

HEEGNER POINTS ON CARTAN NON-SPLIT CURVES

DANIEL KOHEN AND ARIEL PACETTI

ABSTRACT. Let E/\mathbb{Q} be an elliptic curve of conductor N , and let K be an imaginary quadratic field such that the root number of E/K is -1 . Let \mathcal{O} be an order in K and assume that there exists an odd prime p , such that $p^2 \parallel N$, and p is inert in \mathcal{O} . Then although there are no Heegner points in $X_0(N)$ attached to \mathcal{O} , in this article we construct such points from Cartan non-split curves. In order to do that we give a method to compute Fourier expansions for forms in Cartan non-split curves, and prove that the constructed points form a Heegner system as in the classical case.

INTRODUCTION

Let E be an elliptic curve over \mathbb{Q} of conductor N and let K be an imaginary quadratic field such that E/K has root number -1 . One of the main problems in number theory is to construct rational points on E . The only instance in which a general construction is known is via the so called “Heegner points”. Let \mathcal{O} be an order in K of discriminant prime to N satisfying the *Heegner hypothesis for $X_0(N)$* : “assume that all primes dividing N are split in \mathcal{O} ” (see [Dar04] Hypothesis 3.9). Then one can construct points in the modular curve $X_0(N)$ and map them through the modular parametrization to the curve E . Gross-Zagier Theorem says that the constructed points are non-torsion if and only if $L'(E, 1) \neq 0$. More generally, when N is square-free, we can construct Heegner points in certain Shimura curves, provided that the *Heegner hypothesis for Shimura curves* is satisfied: the number of prime numbers dividing N which are inert in \mathcal{O} is even. This hypothesis is the right one for the root number to be -1 , but when N is not square-free, this is not true anymore. For example, suppose that we start with an elliptic curve E over \mathbb{Q} of conductor p^2 (p an odd prime). Let K be an imaginary quadratic field with discriminant D such that D and p are prime to each other and p is inert in K . In this case the root number is still -1 (for example see [Zha01, Definition 1.1.3]), but the Heegner hypothesis is not satisfied. However, one would like to construct Heegner points (and Heegner systems)

2010 *Mathematics Subject Classification*. Primary: 11G05, Secondary: 11F30.

Key words and phrases. Cartan Curves, Heegner points.

DK was partially supported by a CONICET doctoral fellowship.

AP was partially supported by CONICET PIP 2010-2012 GI and FonCyT BID-PICT 2010-0681.

in this case as well and prove that they satisfy a Gross-Zagier-Zhang formula! Of course there will be no points in the classical modular curve $X_0(p^2)$, so one can search in other modular curves for the same phenomena. In the present situation, there are some canonical choices, the so called non-split Cartan curves, which are quotients of the Poincare half-plane by a Cartan non-split group. The two main problems one needs to address regarding modular forms for these groups are the following:

- There are many Cartan non-split curves (one for each non-square modulo p). Which one should we choose? Is the elliptic curve E a quotient of their Jacobians?
- How do we compute the Fourier expansion of the Hecke eigenforms for such groups? What is the coefficient field of such forms?

In this article we will answer these questions, and show how to use them to construct (both theoretically and computationally) Heegner points from points in Cartan non-split curves. We will show that they form the so called *Heegner systems* and satisfy the same properties as the Heegner points coming from classical modular curves.

The present article is organized as follows: in the first section we recall the basic definitions of Cartan non-split curves, and give a moduli space interpretation for them. Our moduli problem is quite different from the classical ones and the one described in [RW14], but it makes the geometric and analytic properties of Hecke operators and Heegner systems more clear. For example, with this moduli interpretation it is easy to define Hecke operators (outside p), and show that this definition agrees with the double coset definition (as in [Che98]). It is also easily generalizable to more general conductors.

After giving the basics of modular forms for Cartan non-split groups, we move to the question of computing their q -expansions. We prove that such expansions, under a suitable normalization that we propose, have coefficients in $\mathbb{Q}(\xi_p)$ (the p -th cyclotomic field). We want to point out that we do not know a way for theoretically computing the q -expansion. Using our normalization, we compute it numerically (by solving a linear system) and once we know the coefficient field, we can compute it exactly. Furthermore, we only need to compute numerically one coefficient of the form (see the computational digression in Section 3). A Theorem of Chen and Edixhoven ([Che98, Edi96]) proves in this case that our curve is isogenous to a quotient of the Jacobian of the Cartan non-split curve, so one can use the Eichler-Shimura construction and the Abel-Jacobi map to compute the modular parametrization. One big obstacle here is that the cusps for the Cartan non-split curves are not defined over \mathbb{Q} (implying that the modular parametrization is not rational), so we average such maps over all the cusps, to get a rational map (which we also call modular parametrization). The effect of averaging over all cusps is the same as that of considering all the Cartan curves (for the different choices of a non-square modulo p), so

an answer to our first question is that for constructing Heegner points one needs all the curves at the same time. It is a natural and interesting question to understand which is the Manin constant in our situation. At the time, we do not have an answer to this question (but we give some examples at the end).

Once one understands the level p^2 case, it is natural to consider mixed cases, i.e. elliptic curves whose conductor is not square-free and an order in an imaginary quadratic field where some primes of the conductor are split and the other ones are inert. There are no extra difficulties, nevertheless, we believe that considering first the conductor p^2 case gives a better understanding of the new ideas involved.

The third and fourth sections are about constructing Heegner points in the general case. We first give some easy remarks on the Abel-Jacobi map and then show how our moduli interpretation allows us to construct Heegner points and Heegner systems satisfying the usual compatibility relations. Using this we can prove a big part of the Birch and Swinnerton-Dyer conjecture for E/K by applying the usual Darmon-Kolyvagin and Gross-Zagier-Zhang formula machinery (Theorem 4.7 and Theorem 4.8).

The last section of the article contains many examples where we show how the method works for different elliptic curves and what are the Manin constants in each case.

Acknowledgments: We would like to thank Professor Henri Darmon for many suggestions and for the discussions the first author had with him while visiting McGill University. We also would like to thank Professor Imin Chen for explaining us the technicalities of the definition of Hecke operators on Cartan non-split groups and Professor Tim Dokchitser for the results in Appendix A. We also thank the referee and Juan Restrepo for useful comments and corrections.

1. CARTAN NON-SPLIT CURVES OF PRIME LEVEL

1.1. **Definition.** Throughout this work, p will denote an odd prime and ε will denote a non-square modulo p . Let $C_{ns}^\varepsilon(p)$ the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ given by the matrices of the form

$$C_{ns}^\varepsilon(p) = \left\{ \begin{pmatrix} a & b \\ b\varepsilon & a \end{pmatrix} \text{ such that } (a, b) \neq (0, 0) \right\}.$$

Given a matrix $A \in \mathrm{M}_{2 \times 2}(\mathbb{Z})$, we denote by \bar{A} its reduction mod p . Let $M_{ns}^\varepsilon(p)$ be the suborder of $\mathrm{M}_{2 \times 2}(\mathbb{Z})$ given by

$$M_{ns}^\varepsilon(p) = \left\{ A \in \mathrm{M}_{2 \times 2}(\mathbb{Z}) : \bar{A} \in C_{ns}^\varepsilon(p) \cup \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}.$$

Denote by Γ_{ns}^ε the elements in $M_{ns}^\varepsilon(p)$ with determinant 1. When it is clear from the context we will omit ε and/or p in the notation.

We can also consider the normalizer of the Cartan subgroup

$$C_{ns}^+(p) = \left\{ \left(\begin{array}{cc} a & b \\ b\varepsilon & a \end{array} \right) \cup \left(\begin{array}{cc} a & b \\ -b\varepsilon & -a \end{array} \right) \text{ such that } (a, b) \neq (0, 0) \right\},$$

and we can define $M_{ns}^+(p)$ and $\Gamma_{ns}^+(p)$ as before.

Consider the extended Poincare half plane \mathcal{H}^* and its quotient $X_{ns}(p) = \Gamma_{ns}(p) \backslash \mathcal{H}^*$, which gives the Cartan non-split modular curve. It corresponds to the compactification of the curve $Y_{ns}(p) = \Gamma_{ns}(p) \backslash \mathcal{H}$. Analogously we can define $X_{ns}^+(p) = \Gamma_{ns}^+(p) \backslash \mathcal{H}^*$. Since $Det : C_{ns}(p) \rightarrow \mathbb{F}_p$ is surjective, the modular curves $X_{ns}(p)$ and $X_{ns}^+(p)$ are defined over \mathbb{Q} .

1.2. Moduli interpretation. For our purposes we will only work with complex points of the Cartan curve, so we will state our moduli interpretation for them. Nevertheless the same computations can be made over any scheme, and prove the existence of an integral model for Cartan non-split curves as well as their normalizers.

Consider pairs $[E, \phi]$, where E/\mathbb{C} is an elliptic curve and $\phi \in \text{End}_{\mathbb{F}_p}(E[p])$ satisfies that ϕ^2 is multiplication by ε . We say that two such pairs $[E, \phi]$, $[E', \phi']$ are isomorphic if there exists an isomorphism of elliptic curves $\Psi : E \rightarrow E'$ such that the following diagram is commutative:

$$\begin{array}{ccc} E[p] & \xrightarrow{\phi} & E[p] \\ \Psi \downarrow & & \downarrow \Psi \\ E'[p] & \xrightarrow{\phi'} & E'[p] \end{array}$$

Proposition 1.1. *The moduli problem of pairs $[E, \phi]$ as above is represented by the Cartan non-split curve $Y_{ns}^\varepsilon(p)$. More concretely, the isomorphism class $\Gamma_{ns}^\varepsilon(p)\tau$ corresponds to the pair $[E_\tau, \phi_\tau]$ where $E_\tau = \mathbb{C}/\langle \tau, 1 \rangle$ and if $B_\tau = \left\{ \frac{1}{p}, \frac{\tau}{p} \right\}$ is a basis of $E_\tau[p]$, then ϕ_τ is the endomorphism of $E_\tau[p]$ whose matrix in the basis B_τ equals $\begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$.*

Proof. We need to check the following facts:

- The previous correspondence between points in $Y_{ns}^\varepsilon(p)$ and pairs $[E, \phi]$ is well defined.
- This map is bijective.

Let τ and τ' be elements in the upper half plane, which correspond to pairs $[E_\tau, \phi_\tau], [E_{\tau'}, \phi_{\tau'}]$. If we prove that such pairs are isomorphic (with the previous identification) if and only if τ and τ' are equivalent under $\Gamma_{ns}^\varepsilon(p)$, we get that the map is well defined and injective.

It is a classical result that any morphism Ψ between two elliptic curves is given by multiplication by a complex number α . In particular, if Ψ is an isomorphism, $\alpha\langle\tau, 1\rangle = \langle\tau', 1\rangle$, so that there exists $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with $\alpha\tau = a\tau' + b$ and $\alpha = c\tau' + d$. From our moduli interpretation, we also need the map Ψ to satisfy $\phi_{\tau'}\Psi = \Psi\phi_\tau$. In the chosen basis, this implies checking that

- $\Psi(\phi_\tau(\frac{1}{p})) = \phi_{\tau'}(\Psi(\frac{1}{p}))$.
- $\Psi(\phi_\tau(\frac{\tau}{p})) = \phi_{\tau'}(\Psi(\frac{\tau}{p}))$.

An easy computation shows that

- $\Psi(\phi_\tau(\frac{1}{p})) = \Psi(\frac{\tau\varepsilon}{p}) = \frac{\alpha\tau\varepsilon}{p} = \frac{a\varepsilon\tau' + b\varepsilon}{p}$.
- $\Psi(\frac{1}{p}) = \frac{\alpha}{p} = \frac{c\tau' + d}{p}$, so $\phi_{\tau'}(\Psi(\frac{1}{p})) = \frac{c + d\varepsilon\tau'}{p}$.

We need the equality to hold modulo $\langle 1, \tau' \rangle$, which implies that $a \equiv d \pmod{p}$ and $c \equiv \varepsilon b \pmod{p}$. In particular, the pairs $[E_\tau, \phi_\tau]$ and $[E_{\tau'}, \phi_{\tau'}]$ are isomorphic by a map satisfying the first condition if and only if τ and τ' are equivalent under $\Gamma_{ns}^\varepsilon(p)$.

The commutative condition for the second basis elements is similar and gives the same constraint.

Surjectivity follows from the following facts:

- Let $M \in \mathrm{GL}_2(\mathbb{F}_p)$ be such that $M^2 = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}$. Then there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $\bar{A}M\bar{A}^{-1} = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$. This will be proved in Lemma 1.2.
- Let $\phi \in \mathrm{End}_{\mathbb{F}_p}(E[p])$, and B, B' bases of $E[p]$. If $[\phi]_B$ denotes the matrix of ϕ in the basis B , and C the change of basis matrix from B to B' , then $[\phi]_{B'} = C^{-1}[\phi]_B C$ (this is just linear algebra).
- Let $[E, \phi]$ be a pair as before, let $\Psi : E \rightarrow E'$ be an isomorphism, B be a basis of $E[p]$, $B' = \Psi(B)$ be the image of such basis and ϕ' the element in $\mathrm{End}_{\mathbb{F}_p}(E'[p])$ making the diagram commute. Then $[\phi]_B = [\phi']_{B'}$.

Let $[E, \phi]$ be any such pair. Up to isomorphism, we can assume that $E = \mathbb{C}/\langle\tau, 1\rangle$, where $\tau \in \mathcal{H}$. Let $B = \left\{ \frac{1}{p}, \frac{\tau}{p} \right\}$ be a basis of $E[p]$. By the first fact, there exists a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $\bar{A}[\phi]_B\bar{A}^{-1} = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$. Then the other two facts prove that $[E, \phi] \simeq [\mathbb{C}/\langle A \cdot \tau, 1 \rangle, \phi']$, where $[\phi']_{\left\{ \frac{1}{p}, \frac{A \cdot \tau}{p} \right\}} = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$. This proves surjectivity. \square

Lemma 1.2. *Let $M \in \mathrm{GL}_2(\mathbb{F}_p)$ satisfying $M^2 = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix}$. Then, there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $\bar{A}M\bar{A}^{-1} = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$.*

Proof. Clearly there exists $B \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $B^{-1}MB = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$. Consider the centralizer of $\begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$, which is given by $C_{ns}^\varepsilon(p)$ and take any matrix C of determinant $\det(B)^{-1}$ there. We have that $BC \in \mathrm{SL}_2(\mathbb{F}_p)$ and $(BC)^{-1}M(BC) = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$. The result follows from the fact that the reduction map $\mathrm{SL}_2(\mathbb{Z}) \mapsto \mathrm{SL}_2(\mathbb{F}_p)$ is surjective. \square

Remark 1.3. If we want to consider not the Cartan non-split but its normalizer, we consider pairs $[E, \phi]$ as before, but where two such pairs are isomorphic if $\Psi\phi = \pm\phi'\Psi$.

It is clear that the same proof works and that we have an involution in $X_{ns}(p)$ given by sending $[E, \phi]$ to $[E, -\phi]$ whose fixed points are precisely $X_{ns}^+(p)$. We call this involution ω_p .

1.3. Modular Forms. As in the classical case, given a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, one can define what modular forms are for such group. Let $f : \mathcal{H} \rightarrow \mathbb{C}$ be an holomorphic function. If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, and $k \in \mathbb{Z}$, we define the slash operator

$$f|_k[\begin{pmatrix} a & b \\ c & d \end{pmatrix}](z) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right).$$

Then $M_k(\Gamma)$ is the space of holomorphic functions which are invariant under the previous action for all elements in Γ and which are holomorphic at all the cusps. $S_k(\Gamma)$ is the subspace of cusp forms, which are those forms in $M_k(\Gamma)$ whose q -expansion at all the cusps have zero constant coefficient.

We want to relate $S_2(\Gamma_{ns}(p))$ to modular forms for classical subgroups. The containment $\Gamma(p) \subset \Gamma_{ns}(p)$ gives the reverse inclusion at the level of modular forms $S_2(\Gamma_{ns}(p)) \subset S_2(\Gamma(p))$. Let $\alpha_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. If $f \in S_2(\Gamma(p))$, $\tilde{f} = f|_2[\alpha_p]$ is a modular form for $(\alpha_p)^{-1}\Gamma(p)\alpha_p$. But if $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\alpha_p^{-1}M\alpha_p = \begin{pmatrix} a & p^{-1}b \\ pc & d \end{pmatrix}$. So if $M \in \Gamma(p)$ we obtain that $(\alpha_p)^{-1}M(\alpha_p) \in \Gamma_0(p^2) \cap \Gamma_1(p)$ and conversely. That is, slashing by the matrix α_p we obtain the isomorphism

$$(1) \quad S_2(\Gamma(p)) \cong S_2(\Gamma_0(p^2) \cap \Gamma_1(p)) \cong \bigoplus_{\{\chi, \chi\kappa_p\}} S_2(\Gamma_0(p^2), \chi^2),$$

where κ_p denotes the quadratic character of conductor p , and the sum is taken over pairs $\{\chi, \chi\kappa_p\}$, with χ any character of conductor dividing p (but we do not want to count $\chi, \chi\kappa_p$ twice). The last isomorphism comes from the fact that the group $\Gamma_0(p^2)/(\Gamma_0(p^2) \cap \Gamma_1(p))$ is abelian, so we can decompose the space of modular forms as a sum of the irreducible representations of such quotient, which correspond to the even (hence square) characters of conductor dividing p .

1.4. Hecke operators. There are two ways to define Hecke operators for classical subgroups. One of them is to define correspondences between the modular curves and, via the moduli interpretation, translate this action to an action on modular forms while the other one is in terms of double coset operators. We want to give this two interpretations in our setting, since each of them has its own advantages.

1.4.1. Geometric definition. Let n be a positive integer prime to p , and $[E, \phi]$ a pair as before, corresponding to the moduli interpretation of the curve $Y_{ns}^\varepsilon(p)$. Define the Hecke operator

$$\mathcal{T}_n^\varepsilon([E, \phi]) = \sum_{\psi: E \rightarrow E'} [E', \frac{1}{n}\psi \circ \phi \circ \hat{\psi}],$$

where the sum is over degree n isogenies $\psi : E \rightarrow E'$, and $\hat{\psi}$ denotes the dual isogeny. Note that since $\gcd(n, p) = 1$, $\frac{1}{n} \in \text{End}_{\mathbb{F}_p}(E'[p])$. Also, since $\psi \circ \hat{\psi}$ and $\hat{\psi} \circ \psi$ are multiplication by n , $(\frac{1}{n}\psi \circ \phi \circ \hat{\psi}) \circ (\frac{1}{n}\psi \circ \phi \circ \hat{\psi})$ equals multiplication by ε , so the points in the sum belong to $Y_{ns}^\varepsilon(p)$.

1.4.2. *Algebraic definition.* We make a little survey of Hecke operators for the Cartan non-split curve, for which we follow closely Shimura's book ([Shi94]). Let

$$\Delta_p := \{A \in M_{2 \times 2}(\mathbb{Z}) : \det(A) > 0 \text{ and } \gcd(p, \det(A)) = 1\}.$$

Let $\Delta_{ns}^\varepsilon(p)$ be the intersection $\Delta_p \cap M_{ns}^\varepsilon(p)$, i.e. the set of matrices in $M_{ns}^\varepsilon(p)$ with positive determinant relatively prime to p . Let $\Gamma(p)$ be the level p congruence subgroup, and let

$$\Delta(p) := \{A \in \Delta_p : \bar{A} \equiv \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix} \pmod{p}\}.$$

Let $R(\Gamma_{ns}^\varepsilon(p), \Delta_{ns}^\varepsilon(p))$ and $R(\Gamma(p), \Delta(p))$ be the Hecke rings as defined in [Shi94] (page 54). We have the following Lemma.

Lemma 1.4. *The Hecke rings $R(\Gamma_{ns}^\varepsilon(p), \Delta_{ns}^\varepsilon(p))$, $R(\text{SL}_2(\mathbb{Z}), \Delta_p)$ and $R(\Gamma(p), \Delta(p))$ are isomorphic.*

Proof. Proposition 3.31 of [Shi94] proves that the last two ones are isomorphic. Clearly we have a map from $R(\Gamma_{ns}^\varepsilon(p), \Delta_{ns}^\varepsilon(p))$ to $R(\text{SL}_2(\mathbb{Z}), \Delta_p)$ given by

$$\Gamma_{ns}^\varepsilon(p)\alpha\Gamma_{ns}^\varepsilon(p) \rightarrow \text{SL}_2(\mathbb{Z})\alpha\text{SL}_2(\mathbb{Z}).$$

Surjectivity is proven in exactly the same way as the classical case. To prove injectivity, note that by Lemma 3.29, part (1) of [Shi94], if $\alpha \in \Delta_{ns}^\varepsilon(p)$, then

$$(2) \quad \Gamma_{ns}^\varepsilon(p)\alpha\Gamma_{ns}^\varepsilon(p) = \left\{ \xi \in \text{SL}_2(\mathbb{Z})\alpha\text{SL}_2(\mathbb{Z}) : \bar{\xi} \in \overline{\Gamma_{ns}^\varepsilon(p)\alpha} \right\}.$$

Then if $\alpha, \beta \in \Delta_{ns}^\varepsilon(p)$ are such that $\text{SL}_2(\mathbb{Z})\alpha\text{SL}_2(\mathbb{Z}) = \text{SL}_2(\mathbb{Z})\beta\text{SL}_2(\mathbb{Z})$, they have the same determinant, and by (2), $\Gamma_{ns}^\varepsilon(p)\alpha\Gamma_{ns}^\varepsilon(p) = \Gamma_{ns}^\varepsilon(p)\beta\Gamma_{ns}^\varepsilon(p)$. \square

If ℓ is a prime number different from p , then the Hecke operator $\mathcal{T}_\ell^\varepsilon$ is given by the action of the double coset $\Gamma_{ns}^\varepsilon(p)\alpha\Gamma_{ns}^\varepsilon(p)$, where $\alpha \in \Delta_{ns}^\varepsilon(p)$ is any matrix with determinant ℓ . In particular, if $\ell \equiv 1 \pmod{p}$, we can take $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}$ and get the classical Hecke operator. By T_ℓ we will denote the classical Hecke operator acting on $S_2(\Gamma(p))$ and by \tilde{T}_ℓ the one acting on $S_2(\Gamma_0(p^2), \chi)$. Using the isomorphism (1), we get the following commutative diagram

$$(3) \quad \begin{array}{ccc} S_2(\Gamma(p)) & \xrightarrow{|\langle \alpha_p \rangle|} & \bigoplus_{\{\chi, \chi \varkappa_p\}} S_2(\Gamma_0(p^2), \chi^2) \\ T_\ell \downarrow & & \downarrow \tilde{T}_\ell \\ S_2(\Gamma(p)) & \xrightarrow{|\langle \alpha_p \rangle|} & \bigoplus_{\{\chi, \chi \varkappa_p\}} S_2(\Gamma_0(p^2), \chi^2) \end{array}$$

Proposition 1.5. *Let ℓ be a prime congruent to 1 modulo p . Let $\gamma_\infty = \begin{pmatrix} \ell c_1 & c_2 \\ p^2 \ell & \ell \end{pmatrix}$ and $\gamma_i = \begin{pmatrix} 1 & i \\ 0 & \ell \end{pmatrix}$, for $i = 0, \dots, \ell - 1$ be representatives for $\mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \mathrm{SL}_2(\mathbb{Z})$ modulo $\mathrm{SL}_2(\mathbb{Z})$. (c_1 and c_2 are integers such that the matrix γ_∞ has determinant ℓ). Then $\{\alpha_p \gamma_\infty \alpha_p^{-1}, \alpha_p \gamma_i \alpha_p^{-1}\}_{i=0}^{\ell-1}$ is a set of representatives for $\Gamma_{ns}^\varepsilon(p) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \Gamma_{ns}^\varepsilon(p)$ modulo $\Gamma_{ns}^\varepsilon(p)$.*

Proof. This is just an easy exercise. Note that $\alpha_p \gamma_\infty \alpha_p^{-1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \pmod{p}$. \square

Corollary 1.6. *If $\ell \equiv 1 \pmod{p}$, then the Hecke operator $\mathcal{T}_\ell^\varepsilon$ acting on $S_2(\Gamma_{ns}^\varepsilon(p))$ is the same as the Hecke operator T_ℓ acting on $S_2(\Gamma(p))$.*

Corollary 1.7. *If $\ell \equiv \pm 1 \pmod{p}$, then the Hecke operator $\mathcal{T}_\ell^\varepsilon$ acting on $S_2(\Gamma_{ns}^{+, \varepsilon}(p))$ is the same as the Hecke operator T_ℓ acting on $S_2(\Gamma(p))$.*

Proof. This is because $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \in \Delta_{ns}^{+, \varepsilon}(p)$. \square

Let ℓ be a prime number different from p , and let $B \in \Delta_{ns}^\varepsilon(p)$ be any matrix with determinant ℓ . Let $A_\ell^\varepsilon \in \mathrm{SL}_2(\mathbb{Z})$ be such that $A_\ell^\varepsilon \equiv B \begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix} \pmod{p}$. The action of A_ℓ^ε in $S_2(\Gamma(p))$ defines an operator that we will denote v_ℓ^ε . Note that such action does not depend on the choice of A_ℓ^ε , but only on B , since any two such matrices are equivalent modulo p .

Lemma 1.8. *The operator v_ℓ^ε is an isomorphism from $S_2(\Gamma_{ns}^\varepsilon(p))$ to $S_2(\Gamma_{ns}^{\varepsilon \ell^2}(p))$ which does not depend on the choice of B .*

Proof. The first statement comes from the fact that $\bar{B} \in C_{ns}^\varepsilon(p)$, and the easy computation $\begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix}^{-1} C_{ns}^\varepsilon(p) \begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix} = C_{ns}^{\varepsilon \ell^2}(p)$. The second fact is immediate as well: if A_1 and A_2 are two matrices in $\mathrm{SL}_2(\mathbb{Z})$ corresponding to B_1 and B_2 , then $A_1 A_2^{-1}$ has determinant 1 and modulo p is in $\Gamma_{ns}^\varepsilon(p)$, hence it acts trivially. \square

Proposition 1.9. *Let ℓ be a prime number different from p . Then $\mathcal{T}_\ell^\varepsilon = T_\ell \circ v_\ell^\varepsilon$.*

Proof. Let A_ℓ^ε be as before. To compute the Hecke operator $\mathcal{T}_\ell^\varepsilon$, we need to find representatives for $\Gamma_{ns}^\varepsilon(p) \backslash (\Gamma_{ns}^\varepsilon(p) A_\ell^\varepsilon \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \Gamma_{ns}^\varepsilon(p))$. Let $\{\gamma_\infty, \gamma_i\}_{i=0}^{\ell-1}$ be the set of representatives for $\mathrm{SL}_2(\mathbb{Z}) \backslash (\mathrm{SL}_2(\mathbb{Z}) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \mathrm{SL}_2(\mathbb{Z}))$. Then $\{A_\ell^\varepsilon \alpha_p \gamma_\infty \alpha_p^{-1}, A_\ell^\varepsilon \alpha_p \gamma_i \alpha_p^{-1}\}_{i=0}^{\ell-1}$ is clearly a set of representatives for our quotient and for these representatives the statement is clear. \square

In particular, if $f \in S_2(\Gamma_{ns}^\varepsilon(p)) \subset S_2(\Gamma(p))$, then $T_\ell(f) \in S_2\left(\Gamma_{ns}^{\varepsilon/\ell^2}(p)\right)$. Moreover, we have the following:

Proposition 1.10. *Let ℓ be a prime number different from p . The operators $T_\ell : S_2(\Gamma_{ns}^\varepsilon(p)) \rightarrow S_2(\Gamma_{ns}^{\varepsilon/\ell^2}(p))$ and $v_\ell : S_2(\Gamma_{ns}^\varepsilon(p)) \rightarrow S_2(\Gamma_{ns}^{\varepsilon\ell^2}(p))$ are morphisms of Hecke modules.*

Proof. Choose $\alpha \in \Delta_{ns}^\varepsilon(p)$ of determinant $q (\neq p)$ such that the entry $(2, 1)$ is divisible by ℓ . It is easy to see that T_ℓ restricted to $S_2(\Gamma_{ns}^\varepsilon(p))$ is equal to $\Gamma_{ns}^\varepsilon(p) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \Gamma_{ns}^{\varepsilon/\ell^2}(p)$. Using Proposition 3.7 part (1) of [Shi94] we find that $T_\ell \mathcal{F}_q^\varepsilon = \Gamma_{ns}^\varepsilon(p) \alpha \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \Gamma_{ns}^{\varepsilon/\ell^2}(p)$. On the other hand, since $\alpha \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \alpha'$ with $\alpha' \in \Delta_{ns}^{\varepsilon/\ell^2}(p)$ of determinant q , it follows by part (2) of the same proposition that $T_\ell \mathcal{F}_q^\varepsilon = \mathcal{F}_q^{\varepsilon/\ell^2} T_\ell$ which clearly implies the first part.

The proof of the second part is exactly the same, by noting that v_ℓ^ε is the double coset operator $\Gamma^\varepsilon(p) A_\ell^\varepsilon \Gamma^{\varepsilon\ell^2}(p)$. \square

Now we can prove the relation between the geometric and the algebraic definition of the Hecke operators.

Theorem 1.11. *The definition of Hecke operators acting as correspondences on the curve $Y_{ns}^\varepsilon(p)$ and that of double quotients agree.*

Proof. We just need to prove that the representatives used for one definition can be taken as representatives for the other one. For simplicity, we restrict to prime Hecke operators $\mathcal{F}_\ell^\varepsilon (\ell \neq p)$. Recall that both definitions for the whole modular group $\mathrm{SL}_2(\mathbb{Z})$ do agree, so we can take as representatives for the degree ℓ isogenies the set $\{\frac{1}{\ell}\alpha_p \gamma_\infty \alpha_p^{-1}, \frac{1}{\ell}\alpha_p \gamma_i \alpha_p^{-1}\}_{i=0}^{\ell-1}$. Then,

$$\mathcal{F}_\ell^\varepsilon([\mathbb{C}/\langle \tau, 1 \rangle, \phi_\tau]) = \sum_{i=0}^{\ell-1} [\mathbb{C}/\langle \frac{\tau+pi}{\ell}, 1 \rangle, \phi_i] + [\mathbb{C}/\langle \ell c_1 \tau + p c_2, p \ell \tau + \ell \rangle, \phi_\infty],$$

where $[\phi_i]_{\{\frac{1}{p}, \frac{\tau+pi}{\ell p}\}} = \begin{pmatrix} 0 & 1/\ell \\ \varepsilon \ell & 0 \end{pmatrix}$. To compute the upper half plane point, we need to compute the change of basis matrix taking ϕ_i to the form $\begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$. For $i = 0, \dots, \ell - 1$, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix}$ is such a matrix. Let $B \in \Delta_{ns}^\varepsilon(p)$ be a matrix of determinant ℓ , and let $A_\ell^\varepsilon \in \mathrm{SL}_2(\mathbb{Z})$ be such that $A_\ell^\varepsilon \equiv B \begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix} \pmod{p}$ as before. Then $[\mathbb{C}/\langle \frac{\tau+pi}{\ell}, 1 \rangle, \phi_i] \simeq [\mathbb{C}/\langle \tau'_i, 1 \rangle, \phi_{\tau'_i}]$, where $\tau'_i = A_\ell^\varepsilon \begin{pmatrix} 1 & pi \\ 0 & \ell \end{pmatrix} \tau$ and $[\phi_{\tau'_i}]_{B_{\tau'_i}} = \begin{pmatrix} 0 & 1 \\ \varepsilon & 0 \end{pmatrix}$ as we wanted.

For ϕ_∞ , $[\phi_\infty]_{\{\frac{\ell}{p}, \frac{\ell c_1 \tau}{p}\}} = \begin{pmatrix} 0 & 1/\ell \\ \varepsilon \ell & 0 \end{pmatrix}$ also, and the matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix}$ takes this matrix to the standard form. Let $B \in \Delta_{ns}^\varepsilon(p)$ as before, and $A_\ell^\varepsilon \in \mathrm{SL}_2(\mathbb{Z})$ such that $A_\ell^\varepsilon \equiv B \begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix}$

(mod p). Then $A_\ell^\varepsilon \alpha_p \gamma_\infty \alpha_p^{-1}$ takes the pair to an upper half plane point with the required property. \square

Recall the following result by Chen and Edixhoven, which is crucial for this work. If \mathcal{C} is a curve, we denote by $\text{Jac}(\mathcal{C})$ its Jacobian.

Theorem 1.12 (Chen-Edixhoven). *The new part of $\text{Jac}(X_0^+(p^2))$ is isogenous to $\text{Jac}(X_{ns}^+(p))$. Moreover, $\text{Jac}(X_{ns}(p))$ and the new part of $\text{Jac}(X_0(p^2))$ are isogenous. Furthermore, the isogenies are Hecke equivariant.*

Proof. See Theorem 1 of [Che98], Theorem 1.1 of [Edi96] and Theorem 2 of [dSE00]. Although the Hecke equivariant condition is not explicitly stated, by Theorem 2 of [dSE00] the decompositions are functorial in (M, α) , hence they are preserved by all endomorphisms of M that commute with the G -action. In the case of Jacobians of modular curves this means that the isogenies commute with all Hecke operators of level prime to p . We want to thank Professor Bas Edixhoven for explaining this subtle detail to us. \square

Remark 1.13 (Multiplicity one for newforms). Recall that if $g \in S_2(\Gamma_0(N), \chi)$ is a newform, then any other form in the same space with the same Hecke eigenvalues is a multiple of it (see Theorem 5.8.2 of [DS05]).

In particular, if we start with a normalized newform $g \in S_2(\Gamma_0(p^2))$ such that $T_\ell g = \lambda_\ell g$ for all primes $\ell \neq p$, the last Theorem implies the existence of a normalized form $f \in S_2(\Gamma_{ns}^\varepsilon(p))$ such that $\mathcal{T}_\ell^\varepsilon f = \lambda_\ell f$ for all $\ell \neq p$. Moreover, since we have multiplicity one for classical newforms in $S_2(\Gamma_0(p^2))$ we must have multiplicity one for a system of eigenvalues (outside p) for the Hecke algebra $R(\Gamma_{ns}^\varepsilon(p), \Delta_{ns}^\varepsilon(p))$.

We need to compute the Fourier expansion of f from that of g . Using such expansion, we can compute the modular parametrization needed for constructing Heegner points. If χ is a character of conductor p , and $g \in S_2(\Gamma_0(p^2))$, we denote by $g \otimes \chi \in S_2(\Gamma_0(p^2), \chi^2)$ the twist of the g by χ .

Theorem 1.14. *Let $g \in S_2^{\text{new}}(\Gamma_0(p^2))$ be a normalized newform with eigenvalues λ_ℓ ($\forall \ell \neq p$), and let $f \in S_2(\Gamma_{ns}^\varepsilon(p))$ be the unique normalized eigenform such that $\mathcal{T}_\ell^\varepsilon f = \lambda_\ell f$ ($\forall \ell \neq p$). Let π_p be the local automorphic representation of g at p . Then*

- *If π_p is supercuspidal $g \otimes \chi$ is a newform in $S_2(\Gamma_0(p^2), \chi^2)$ for all characters χ of conductor p and*

$$\tilde{f} = f|_2[\alpha_p] = \sum a_\chi(g \otimes \chi),$$

where the sum is over all characters of conductor dividing p and $a_\chi \in \mathbb{C}$.

- If π_p is Steinberg there exists a newform $h \in S_2(\Gamma_0(p))$ such that $h \otimes \varkappa_p = g$, where \varkappa_p is the quadratic character of conductor p , and

$$\tilde{f} = f|_2[\alpha_p] = \sum a_\chi(g \otimes \chi) + ah,$$

where the sum is over all characters of conductor dividing p and $a_\chi, a \in \mathbb{C}$.

- If π_p is a ramified Principal Series there exists a non-quadratic character θ_p of conductor p and newforms $h \in S_2(\Gamma_0(p), \overline{\theta_p}^2)$, $\bar{h} \in S_2(\Gamma_0(p), \theta_p^2)$ such that $h \otimes \theta_p = g = \bar{h} \otimes \bar{\theta}_p$. Then

$$\tilde{f} = f|_2[\alpha_p] = \sum a_\chi(g \otimes \chi) + a_1 h + a_2 \bar{h},$$

where the sum is over all characters of conductor dividing p and $a_\chi, a_1, a_2 \in \mathbb{C}$.

Before proving the Theorem, recall the following result, which is a consequence of Serre's open image Theorem (or the Sato-Tate Conjecture).

Proposition 1.15. *Let $g \in S_2(\Gamma_0(p^2))$ be an eigenform with rational eigenvalues, without complex multiplication. Then the set of primes ℓ satisfying $\lambda_\ell = 0$ has zero density. In particular, given any nonzero class $a \bmod p$ we can find a prime number ℓ such that $\ell \equiv a \bmod p$ and $\lambda_\ell \neq 0$.*

Proof of Theorem 1.14. Assume first that f does not have CM. Let χ be a character of conductor dividing p , and let

$$F_\chi(f) = \sum_{\ell} \chi(\ell^{-1}) \frac{T_\ell(f)}{\lambda_\ell},$$

where the sum is over any set of representatives $\{\ell\}$ of elements in \mathbb{F}_p^\times satisfying $\lambda_\ell \neq 0$.

Claim: The sum does not depend on the choice of representatives.

Let ℓ, q be two relatively prime numbers such that $\ell \equiv q \bmod p$ and both λ_ℓ and λ_q are non-zero (they exist by Proposition 1.15). Then $\frac{T_\ell(f)}{\lambda_\ell}$ and $\frac{T_q(f)}{\lambda_q}$ are eigenforms for $S_2(\Gamma_{ns}^{\varepsilon/q^2})$, and have the same Hecke eigenvalues, so from multiplicity one, one is a multiple of the other. Applying T_r where r is a prime such that $\lambda_r \neq 0$, $(r : \ell q) = 1$, $r\ell \equiv 1 \bmod p$ and using that $T_{r\ell} = \mathcal{T}_{r\ell}$ we get the claim.

It is clear that the form f is a linear combination of the forms $F_\chi(f)$ (by the orthogonality relations of the characters), so we just need to relate the forms $F_\chi(f)|_2[\alpha_p]$ with the forms $g \otimes \chi$.

Let $q \neq p$ be any prime such that $\lambda_q \neq 0$. Without loss of generality, we can assume that ℓ is prime to q and that $\lambda_\ell \neq 0$. If this is not the case, we can choose $\ell' \equiv \ell$

(mod p) such that $\lambda_{\ell'} \neq 0$ and work with this prime instead. Using Diagram (3) we get

$$\begin{aligned} \tilde{T}_q(F_\chi(f)|_2[\alpha_p]) &= \sum_{\ell} \chi(\ell^{-1}) \tilde{T}_q \left(\frac{\tilde{T}_\ell(\tilde{f})}{\lambda_\ell} \right) = \sum_{\ell} \chi(\ell^{-1}) \frac{\tilde{T}_q \tilde{T}_\ell(\tilde{f})}{\lambda_\ell} = \\ &= \sum_{\ell} \chi(\ell^{-1}) \frac{\tilde{T}_{q\ell}(\tilde{f})}{\lambda_\ell} = \chi(q) \lambda_q \sum_{\ell} \chi((q\ell)^{-1}) \frac{\tilde{T}_{q\ell} \tilde{f}}{\lambda_{q\ell}} = \chi(q) \lambda_q F_\chi(f)|_2[\alpha_p]. \end{aligned}$$

Therefore, $F_\chi(f)|_2[\alpha_p]$ is an eigenform with the same eigenvalues as $g \otimes \chi$. Suppose now that $\lambda_q = 0$; we want to prove that $T_q(F_\chi(f)) = 0$ as well. It suffices to show that in such case $T_q(f) = 0$. Suppose this is not the case, i.e. that $\lambda_q = 0$ but $T_q(f) \neq 0$. Let r be a prime such that $r \equiv q \pmod{p}$ and $\lambda_r \neq 0$. Then, by multiplicity one, there exists a constant c such that $cT_q f = T_r f$. Applying a proper Hecke operator as before, we get a contradiction.

Then $F_\chi(f)|_2[\alpha_p]$ is a form in $S_2(\Gamma_0(p^2) \cap \Gamma_1(p))$ with the same eigenvalues as $g \otimes \chi$. If $g \otimes \chi$ turns out to be a newform, then one is a multiple of the other and we are done. If $g \otimes \chi$ is not new (for some χ), then π_p corresponds to a ramified principal series (there are exactly two conjugated characters for which $g \otimes \chi$ is old) or π_p is Steinberg (in which case $g \otimes \chi$ is old). In both cases, there exists a form h as in the statement, such that $F_\chi(f)|_2[\alpha_p]$ is a linear combination of $h(z)$ and $h(pz)$. But $\langle h(z), h(pz) \rangle = \langle h(z), h \otimes 1_p \rangle$, where 1_p is the non-primitive trivial character of conductor p . (note that by hypothesis $h \otimes 1_p$ is a twist of g). In all cases, depending on the local type of the representation π_p , the statement follows.

If f has CM, then $f = f \otimes \varkappa_p$. In particular, if n is not a square modulo p , $a_n = 0$. On the contrary, if n is a non-zero quadratic residue modulo p , we can find, as before, a prime ℓ such that $n \equiv \ell \pmod{p}$ and $\lambda_\ell \neq 0$. The same argument as in the previous case works, but considering the sum only over representatives of $\{\text{squares in } \mathbb{F}_p^\times\}$.

As before, it is easy to see that this definition does not depend on the representatives chosen and if we apply to this sum any T_n with n a non-square modulo p then $T_n F_\chi(f) = \lambda_n f = 0$, while if n is a square the same proof works. \square

Remark 1.16. If $f \in S_2(\Gamma_{ns}^{+, \varepsilon}(p))$ is an eigenform then $T_\ell f = \lambda_\ell f$ for $\ell \equiv -1 \pmod{p}$. In particular, if χ is an odd character, $F_\chi(f) = \sum_{\ell} \chi(\ell^{-1}) \frac{T_\ell(f)}{\lambda_\ell} = 0$, so all the non-zero coefficients in the linear combination of Theorem 1.14 are those corresponding to even characters.

Similarly, if $f \in S_2(\Gamma_{ns}^{-, \varepsilon}(p))$ (i.e. any matrix in the normalizer but not on the Cartan itself acts as -1), then it is easy to see that v_ℓ acts as -1 for $\ell \equiv -1 \pmod{p}$. Then $\lambda_\ell f = \mathcal{T}_\ell f = T_\ell v_\ell f = -T_\ell f$, which implies that $F_\chi(f) = \sum_{\ell} \chi(\ell^{-1}) \frac{T_\ell(f)}{\lambda_\ell} = 0$

whenever χ is even, so the non-zero coefficients in the linear combination of Theorem 1.14 are those corresponding to odd characters.

1.5. Fourier expansions. To compute the modular parametrization we need to compute the Fourier expansion, and find the appropriate normalization of it (which does not coincide with the one for classical modular forms). For that purpose, we first need to understand the action of the Galois group $\text{Gal}(\mathbb{C}/\mathbb{Q})$ on modular forms.

For $a \in \mathbb{Q}^2$ and $z \in \mathcal{H}$ define

$$f_a(z) = \frac{g_2(z, 1)g_3(z, 1)}{\Delta(z, 1)} \wp(a \begin{pmatrix} z \\ 1 \end{pmatrix}; z, 1),$$

where $\wp(-; \omega_1, \omega_2)$ is the classical Weierstrass function associated to the lattice $L = \langle \omega_1, \omega_2 \rangle$; $g_2(L) = 60G_4(L)$, and $g_3(L) = 140G_6(L)$ correspond to the lattice functions $G_{2n}(L) = \sum_{w \in L} \frac{1}{w^{2n}}$ (see Section 6.1 of [Shi94] for example). These functions satisfy $f_a(\gamma(z)) = f_{a\gamma}(z)$ for every $\gamma \in \text{SL}_2(\mathbb{Z})$. Let \mathcal{R}_p be the field of modular functions of level p , which by Proposition 6.1 of [Shi94] is

$$\mathcal{R}_p = \mathbb{C}(j, f_a \mid a \in (p^{-1}\mathbb{Z}^2)/\mathbb{Z}^2, a \notin \mathbb{Z}^2).$$

Let $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{Q}(\xi_p))$. Since the functions j, f_a have Fourier expansions belonging to $\mathbb{Q}(\xi_p)$ we have that if $f = cj + \sum_a c_a f_a$,

$$\sigma(f) = \sigma(c)j + \sum_a \sigma(c_a) f_a.$$

Choose representatives β_j for $\pm\Gamma(p) \backslash \Gamma_{ns}^\varepsilon(p)$ such that $b \equiv 0 \pmod{\ell}$ (the number ℓ is auxiliary and we will choose it in different ways depending on our purposes). Then we can easily see that the field of modular functions for the non-split Cartan is the subfield of \mathcal{R}_p given by

$$\mathcal{R}_{ns}^\varepsilon(p) = \mathbb{C}(j, \sum_i f_{a\beta_i}).$$

Clearly it does not depend on the representatives chosen. In order to understand the action of $\text{Gal}(\mathbb{C}/\mathbb{Q})$ on modular forms for the Cartan subgroup, it is enough to understand the effect of $\text{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ on them. Let ξ_p a fixed p -th root of unity, and consider the automorphism σ_ℓ given by $\sigma_\ell(\xi_p) = \xi_p^{\ell^{-1}}$. Extend this automorphism to \mathbb{C} and call it σ . By theorem 6.6 of [Shi94] and Theorem 3 (Chapter 6, section 3) of [Lan87] this automorphism acting on the meromorphic modular functions f_a , is given by $f_{a\alpha_{\ell^{-1}}}$.

Proposition 1.17. *Let f be a meromorphic form of weight 0 for $\Gamma_{ns}^\varepsilon(p)$. Let $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{Q})$ such that $\sigma = \sigma_\ell$ when restricted to $\mathbb{Q}(\xi_p)$. Then $\sigma(f)$ is a meromorphic form of weight 0 for $\Gamma_{ns}^{\varepsilon\ell^2}(p)$.*

Proof. Since f is a meromorphic form of weight 0, we have

$$f = \lambda j + \sum_a \lambda_a \left(\sum_i f_{a\beta_i} \right).$$

Then

$$\sigma(f) = \sigma(\lambda)j + \sum_a \sigma(\lambda_a) \left(\sum_i f_{a\beta_i\alpha_{\ell-1}} \right).$$

The action on each f_a can be written as $f_{a\beta_i\alpha_{\ell-1}} = f_{a\alpha_{\ell-1}(\alpha_{\ell}\beta_i\alpha_{\ell-1})}$. Since $(\alpha_{\ell}\beta_i\alpha_{\ell-1})$ are representatives for $\pm\Gamma(p)\backslash\Gamma_{ns}^{\varepsilon\ell^2}(p)$ we see that $\sigma(f)$ is an automorphic form for the required group. \square

Remark 1.18. Although the last result is only stated for weight 0 forms, it also applies to modular forms of other weights by dividing the form by an appropriate Eisenstein series with rational Fourier coefficients.

If $f \in S_2(\Gamma_{ns}^{\varepsilon})$ is an eigenform for the Hecke operators then we know that $\sigma(f) \in S_2(\Gamma_{ns}^{\varepsilon\ell^2})$. We want to prove that $\sigma(f)$ is an eigenform for its respective Hecke operators with Galois conjugate eigenvalues.

Proposition 1.19. *Let f be a meromorphic modular function for $\Gamma_{ns}^{\varepsilon}(p)$. Then $\sigma_q(v_{\ell}^{\varepsilon}(f)) = v_{\ell}^{\varepsilon q^2}(\sigma_q(f))$.*

Proof. Choose A_{ℓ}^{ε} in such a way that its $(1, 2)$ entry is divisible by q . It is easy to see that $\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} A_{\ell}^{\varepsilon} \begin{pmatrix} 1 & 0 \\ 0 & 1/q \end{pmatrix}$, which belongs to $\mathrm{SL}_2(\mathbb{Z})$ by our choice of A_{ℓ}^{ε} , gives the same action on the f_a as $A_{\ell}^{\varepsilon q^2}$ (since both matrices are easily seen to be equivalent modulo p). This proves the result on weight zero forms. For general weights, the same argument as in Remark 1.18 applies. \square

Corollary 1.20. *With the previous notation, $\mathcal{T}_q^{\varepsilon\ell^2}(\sigma_{\ell}(f)) = \sigma_{\ell}(\mathcal{T}_q^{\varepsilon}(f))$.*

Proof. This follows from the previous Proposition and the fact that σ_{ℓ} commutes with T_q (this is easily obtained by looking at the action on q -expansions). \square

Recall from Theorem 1.12 that the eigenforms in $S_2(\Gamma_{ns}^{\varepsilon\ell^2}(p))$ are in correspondence with eigenforms in $S_2(\Gamma_0(p^2))^{new}$. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $S_2(\Gamma_0(p^2))$ and commutes with Hecke operators. If σ is an element of such group and h is a modular form, we denote this action by h^{σ} .

If f is an eigenform in $S_2(\Gamma_{ns}^{\varepsilon\ell^2}(p))$ which corresponds to a form $g \in S_2(\Gamma_0(p^2))^{new}$, we denote by f^{σ} any non-zero eigenform that corresponds to the form g^{σ} .

Corollary 1.21. *With the previous notations, let $f \in S_2(\Gamma_{ns}^{\varepsilon}(p))$ be an eigenform. Then there exists c such that $T_{\ell}f = c\sigma_{\ell-1}(f^{\sigma_{\ell}})$.*

Proof. By Proposition 1.10, $T_\ell(f)$ is an eigenform in $S_2\left(\Gamma_{ns}^{\varepsilon/\ell^2}(p)\right)$ with the same eigenvalues as f . By Corollary 1.20, $\sigma_{\ell^{-1}}(f^{\sigma_\ell})$ is an eigenform whose eigenvalues are $\sigma_{\ell^{-1}}$ applied to that of f^{σ_ℓ} , which equals that of f as well. The result now follows from multiplicity one. \square

With this setup we can give a first statement on the coefficient field of eigenforms for the Cartan subgroup.

Theorem 1.22. *Let $f \in S_2(\Gamma_{ns}^\varepsilon(p))$ be an eigenform which has the same eigenvalues as a rational newform $g \in S_2(\Gamma_0(p^2))$. Normalize \tilde{f} such that the first Fourier coefficient is rational. Then \tilde{f} (and f) have a q -expansion belonging to $\mathbb{Q}(\xi_p)$.*

Proof. Let $\ell \equiv 1 \pmod{p}$ be a prime number such that $\lambda_\ell \neq 0$, and $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{Q}(\xi_p))$ arbitrary. By Corollary 1.21 and the fact that $g^{\sigma_\ell} = g$ (so $f^{\sigma_\ell} = f$), there is a c such that

$$T_\ell f = c\sigma_{\ell^{-1}}(f).$$

We know that $T_\ell f = \lambda_\ell f$ (by Corollary 1.6). Looking at the first Fourier coefficient (which is rational), we get that $c = \lambda_\ell$ and hence $f = \sigma_{\ell^{-1}}(f)$. Since $\sigma_{\ell^{-1}} \in \text{Gal}(\mathbb{C}/\mathbb{Q}(\xi_p))$ is arbitrary it follows that the q -expansion of f lies in the desired extension. \square

Remark 1.23. If we start with a newform g with coefficient field F , then the same result proves that the coefficient field of f is contained in $F(\xi_p)$.

Remark 1.24. By the orthogonality relations of the characters it follows that under the previous normalization, the coefficient a_{χ_0} attached to g in the linear combination of \tilde{f} in Theorem 1.14 belongs to $\mathbb{Q}(\xi_p)$, and the other coefficients belong to $\mathbb{Q}(\xi_p, \xi_{p-1})$.

1.6. Rational modular forms. The curve $X_{ns}^\varepsilon(p)$ is defined over \mathbb{Q} and has $(p-1)$ cusps which are all defined over $\mathbb{Q}(\xi_p)$ and are Galois conjugate of each other (see [Ser97] Appendix 5). If $\sigma_\ell \in \text{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$, then there exists $A \in \text{SL}_2(\mathbb{Z})$ such that $\sigma_\ell(\infty) = A \cdot \infty$. The matrix A can be taken to be equal to A_ℓ^ε as defined before Lemma 1.8. Recall that if f is a weight k modular form, its Fourier expansion at the cusp $A_\ell^\varepsilon \infty$ is given by the Fourier expansion of the form $f|_k[(A_\ell^\varepsilon)^{-1}]$ at the infinity cusp.

Let $\mathcal{F}_{ns}^\varepsilon(p)$ be the field of rational meromorphic functions for the Cartan non-split group $\Gamma_{ns}^\varepsilon(p)$, i.e. $\mathcal{F}_{ns}^\varepsilon(p) := \mathbb{Q}(j, \sum_i f_{a\beta_i})$. Combining Proposition 1.17 with Lemma 1.8, it is easy to see that $\mathcal{F}_{ns}^\varepsilon(p)$ consists of all meromorphic functions invariant for the Cartan non-split, whose q -expansion at infinity belongs to $\mathbb{Q}(\xi_p)$ and such that the Fourier expansion at $\sigma_\ell(\infty)$ equals $\sigma_{\ell^{-1}}(f)$. As in Remark 1.18, the same argument applies to other weights.

Definition 1.25 (Rational Modular Forms). A form $f \in S_2(\Gamma_{ns}^\varepsilon(p))$ is called *rational* if its q -expansion at every cusp belongs to $\mathbb{Q}(\xi_p)$ and the expansion at the cusp $\sigma_\ell(\infty)$ equals that of $\sigma_{\ell-1}(f)$ at the infinity cusp for all $\ell \in \mathbb{F}_p^*$.

Recall that if X is a curve defined over a field K , a differential form defined over K is a differential form which is locally of the form $f dg$, where f and g are meromorphic forms defined over K .

Proposition 1.26. *If $f \in S_2(\Gamma_{ns}^\varepsilon(p))$ is rational, it defines a rational meromorphic differential form $f(q) \frac{dq}{q}$ on $X_{ns}^\varepsilon(p)$, where $q = e^{\frac{2\pi iz}{p}}$.*

Proof. Note that

$$f(q) \frac{dq}{q} = \frac{2\pi i}{p} f(z) dz = \frac{f(z)}{\frac{pj'(z)}{2\pi i}} dj.$$

Since j belongs to $\mathcal{F}_{ns}^\varepsilon(p)$ and $\frac{pj'}{2\pi i}$ is a rational weight 2 meromorphic for $\mathrm{SL}_2(\mathbb{Z})$, their quotient lies in $\mathcal{F}_{ns}^\varepsilon(p)$ as claimed. \square

Theorem 1.22 says that if f is an eigenform with rational eigenvalues, normalizing the form f in a way that its first coefficient is rational gives a form whose q -expansion belongs to $\mathbb{Q}(\xi_p)$. If we multiply the form by any constant in such field, the same holds. So the problem is the following: what is the right way to normalize f ?

Theorem 1.27. *Let $f \in S_2(\Gamma_{ns}^\varepsilon(p))$ be an eigenform with rational eigenvalues. Then there exists a constant $c \in \mathbb{Q}(\xi_p)$ such that cf is rational, and this constant is unique up to multiplication by a non-zero rational number.*

Proof. It is clear that c , if exists, is unique up to a rational constant. By Proposition 1.9, it is enough to prove that for all prime numbers ℓ

$$T_\ell(cf) = \lambda_\ell \sigma_{\ell-1}(cf).$$

To prove existence, we consider two separate cases depending on whether the coefficient a_{χ_0} corresponding to g in the linear combination of f is zero or is non-zero.

• If $a_{\chi_0} \neq 0$, it belongs to $\mathbb{Q}(\xi_p)$ by Remark 1.24, so we take $c = \frac{1}{a_{\chi_0}}$. We know that both $T_\ell f$ and $\sigma_{\ell-1}(f)$ are forms in the same Cartan with the same eigenvalues for the Hecke operators outside p , so one is a multiple of the other, i.e. there exists a constant k such that

$$T_\ell f = k \sigma_{\ell-1}(f).$$

Extend the automorphism $\sigma_{\ell-1}$ to the extension $\mathbb{Q}(\xi_p, \xi_{p-1})$, trivially in ξ_{p-1} . By Theorem 1.14

$$\tilde{f} = \sum a_\chi (g \otimes \chi) + a_1 h + a_2 \bar{h}.$$

Let μ_ℓ denote the eigenvalue of T_ℓ acting on h . Applying \tilde{T}_ℓ and $\sigma_{\ell-1}$ to this equality we get

$$\sum_x a_\chi \lambda_\ell \chi(\ell) (g \otimes \chi) + \mu_\ell a_1 h + \bar{\mu}_\ell a_2 \bar{h} = \tilde{T}_\ell \tilde{f} = k \sigma_{\ell-1}(\tilde{f})$$

$$k \sigma_{\ell-1}(\tilde{f}) = k \left(\sum_x \sigma_{\ell-1}(a_\chi) (g \otimes \chi) + \sigma_{\ell-1}(a_1) h + \sigma_{\ell-1}(a_2) \bar{h} \right).$$

Since the functions $g \otimes \chi, h, \bar{h}$ are linearly independent, the result follows by looking at the coefficient a_{χ_0} (which is rational and non-zero).

• If $a_{\chi_0} = 0$, the argument is a little more subtle. We start normalizing f such that its first non-zero coefficient is rational, so Theorem 1.22 implies that the q -expansion belongs to $\mathbb{Q}(\xi_p)$. We have that for each ℓ , there exists $c_\ell \in \mathbb{Q}(\xi_p)$, which only depends on the class of ℓ modulo p , such that $T_\ell f = \lambda_\ell c_\ell \sigma_{\ell-1}(f)$. We need to find a non-zero $c \in \mathbb{Q}(\xi_p)$ such that $T_\ell(c f) = \lambda_\ell \sigma_{\ell-1}(c f)$, ie, $c_\ell = \sigma_{\ell-1}(c)/c$.

Let ℓ be a generator of \mathbb{F}_p^* such that $\lambda_\ell \neq 0$ (if g has CM take the square of a generator). Let $\ell_i, 1 \leq i \leq p-1$, be distinct primes in the same class of ℓ modulo p such that $\lambda_{\ell_i} \neq 0$. Then $\prod_{i=1}^{p-1} \ell_i \equiv 1 \pmod{p}$ and

$$(\prod \lambda_{\ell_i}) f = \mathcal{T}_{\prod \ell_i}(f) = T_{\prod \ell_i}(f) = T_{\ell_1} \circ \dots \circ T_{\ell_{p-1}}(f) = (\prod \lambda_{\ell_i}) \text{Nm}(c_\ell) f.$$

Then $\text{Nm}_{\mathbb{Q}(\xi_p)}^{\mathbb{Q}}(c_\ell) = 1$ and by Hilbert theorem 90 there exists $c \in \mathbb{Q}(\xi_p)$ that satisfies $c_\ell = \sigma_{\ell-1}(c)/c$. Since ℓ is a generator of \mathbb{F}_p^* it is easy to see that c satisfies $c_q = \sigma_{q-1}(c)/c$ for every q prime to p . \square

Proposition 1.28. *With our normalization, the coefficients a_χ satisfy for all primes $\ell \neq p$ that $\sigma_{\ell-1}(a_\chi) = a_\chi \chi(\ell)$ where $\sigma_{\ell-1} \in \text{Gal}(\mathbb{Q}(\xi_p, \xi_{p-1})/\mathbb{Q}(\xi_{p-1}))$.*

Proof. Follows at once from Theorem 1.27. \square

Remark 1.29. Let $f \in S_2(\Gamma_{ns}^+(p))$. If $\ell \equiv -1 \pmod{p}$, σ_ℓ corresponds to complex conjugation in $\mathbb{Q}(\xi_p)$. Since the characters involved in the sum are even characters, $\chi(\ell) = 1$, and by the last Proposition σ_ℓ acts trivially. This implies that the coefficients of the modular forms in fact lie in $\mathbb{Q}(\xi_p + \xi_p^{-1}) = \mathbb{Q}(\xi_p^+)$. Similarly, if $f \in S_2(\Gamma_{ns}^-(p))$ the coefficients will be purely imaginary.

Note that even for a rational modular form, it is not clear how to choose the rational multiple of it which should correspond to “ $a_1 = 1$ ” in the classical case. The best one can do is to choose the coefficients to be algebraic integers and have no common rational integer factor.

Definition 1.30. Let $f \in S_2(\Gamma_{ns}^e(p))$ be a rational eigenform with rational eigenvalues. We normalize f such that the following properties hold:

- The Fourier expansion of f has algebraic integer coefficients.

- If $n \in \mathbb{Z}$ and $n \geq 2$, $\frac{f}{n}$ does not have integral coefficients.

Clearly there exists a unique (up to multiplication by ± 1) normalization satisfying the above conditions. The choice of the sign is not clear.

Remark 1.31. If $f \in S_2(\Gamma_{ns}^\varepsilon(p))$ is a rational normalized eigenform with rational eigenvalues then $\sigma_q f \in S_2(\Gamma_{ns}^{\varepsilon q^2}(p))$ is a rational normalized eigenform with rational eigenvalues. Moreover since f is rational, we must have $\sigma_q f = f|_k[(A_q^\varepsilon)]$. (See Definition 1.25).

Recall that if we start with an eigenform $f \in S_2(\Gamma_{ns}^\varepsilon(p))$ (associated to a newform g of level p^2) we can do the Eichler-Shimura construction (Theorem 7.9 of [Shi94]) and associate to f the abelian variety $\mathcal{A}_f^\varepsilon := \text{Jac}(X_{ns}^\varepsilon(p))/(I_f \text{Jac}(X_{ns}^\varepsilon(p)))$ where I_f is the kernel of the morphism from $R(\Gamma_{ns}^\varepsilon(p), \Delta_{ns}^\varepsilon(p)) \rightarrow \mathbb{Z}$ which is given by sending $\mathcal{T}_\ell^\varepsilon$ to the eigenvalue λ_ℓ of f . This can be summarized with the following diagram

$$\begin{array}{ccc} X_{ns}^\varepsilon(p) & \xrightarrow{i} & \text{Jac}(X_{ns}^\varepsilon(p)) \\ & \searrow \text{dotted} & \downarrow \\ & & \mathcal{A}_f^\varepsilon \end{array}$$

where i is the map sending P to $(P) - (\infty)$ and the vertical map (which is clearly rational) is given by the classical Abel-Jacobi map obtained by integrating the differential form $f(q) \frac{dq}{q}$ and its Galois conjugates over cycles. Since we are considering the case where all the eigenvalues λ_ℓ are rational the abelian variety $\mathcal{A}_f^\varepsilon$ is of dimension 1, and by Theorem 1.12 must be isogenous to the elliptic curve over \mathbb{Q} corresponding to the classical rational newform g . Such elliptic curve will be referred as the optimal quotient of $\text{Jac}(X_{ns}^\varepsilon(p))$ (note that it might not be isomorphic to the strong Weil curve attached to g).

Since the cusps of the Cartan curve are defined over $\mathbb{Q}(\xi_p)$ (and are Galois conjugates over that field) the map i will not be defined over \mathbb{Q} . Nevertheless, we can solve this problem by averaging over all the conjugates of this map; that is, we consider the following diagram

$$\begin{array}{ccc} X_{ns}^\varepsilon(p) & \xrightarrow{\iota} & \text{Jac}(X_{ns}^\varepsilon(p)) \\ & \searrow \text{dotted} \Phi_p^\varepsilon & \downarrow \\ & & \mathcal{A}_f \end{array}$$

where ι is the map sending P to $\sum_{\sigma_\ell \in \text{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})} (P) - (\sigma_\ell(\infty))$. Note that this is the right and natural definition to make a map defined over \mathbb{Q} out of i . Therefore, the dot map (the so called *modular parametrization*) is defined over \mathbb{Q} .

Remark 1.32. If $f \in S_2(\Gamma_{ns}^+(p))$, since the normalizer has $(p-1)/2$ cusps, all defined and conjugated over the maximal real subfield of $\mathbb{Q}(\xi_p)$, we will take the average in the definition of ι over all such cusps.

Lemma 1.33. *Let q be a number not divisible by p . Then $\mathcal{A}_f^\varepsilon = \mathcal{A}_f^{\varepsilon q^2}$.*

Proof. It is enough to see that the lattice of periods of f is the same as the lattice of periods of $\sigma_q(f)$ which is a rational eigenform for $S_2(\Gamma_{ns}^{\varepsilon q^2}(p))$ (Remark 1.31). Let D be the trivial cycle $\{\tau, M^\varepsilon \tau\}$ with $M^\varepsilon \in \Gamma_{ns}^\varepsilon(p)$. Integrating f over that cycle we get

$$\int_{\tau}^{M^\varepsilon \tau} f(q) \frac{dq}{q}.$$

By changing variables $z \mapsto [A_q^\varepsilon]^{-1}z$ we obtain

$$\int_{[A_q^\varepsilon]^{-1}\tau}^{[A_q^\varepsilon]^{-1}M^\varepsilon \tau} f|_k[(A_q^\varepsilon)] \frac{dq}{q} = \int_{[A_q^\varepsilon]^{-1}\tau}^{[A_q^\varepsilon]^{-1}M^\varepsilon [A_q^\varepsilon][A_q^\varepsilon]^{-1}\tau} \sigma_q(f) \frac{dq}{q}.$$

This expression is the integral of $\sigma_q(f)$ over the cycle $\{\tau', [A_q^\varepsilon]^{-1}M^\varepsilon [A_q^\varepsilon] \tau'\}$, where $\tau' = [A_q^\varepsilon]^{-1}\tau$. Notice that since $[A_q^\varepsilon]^{-1}M^\varepsilon [A_q^\varepsilon] \in \Gamma_{ns}^{\varepsilon q^2}(p)$ we have a trivial cycle in $\text{Jac}(X_{ns}^{\varepsilon q^2}(p))$. □

Let E denote the elliptic curve \mathcal{A}_f (which does not depend on ε). If ω_E is a holomorphic differential on \mathbb{C}/Λ_E , then by multiplicity one, its pullback under Φ_p^ε is a constant multiple of $f(q) \frac{dq}{q}$, where $q = e^{\frac{2\pi iz}{p}}$. Such constant will be called the Manin constant c_ε . Since E, Φ_p^ε and $f(q) \frac{dq}{q}$ are rational, the Manin constant must be a rational number. Finally is not difficult to see that the Manin constant does not depend on ε so we can speak of the Manin constant c .

Proposition 1.34. *Let Λ_f be the lattice attached to f and c the Manin constant. Let $\Phi_\omega : \mathbb{C}/\Lambda_f \rightarrow E$ be the Weierstrass uniformization. Then $\Phi_p^\varepsilon(\tau) = \Phi_\omega(z_\tau)$, where*

$$z_\tau = c \left(\frac{2\pi i}{p} \left(\sum_{\sigma_\ell \in \text{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})} \int_{\infty}^{A_\ell^{-1}\tau} \sigma_\ell(f^\varepsilon)(z) dz \right) \right)$$

Proof. This follows from Proposition 2.11 of [Dar04] and the identity

$$\int_{\sigma_\ell(\infty)}^{\tau} f(q) \frac{dq}{q} = \int_{\infty}^{A_\ell^{-1}\tau} f|_2[A_\ell](q) \frac{dq}{q} = \int_{\infty}^{A_\ell^{-1}\tau} \sigma_\ell(f(q)) \frac{dq}{q}.$$

□

2. GENERAL LEVELS

In this section we generalize the previous results to more general conductors. Thanks to the Chinese Remainder Theorem, the theory works exactly the same as in the p^2 case. Let E/\mathbb{Q} be an elliptic curve of conductor N^2m with $\gcd(N : m) = 1$, and $N = p_1 \dots p_r$ (p_i distinct odd primes). By Shimura-Taniyama, it corresponds to an eigenform $g \in S_2^{new}(\Gamma_0(N^2m))$ with rational eigenvalues. Let ε_i be a non-square modulo p_i , for $i = 1, \dots, r$ and let $\vec{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_r)$. Let $\Gamma_{ns}^{\vec{\varepsilon}}(N, m) = \cap_{i=1}^r \Gamma_{ns}^{\varepsilon_i}(p_i) \cap \Gamma_0(m)$ and consider the curve $X_{ns}^{\vec{\varepsilon}}(N, m) = \Gamma_{ns}^{\vec{\varepsilon}}(N, m) \backslash \mathcal{H}^*$.

The moduli interpretation is a mix of the classical one and the one of the previous section. We consider tuples $[E, \psi, \phi_1, \dots, \phi_r]$, where E/\mathbb{C} is an elliptic curve, $\psi : E \rightarrow E'$ is a cyclic degree m isogeny (or equivalently a cyclic subgroup of order m), and $\phi_i \in \text{End}_{\mathbb{F}_{p_i}}(E[p_i])$ is such that ϕ_i^2 corresponds to multiplication by ε_i for $i = 1, \dots, r$. A computation similar to that of Proposition 1.1 shows that $X_{ns}^{\vec{\varepsilon}}(N, m)$ represents the moduli problem stated.

We have the following generalization of Theorem 1.12.

Theorem 2.1. *Jac($X_{ns}^{\vec{\varepsilon}}(N, m)$) is isogenous over \mathbb{Q} to $\text{Jac}(X_0(N^2m))^{N^2\text{-new}}$ by a Hecke equivariant map.*

Proof. Let $X(Nm)$ be the modular curve which is the compactified moduli space of triples $(E/S/\mathbb{Q}, \phi)$, where S is a \mathbb{Q} scheme, E/S is an elliptic curve and $\phi : (\mathbb{Z}/Nm)_{\mathbb{S}}^2 \mapsto E[Nm]$ is an isomorphism of group schemes over S . The group $\text{GL}_2(\mathbb{Z}/Nm)$ acts on the right on $X(Nm)$. If Γ is any subgroup of $\text{GL}_2(\mathbb{Z}/Nm)$, one can consider the quotient $X(Nm)/\Gamma$ via an appropriate moduli interpretation. We are interested in the following two subgroups (as subgroups of $\text{GL}_2(\mathbb{Z}/Nm)$): $\Gamma_{ns}^{\vec{\varepsilon}}(N, m)$ and $\tilde{\Gamma} := \cap_{i=1}^r T(p_i) \cap \Gamma_0(m)$, where $T(p)$ is the standard maximal torus modulo p (consisting of diagonal matrices). The quotients correspond respectively to $X_{ns}^{\vec{\varepsilon}}(N, m)$ and $X_0(N^2m)$ (as in [Edi96], (1.0.4)).

Using an inductive argument, it is enough to prove that the Jacobian of the quotient by $\Gamma_1 = \cap_{i=1}^r T(p_i) \cap \Gamma_0(m)$ is isomorphic to the p_1 -new part of the quotient by $\Gamma_2 = \cap_{i=2}^r T(p_i) \cap \Gamma_0(p_1^2m)$. But in this case, one can prove Proposition 1.2 of [Edi96] in exactly the same way, where now the subgroups of such paper correspond to the local components at p_1 of our subgroups (since both groups are the same at all the other primes). Then the same formalism as Theorem 1.3 (of [Edi96]) proves our claim. \square

The previous theorem, together with the comments in the proof of Theorem 1.12, imply that there exists $f \in S_2(\Gamma_{ns}^{\vec{\varepsilon}}(N, m))$ with the same eigenvalues for the Hecke operators $\mathcal{F}_\ell^{\vec{\varepsilon}}$ as g outside the primes p_i . The theory works the same as in the level p^2 case, with some minor changes.

The geometric definition of Hecke operators is the same as before. We consider all degree n isogenies (for n prime to Nm) and consider the same action on each ϕ_i and, as in the classical case, the image of the cyclic subgroup by our isogeny.

The algebraic definition is also the same, and the operator $v_\ell^{\vec{\varepsilon}}$, as well as coset representatives, are defined via a matrix $A_\ell^{\vec{\varepsilon}} \in \mathrm{SL}_2(\mathbb{Z})$ which satisfies the corresponding congruence modulo all the prime numbers p_i and such that they belong to $\Gamma_0(m)$.

Note that in particular $\sigma_{\ell-1}$ and T_ℓ will send modular forms for $\Gamma_{ns}^{\vec{\varepsilon}}(N, m)$ to modular forms for $\Gamma_{ns}^{\vec{\varepsilon}/\ell^2}(N, m)$, and all the results from the previous Section generalize trivially. In particular we have the analogue of Theorem 1.14.

Theorem 2.2. *Let $f \in S_2(\Gamma_{ns}^{\vec{\varepsilon}}(N, m))$ be an eigenform. Then there exists eigenforms $h_i \in S_2(\Gamma_0(N_i m), \chi_i)$, with $N_i \mid N^2$, and χ_i a character of conductor N^2/N_i such that*

$$\tilde{f} = \sum a_\chi(g \otimes \chi) + \sum_i a_i^1 h_i + a_i^2 \bar{h}_i,$$

where the first sum is over all characters of conductor dividing N .

Proof. The proof is similar to that of Theorem 1.14. The CM case works exactly the same. If f does not have CM, we look at the local representations of our form g . Let p be a prime dividing N . If g is supercuspidal at p , then all of its twists by characters of conductor p have the same level as g (but with a character). If g is a ramified principal series or Steinberg at p , then there exists a twist by a character χ_p of it belonging to $S_2\left(\Gamma_0\left(\frac{N^2}{p}m, \chi_p^2\right)\right)$ (note that this is true locally, but since the class number of \mathbb{Q} is one, and there are no units, all local characters can be extended to global characters). Then we take $\chi_i = \prod_p \chi_p$ and h_i the new form attached to $g \otimes \chi_i$. Note that for each prime at which the representation is a ramified Principal Series we have two choices of the character (χ_p ad $\bar{\chi}_p$) giving us also $\bar{\chi}_i = \prod_p \bar{\chi}_p$ and \bar{h}_i the newform associated to $g \otimes \bar{\chi}_i$. Now the same proof as in Theorem 1.14 applies. \square

Using this Theorem we can also compute the Fourier expansion as in the p^2 case. Now the coefficient field will be $\mathbb{Q}(\xi_{p_1}, \dots, \xi_{p_r})$, whose Galois group is isomorphic to $\prod_i \mathbb{F}_{p_i}^\times$ and the modular parametrization $\Phi_N^{\vec{\varepsilon}}$ map can be written in the form $\Phi_\omega(z_\tau)$ where

$$(4) \quad z_\tau = \frac{2\pi i}{N} \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})} \int_\infty^{A_\sigma^{-1}\tau} \sigma(f^{\vec{\varepsilon}})(z) dz.$$

Using the Fourier expansion for $f^{\vec{\varepsilon}}$, we can calculate the integral numerically to arbitrary precision. Recall that the convergence of such integral is exponential depending on the imaginary part of the point in the upper half plane.

Summing up, we have obtained a modular parametrization

$$(5) \quad \Phi_N^{\vec{e}} : X_{ns}^{\vec{e}}(N, m) \rightarrow E(\mathbb{C})$$

defined over \mathbb{Q} .

We make the following observation about the Manin constant, which is supported by the evidence shown in the examples.

Conjecture 2.3. The Manin constant belongs to $\mathbb{Z}[1/N]$.

This conjecture should follow from similar arguments as exposed in [Maz78].

3. COMPUTATIONAL DIGRESSION

In order to compute explicitly the Fourier expansion of \tilde{f} , we need to write it as in Theorem 2.2. For that purpose, first we need to compute the local type of each prime dividing the conductor of E . This can be done either by looking at the reduced curve and the field where it gets semistable reduction or considering twists, as in [Pac13].

If there are some ramified principal series primes, one can compute the form h from the elliptic curve (see Appendix A).

Proposition 3.1. *Let $g_1, g_2 \in S_2(\Gamma_0(N^2m))$ be normalized newforms whose eigenvalues coincide in the set $\{n \in \mathbb{N} : n \equiv 1 \pmod{N}\}$. Then there exists $N' \mid N$ such that $g_1 = g_2 \otimes \chi_{N'}$.*

Proof. Suppose first that $N = p$ and $m = 1$. Let μ_n and λ_n the eigenvalues of g_1 and g_2 respectively. Furthermore assume that g_2 does not have CM (if it has CM the proof is similar).

Claim: $\mu_n = 0$ if and only if $\lambda_n = 0$. In particular this tells us that g_1 is not CM (since g_2 is not CM).

Proof of Claim: If $\mu_n = 0$ then by Proposition 1.15 we can find a prime $\ell \nmid n$, with $\ell n \equiv 1 \pmod{p}$ and $\lambda_\ell \neq 0$. Then $\lambda_\ell \lambda_n = \lambda_{\ell n} = \mu_{\ell n} = \mu_n \mu_\ell = 0$. Since λ_ℓ is not equal to zero it follows that $\lambda_n = 0$ as claimed.

For a a positive integer such that $\lambda_a \neq 0$, define the constant $c(a)$ such that $\lambda_a = c(a)\mu_a \neq 0$. The function $c(a)$ satisfies:

- (1) It depends only on a modulo p .
- (2) It is multiplicative, i.e. $c(a_1 a_2) = c(a_1)c(a_2)$.

To prove (1), let $a' \equiv a \pmod{p}$, so that $\lambda_{a'} = c(a')\mu_{a'}$. Fix such a' and choose ℓ such that $\mu_\ell \neq 0$, $(\ell : aa') = 1$ and $\ell a \equiv 1 \pmod{p}$. Then, as before, $\lambda_\ell \lambda_a = \mu_\ell \mu_a$, so $\lambda_\ell = c(a)^{-1} \mu_\ell \neq 0$. Similarly, $\lambda_\ell \lambda_{a'} = \mu_\ell \mu_{a'}$, so $\lambda_{a'} = c(a)\mu_{a'}$ as claimed.

To prove (2), we can assume that $\gcd(a_1, a_2) = 1$, and in this case, choosing n_1, n_2 inverses for a_1 and a_2 modulo p respectively with $\lambda_{n_i} \neq 0$, a similar computation gives the result.

In particular, if ℓ is a prime number which generates \mathbb{F}_p^* and such that $\lambda_\ell \neq 0$, $c(\ell^i) = c(\ell)^i$ implying that $c(\ell)$ is a $(p-1)$ -th root of unity. It is easy to see that this relation implies that g_2 is a twist of g_1 by a character of conductor dividing p . Since both are forms in $S_2(\Gamma_0(p^2))$ the only possibilities are $g_1 = g_2$ or $g_1 = g_2 \otimes \varkappa_p$ as claimed. The general case is an easy application of the Chinese Remainder Theorem. \square

Suppose we have all the forms of the linear combination of Theorem 2.2 (which span a space S), and we need to find the coefficients in such combination in order for the form to be invariant under $\Gamma_{ns}^\varepsilon(N, m)$. These forms are clearly invariant under $\Gamma(N) \cap \Gamma_0(m)$, so we have to ask for invariance under $\Gamma_{ns}^\varepsilon(N, m) / (\Gamma(N) \cap \Gamma_0(m))$. For each prime p dividing N we have that $\Gamma_{ns}^\varepsilon(p) / \Gamma(p) \cong \mathbb{Z}/(p+1)$. Then, by the Chinese Remainder Theorem we have that $\Gamma_{ns}^\varepsilon(N, m) / (\Gamma(N) \cap \Gamma_0(m)) \cong \prod_{p|N} \mathbb{Z}/(p+1)$. Choose generators for that group and several points in the upper half plane. We know that \tilde{f} is invariant for those matrices (conjugated by α_N^{-1}), so we evaluate h and its twists at the chosen points and impose these extra invariance conditions (which corresponds to a linear system). What is the dimension of this invariant subspace?

Proposition 3.2. *Suppose that g has no CM, and let a, b, c be the number of primes p dividing N such that the corresponding local representation π_p is: supercuspidal, ramified principal series or Steinberg respectively. The subspace of S generated by forms invariant for the Cartan group is of dimension 2^{a+b} .*

Proof. Since all the forms in the linear combination of Theorem 2.2 are eigenforms with the same Hecke eigenvalues in the set $\{n \in \mathbb{N} : n \equiv 1 \pmod{N}\}$, Proposition 3.1 tells us that the eigenforms which are solutions of our linear system are in correspondence with g and its quadratic twists which do not lower the level. Let p be a prime dividing N . If π_p is supercuspidal or ramified principal series then both g and $g \otimes \varkappa_p$ are newforms with the same level, so we have a dimension 2 subspace. If π_p is Steinberg then $g \otimes \varkappa_p$ is not new, so we can distinguish between g and $g \otimes \varkappa_p$. Applying these observations to each prime dividing N the result follows by the Chinese Remainder Theorem. \square

Suppose the form g has some supercuspidal or ramified principal series primes. Then we want to compute the 1- dimensional subspace corresponding to f . Here is a way to do it:

- Suppose that π_p is supercuspidal. Let ϵ_p denote the local sign at p .

Claim: if $\epsilon_p = 1$ then in the linear combination of Theorem 2.2 for g only twists of g with characters having even p -part are involved, while for $g \otimes \varkappa_p$ only twists of g

by characters with odd p -part are involved. If $\epsilon_p = -1$, the situation is the opposite one.

Proof of claim: Recall from Remark 1.16 that if $\epsilon_p = 1$ (resp. $\epsilon_p = -1$) then only twists of g with even p -part (resp. odd p -part) are in the sum. By Corollary 3.3 of [Pac13], the local sign at p changes while twisting g by \varkappa_p like $-\left(\frac{-1}{p}\right) = -\varkappa_p(-1)$. Then the variation of the sign at p of the characters involved in the combination for g and $g \otimes \varkappa_p$ (as twists of g and $g \otimes \varkappa_p$) is opposite to the sign of \varkappa_p , so if we write them as twists only of g , the signs at p are different.

- Suppose π_p is Principal Series. Let q be a non-square modulo p . Then the operator $T_q \nu_q / \lambda_q$ is an involution on the invariant subspace. Furthermore, it acts as $+1$ in the subspace spanned by (the form attached to) g and as -1 in the subspace spanned by $g \otimes \varkappa_p$. So, applying this operator we can get a 1-dimensional subspace as well.

To compute the 1-dimensional subspace, we take a non-trivial approximate solution for it and normalize as previously explained. Since we know that the first coefficient of the Fourier expansion lies in $\mathbb{Q}(\xi_N)$, we recover the exact such value from the approximate one. Recall that such coefficient is given by $\sum_{\chi} a_{\chi}$ (since g is normalized to start with q^1). Then if $p_i \nmid n$, the n -th coefficient of \tilde{f} is given by

$$(6) \quad a_n(g) \sum_{\chi} a_{\chi} \chi(n) = a_n(g) \sigma_{n-1} \left(\sum_{\chi} a_{\chi} \right),$$

where the last equality comes from Proposition 1.28. This gives the exact Fourier expansion, since we can also compute the coefficient at the various p_i^{α} . Note that the last sum of (6) only depends on n modulo $\prod p_i = N$, so we only compute it once for the $\phi(N)$ relatively prime to N remainders.

4. HEEGNER POINTS ON GENERAL CARTAN NON-SPLIT CURVES

Let E be an elliptic curve of conductor $N^2 m$ as before, with $N \neq 1$, and let $\mathcal{O} = \langle 1, \omega \rangle$ be an order in an imaginary quadratic field K which satisfies:

- The discriminant d of \mathcal{O} is prime to Nm .
- Every prime that divides m is split in \mathcal{O} .
- Every prime that divides N is inert in \mathcal{O} .

In particular, \mathcal{O} satisfies the classical Heegner hypothesis at the primes dividing m but not at the primes dividing N . We call such condition the *Cartan Heegner hypothesis* at (N, m) .

Remark 4.1. If we want to construct Heegner points for \mathcal{O} in the curve $X_0(N^2 m)$, we need points fixed by a matrix M in $M_0(N^2 m)$ with the same trace and determinant

as ω , but under our hypothesis, there are no such matrices (by looking modulo p for any prime p dividing N).

A Heegner point for $X_{ns}^{\vec{\varepsilon}}(N, m)$ is a point τ in the upper half plane which is fixed by a matrix $M \in M_{ns}^{\vec{\varepsilon}}(N) \cap M_0(m)$ giving an embedding of \mathcal{O} into $M_{ns}^{\vec{\varepsilon}}(N) \cap M_0(m)$ (sending ω to M), i.e. M satisfies

- $\text{Tr}(\omega) = \text{Tr}(M)$.
- $\text{Nm}(\omega) = \det(M)$.

Then τ is a fixed point by the usual action of this matrix group in the upper half plane. Each Heegner point τ gives rise to a pair of conjugate points (under the generator of the Galois extension $H/\mathbb{Q}(j(E_\tau))$) in $X_{ns}^{\vec{\varepsilon}}(N, m)(H)$, where H is the Hilbert class field corresponding to \mathcal{O} and E_τ is the elliptic curve $\mathbb{C}/\langle 1, \tau \rangle$. For the details of this construction see [Ser97] (appendix A.5). Then if we apply the modular parametrization (4), we get a point in $E(H)$.

4.1. Heegner systems. For constructing systems of Heegner points, it is also useful to have a definition of Heegner points in terms of the moduli interpretation.

Definition 4.2. A Heegner point for $X_{ns}^{\vec{\varepsilon}}(N, m)$ is a tuple $[\mathcal{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha]$ where \mathcal{O} is as before, $[\mathfrak{a}]$ is an element in $\text{Pic}(\mathcal{O})$ which determines an elliptic curve $E_{\mathfrak{a}}$ with CM by \mathcal{O} , \mathfrak{m} is an ideal in \mathcal{O} of norm m and such that \mathcal{O}/\mathfrak{m} is cyclic and $\phi_\alpha \in \prod_{p|N} \text{End}_{\mathbb{F}_p}(E_{\mathfrak{a}}[p])$ is such that

- ϕ_α^2 is given by multiplication by $\vec{\varepsilon}$.
- There exists $\alpha \in \mathcal{O}$ such that ϕ_α is given by multiplication by α on each coordinate.

Remark 4.3. The element α is well defined modulo N , which is a product of inert primes of \mathcal{O} , so we can just take $\alpha \in \mathcal{O}/N$.

Proposition 4.4. *Let $[\mathcal{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha]$ be a Heegner point.*

- (1) *If τ denotes complex conjugation, then $(\mathcal{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha)^\tau = (\mathcal{O}, [\mathfrak{a}^{-1}], \overline{\mathfrak{m}}, \phi_{-\alpha})$*
- (2) *Let $[\mathfrak{b}]$ be a fractional ideal, and $\sigma_{\mathfrak{b}} \in \text{Gal}(H/K)$ the Artin symbol associated to $[\mathfrak{b}]$. Then*

$$(\mathcal{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha)^{\sigma_{\mathfrak{b}}} = (\mathcal{O}, [\mathfrak{a}\mathfrak{b}^{-1}], \mathfrak{m}, \phi_\alpha)$$

- (3) *If $p \mid N$, then $\omega_p(\mathcal{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha) = (\mathcal{O}, [\mathfrak{a}], \mathfrak{m}, \phi_{-\alpha})$.*

Proof. The items (1) and (2) follow from [Ser67] (since \mathfrak{m} and α are defined over K), while (3) follows from Remark 1.3. \square

Using the geometric interpretation of Hecke operators as described in section 1.4.1 it is clear that we have the following formula for Hecke operators (for ℓ prime to Nm) acting on Heegner points, analogous to the one given in [Gro84] (section 6):

$$(7) \quad \mathcal{F}_\ell^\varepsilon([\mathcal{O}, \mathbf{a}, \mathbf{m}, \phi_\alpha]) = \sum_{\mathfrak{a}/\mathfrak{b} \cong \mathbb{Z}/\ell} (\text{End}(\mathfrak{b}), \mathfrak{b}, \mathbf{m} \cdot \text{End}(\mathfrak{b}) \cap \text{End}(\mathfrak{b}), \phi_\alpha).$$

Heegner points are points in $X_{ns}^\varepsilon(N, m)$ which are constructed from orders in imaginary quadratic fields satisfying the Cartan Heegner hypothesis at (N, m) . Such orders are indexed by positive integers n prime to Nm (the conductor of the order). Let \mathcal{O}_n be the order of conductor n in K , and let K_n be its Hilbert class field. Recall that if $n_1 \mid n_2$, $\mathcal{O}_{n_2} \subset \mathcal{O}_{n_1}$ and $K_{n_1} \subset K_{n_2}$, in particular if Q_{n_1} is a Heegner point attached to \mathcal{O}_{n_1} and Q_{n_2} is a Heegner point attached to \mathcal{O}_{n_2} , there should be some relation between these two points.

To define a *Heegner system* we follow [Dar04] (Definition 3.12).

Definition 4.5. A *Heegner system* attached to (E, K) is a collection of points $P_n \in E(K_n)$ (with n prime to Nm) which are the images of Heegner points $Q_n \in X_{ns}^\varepsilon(N, m)(K_n)$ under the modular parametrization satisfying the following properties:

- (1) Write $n = \ell k$, with ℓ a prime number inert in K , and consider a Heegner point Q_n associated to \mathcal{O}_n . Then there exists a Heegner point Q_k associated to \mathcal{O}_k such that

$$\text{Tr}_{K_n/K_k} Q_n = \mathcal{F}_\ell Q_k.$$

Moreover, if P_n and P_k denote the images of Q_n and Q_k under the modular parametrization, we have

$$\text{Tr}_{K_n/K_k} P_n = a_\ell P_k,$$

where $a_\ell = 1 + \ell - \text{card}(\tilde{E}(\mathbb{F}_\ell))$.

- (2) Let τ denote complex conjugation. Then there exists $\sigma \in \text{Gal}(K_n/K)$ such that

$$P_n^\tau \equiv -\text{sign}(E, \mathbb{Q}) P_n^\sigma \pmod{E(K_n)_{\text{tors}}},$$

where $\text{sign}(E, \mathbb{Q})$ is the root number of E .

Proposition 4.6. *For each positive square-free integer n prime to the discriminant of \mathcal{O}_K , let $\{P_n\}$ be the collection of Heegner points attached to \mathcal{O}_n as in Definition 4.2. Then this collection of points form a Heegner system.*

Proof. From Proposition 4.4, equation (7) and the discussion in between, the result follows quite formally. See for example [Gro91] Proposition 3.7 and Proposition 5.3 or [Dar04] section 3.4 and [GZ86] section II.1. \square

Once a Heegner System is constructed, Kolyvagin's machinery works and we get the following result.

Theorem 4.7. *Let $\{P_n\}$ be a Heegner system attached to (E, K) where the elliptic curve does not have CM. Define $P_K = \text{Tr}_{K_1/K} P_1 \in E(K)$. If P_K is non-torsion then the following are true*

- *The Mordell-Weil group $E(K)$ is of rank one.*
- *The Shafarevich-Tate group of E/K is finite.*

Proof. See Theorem 10.1 of [Dar04]. □

Furthermore, we have the following relation with L-series derivatives.

Theorem 4.8 (Gross-Zagier-Zhang). *The point P_1 is non-torsion if and only if $L'(E/K, 1) \neq 0$.*

Proof. This is part of Zhang's result in [Zha04], although it is not stated in this way. The natural choice for the Shimura curve in our hypothesis is to consider a Shimura curve ramified at the primes dividing N where the local root number is -1 . Nevertheless, if we take the matrix algebra as the quaternion algebra, his choice of order of level N in (6.3) (page 15) coincides with the Cartan non-split one. Then Theorem 6.1 applies, giving a relation between the L-series derivative and the Neron-Tate height pairing (inside the Jacobian) of the projection of the Heegner point to the f -isotypical component. We should point out that the point we construct is $\phi(N)$ times the point constructed by Zhang, since he takes the average of the cusps to define the map ι (in formula (6.8)).

As is already explained in Zhang's article we cannot deduce the whole Birch and Swinnerton-Dyer conjecture from this formula, since the constant appearing in Theorem 6.1 does not look like periods of E under the modular parametrization (which should include the Manin constant). □

5. EXAMPLES

We want to show how our computations work in some concrete examples. First choose representatives \mathfrak{a}_i of the Class group of \mathcal{O} , and choose $\omega_i \in \mathcal{H}$ such that $\mathfrak{a}_i = \langle 1, \omega_i \rangle$ (as an element of the Class group). Then, as in the classical case, let M_{ω_i} be the order of matrices in $M_2(\mathbb{Z})$ that fixes ω_i , which is clearly isomorphic to \mathcal{O} . Each order contains a matrix N_i whose trace equals $\text{Tr}(\omega)$ and whose determinant equals $\text{Nm}(\omega)$. We search for matrices $A_i \in \text{SL}_2(\mathbb{Z})$ such that $A_i N_i A_i^{-1}$ belongs to $M_{ns}^{\vec{\epsilon}}(N) \cap M_0(m)$. Then the point $\tau_i = A_i \omega_i$ is a Heegner point for $X_{ns}^{\vec{\epsilon}}(N, m)$.

As discussed before, the matrices A_i are computed using the Chinese Remainder Theorem, via a local condition at the primes dividing $N^2 m$:

- At a prime p dividing m , we chose $A_i^{(p)}$ modulo $p^{v_p(m)}$ of determinant one, taking N_i to an upper triangular matrix. This can be done, since the roots of

the characteristic polynomial of N_i are in \mathbb{F}_p (since every prime that divides m splits in \mathcal{O}), so we just take a basis of the Jordan form.

- At a prime p dividing N , since p is inert, the characteristic polynomial of N_i is irreducible in $\mathbb{F}_p[x]$. If $N_i = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, then we want the matrix A_i to satisfy

$$A_i \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} \frac{\alpha+\delta}{2} & \sqrt{\frac{d}{\varepsilon}} \\ \varepsilon\sqrt{\frac{d}{\varepsilon}} & \frac{\alpha+\delta}{2} \end{pmatrix} A_i \pmod{p}.$$

We just chose A_i as a matrix in 4 indeterminates and search for a non-zero solution of the system (the matrix determinant is zero, so there is always such a solution). If the determinant is not 1, we just multiply the matrix via an appropriate matrix, as in the proof of Lemma 1.2.

This gives us a matrix in $\mathrm{SL}_2(\mathbb{Z}/N^2m\mathbb{Z})$, and we lift it to a matrix in $\mathrm{SL}_2(\mathbb{Z})$.

In Table 1 we give some examples of our method following the previous notation. All the examples were done using [PAR14]. The table notation is as follows: the first column is the elliptic curve label (in Cremona's notation), the next three columns show which primes (dividing N) of the curve are supersingular, Steinberg and ramified principal series respectively. The next row gives the chosen ω (that determines the order in the imaginary quadratic field), and which primes give rise to Cartan non-split groups (the remaining are classical ones). It is easy to see that in each example the Cartan Heegner condition is satisfied. Then we list the matrices A_i for some ε . The next column contains the first Fourier coefficient (where we use the notation $\zeta_i := \xi_N^i + \xi_N^{-i}$, and a vector $[a_1, \dots, a_N]$ means $a_1\zeta_1 + \dots + a_N\zeta_N$). Finally in the last column we have c , the Manin constant for the optimal quotient.

EC	Sc	St	Ps	ω	C_{ns}	A_i	b_1	c
121b	{11}	\emptyset	\emptyset	$\frac{1+\sqrt{-3}}{2}$	{11}	$\begin{pmatrix} 6 & -31 \\ 1 & -5 \end{pmatrix}$	$[-3, -1, -5, -4, 2]$	$\frac{1}{11}$
225a	{3, 5}	\emptyset	\emptyset	$\frac{1+\sqrt{-91}}{2}$	{3}	$\begin{pmatrix} 1 & -23 \\ 1 & 0 \end{pmatrix}$	1	1
				$\frac{3+\sqrt{-91}}{10}$	{3}	$\begin{pmatrix} 2 & -5 \\ 5 & -1 \end{pmatrix}$	1	
225a	{3, 5}	\emptyset	\emptyset	$\frac{1+\sqrt{-7}}{2}$	{3, 5}	$\begin{pmatrix} 8 & -58 \\ 1 & -7 \end{pmatrix}$	$\frac{1-\sqrt{5}}{2}$	1
289a	\emptyset	{17}	\emptyset	$\frac{1+\sqrt{-3}}{2}$	{17}	$\begin{pmatrix} 9 & -73 \\ 1 & 8 \end{pmatrix}$	$[-6, -7, -4, -1, -5, -2, -4, -5]$	$\frac{1}{17}$
1617a	\emptyset	\emptyset	{7}	$\sqrt{-2}$	{7}	$\begin{pmatrix} 14 & -6 \\ 33 & -14 \end{pmatrix}$	$[-2, -1, -4]$	$\frac{1}{7}$
49a	{7}	\emptyset	\emptyset	$\frac{1+\sqrt{-11}}{2}$	{7}	$\begin{pmatrix} 4 & -15 \\ 1 & -3 \end{pmatrix}$	$\sqrt{-7}$	$\frac{1}{7}$

TABLE 1. Examples of the q -expansion and related computational data

In Table 2 we show the points constructed on the curves of Table 1 and the multiple of the generator obtained (up to torsion). Note that in the last case, the curve has rank 0 over \mathbb{Q} , and this is why the point is not rational.

EC	K	P	m_P
121b	$\mathbb{Q}(\sqrt{-3})$	$(\frac{2411156245}{(37062)^2}, -\frac{52866724475375}{(37062)^3})$	15
225a	$\mathbb{Q}(\sqrt{-91})$	(1, 1)	1
225a	$\mathbb{Q}(\sqrt{-7})$	(-1, 0)	2
289a	$\mathbb{Q}(\sqrt{-3})$	$(-\frac{15858973521095}{1083383^2}, -\frac{22895413346586388187}{1083383^3})$	3
1617a	$\mathbb{Q}(\sqrt{-2})$	$(\frac{3702}{17^2}, \frac{184078}{17^3})$	3
49a	$\mathbb{Q}(\sqrt{-11})$	$(\frac{1261982}{11(127)^2}, -\frac{680991}{11(127)^2} - \frac{327847275}{11^2(127)^3} \sqrt{-11})$	-

TABLE 2. Heegner points constructed

Remark 5.1. In all the examples of Table 1 but the last one, the optimal quotient coincides with the strong Weil curve. In the last example, the optimal quotient corresponds to the curve 49a2 in Cremona's notation.

APPENDIX A. THE PRINCIPAL SERIES CASE COMPUTATION

The purpose of this short Appendix is to show how the work [DD11] allows to, given an elliptic curve E with a ramified principal series at p , compute the character to twist by, and the local p -th Fourier coefficient of the forms h_i in Theorem 2.2. We thank Tim Dokchitser for explaining us some details of the algorithm. See the Example 5 of such article.

- (1) Compute $v_p =$ the valuation at p of the discriminant of E . Then the order of the character is $\frac{12}{\gcd(12:v_p)}$. This number will be denoted by e .
- (2) Let $L = \mathbb{Q}(x)/(x^e - p)$. Then E attains good reduction at the prime ideal (x) . Compute the characteristic polynomial $\chi_L(t) = t^2 - a_p t + p$ of Frobenius at such prime ideal by counting the number of points over the finite field (this is implemented in SAGE or Magma). The two roots are the p -th coefficients we are looking for (since there are 2 forms, conjugate to each other), but we need to match each root with its corresponding character.
- (3) Let g be a generator of \mathbb{F}_p^\times , and let $L' = \mathbb{Q}(x)/(x^e - g \cdot p)$. As before, compute the characteristic polynomial $\chi_{L'}(t)$ for the prime ideal (x) (the curve is again unramified). Then the product of a root of $\chi_L(t)$ multiplied by the correct character (evaluated at g) must be a root of $\chi_{L'}(t)$.

REFERENCES

- [Che98] Imin Chen. The Jacobians of non-split Cartan modular curves. *Proc. London Math. Soc.* (3), 77(1):1–38, 1998.
- [Dar04] Henri Darmon. *Rational points on modular elliptic curves*, volume 101 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004.
- [DD11] Tim Dokchitser and Vladimir Dokchitser. Euler factors determine local weil representations. *arXiv:1112.4889*, 2011.
- [DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.
- [dSE00] Bart de Smit and Bas Edixhoven. Sur un résultat d’Imin Chen. *Math. Res. Lett.*, 7(2-3):147–153, 2000.
- [Edi96] Bas Edixhoven. On a result of imin chen. *arXiv:alg-geom/9604008*, 1996.
- [Gro84] Benedict H. Gross. Heegner points on $X_0(N)$. In *Modular forms (Durham, 1983)*, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., pages 87–105. Horwood, Chichester, 1984.
- [Gro91] Benedict H. Gross. Kolyvagin’s work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 235–256. Cambridge Univ. Press, Cambridge, 1991.
- [GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L -series. *Invent. Math.*, 84(2):225–320, 1986.
- [Lan87] Serge Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, NY, 1987.
- [Maz78] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.
- [Pac13] Ariel Pacetti. On the change of root numbers under twisting and applications. *Proc. Amer. Math. Soc.*, 141(8):2615–2628, 2013.
- [PAR14] PARI Group, Bordeaux. *PARI/GP version 2.7.0*, 2014. available from <http://pari.math.u-bordeaux.fr/>.
- [RW14] Marusia Rebolledo and Christian Wuthrich. A moduli interpretation for the non-split cartan modular curve. *arXiv:1402.3498*, 2014.
- [Ser67] J.-P. Serre. Complex multiplication. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*, pages 292–296. Thompson, Washington, D.C., 1967.
- [Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.
- [Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.
- [Zha01] Shou-Wu Zhang. Gross-Zagier formula for GL_2 . *Asian J. Math.*, 5(2):183–290, 2001.
- [Zha04] Shou-Wu Zhang. Gross-Zagier formula for $GL(2)$. II. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 191–214. Cambridge Univ. Press, Cambridge, 2004.

IMAS-CONICET, BUENOS AIRES, ARGENTINA

E-mail address: kohendaniel@gmail.com

DEPARTAMENTO DE MATEMÁTICA, FACULTAD DE CIENCIAS EXACTAS Y NATURALES, UNIVERSIDAD DE BUENOS AIRES AND IMAS, CONICET, ARGENTINA

E-mail address: apacetti@dm.uba.ar