Canad. J. Math. Vol. **68** (2), 2016 pp. 422–444
http://dx.doi.org/10.4153/CJM-2015-047-6

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 $\mathscr{O}$ 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 $\mathscr{O}$. Although there are no Heegner points on $X_0(N)$ attached to $\mathscr{O}$, in this article we construct such points on Cartan non-split curves. In order to do that, we give a method to compute Fourier expansions for forms on 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. A difficult unsolved problem is to construct a set of generators for the rational points on E. To date, "Heegner points" construction is the only general method known. Let K be an imaginary quadratic field such that E/K has root number -1. Let $\mathscr{O}$ be an order in K of discriminant prime to N satisfying the *Heegner hypothesis for* $X_0(N)$; that is, all primes dividing N are split in $\mathscr{O}$ (see [Dar04, Hypothesis 3.9]). Then one can construct points on the modular curve $X_0(N)$ and map them through the modular parametrization to get points on E. The Gross–Zagier Theorem says that the constructed points are non-torsion if and only if $L'(E/K,1) \neq 0$.

Heegner's construction can be generalized to any square-free N using Shimura curves provided the *Heegner hypothesis for Shimura curves* is satisfied: the number of prime numbers dividing N that are inert in $\mathscr{O}$ is even. Although the hypothesis might look awkward, when N is square-free it is the right one for the root number of E/K to be -1. When N is not square-free, this is not true anymore. For example, suppose E is an elliptic curve over $\mathbb{Q}$ of conductor p^2 (p an odd prime) and K is an imaginary quadratic field with discriminant D such that D and p are relatively prime and p is inert in K. In this case, the root number is still -1 (see, for example, [Zha01, Definition 1.1.3]), but the Heegner hypothesis is not satisfied. Nevertheless, there should exist some Heegner point construction (and Heegner systems) and a Gross–Zagier–Zhang formula should hold. Since there are no Heegner points on the classical modular curve $X_0(p^2)$ associated with $\mathscr{O}$, we need to consider other modular curves. A canonical choice in this case is to consider the so-called Cartan non-split curve, which is a quotient of the Poincaré upper half-plane by a Cartan non-split group. Since such group is a subgroup of a matrix algebra, once we proved that our curve E is a quotient of the

Received by the editors February 23, 2015; revised October 7, 2015.
Published electronically January 28, 2016.
D. K. was partially supported by a CONICET doctoral fellowship. A. P. was partially supported by CONICET PIP 2010-2012 GI and FonCyT BID-PICT 2010-0681.
AMS subject classification: **11G05**, 11F30.
Keywords: Cartan curves, Heegner points.

Jacobian of the Cartan non-split curve, the modular parametrization can be explicitly computed using the Fourier expansion of modular forms for it.

Some new problems appear while working with such groups; for example, what is the right normalization of a modular form? (There is not an easy formula to relate all Hecke operators eigenvalues with Fourier coefficients of eigenforms for such groups.) Some interesting problems that will not be addressed in this article (and are unknown in general) are determining the strong Weil curve for the Cartan non-split curve (even deciding when it coincides with the strong Weil curve for $\Gamma_0(N)$) and determining the Manin constant for it.

In this article we show how to compute Hecke operators for Cartan non-split curves (and curves that are mixed situations of classical curves for some primes and Cartan non-split for the other ones) and how to compute the Fourier expansion of Cartan modular forms. We propose a natural normalization (well defined up to ± 1) and show how to construct Heegner points (and Heegner systems) on modular curves over imaginary quadratic fields satisfying the Cartan–Heegner hypothesis using the presented theory.

This article is organized as follows: we start with the case $N = p^2$ where all new ideas appear while avoiding dealing with subindices in a first reading. 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 different from the classical one and also from the one presented 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 the mixed situations.

Next we focus on the problem of computing Fourier expansions of Cartan modular forms. We propose a suitable normalization and prove that with this normalization, the Fourier expansion of a Cartan modular form has coefficients in $\mathbb{Q}(\xi_p)$ (the p-th cyclotomic field). The way to compute the Fourier expansion is to write the form as a linear combination of other modular forms (twists of the weight 2 modular form attached to E) and then solve a linear system to compute the combination explicitly. A theorem of Chen and Edixhoven ([Che98, Edi96]) proves that our curve is isogenous to a quotient of the Jacobian of the Cartan non-split curve, so the Eichler-Shimura construction and the Abel–Jacobi map give the modular parametrization. A difference with the $\Gamma_0(N)$ case is that the cusps for the Cartan non-split curve are not defined over $\mathbb{Q}$ (implying the natural modular parametrization is not rational), so we average over all conjugate cusps to get a rational map (which we also call modular parametrization). Galois conjugation sends a Cartan modular form to another Cartan modular form but for another Cartan subgroup, *i.e.*, it corresponds to another choice of a non-square modulo p, so in the modular parametrization, all Cartan non-split groups are involved.

After the theory for level p^2 is done, we move to the general case of mixed types; *i.e.,* elliptic curves whose conductor are not square-free, and some primes dividing the conductor are split in $\mathscr{O}$ while others are inert. Although no extra difficulties appear, we believe that considering the conductor p^2 case first gives a better understanding of the new ideas involved.

The third and fourth sections are about constructing 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 (Theorems 3.6 and 3.7). We also include some computational details on how our construction can be carried out for any particular curve E and any order $\mathscr{O}$ satisfying the Cartan–Heegner hypothesis.

The last section of this article contains many examples where we show how the method works for different elliptic curves, including the Manin constants and Heegner points obtained by our method for each of them.

1 Cartan Non-split Curves of Prime Level

Notation and conventions Throughout this article, p will denote an odd prime and ε will be a non-square modulo p. Given a matrix $A \in \mathrm{M}_{2\times 2}(\mathbb{Z})$, $\overline{A}$ will denote its reduction modulo p.

1.1 Definition

The Cartan non-split ring modulo p is the ring

$$C_{ns}^{\varepsilon}(p) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in M_{2\times 2}(\mathbb{F}_p) : a \equiv d, c \equiv b\varepsilon \bmod p \right\}.$$

The group of invertible elements $(C_{ns}^{\varepsilon}(p))^{\times}$ is isomorphic to the cyclic group $\mathbb{F}_{p^2}^{\times} = \mathbb{F}_p(\sqrt{\varepsilon})^{\times}$. We also define the ring

$$M_{ns}^{\varepsilon}(p) = \left\{ A \in \mathrm{M}_{2\times 2}(\mathbb{Z}) : \overline{A} \in C_{ns}^{\varepsilon}(p) \right\}.$$

The Cartan non-split group $\Gamma_{ns}^{\varepsilon}(p)$ is the group of determinant 1 matrices in $M_{ns}^{\varepsilon}(p)$. We can also consider

$$C_{ns}^{\varepsilon+}(p) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in M_{2\times 2}(\mathbb{F}_p) : a \equiv d, c \equiv b\varepsilon \text{ or } a \equiv -d, c \equiv -b\varepsilon \right\},$$

and define $M_{ns}^{\varepsilon+}(p)$ and $\Gamma_{ns}^{\varepsilon+}(p)$ as before. The group $\Gamma_{ns}^{\varepsilon+}(p)$ is called the normalizer of the Cartan non-split group.

Let $\mathcal{H}$ be the Poincaré upper half-plane, and consider the complex curve $Y_{ns}^{\varepsilon}(p) = \Gamma_{ns}^{\varepsilon}(p)\backslash\mathcal{H}$ whose compactification obtained by adding the cusps is the Cartan non-split modular curve of level p, $X_{ns}^{\varepsilon}(p) = \Gamma_{ns}^{\varepsilon}(p)\backslash\mathcal{H}^*$. Analogously, we can define $X_{ns}^{\varepsilon+}(p) = \Gamma_{ns}^{\varepsilon+}(p)\backslash\mathcal{H}^*$. Since $\det\colon (C_{ns}^{\varepsilon}(p))^{\times} \to \mathbb{F}_p^{\times}$ is surjective, the modular curves $X_{ns}^{\varepsilon}(p)$ and $X_{ns}^{\varepsilon+}(p)$ are both defined over $\mathbb{Q}$ (see [Shi94, Section 6.4, Proposition 6.27]).

1.2 Moduli Interpretation

We will give a new moduli interpretation for the complex points of the Cartan non-split curve. For other moduli interpretations, see [Ser97, Appendix 5] and [RW14]. Consider pairs (E,ϕ), where $E/\mathbb{C}$ is an elliptic curve and $\phi \in \mathrm{End}_{\mathbb{F}_p}(E[p])$ satisfies that ϕ^2 is multiplication by ε. We identify two such pairs (E,ϕ), (E',ϕ') if there exists an isomorphism of elliptic curves $\Psi: E \to E'$ such that the following diagram is commutative:

$$\begin{tikzcd} E[p] \arrow[r, "\phi"] \arrow[d, "\Psi"'] & E[p] \arrow[d, "\Psi"] \\ E'[p] \arrow[r, "\phi'"'] & E'[p]. \end{tikzcd}$$

For any number field K, we say that the point (E, ϕ) is a K-rational point of the Cartan non-split curve if E is an elliptic curve defined over K and ϕ is defined over K. Recall that by definition ϕ is defined over K if $\phi^\sigma = \phi$ for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$, *i.e.,* $\phi(P^\sigma) = \phi(P)^\sigma$ for every $P \in E[p]$ and every $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Proposition 1.1 *The moduli problem of pairs (E, ϕ) is represented by the Cartan non-split curve $Y^\varepsilon_{ns}(p)$. The point $\Gamma^\varepsilon_{ns}(p)\tau$ corresponds to the pair (E_τ, ϕ_τ), where $E_\tau = \mathbb{C}/\langle \tau, 1\rangle$ and ϕ_τ is the endomorphism of $E_\tau[p]$ whose matrix in the basis $B_\tau = \{\frac{1}{p}, \frac{\tau}{p}\}$ equals $\left(\begin{smallmatrix} 0 & 1 \\ \varepsilon & 0 \end{smallmatrix}\right)$.*

Before writing the proof, we need an auxiliary lemma.

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

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

Proof of Proposition 1.1 We need to check that the previous correspondence between points on $Y^\varepsilon_{ns}(p)$ and pairs (E, ϕ) is well defined and bijective.

Let τ and τ' be points on $\mathcal{H}$ corresponding to pairs $(E_\tau, \phi_\tau), (E_{\tau'}, \phi_{\tau'})$, respectively. To prove that the map is well defined and injective is enough to prove that such pairs are isomorphic if and only if τ and τ' are equivalent under $\Gamma^\varepsilon_{ns}(p)$. It is well known 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\alpha\tau = a\tau' + b$ and $\alpha = c\tau' + d$. Moreover, Ψ must satisfy $\phi_{\tau'}\Psi = \Psi\phi_\tau$. In the chosen basis, this is equivalent to

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

It is easy to see that the following hold

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

Since equality holds modulo $\langle 1, \tau'\rangle$, we get that $a \equiv d \bmod p$ and $c \equiv \varepsilon b \bmod p$. This proves that the pairs (E_τ, ϕ_τ) and $(E_{\tau'}, \phi_{\tau'})$ are isomorphic by a map satisfying

https://doi.org/10.4153/CJM-2015-047-6 Published online by Cambridge University Press

the first condition if and only if τ and τ' are equivalent under $\Gamma^{\varepsilon}_{ns}(p)$. The commutative condition for the second basis elements is similar and gives the same constraint.

To prove surjectivity, let (E,ϕ) be any pair as before. 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 Lemma 1.2, there exists a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $\overline{A}[\phi]_B\overline{A}^{-1} = \left(\begin{smallmatrix} 0 & 1\\ \varepsilon & 0\end{smallmatrix}\right)$. Hence, $[E,\phi] \simeq [\mathbb{C}/\langle A\cdot\tau,1\rangle,\phi']$, where $[\phi']_{\{1/p,(A\cdot\tau)/p\}} = \left(\begin{smallmatrix} 0 & 1\\ \varepsilon & 0\end{smallmatrix}\right)$. ∎

Remark 1.3 The moduli problem for $\Gamma^{\varepsilon+}_{ns}(p)$ consists of pairs (E,ϕ) as before, where two pairs $(E,\phi),(E',\phi')$ are isomorphic if $\Psi\phi = \pm\phi'\Psi$. There is an involution ω^{ε}_p acting on $X^{\varepsilon}_{ns}(p)$ given by $\omega^{\varepsilon}_p(E,\phi) = (E,-\phi)$ and $X^{\varepsilon+}_{ns}(p) = X^{\varepsilon}_{ns}(p)/\omega^{\varepsilon}_p$.

1.3 Modular Forms and Hecke Operators

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Let $f\colon\mathcal{H}\to\mathbb{C}$ be an holomorphic function. If $\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right) \in \Gamma$, and $k \in \mathbb{Z}$, we define the slash operator

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

Let $M_k(\Gamma)$ be the space of holomorphic functions that are invariant under the previous action for all elements in Γ and that are holomorphic at all the cusps, and let $S_k(\Gamma)$ be the subspace of cusp forms, *i.e.*, those forms in $M_k(\Gamma)$ whose q-expansions at all the cusps have zero constant coefficient. Let $\Gamma(p)$ be the principal congruence subgroup of level p. The inclusion $\Gamma(p) \subset \Gamma^{\varepsilon}_{ns}(p)$ gives a reverse inclusion at the level of modular forms $S_2(\Gamma^{\varepsilon}_{ns}(p)) \subset S_2(\Gamma(p))$. If $\alpha_p = \left(\begin{smallmatrix} p & 0\\ 0 & 1\end{smallmatrix}\right)$ and $f \in S_2(\Gamma(p))$, $\widetilde{f} = f|_2[\alpha_p]$ is a modular form with respect to $(\alpha_p)^{-1}\Gamma(p)\alpha_p = \Gamma_0(p^2)\cap\Gamma_1(p)$. Define $\widetilde{\Gamma}(p) := \Gamma_0(p^2)\cap\Gamma_1(p)$. Thus, slashing by α_p gives the isomorphism $S_2(\Gamma(p)) \cong S_2(\widetilde{\Gamma}(p))$.

There are two ways to define Hecke operators for classical subgroups. The geometric way is to define them as correspondences on the modular curve and, via the moduli interpretation, translate this action to an action on modular forms. The algebraic way is to define them in terms of double coset operators. We will describe both definitions and prove that they agree.

1.3.1 Geometric Definition

Let n be a positive integer prime to p and let (E,ϕ) be a pair corresponding to a point on the moduli interpretation of the curve $Y^{\varepsilon}_{ns}(p)$. Define the Hecke operator

$$\mathcal{T}^{\varepsilon}_n((E,\phi)) := \sum_{\psi: E\to E'} \Big(E', \frac{1}{n}\psi\circ\phi\circ\widehat{\psi}\Big),$$

where the sum is over degree n isogenies $\psi\colon E \to E'$ of cyclic kernel, and $\widehat{\psi}$ denotes the dual isogeny. Note that since $\gcd(n,p) = 1$, $\frac{1}{n} \in \mathrm{End}_{\mathbb{F}_p}(E'[p])$. Also, since $\psi\circ\widehat{\psi}$ and $\widehat{\psi}\circ\psi$ are multiplication by n, $(\frac{1}{n}\psi\circ\phi\circ\widehat{\psi})\circ(\frac{1}{n}\psi\circ\phi\circ\widehat{\psi})$ is multiplication by ε, so the points in the formula belong to $Y^{\varepsilon}_{ns}(p)$.

1.3.2 Algebraic Definition

We provide a little survey of Hecke operators for the Cartan non-split curve, following Shimura's book [Shi94]. Define

$$\Delta_p := \left\{ A \in \mathrm{M}_{2\times 2}(\mathbb{Z}) : \det(A) > 0 \text{ and } \gcd(p, \det(A)) = 1 \right\}$$

and $\Delta^{\varepsilon}_{ns}(p) := \Delta_p \cap M^{\varepsilon}_{ns}(p)$. Moreover, consider

$$\Delta(p) := \left\{ A \in \Delta_p : \overline{A} \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix} \right) \bmod p \right\}.$$

Let $R(\Gamma^{\varepsilon}_{ns}(p), \Delta^{\varepsilon}_{ns}(p))$ and $R(\Gamma(p), \Delta(p))$ be the Hecke rings as defined in [Shi94, p. 54].

We need to introduce a new operator. Let $n \in \mathbb{Z}$ satisfy $p \nmid n$ and let $B \in \Delta^{\varepsilon}_{ns}(p)$ be any matrix with determinant congruent to n modulo p. Let $A^{\varepsilon}_n \in \mathrm{SL}_2(\mathbb{Z})$ be such that $A^{\varepsilon}_n \equiv B\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1/n \end{smallmatrix} \right) \bmod p$. The action of A^{ε}_n on $S_2(\Gamma^{\varepsilon}_{ns}(p))$ defines an operator that we will denote v^{ε}_n.

Lemma 1.4 *The operator v^{ε}_n defines an isomorphism from $S_2(\Gamma^{\varepsilon}_{ns}(p))$ to $S_2(\Gamma^{\varepsilon n^2}_{ns}(p))$ which depends only on the class of n modulo p. It is equal to the double coset operator $\Gamma^{\varepsilon}_{ns}(p) A^{\varepsilon}_n \Gamma^{\varepsilon n^2}_{ns}(p)$.*

Proof Since $\overline{B} \in C^{\varepsilon}_{ns}(p)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1/n \end{smallmatrix} \right)^{-1} C^{\varepsilon}_{ns}(p) \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1/n \end{smallmatrix} \right) = C^{\varepsilon n^2}_{ns}(p)$, the first assertion follows. Let B and B' be matrices in $\Delta^{\varepsilon}_{ns}(p)$ of determinant n and n' respectively with $n \equiv n' \bmod p$. Choose any two matrices A^{ε}_n and $A^{\varepsilon}_{n'}$ corresponding to B and B' respectively. Clearly, $A^{\varepsilon}_n {A^{\varepsilon}_{n'}}^{-1} \in \Gamma^{\varepsilon}_{ns}(p)$, therefore, this matrix acts trivially. ∎

Let $h\colon R(\Gamma(p), \Delta(p)) \to R(\Gamma^{\varepsilon}_{ns}(p), \Delta^{\varepsilon}_{ns}(p))$ be the map given by $\Gamma(p)\beta\Gamma(p) \mapsto \Gamma^{\varepsilon}_{ns}(p) A^{\varepsilon}_{\det(\beta)} \beta \Gamma^{\varepsilon}_{ns}(p)$.

Proposition 1.5 *The map h is an isomorphism of Hecke rings.*

Proof We have a map $h_1\colon R(\Gamma^{\varepsilon}_{ns}(p), \Delta^{\varepsilon}_{ns}(p)) \to R(\mathrm{SL}_2(\mathbb{Z}), \Delta_p)$ given by

$$\Gamma^{\varepsilon}_{ns}(p)\alpha\Gamma^{\varepsilon}_{ns}(p) \mapsto \mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z}),$$

and a map $h_2\colon R(\Gamma(p), \Delta(p)) \to R(\mathrm{SL}_2(\mathbb{Z}), \Delta_p)$ given by

$$\Gamma(p)\beta\Gamma(p) \mapsto \mathrm{SL}_2(\mathbb{Z})\beta\,\mathrm{SL}_2(\mathbb{Z}).$$

Both maps are easily seen to be isomorphisms of Hecke rings by the same proof used in [Shi94, Proposition 3.31]. Moreover, the map $h = h_1^{-1} h_2$ is given by $\Gamma(p)\beta\Gamma(p) \mapsto \Gamma^{\varepsilon}_{ns}(p) A^{\varepsilon}_{\det(\beta)} \beta \Gamma^{\varepsilon}_{ns}(p)$ and gives the desired isomorphism. ∎

We can consider the classical Hecke operators T_n acting on $S_2(\widetilde{\Gamma}(p))$ for n relatively prime to p. Slashing by α_p we obtain the corresponding Hecke operator T_n acting on $S_2(\Gamma(p))$. In view of the above proposition we define the Hecke operator $\mathscr{T}^{\varepsilon}_n \in R(\Gamma^{\varepsilon}_{ns}(p), \Delta^{\varepsilon}_{ns}(p))$ as the operator $h(T_n)$.

Lemma 1.6 *If $\beta \in \Delta(p)$, the operator $\Gamma(p)\beta\Gamma(p)$ acting on $S_2(\Gamma^{\varepsilon n^2}_{ns}(p))$ is equal to the operator $\Gamma^{\varepsilon n^2}_{ns}(p)\beta\Gamma^{\varepsilon}_{ns}(p)$.*

Proof This mimics the proof of Lemma 1.4. ∎

Proposition 1.7 *As operators on $S_2(\Gamma_{ns}^{\varepsilon}(p))$, $\mathcal{T}_n^{\varepsilon} = T_n \circ v_n^{\varepsilon}$.*

Proof Proposition 3.7 of [Shi94] says that

$$\Gamma_{ns}^{\varepsilon}(p)A_{\det(\beta)}^{\varepsilon}\beta\Gamma_{ns}^{\varepsilon}(p) = \Gamma_{ns}^{\varepsilon}(p)A_n^{\varepsilon}\Gamma_{ns}^{\varepsilon n^2}(p)\Gamma_{ns}^{\varepsilon n^2}(p)\beta\Gamma_{ns}^{\varepsilon}(p).$$

Therefore, the result follows from Lemmas 1.4 and 1.6. ∎

Corollary 1.8 *If $n \equiv 1 \bmod p$, then $\mathcal{T}_n^{\varepsilon} = T_n$.*

Proof Since the matrix A_n^{ε} can be taken to be the identity, v_n^{ε} is the identity map. ∎

We can prove the following proposition in the same way as Proposition 1.7.

Proposition 1.9 *For any n prime to p, the operators $T_n \colon S_2(\Gamma_{ns}^{\varepsilon}(p)) \to S_2(\Gamma_{ns}^{\varepsilon/n^2}(p))$ and $v_n^{\varepsilon} \colon S_2(\Gamma_{ns}^{\varepsilon}(p)) \to S_2(\Gamma_{ns}^{\varepsilon n^2}(p))$ are morphisms of Hecke modules.*

Theorem 1.10 *The geometric and algebraic definitions of Hecke operators coincide.*

Proof We can restrict to n prime and $n \neq p$. It is enough to see that the set of representatives used in one definition can be taken as representatives for the other one. Take representatives for $\Gamma_{ns}^{\varepsilon}(p)A_n^{\varepsilon}\left(\begin{smallmatrix}1&0\\0&n\end{smallmatrix}\right)\Gamma_{ns}^{\varepsilon}(p)$ modulo $\Gamma_{ns}^{\varepsilon}(p)$. By [Shi94, Lemma 3.29(5)], these are also representatives for

$$\mathrm{SL}_2(\mathbb{Z})A_n^{\varepsilon}\left(\begin{smallmatrix}1&0\\0&n\end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})\left(\begin{smallmatrix}1&0\\0&n\end{smallmatrix}\right)\mathrm{SL}_2(\mathbb{Z})$$

modulo $\mathrm{SL}_2(\mathbb{Z})$. This set of representatives coincides with a set of representatives of cyclic isogenies of degree n. Each representative is a matrix A of determinant n. The dual isogeny is given by the matrix $\mathrm{Adj}(A)$. Both matrices belong to $\Delta_{ns}^{\varepsilon}(p)$; thus, they commute with the matrix $\left(\begin{smallmatrix}0&1\\\varepsilon&0\end{smallmatrix}\right)$ modulo p and $A\,\mathrm{Adj}(A) = n\,\mathrm{Id}$. Therefore, recalling the geometric definition, we have that $\mathcal{T}_n^{\varepsilon}([\mathbb{C}/\langle\tau,1\rangle,\phi_\tau]) = \sum_A[\mathbb{C}/\langle A\tau,1\rangle,\phi_A]$, where $[\phi_A]_{\left\{\frac{1}{p},\frac{A\tau}{p}\right\}} = \left(\begin{smallmatrix}0&1\\\varepsilon&0\end{smallmatrix}\right)$ as desired. ∎

1.4 Chen–Edixhoven Isogeny Theorem

If $\mathcal{C}$ is a curve, we denote its Jacobian by $\mathrm{Jac}(\mathcal{C})$.

Theorem 1.11 (Chen–Edixhoven) *The new part of $\mathrm{Jac}(X_0^+(p^2))$ is isogenous to $\mathrm{Jac}(X_{ns}^{\varepsilon+}(p))$. Furthermore, the new part of $\mathrm{Jac}(X_0(p^2))$ and $\mathrm{Jac}(X_{ns}^{\varepsilon}(p))$ are isogenous. In addition, the isogenies are Hecke equivariant.*

Proof See [Che98, Theorem 1] , [Edi96, Theorem 1.1], and [dSE00, Theorem 2]. Although the Hecke equivariant condition is not explicitly stated, by [dSE00, Theorem 2] 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 relatively prime to p. ∎

https://doi.org/10.4153/CJM-2015-047-6 Published online by Cambridge University Press

In particular, if we start with a normalized newform $g \in S_2(\Gamma_0(p^2))$ such that $T_n g = \lambda_n g$ for all n relatively prime to p, Theorem 1.11 implies the existence of a form $g_\varepsilon \in S_2(\Gamma_{ns}^\varepsilon(p))$ such that $\mathscr{T}_n^\varepsilon g_\varepsilon = \lambda_n g_\varepsilon$ for all n relatively prime to p.

Chen–Edixhoven's Theorem plus multiplicity one for classical newforms ([DS05, Theorem 5.8.2]) for $S_2(\Gamma_0(p^2))$ give multiplicity one for a system of eigenvalues for the Hecke algebra $R(\Gamma_{ns}^\varepsilon(p), \Delta_{ns}^\varepsilon(p))$.

Our primary goal is to compute the Fourier expansion of g_ε. Since g_ε is an eigenfunction for the Hecke operators $\mathscr{T}_n^\varepsilon$, and since such operators coincide with T_n if $n \equiv 1 \pmod p$, our form lies in the space of eigenfunctions for T_n with eigenvalues λ_n for $n \equiv 1 \pmod p$. Then we can write $\widetilde{g_\varepsilon} = g_\varepsilon|_2[\alpha_p]$ as a linear combination of eigenforms on $S_2(\widetilde{\Gamma}(p))$ that have the same eigenvalues as g for $n \equiv 1 \pmod p$.

Let $\mathfrak{G}_g = \{f \in S_2(\widetilde{\Gamma}(p)) \text{ eigenform } : \lambda_n(g) = \lambda_n(f) \text{ for all } n \equiv 1 \pmod p\}$. Can we characterize $\mathfrak{G}_g$?

In general, if χ is a character modulo N and $h \in S_2(\Gamma(N))$ is a newform, we denote by $h \otimes \chi$ the *twist* of h by χ. If $T_n h = \lambda_n(h)h$, then $T_n(h \otimes \chi) = \lambda_n(h)\chi(n)(h \otimes \chi)$. This implies that if χ is a character modulo p, $g \otimes \chi \in \mathfrak{G}_g$.

Theorem 1.12 *Let $f \in S_2(\Gamma_0(p^2), \psi)$ be an eigenform for the classical Hecke algebra, where ψ is a character modulo p. Let $g \in S_2^{\mathrm{new}}(\Gamma_0(p^2))$ be an eigenform without complex multiplication, and suppose that f and g have the same eigenvalues on a set of primes of positive upper density. Then there exists a Dirichlet character χ modulo p such that the eigenforms $g \otimes \chi$ and f have the same eigenvalues at all but a finite number of primes.*

Proof See [Raj98, Corollary 1]. ∎

Therefore, all elements of $\mathfrak{G}_g$ are the form $g \otimes \chi$ (where χ varies over the characters of conductor p) or are newforms attached to them, since it may happen that $g \otimes \chi \in S_2(\Gamma_0(p^2), \chi^2)$ is not a newform (it may fail to be new at p). In that case there is an associated newform living on $S_2(\Gamma_0(p), \chi^2)$ that appears in the linear combination as well. Being new at p can be read from the type of the local automorphic representation of g at the prime p, as explained in [AL78]. We have proved the following theorem.

Theorem 1.13 *Let $g \in S_2^{\mathrm{new}}(\Gamma_0(p^2))$ be a normalized eigenform with eigenvalues λ_n (n relatively prime to p), and suppose that g does not have complex multiplication. Let $g_\varepsilon \in S_2(\Gamma_{ns}^\varepsilon(p))$ be the unique normalized eigenform such that $\mathscr{T}_n^\varepsilon g_\varepsilon = \lambda_n g_\varepsilon$ (n relatively prime to p). Let π_p be the local automorphic representation of g at p.*

- *If π_p is supercuspidal, then $g \otimes \chi$ is a newform in $S_2(\Gamma_0(p^2), \chi^2)$ for all characters χ modulo p and*
$$\widetilde{g_\varepsilon} = \sum_\chi a_\chi (g \otimes \chi),$$
for some $a_\chi \in \mathbb{C}$, where the sum is over all characters modulo p.
- *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 modulo p and*
$$\widetilde{g_\varepsilon} = \sum_\chi a_\chi (g \otimes \chi) + ah$$

for some $a_\chi, a \in \mathbb{C}$, where the first sum is over all characters modulo p.

- *If π_p is a ramified Principal Series, there exists a non-quadratic character θ_p modulo p and newforms*

$$h \in S_2(\Gamma_0(p), \overline{\theta_p}^2), \quad \overline{h} \in S_2(\Gamma_0(p), \theta_p^2)$$

such that $h \otimes \theta_p = g = \overline{h} \otimes \overline{\theta_p}$. Then

$$\widetilde{g_\varepsilon} = \sum_\chi a_\chi (g \otimes \chi) + a_1 h + a_2 \overline{h},$$

for some $a_\chi, a_1, a_2 \in \mathbb{C}$, where the first sum is over all characters modulo p.

Remark 1.14 If $g_\varepsilon \in S_2(\Gamma_{ns}^{\varepsilon+}(p))$ is an eigenform, then $T_n f = \lambda_n f$ for $n \equiv -1 \bmod p$ as well. Therefore, all the non-zero coefficients in the linear combination of Theorem 1.13 are those corresponding to even characters.

Similarly, if $g_\varepsilon \in S_2(\Gamma_{ns}^{\varepsilon-}(p))$ (*i.e.,* any matrix in the normalizer but not in the Cartan itself acts as −1), then the non-zero coefficients in the linear combination of Theorem 1.13 are those corresponding to odd characters.

1.5 Fourier Expansions

In order to compute the Fourier expansion of the normalized newform g_ε, we first need to understand the action of the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ on modular forms. For $a \in \mathbb{Q}^2$ and $z \in \mathcal{H}$ define

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

where $\wp(-;\omega_1,\omega_2)$ is the classical Weierstrass function associated with 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 [Shi94, Section 6.1] for example). These functions satisfy $f_a(\gamma(z)) = f_{a\gamma}(z)$ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Let $\mathcal{R}_p$ be the field of modular functions of level p, which by [Shi94, Proposition 6.1] is

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

Let ξ_p be a fixed p-th root of unity and let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}(\xi_p))$. Since the functions j, f_a have Fourier expansions belonging to $\mathbb{Q}(\xi_p)$, if $f = cj + \sum_a c_a f_a$, then $\sigma(f) = \sigma(c)j + \sum_a \sigma(c_a) f_a$. If we choose representatives $\{\beta_k\}$ for $\pm\Gamma(p)\backslash\Gamma_{ns}^\varepsilon(p)$, the field of modular functions for the non-split Cartan is the subfield of $\mathcal{R}_p$ given by

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

Clearly it does not depend on the representatives chosen. In order to understand the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ on modular forms for the Cartan non-split group, it is enough to understand the effect of $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ on them. For every n relatively prime to p consider the automorphism σ_n given by $\sigma_n(\xi_p) = \xi_p^{n^{-1}}$. This Galois automorphism depends only on the class of n modulo p. By [Shi94, Theorem 6.6] and [Lan87, Theorem 3, Chapter 6, section 3] this automorphism acting on the meromorphic modular functions f_a is given by $f_{a\alpha_{n^{-1}}}$, where $\alpha_k := \big(\begin{smallmatrix} 1 & 0 \\ 0 & k \end{smallmatrix} \big)$.

https://doi.org/10.4153/CJM-2015-047-6 Published online by Cambridge University Press

Proposition 1.15 *Let f be a meromorphic form of weight 0 for $\Gamma_{ns}^{\varepsilon}(p)$. Let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ satisfying $\sigma|_{\mathbb{Q}(\xi_p)} = \sigma_n$. Then $\sigma(f)$ is a meromorphic form of weight 0 for $\Gamma_{ns}^{\varepsilon n^2}(p)$.*

Proof Choose representatives $\{\beta_k\}$ for $\pm\Gamma(p)\backslash\Gamma_{ns}^{\varepsilon}(p)$ such that the $(1,2)$ entries of the matrices are divisible by n. Since f is a meromorphic form of weight 0, we have

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

Then

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

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

Remark 1.16 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.

Proposition 1.17 *Let f be a meromorphic modular function for $\Gamma_{ns}^{\varepsilon}(p)$ and let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ satisfying $\sigma|_{\mathbb{Q}(\xi_p)} = \sigma_n$. Then $\sigma(v_m^{\varepsilon}(f)) = v_m^{\varepsilon n^2}(\sigma(f))$.*

Proof Choose A_m^{ε} in such a way that its $(1,2)$ entry is divisible by n. It is easy to see that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right) A_m^{\varepsilon} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1/n \end{smallmatrix}\right)$, which belongs to $\mathrm{SL}_2(\mathbb{Z})$ by our choice of A_m^{ε}, gives the same action on the f_a as $A_m^{\varepsilon n^2}$ (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 1.16 applies. ∎

Corollary 1.18 *With the previous notation, $\mathcal{T}_m^{\varepsilon n^2}(\sigma(f)) = \sigma(\mathcal{T}_m^{\varepsilon}(f))$.*

Proof This follows from the previous proposition and the fact that σ commutes with T_m (this is easily obtained by looking at the action on q-expansions). ∎

Corollary 1.19 *Suppose that $g \in S_2(\Gamma_0(p^2))$ is a newform with rational eigenvalues. Then $\sigma(g_{\varepsilon}) \in S_2(\Gamma_{ns}^{\varepsilon n^2}(p))$ is a normalized newform with the same eigenvalues as g_{ε},* i.e., *if $\mathcal{T}_m^{\varepsilon}(g_{\varepsilon}) = \lambda_m g_{\varepsilon}$ with $\lambda_m \in \mathbb{Q}$, then $\mathcal{T}_m^{\varepsilon n^2}(\sigma(g_{\varepsilon})) = \lambda_m \sigma(g_{\varepsilon})$.*

Corollary 1.20 *With the previous notations, if m is relatively prime to p and satisfies $mn \equiv 1 \bmod p$, then there exists $c_m \in \mathbb{C}$ such that $T_m g_{\varepsilon} = c_m \sigma(g_{\varepsilon})$.*

Proof By Proposition 1.9, $T_m(g_{\varepsilon})$ is an eigenform in $S_2(\Gamma_{ns}^{\varepsilon n^2}(p))$ with the same eigenvalues as g_{ε}. By Corollary 1.18, $\sigma(g_{\varepsilon})$ is an eigenform whose eigenvalues are the same as those from g_{ε}. The result now follows from multiplicity one. ∎

Theorem 1.21 *Let $g_{\varepsilon} \in S_2(\Gamma_{ns}^{\varepsilon}(p))$ be a normalized eigenform that has the same eigenvalues as a rational newform $g \in S_2(\Gamma_0(p^2))$. Then g_{ε} has a q-expansion belonging to $\mathbb{Q}(\xi_p)$.*

Proof Let $\ell \equiv 1 \bmod p$ be such that $\lambda_\ell \neq 0$, and let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}(\xi_p))$ be arbitrary. By Corollary 1.20 , there is a c_ℓ such that $T_\ell g_\varepsilon = c_\ell \sigma(g_\varepsilon)$. We know that $T_\ell g_\varepsilon = \lambda_\ell g_\varepsilon$ (by Corollary 1.8). Looking at the first Fourier coefficient, we get that $c_\ell = \lambda_\ell$ and hence $g_\varepsilon = \sigma(g_\varepsilon)$. Since $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}(\xi_p))$ is arbitrary it follows that the q-expansion of g_ε lies in the desired extension. ∎

1.6 Rational Modular Forms

The curve $X^\varepsilon_{ns}(p)$ is defined over $\mathbb{Q}$ and has $(p-1)$ cusps, all of which are defined over $\mathbb{Q}(\xi_p)$ and conjugate by $\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$ (see [Ser97, Appendix 5]). If $\sigma_n \in \mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})$, then there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma_n(\infty) = A\infty$. The matrix A can be taken to be equal to A^ε_n as defined before Lemma 1.4. Recall that if f is a weight k modular form, its Fourier expansion at the cusp $A^\varepsilon_n\infty$ is given by the Fourier expansion of the form $f|_k[(A^\varepsilon_n)^{-1}]$ at the infinity cusp.

Let $\mathcal{F}^\varepsilon_{ns}(p)$ be the field of rational meromorphic functions for the Cartan non-split group $\Gamma^\varepsilon_{ns}(p)$, *i.e.*, $\mathcal{F}^\varepsilon_{ns}(p) := \mathbb{Q}(j, \sum_i f_{a\beta_i})$. Combining Proposition 1.15 with Lemma 1.4, it is easy to see that $\mathcal{F}^\varepsilon_{ns}(p)$ consists of all meromorphic functions invariant for $\Gamma^\varepsilon_{ns}(p)$, whose q-expansions at infinity belong to $\mathbb{Q}(\xi_p)$ and such that the Fourier expansion at $\sigma_n(\infty)$ equals $\sigma_{n^{-1}}(f)$. As in Remark 1.16, the same argument applies to other weights.

Definition 1.22 (Rational Modular Forms) A form $f \in S_2(\Gamma^\varepsilon_{ns}(p))$ is called *rational* if its q-expansion at every cusp belongs to $\mathbb{Q}(\xi_p)$ and the expansion at the cusp $\sigma_n(\infty)$ equals that of $\sigma_{n^{-1}}(f)$ at the infinity cusp for all n relatively prime to p.

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

Proposition 1.23 *If $f \in S_2(\Gamma^\varepsilon_{ns}(p))$ is rational, it defines a rational meromorphic differential form $f(q)\frac{dq}{q}$ on $X^\varepsilon_{ns}(p)$, where $q = e^{(2\pi i z)/p}$.*

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 $\mathcal{F}^\varepsilon_{ns}(p)$ and $\frac{pj'}{2\pi i}$ is a rational meromorphic function with respect to $\mathrm{SL}_2(\mathbb{Z})$ (of weight two) , their quotient lies in $\mathcal{F}^\varepsilon_{ns}(p)$ as claimed. ∎

Theorem 1.21 says that g_ε has q-expansion with coefficients in $\mathbb{Q}(\xi_p)$. If we multiply the form by any constant in such field, the same holds. What is the right way to normalize g_ε?

Theorem 1.24 *Let $g_\varepsilon \in S_2(\Gamma^\varepsilon_{ns}(p))$ be an eigenform with rational eigenvalues. Then there exists a constant $c \in \mathbb{Q}(\xi_p)$ such that cg_ε is rational. Such a constant is unique up to multiplication by a non-zero rational number.*

Proof It is clear that c, if exists, is unique up to multiplication by a non-zero rational number. By Proposition 1.7, it is enough to find $c \in \mathbb{Q}(\xi_p)$ such that that for all prime numbers ℓ, $T_\ell(cg_\varepsilon) = \lambda_\ell \sigma_{\ell^{-1}}(cg_\varepsilon)$.

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 $T_\ell g_\varepsilon = \lambda_\ell c_\ell \sigma_{\ell^{-1}}(g_\varepsilon)$. We need to find a non-zero $c \in \mathbb{Q}(\xi_p)$ such that $T_\ell(cg_\varepsilon) = \lambda_\ell \sigma_{\ell^{-1}}(cg_\varepsilon)$, *i.e.*, $c_\ell = \sigma_{\ell^{-1}}(c)/c$.

Let ℓ be such that its class modulo p is a generator of $\mathbb{F}_p^*$ and let $\{\ell_i\}_{1\le i\le p-1}$ be distinct primes in the same class of ℓ modulo p such that $\lambda_{\ell_i} \neq 0$ (since g does not have complex multiplication, such primes exist by Serre's open image theorem or Sato-Tate theorem). In that case, $\prod_{i=1}^{p-1} \ell_i \equiv 1 \bmod p$ and

$$\begin{aligned}(\Pi\, \lambda_{\ell_i}) g_\varepsilon = \mathscr{T}_{\Pi\, \ell_i}(g_\varepsilon) = T_{\Pi\, \ell_i}(g_\varepsilon) = T_{\ell_1} \circ \cdots \circ T_{\ell_{p-1}}(g_\varepsilon) \\ = (\Pi\, \lambda_{\ell_i})\, \mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}(\xi_p)}(c_\ell) g_\varepsilon.\end{aligned}$$

Since $\mathrm{Nm}_{\mathbb{Q}}^{\mathbb{Q}(\xi_p)}(c_\ell) = 1$, by Hilbert's 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 relatively prime to p. ∎

Remark 1.25 Let $g_\varepsilon \in S_2(\Gamma_{ns}^{\varepsilon+}(p))$. If $\ell \equiv -1 \bmod p$, 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 $g_\varepsilon \in S_2(\Gamma_{ns}^{\varepsilon-}(p))$, the coefficients will be purely imaginary.

Note that even for a rational modular form, it is not clear how to choose the rational multiple that 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 1.26 The *proper normalization* of g_ε is the unique (up to sign) renormalization G_ε of g_ε that satisfies the following.

- G_ε is a rational newform.
- The Fourier expansion of G_ε has algebraic integer coefficients.
- If $n \in \mathbb{Z}$ and $n \geq 2$, then $\frac{G_\varepsilon}{n}$ does not have integral coefficients.

Remark 1.27 If $G_\varepsilon \in S_2(\Gamma_{ns}^{\varepsilon}(p))$ is a properly-normalized eigenform with rational eigenvalues, then $\sigma_n(G_\varepsilon) \in S_2(\Gamma_{ns}^{\varepsilon n^2}(p))$ is a properly-normalized eigenform with rational eigenvalues. Moreover since G_ε is rational, we must have $\sigma_n(G_\varepsilon) = G_\varepsilon|_k[(A_n^\varepsilon)]$ (see Definition 1.22).

1.7 Eichler–Shimura

The Eichler–Shimura construction ([Shi94, Theorem 7.9]) associates with G_ε the abelian variety $\mathscr{A}_{G_\varepsilon} := \mathrm{Jac}(X_{ns}^\varepsilon(p))/(I_{G_\varepsilon}\, \mathrm{Jac}(X_{ns}^\varepsilon(p)))$, where I_{G_ε} is the kernel of

https://doi.org/10.4153/CJM-2015-047-6 Published online by Cambridge University Press

the morphism from $R(\Gamma_{ns}^{\varepsilon}(p), \Delta_{ns}^{\varepsilon}(p)) \to \mathbb{Z}$ which is given by sending $\mathscr{T}_n^{\varepsilon}$ to the eigenvalue λ_n. We have the diagram

$$\begin{tikzcd} X_{ns}^{\varepsilon}(p) \arrow[r, hook, "i"] \arrow[dr, dotted] & \operatorname{Jac}(X_{ns}^{\varepsilon}(p)) \arrow[d] \\ & \mathscr{A}_{G_\varepsilon} \end{tikzcd}$$

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 given by integrating the differential form $G_\varepsilon(q)\frac{dq}{q}$ and its Galois conjugates over cycles. By Proposition 1.23 this differential is rational, thus the abelian variety $\mathscr{A}_{G_\varepsilon}$ is of dimension 1, and by Theorem 1.11 isogenous to the strong Weil curve E_g attached to g. The elliptic curve $\mathscr{A}_{G_\varepsilon}$ will be called the optimal quotient of $\operatorname{Jac}(X_{ns}^{\varepsilon}(p))$ (note that it might not be isomorphic to E_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

$$\begin{tikzcd} X_{ns}^{\varepsilon}(p) \arrow[r, hook, "\iota"] \arrow[dr, dotted, "\Phi_p^{\varepsilon}"'] & \operatorname{Jac}(X_{ns}^{\varepsilon}(p)) \arrow[d] \\ & \mathscr{A}_{G_\varepsilon} \end{tikzcd}$$

where ι is the map sending P to $\sum_{\sigma \in \operatorname{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})} (P) - (\sigma(\infty))$. This is the right and natural definition to make a map defined over $\mathbb{Q}$ out of i. Therefore, the dot map (that we still call *modular parametrization*) is defined over $\mathbb{Q}$.

Remark 1.28 If $G_\varepsilon \in S_2(\Gamma_{ns}^{\varepsilon+}(p))$, since the normalizer has $(p-1)/2$ cusps, all defined and conjugate 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 1.29 *Let n be relatively prime to p. Then $\mathscr{A}_{G_\varepsilon} = \mathscr{A}_{G_{\varepsilon n^2}}$.*

Proof It is enough to see that the lattice of periods of G_ε is the same as the lattice of periods of $\sigma_n(G_\varepsilon) = G_{\varepsilon n^2}$ which is a rational eigenform for $S_2(\Gamma_{ns}^{\varepsilon n^2}(p))$ (Remark 1.27). Let D be the closed cycle $\{\tau, M^\varepsilon \tau\}$ with $M^\varepsilon \in \Gamma_{ns}^{\varepsilon}(p)$. Integrating G_ε over that cycle, we get

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

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

$$\int_{[A_n^\varepsilon]^{-1}\tau}^{[A_n^\varepsilon]^{-1}M^\varepsilon \tau} G_\varepsilon|_k[(A_n^\varepsilon)]\frac{dq}{q} = \int_{[A_n^\varepsilon]^{-1}\tau}^{[A_n^\varepsilon]^{-1}M^\varepsilon[A_n^\varepsilon][A_n^\varepsilon]^{-1}\tau} \sigma_n(G_\varepsilon)\frac{dq}{q}.$$

https://doi.org/10.4153/CJM-2015-047-6 Published online by Cambridge University Press

This expression is the integral of $\sigma_n(G_\varepsilon)$ over the cycle $\{\tau', [A_n^\varepsilon]^{-1}M^\varepsilon[A_n^\varepsilon]\tau'\}$, where $\tau' = [A_n^\varepsilon]^{-1}\tau$. Since $[A_n^\varepsilon]^{-1}M^\varepsilon[A_n^\varepsilon] \in \Gamma_{ns}^{\varepsilon n^2}(p)$, it gives a closed cycle on $\mathrm{Jac}(X_{ns}^{\varepsilon n^2}(p))$. ∎

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

Proposition 1.30 *Let Λ_{G_ε} be the lattice attached to G_ε and c the Manin constant. Let $\Phi_\omega\colon \mathbb{C}/\Lambda_{G_\varepsilon} \to E$ be the Weierstrass uniformization. Then $\Phi_p^\varepsilon(\tau) = \Phi_\omega(z_\tau)$, where*

$$z_\tau = c\left(\frac{2\pi i}{p}\Big(\sum_{\sigma_n\in\mathrm{Gal}(\mathbb{Q}(\xi_p)/\mathbb{Q})} \int_\infty^{A_n^{\varepsilon\,-1}\tau} \sigma_n(G_\varepsilon)(z)dz\Big)\right)$$

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

$$\int_{\sigma_n(\infty)}^{\tau} G_\varepsilon(q)\frac{dq}{q} = \int_\infty^{A_n^{\varepsilon\,-1}\tau} G_\varepsilon|_2[A_n^\varepsilon](q)\frac{dq}{q} = \int_\infty^{A_n^{\varepsilon\,-1}\tau} \sigma_n(G_\varepsilon(q))\frac{dq}{q}.$$ ∎

2 General Levels

In this section we generalize the previous results to more general conductors. Thanks to the Chinese Remainder Theorem, the theory works in exactly the same way 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–Wiles, there exists an eigenform $g \in S_2^{\mathrm{new}}(\Gamma_0(N^2m))$ with rational eigenvalues whose attached elliptic curve is isogenous to E. 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 from the previous section. We consider tuples $(E,\psi,\phi_1,\dots,\phi_r)$, where $E/\mathbb{C}$ is an elliptic curve, $\psi\colon E \to E'$ is a cyclic degree m isogeny (or equivalently a cyclic subgroup of order m), and $\phi_i \in \mathrm{End}_{\mathbb{F}_{p_i}}(E[p_i])$ 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 1.11.

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

Proof Let $X(Nm)$ be the modular curve that 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 $\phi\colon(\mathbb{Z}/Nm)_S^2 \mapsto E[Nm]$ is an isomorphism of group schemes over S. The group $\mathrm{GL}_2(\mathbb{Z}/Nm)$ acts on

https://doi.org/10.4153/CJM-2015-047-6 Published online by Cambridge University Press

the right on $X(Nm)$. If Γ is any subgroup of $\mathrm{GL}_2(\mathbb{Z}/Nm)$, one can consider the quotient $X(Nm)/\Gamma$ via an appropriate moduli interpretation. We are interested in the following two subgroups (as subgroups of $\mathrm{GL}_2(\mathbb{Z}/Nm)$): $\Gamma_{ns}^{\vec{\varepsilon}}(N,m)$ and $\widetilde{\Gamma} := \cap_{i=1}^{r} T(p_i) \cap \Gamma_0(m)$, 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 $\Gamma_2 = \cap_{i=2}^{r} T(p_i) \cap \Gamma_0(p_1^2 m)$. But in this case, one can prove [Edi96, Proposition 1.2] in exactly the same way, where now the subgroups of that 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 [Edi96, Theorem 1.3] proves our claim. ∎

The previous theorem, together with the comments in the proof of Theorem 1.11, imply that there exists $g_{\vec{\varepsilon}} \in S_2(\Gamma_{ns}^{\vec{\varepsilon}}(N,m))$ with the same eigenvalues for the Hecke operators $\mathscr{T}_n^{\vec{\varepsilon}}$ as g outside the primes p_i. The theory works in the same way as 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 cyclic 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 $v_n^{\vec{\varepsilon}}$, as well as coset representatives, are defined via a matrix $A_n^{\vec{\varepsilon}} \in \Gamma_0(m)$ that satisfies the corresponding congruence modulo all the prime numbers p_i.

Note that $\sigma_{n^{-1}}$ and T_n will send modular forms for $\Gamma_{ns}^{\vec{\varepsilon}}(N,m)$ to modular forms for $\Gamma_{ns}^{\vec{\varepsilon}/n^2}(N,m)$, and all the results from the previous section generalize trivially. In particular, we have the analogue of Theorem 1.13.

Theorem 2.2 *Let $g_{\vec{\varepsilon}} \in S_2(\Gamma_{ns}^{\vec{\varepsilon}}(N,m))$ be an eigenform with the same eigenvalues as g away from N. Then there exist eigenforms $h_i \in S_2(\Gamma_0(N_i m),\chi_i)$, with $N_i \mid N^2$, and χ_i a character modulo N^2/N_i such that*

$$\widetilde{g}_{\vec{\varepsilon}} = \sum_{\chi} a_\chi (g\otimes\chi) + \sum_i b_i h_i,$$

where the first sum is over all characters modulo N.

Remark 2.3 As in Theorem 1.13, the forms h_i are exactly those forms such that when twisted by the appropriate character modulo N, we obtain the newform g. Furthermore, the existence (or non-existence) of such forms is given by the type of the local automorphic representation of g at the primes dividing N.

Using this theorem we can also compute the Fourier expansion and define $G_{\vec{\varepsilon}}$ as a proper-normalization of $g_{\vec{\varepsilon}}$. 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

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

Using the Fourier expansion of $G_{\vec{\varepsilon}}$, 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 on the upper half plane.

Summing up, we have obtained a modular parametrization

$$\Phi_N^{\vec{\varepsilon}}: X_{ns}^{\vec{\varepsilon}}(N,m) \longrightarrow E(\mathbb{C}) \tag{2.1}$$

defined over $\mathbb{Q}$. We make the following observation about the Manin constant, which is supported by the evidence shown in the examples.

Conjecture 2.4 The Manin constant belongs to $\mathbb{Z}[1/N]$.

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

3 Heegner Points on General Cartan Non-split Curves

Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathcal{O} = \langle 1, \omega \rangle$ be an order in an imaginary quadratic field K. We say that the pair $(E, \mathcal{O})$ satisfies the *Cartan–Heegner hypothesis* if the following hold.

- The conductor of E is $N^2 m$, where $\gcd(N,m) = 1$ and N is an odd square-free number.
- The discriminant d of $\mathcal{O}$ is prime to Nm.
- Every prime dividing m is split in $\mathcal{O}$.
- Every prime dividing N is inert in $\mathcal{O}$.

Note that $\mathcal{O}$ satisfies the classical Heegner hypothesis at the primes dividing m but not at the primes dividing N; therefore, we will not be able to construct Heegner points on $X_0(N^2m)$. Given a pair $(E, \mathcal{O})$ satisfying the Cartan–Heegner hypothesis, we will use the letters N and m to denote the factorization of the conductor of E as in the definition.

Recall that a matrix $M \in M_{2\times 2}(\mathbb{Z})$ with $\mathrm{Tr}(M) = \mathrm{Tr}(\omega)$ and $\det(M) = \mathrm{Nm}(\omega)$ gives an embedding $\mathcal{O} \hookrightarrow M_{2\times 2}(\mathbb{Z})$ given by sending ω to M. A Heegner point on $X_{ns}^{\vec{\varepsilon}}(N,m)$ with endomorphism ring $\mathcal{O}$ is a point τ on the upper half plane that is fixed by a matrix $M \in M_{ns}^{\vec{\varepsilon}}(N) \cap M_0(m)$ satisfying the above conditions.

Let H be the Hilbert class field of $\mathcal{O}$. One associates the elliptic curve $E_\tau = \mathbb{C}/\langle 1, \tau \rangle$ with a Heegner point τ. The fact that τ is fixed by M allows to associate with τ a pair of points in $X_{ns}^{\vec{\varepsilon}}(N,m)(H)$ conjugate under $\mathrm{Gal}(H/\mathbb{Q}(j(E_\tau)))$ (see [Ser97] Appendix 5 for more details). A Heegner point on E with endomorphism ring $\mathcal{O}$ is the image of a Heegner point with endomorphism ring $\mathcal{O}$ in $X_{ns}^{\vec{\varepsilon}}(N,m)(H)$ under the modular parametrization (2.1).

3.1 Moduli Interpretation

In order to construct systems of Heegner points, it is also useful to have a definition of Heegner points in terms of the moduli interpretation.

Definition 3.1 A Heegner point on $X_{ns}^{\vec{\varepsilon}}(N,m)$ is a tuple $[\mathscr{O},[\mathfrak{a}],\mathfrak{m},\phi_\alpha]$ where $\mathscr{O}$ is as before, $[\mathfrak{a}]$ is an element in $\mathrm{Pic}(\mathscr{O})$ that determines an elliptic curve $E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ with complex multiplication by $\mathscr{O}$, $\mathfrak{m}$ is a cyclic ideal in $\mathscr{O}$ of norm m, and $\phi_\alpha \in \prod_{p|N} \mathrm{End}_{\mathbb{F}_p}(E_{\mathfrak{a}}[p])$ is such that

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

Remark 3.2 The element α is well defined modulo N, which is a product of inert primes of $\mathscr{O}$, so we can just take $\alpha \in \mathscr{O}/N$.

Proposition 3.3 *Let* $[\mathscr{O},[\mathfrak{a}],\mathfrak{m},\phi_\alpha]$ *be a Heegner point.*

(i) *If τ denotes complex conjugation, then* $(\mathscr{O},[\mathfrak{a}],\mathfrak{m},\phi_\alpha)^\tau = (\mathscr{O},[\mathfrak{a}^{-1}],\overline{\mathfrak{m}},\phi_{-\alpha})$

(ii) *Let $[\mathfrak{b}]$ be a fractional ideal, and let $\sigma_{\mathfrak{b}} \in \mathrm{Gal}(H/K)$ be the Artin symbol associated with $[\mathfrak{b}]$. Then*

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

(iii) *If $p \mid N$, then $\omega_p(\mathcal{O},[\mathfrak{a}],\mathfrak{m},\phi_\alpha) = (\mathcal{O},[\mathfrak{a}],\mathfrak{m},\phi_{-\alpha})$, where ω_p is defined as in Remark 1.3.*

Proof Items (i) and (ii) follow from [Ser67] (since $\mathfrak{m}$ and α are defined over K), while (iii) follows from Remark 1.3. ∎

Using the geometric interpretation of Hecke operators as described in Section 1.3.1, it is clear that we have the following formula for Hecke operators (for ℓ relatively prime to Nm) acting on Heegner points, analogous to the one given in [Gro84, Section 6]:

$$\mathscr{T}_\ell^{\vec{\varepsilon}}\big([\mathscr{O},\mathfrak{a},\mathfrak{m},\phi_\alpha]\big) = \sum_{\mathfrak{a}/\mathfrak{b}\cong\mathbb{Z}/\ell}\big(\mathrm{End}(\mathfrak{b}),\mathfrak{b},\mathfrak{m}\cdot\mathrm{End}(\mathfrak{b})\cap\mathrm{End}(\mathfrak{b}),\phi_\alpha\big). \tag{3.1}$$

3.2 Heegner Systems

Fix an elliptic curve E as before, and let K be an imaginary quadratic field whose maximal order satisfies the Cartan–Heegner hypothesis. Let n be a positive integer prime to $\mathrm{Cond}(E)\cdot\mathrm{Disc}(K)$. Let $\mathscr{O}_n$ be the unique order in K of conductor n and let K_n be the corresponding Hilbert class field. The order $\mathscr{O}_n$ satisfies the Cartan–Heegner hypothesis, so, it gives rise to a set of Heegner points $HP(n) \subset E(K_n)$.

Proposition 3.4

(i) *Let n be an integer and let ℓ be a prime number, both relatively prime to* $\mathrm{Cond}(E)\cdot\mathrm{Disc}(K)$. *Consider any $P_{n\ell} \in HP(n\ell)$. Then there exist points $P_n \in E(H_n)$ and (when $\ell \mid n$) $P_{n/\ell} \in HP(n/\ell)$ such that*

- *if $\ell \nmid n$ is inert in K,* $\mathrm{Tr}_{K_{n\ell}/K_n} P_{n\ell} = a_\ell P_n$;

- *if* $\ell = \lambda\bar{\lambda} \nmid n$ *is split in* K, $\mathrm{Tr}_{K_{n\ell}/K_n} P_{n\ell} = (a_\ell - \sigma_\lambda - \sigma_\lambda^{-1})P_n$;
- *if* $\ell \mid n$, $\mathrm{Tr}_{K_{n\ell}/K_n} P_{n\ell} = a_\ell P_n - P_{n/\ell}$.

where $a_\ell = 1 + \ell - \mathrm{card}(\widetilde{E}(\mathbb{F}_\ell))$*;*

(ii) *There exists* $\sigma \in \mathrm{Gal}(K_n/K)$ *such that*

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

where τ *is complex conjugation and* $\mathrm{sign}(E,\mathbb{Q})$ *is the root number of* $E/\mathbb{Q}$.

Proof From Proposition 3.3, equation (3.1), and the discussion in between, the result follows quite formally. See, for example, [Gro91, Propositions 3.7 and 5.3] or [Dar04, Section 3.4] and [GZ86, section II.1]. ∎

Definition 3.5 A *Heegner system* attached to (E,K) is a collection of points $P_n \in E(K_n)$ (one for each positive integer n relatively prime to $\mathrm{Cond}(E)\cdot\mathrm{Disc}(K)$) that satisfies the conditions of the previous Proposition.

If E is a rational elliptic curve and K satisfies the Cartan–Heegner hypothesis, we can obtain a Heegner system from the Heegner points on the elliptic curve E. Given a Heegner system, Kolyvagin's machinery works, and we get the following result.

Theorem 3.6 *Let* $\{P_n\}$ *be the Heegner system attached to* (E,K) *as constructed above, where the elliptic curve does not have complex multiplication. Define* $P_K = Tr_{K_1/K}P_1 \in E(K)$. *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 [Dar04, Theorem 10.1]. ∎

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

Theorem 3.7 (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]. Note that 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. ∎

Remark 3.8 Zhang's formula is proved for points on the Jacobian of the Cartan non-split curve. To get some version of the Birch and Swinnerton–Dyer conjecture in this context, the Manin constant and the degree of the modular parametrization need to be computed for such curve. Unfortunately, no such formulas are known.

4 Computational Digression

4.1 Computing Eigenforms

Let $g \in S_2(\Gamma_0(N^2m))$ be an eigenform with rational eigenvalues. We need to compute the Fourier expansion of $g_{\vec{\varepsilon}}$.

Lemma 4.1 *We have* $\Gamma_{ns}^{\vec{\varepsilon}}(N,m)/(\Gamma(N)\cap\Gamma_0(m)) \simeq \prod_{p\mid N}\mathbb{Z}/(p+1)$.

Proof The morphism $\Gamma_{ns}^{\varepsilon}(p)/\Gamma(p) \to \mathbb{F}_p[\sqrt{\varepsilon}]$ given by $\left(\begin{smallmatrix} a & b \\ \varepsilon b & a\end{smallmatrix}\right) \to a + b\sqrt{\varepsilon}$ sends $\Gamma_{ns}^{\varepsilon}(p)/\Gamma(p)$ to $\{\alpha \in \mathbb{F}_{p^2}^{\times} : \mathrm{Nm}(\alpha) = 1\}$, which is isomorphic to $\mathbb{Z}/(p+1)$. The result follows from the Chinese Remainder Theorem. ∎

To compute the Fourier expansion of $g_{\vec{\varepsilon}}$ we proceed as follows.

(a) We compute the local type at each prime dividing N. This can be done either by looking at the reduced curve and the field where it gets semi-stable reduction or by considering twists, as in [Pac13]. Using the local type information, we compute the newforms h_i of smaller level that appear in Theorem 2.2. If there are some ramified principal series primes, one can compute the form from the elliptic curve as explained in Appendix A.

(b) Once we have all the forms appearing in Theorem 2.2, we are led to compute the linear combination. We take a formal linear combination with variables x_i. The forms appearing are invariant under $\Gamma(N)\cap\Gamma_0(m)$, so we have to impose invariance under $\Gamma_{ns}^{\vec{\varepsilon}}(N,m)/(\Gamma(N)\cap\Gamma_0(m))$. Using Lemma 4.1 we get a set $\{\alpha_i\}_i$ of generators for the quotient. Imposing invariance under α_i (via evaluating the linear combination at some point in $\mathcal{H}$) gives a linear equation on the x_i's (with complex coefficients). Asking invariance for the whole set of generators, we get a linear system, whose solution set $\mathfrak{G}_g$ are the forms in $S_2(\Gamma_{ns}^{\vec{\varepsilon}}(N,m))$ with the same eigenvalues as g for $n \equiv 1 \pmod{N}$.

By Theorem 1.12, $\mathfrak{G}_g$ is the set of twists of the newform g by quadratic characters χ modulo N that are newforms of level N^2m. This implies that the space $\mathfrak{G}_g$ has dimension 2^d, where d is the number of primes dividing N, where the local representation is supercuspidal or a principal series (minimal by quadratic twist). We need to pin down $g_{\vec{\varepsilon}}$. Let $p \mid N$ be a prime number and let $\varkappa_p$ be the quadratic character modulo p.

Fact 1: If π_p is supercuspidal, let ϵ_p denote the local sign at p. If $\epsilon_p = 1$, then g can be written as a linear combination such as in Theorem 2.2 where only twists of g by characters with 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.

Fact 2: If π_p is Principal Series, let q be a non-square modulo p. The operator $\mathcal{T}_q^{\varepsilon} = T_q v_q^{\varepsilon}$ acts as λ_q on the subspace spanned by $g_{\vec{\varepsilon}}$ and as $-\lambda_q$ on the subspace spanned by $(g\otimes\varkappa_p)_{\vec{\varepsilon}}$.

Proof of Fact 1: Recall from Remark 1.14 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 $-\left(\frac{-1}{p}\right) = -\varkappa_p(-1)$. Therefore, the variation of the sign at p of the characters involved in the combination for g and $g \otimes \varkappa_p$ are different.

Each condition halves the dimension and altogether determine $g_{\vec{\varepsilon}}$ up to a constant. Note that the solution is computed using real arithmetic, so from an approximate solution, we first normalize it such that the first Fourier coefficient is 1 (so all coefficients lie in $\mathbb{Q}(\xi_N)$) and then we proper-normalize it using an explicit version of Hilbert's 90 Theorem. Finally, recall that if $\gcd(n, N) = 1$, the n-th coefficient b_n of $\widetilde{G}_{\vec{\varepsilon}}$ satisfies

$$b_n = \lambda_n \sigma_{n^{-1}}(b_1).$$

Thus, we can obtain the exact Fourier expansion once we have found $b_1 \in \mathbb{Q}(\xi_N)$ and the coefficients at the various p_i^{α}.

4.2 Computing Heegner Points

Let $\{\mathfrak{a}_i\}$ be a set of representatives of the Class group of $\mathcal{O}$ and let $\omega_i \in \mathcal{H}$ be such that $\mathfrak{a}_i = \langle 1, \omega_i \rangle$. Let M_{ω_i} be the set of matrices in $M_2(\mathbb{Z})$ that fixes ω_i, which is an order isomorphic to $\mathcal{O}$. Then M_{ω_i} contains a matrix N_i satisfying $\operatorname{Tr}(N_i) = \operatorname{Tr}(\omega)$ and $\det(N_i) = \operatorname{Nm}(\omega)$.

Claim: there exists $A_i \in \mathrm{SL}_2(\mathbb{Z})$ such that $A_i N_i {A_i}^{-1} \in M_{ns}^{\vec{\varepsilon}}(N) \cap M_0(m)$.

Then the point $\tau_i = A_i \omega_i$ is a Heegner point on $X_{ns}^{\vec{\varepsilon}}(N, m)$ with endomorphism ring $\mathcal{O}$, as wanted.

The matrices A_i are computed in the following way:

- At a prime p dividing m, we chose $A_i^{(p)}$ modulo $p^{\nu_p(m)}$ 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 for the Jordan form.
- At a prime p dividing N, since p is inert in K, the characteristic polynomial of N_i is irreducible in $\mathbb{F}_p[x]$. If $N_i = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, then we want the matrix A_i to satisfy

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

  We just chose A_i as a matrix in 4 indeterminates and search for a non-zero solution of the system (the determinant of this system 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.

Lastly, the Chinese Remainder Theorem gives a matrix in $\mathrm{SL}_2(\mathbb{Z}/N^2 m\mathbb{Z})$ satisfying our hypotheses, and we lift it to a matrix in $\mathrm{SL}_2(\mathbb{Z})$.

5 Examples

In Table 1 we show some examples of our method. All of the examples were calculated using Pari/GP [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 supercuspidal, Steinberg and ramified principal series,

https://doi.org/10.4153/CJM-2015-047-6 Published online by Cambridge University Press

respectively. The next column 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 $M_i := A_i N_i A_i^{-1}$ for some $\vec{\varepsilon}$. The next column contains the first Fourier coefficient (where we use the notation $\zeta_i := \xi_N^i + \overline{\xi_N}^i$, and a vector $[a_1, \ldots, a_N]$ means $a_1\zeta_1 + \cdots + a_N\zeta_N$), and the last column gives the Manin constant c for the optimal quotient.

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

Table 1: Examples of the q-expansion and related computational data

Remark 5.1 In all examples of Table 1 except 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.

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	$\mathbb{Q}(\sqrt{-3})$	$\left(\frac{2411156245}{(37062)^2}, -\frac{52866724475375}{(37602)^3}\right)$	15
225a	$\mathbb{Q}(\sqrt{-91})$	$(1,1)$	1
225a	$\mathbb{Q}(\sqrt{-7})$	$(-1,0)$	2
289a	$\mathbb{Q}(\sqrt{-3})$	$\left(-\frac{15858973521095}{1083383^2}, -\frac{22895413346586388187}{1083383^3}\right)$	3
1617a	$\mathbb{Q}(\sqrt{-2})$	$\left(\frac{3702}{17^2}, \frac{184078}{17^3}\right)$	3
49a	$\mathbb{Q}(\sqrt{-11})$	$\left(\frac{1261982}{11(127)^2}, -\frac{680991}{11(127)^2} - \frac{327847275}{11^2(127)^3}\sqrt{-11}\right)$	3

Table 2: Heegner points constructed

Appendix A The Principal Series Case Computation

The purpose of this short appendix is to show how the work [DD11] (in particular example 5) allows us 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 to us some details of the algorithm.

(a) Compute v_p = the valuation at p of the discriminant of E. The order of the character is $e := 12/(\gcd(12, v_p))$.

(b) 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 two forms, conjugate to each other), but we need to match each root with its corresponding character.

(c) 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 $\chi_{L'}(t)$.

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 thank Professors Imin Chen and Bas Edixhoven for explaining some 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.

References

[AL78] A. O. L. Atkin and W. C. W. Li, *Twists of newforms and pseudo-eigenvalues of W-operators.* Invent. Math. **48**(1978), no. 3, 221–243. http://dx.doi.org/10.1007/BF01390245 http://dx.doi.org/10.1007/BF01390245

[Che98] I. Chen, *The Jacobians of non-split Cartan modular curves.* Proc. London Math. Soc. 77(1998), 1–38. http://dx.doi.org/10.1112/S0024611598000392

[Dar04] H. Darmon, *Rational points on modular elliptic curves.* CBMS Regional Conference Series in Mathematics, 101, American Mathematical Society, Providence, RI, 2004.

[DD11] T. Dokchitser and V. Dokchitser, *Euler factors determine local Weil representations.* arxiv:1112.4889

[DS05] F. Diamond and J. Shurman, *A first course in modular forms.* Graduate Texts in Mathematics, 228, Springer-Verlag, New York, 2005.

[dSE00] B. de Smit and B. Edixhoven, *Sur un résultat d'Imin Chen.* Math. Res. Lett. 7(2000), no. 2–3, 147–153. http://dx.doi.org/10.4310/MRL.2000.v7.n2.a1

[Edi96] B. Edixhoven, *On a result of Imin Chen.* arxiv:alg-geom/9604008

[Gro84] B. H. Gross, *Heegner points on X0(N).* In: Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105.

[Gro91] ———, *Kolyvagin's work on modular elliptic curves.* In: L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., 153, Cambridge University Press, Cambridge, 1991, pp. 235–256. http://dx.doi.org/10.1017/CBO9780511526053.009

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series.* Invent. Math. **84**(1986), no. 2, 225–320. http://dx.doi.org/10.1007/BF01388809

[Lan87] S. Lang, *Elliptic functions.* Second ed., Graduate Texts in Mathematics, 112, Springer-Verlag, New York, 1987. http://dx.doi.org/10.1007/978-1-4612-4752-4

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld).* Invent. Math. **44**(1978), no. 2, 129–162. http://dx.doi.org/10.1007/BF01390348

[Pac13] A. Pacetti, *On the change of root numbers under twisting and applications.* Proc. Amer. Math. Soc. **141**(2013), no. 8, 2615–2628. http://dx.doi.org/10.1090/S0002-9939-2013-11532-7

[PAR14] PARI Group, Bordeaux. PARI/GP version 2.7.0, 2014. http://pari.math.u-bordeaux.fr/

[Raj98] C. S. Rajan, *On strong multiplicity one for l-adic representations.* Internat. Math. Res. Notices **1998**, no. 3, 161–172. http://dx.doi.org/10.1155/S1073792898000142

[RW14] M. Rebolledo and C. Wuthrich, *A moduli interpretation for the non-split Cartan modular curve.* arxiv:1402.3498

[Ser67] J.-P. Serre, *Complex multiplication.* In: Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 292–296.

[Ser97] ———, *Lectures on the Mordell-Weil theorem.* Third ed., Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1997.

[Shi94] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Publications of the Mathematical Society of Japan, 11, Princeton University Press, Princeton, NJ, 1994.

[Zha01] S.-W. Zhang, *Gross-Zagier formula for GL2.* Asian J. Math. 5(2001), no. 2, 183–290.

[Zha04] ———, *Gross-Zagier formula for GL(2). II.* In: Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., 49, Cambridge University Press, Cambridge, 2004, pp. 191–214. http://dx.doi.org/10.1017/CBO9780511756375.008

IMAS-CONICET, Buenos Aires, Argentina
e-mail: kohendaniel@gmail.com

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires and IMAS, CONICET, Argentina
e-mail: apacetti@dm.uba.ar