mathbb{T}$.

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 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 [11], 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 $X_0^+(p^2)$.*

8. Conclusion

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 (minimal) kernel of this isogeny is.

A more enlightening proof that the L-functions are the same using a description of Hecke actions on the reduction of the modular curves involved may yield a more geometric explanation of the phenomenon as suggested by S. Edixhoven. Indeed, Edixhoven has subsequently proved the isogeny in Theorem 1 without using the trace calculation in Theorem 2 [8]. His proof is based on the representation theory of $\mathrm{GL}_2(\mathbb{F}_p)$ and in principle gives the isogeny in question explicitly, though it would be still interesting to pursue this in more detail.

We have been mainly interested in $X^+_{\text{non-split}}(p)$, but our calculations also give a similar result for the jacobian of $X_{\text{non-split}}(p)$ (i.e. the modular curve associated to a non-split Cartan subgroup, rather than the normaliser of a non-split Cartan subgroup), namely, that it is isogenous to the new part of the jacobian of $X_{\text{split}}(p)$. This follows from the fact that

$$c_p^+(\alpha,\mathfrak{r})[X_{\text{non-split}}(p)] = c_p(\alpha,\mathfrak{r})[X^+_{\text{non-split}}(p)] \tag{74}$$

$$c_p^+(\alpha,\mathfrak{r})[X_{\text{split}}(p)] = c_p(\alpha,\mathfrak{r})[X^+_{\text{split}}(p)]. \tag{75}$$

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 (5.22) are not necessary. Also, implicit in our calculations is an explicit trace formula for $X_0^+(p^2) \cong X^+_{\text{split}}(p)$.

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:

$$\begin{aligned} &\mathrm{tr}(T_n \mid S_k(\Gamma^+_{\text{non-split}}(p))) - \mathrm{tr}(T_n \mid S_k(\Gamma(1)) \\ &= \mathrm{tr}(T_n \mid S_k(\Gamma^+_{\text{split}}(p))) - \mathrm{tr}(T_n \mid S_2(\Gamma_0(p)) \end{aligned} \tag{76}$$

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.

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 to look into the possibility of a twisting operator [1] for $X^+_{\text{non-split}}(p)$.

One may also ask what other non-trivial relations exist between the jacobians of arithmetic congruence groups. For example, in [26], it is shown using the trace formula that the zeta functions of the new part of the jacobian of $X_0(N)$ and the jacobian of the unit group of a maximal order in the quaternion algebra ramified at N are the same if N is a product of an even number of distinct primes. By a method in [22], one can show that that the two abelian varieties above are isogenous.

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.

References

[1] A.O.L. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Mathematische Annalen*, 185:134–160, 1970.

[2] P. Bayer and T. Travesa, editors. *Corbes Modulars: Taules*, Notes del Seminari Teoria de Nombres, Barcelona, 1992.
[3] B.J. Birch and W. Kuyk, editors. *Modular Functions of One Variable IV*, number 476 in Lecture Notes in Mathematics. Springer-Verlag, 1972.
[4] 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.
[5] P.M. Cohn. *Algebra*, volume 2. John Wiley & Sons, second edition, 1982.
[6] 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.
[7] 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.
[8] S.J. Edixhoven. On a result of Imin Chen. Preprint (Duke algebraic geometry preprint server), 1996.
[9] M. Eichler. Eine verallgemeinerung der abelschen integrale. *Mathematische Zeitschrift*, 67:267–298, 1957.
[10] 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.
[11] G. Faltings. Finiteness theorems for abelian varieties. In G. Cornell and J. Silverman, editors, *Arithmetic Geometry*. Springer-Verlag, 1986.
[12] B. Gross. *Arithmetic on Elliptic Curves with Complex Multiplication*. Number 776 in Lecture Notes in Mathematics. Springer-Verlag, 1980.
[13] 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.
[14] J. Igusa. On the algebraic theory of elliptic modular functions. *Journal of the Mathematical Society of Japan*, 20:96–106, 1968.
[15] H. Ishikawa. On the trace formula for Hecke operators. *Journal of the Faculty of Science of the University of Tokyo*, 20:217–238, 1973.
[16] N. Katz and B. Mazur. *Arithmetic Moduli of Elliptic Curves*. Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985.
[17] 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.
[18] B. Mazur. Modular curves and the Eisenstein ideal. *I.H.E.S. Publications Mathématiques*, 47:33–186, 1977.
[19] B. Mazur. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978.
[20] T. Miyake. *Modular Forms*. Springer-Verlag, 1989.
[21] F. Momose. Rational points on the modular curves $X_{\text{split}}(p)$. *Compositio Mathematica*, 52:115–137, 1984.
[22] K. Ribet. Sur les variétés abéliennes à multiplications réelles. *Comptes Rendus de l'Académie des Sciences de Paris*, 291:121–123, 1980. Série A.
[23] K. Ribet. On the equation $a^p + 2^\alpha b^p + c^p = 0$. Preprint (MSRI preprint server), 1995.
[24] H. Saito. On Eichler's trace formula. *Journal of the Mathematical Society of Japan*, 24(2):333–340, 1971.
[25] J.P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones Mathematicae*, 15:259–331, 1972.
[26] H. Shimizu. On zeta functions of quaternion algebras. *Annals of Mathematics*, 81:166–193, 1965.
[27] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Iwanami Shoten, Publishers and Princeton University Press, 1971.
[28] A. Wiles. Modular Elliptic Curves and Fermat's Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995.

Mathematical Institute, 24-29 St. Giles', Oxford, England, OX1 3LB
E-mail address: chen@maths.oxford.ac.uk