Invent. math. 98, 75–106 (1989)

Inventiones mathematicae
© Springer-Verlag 1989

Stickelberger elements and modular parametrizations of elliptic curves

Glenn Stevens*
Boston University, Department of Mathematics, Boston, MA 02215, USA

In the present paper we shall give evidence to support the claim (Conjecture I below and (1.3)) that every elliptic curve $A_{/\mathbf{Q}}$ which can be parametrized by modular functions admits a *canonical* modular parametrization whose properties can be related to intrinsic properties of A. In particular, we will see how such a parametrization can be used to prove some rather pleasant integrality properties of Stickelberger elements ad p-adic L-functions attached to A. In addition, if Conjecture I is true then we can give an *intrinsic* characterization of the isomorphism class of a special elliptic curve in the $\mathbf{Q}$-isogeny class of A distinguished by modular considerations.

For most of the paper we have opted for the concrete approach and defined modular parametrizations in terms of $X_1(N)$ (Definition 1.1). However, to justify our view of these parametrizations as being canonical, we begin here with a more intrinsic definition. Recall that Shimura ([19], Chap. 6; see § 1 of this paper) has defined a compatible system of canonical models of modular curves $\{X_S,\ S\in\mathscr{S}\}$, where $\mathscr{S}$ is a certain collection of open subgroups of the group $\mathrm{GL}(2, \mathbf{A}_f)$ over the finite adeles $\mathbf{A}_f$ of $\mathbf{Q}$. We define the adelic upper half-plane to be the pro-variety $\hat{X}=\varprojlim_{S} X_S$ and give $\hat{X}$ the $\mathbf{Q}$-structure induced by the field of modular functions whose q-expansions at the 0-cusp have coefficients in $\mathbf{Q}$.

A modular parametrization of A is a $\mathbf{Q}$-morphism $\hat{\pi}\colon \hat{X}\to A$ which sends to 0-cusp to the origin of A and for which $\hat{\pi}^*\omega_A=c\cdot f(q)\dfrac{dq}{q}$ where ω_A is a Neron differential on A, f is a normalized weight two newform, and $c\in\mathbf{Q}^*$. We refer to c as the Manin constant of the parametrization $\hat{\pi}$.

In Theorem 1.9 we will see that every modular parametrization factors through a morphism $\pi\colon X_1(N)\to A$ where N is the conductor of A. Thus we lose no generality if we restrict (as we will) our attention to $X_1(N)$-parametrizations.

We will investigate the following basic conjecture and its consequences.

* Research supported by the National Science Foundation.

Conjecture I. *For each modular elliptic curve $A_{/\mathbf{Q}}$ there is a unique (up to sign) modular parametrization $\hat{\pi}: \hat{X} \to A$ whose Manin constant is* ± 1.

This should be viewed as a refinement of a conjecture of Manin [11, 14]. In [14] Mazur and Swinnerton-Dyer introduce what they call the *strong* parametrization, $X_0(N) \to A_0$, of a special curve A_0, the so-called *strong* curve, in the $\mathbf{Q}$-isogeny class of A. This parametrization is determined by the property that its degree is minimal among all $X_0(N)$-parametrizations of curves $\mathbf{Q}$-isogenous to A. For this strong parametrization, Manin [11] conjectured that $c = \pm 1$.

Thus the novelty in our formulation is the assertion that *any* curve in the $\mathbf{Q}$-isogeny class of A can be parametrized by *some* modular curve in such a way that the Manin constant is ± 1. The corresponding statement is false for $X_0(N)$-parametrizations (Example 1.11).

Let $\mathscr{A}$ denote the $\mathbf{Q}$-isogeny class containing A. Following the example of Mazur and Swinnerton-Dyer we distinguish a special modular parametrization of a special curve in $\mathscr{A}$. Define the relative degree of a modular parametrization $\hat{\pi}: \hat{X} \to A$, $A \in \mathscr{A}$ to be $\frac{1}{[\mathrm{SL}(2, \mathbf{Z}): \Gamma_S]} \cdot \deg(\pi_S)$, where $\pi_S: X_S \to A$, $S \in \mathscr{S}$, is any representative of $\hat{\pi}$. As a corollary of Theorem 1.9 we see that there is a unique curve $A_1 \in \mathscr{A}$ and a unique (up to sign) parametrization $\hat{\pi}_1$ of A_1 whose relative degree is minimal among all parametrizations of all curves in $\mathscr{A}$. We refer to A_1 as the *optimal curve* in $\mathscr{A}$ and to $\hat{\pi}_1$ as the *optimal parametrization*. More concretely, the optimal curve is characterized as the curve in $\mathscr{A}$ which occurs as a subvariety of the Jacobian of $X_1(N)$.

As another corollary of Theorem 1.9 we discover that there is a canonical lattice $\mathscr{L}(f) \subseteq \mathbf{C}$ associated to the weight 2 newform f which is defined as follows. For any congruence subgroup Γ of $\Gamma_0(N)$, $f(q)\frac{dq}{q}$ defines a regular differential 1-form on the Riemann surface X_Γ associated to Γ. The periods of $f(q)\frac{dq}{q}$ over singular 1-cycles on X_Γ span a lattice $\mathscr{L}_\Gamma(f)$ in the complex numbers. We define

$$\mathscr{L}(f) = \bigcap_{\Gamma \subseteq \Gamma_0(N)} \mathscr{L}_\Gamma(f).$$

Using Theorem 1.9 we derive the equality $\mathscr{L}(f) = \mathscr{L}_{\Gamma_1(N)}(f)$. Thus $\mathscr{L}(f)$ is a full lattice in $\mathbf{C}$.

We feel that the lattice $\mathscr{L}(f)$ induces the 'right' integral structure within which one should measure integrality properties of special values of L-functions associated to f. This point of view is motivated in part by §2 of [21] especially Theorem 2.1. Our basic conjecture relates $\mathscr{L}(f)$ to the period lattices of elliptic curves associated to f (see (2.9)). It is this relation which allows us to deduce integrality properties of values of L-functions in §§3 and 4. Conversely, in §6 we will use arithmetic properties of values of L-functions to prove a weak form (2.4) of the conjecture for certain elliptic curves with complex multiplication.

In §2 we show that if $\mathscr{A}$ is any $\mathbf{Q}$-isogeny class of elliptic curves (modular or not), then there is a canonical curve $A_{\min}$ in $\mathscr{A}$ whose Neron lattice $\mathscr{L}(A_{\min})$

is contained in the Neron Lattice $\mathscr{L}(A)$ of any other curve $A \in \mathscr{A}$. Equivalently, $A_{\min}$ is distinguished as the curve of minimal Parshin-Faltings height in $\mathscr{A}$. In case $\mathscr{A}$ is modular with newform f, we prove that Conjecture I is equivalent to the equality of lattices $\mathscr{L}(f)=\mathscr{L}(A_{\min})$ (Conjecture I″ (2.9)). In particular, the following statement (see (2.4)) is a consequence of Conjecture I.

Conjecture II. $A_1 \cong A_{\min}$.

Note that this relates a curve distinguished by modular considerations to one distinguished intrinsically without mention of modular forms.

In § 3 we will attach to a modular elliptic curve $A_{/\mathbf{Q}}$ Stickelberger elements $\Theta_M \in \mathbf{C}[G_M]$, $M \in \mathbf{Z}^+$, similar to those studied by Mazur and Tate [15]. Here $G_M \cong (\mathbf{Z}/M\mathbf{Z})^*$ is the strict ray class group of conductor M over $\mathbf{Q}$. The coefficients of Θ_M are known to lie in the $\mathbf{Q}$-span $\mathscr{L}(A)\otimes\mathbf{Q}$ of the Neron lattice of A. With respect to the integral structure imposed by $\mathscr{L}(A)$, we will show how Conjecture I implies integrality properties for Θ_M which are analogous to those known for the Stickelberger elements associated to totally real number fields [5].

We will also look at the integrality properties of the Mazur, Swinnerton-Dyer p-adic L-functions attached to A for primes $p \neq 2$ of good ordinary reduction. By the philosophy of the Main Conjecture of Iwasawa Theory we expect these to be p-integral, but no proof is known at present. In § 4 we will show this integrality is a consequence of Conjecture I. We shall also derive lower bounds for the μ-invariants of these p-adic L-functions which match bounds proved by Greenberg ([8], formula (75)) for the characteristic power series on the other side of the Main Conjecture.

The remainder of the paper is devoted to the presentation of evidence supporting the basic conjecture. In § 5 we will prove that if Conjecture I is true for a curve A, then it is also true for any twist A^{ψ} of A by a quadratic Galois character ψ which is unramified at the primes of additive reduction.

In § 6 we study the conjectures for certain elliptic curves with complex multiplication. We will use integrality properties and congruence formulas due to Rubin [18] for algebraic parts of special values of L-functions to prove Conjecture II for these curves. Comparing the congruences with 'special values of L-functions' attached to subgroups of the cuspidal divisor class group, we are also able to show that a certain torsion subgroup of the optimal curve A_1 is contained in the cuspidal group (see Theorem 6.4).

Finally, in § 7, we present the known numerical evidence for Conjecture I. By direct calculation on a Macintosh Plus personal computer we have verified the conjecture for the 749 curves (281 isogeny classes) of conductor less than or equal to 200 appearing in the Antwerp tables [22]. The results of these calculations are being compiled on disks which can be used on any Macintosh computer and are available to anyone for the cost of the disks and postage.

Even assuming that Conjecture I is true and that we can prove it, there is good reason for dissatisfaction. We should then expect that our conjecture is just a manifestation, in the one dimensional factors of the Jacobian of $X_1(N)$, of some deeper property of the entire Jacobian. Perhaps, conversely, an identification of this deeper property will lead to a proof of Conjecture I.

§ 1. Modular elliptic curves

The celebrated conjecture of Taniyama, Shimura, and Weil asserts that every elliptic curve over $\mathbf{Q}$ can be parametrized by modular functions. Motivated by this conjecture, Mazur and Swinnerton-Dyer [14] introduced the notion of *strong* parametrization $X_0(N) \to A$ of an elliptic curve $A_{/\mathbf{Q}}$ by the modular curve $X_0(N)_{/\mathbf{Q}}$. Such a parametrization provides a powerful tool for viewing the arithmetic of A by relating it to the arithmetic of $X_0(N)$ which, in turn, can be studied moduli-theoretically.

The choice of $X_0(N)$ (as opposed to $X_1(N)$ or $X(N)$) as parametrizing object is justified by the relative simplicity of the associated moduli problem. Nevertheless, the use of $X_0(N)$ does involve a *choice.*

In the present work we have made a different choice. We will present evidence to support the claim (see e.g. Conjecture I (1.3)) that parametrizations by $X_1(N)$ are simpler than those by $X_0(N)$. Moreover, parametrizations by $X_1(N)$ satisfy a certain universal property (see Theorem 1.9) which suggests that our "choice" of $X_1(N)$ is hardly a choice at all.

Throughout this paper, $X_1(N)_{/\mathbf{Q}}$ will denote Shimura's canonical model over $\mathbf{Q}$ of $X_1(N)$ ([19], Chap. 6) in which the 0-cusp is a rational point. In this model, a rational function on $X_1(N)$ is defined over $\mathbf{Q}$ if and only if its q-expansion at the 0-cusp has coefficients in $\mathbf{Q}$.

(1.1) **Definition.** An elliptic curve $A_{/\mathbf{Q}}$ is *modular* of level N if there is a morphism

$$X_1(N) \xrightarrow{\pi} A$$

of algebraic curves over $\mathbf{Q}$ such that

(i) π sends the 0-cusp to the origin, and

(ii) $\pi^* \omega_A = c(\pi) \cdot \omega_f$

where ω_A is a Neron differential on A, $\omega_f = f(q)\dfrac{dq}{q}$ is the differential 1-form on $X_1(N)$ associated to a normalized newform f of level N, and $c(\pi) \in \mathbf{Q}^*$.

The map π is called a *modular parametrization* of A. The constant $c(\pi)$ is called the *Manin constant* of the parametrization π. □

(1.2) *Remark.* By the work of Carayol [1] we know that the level of a modular elliptic curve is equal to its conductor. □

The basic conjecture which we propose to study is as follows.

(1.3) **Conjecture I.** *Let $A_{/\mathbf{Q}}$ be a modular elliptic curve of level N. Then there is a modular parametrization*

$$\pi\colon X_1(N) \to A$$

for which $c(\pi) = \pm 1$. □

This conjecture is related to a conjecture of Manin (see [11, 14]), but is stronger than that conjecture. Manin's conjecture asserts that *some* curve in the isogeny class of A (namely the strong one) admits a parametrization π by $X_0(N)$ with $c(\pi)=\pm 1$. Conjecture I asserts that if we replace $X_0(N)$ by $X_1(N)$ then *every* curve isogenous to A admits such a parametrization. The analogous statement for $X_0(N)$ is false (see Example 1.11).

To approach Conjecture I, it is useful to decompose it into two subconjectures. This is achieved by singling out a special parametrization $\pi_1: X_1(N) \to A_1$ of a special curve A_1 in each isogeny class of modular elliptic curves $\mathscr{A}$ over $\mathbf{Q}$ (see (1.4), (1.5) below). The first subconjecture is then a statement about π_1 (namely, $c(\pi_1)=\pm 1$), and the second statement concerns isogenies from A_1 to the other curves in $\mathscr{A}$.

We first recall some basic facts about modular parametrizations. The following proposition is easily verified (compare [14]).

(1.4) **Proposition.** *Let $\mathscr{A}$ be an isogeny class (over $\mathbf{Q}$) of modular elliptic curves of level N. Then there is a curve $A_1 \in \mathscr{A}$ and a modular parametrization*

$$\pi_1: X_1(N) \to A_1$$

satisfying the following equivalent conditions.

(1) *π_1 is optimal in the following sense. If $\pi: X_1(N) \to A$ is a parametrization of a curve $A \in \mathscr{A}$, then there is an isogeny $\beta: A_1 \to A$ which makes the following diagram commutative:*

$$\begin{tikzcd} X_1(N) \arrow[r, "\pi_1"] \arrow[dr, "\pi"'] & A_1 \arrow[d, "\beta"] \\ & A. \end{tikzcd}$$

(2) *The induced map on singular homology*

$$\pi_{1*}: H_1(X_1(N); \mathbf{Z}) \twoheadrightarrow H_1(A_1; \mathbf{Z})$$

is surjective.

(3) *The induced map on* Pic^0

$$\pi_1^*: A_1 \cong \mathrm{Pic}^0(A_1) \hookrightarrow Pic^0(X_1(N))$$

is injective.

The curve $A_1 \in \mathscr{A}$ is uniquely determined by these conditions and π_1 is determined up to sign. □

(1.5) **Definition.** We will refer to A_1 as the *optimal curve* in $\mathscr{A}$ and to

$$\pm \pi_1: X_1(N) \to A_1$$

as the *optimal parametrizations.* □

(1.6) **Theorem.** *For any modular parametrization $\pi: X_1(N) \to A$, we have $c(\pi) \in \mathbf{Z}$.*

Proof. The proof is a straightforward application of the techniques of [4, 10]. Recall that a $\Gamma_1(N)^{\text{arith}}$-structure on a generalized elliptic curve A is defined to be an inclusion of group schemes $\mu_N \hookrightarrow A$. There is a smooth connected scheme $M_1(N)_{/\mathbf{Z}}$ which classifies generalized elliptic curves with $\Gamma_1(N)^{\text{arith}}$-structure.

Let Tate(q) be the Tate curve "$\mathbf{G}_m/q^{\mathbf{Z}}$" ([4], VII), and let $i\colon \mu_N \hookrightarrow \text{Tate}(q)$ be the $\Gamma_1(N)^{\text{arith}}$-structure induced by the natural inclusion $\mu_N \hookrightarrow \mathbf{G}_m$. The pair (Tate$(q)$, i) corresponds to a morphism

$$\tau\colon \operatorname{Spec}(\mathbf{Z}[[q]]) \to M_1(N)_{/\mathbf{Z}}.$$

After base change to $\mathbf{C}$ we have $M_1(N)_{/\mathbf{C}} \cong X_1(N)_{/\mathbf{C}}$ and τ defines the formal neighborhood of the 0-cusp on $X_1(N)_{\mathbf{C}}$ corresponding to the local parameter $q = e^{-2\pi i/Nz}$. This can be seen as follows. For z in the upper half plane, let $E(z) = \mathbf{C}/\langle z, 1\rangle$ be the elliptic curve whose period lattice $\langle z, 1\rangle$ is generated by z and 1. For each primitive element $\omega \in \langle z, 1\rangle$ let $i_\omega\colon \mu_N \to E(z)$ be the $\Gamma_1(N)^{\text{arith}}$-structure given by $e^{2\pi i/N} \mapsto \omega/N (\operatorname{mod} \langle z, 1\rangle)$. Then z corresponds to the point $(E(z), i_z) \in X_1(N)_{\mathbf{C}}$. After a simple calculation we see $(E(z), i_z) \cong (E(-1/Nz), i_1)$. But this latter pair is clearly isomorphic to (Tate$(e^{-2\pi i/Nz})$, i).

Now consider τ over $\mathbf{Q}$. Since $M_1(N)_{/\mathbf{Q}}$ is irreducible, we see that a function on $M_1(N)_{/\mathbf{Q}}$ is defined over $\mathbf{Q}$ if and only if its q-expansion at the 0-cusp has rational coefficients. Thus $M_1(N)_{/\mathbf{Q}} \cong \mathrm{X}_1(\mathrm{N})_{/\mathbf{Q}}$.

By the universal property of Neron models, the parametrization $\pi\colon X_1(N)_{/\mathbf{Q}} \to \mathrm{A}_{/\mathbf{Q}}$ extends to a $\mathbf{Z}$-morphism

$$\pi\colon M_1(N)_{/\mathbf{Z}} \to A_{/\mathbf{Z}}$$

where $A_{/\mathbf{Z}}$ denotes the Neron model of A.

Now let $\omega_A \in \mathrm{H}^0(\mathrm{A}_{/\mathbf{Z}}; \Omega^1)$ be a Neron differential on A. From the commutative diagram

$$\begin{tikzcd}
H^0(A_{/\mathbf{Z}}; \Omega^1) \arrow[r, "\pi^*"] \arrow[d] & H^0(M_1(N)_{/\mathbf{Z}}; \Omega^1) \arrow[r, "\tau^*"] \arrow[d] & \mathbf{Z}[[q]]\,dq \arrow[d] \\
H^0(A_{/\mathbf{C}}; \Omega^1) \arrow[r, "\pi^*"] & H^0(M_1(N)_{/\mathbf{C}}; \Omega^1) \arrow[r, "\tau^*"] & \mathbf{C}[[q]]\,dq
\end{tikzcd}$$

we see at once that $\pi^*\omega_A = c \cdot \omega_f$ has an integral q-expansion at the 0-cusp. But the Atkin-Lehner operator W_N interchanges the 0-cusp and the ∞-cusp and acts on ω_f as ± 1. Thus $c \cdot \omega_f$ also has an integral q-expansion at the ∞-cusp. This proves the theorem. □

Remarks. For an isogeny class of modular elliptic curves with square free conductor Mazur [13] has shown that the Manin constant, c_{strong}, of the strong parametrization is a power of 2. In [14] this was strengthened to $c_{\text{strong}} = \pm 1$ if the strong curve is involutory. In a letter to Mestre (February, 1985), Raynaud has stated general results concerning parametrizations by algebraic curves of stable elliptic curves. These results imply $c(\pi_1) = \pm 1$ or ± 2 for square free conductor.

We can now give the second form of the basic conjecture.

(1.7) **Conjecture I′.** *Let $\mathscr{A}$ be an isogeny class of modular elliptic curves of level N, and let $\pi_1: X_1(N) \to A_1$ be the optimal parametrization. Then*

(a) $c(\pi_1) = \pm 1$;

(b) *For any $A \in \mathscr{A}$ there is a (necessarily cyclic) isogeny $\phi: A_1 \to A$ for which $\phi^* \omega_A = \pm \omega_{A_1}$ where ω_A, ω_{A_1} are Neron differentials on A, A_1.* □

Remark. In §2 we will show that any **Q**-isogeny class (not necessarily modular) contains a unique curve A_1 satisfying (b). This curve is characterized by the property that every cyclic **Q**-isogeny with domain A_1 extends to an *étale* morphism on Neron models over **Z**.

(1.8) **Theorem.** *Conjectures I and I′ are equivalent.*

Proof. Conjecture I is clearly a consequence of Conjecture I′. So suppose Conjecture I is true.

Let $A \in \mathscr{A}$ be an arbitrary curve in the isogeny class, and let $\pi: X_1(N) \to A$ be a parametrization for which $c(\pi) = 1$. By the definition of optimality, π factors through π_1:

$$\begin{tikzcd}
X_1(N) \arrow[r, "\pi_1"] \arrow[dr, "\pi"'] & A_1 \arrow[d, "\phi"] \\
 & A.
\end{tikzcd}$$

If ω_A, ω_{A_1} are Neron differentials on A, A_1 then $\phi^* \omega_A = \mathrm{n} \cdot \omega_{A_1}$ for some integer $n \in \mathbf{Z}$. Thus $1 = c(\pi) = n \cdot c(\pi_1)$. Since both n and $c(\pi_1)$ are integers (1.6(a)), $n = c(\pi_1) = \pm 1$. □

We next turn to the question of how much our definitions depend on their reference to $X_1(N)$.

Shimura ([19], Chap. 6) has studied the field $\mathscr{F}$ of modular functions of all levels having Fourier coefficients in cyclotomic fields. He showed that $\mathscr{F}$ is Galois over **Q** and constructed a surjective homomorphism $\rho: \mathrm{GL}_2(\mathbf{A}_f) \to \mathrm{Aut}(\mathscr{F})$ whose kernel is the group of rational matrices $Z(\mathbf{Q})$ in the center of GL_2. Let $\mathscr{S}$ be the collection of open subgroups of $\mathrm{GL}_2(\mathbf{A}_f)$ for which $Z(\mathbf{Q}) \subseteq S$ and $S/Z(\mathbf{Q})$ is compact. For each $S \in \mathscr{S}$ let k_S be the cyclotomic field associated to the open subgroup $\mathbf{Q}^* \mathbf{R}^+ \det(S)$ of $\mathbf{A}^*$ by class field theory. Shimura has shown that the fixed field $\mathscr{F}_S$ of $\rho(S)$ in $\mathscr{F}$ defines a structure of algebraic curve over k_S on the modular curve X_{Γ_S} associated to the congruence group $\Gamma_S = \mathrm{GL}_2^+(\mathbf{Q}) \cap S$. For example, if we define

$$K_1(N) = \left\{ g \in \prod_p \mathrm{GL}_2(\mathbf{Z}_p) \,\middle|\, g \equiv \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\, N) \right\},$$

then the group $S_1(N)=Z(\mathbf{Q})K_1(N)$ defines the model of $X_1(N)$ we have been using.

Define $\hat{X}$ to be the pro-variety $\varprojlim_{S} X_S$. We give $\hat{X}$ the $\mathbf{Q}$-structure induced by the subfield $\mathscr{F}_{\mathbf{Q}}$ of $\mathscr{F}$ consisting of modular functions whose q-expansions at the 0-cusp have rational coefficients. An $\hat{X}$-parametrization of an elliptic curve $A_{/\mathbf{Q}}$ is a compatible system $\hat{\pi}=\{\pi_S\}$ of k_S-morphisms $\pi_S\colon X_S \to A$ for all sufficiently small $S\in\mathscr{S}$. The parametrization $\hat{\pi}$ is defined over $\mathbf{Q}$ if the image of the induced inclusion $\hat{\pi}^*\colon \mathbf{Q}(A) \hookrightarrow \mathscr{F}$ is contained in $\mathscr{F}_{\mathbf{Q}}$.

(1.9) **Theorem.** *Let f be a weight two normalized newform of level N with rational Fourier coefficients, $\mathscr{A}_f$ be its associated isogeny class of elliptic curves, and $\hat{\omega}_f$ the differential 1-form on $\hat{X}$ associated to $f(q)\dfrac{dq}{q}$, $q=e^{2\pi i z}$. Let*

$$\hat{\pi}\colon \hat{X} \to A$$

be a parametrization of a curve $A\in\mathscr{A}_f$ such that

(i) *$\hat{\pi}$ is defined over $\mathbf{Q}$;*

(ii) *$\hat{\pi}$ sends the 0-cusp to the origin; and*

(iii) $\hat{\pi}^*\omega_A = c\cdot\hat{\omega}_f$

where ω_A is a Neron differential on A and $c\in\mathbf{Q}^*$. Then $\hat{\pi}$ factor through a modular parametrization

$$\pi\colon X_1(N)\to A.$$

Proof. Let $\pi_S\colon X_S \to A$ be a k_S-morphism representing $\hat{\pi}$ where $S\in\mathscr{S}$ is chosen so that $S\subseteq S_1(N)$. We must show that π_S factors through a $\mathbf{Q}$-morphism $X_1(N) \to A$. We first prove the corresponding statement over $\mathbf{C}$.

Let $\Gamma=\Gamma_S$, $J_\Gamma=\mathrm{Pic}^0(X_S)_{/\mathbf{C}}$ and $J_1=\mathrm{Pic}^0(X_1(N))_{/\mathbf{C}}$. The natural projection

$$X_{S_{/\mathbf{C}}} \to X_1(N)_{/\mathbf{C}}$$

induces a morphism $\phi\colon J_1(N)\to J_\Gamma$.

We first show that ϕ is injective. Since the principal congruence groups are cofinal in the lattice of congruence groups we may suppose $\Gamma=\Gamma(M)$ for some integer M divisible by N. With this assumption $X_{S/\mathbf{C}} \to X_1(N)_{/\mathbf{C}}$ is a Galois cover of Riemann surfaces. By Kummer theory we know that the group $\ker(\phi)$ is Pontrjagin dual to the Galois group $\mathrm{Gal}(X_{\mathrm{unr}}/X_1(N))$ of the maximal abelian unramified cover $X_{\mathrm{unr}/\mathbf{C}} \to X_1(N)_{/\mathbf{C}}$ intermediate to $X_{S/\mathbf{C}} \to X_1(N)_{/\mathbf{C}}$. But the inertia groups of the cusps of $X_1(N)_{/\mathbf{C}}$ are the parabolic subgroups of $\Gamma_1(N)$, and a theorem of Fricke and Wohlfahrt [24] tells us that $\Gamma_1(N)$ is generated by its parabolic elements together with any congruence subgroup. Thus $X_{\mathrm{unr}/\mathbf{C}} = X_1(N)_{/\mathbf{C}}$ and $\ker(\phi)=0$.

Next we show that there is a map $\psi\colon A_{/\mathbf{C}} \to J_1$ for which the diagram

$$\begin{tikzcd}
J_\Gamma & A_{/\mathbf{C}} \arrow[l, "\pi^*"'] \arrow[dl, "\psi"] \\
J_1 \arrow[u, "\phi"] &
\end{tikzcd} \tag{1.10}$$

is commutative. The hypothesis (1.9)(iii) gives us the desired diagram on tangent spaces at the origin. Exponentiating and using the injectivity of ϕ gives us (1.10).

Finally, we dualize (1.10) and consider the canonical embeddings $X_{S/\mathbf{C}} \hookrightarrow J_\Gamma$ and $X_1(N)_{/\mathbf{C}} \hookrightarrow J_1$, each of which sends the 0-cusp to the origin. This gives us the following commutative diagram where the leftmost vertical arrow is the natural projection.

$$\begin{tikzcd}
X_{S/\mathbf{C}} \arrow[r, hook] \arrow[d] \arrow[rr, bend left, "\pi_S"] & J_\Gamma \arrow[r] \arrow[d] & A_{/\mathbf{C}} \\
X_1(N)_{/\mathbf{C}} \arrow[r, hook] & J_1 \arrow[ur] &
\end{tikzcd}$$

From this diagram we see that the functions in the image of the inclusion $\pi_S^*\colon \mathbf{Q}(A) \hookrightarrow \mathscr{F}_S$ are fixed by $\Gamma_1(N)$. Since $\hat{\pi}$ is defined over $\mathbf{Q}$ we also have $\pi_S^*(\mathbf{Q}(A)) \subseteq \mathscr{F}_\mathbf{Q}$. From ([19], Ex. 6.26) we see that $\mathscr{F}_\mathbf{Q}$ is the fixed field of $\rho(T)$ where T is the group $\left\{\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}\right\} \subseteq \mathrm{GL}_2(\mathbf{A}_f)$. Thus $\pi_S^*(\mathbf{Q}(A))$ is contained in the fixed field of $\rho(\Gamma_1(N) \cdot S \cdot T)$. But $\Gamma_1(N) \cdot S \cdot T = S_1(N)$ by the strong approximation theorem for SL_2. This proves the theorem. □

We close this section with an example.

(1.11) *Example.* There are three elliptic curves of conductor 11. The minimal Weierstrass equations of these curves are given in the Antwerp tables [22] where the curves are labeled [11 A], [11 B], and [11 C]. It can be verified (see §7) that $[11\,A] = X_1(11)$, $[11\,B] = X_0(11)$, and [11 C] is the quotient of $X_0(11)$ by the subgroup of order 5 generated by the cusps. We have the following diagram.

$$\begin{tikzcd}
\omega_A & \omega_B \arrow[l, mapsto] & \omega_C \arrow[l, mapsto] \\
{[11\,A]} \arrow[r] \arrow[d, equal] & {[11\,B]} \arrow[r] \arrow[d, equal] & {[11\,C]} \\
X_1(11) \arrow[r] & X_0(11) &
\end{tikzcd}$$

The horizontal arrows are isogenies of degree 5 under which a Neron differential on [11 C] pulls back to a Neron differential on [11 B] which in turn pulls back to a Neron differential on [11 A]. Note, however, that under the isogeny [11 B] → [11 A] of degree 5 a Neron differential on [11 A] pulls back to 5 times a Neron differential on [11 B]. This shows that we cannot replace $X_1(N)$ by $X_0(N)$ in Conjecture I (1.3). □

§ 2. Parshin-Faltings heights

In § 1 we used modular considerations to distinguish the "optimal" curve A_1 in an isogeny class $\mathscr{A}$ of modular elliptic curves. Conjecture I′(b) (1.7) then asserts that A_1 should have a rather remarkable property. I have not been able to find a statement in the literature which would guarantee the existence in $\mathscr{A}$ of a curve with this property. Thus, to make our conjecture sensible we should prove that every isogeny class $\mathscr{A}$ (modular or not) contains a curve A_1 satisfying (b) of Conjecture I′. This is the essential content of Theorem 2.3 which is the main result of this section.

(2.1) **Definition.** Let ω_A be a Neron differential on the elliptic curve $A_{/\mathbf{Q}}$.

(a) The *lattice of Neron periods* of A is defined by

$$\mathscr{L}(A) \overset{\text{def}}{=} \operatorname{Image}(H_1(A_{\mathbf{C}}; \mathbf{Z}) \xrightarrow{\int \omega_A} \mathbf{C}).$$

(b) The *Parshin-Faltings height* of A is

$$H(A) = \frac{1}{\sqrt{\operatorname{covolume}(\mathscr{L}(A))}} = \left(\frac{1}{2\pi i} \int_{A_{\mathbf{C}}} \omega_A \wedge \bar{\omega}_A\right)^{-1/2}.$$

We say that an isogeny $\phi: A_{/\mathbf{Q}} \to B_{/\mathbf{Q}}$ of elliptic curves is *étale* if its extension to Neron models is an étale morphism. The following easily established lemma provides a useful criterion for an isogeny to be étale.

(2.2) **Lemma.** *Let K be a finite extension of $\mathbf{Q}_p$ and $R \subseteq K$ be the integers of K. An isogeny $\phi: A \to B$ of elliptic curves over K is étale if any only if ϕ induces an isomorphism on Neron differentials*

$$\phi^*: H^0(B_{/R}; \Omega^1_{B/R}) \xrightarrow{\sim} H^0(A_{/R}; \Omega^1_{A/R}). \quad \square$$

We can now state the main theorem of this section.

(2.3) **Theorem.** *In any isogeny class $\mathscr{A}$ of elliptic curves over $\mathbf{Q}$ there is a unique curve $A_{\min} \in \mathscr{A}$ which satisfies the following equivalent conditions.*

(a) *For every $A \in \mathscr{A}$*

$$H(A_{\min}) \leqq H(A).$$

(b) *For every $A \in \mathscr{A}$ there is an étale isogeny*

$$\phi: A_{\min} \to A.$$

(c) *For every $A \in \mathscr{A}$*

$$\mathscr{L}(A_{\min}) \subseteq \mathscr{L}(A).$$

Before giving the proof of this theorem, a few remarks are in order.

Remarks. (i) It is not true in general that there is a unique curve of *maximal* height in the isogeny class. The isogeny class of conductor 17 in the Antwerp tables [22] provides an example. The curves [17C] and [17D] have the same maximal height. (The curve [17A] is the unique curve of minimal height.)

(ii) The hypothesis that elliptic curves and isogenies be defined over $\mathbf{Q}$ will be used in an essential way. The main local lemma (2.5) is valid only over unramified extensions of $\mathbf{Q}_p$. Consequently, our proof of Theorem 2.3 will be valid only over number fields everywhere unramified over $\mathbf{Q}$, that is, only over $\mathbf{Q}$ itself. There is no reason to believe the theorem over any number field other than $\mathbf{Q}$.

Note also that by (2.2) and (2.3) the following conjecture is a consequence of Conjecture I (more precisely, is equivalent to Conjecture I′(b) (1.7)).

(2.4) **Conjecture II.** *The optimal curve in an isogeny class of modular elliptic curves is the curve of minimal height.* □

Our proof of Theorem 2.3 makes use of a property of isogenies which is well known for isogenies with quasi-finite flat kernels. Let K be a finite extension of $\mathbf{Q}_p$ and $R \subseteq K$ be the integers of K. If $\phi: A \to B$ is an isogeny of elliptic curves over K and if the kernel $A[\phi]$ of ϕ in the Neron model of A is a quasi-finite flat group scheme then the exact sequence

$$0 \to A[\phi]^0 \to A[\phi] \to A[\phi]^{\text{ét}} \to 0$$

gives rise to a factorization $\phi = \phi_{\text{ét}} \circ \phi_0$

$$\begin{tikzcd}
A \arrow[rr, "\phi"] \arrow[dr, "\phi_0"'] & & B \\
& C \arrow[ur, "\phi_{\text{et}}"'] &
\end{tikzcd}$$

where $\phi_{\text{ét}}$ is étale and $\ker(\phi_0) = A[\phi]^0$. If $A[\phi]$ is not flat, but K is unramified over $\mathbf{Q}_p$, then we can still make the following statement.

(2.5) **Lemma.** *Suppose K is unramified over $\mathbf{Q}_p$ and ϕ: $A_{/K} \to B_{/K}$ is a cyclic isogeny of degree p^n. Then there is a factorization $\phi = \phi_{\text{ét}} \circ \phi_0$*

$$\begin{tikzcd}
A \arrow[rr, "\phi"] \arrow[dr, "\phi_0"'] & & B \\
& C \arrow[ur, "\phi_{\text{et}}"'] &
\end{tikzcd}$$

where $\phi_{\text{ét}}$ and $\check{\phi}_0$ are étale.

Proof. We proceed by induction on n. If $n=1$, then $\phi \circ \check{\phi}$ is multiplication by p on B. Since p is a uniformizing parameter for K, we can choose Neron differentials ω_A, ω_B on A, B such that either $\phi^* \omega_B = \omega_A$ or $\check{\phi}^* \omega_A = \omega_B$. By Lemma 2.2 this means that either ϕ or $\check{\phi}$ is étale. This proves Lemma 2.5 if $n=1$.

Now suppose $n>1$ and that the lemma is known for cyclic isogenies of degree p^{n-1}. Since ϕ is a *cyclic* isogeny we can write $\phi=\alpha\circ\beta$

$$\begin{tikzcd}
A \arrow[rr, "\phi"] \arrow[dr, "\beta"'] & & B \\
& A' \arrow[ur, "\alpha"'] &
\end{tikzcd}$$

where α, β are cyclic isogenies of degrees p^{n-1}, p respectively. By the induction hypothesis, we can factor $\alpha=\alpha_{\text{ét}}\circ\alpha_0$ to obtain the following commutative diagram.

$$\begin{tikzcd}
A \arrow[r, "\phi"] \arrow[d, "\beta"'] & B \\
A' \arrow[r, "\alpha_0"'] \arrow[ur, "\alpha"] & C \arrow[u, "\alpha_{\text{et}}"']
\end{tikzcd}$$

If α_0 is an isomorphism, the lemma follows at once. Otherwise α_0 has a factor $\psi: A'\to C'$ of degree p. Since $\hat{\psi}: C'\to A'$ is étale, Lemma 2.6 (below) guarantees that β is not étale. Then $\phi_0=\alpha_0\circ\beta$ and $\phi_{\text{ét}}=\alpha_{\text{ét}}$ gives the desired factorization of ϕ and Lemma 2.5 is proved. □

(2.6) **Lemma.** *Let A, B, C be elliptic curves over a finite extension K of $\mathbf{Q}_p$. If $\phi: A\to C$ and $\psi: B\to C$ are étale isogenies of degree p then there is an isomorphism $\alpha: A\xrightarrow{\sim}B$ making the following diagram commutative.*

$$\begin{tikzcd}
A \arrow[rr, "\alpha"] \arrow[dr, "\phi"'] & & B \arrow[dl, "\psi"] \\
& C &
\end{tikzcd}$$

Proof. Let R be the ring of integers of K. Let $A_{/R}$, $B_{/R}$, $C_{/R}$ be the Neron models and $(A\times_C B)_{/R}$ be the fiber product of $A_{/R}$ and $B_{/R}$ over $C_{/R}$. Then we have the following diagram of algebraic groups over R.

$$\begin{tikzcd}
& A\times_C B \arrow[dl] \arrow[dr] \arrow[dd, "\pi"] & \\
A \arrow[dr, "\phi"'] & & B \arrow[dl, "\psi"] \\
& C &
\end{tikzcd}$$

Now suppose there is no isomorphism α as claimed in the lemma. Then on generic fibers we have $(A \times_C B)_{/K} \cong A_{/K} \times_C B_{/K} \cong C_{/K}$ and $\pi_{/K}: C_{/K} \to C_{/K}$ is multiplication by p. Using the universal properties of Neron models and of fiber products we see that $(A \times_C B)_{/R} \cong C_{/R}$ and that π corresponds to multiplication by p on $C_{/R}$. But π is the fiber product of two étale morphisms and is therefore étale. This is a contradiction and Lemma 2.6 is proved. □

Proof of Theorem 2.3. Since $\mathscr{A}$ is a finite set, the existence of a curve $A_{\min} \in \mathscr{A}$ satisfying (a) is clear. On the other hand, there can be at most one curve satisfying (c). So the theorem will be proved if we establish the equivalence of (a), (b), and (c).

To prove (a)⇒(b) let $A_{\min}$ be as in (a), $A \in \mathscr{A}$, and $\phi: A_{\min} \to A$ be a cyclic isogeny. We must show that ϕ is étale. By Lemma 2.5, $\phi = \phi_{\text{ét}} \circ \phi_0$ with $\phi_{\text{ét}}$ and $\check{\phi}_0$ étale.

$$\begin{tikzcd}
A_{\min} \arrow[rr, "\phi"] \arrow[dr, "\phi_0"'] & & A \\
& C \arrow[ur, "\phi_{\text{ét}}"'] &
\end{tikzcd}$$

Let $\omega_{\min}$ be a Neron differential on A_{min}. Since $\check{\phi}_0$ is étale, $\omega_C = \check{\phi}_0^* \omega_{\min}$ is a Neron differential on C. Then $\phi_0^* \omega_C = \deg(\phi_0) \cdot \omega_{\min}$ and

$$\begin{aligned}
H(A_{\min}) &= \left(\frac{1}{2\pi i} \int_{A_{\min}(\mathbf{C})} \omega_{\min} \wedge \bar{\omega}_{\min}\right)^{-1/2} \\
&= \deg(\phi_0) \cdot \left(\frac{1}{2\pi i} \int_{A_{\min}(\mathbf{C})} (\phi_0^* \omega_C) \wedge (\phi_0^* \bar{\omega}_C)\right)^{-1/2} \\
&= \deg(\phi_0) \cdot \left(\deg(\phi_0) \cdot \frac{1}{2\pi i} \int_{C(\mathbf{C})} \omega_C \wedge \bar{\omega}_C\right)^{-1/2} \\
&= \sqrt{\deg(\phi_0)} \cdot H(C).
\end{aligned}$$

But $C \in \mathscr{A}$, so $H(C) \geqq H(A_{\min})$ and we see that $\deg(\phi_0) = 1$. Thus ϕ is étale.

To prove (b)⇒(c) we let $\phi: A_{\min} \to A$ be an étale isogeny and will prove $\mathscr{L}(A_{\min}) \subseteq \mathscr{L}(A)$. Let $\omega_{\min}$ be a Neron differential on $A_{\min}$. Then Lemma 2.2 guarantees that there is a Neron differential ω_A on A such that $\phi^* \omega_A = \omega_{\min}$. For each $\Omega \in \mathscr{L}(A_{\min})$ there is a $\gamma \in H_1(A_{\min}(\mathbf{C}); \mathbf{Z})$ such that

$$\Omega = \int_\gamma \omega_{\min} = \int_\gamma \phi^* \omega_A = \int_{\phi^* \gamma} \omega_A \in \mathscr{L}(A)$$

and (c) follows.

The implication (c)$\Rightarrow$(a) follows at once from Definition 2.1. This completes the proof of Theorem 2.3. □

Remark. Using (2.5) it is not hard to see that the set $\{\mathscr{L}(A)|A\in\mathscr{A}\}$ of Neron lattices of $\mathscr{A}$ is closed under intersection. Indeed, if $A, B\in\mathscr{A}$, then there is a cyclic isogeny $\phi\colon A\to B$. By (2.5) ϕ factors as $A\xrightarrow{\phi_0}C\xrightarrow{\phi_{\mathrm{et}}}B$ where $\phi^{\text{ét}}$ and ϕ_0 are étale. Then $\mathscr{L}(C)=\mathscr{L}(A)\cap\mathscr{L}(B)$.

We conclude this section with a third equivalent formulation of Conjecture I which will be useful in the sequel.

Let $\mathscr{A}$ be a $\mathbf{Q}$-isogeny class of modular elliptic curves of level N and let f be the associated weight 2 normalized newform. Integration of the differential 1-form $f(q)\frac{dq}{q}$ over singular 1-cycles on $X_1(N)_{\mathbf{C}}$ gives a linear map

$$H_1(X_1(N)_{\mathbf{C}};\mathbf{Z})\xrightarrow{\int f(q)\frac{dq}{q}}\mathbf{C}.$$

The image of this map is a lattice

$$\mathscr{L}(f)\subseteq\mathbf{C}. \tag{2.7}$$

Indeed, using (1.4(2)), one easily verifies the equality

$$\mathscr{L}(f)=c(\pi_1)^{-1}\mathscr{L}(A_1) \tag{2.8}$$

where A_1 is the optimal curve in $\mathscr{A}$, $\pi_1\colon X_1(N)\to A_1$ is the optimal parametrization, and $c(\pi_1)$ is the Manin constant. Thus Conjecture I′ is equivalent to the following statement.

(2.9) **Conjecture I″.** *Let $A_{\min}$ be the curve of minimal height in $\mathscr{A}$. Then*

$$\mathscr{L}(f)=\mathscr{L}(A_{\min}).$$

§ 3. Integrality properties of Stickelberger elements

Mazur and Tate [15] have recently formulated some intriguing new conjectures of Birch, Swinnerton-Dyer type about certain Stickelberger elements, $\Theta_M^{(M-T)}$, associated to a modular elliptic curve A. These conjectures predict congruence formulas relating $\Theta_M^{(M-T)}$ to the arithmetic of A and so are quite sensitive to the integrality properties of these Stickelberger elements. In this section we will define a variation Θ_M (Definition 3.3) of $\Theta_M^{(M-T)}$ and show how Conjecture I implies integrality properties of Θ_M analogous to those known for Stickelberger elements associated to totally real number fields [5]. The relation between our

Stickelberger elements and those studied by Mazur and Tate is exhibited in (3.4) and (3.5).

Let f be the weight 2 normalized newform of level N associated to the modular elliptic curve A.

(3.1) **Definition.** The *modular symbol* associated to f is the function $[\;]_f\colon \mathbf{P}^1(\mathbf{Q}) \to \mathbf{C}$ defined by

$$[r]_f = \int_0^r f(q)\frac{dq}{q}$$

where the integral is over the geodesic in the upper half plane joining 0 to r. □

The reader should note that our modular symbol is a variation of the one used by Mazur and Tate. Their modular symbol is given as an integral from $i\infty$ to r.

We know from the Manin-Drinfeld theorem [6] that the values of the modular symbol lie in the $\mathbf{Q}$-span of the lattice of Neron periods of A:

$$[r]_f \in \mathscr{L}(A) \otimes \mathbf{Q}. \tag{3.2}$$

For each positive integer M let $F_M = \mathbf{Q}(e^{2\pi i/M})$, let $G_M = \mathrm{Gal}(F_M/\mathbf{Q}) \cong (\mathbf{Z}/M\mathbf{Z})^*$ and let $G_M^+ = \mathrm{Gal}(F_M^+/\mathbf{Q}) \cong (\mathbf{Z}/M\mathbf{Z})^*/(\pm 1)$ be the Galois group of the totally real subfield F_M^+ of F_M. The standard isomorphism $(\mathbf{Z}/M\mathbf{Z})^* \to G_M$ is given by $a \mapsto (\sigma_a\colon e^{2\pi i/M} \mapsto e^{2\pi i a/M})$.

(3.3) **Definition.** To each integer $M > 0$ we associate the following objects.

(a) The *Stickelberger function of layer M*:

$$\begin{aligned} \theta_M\colon G_M &\to \mathscr{L}(A) \otimes \mathbf{Q} \\ \sigma_a &\mapsto \left[\frac{a'}{M}\right]_f \end{aligned}$$

where a' represents the inverse of a in $(\mathbf{Z}/M\mathbf{Z})^*$.

(b) The *Stickelberger element of layer M*:

$$\Theta_M = \sum_{\sigma \in G_M} \theta_M(\sigma) \otimes \sigma^{-1} \in \mathscr{L}(A) \otimes \mathbf{Q}[G_M].$$

To express the relationship between our Stickelberger element and the one used by Mazur and Tate we note that $\theta_M(\sigma_{-1} \cdot \sigma) = \overline{\theta_M(\sigma)}$ for each $\sigma \in G_M$ and so

$$\Theta_M^+ \overset{\mathrm{def}}{=} \sum_{\sigma \in G_M^+} \mathrm{Re}(\theta_M(\sigma)) \cdot \sigma^{-1} \in \mathbf{R}[G_M^+] \tag{3.4}$$

is well defined. Then

$$\Theta_M^{(M-T)} = \frac{1}{\Omega_A^+}\Big(\Theta_M^+ + L(f,1)\sum_{\sigma\in G_M^+}\sigma\Big) \tag{3.5}$$

where $\Omega_A^+ = \frac{1}{2}\int_{A(\mathbf{R})} |\omega_A|$ is a (half-)period of a Neron differential on A.

By analogy with what is known about Stickelberger elements attached to totally real number fields [5] we might hope that the following conjecture is true.

(3.6) **Conjecture III.** *Let $J_M \subseteq \mathbf{Z}[G_M]$ be the annihilator of $A(F_M)_{\text{tor}}$. Then*

$$J_M \cdot \Theta_M \subseteq \mathscr{L}(A) \otimes \mathbf{Z}[G_M].$$

As a corollary of the next theorem we will see that Conjecture III is a consequence of Conjecture I (1.3).

Fix a modular parametrization of A

$$\pi\colon X_1(N) \to A,$$

and let $C_\pi \subseteq A_{\text{tor}}$ be the subgroup generated by the image of the cusps of $X_1(N)$. For $r \in \mathbf{P}^1(\mathbf{Q})$ we let

$$\{r\}_\pi \in C_\pi \tag{3.7}$$

be the corresponding torsion point on A. The geodesic from 0 to r in the upper half plane projects to a path $\{0, r\}$ on $A(\mathbf{C})$ joining the origin to $\{r\}_\pi$. The *modular symbol* associated to π is the function $[\cdot]_\pi\colon \mathbf{P}^1(\mathbf{Q}) \to \mathscr{L}(A) \otimes \mathbf{Q}$ defined by

$$[r]_\pi = \int_{\{0,r\}_\pi} \omega_A. \tag{3.8}$$

If ξ denotes the natural map

$$\xi\colon \mathscr{L}(A) \otimes \mathbf{Q} \to A_{\text{tor}}, \tag{3.9}$$

then $\xi([r]_\pi) = \{r\}_\pi$.

Now fix a positive integer M and define $\Theta_{\pi,M}\colon \mathbf{Z}[G_M] \to \mathscr{L}(A) \otimes \mathbf{Q}$ and $\tilde{\theta}_{\pi,M} = \xi \circ \theta_{\pi,M}\colon \mathbf{Z}[G_M] \to C_\pi$ by

$$\begin{aligned} \theta_{\pi,M}(\sigma_a) &= \left[\frac{a'}{M}\right]_\pi \\ \tilde{\theta}_{\pi,M}(\sigma_a) &= \left\{\frac{a'}{M}\right\}_\pi \end{aligned} \tag{3.10}$$

where $a \cdot a' \equiv 1 \pmod{M}$. Let $C_{\pi,M} \subseteq C_\pi$ be the image of $\tilde{\theta}_{\pi,M}$.

(3.11) **Lemma.** *The points of $C_{\pi,M}$ are defined over F_M and the map $\tilde{\theta}_{\pi,M}$: $\mathbf{Z}[G_M] \to C_{\pi,M}$ commutes with the action of G_M.*

Proof. The cusps of $X_1(N)$ are defined over F_N. For each pair $x, y \in \mathbf{Z}/N\mathbf{Z}$ with $(x, y, N)=1$, we let $\begin{bmatrix}x\\y\end{bmatrix}$ denote the cusp on $X_1(N)$ represented by rational numbers $\frac{a}{b}$ with $(a, b)=1$ and $a \equiv x$, $b \equiv y (\operatorname{mod} N)$. The action of G_N on the cusps is given by

$$\begin{bmatrix}x\\y\end{bmatrix}^{\sigma_d}=\begin{bmatrix}d'x\\y\end{bmatrix} \tag{3.12}$$

where $d, d' \in (\mathbf{Z}/N\mathbf{Z})^*$ and $dd' \equiv 1 (\operatorname{mod} N)$ (compare [20], p. 12, where the model for $X_1(N)$ was chosen so that the ∞-cusp was rational).

Now let $\sigma, \tau \in G_M$, and choose $a, b \in (\mathbf{Z}/M\mathbf{Z})^*$ such that $\sigma=\sigma_a$, $\tau=\sigma_b$. We lift a, b to $\tilde{a}, \tilde{b} \in (\mathbf{Z}/MN\mathbf{Z})^*$ and let $a', b' \in \mathbf{Z}$ represent the inverses of $\tilde{a}, \tilde{b}$. Then

$$\begin{aligned}\tilde{\theta}_{\pi,M}(\sigma\tau)=\tilde{\theta}_{\pi,M}(\sigma_{ab})&=\left\{\frac{a'b'}{M}\right\}_\pi\\ &=\pi\left(\begin{bmatrix}a'b'\\M\end{bmatrix}\right)=\pi\left(\begin{bmatrix}b'\\M\end{bmatrix}^{\sigma_a}\right)\\ &=\pi\left(\begin{bmatrix}b'\\M\end{bmatrix}\right)^{\sigma_a}\\ &=(\tilde{\theta}_{\pi,M}(\tau))^{\sigma}.\end{aligned}$$

This proves the lemma. □

We define the Stickelberger element of layer M associated to π by

$$\Theta_{\pi,M}=\sum_{\sigma\in G_m}\theta_{\pi,M}(\sigma)\otimes\sigma^{-1}\in\mathscr{L}(A)\otimes\mathbf{Q}[G_M]. \tag{3.13}$$

(3.14) **Theorem.** *Let $J_{\pi,M}\subseteq\mathbf{Z}[G_M]$ be the annihilator of $C_{\pi,M}$. Then*

$$J_{\pi,M}\cdot\Theta_{\pi,M}\subseteq\mathscr{L}(A)\otimes\mathbf{Z}[G_M].$$

Proof. We extend ξ (3.9) by linearity to a map

$$\xi\colon \mathscr{L}(A)\otimes\mathbf{Q}[G_M]\to A_{\mathrm{tor}}\otimes\mathbf{Z}[G_M].$$

Then the theorem is equivalent to the statement $\xi(J_{\pi,M}\cdot\Theta_{\pi,M})=0$.

We define $\tilde{\Theta}_{\pi,M}\in C_{\pi,M}\otimes\mathbf{Z}[G_M]$ by

$$\tilde{\Theta}_{\pi,M}=\xi(\Theta_{\pi,M})=\sum_{\sigma\in G_M}\tilde{\theta}_{\pi,M}(\sigma)\otimes\sigma^{-1}.$$

Now $C_{\pi,M}\otimes\mathbf{Z}[G_M]$ is a $\mathbf{Z}[G_M]\otimes\mathbf{Z}[G_M]$-module and Lemma 3.11 tells us

$$(1\otimes\alpha)\,\tilde{\Theta}_{\pi,M}=(\alpha\otimes1)\,\tilde{\Theta}_{\pi,M}$$

for every $\alpha \in \mathbf{Z}[G_M]$. Thus

$$\begin{aligned}\xi(J_{\pi,M}\cdot\Theta_{\pi,M}) &= (1\otimes J_{\pi,M})\cdot\tilde{\Theta}_{\pi,M}\\ &= (J_{\pi,M}\otimes 1)\cdot\tilde{\Theta}_{\pi,M}\\ &= 0.\end{aligned}$$

This proves the theorem. □

(3.15) **Corollary.** *Conjecture I* (1.3)$\Rightarrow$*Conjecture III* (3.6).

Proof. A simple calculation shows $\Theta_{\pi,M}=c(\pi)\cdot\Theta_M$. Thus Conjecture I implies $\Theta_{\pi,M}=\pm\Theta_M$. Since $J_M\subseteq J_{\pi,M}$, we have $J_M\cdot\Theta_M\subseteq J_{\pi,M}\cdot\Theta_{\pi,M}\subseteq\mathscr{L}(A)\otimes\mathbf{Z}[G_M]$ and the corollary is proved. □

§ 4. *P*-adic *L*-functions and μ-invariants

Let $\mathscr{A}$ be an isogeny class of modular elliptic curves associated to a newform f of level N and let $p \neq 2$ be a prime of good ordinary reduction. Mazur and Swinnerton-Dyer [14] have constructed p-adic measures whose p-adic Mellin transforms furnish p-adic analogs of the complex L-functions associated to $\mathscr{A}$ (see Theorem 4.4). Because of the Main Conjecture of Iwasawa Theory in this setting, we expect these measures to be integral (Conjecture IV (4.5)). Unfortunately, the answer to even this simple question is unknown at present. On the other hand, if our Conjecture I is true for $\mathscr{A}$ then the measures of Mazur and Swinnerton-Dyer must be integral (at least if $p \neq 2$), as we shall see in this section (Theorem 4.6, Corollary 4.7). We will also see how Conjecture IV leads to lower bounds for μ-invariants of p-adic L-functions which are consistent with bounds proved by Greenberg [8] for μ-invariants of Selmer groups in cyclotomic towers.

Let $\mathbf{C}_p$ be a fixed p-adic completion of an algebraic closure of $\mathbf{Q}_p$, let $\bar{\mathbf{Q}}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, and fix an imbedding of $\bar{\mathbf{Q}}$ into $\mathbf{C}_p$. When we speak about p-adic properties of algebraic numbers, we shall always be referring to the p-adic properties with respect to this fixed imbedding.

The data required to build the p-adic measures consists in the unit root α of Frobenius at p, and the modular symbol $[\;]_f$: $\mathbf{P}^1(\mathbf{Q})\to\mathscr{L}(A)\otimes\mathbf{Q}$ (3.1). For each integer $\Delta>0$ with $(\Delta,p)=1$ let $\mathbf{Z}_{p,\Delta}^*=\varprojlim_n(\mathbf{Z}/p^n\Delta\mathbf{Z})^*$ be the group of units in the ring $\mathbf{Z}_{p,\Delta}=\varprojlim_n(\mathbf{Z}/p^n\Delta\mathbf{Z})$. The sets $a+p^n\Delta\mathbf{Z}_{p,\Delta}\subseteq\mathbf{Z}_{p,\Delta}^*$ ($n\geqq 1$, $a\in(\mathbf{Z}/p^n\Delta\mathbf{Z})^*$) form a basis of open sets in $\mathbf{Z}_{p,\Delta}^*$. If we define g: $\mathbf{P}^1(\mathbf{Q})\to\mathscr{L}(A)\otimes\mathbf{Q}$ by

$$g(r)=\int_{i\infty}^{r} f(q)\frac{dq}{q}=[r]_f-[i\infty]_f, \tag{4.1}$$

then the formulas

$$\nu_{A,\Delta}(a+p^n\Delta\mathbf{Z}_{n,\Delta})=\alpha^{-n-1}\left(\alpha\cdot g\left(\frac{a}{p^n\Delta}\right)-g\left(\frac{a}{p^{n-1}\Delta}\right)\right) \tag{4.2}$$

for $n \geqq 1$, $a \in (\mathbf{Z}/p^n \Delta \mathbf{Z})^*$, define a distribution $\nu_{A,\Delta}$ on $\mathbf{Z}_{p,\Delta}^*$ which takes values in $\mathscr{L}(A) \otimes \mathbf{Q}_p$ (compare [16, 20]).

The distribution $\nu_{A,\Delta}$ is bounded because of the Manin-Drinfeld theorem and because α is a unit in $\mathbf{Z}_p^*$. We can therefore use $\nu_{A,\Delta}$ to define p-adic L-functions as follows. Let $\langle \cdot \rangle: \mathbf{Z}_{p,\Delta}^* \to 1 + p\mathbf{Z}_p$ be projection to the first factor in the canonical isomorphism $\mathbf{Z}_{p,\Delta}^* \cong (1+p\mathbf{Z}_p) \times (\mathbf{Z}/p\Delta \mathbf{Z})^*$. For $s \in \mathbf{Z}_p$ and $x \in \mathbf{Z}_{p,\Delta}^*$ we define $\langle x \rangle^s = \exp(s \log(\langle x \rangle))$ using the convergent Taylor series. Then for each primitive Dirichlet character χ of conductor $p^n \Delta$, $n \geqq 0$, we define a p-adic L-function by

$$L_p(\nu_{A,\Delta}, \chi, s) = \int_{\mathbf{Z}_{p,\Delta}^*} \chi(x) \langle x \rangle^{s-1} \, d\nu_{A,\Delta}(x). \tag{4.3}$$

The result of Mazur and Swinnerton-Dyer can be formulated as follows.

(4.4) **Theorem.** *Let χ be a primitive Dirichlet character of conductor $p^n \Delta$, $n \geqq 0$, and let $\mathbf{Q}[\chi, \alpha]$ be the subfield of $\bar{\mathbf{Q}}$ generated by α and the values of χ. Then:*

(a) $L_p(\nu_{A,\Delta}, \chi, 1) \in \mathscr{L}(A) \otimes \mathbf{Q}[\chi, \alpha]$;

(b) *Under the natural map, $\mathscr{L}(A) \otimes \mathbf{Q}[\chi, \alpha] \to \mathbf{C}$, $(\lambda \otimes \beta \mapsto \lambda \beta)$ we have*

$$L_p(\nu_{A,\Delta}, \chi, 1) \mapsto \alpha^{-n} \cdot (1 - \chi(p)\alpha^{-1}) \cdot (1 - \bar{\chi}(p)\alpha^{-1}) \cdot \tau(\chi) \, L(A, \bar{\chi}, 1)$$

where $\tau(\chi)$ is the Gauss sum associated to χ.

Proofs of this can be found in [14, 20].

The Main Conjecture of Iwasawa Theory predicts the following (and much more).

(4.5) **Conjecture IV.** *For each $A \in \mathscr{A}$ the measure $\nu_{A,\Delta}$ take values in $\mathscr{L}(A) \otimes \mathbf{Z}_p$.*

At least we can prove:

(4.6) **Theorem.** *Suppose $p \neq 2$, and let $\pi: X_1(N) \to A$ be a modular parametrization of a curve $A \in \mathscr{A}$. Let $c(\pi)$ be the Manin constant. Then $c(\pi) \cdot \nu_{A,\Delta}$ takes values in $\mathscr{L}(A) \otimes \mathbf{Z}_p$.*

The next corollary is an immediate consequence.

(4.7) **Corollary.** *If $p \neq 2$, then Conjecture $I \Rightarrow$ Conjecture IV.*

Proof of Theorem 4.6. Let $A[p^\infty] \subseteq A(\bar{\mathbf{Q}})$ be the p-power torsion subgroup and let

$$\xi_p: \mathscr{L}(A) \otimes \mathbf{Q}_p \to A[p^\infty]$$

be the p-primary component of the homomorphism $\xi: \mathscr{L}(A) \otimes \mathbf{Q} \to A_{\text{tor}}$ defined in (3.9). The kernel of ξ_p is $\mathscr{L}(A) \otimes \mathbf{Z}_p$.

Next define $\tilde{g}: \mathbf{P}^1(\mathbf{Q}) \to A[p^\infty]$ by

$$\tilde{g}(r) = \xi_p(c(\pi) \cdot g(r)) \tag{4.8}$$

where $g(r)$ is given by (4.1). Equivalently, $\tilde{g}(r)$ is the difference of the images under π of the cusps on $X_1(N)$ corresponding to r and $i\infty$. The image of

$\tilde{g}$ generates the p-primary component $C_{\pi,p}$ of the cuspidal group $C_\pi \subseteq A(\bar{\mathbf{Q}})$ (see §3 for the definition of C_π). Since $p \nmid N$, the action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on the cusps of $X_1(N)$ is unramified at p. Let $\sigma_p \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ be a Frobenius element at p. The action of σ_p on the cusps was exhibited in (3.12). From this we easily derive the following identity, for $n \geqq 1$, $a \in (\mathbf{Z}/p^n \Delta \mathbf{Z})^*$:

$$\left(\tilde{g}\left(\frac{a}{p^n \Delta}\right)\right)^{\sigma_p} = \tilde{g}\left(\frac{a}{p^{n-1}\Delta}\right). \tag{4.9}$$

Indeed,

$$\left(\tilde{g}\left(\frac{a}{p^n \Delta}\right)\right)^{\sigma_p} = \left(\pi\left(\begin{bmatrix} a \\ p^n \Delta \end{bmatrix}\right) - \pi\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right)\right)^{\sigma_p} = \left(\pi\left(\begin{bmatrix} pa \\ p' p^n \Delta \end{bmatrix}\right) - \pi\left(\begin{bmatrix} p \\ 0 \end{bmatrix}\right)\right)^{\sigma_p}$$

(because f is modular for $\Gamma_0(N)$), and this last expression is equal to

$$\pi\left(\begin{bmatrix} pa \\ p^{n-1} \Delta \end{bmatrix}\right)^{\sigma_p} - \pi\left(\begin{bmatrix} p \\ 0 \end{bmatrix}\right)^{\sigma_p} = \pi\left(\begin{bmatrix} a \\ p^{n-1} \Delta \end{bmatrix}\right) - \pi\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \tilde{g}\left(\frac{a}{p^{n-1}\Delta}\right).$$

Since the Galois module $C_{\pi,p}$ is unramified at p, there is a finite flat étale group scheme $C_{\pi,p/\mathbf{Z}_p}$ whose generic fiber is $C_{\pi,p/\mathbf{Q}_p} = C_{\pi,p} \times_{\mathbf{Q}} \mathrm{Spec}(\mathbf{Q}_p)$. Let $A_{/\mathbf{Z}_p}$ be the Neron model of $A_{/\mathbf{Q}_p} = A \times_{\mathbf{Q}} \mathrm{Spec}(\mathbf{Q}_p)$. By the universal property of Neron models the injection $C_{\pi,p/\mathbf{Q}_p} \hookrightarrow A_{/\mathbf{Q}_p}$ extends to a morphism over $\mathbf{Z}_p$, $C_{\pi,p/\mathbf{Z}_p} \to A_{/\mathbf{Z}_p}$. By Raynaud's theorem [17], since $p \neq 2$, this is a monomorphism:

$$C_{\pi,p/\mathbf{Z}_p} \hookrightarrow A_{/\mathbf{Z}_p}.$$

Since the Frobenius endomorphism acts on the étale quotient of the p-divisible group of A by multiplication by α, it follows that σ_p acts on the Galois module $C_{\pi,p}$ by multiplication by α as well. In particular we have

$$\left(\tilde{g}\left(\frac{a}{p^n \Delta}\right)\right)^{\sigma_p} = \alpha \cdot \tilde{g}\left(\frac{a}{p^n \Delta}\right). \tag{4.10}$$

Comparing (4.9) and (4.10) gives $\alpha \cdot \tilde{g}\left(\frac{a}{p^n \Delta}\right) = \tilde{g}\left(\frac{a}{p^{n-1}\Delta}\right)$ which according to (4.8) is equivalent to $c(\pi) \cdot \left(\alpha \cdot g\left(\frac{a}{p^n \Delta}\right) - g\left(\frac{a}{p^{n-1}\Delta}\right)\right) \in \ker(\xi_p)$. From (4.2) and the fact that $\ker(\xi_p) = \mathscr{L}(A) \otimes \mathbf{Z}_p$ we conclude

$$c(\pi) \cdot v_{A,\Delta}(a + p^n \Delta \mathbf{Z}_{p,\Delta}) \in \mathscr{L}(A) \otimes \mathbf{Z}_p$$

for all $n \geqq 1$ and $a \in (\mathbf{Z}/p^n \Delta \mathbf{Z})^*$. This completes the proof. □

We now turn to the question of μ-invariants. For simplicity, we take $\Delta = 1$. Let ε: $(\mathbf{Z}/p\mathbf{Z})^* \to \mathbf{Z}_p^*$ be the Teichmüller character. Complex conjugation decomposes $\mathscr{L}(A) \otimes \mathbf{Z}_p$ into 2 rank one eigenspaces $\mathscr{L}(A)^{\pm} \otimes \mathbf{Z}_p$ with eigenvalues ± 1. Choose $\Omega_A^{\pm} \in \mathscr{L}(A)^{\pm}$ so that $\Omega_A^{\pm} \otimes 1$ are generators of $\mathscr{L}(A)^{\pm} \otimes \mathbf{Z}_p$.

If we fix a topological generator u of $1+p\mathbf{Z}_p$, then for each i, $0 \leqq i \leqq p-1$, there is a power series $F_A^i(T) \in \mathbf{Z}_p[[T]]$ for which

$$L_p(\nu_{A,1}, \varepsilon^i, s) = \Omega_A^{(-1)^i} \otimes F_A^i(u^s - 1) \tag{4.11}$$

The μ-invariant $\mu(F_A^i(T))$ is the highest power of p which divides every coefficient of $F_A^i(T)$.

(4.12) **Proposition.** *Let $\phi: A \to A_{\min}$ be a cyclic $\mathbf{Q}$-isogeny to the curve of minimal height and let K be the kernel of ϕ viewed as a Galois module. Let $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ be a complex conjugation. Then*

$$\mu(F_A^i(T)) = \mu(F_{A_{\min}}^i(T)) + m$$

where

$$m = \begin{cases} \mathrm{ord}_p(\# K) & \text{if } \sigma \text{ acts on } K \text{ as } (-1)^{i+1}; \\ 0 & \text{if } \sigma \text{ acts on } K \text{ as } (-1)^i. \end{cases}$$

Proof. The kernel K^* of the dual isogeny $\hat{\phi}: A_{\min} \to A$ is Cartier dual to K so that the eigenvalue of σ on K is minus that on K^*. Since $A_{\min}$ is the minimal height curve, we know $\mathscr{L}(A_{\min}) \subseteq \mathscr{L}(A)$. Moreover, as modules for complex conjugation we have an isomorphism $K^* \cong (\mathscr{L}(A)/\mathscr{L}(A_{\min}))$. We can therefore choose the p-adic generators $\Omega_A^{\pm} \in \mathscr{L}(A)^{\pm}$, $\Omega_{A_{\min}}^{\pm} \in \mathscr{L}(A_{\min})^{\pm}$ so that

$$\Omega_{A_{\min}}^{(-1)^i} = p^m \cdot \Omega_A^{(-1)^i},$$
$$\Omega_{A_{\min}}^{(-1)^{i+1}} = \Omega_A^{(-1)^{i+1}}.$$

The proposition follows at once. □

(4.13) **Corollary.** *With the notation of Proposition 4.12, if Conjecture IV is true then*

$$\mu(F_A^i(T)) \geqq m.$$

It would be surprising, if the μ-invariants for $A_{\min}$ were ever positive. Correspondingly, we expect that the above inequality is actually an equality.

(4.14) *Remark.* The group K is the maximal μ-type subgroup of $A[p^\infty]$, and therefore Corollary 4.13 is consistent with the Main Conjecture and recent work of Greenberg [8]. Indeed, the bound (4.13) is precisely the bound predicted by formula (75) of [8].

§ 5. Twisting

In this section we examine the behavior of Conjecture I (1.3) under twisting. We will show that if the conjecture is true for a $\mathbf{Q}$-isogeny class of elliptic curves then it is also true for all twists by quadratic fields which are unramified at the primes of additive reduction.

From class field theory we have a correspondence between Galois characters and primitive Dirichlet characters. We shall try to consistently distinguish between the two by underlining Galois characters. Thus, if $\underline{\chi}$: $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{C}^*$ is a Galois character, then χ: $\mathbf{Z} \to \mathbf{C}$ is the corresponding primitive Dirichlet character, and vice versa.

If $A_{/\mathbf{Q}}$ is an elliptic curve and $\underline{\psi}$: $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \pm 1$ is a quadratic Galois character, then A^{ψ} will denote the twist of A by $\underline{\psi}$. Similarly, $\mathscr{A}^{\psi}$ is the twisted isogeny class.

The main theorem of this section is as follows.

(5.1) **Theorem.** *Let $\mathscr{A}$ be an isogeny class of modular elliptic curves, and let $\underline{\psi}$ be a quadratic Galois character which is unramified outside the primes where $\mathscr{A}$ has semistable reduction. If Conjecture I″ (2.9) is true for $\mathscr{A}$ then it is also true for $\mathscr{A}^{\psi}$.*

The proof is based on the two lemmas 5.2, 5.4 below.

(5.2) **Lemma.** *Let $A_{/\mathbf{Q}}$ be an elliptic curve and $\underline{\psi}$ be a quadratic Galois character. If $\underline{\psi}$ is unramified outside the primes where A has semistable reduction then*

$$\mathscr{L}(A^{\psi}) = \frac{\eta}{\tau(\psi)} \mathscr{L}(A)$$

where $\tau(\psi)$ is the Gauss sum of ψ and

$$\eta = \begin{cases} 2 & \text{if the conductor of } \psi \text{ is divisible by 8, and} \\ & A \text{ has good supersingular reduction at 2;} \\ 1 & \text{otherwise.} \end{cases}$$

Sketch of Proof. Let ω_A be a Neron differential on A. Since $\tau(\psi)^2 = D_{\psi}$ is the discriminant of the quadratic field associated to $\underline{\psi}$, $\tau(\psi)^{-1} \cdot \omega_A$ is a regular 1-form on A^{ψ} which is defined over $\mathbf{Q}$. Thus, a Neron differential on A is given by

$$\omega_{A^{\psi}} = \frac{\eta}{\tau(\psi)} \cdot \omega_A$$

for some positive $\eta \in \mathbf{Q}^*$. The resulting relation between minimal discriminants, $\Delta(A^{\psi}) = \eta^{-12} D_{\psi}^6 \cdot \Delta(A)$, reduces the calculation of η to an application of Tate's algorithm [23]. □

Since η is an invariant of the isogeny class, the following corollary is an immediate consequence of the lemma.

(5.3) **Corollary.** *Assume the hypotheses of Lemma 5.2. Let $A_{\min} \in \mathscr{A}$ be the curve of minimal height. Then $A_{\min}^{\psi}$ is the curve of minimal height in $\mathscr{A}^{\psi}$.*

Now let f be the weight 2 normalized newform associated to $\mathscr{A}$. If the q-expansion of f is $\sum a_n q^n$, then $f_{\psi} = \sum \psi(n) a_n q^n$ is the normalized newform associated to $\mathscr{A}^{\psi}$.

(5.4) **Lemma.** *Assume the hypotheses of Lemma 5.2 and define $\eta = 1$ or 2 as in the conclusion of that lemma. Then*

$$\mathscr{L}(f_\psi) \subseteq \frac{\eta}{\tau(\psi)} \mathscr{L}(f).$$

Proof. It is enough to prove the lemma when the conductor $D = D_\psi$ of ψ is a prime power: $D = p^n$. *Let* N be the level of f and N' be the level of f_ψ. Then ND is a divisor of N'.

From the definition of the modular symbols (3.1) we have:

$$\mathscr{L}(f) = \{[\gamma \cdot 0]_f \mid \gamma \in \Gamma_1(N)\}$$

$$\mathscr{L}(f_\psi) = \{[\gamma \cdot 0]_{f_\psi} \mid \gamma \in \Gamma_1(N')\}.$$

Moreover, a standard calculation [16] allows us to express $[\,]_{f_\psi}$ in terms of $[\,]_f$:

$$[r]_{f_\psi} = \frac{1}{\tau(\psi)} \sum_{a \in (\mathbf{Z}/D\mathbf{Z})^*} \psi(a) \left(\left[r + \frac{a}{D} \right]_f - \left[\frac{a}{D} \right]_f \right). \tag{5.5}$$

Now let $\Omega \in \mathscr{L}(f_\psi)$. Then $\Omega = [r]_{f_\psi}$ for some rational cusp $r \in \mathbf{P}^1(\mathbf{Q})$ which is $\Gamma_1(N')$-equivalent to 0. Then r can be expressed as $r = b/M$ with $(b, M) = 1$ and $M \equiv 1 (\operatorname{mod} N')$. In particular we have $(M, D) = 1$.

The cusp $r + \frac{a}{D} = \frac{aM + bD}{MD}$ is easily seen to be $\Gamma_1(N)$-equivalent to $\frac{a}{D}$, so that $\left[r + \frac{a}{D} \right]_f - \left[\frac{a}{D} \right]_f \in \mathscr{L}(f)$. Then by (5.5), $\Omega = [r]_{f_\psi} \in \frac{1}{\tau(\psi)} \cdot \mathscr{L}(f)$ and we have proven $\mathscr{L}(f_\psi) \subseteq \frac{1}{\tau(\psi)} \mathscr{L}(f)$. This proves the lemma, unless $\eta = 2$.

So, suppose $\eta = 2$. Then $D = 8$ and $\mathscr{A}$ is supersingular at 2. The supersingularity at 2 means that the eigenvalue a_2 of the Hecke operator T_2 is divisible by 2.

From the definition of the Hecke operator T_2 we see that for any pair of rational cusps $s_1, s_2, \in \mathbf{P}^1(\mathbf{Q})$:

$$\begin{aligned} &\left(\left[\frac{s_1}{2} \right]_f - \left[\frac{s_2}{2} \right]_f \right) + \left(\left[\frac{s_1 + 1}{2} \right]_f - \left[\frac{s_2 + 1}{2} \right]_f \right) + ([2 s_1]_f - [2 s_2]_f) \\ &\quad = a_2 \cdot ([s_1]_f - [s_2]_f). \end{aligned} \tag{5.6}$$

If moreover s_1 and s_2 are $\Gamma_1(N)$-equivalent, then this lies in $2 \cdot \mathscr{L}(f)$.

Using our assumption that r is $\Gamma_1(N')$-equivalent to 0, it is not hard to establish the following congruences modulo $\mathscr{L}(f)$:

$$\begin{aligned}
&\left[r+\frac{a}{8}\right]_f \equiv \left[\frac{a}{8}\right]_f \qquad \text{for } a \in (\mathbf{Z}/8\,\mathbf{Z})^*;\\
&\left[2r+\frac{a}{4}\right]_f \equiv \left[\frac{a}{4}\right]_f \qquad \text{for } a \in (\mathbf{Z}/4\,\mathbf{Z})^*;\\
&\left[4r+\frac{1}{2}\right]_f \equiv \left[\frac{1}{2}\right]_f.
\end{aligned} \tag{5.7}$$

It is now a routine matter to calculate $\tau(\psi)[r]_{f_\psi}$ modulo $2\cdot\mathscr{L}(f)$. Beginning with (5.5) we work modulo $2\cdot\mathscr{L}(f)$:

$$\begin{aligned}
\tau(\psi)[r]_{f_\psi} &\equiv \sum_{a\in(\mathbf{Z}/8\,\mathbf{Z})^*}\left(\left[r+\frac{a}{8}\right]_f-\left[\frac{a}{8}\right]_f\right)\\
&=\left(\left[r+\frac{1}{8}\right]_f-\left[\frac{1}{8}\right]_f\right)+\left(\left[r+\frac{5}{8}\right]_f-\left[\frac{5}{8}\right]_f\right)\\
&\quad+\left(\left[r+\frac{3}{8}\right]_f-\left[\frac{3}{8}\right]_f\right)+\left(\left[r+\frac{7}{8}\right]_f-\left[\frac{7}{8}\right]_f\right).
\end{aligned}$$

By (5.6) first with $s_1=2r+\frac{1}{4}$, $s_2=\frac{1}{4}$ and then with $s_1=2r+\frac{3}{4}$, $s_2=\frac{3}{4}$, this simplifies modulo $2\cdot\mathscr{L}(f)$ to

$$\begin{aligned}
\tau(\psi)\cdot[r]_{f_\psi} &\equiv ([4r+\tfrac{1}{2}]_f-[\tfrac{1}{2}]_f)+([4r+\tfrac{3}{2}]_f-[\tfrac{3}{2}]_f)\\
&=2([4r+\tfrac{1}{2}]_f-[\tfrac{1}{2}]_f)\\
&\equiv 0.
\end{aligned}$$

Thus $\Omega=[r]_{f_\psi}\in\dfrac{2}{\tau(\psi)}\,\mathscr{L}(f)=\dfrac{\eta}{\tau(\psi)}\,\mathscr{L}(f)$ and the lemma is proved. □

We are now ready to prove Theorem 5.1.

Proof of Theorem 5.1. Let f be the weight two newform associated to $\mathscr{A}$ and let f_ψ be the twist of f by ψ. Let $A_1(f)$, $A_1(f_\psi)$ be the optimal curves in $\mathscr{A}$, $\mathscr{A}^\psi$.

Since we have assumed that Conjecture I″ is true for $\mathscr{A}$ we know $A_1(f)$ is the curve of minimal height in $\mathscr{A}$ and

$$\mathscr{L}(f)=\mathscr{L}(A_1(f)).$$

From Corollary (5.3) we know that $A_1(f)^\psi$ is the curve of minimal height in $\mathscr{A}^\psi$,

$$\mathscr{L}(A_1(f)^\psi)=\frac{\eta}{\tau(\psi)}\cdot\mathscr{L}(A_1(f)).$$

From the fact that $A_1(f)^\psi$ is the curve of minimal height in $\mathscr{A}^\psi$ and from (2.3(c)) we obtain an inclusion

$$\mathscr{L}(A_1(f)^\psi) \subseteq \mathscr{L}(A_1(f_\psi)).$$

But we also know from (1.4(2)) and (1.7(a)) that $\mathscr{L}(A_1(f_\psi)) = c \cdot \mathscr{L}(f_\psi)$ for some integer $c \in \mathbf{Z}$. Thus we derive an inclusion

$$\mathscr{L}(A_1(f_\psi)) \subseteq \mathscr{L}(f_\psi).$$

Finally, we use Lemma 5.4 to get an inclusion

$$\mathscr{L}(f_\psi) \subseteq \frac{\eta}{\tau(\psi)} \mathscr{L}(f).$$

Combining all of the above inclusions we obtain a diagram

$$\begin{tikzcd}
\mathscr{L}(f_\psi) \arrow[r, phantom, "\supseteq"] \arrow[d, phantom, sloped, "\subseteq"] & \mathscr{L}(A_1(f_\psi)) \arrow[r, phantom, "\supseteq"] & \mathscr{L}(A_1(f)^\psi) \arrow[d, equal] \\
\frac{\eta}{\tau(\psi)} \mathscr{L}(f) \arrow[rr, equal] & & \frac{\eta}{\tau(\psi)} \mathscr{L}(A_1(f)).
\end{tikzcd}$$

Therefore all of these inclusions are equalities and in particular

$$\mathscr{L}(f_\psi) = \mathscr{L}(A_1(f)^\psi).$$

As already stated, $A_1(f)^\psi$ is the curve of minimal height in $\mathscr{A}^\psi$. So Conjecture I″ is true for $\mathscr{A}^\psi$ and Theorem 5.1 is proved. □

§ 6. Elliptic curves with complex multiplication

In this section we will use congruence formulas for algebraic parts of special values of L-functions [18, 21] to prove Conjecture II for certain $\mathbf{Q}$-isogeny classes of elliptic curves with complex multiplication (CM) (Theorem 6.4). The basic conjecture (1.3) would then follow for these curves, if we also knew that the Manin constants of the optimal parametrizations were ± 1.

Of course, up to twist, there are only finitely many CM curves over $\mathbf{Q}$. Moreover, up to quadratic twist, there are only finitely many CM curves of the type considered in this section. So the results of the last section reduce the proof of Conjecture I for these curves to a finite calculation (see § 7). Unfortunately, if the imaginary quadratic field has large discriminant, these calculations require far more memory than is available on the personal computer used to obtain the results in § 7. In any case, it is clearly preferable to have a conceptual explanation of our conjectures.

For the rest of this section we fix a prime $p > 3$ satisfying the congruence $p \equiv 3 \pmod 4$ and let $K = \mathbf{Q}(\sqrt{-p})$. We suppose that the class number of K is 1, so that $p \in \{7, 11, 19, 43, 67, 163\}$. It is well known that there is a unique $\mathbf{Q}$-isogeny class $\mathscr{A}(p)$ of conductor p^2 and having CM by K. If $\mathscr{A}$ is another isogeny class with CM by K then there is a unique quadratic Galois character ψ satisfying

$$\begin{aligned}&\text{(a) } \psi \text{ is unramified at } p,\\ &\text{(b) } \mathscr{A} = \mathscr{A}(p)^{\psi}.\end{aligned} \tag{6.1}$$

Moreover, there is a unique curve $A(p) \in \mathscr{A}(p)$ with CM by the full ring $\mathcal{O}_K$ of integers in K and whose minimal discriminant is $-p^3$ [9]. Thus, the curves

$$A(p)^{\psi} \in \mathscr{A}(p)^{\psi} \tag{6.2}$$

where ψ runs through quadratic characters unramified at p give us a complete set of representatives for the isogeny classes of elliptic curves over $\mathbf{Q}$ having CM by K. The arithmetic of these curves has been studied by B. Gross [9]. We will combine his results with congruence formulas for algebraic parts of special values of L-functions [18, 20] to prove Theorem 6.4 which is the main result of this section.

Now fix ψ and $\mathscr{A}$ as in (6.1). We can distinguish 4 curves in $\mathscr{A}$: (1) the curve of minimal height $A_{\min} \in \mathscr{A}$; (2) the optimal curve $A_1 \in \mathscr{A}$; (3) the curve $A = A(p)^{\psi} \in \mathscr{A}$; and (4) the curve $A^* = A(p)^{*\psi} \in \mathscr{A}$ where $A(p)^* = A(p)^{\chi_{-p}}$ is the twist of $A(p)$ by the quadratic character of conductor p associated to K. We will make use of the fact that A and A^* are the only two curves in $\mathscr{A}$ which admit complex multiplication by the full ring of integers $\mathcal{O}_K$ ([9], Theorem 10.2.1). Multiplication by $\sqrt{-p}$ induces an isogeny

$$\phi\colon A \to A^* \tag{6.3}$$

of degree p which is defined over $\mathbf{Q}$ ([9], § 13).

(6.4) **Theorem.** *Let A, A^*, $A_{\min}$, $A_1 \in \mathscr{A}$ be as above. Then*

(a) $A = A_{\min} = A_1$;

(b) *the kernel of $\phi\colon A \to A^*$ (6.3) is contained in the cuspidal subgroup of A_1.*

In particular, Conjecture II (2.4) is true for the isogeny class $\mathscr{A}$.

We will prove Theorem 6.4 through a sequence of lemmas.

(6.5) **Lemma.** $A = A_{\min}$.

Proof. By Corollary 5.3 it suffices to prove this when ψ is the trivial character.

Since the minimal discriminant of $A^* = A(p)^*$ is $-p^9$ ([9], Theorem 12.2.1), a Neron differential on A^* is given by $\omega_{A^*} = \dfrac{1}{\sqrt{-p}} \cdot \omega_A$. Thus $\mathscr{L}(A) = \sqrt{-p} \cdot \mathscr{L}(A^*) \subseteq \mathscr{L}(A^*)$ and the isogeny $\phi\colon A \to A^*$ is étale.

If A' is any other curve in $\mathscr{A}(p)$ then the K-endomorphisms of A' define a suborder $\mathcal{O}' \subseteq \mathcal{O}_K$ of finite index. Since A' is defined over $\mathbf{Q}$, $\mathcal{O}'$ has class number 1. On the other hand $\mathcal{O}' = \mathbf{Z} + c\mathcal{O}_K$ for some positive integer $c > 0$, and the class number h' of $\mathcal{O}'$ can be expressed in terms of c:

$$h' = c \cdot \prod_{l \mid c} (1 - \chi_{-p}(l) \cdot l^{-1}),$$

the product being over prime divisors of c. Since $h' = 1$ we conclude that either $c = 1$ or $c = 2$ and 2 splits in K. Thus either $\mathcal{O}' = \mathcal{O}_K$ or $p = 7$ and $\mathcal{O}' = \mathbf{Z}[\sqrt{-7}]$. In the first case $\mathcal{A}(p)$ contains only the two curves A, A^* and we are done.

If $p = 7$, there are 4 curves in $\mathcal{A}(7)$ labeled 49 A–D in the Antwerp tables [22]. Since [49 A] and [49 C] have CM by all of $\mathcal{O}_K$ and have minimal discriminants -7^3, -7^9 we have $[49\text{A}] = A$ and $[49\text{C}] = A^*$. Thus, as above, the cyclic isogeny $[49\text{A}] \to [49\text{C}]$ is étale. The kernel of the cyclic isogeny $[49\text{A}] \to [49\text{B}]$ has order 2 and is generated by the point $P = (2, -1)$ in the minimal model $y^2 + xy = x^3 - 2x^2 - x - 1$ for [49 A]. The group generated by P in $[49\text{A}]_{/\mathbf{Q}}$ visibly extends to an étale subgroup of the Neron model $[49\text{A}]_{/\mathbf{Z}}$. Thus the isogeny $[49\text{A}] \to [49\text{B}]$ is étale. It is now immediate that [49 A] is the curve of minimal height in $\mathcal{A}(7)$. Thus $A = [49\text{A}] = A_{\min}$. □

(6.6) **Lemma.** *A_1 has* CM *by all of $\mathcal{O}_K$.*

Proof. Since $\mathcal{A}(p)^\psi$ has conductor $p^2 D_\psi^2$, there is a weight two newform f of level $p^2 D_\psi^2$ and trivial Nebentypus character whose L-series is the L-series of the isogeny class. Indeed, if ξ is the Hecke character associated to $\mathcal{A}(p)^\psi$ then the q-expansion of f is

$$f(z) = \sum_{n > 0} a_n q^n = \sum_{\substack{\mathscr{C} \subseteq \mathcal{O} \\ (p, \mathscr{C}) = 1}} \xi(\mathscr{C}) \cdot q^{N\mathscr{C}}, \qquad (q = e^{2\pi i z})$$

where the sum is over ideals $\mathscr{C} \subseteq \mathcal{O}_K$ prime to p, and $N\mathscr{C}$ is the norm of $\mathscr{C}$. From this we see

$$a_n = 0 \quad \text{unless} \quad \chi_{-p}(n) = 1. \tag{6.7}$$

A straightforward calculation shows that the following elements of $\mathbf{Z}[SL_2(\mathbf{Q})]$ define correspondences on the modular curve $X = X_1(p^2 D_\psi^2)$:

$$U = \sum_{a=1}^{p-1} \begin{pmatrix} 1 & a/p \\ 0 & 1 \end{pmatrix},$$

$$U_{\chi_{-p}} = \sum_{a=1}^{p-1} \chi_{-p}(a) \begin{pmatrix} 1 & a/p \\ 0 & 1 \end{pmatrix},$$

$$\Pi = \frac{1}{2}(U + U_{\chi_{-p}}) = \sum_{\substack{a=1 \\ \chi_{-p}(a) = 1}} \begin{pmatrix} 1 & a/p \\ 0 & 1 \end{pmatrix}.$$

These induce endomorphisms of $\mathrm{Pic}^0(X)$. We will show that these endomorphisms induce endomorphisms of the subvariety $A_1 \subseteq \mathrm{Pic}^0(X)$ and moreover that Π

corresponds to a complex multiplication by $\frac{1}{2}(-1+\tau(\chi_{-p}))$ which is a generator of $\mathcal{O}_K$ over $\mathbf{Z}$. It suffices to verify these claims on the tangent spaces at the origin.

Now the tangent space to $\mathrm{Pic}^0(X)$ is canonically isomorphic to the space of weight 2 cusp forms of level $p^2 D_\psi^2$, and the subspace defining A_1 is the line spanned by the newform f. A simple calculation shows

$$f\,|\,U=-f+\sum_{n>0} a_{np}\,q^{np}$$

$$f\,|\,U_{\chi_{-p}}=\tau(\chi_{-p})\sum_{n>0}\chi_{-p}(n)\,a_n\,q^n.$$

By (6.7) this means $f\,|\,U=-f$ and $f\,|\,U_{\chi_{-p}}=\tau(\chi_{-p})\cdot f$. Thus $f\,|\,\Pi=\frac{1}{2}(-1+\tau(\chi_{-p}))\cdot f$ and the lemma is proved. □

From Lemma 6.6 we conclude that the optimal curve A_1 is either A or A^*. To determine which, we need the following theorem (6.8) of Rubin ([18], Theorem 1).

We will write $\underline{\varepsilon}$: $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})\to(\mathbf{Z}/p\mathbf{Z})^*$ for the cyclotomic character giving the action of Galois on the group of pth roots of unity. Since ψ is quadratic we can view it as having values in $(\mathbf{Z}/p\mathbf{Z})^*$ as well.

Let $R=\mathcal{O}_K[\mu_{p-1}]$ be the subring of $\mathbf{C}$ generated over $\mathcal{O}_K$ by the group μ_{p-1} of $(p-1)$st roots of unity, and fix a prime $\wp$ in R lying over p. Reduction modulo $\wp$ induces a group isomorphism $\mu_{p-1}\to(R/\wp)^*$. Let ε: $\mathbf{Z}\to R$ be the primitive Dirichlet character of conductor p associated to the Galois character

$$\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})\xrightarrow{\underline{\varepsilon}}(\mathbf{Z}/p\mathbf{Z})^*\xrightarrow{\sim}(R/\wp)\xrightarrow{\sim}\mu_{p-1}\hookrightarrow R^*.$$

Fix once and for all, a prime $\mathscr{P}$ in $\bar{\mathbf{Q}}$ lying over $\wp$.

(6.8) **Theorem** (Rubin [18]). *Let ω be a fundamental period of the Neron lattice $\mathscr{L}(A)$ of the curve $A=A(p)^\psi$. (Thus, $\mathscr{L}(A)=\Omega\cdot\mathcal{O}_K$.) Then there is a p-unit $u\in\mathbf{Z}$ such that for every primitive Dirichlet character χ of conductor m_χ prime to $p\cdot D_\psi$ the following hold:*

(a) $L^*(A,\chi,1)\overset{\mathrm{def}}{=}u\cdot\dfrac{\tau(\bar\chi)\,L(A,\chi,1)}{\Omega}\in\mathcal{O}_K[\chi]$

(b) $L^*(A,\chi,1)$

$$\equiv\frac{-1}{2}\cdot\chi(pD_\psi)\cdot\psi\varepsilon^{\frac{3p-1}{4}}(m_\chi)\cdot\mathbf{B}_1(\psi\varepsilon^{\frac{p-3}{4}}\chi)\cdot\mathbf{B}_1(\psi\varepsilon^{\frac{p-3}{4}}\bar\chi)\pmod{\mathscr{P}}\quad\square$$

(6.9) **Lemma.** $A_1=A$.

Proof. Let f be the weight two normalized newform associated to $\mathscr{A}$. Since $A=A_{\min}$ we have inclusions

$$\mathscr{L}(A)\subseteq\mathscr{L}(A_1)\subseteq\mathscr{L}(f)\tag{6.10}$$

as in the proof of Theorem 5.1.

Now let X be the Riemann surface underlying $X_1(p^2 D_\psi^2)$ and let $\varphi\colon H^1(X;\mathbf{Z})\to(\mathscr{L}(f)/\mathscr{L}(A))\otimes\mathbf{Z}_p$ be the composition

$$H^1(X;\mathbf{Z})\to\mathscr{L}(f)\to(\mathscr{L}(f)/\mathscr{L}(A))\otimes\mathbf{Z}_p.$$

In [12, 20] it was shown how to associate to φ a 'special value of the L-function'

$$\Lambda(\varphi,\chi)\in(\mathscr{L}(f)/\mathscr{L}(A))\otimes\mathbf{Z}_p[\chi]$$

for any primitive Dirichlet character χ whose conductor is prime to pD_ψ. From the definitions we have

$$\Lambda(\varphi,\chi)\equiv\tau(\chi)L(A,\bar{\chi},1)\quad(\operatorname{mod}\mathscr{L}(A)\otimes\mathbf{Z}_p[\chi]).$$

But (a) of Rubin's theorem (6.8) guarantees that $\tau(\chi)L(A,\bar{\chi},1)\in\mathscr{L}(A)\otimes\mathbf{Z}_p[\chi]$, so

$$\Lambda(\varphi,\chi)=0$$

for every primitive Dirichlet character χ of conductor prime to pD_ψ. By ([21], Theorem 2.1) we conclude $\varphi=0$. Since φ is surjective we must have $\mathscr{L}(f)\otimes\mathbf{Z}_p=\mathscr{L}(A)\otimes\mathbf{Z}_p$ and from (6.10) follows $\mathscr{L}(A_1)\otimes\mathbf{Z}_p=\mathscr{L}(A)\otimes\mathbf{Z}_p$. Since $\mathscr{L}(A^*)=\frac{1}{\sqrt{-p}}\cdot\mathscr{L}(A)$ we can now conclude $A_1\neq A^*$. Thus $A_1=A$ and the proof is complete. □

Theorem 6.4 (a) follows from Lemmas 6.5 and 6.9.

To prove 6.4 (b) we will use the ideas of [20, 21]. Let X be the Riemann surface underlying $X_1(p^2 D_\psi^2)$ and recall from 1.4 (3) that there is a natural inclusion $A_1\hookrightarrow\operatorname{Pic}^0(X)$. Let B be the finite subgroup of $\operatorname{Pic}^0(X)$ corresponding to the kernel of ϕ (6.3). We must show that B is contained in the cuspidal divisor class group of $\operatorname{Pic}^0(X)$.

In [20, 21] the author showed how weight 2 Eisenstein series on $\Gamma_1(p^2 D_\psi^2)$ cut out subgroups of the cuspidal group in $\operatorname{Pic}^0(X)$. By ([21], Proposition 4.7) there is a weight 2 Eisenstein series E on $\Gamma_1(p^2 D_\psi^2)$ whose L-series is

$$L(E,s)=-\tau(\psi\varepsilon^{\frac{p-3}{4}})\cdot L(\psi\varepsilon^{\frac{3p-1}{4}},s)\cdot L(\psi\varepsilon^{\frac{p-3}{4}},s-1).\tag{6.11}$$

(In the notation of [21]: $N=p^2 D_\psi^2$, $N_1=N_2=d=pD_\psi$, $\varepsilon_1=\psi\varepsilon^{\frac{3p-1}{4}}$, $\varepsilon_2=\psi\varepsilon^{\frac{p-3}{4}}$, $\Psi\colon T(N)\to\mathbf{C}^*$ is given by ([21], (4.13)), and $E=E_d(\Psi)$ ([21], Defn. 4.6)). Let $C\subseteq\operatorname{Pic}^0(X)$ be the p-torsion subgroup of the cuspidal subgroup associated to E. From ([21], Examples 4.9 and 4.10) we know that C has order p. We will show $B=C$.

By Pontrjagin duality, as in ([20], § 1.7), we can associate to the groups B, C, homomorphisms

$$\varphi_B,\varphi_C\colon H^1(X;\mathbf{Z})\to\mathbf{Z}/p\mathbf{Z}.$$

To φ_B, φ_C in turn, we have 'special values of L-functions' $\Lambda(\varphi_B,\chi)$, $\Lambda(\varphi_C,\chi)\in\overline{\mathbf{F}}_p$ which in both cases can be computed explicitly. Indeed, $\Lambda(\varphi_B,\chi)$ is given by the right hand side of Rubin's congruence (6.8(b)) and $\Lambda(\varphi_C, \chi)$ is given by ([21], Proposition 4.7(c)) with E as in (6.11). Comparison of these expressions reveals $\Lambda(\varphi_B, \chi)=\Lambda(\varphi_C, \chi)$ for every primitive Dirichlet character χ whose conductor is prime to pD_ψ. By ([21], Theorem 2.1) we then have $\varphi_B=\varphi_C$ and by Pontrjagin duality, $B=C$. This proves 6.4(b). □

§ 7. Numerical evidence

We record the numerical evidence for Conjecture I in Theorem 7.1 below. This was established by direct calculation on a Macintosh Plus personal computer. The programs were written in the C programming language using LightSpeedC^{TM} v. 1.02 produced by Think Technologies of Bedford, Massachusetts, USA. Tables containing the results of these calculations, including period lattices and modular symbols, are being compiled on disks which can be used on any Macintosh personal computer. Programs in C and in Pascal will be included which read to tables so that the data can be used by other programmers to test other conjectures.

(7.1) **Theorem.** *Conjecture I is true for the 749 elliptic curves (281 isogeny classes) of conductor less than or equal to 200 listed in the Antwerp tables* [22].

For computational purposes, it is easier to verify Conjecture I'' (2.8). Thus, for each isogeny class we must show $\mathscr{L}(A_{\min})=\mathscr{L}(f)$ where $A_{\min}$ is the curve of minimal height and f is the associated weight two newform.

Since the Parshin-Faltings height is an approximation to the naive height of an elliptic curve, we should expect for each isogeny class that the minimal height curve would be the first curve found by the search method used to produce the Antwerp tables. This is indeed the case with 7 exceptions (listed below).

We have used Gauss's AGM algorithm [2] to compute the lattice of Neron periods (with 16 places of reliable accuracy) of each curve in the Antwerp tables. Within each isogeny class the inclusions among these lattices were tabulated and the graphs in the Antwerp tables [22] were replaced by directed graphs. As predicted in the last paragraph, the unique minimal lattice (whose existence is guaranteed by Theorem 2.3) corresponds to the first curve listed in the Antwerp tables in almost every case. For example, the curve 11A is the minimal height curve in the isogeny class 11ABC. Here is the complete list of minimal height curves which appear in the Antwerp tables but are not listed first in their respective isogeny classes:

89B, 98B, 128H, 130J, 141G, 150G, 168B.

For example, the curve 168B is the minimal height curve in the isogeny class 168ABCD.

Much more time consuming is the calculation of the lattice $\mathscr{L}(f)$.

The modular form f is represented in the computer by its first 100 Fourier coefficients. The Fourier coefficients a_p for p prime are calculated essentially by counting points modulo p on a representative curve in the isogeny class. For $p \neq 2$ of course, this is equivalent to evaluating $p+1-\sum_{x=0}^{p-1}\left(\frac{P(x)}{p}\right)$ where $y^2=P(x)$ is a minimal Weierstrass equation at p and $\left(\frac{\cdot}{p}\right)$ is the quadratic residue symbol.

With the modular form in hand, we next calculate the modular symbol $[\ ]_f$. This is accomplished by the methods outlined in [11]. We first solve the rather large system of linear equations over $\mathbf{Z}$ imposed by the Manin relations to obtain a basis for the $\mathbf{Z}$-module of all $\mathbf{Z}$-valued modular symbols. We then apply Hecke operators to these modular symbols and extract the rank 2 eigenspace corresponding to f. This gives us $[\ ]_f$ up to the transcendental periods. These periods are obtained by integrating $f(q)\frac{dq}{q}$ over the geodesic in the upper half plane joining 0 to r for one appropriately chosen r. This integral is approximated using a trick of Hecke which expresses the integral as an infinite sum involving the Fourier coefficients. Fortunately, we do not require too much accuracy in this calculation: using Theorem 1.7(a) with A taken to be the quotient of the optimal curve $A_1(f)$ by the cuspidal subgroup, it can be shown that the lattice of values of $[\ ]_f$ is $\frac{1}{c}\mathscr{L}(A)$ for some integer c (in the calculations we found always $c=1$ or $c=2$).

Finally, to find $\mathscr{L}(f)$ we use the characterization

$$\mathscr{L}(f)=\{[\gamma\cdot 0]_f \mid \gamma\in\Gamma_1(N)\}.$$

To find a set of generator for $\Gamma_1(N)$, we proceed as follows. Let $\sigma=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ and $\tau=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ be the standard generators of $\mathrm{SL}(2,\mathbf{Z})$. Let $S\subseteq \mathrm{SL}(2,\mathbf{Z})$ be a set of representatives for $\mathrm{SL}(2,\mathbf{Z})/\Gamma_1(N)$ containing the identity matrix and let $s\colon \mathrm{SL}(2,\mathbf{Z})/\Gamma_1(N)\to R$ be the corresponding section of the natural projection $\mathrm{SL}(2,\mathbf{Z})\to \mathrm{SL}(2,\mathbf{Z})/\Gamma_1(N)$. Then the set

$$\{\gamma^{-1}\sigma^{-1}s(\sigma\gamma), \gamma^{-1}\tau^{-1}s(\tau\gamma) \mid \gamma\in S\}$$

is easily seen to be a generating set for $\Gamma_1(N)$.

As a double check we also calculated the strong lattice and the Manin constant of the strong parametrization for each isogeny class. Our calculations verified that the curve marked in the Antwerp tables as the strong curve is indeed the strong curve, and that the Manin constant is 1 in each case.

Only one minor error was noted in the Antwerp tables. The isogeny between the curves 153A and 153B is a 3-isogeny and not a 2-isogeny as marked in the tables.

References

1. Carayol, H.: Sur les representations l-adiques attachées aux formes modulaires de Hilbert. C.R. Acad. Sci. Paris Sér. I Math. **296**, 629–632 (1983)

2. Cox, D.: Gauss and the arithmetic-geometric mean. Notices of the Am. Math. Sci. **32**, 147–151 (1985)
3. Deligne, P.: Preuve des conjectures de Tate et de Shafarevitch [d'aprèv G. Faltings]. Séminaire Bourbaki, 36e année, **616**, 1983/84
4. Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. In: Deligne, P., Kuijk, W. (eds.) Modular Forms in One Variable II. Proceedings Antwerp 1872 (Lect. Notes Math., vol. 349) Berlin Heidelberg New York: Springer 1973
5. Deligne, P., Ribet, K.: Values of Abelian L-functions at negative integers over totally real fields. Invent. Math. **59**, 227–286 (1980)
6. Drinfeld, V.G.: Two theorems on modular curves. Funct. Anal. App. **7**, 155–156 (1973)
7. Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**, 349–366 (1983)
8. Greenberg, R.: Iwasawa theory for p-adic representations. (To appear in Adv. Stud. Pure Math. **17**)
9. Gross, B.H.: Arithmetic on elliptic curves with complex multiplication. (Lect. Notes Math., vol. 776) Berlin Heidelberg New York: Springer 1980
10. Katz, N.: P-adic L-functions via moduli of elliptic curves. Algebraic Geometry Arcata 1974, Proc. Symp. Pure Math. **29**, 479–506 (1975)
11. Manin, J.: Parabolic points and zeta functions of modular curves (Russian). Izv. Akad. Nauk SSSR Ser. Mat. **36**, 19–65 (1972). Engl. transl. in Math. USSR-Izv. **6**, 19–64 (1972)
12. Mazur, B.: On the arithmetic of special values of L-functions. Invent. Math. **55**, 207–240 (1979)
13. Mazur, B.: Rational isogenies of prime degree. Invent. Math. **44**, 129–162 (1978)
14. Mazur, B., Swinnerton-Dyer, P.: Arithmetic of Weil curves. Invent. Math. **25**, 1–16 (1974)
15. Mazur, B., Tate, J.: Refined conjectures of the 'Birch and Swinnerton-Dyer type'. Duke Math. J. **54**, 711–750 (1987)
16. Mazur, B., Tate, J., Teitelbaum, J.: On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. Invent. Math. **84**, 1–48 (1986)
17. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. Fr. **102**, 241–280 (1974)
18. Rubin, K.: Congruences for special values of L-functions of elliptic curves with complex multiplication. Invent. Math. **71**, 339–364 (1983)
19. Shimura, G.: Introduction to the arithmetic theory of automorphic forms. Publications of the Mathematical Society of Japan 11. Princeton: Princeton University Press 1971
20. Stevens, G.: Arithmetic on modular curves. Progr. Math. 20. Boston: Birkhäuser 1982
21. Stevens, G.: The cuspidal group and special values of L-functions. Trans. Am. Math. Soc. **291**, 519–549 (1985)
22. Swinnerton-Dyer, P., et al.: table 1; Modular functions of one variable (Lect. Notes Math., vol. 476, pp. 81–113) Berlin Heidelberg New York: Springer 1975
23. Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Birch, B., Kuijk, W. (eds.) Modular functions of one variable. (Lect. Notes Math., vol. 476, pp. 33–52) Berlin Heidelberg New York: Springer 1975
24. Wohlfahrt, K.: An extension of F. Klein's level concept. Ill. J. Math. **8**, 529–535 (1964)

Oblatum IX-1987 & 6-II-1989