Journal of the Inst. of Math. Jussieu (2005) **4**(2), 281–316
DOI:10.1017/S147474800500006X Printed in the United Kingdom

MULTIPLICATIVE SUBGROUPS OF $J_0(N)$ AND APPLICATIONS TO ELLIPTIC CURVES

V. VATSAL

Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Vancouver, British Columbia V6T 1Z2, Canada (vatsal@math.ubc.ca)

(Received 7 July 2002; accepted 14 April 2003)

Abstract In this paper, we prove a certain maximality property of the Shimura subgroup amongst the multiplicative-type subgroups of $J_0(N)$, and apply this to verify conjectures of Stevens on the existence of certain canonical parametrizations of rational elliptic curves by modular curves. We are also able to verify some of Stevens's conjectures on the characterization of the elliptic curve in an isogeny class with minimal Faltings–Parshin height.

Keywords: elliptic curves; modular curves; complex multiplication

AMS 2000 *Mathematics subject classification:* Primary 11G05; 11G18

1. Introduction

The goal of this paper is to study two related problems. The first is a certain maximality property of the Shimura subgroup among multiplicative-type subgroups of the Jacobian $J_0(N)$. The second is a conjecture of Stevens, which characterizes the unique curve of minimal Faltings–Parshin height in an isogeny class of elliptic curves over $\mathbb{Q}$. As a consequence, we obtain a number of arithmetic applications to elliptic curves with positive μ-invariant, and to the existence of canonical parametrizations by modular curves.

To explain the first object of our study, we let $X_1(N) = \Gamma_1(N) \setminus \mathcal{H}^*$ and $X_0(N) = \Gamma_0(N) \setminus \mathcal{H}^*$ denote the usual modular curves. We fix models for these curves over $\mathbb{Q}$, for example, the canonical models of Shimura. Since $\Gamma_0(N) \subset \Gamma_1(N)$, there is a finite map $\pi : X_1(N) \to X_0(N)$ given over the complex numbers by the natural projection $\Gamma_1(N) \setminus \mathcal{H}^* \to \Gamma_0(N) \setminus \mathcal{H}^*$. In fact, π is defined over $\mathbb{Q}$, and gives a finite map of the canonical $\mathbb{Q}$-models.

By Picard functoriality, we deduce a morphism of Jacobians $\pi^* : J_0(N) \to J_1(N)$. The kernel of π^* is a finite subgroup V of $J_0(N)(\bar{\mathbb{Q}})$, known as the Shimura subgroup. Since π^* is a $\mathbb{Q}$-rational map, the subgroup V is stable under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. It is known that V is of multiplicative type, meaning that the Cartier dual $W = \hom(V, \mathbb{G}_m)$ is trivial for the action of Galois. Furthermore, it is known that V is *Eisenstein* for the action of the Hecke algebra $\mathbb{T}$, in the sense that it is annihilated by the operators

$T_p - p - 1$, for $p \nmid N$. For this, and other details about the structure of V (including a formula for the order), we refer the reader to the paper [**LO91**].

Mazur proved in 1977 that the Shimura subgroup is the maximal multiplicative type subgroup of $J_0(N)$, *when N is a prime*. Specifically, he proved that if N is a prime, and X is any finite flat subgroup of $J_0(N)$ isomorphic to μ_n, then $X \subset V$. This is part of his detailed study of the kernel in $J_0(N)$ of the Eisenstein ideal $I \subset \mathbb{T}$, where I is the ideal generated by the operators $T_p - p - 1$, for $p \nmid N$. For the details, we refer the reader to [**Maz77**, Chapter 3, § 1]. Our goal here is to understand the extent to which such a result may be generalized to non-prime N. Specifically, we shall prove the following result.

Theorem 1.1. *Let W denote any finite $\mathbb{Q}$-rational subgroup of $J_0(N)(\bar{\mathbb{Q}})$ such that*

(i) *$W \cong \mu_n$ for some odd integer n; and*

(ii) *$J_0(N)$ has semi-stable reduction at ℓ for each prime ℓ dividing n.*

Then W is contained in the Shimura subgroup.

We will sketch the proof of this theorem below, as the techniques are entirely different from those used by Mazur. We also point out that this theorem does *not* help to identify the full kernel of the Eisenstein ideal in $J_0(N)$, and that it does not say anything about the Gorenstein property for Hecke algebras at Eisenstein primes. Since these questions are tangential to the present work, we will not discuss them here.

Next we would like to describe the conjecture of Stevens from [**Ste89**], and explain the relation with the theorem above. Thus, let $\mathcal{C}$ denote an isogeny class of (modular) elliptic curves over $\mathbb{Q}$. As is well known, isogenous elliptic curves give rise to isomorphic Galois representations, and have identical L-series. However, the arithmetic of isogenous curves might be quite different, especially at primes ℓ dividing the degree of an isogeny between them. For example, the coincidence of the L-series does *not* imply the coincidence of the individual terms appearing in the Birch–Swinnerton–Dyer formula (although the formula as a whole is, of course, invariant under isogeny). One way to see this is as follows. If E and E' are isogenous elliptic curves, then an isogeny $\phi : E' \to E$ induces a map of Tate modules $T_p(E') \to T_p(E)$, for each prime p. There is an induced identification $V_p(E') = T_p(E') \otimes \mathbb{Q} \cong T_p(E) \otimes \mathbb{Q} = V_p(E)$, and the subsets $T_p(E)$ and $T_p(E')$ are Galois-stable lattices in $V_p(E) = V_p(E')$. The Birch–Swinnerton–Dyer numbers are encoded in the Selmer groups defined by these lattices, but the lattices corresponding to non-isomorphic curves will, in general, be non-isomorphic themselves, as will be the Selmer groups.

In short, there is no evident way to choose a *canonical* invariant lattice starting from the representation space V_p. Equivalently, there is no obvious way to choose a representative for the isogeny class $\mathcal{C}$. The only plausible candidate is the so-called strong-Weil curve in $\mathcal{C}$ (see Lemma 1.5 below for the definition), but even in very simple cases it is clear that this choice is not the best.

Example 1.2. Consider the isogeny class consisting of the three elliptic curves of conductor 11. The corresponding representation space is the one associated to the modular

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

form $\eta(z)\eta(11z)$ on $\Gamma_0(11)$. We will write A, B, C to denote the curves $11A$, B, C, respectively, with the notation of the Antwerp tables. Then one has $A \cong X_1(11)$, $B \cong X_0(11)$ and C is the quotient of $X_0(11)$ by the cyclic group of order 5 generated by the cusps. We have the sequence of isogenies

$$A = X_1(11) \to B = X_0(11) \to C,$$

where the arrows are as follows. The first is the natural projection $X_1(11) \to X_0(11)$, as described above. The kernel is a cyclic group of order 5, with trivial action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. The second arrow is the projection of $X_0(11)$ onto the quotient by the subgroup of order 5 generated by the cusps. Once again, the kernel is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ as a Galois module.

Let us write $\Omega_E = \Omega_E^+$ for the real Néron period attached to E, for any elliptic curve E over $\mathbb{Q}$. Let χ denote an even quadratic Dirichlet character, of conductor prime to 11, and let $L(E, \chi, s)$ denote the L-series of E, twisted by the character χ. Then it is a classical fact that the special values $L(E, \chi, 1)/\Omega_E$ are rational, for every χ, where E is one of the curves A, B, C. It was shown by Mazur in [**Maz77**] that

$$L(B, \chi, 1)/\Omega_B \equiv 0 \pmod 5,$$

for every non-trivial even quadratic character χ, where B is the elliptic curve $X_0(11)$. If we consider instead the elliptic curve C, the same congruences hold modulo 25. On the other hand, if we take the curve $A = X_1(11)$, then the special values on the left of the formula above are typically 5-adic units. Thus the Birch–Swinnerton–Dyer numbers of even twists of A, B, C are all entirely different.

From the viewpoint of Iwasawa theory, the difference is even more clear. The 5-adic Selmer groups defined by the lattices coming from the Tate modules of B and C have positive μ-invariant, equal to 1 and 2, respectively. On the other hand, the μ-invariant of A is trivial. See [**GV00**] for a discussion from the viewpoint of Iwasawa theory.

Finally, one can calculate the period lattices of A, B and C. One finds that the period lattice of A is minimal, contained inside the lattices of B and C with index 5 and 25, respectively.

In short, it seems reasonable to consider $A = X_1(11)$ as being the 'minimal' curve in the isogeny class $\mathcal{C}$, at least as far as integrality and divisibility properties are concerned. However, it is not apparent *a priori*, why this should be the case. In particular, the strong Weil curve $X_0(11)$ is not the minimal curve to study in this context.

The essence of Stevens's conjecture is that there is indeed a canonical isomorphism class of curves in any isogeny class, and therefore a canonical lattice in the associated representation space. Indeed, given an isogeny class of elliptic curves, Stevens defines a canonical curve $E^* \in \mathcal{C}$ (which he calls the *minimal* curve) and shows that any other $E \in \mathcal{C}$ is given as the quotient of E^* by an étale isogeny (over $\mathbb{Z}$). The novelty of this construction is that the definition of the minimal curve makes no reference at all to 'modular' properties of elliptic curves; one does not even need to make the assumption of modularity for the purposes of the definition. Rather, the minimal curve E^* is defined in terms of its Faltings–Parshin height, which is a purely arithmetic invariant. Stevens's

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

conjecture then relates this minimal curve, defined in terms of heights, to curves defined by modular parametrizations.

We will state the conjecture more precisely below. But before doing this, we need to fix some notation and terminology. Thus let the isogeny class $\mathcal{C}$ be fixed. For any $E \in \mathcal{C}$, we let $E_{\mathbb{Z}}$ denote the Néron model over $\mathbb{Z}$. Note that $H^0(E_{\mathbb{Z}}, \Omega^1) \cong \mathbb{Z}$ for any elliptic curve over $\mathbb{Q}$. Write ω_E for a Néron differential on E, so that $H^0(E_{\mathbb{Z}}, \Omega^1) = \mathbb{Z}\omega_E$. Let

$$\phi : E' \to E$$

be an isogeny with $E', E \in \mathcal{C}$. We say that ϕ is *étale* if the extension $E'_{\mathbb{Z}} \to E_{\mathbb{Z}}$ to Néron models is étale. Equivalently, ϕ is étale if the induced morphism on $\mathbb{Z}$-differentials $\phi^* : H^0(E_{\mathbb{Z}}, \Omega^1) \to H^0(E'_{\mathbb{Z}}, \Omega^1)$ is an isomorphism.

Finally, we want to recall a simple fact about étale isogenies of elliptic curves, which we will use often in the sequel. If $\phi : E' \to E$ is any isogeny over $\mathbb{Q}$, then we have $\phi^*(\omega_E) = n\omega_{E'}$, for some $n = n_\phi \in \mathbb{Z}$. Since ϕ induces an isogeny over $\mathbb{Q}$, the integer n_ϕ is non-zero. The isogeny ϕ is étale if and only if $n_\phi = \pm 1$. If $\phi : E \to E$ is the multiplication by an integer m, then $\phi^*(\omega_E) = m\omega_E$. Thus, if ϕ is any isogeny of degree p, for a prime number p, we must have $n_\phi = 1$ or $n_\phi = p$. Indeed, if $\hat{\phi}$ denotes the dual isogeny, then $\hat{\phi} \circ \phi = [p]$ is the multiplication by p. It follows that precisely one of ϕ and $\hat{\phi}$ is étale.

Now recall that for any elliptic curve E over $\mathbb{Q}$, the Faltings–Parshin height $h(E)$ is defined by

$$h(E) = \left(\frac{1}{2\pi \mathrm{i}} \int_{E_{\mathbb{C}}} \omega_E \wedge \bar{\omega}_E \right)^{-1/2}.$$

Note that $h(E)^{-2} = \mathrm{covolume}(\mathcal{L}(E))$, where $\mathcal{L}(E)$ is the lattice of Néron periods of E. One can show that, for any isogeny class $\mathcal{C}$ of elliptic curves over $\mathbb{Q}$, there is a *unique* curve $E^* \in \mathcal{C}$ with minimal height $h(E^*)$. Indeed, Stevens proved the following striking result. To state the theorem, we shall write $\mathcal{L}(E)$ to denote the lattice of Néron periods of E. Thus $\mathcal{L}(E) \subset \mathbb{C}$ denotes the image of $H_1(E_{\mathbb{C}}, \mathbb{Z})$ under the map $\gamma \mapsto \int_\gamma \omega_E$.

Theorem 1.3 (Stevens). *Let $\mathcal{C}$ denote an arbitrary isogeny class of elliptic curves over $\mathbb{Q}$. Then there exists a unique curve $E^* \in \mathcal{C}$ satisfying the following equivalent conditions.*

(1) *For every $E \in \mathcal{C}$, we have $h(E^*) \leqslant h(E)$.*

(2) *For every $E \in \mathcal{C}$, there is an étale isogeny $E^* \to E$.*

(3) *For every $E \in \mathcal{C}$, we have $\mathcal{L}(E^*) \subset \mathcal{L}(E)$.*

The curve E^* is called the minimal curve in $\mathcal{C}$.

Proof. See [**Ste89**, Theorem 2.3]. □

Remark 1.4. Note that any étale isogeny is necessarily cyclic. Furthermore, one checks that any two cyclic étale isogenies $E^* \to E$ are necessarily equal up to an automorphism.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Now recall the other basic way to construct a distinguished curve in the isogeny class $\mathcal{C}$, using modular parametrizations rather than heights. Thus we need to know that $\mathcal{C}$ is an isogeny class of *modular* elliptic curves over $\mathbb{Q}$. Letting N denote the common conductor of the curves in $\mathcal{C}$, we know from work of Taylor and Wiles and Breuil *et al.* that there exists a non-constant map $X_0(N) \to E$, for any curve $E \in \mathcal{C}$. We say that a non-constant map $\pi : X_0(N) \to E$ is a *modular parametrization* if it is defined over $\mathbb{Q}$, and carries the zero cusp to the identity element in E. Since N is the conductor of the curves in $\mathcal{C}$, we see that $\pi^*(\omega_E) = c(\pi)\omega_f$, where $\omega_f = f(q)\,\mathrm{d}q/q$ is the differential 1-form associated to a normalized newform f of level N. The number $c(\pi)$ is non-zero and rational; it is called the Manin constant of the parametrization π. Since there is a finite $\mathbb{Q}$-rational map $X_1(N) \to X_0(N)$, we deduce that there is a non-constant $\mathbb{Q}$-rational map $X_1(N) \to E$ which carries the zero cusp to the identity, and one can then make the analogous definitions for modular parametrizations of E by the curve $X_1(N)$ as well.

Using this, we can define the strong Weil curves associated to a modular parametrization. Indeed, the following lemma is easy to prove (see [**Maz**], for example).

Lemma 1.5. *Let $\mathcal{C}$ denote an isogeny class of modular elliptic curves with conductor N. Let X denote one of the modular curves $X_0(N)$ or $X_1(N)$. Then there is a unique curve $E_X \in \mathcal{C}$ and a parametrization $\pi_X : X \to E_X$ satisfying the following equivalent conditions.*

(1) *For any $E \in \mathcal{C}$ and any parametrization $\pi' : X \to E$, there is an isogeny $\phi : E_X \to E$ such that $\phi \circ \pi_X = \pi'$.*

(2) *The induced map on homology $H_1(X, \mathbb{Z}) \to H_1(E_X, \mathbb{Z})$ is surjective.*

(3) *The induced map on $\mathrm{Pic}^0 : E_X \cong \mathrm{Pic}(E_X) \to \mathrm{Pic}^0(X)$ is injective.*

The curve E_X is called the strong Weil curve for X.

Remark 1.6. By property (3) above, the strong Weil curve is the unique representative of $\mathcal{C}$ that occurs in the Jacobian $J(X)$. This will be useful in the proofs (see also Remark 1.8 below).

Remark 1.7. The strong Weil curve E_X really does depend on X. For example, in the case of curves of conductor 11 discussed above, the strong Weil curve for $X_0(11)$ is $X_0(11)$ itself. The analogous statement is true for $X_1(11)$, since all these curves have genus 1. The curve usually called the strong Weil curve in the literature is the strong Weil curve for $X_0(N)$. But, as the example of $N = 11$ shows, the lattice associated to the strong Weil curve for $X_0(N)$ is not always the minimal choice.

Remark 1.8. We want to introduce some notations that we will use in the rest of this paper. Fix an isogeny class $\mathcal{C}$ of elliptic curves over $\mathbb{Q}$. We will write E^* to denote the minimal curve in the isogeny class, as defined in Theorem 1.3. We shall also write E_0 and E_1 to denote the strong Weil curves for $X_0(N)$ and $X_1(N)$, respectively. Note that it is easy to describe the relationship between E_0 and E_1; since E_i is the unique member of $\mathcal{C}$ that occurs in $J_i(N)$, we find that E_1 is the quotient of E_0 by the subgroup $V_0 = E_0 \cap V$,

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

for the Shimura subgroup V. Thus $E_0 \cong E_1$ if and only if E_0 has trivial intersection with the Shimura subgroup. Since the Shimura subgroup is of multiplicative type, we see that there is an isogeny $E_1 \to E_0$ with kernel equal to a *constant* group scheme. We shall refer to $E_1 \to E_0$ as the Shimura cover.

The basic conjecture we shall study is the following.

Conjecture 1.9 (Stevens). *We have an isomorphism $E^* \to E_1$ over $\mathbb{Q}$. Equivalently, the strong Weil curve for $X_1(N)$ is the curve of minimal height.*

We are unable to prove this conjecture in full generality. However, we can still make a good deal of progress. We know from Theorem 1.3 that there exists an étale isogeny $\phi : E^* \to E_1$, and the conjecture states that ϕ has degree 1. Let ℓ be any prime number. We shall say that Stevens's conjecture is true at ℓ if the degree of ϕ is prime to ℓ. Then it suffices to prove the conjecture is true at every ℓ. With this convention, we can state the following result.

Theorem 1.10. *Suppose that the isogeny class $\mathcal{C}$ consists of semi-stable curves, and let ℓ denote an odd prime. Then Stevens's conjecture is true at ℓ. Equivalently, the cyclic étale isogeny $E^* \to E_1$ given by Theorem 1.3 has degree a power of two.*

The theorem above is quite restrictive. For example, it is known that any elliptic curve admitting a non-trivial 13-isogeny cannot be semi-stable. However, we can remedy this defect to a reasonable extent.

Theorem 1.11. *Let $\ell \geqslant 7$. Let $\mathcal{C}$ denote an isogeny class of elliptic curves over $\mathbb{Q}$, such that $E[\ell]$ is reducible for some (and hence all) $E \in \mathcal{C}$. Suppose E is ordinary at ℓ. Then Stevens's conjecture is true for the isogeny class $\mathcal{C}$.*

Remark 1.12. In contrast to Theorem 1.10, there is no restriction on the prime 2, or, indeed, at any prime $p \neq \ell$, in the statement above. This is pure serendipity: Mazur's list of rational isogenies, as completed by Kenku (see [**Maz78**, **Ken82**]), implies that there are only finitely many isomorphism classes (up to twist) of elliptic curves E such that $E[p]$ and $E[\ell]$ are *both* reducible, when $\ell \geqslant 7$, and p is a prime distinct from ℓ. In fact, the only time this occurs is when $\ell p = 14$ or $\ell p = 21$. In the former case, the curve $X_0(14)$ has two non-cuspidal rational points, and the corresponding j-invariants and isogenies may be exhibited as complex multiplication (CM) curves of level 49. In the latter, the curve $X_0(21)$ has four non-cuspidal rational points, and the corresponding j-invariants occur at level 162. For explicit constructions of such isogenies of degree 14 and 21, we refer the reader to [**BK75**, p. 79].

Let us show how to reduce the proof of Stevens's conjecture in the case that $E[\ell]$ and $E[p]$ are both reducible to finite amount of computation. There are two cases to consider, namely, $\ell p = 21$ and $\ell p = 14$. We begin with the former. In this event, we look at the isogeny class $\mathcal{C}$ denoted by 162B in Cremona's tables (see [**Cre92**], or the more extensive version available on the web). One checks from the tables in [**BK75**] that the four curves in this isogeny class correspond to the four non-cuspidal rational points on $X_0(21)$, and that each curve in $\mathcal{C} = 162\text{B}$ admits a cyclic isogeny of degree 21. Now, if E' is *any* curve

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

admitting a cyclic isogeny of degree 21, it follows that E is a quadratic twist of a curve in 162B, so that

$$E' = E \otimes \chi_D$$

for some curve $E \in$ 162B, and some quadratic Dirichlet character χ of conductor D. (Note here that the curves in 162B do *not* have any non-trivial endomorphisms.)

But Stevens has proven that if his conjecture for any given curve E, it is also true for quadratic twists $E \otimes \chi_D$ of E, *provided* that D is not divisible by any prime of additive reduction for E (see [**Ste89**, Theorem 5.1]). Thus the conjecture would follow for the isogeny class of E' if it were known for the class 162B, and if the character χ_D satisfied $(D, 3) = 1$ (since $162 = 2 \cdot 3^4$, the curves in 162B are semi-stable at 2 and additive at 3). On the other hand, if $D = 3D'$ with $(3, D') = 1$, we can write $\chi_D = \chi_3 \cdot \chi_{D'}$, where χ_3 denotes the unique quadratic character of conductor 3. Thus we get

$$E' = (E \otimes \chi_3) \otimes \chi_{D'},$$

and D' is not divisible by any prime of additive reduction for $E \otimes \chi_3$. In view of Stevens's theorem, the conjecture would follow for the given E' if one knew it for the cases of 162B and its twist by the character χ_3. It turns out that this twisted isogeny class is nothing more than 162C. Thus we have only to compute the minimal and optimal curves in the isogeny classes 162B and 162C to get Stevens's conjecture for curves admitting isogenies of degree 21. This was, in fact, done by Stevens (see [**Ste89**]), who checked all curves of conductor less than 200. We were able to confirm his results for the curves of interest by making use of William Stein's elliptic curve calculator to determine the period lattices and the degrees of the modular parametrizations. In the case of 162B, for instance, the minimal is the optimal curve, as both turn out to be 162B − 1. In the case of 162C, the minimal curve and optimal curve are both given by 162C − 1. We omit the verification of these claims, as they are easy but somewhat tedious.

One can do a similar check to handle all isogenies of degree 14 (we omit the details). Thus we reduce the proof Theorem 1.11 to the case where $E[\ell]$ is reducible for $\ell \geqslant 7$, and $E[p]$ is irreducible for all $p \neq \ell$. In this case, Stevens's conjecture is trivial at $p \neq \ell$. Furthermore, the list of possible isogenies also implies that there are no cyclic isogenies of degree ℓ^r, where $r \geqslant 2$. Therefore, to prove the theorem above, one needs only to prove that the conjecture is true at ℓ, and here the only possible isogeny is one of degree ℓ. This we can accomplish exploiting the ordinariness hypothesis (see proposition 5.3).

We can also extract from our results cases of a conjecture of Greenberg giving lower bounds on the Iwasawa μ-invariant of an elliptic curve with reducible mod ℓ representation. To state the result, we let E denote any elliptic curve over $\mathbb{Q}$. Let ℓ denote any odd prime number such that E has ordinary reduction at ℓ. Since E is ordinary, the construction of Mazur and Swinnerton and Dyer yields an ℓ-adic L-function $\mathcal{L}_E(T) \in \mathbb{Z}_\ell[\![T]\!] \otimes \mathbb{Q}_\ell$. It is not known in general whether the ℓ-adic L-function has integral coefficients, nor how to calculate the μ-invariant. (The μ-invariant is the unique positive integer μ such that $\ell^{-\mu}\mathcal{L}_E(T)$ is an integral power series with at least one unit coefficient.)

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Let us briefly recall what is known (and not known) about integrality properties and the μ-invariant of the ℓ-adic L-functions. There are two basic cases to consider, depending on whether $E[\ell]$ is reducible or not.

Theorem 1.13. *Suppose that ℓ is a prime of ordinary reduction, and that $E[\ell]$ is irreducible. Then $\mathcal{L}_E(T)$ is integral.*

The proof of this result is easy, and may be found in [**GV00**]. Nothing is known about the μ-invariant when $E[\ell]$ is irreducible, although one could guess that it vanishes.

It remains to consider the case when $E[\ell]$ is reducible. In this case, write $E[\ell]^{\mathrm{ss}}$ for the semi-simplification of $E[\ell]$. Then there is a decomposition of $G_{\mathbb{Q}}$-modules

$$E[\ell]^{\mathrm{ss}} = C \oplus D, \tag{1.1}$$

where $G_{\mathbb{Q}}$ acts on C and D via $\mathbb{F}_\ell^\times$-valued characters χ and $\psi = \chi^{-1}\omega$, respectively. Here ω denotes the Teichmüller character. The module $E[\ell]$ itself may or may not be semi-simple, but since ℓ is an ordinary prime, we see that precisely one of χ and $\psi = \chi^{-1}\omega$ is unramified at ℓ. Furthermore, since ω is odd, we see that precisely one of χ and ψ is even.

The following conjectures are part of the folklore, and motivated by Greenberg's bounds on the μ-invariants of the corresponding Selmer groups.

Conjecture 1.14. *Suppose that E is an elliptic curve over $\mathbb{Q}$. Let ℓ denote a prime of ordinary reduction for E such that $E[\ell]$ is reducible. Then the following statements hold.*

(1) *The L-function $\mathcal{L}_E(T)$ is integral.*

(2) *The invariant μ is characterized as the largest positive integer such that $E[\ell^\infty]$ contains a cyclic $\mathbb{Q}$-rational subgroup K of order ℓ^μ with the property that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on K via a character that is odd, and ramified at ℓ.*

To understand this more concretely, observe that we may split the case where $E[\ell]$ is reducible into two mutually exclusive subcases. We write χ and ψ for the characters appearing in the decomposition (1.1), as before. Without loss of generality, we fix the notation so that χ is unramified and ψ is ramified. Then we get two subcases as follows.

Even subcase. χ is unramified and even. This case arises (for instance) when E or some isogenous curve has a rational point of order ℓ. (So $\chi = 1$.)

Odd subcase. χ is unramified and odd. This occurs when E is a an odd quadratic twist of a curve in the even subcase.

It turns out that these two subcases behave rather differently. Indeed, an equivalent statement of part 2 of the conjecture may be given as follows.

(i) If χ is even, then $\mu = 0$ if and only if there is a *non-split* exact sequence $0 \to \chi \to E[\ell] \to \psi \to 0$.

(ii) If χ is odd, then $\mu = 0$ in general.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Greenberg's conjecture was completely proven for χ odd in the paper [**GV00**].

Theorem 1.15 (cf. [GV00]). *Suppose that the character χ is odd. Then $\mathcal{L}_E(T)$ is integral, and the μ-invariant is trivial.*

In this paper, we prove results toward Greenberg's conjecture for even χ, in the special situation (sub-subcase!) that the unramified even character χ is actually *trivial*. Specifically, we can offer the following result.

Theorem 1.16. *Let the notation and hypotheses be as above. Suppose that the character χ is trivial, so that $E[\ell]^{\mathrm{ss}} = 1 \oplus \omega$. Then $\mathcal{L}_E(T)$ is integral. If $K \subset E[\ell^\infty]$ is the largest subgroup of order ℓ^r such that the action of $G_{\mathbb{Q}}$ on K is via an odd ramified character, then the μ-invariant of $\mathcal{L}_E(T)$ is at least r.*

For the convenience of the reader, we summarize what remains to be done to complete the proof of Greenberg's conjecture. Firstly, nothing is known about the μ-invariant when $E[\ell]$ is irreducible. In the reducible case, nothing is known when χ is even and $\chi \neq 1$. When $\chi = 1$, it is not known that the lower bound given by our Theorem 1.16 is actually sharp.

1.1. Sketch of the proofs

We want to describe the proof of Theorem 1.1, and explain how to deduce Theorem 1.10, starting with the former. Thus suppose that W is a subgroup of $J_0(N)$, isomorphic to μ_n. For simplicity, we will assume in this introduction that $n = \ell^r$ is a power of an odd prime ℓ. Our goal is to prove that W is contained in the Shimura subgroup V.

The first thing to note is that subgroups of the Jacobian variety J_X of a curve X parametrize certain kinds of unramified covers of X, at least over a suitable class of fields. This is simply class field theory for curves, since $J_X \cong \mathrm{Pic}^0(X)$. Specifically, suppose that k is either a finite field or a field of characteristic zero, and that X is a smooth, proper and geometrically irreducible curve over k, equipped with a k-rational point x. Assume that X is embedded into J_X via the point x. We want to define the notion of a k-rational cover of X, following Serre's book [**Ser59**, § VI.2.7]. Thus a curve Y defined over k and equipped with a non-constant k-rational map $\pi : Y \to X$ is said to be a *cover* of X if Y is proper, smooth and geometrically connected over the algebraic closure $\bar{k}$ of k, and if the extension $k(Y)/k(X)$ of function fields induced by the map π is separable. If $k(Y)/k(X)$ is Galois (respectively, abelian), we say that Y is Galois (respectively, abelian). Observe that Y/X may well be Galois over $\bar{k}$ without being Galois over k. In this case, the group $\mathrm{Gal}(\bar{k}(Y)/\bar{k}(X))$ is endowed with a natural action of $\mathrm{Gal}(\bar{k}/k)$. Note also that one could drop the requirement that Y be geometrically connected, simply by requiring $\bar{k}(Y)$ to be a separable algebra over $\bar{k}(X)$. In any case, we shall say that Y/X is unramified if the morphism $Y \to X$ is unramified.

With these conventions, we have the following theorem, which will be used frequently in the sequel.

Theorem 1.17. *Suppose that k is algebraically closed. Then there is a bijective correspondence between finite subgroups $W \subset J_X$ and isomorphism classes of unramified*

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

and geometrically connected covers $X_W \to X$. Explicitly, the correspondence is given by the following recipe. If $W \subset J_X$ is a finite subgroup, and J_W denotes the abelian variety dual to J_X/W, then X_W is the curve which renders the following square Cartesian:

$$\begin{array}{ccc} X_W & \longrightarrow & J_W \\ \downarrow & & \downarrow \\ X & \longrightarrow & J_X \end{array}$$

Proof. This is the corollary of [**Ser59**, p. 128]. □

Remark 1.18. It is part of the theorem that the curve X_W is connected (which is perhaps not obvious from the definition). Note also that if k is not algebraically closed, the same definition allows us to associate a k-curve X_W to any finite k-rational subgroup $W \subset J_X(\bar{k})$. The curve X_W is geometrically connected by the theorem, and the Galois group $\mathrm{Aut}_{\bar{k}}(X_W/X)$ is canonically isomorphic as a $\mathrm{Gal}(\bar{k}/k)$-module to $\hom(W, \mathbb{G}_m)$. In particular, X_W/X is Galois if and only if $\hom(W, \mathbb{G}_m)$ is a constant group scheme over k, at least if k has characteristic zero (see [**LO91**, Proposition 6, p. 191]), or if k is a finite field (see [**Ser59**, Théorème 1, p. 135]).

From the viewpoint of the theorem above, the Shimura subgroup, which is the kernel of the map $J_0(N) \to J_1(N)$ induced by Picard functoriality from the natural projection $X_1(N) \to X_0(N)$, corresponds precisely to those unramified covers of $X_0(N)$ which become trivial (meaning isomorphic to the disjoint union of copies of the base) upon pullback to $X_1(N)$. Reformulated in these terms, the claim of Theorem 1.1 that the given subgroup W is contained in the Shimura subgroup becomes the assertion that the cover $X_W \to X_0(N)$ deduced from W becomes trivial over $X_1(N)$.

Let us now specialize these ideas to the context of Theorem 1.1. Our hypothesis on the subgroup W is that $W \cong \mu_n$, as group schemes over $\mathbb{Q}$. Writing $J_W = (J_0(N)/W)^{\mathrm{dual}}$ as in Theorem 1.17, there is an isogeny $J_W \to J_0(N)$, with kernel $\hom(W, \mathbb{G}_m) = \mathbb{Z}/n\mathbb{Z}$, and we deduce the existence of a curve X_W over $\mathbb{Q}$, and a Galois cover $X_W \to X_0(N)$ with Galois group $\mathbb{Z}/n\mathbb{Z}$ (over $\mathbb{Q}$). As we have seen, W is contained in the Shimura group if and only if the pullback $X_1(N) \times_{X_0(N)} X_W \to X_1(N)$ is trivial as a cover of $X_1(N)$.

The point of this kind of tautological reformulation is that there is a very explicit criterion, due to Ihara, for determining whether a cover of $X_0(N)$ is trivial over $X_1(N)$, in terms of the splitting of super-singular points in characteristic q, where q is any prime such that $q \nmid N$. Thus let $S_q \subset X_0(N)(\bar{\mathbb{F}}_q)$ denote the set of super-singular points. It is well known that all points of S_q are rational over $\mathbb{F}_{q^2}$. Given a degree d cover $X_q \to X_0(N)$ over $\mathbb{F}_q$, we say that a point $x \in S_q$ splits completely in X_q if the fibre over x consists of d distinct points, each rational over the same field $\mathbb{F}_{q^2}$. Then a theorem of Ihara (Theorem 4.4 below) states that if X_q is a smooth and geometrically connected curve, and the cover $X_q \to X_0(N)$ is unramified and defined over $\mathbb{F}_q$, then the pullback of X_q to X_1 is trivial if all super-singular points split completely in X_q.

Thus our strategy is the obvious one: we reduce the cover $X_W \to X_0(N)$ to characteristic q, and attempt to study the splitting pattern of the super-singular points. The main

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

issue is to make a good choice of q, so as to make applicable the theorem of Ihara. This, of course, is a global question, since $X_0(N)$ has plenty of unramified covers in positive characteristic, coming from the fundamental group*. Any successful argument has to be global, and so we study the super-singular points by choosing an auxiliary imaginary quadratic field K, and an auxiliary prime p, and then studying the splitting patterns of CM points defined over the anti-cyclotomic tower H_∞ of conductor p^∞. (Recall here that we are dealing with a cover of degree ℓ^r.) As is well known (see the results of [**Vat02**]), the CM points defined over H_∞ lift the super-singular points in characteristic q, for *every* q which remains inert in K. Given a CM point $P \in X_0(N)(H_\infty)$, we see that the points over P in the cover X_W are defined over an extension L/H_∞, of degree dividing ℓ^r. The main point of our strategy is to show that the field generated by the fibres above *all* the CM points is *finite* over H_∞.

Indeed, we will prove in § 4 below the following results. The notation in the statements is as above. We fix an auxiliary imaginary quadratic field K of discriminant D, such that all primes dividing $N\ell$ are split in K, and write H_∞ to denote the compositum of all anti-cyclotomic fields over K of conductor p^n, as n tends to ∞. Here p is a prime such that $p \nmid ND\ell$.

Theorem 1.19. *Let L/H_∞ be the compositum of all extensions of H_∞ of degree dividing ℓ^r which are unramified outside the set Σ consisting of primes above $r \mid N$, with $r \neq \ell$. (In particular, L is unramified at primes above ℓ, and all the primes in Σ are split in K.) Then the extension L/H_∞ is finite.*

Theorem 1.20. *Let N be a positive integer, and let $X_W \to X_0(N)$ be a cover arising from an isogeny $J_W \to J_0(N)$, where $W \subset J_0(N)$ is a finite $\mathbb{Q}$-rational subgroup isomorphic to μ_n as a Galois module. Let $P \in X_0(N)(H_\infty)$ be any CM point. Then any point in the fibre over P in X_W is rational over the extension L/H_∞ defined above.*

In light of Ihara's criterion, it is clear that the two theorems above imply Theorem 1.1. Indeed, using the Tchebotarev density theorem, one shows that there exist infinitely many primes q which are inert in K and split completely in L/K. Note that any inert prime automatically splits in H_∞/K, since the latter is anti-cyclotomic, and that L/H_∞ is finite by Theorem 1.19. Thus $L/\mathbb{Q}$ is locally of degree 2 at primes above such q. But now Theorem 1.20 implies that the fibres over the CM points are rational over L, and reducing mod q shows that the fibres above the super-singular points are rational over $\mathbb{F}_{q^2}$.

We will briefly discuss the proofs of Theorems 1.19 and 1.20, starting with the former. Basically, one needs to control the ℓ-part of the class group in the p^∞-anti-cyclotomic tower over K; this is an anti-cyclotomic analogue of a theorem of Washington [**Was78**]. We accomplish this by using recent results of Hida [**Hid03**] on the indivisibility of special values of Hecke L-functions, and the main conjecture for Hecke characters that was proved by Rubin [**Rub94**]. However, the required bounds for the class groups do not follow directly from the results of Hida and Rubin, as the orders of the class groups are

* We need to explain at some point what is meant by reducing a given cover $X_W \to X_0(N)$ to characteristic q, since the given X_W is defined only over $\mathbb{Q}$. Since this is a somewhat technical point, we postpone the discussion to § 4.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

not given by critical values of L-functions. Indeed, if H_n denotes the ring class field of conductor p^n and χ is a character of H_n/K, then the L-function $L(s,\chi)$ is the L-function of a theta series associated to a weight one modular form, and so admits no critical values at all. Thus we proceed by a slightly circuitous route, replacing the character χ by a congruent character $\chi\xi$ which does admit critical values, and studying the ℓ-adic Iwasawa theory of $\chi\xi$.

To complete the proof of Theorem 1.19, we have to control the possibilities for ramification at the specified finite set of primes. This is easy, since we only allow ramification at split primes (which are finitely decomposed in H_∞), and we are excluding the possibility of ramification above ℓ. Note that the theorem is false if we allow ramification at inert primes, or at primes above ℓ. The proof of Theorem 1.19 may be found in § 3.

On the other hand, Theorem 1.20 is geometric, and boils down to a certain property of isogenies of semi-stable abelian varieties over unramified extensions of $\mathbb{Q}_p$. The main result states that if $A' \to A$ is an isogeny of abelian varieties over an unramified extension of $\mathbb{Q}_p$, with kernel isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$, then the induced map $A'(E) \to A(E)$ is surjective, where E denotes the maximal unramified extension of $\mathbb{Q}_p$, provided either that A and A' have good reduction at p, or are semi-stable at p and $\ell = p$. The latter case is crucial to ensure that the fields appearing in Theorem 1.19 are unramified above ℓ. Note also that $A'(E) \to A(E)$ is *not* necessarily surjective if the isogeny $A' \to A$ has kernel isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$, with $\ell \neq p$. (We would like to point out to the reader that the p appearing in this discussion is not the same p as the conductor of the ring class extensions above. However, since ℓ, p and q are all already assigned, we are forced to recycle.)

Finally, we make a few comments about the proof of Theorem 1.10. The basic idea is very simple. Suppose that $\mathcal{C}$ is an isogeny class of semi-stable elliptic curves. Let $E_0 \in \mathcal{C}$ denote the strong Weil curve for $X_0(N)$, and consider any étale isogeny $E' \to E_0$. If E_1 denotes the strong Weil curve for X_1, we want to show that E_1 is minimal. Equivalently, we want to show that there is an étale map $E_1 \to E'$. We know in any case from Remark 1.8 that the Shimura cover $E_1 \to E_0$ has constant kernel, and it is easy to check that it is in fact étale, at least over $\mathbb{Z}[\frac{1}{2}]$.

It suffices to show that $E' \to E_0$ is a subcover of the Shimura cover. Thus let $K \subset E_0 \subset J_0(N)$ denote the kernel of the dual isogeny $E_0 \to E'$. Then we must show that K is contained in the Shimura subgroup. Now suppose that $E' \to E_0$ has degree ℓ, for some odd prime ℓ. Then $E_0[\ell]$ is reducible and has composition factors $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ (since E_0 is semi-stable). Since $E' \to E_0$ is étale, one checks that $K \cong \mu_\ell$. But now Theorem 1.1 implies that any subgroup isomorphic to μ_ℓ is contained in the Shimura subgroup, as required.

To handle the case of a general étale isogeny $E' \to E_0$, one has to work a bit harder. It suffices to consider an étale isogeny $E' \to E_0$ of degree ℓ^r, for a number prime ℓ, and show that the subgroup K constructed above is contained in the Shimura subgroup. This is not so easy, because it is false in general that the kernel of a cyclic étale ℓ^r-isogeny is isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z}$. (For example, $X_1(11)$ admits a cyclic and étale 25-isogeny, but there are no elliptic curves with points of order 25.) Thus one cannot apply our results on the Shimura subgroup directly. To circumvent this problem, we show that the case $r \geqslant 2$

happens only finitely often. The basic idea is to construct an étale isogeny $E_0 \to E''$ of degree ℓ using a subgroup coming from the cuspidal group in $J_0(N)$ (and a multiplicity one theorem to ensure that it is contained in E_0). Then Mazur's list of rational isogenies implies that any cyclic étale isogeny $E' \to E_0$ of degree ℓ^r must have $r \leqslant 1$, as the composite $E' \to E_0 \to E''$ is an étale, hence cyclic, isogeny of degree ℓ^{r+1}, so that $r + 1 \leqslant 2$ except for finitely many explicitly known cases. One can check Stevens's conjecture by computer in these finitely many cases, as in Remark 1.12, so that we may in our analysis restrict to isogenies of degree ℓ, and these may be handled as described above. We point out also that the proof of Theorem 1.11 follows very similar lines to those sketched above.

2. Galois covers

In this section we want to consider the following situation. Let $L/\mathbb{Q}$ denote a number field, and let A denote an abelian variety over L. We consider an isogeny $A' \to A$, whose kernel is isomorphic as a group scheme to the constant group $\mathbb{Z}/n\mathbb{Z}$ over L. Here $n = \ell^r$ is a power of an odd prime ℓ. Let P denote any point in $A(L)$. Then it is clear that the fibre above P is rational over some extension L'/L of degree dividing n, and our goal is to control the possible ramification in L'. Not surprisingly, the answer will turn out to depend on the reduction types of the abelian varieties A and A', as well as the ramification over $\mathbb{Q}$ in the field L. Analysing the ramification at primes of bad reduction of A, or at primes above 2ℓ, will require special care.

2.1. For our purposes, it suffices to work under the following simplifying assumptions.

(i) ℓ is odd.

(ii) A is semi-stable.

Since there are still several cases to consider, and since we will actually make some more assumptions later, the reader may wish to look immediately at Corollary 2.5 to get an idea of the final result.

In any case, if $\mathcal{P}$ denotes any prime of L of residue characteristic p, we may analyse the ramification in L' at primes above $\mathcal{P}$ simply by studying the corresponding local problem and working over the completion $F = L_{\mathcal{P}}$ of L at $\mathcal{P}$. Thus F is a finite extension of $\mathbb{Q}_p$. We consider an abelian variety A over F, and a fixed F-isogeny $\phi : A' \to A$ such that the kernel K is isomorphic as a G_F-module to $\mathbb{Z}/n\mathbb{Z}$, where $n = \ell^r$, for some odd prime ℓ. In order to proceed, we need to impose a further hypothesis.

(iii) If $\mathcal{P}$ has residue characteristic $p = 2$, then A and A' have good reduction at $\mathcal{P}$. (But ℓ is always assumed to be odd.)

Note that we have *not* excluded the case $\ell = p$ if p is odd.

We start by considering the case where $L/\mathbb{Q}$ is unramified at $\mathcal{P}$. Thus $F/\mathbb{Q}_p$ is a finite unramified extension, Write $\mathcal{O}_F$ for the ring of integers in F. We will write $E = \mathbb{Q}_p^{\mathrm{unr}}$ to denote the maximal unramified extension of $\mathbb{Q}_p$ (or F, since $F/\mathbb{Q}_p$ is unramified), and

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

let $R = \mathbb{Z}_p^{\mathrm{unr}}$ denote the ring of integers in E. For an abelian variety A over F, we write A_R for the Néron model of A over R, and A_s for the special fibre. Here s denotes the closed point of $\mathrm{Spec}(R)$. Recall also that we have assumed that our abelian varieties A and A' are semi-stable.

Lemma 2.2. *Let A' be a semi-stable abelian variety over F, and let K denote a subgroup of $A(F)$ isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Then the reduction map induces an injection $K \to A'_s$.*

Proof. If $p = 2$, our hypotheses require that ℓ be odd, and that A have good reduction, and the result is well known in this case (for any p of good reduction, and $\ell \neq p$).

Thus we may assume that p is odd. Let $K = K_R$ denote the scheme theoretic closure of $(\mathbb{Z}/n\mathbb{Z})_F$ in the Néron model A'_R. Then K is a quasi-finite and flat scheme over $\mathrm{Spec}(R)$, since A' is a semi-stable abelian variety. Furthermore, we have a morphism $(\mathbb{Z}/n\mathbb{Z})_R \to K$, which is an isomorphism along the generic fibre.

Since R is Henselian and K is separated, we may consider the finite part K_0 of K. Then K_0 is a finite flat group scheme over $\mathrm{Spec}(R)$, and the complement of K_0 in K has empty special fibre. Since $(\mathbb{Z}/n\mathbb{Z})_R$ is finite flat, and formation of the finite part is functorial, the morphism $(\mathbb{Z}/n\mathbb{Z})_R \to K_R$ factors through K_0. Since $(\mathbb{Z}/n\mathbb{Z})_R \to K_R$ is an isomorphism along the generic fibre, and the complement of K_0 in K has empty special fibre, we see that in fact $K = K_0$ and K is finite as well as flat. But $F/\mathbb{Q}_p$ is unramified, and $(\mathbb{Z}/n\mathbb{Z})_R \to K_0$ is an isomorphism on generic fibres. Now since p is odd, and $F/\mathbb{Q}_p$ is unramified, a theorem of Raynaud [**Ray74**] implies that $(\mathbb{Z}/n\mathbb{Z})_R \to K_0 = K$ is an isomorphism. Since K_R is a closed subscheme of A'_R, the result follows. □

Proposition 2.3. *Let $F/\mathbb{Q}_p$ be unramified. Suppose that $A' \to A$ is an isogeny of abelian varieties over F with kernel isomorphic to $\mathbb{Z}/n\mathbb{Z}$, with $n = \ell^r$ as above. Suppose that either of the following conditions hold.*

(1) *A and A' have good reduction at p, and ℓ is odd.*

(2) *A and A' have semi-stable reduction, and $\ell = p$ is odd.*

Then the induced homomorphism $A'(E) \to A(E)$ of E-valued points is a surjection, where $E = \mathbb{Q}_p^{\mathrm{unr}}$

Proof. Suppose first that p is a prime of good reduction for A and A'. Then the sequence $0 \to K_R \to A'_R \to A_R \to 0$ is exact, and there is a surjection of abelian varieties $A'_s \to A_s$ over $\bar{\mathbb{F}}_p$. Since the residue field of R is algebraically closed, Hensel's lemma implies that for each $P \in A(R)$, there exists $P' \in A'(R)$ such that $P' \mapsto P$, modulo the kernel A_0 of the reduction map $A \to A_s$. But the kernel of our isogeny is constant, and has trivial intersection with A'_0 (the kernel of reduction in A') by the lemma above. Since A_0 and A'_0 are given by the formal groups of A and A', respectively, one checks that there is an isomorphism $A'_0 \to A_0$ (for example, by looking at the Tate modules), and the claim follows in this case.

Now consider the case when A and A' have bad reduction at p. According to our hypotheses, this implies that $\ell = p$ and that the reduction is semi-stable. Under

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

these conditions, we are required to show that $H^0(I, A') \to H^0(I, A)$ is surjective, where $I = I_F = G_E$ denotes the inertia group. Equivalently, we need to show that $H^1(I, K) \to H^1(I, A')$ is injective. Let $\kappa_{A'}$ denote the usual Kummer map on A', so that $\kappa_{A'}(A'(E) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \subset H^1(G_E, A'[p^\infty])$. Since A' is semi-stable, results of Coates and Greenberg (see [**CG96**, formula (4.9), p. 153]) show that the image of $\kappa_{A'}$ maps to zero in $H^1(I_F, A'[p^\infty]^{\mathrm{unr}})$, where $A'[p^\infty]^{\mathrm{unr}}$ is the maximal étale quotient of the p-divisible group of A'. But $K_s \to A'_s$ being injective by the lemma above, we see that K has trivial intersection with the connected part of $A'[p^\infty]$, which implies that $K \to A'[p^\infty]^{\mathrm{unr}}$ is injective. In particular, $A'[p^\infty]^{\mathrm{unr}}$ is non-trivial. Since I_F acts trivially on $A'[p^\infty]^{\mathrm{unr}}$ and K, we see that $H^1(I_F, K) \to H^1(I_F, A'[p^\infty]^{\mathrm{unr}})$ is injective as well. It follows that the image of $H^1(I_F, K)$ in $H^1(I_F, A'[p^\infty])$ has trivial intersection with the image of $\kappa_{A'}$. Since the image of $\kappa_{A'}$ is the kernel of $H^1(I_F, A'[p^\infty]) \to H^1(I, A')_p$, the result follows. □

Remark 2.4. Note that the argument at the beginning of the proof is valid even if $F/\mathbb{Q}_p$ is ramified, provided that A and A' have good reduction at p, and $\ell \neq p$. We we will use this below.

The following corollary is now immediate.

Corollary 2.5. *Let $F/\mathbb{Q}_p$ be any finite extension. Let A denote an abelian variety over F, and let $A' \to A$ denote an isogeny with kernel K isomorphic to $\mathbb{Z}/n\mathbb{Z}$ (as a G_F-module), where $n = \ell^r$, for an odd prime ℓ. Let P denote any point in $A(F)$ and let $P' \in A'(\bar{F})$ denote any point in the fibre above P. Then the point P' is rational over an unramified extension of F under each of the following hypotheses.*

(1) *A has good reduction and $\ell \neq p$ ($p = 2$ is allowed).*

(2) *A has semi-stable reduction, and $\ell = p$ is odd, and $F/\mathbb{Q}_p$ is unramified.*

Corollary 2.6. *Let $F/\mathbb{Q}_p$ be any finite extension. Let X denote a smooth curve over F, and let J denote its Jacobian. Assume that X has an F-rational point y, and let $J' \to J$ denote an isogeny with kernel K isomorphic to $\mathbb{Z}/n\mathbb{Z}$ (as a G_F-module), where $n = \ell^r$, for an odd prime ℓ.*

Let $X' \to X$ denote the pullback of $J' \to J$, under the inclusion $\iota : X \to J$ induced by the rational point y. Let $x \in X(F)$, and let $x' \in X'$ denote any point in the fibre over x. Then the point x' is rational over an unramified extension of F under each of the two conditions listed in Corollary 2.5 (with $A = J$).

Proof. The fibre in X' over x may be canonically identified with the fibre in J' over $\iota(x)$. □

Applying this to the case of $X = X_0(N)$, and $J = J_0(N)$, we obtain the following result.

Corollary 2.7. *Let L denote a number field which is unramified at all primes dividing N, and let P denote any point in $X_0(N)(L)$. Let $J' \to J_0(N)$ be any L-isogeny with kernel K isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Here $n = \ell^r$ for an odd prime ℓ, where ℓ is a prime such that $\ell^2 \nmid N$, and such that ℓ is unramified in L.*

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Then if $X' \to X_0(N)$ is the induced cover of $X_0(N)$, and P' is any point in $X'(\bar{\mathbb{Q}})$ lying over P, then $P' \in X'(L')$, where L'/L is a finite abelian extension of degree dividing ℓ^r, unramified outside the primes dividing N. If N is divisible by precisely the first power of ℓ, then L' is unramified at primes above ℓ.

Proof. It is clear by Galois theory that L' is a finite abelian extension of L, with degree dividing ℓ^r. By the corollary above, L' is unramified at primes above p if p is a prime of good reduction, namely, if p is away from N. Furthermore, the corollary also implies that L' is unramified at primes above ℓ if ℓ is odd and if $\ell^2 \nmid N$, since it is well known that J_0 has semi-stable reduction at ℓ in that situation. □

3. Unramified extensions of anti-cyclotomic fields

In this section, we consider an imaginary quadratic field K, and the extensions H_n/K, where H_n is the ring class field of conductor p^n, for an odd prime p which is unramified in K. Our goal is to bound the ℓ-part of the class group of H_n, where ℓ is a prime distinct from p, as n tends towards infinity. Our main tools will be Rubin's main conjectures for imaginary quadratic fields, and a theorem of Hida on the ℓ-part of special values of Hecke L-functions. As we have already remarked in the introduction, the proof is somewhat circuitous, since the orders of the class groups of interest are not given by critical values of L-functions.

For the convenience of the reader, we remark also that the prime p in this section does not play the same role in our arguments as the prime called p in the section above.

3.1. We shall make the following assumptions on the data K, ℓ and p.

(1) The unit group $\mathcal{O}_K^\times$ consists of ± 1.

(2) The prime ℓ is odd, and split in K.

(3) The number $p-1$ is relatively prime to ℓ if p is split in K.

(4) The number $p+1$ is relatively prime to ℓ if p is inert in K.

Now let $\mathcal{O}_n$ denote the order $\mathbb{Z} + p^n\mathcal{O}_K$ of conductor p^n in K. Let $G_n = \mathrm{Pic}(\mathcal{O}_n)$ denote the Picard group of $\mathcal{O}_n$. Then $\#G_n = h_K \cdot p^{n-1} \cdot (p \pm 1)/u$, where h_K is the class number of K, and $u = \frac{1}{2}\#\mathcal{O}_K^\times = 1$ under our hypotheses. The sign $\pm$ is $+$ if p is inert in K, and $-$ if p is split.

We may decompose $G_n = \Delta \times \mathfrak{g}_n$, where Δ is the ℓ-Sylow subgroup of G_n, and the order of $\mathfrak{g}_n$ is relatively prime to ℓ. Note that the group Δ is independent of n, and is trivial if the class number of K is prime to ℓ. The possibility that Δ is non-trivial will cause some complications in the sequel. However, it does not seem to be possible to exclude this case in our applications. We write $F_n \subset H_n$ for the fixed field of Δ. Thus F_n/K is the maximal subfield of H_n/K of degree prime to ℓ.

Let N be any $\mathbb{Z}_\ell[G_n]$ module. Since the order of G_n may be divisible by ℓ, we cannot immediately break up N according to the characters of G_n. However, we can still

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

decompose according to the characters χ of $\mathfrak{g}_n$. Thus let $\mathfrak{o}$ denote a finite extension of $\mathbb{Z}_\ell$ containing the values of the character χ, and let

$$e_\chi = \frac{1}{\#\mathfrak{g}_n} \sum_{\sigma \in \mathfrak{g}_n} \chi(\sigma)\sigma^{-1} \in \mathfrak{o}[\mathfrak{g}_n]$$

denote the usual idempotent associated to χ. This makes sense since the order of $\mathfrak{g}_n$ is prime to ℓ. For any character χ of $\mathfrak{g}_n$, we will write N^χ to denote $e_\chi(N \otimes \mathfrak{o})$. Then $N \otimes \mathfrak{o} \cong \oplus N^\chi$, as χ runs over all characters of $\mathfrak{g}_n$, provided, of course, that $\mathfrak{o}$ is sufficiently large. The precise choice of $\mathfrak{o}$ will not be relevant to our arguments. We only need the fact that N is finite (respectively, zero) if and only if each N^χ is finite (respectively, zero), which is independent of the choice of $\mathfrak{o}$. Our basic example will be obtained by taking N to be the ℓ-Sylow subgroup A_n of the class group of F_n.

Before proceeding, we make one simple observation, which is basic to everything that follows. Let χ denote a character of $\mathfrak{g}_n$, and let A_n^χ denote the χ-component of the ℓ-Sylow subgroup A_n of the ideal class group of F_n. If $m > n$, we may equally well view χ as a character of $\mathfrak{g}_m$ by inflation, and form the χ-part A_m^χ of A_m. There is a natural map $A_n \to A_m$ induced by extension of ideals, which gives rise to a map $A_n^\chi \to A_m^\chi$.

Lemma 3.2. *Suppose that $m \geqslant n$, and χ is any character of $\mathfrak{g}_n$. Then the natural map $A_n^\chi \to A_m^\chi$ is an isomorphism.*

Proof. Let F_i^{un} denote the subfield of the Hilbert class field of F_i cut out by A_i, and let $\chi' = \prod \chi^\sigma$, where the product is taken over the conjugates of χ over $\mathbb{Q}_\ell$. Then χ' is an irreducible $\mathbb{Z}_\ell$-representation, and we write $F_i^{\chi'}$ for the subfield of F_i^{un} corresponding to the χ'-isotypic component of A_i. To prove the lemma it suffices to show that

$$F_n^{\chi'} \cdot F_m = F_m^{\chi'}.$$

Notice that $F_i^{\chi'}/F_i$ is an unramified abelian ℓ-extension. In particular, $F_n^{\chi'} \cap F_m = F_n$, since the degree of the fields F_i over the base K is assumed prime to ℓ. Thus $F_n^{\chi'} \cdot F_m$ is contained in $F_m^{\chi'}$.

To prove the reverse inclusion, we may argue as follows. Since $\mathrm{Gal}(F_m/K)$ is a group of order prime to ℓ, we see that the extension

$$0 \to \mathrm{Gal}(F_m^{\chi'}/F_m) \to \mathrm{Gal}(F_m^{\chi'}/K) \to \mathrm{Gal}(F_m/K) \to 0 \tag{3.1}$$

is in fact a semidirect product. Choose a section $\mathrm{Gal}(F_m/K) \to \mathrm{Gal}(F_m^{\chi'}/K)$. Then the subgroup $\mathrm{Gal}(F_m/F_n) \subset \mathrm{Gal}(F_m/K)$ is normal inside $\mathrm{Gal}(F_m^{\chi'}/K)$, since $\mathrm{Gal}(F_m/K)$ acts on $\mathrm{Gal}(F_m^{\chi'}/F_m)$ via the representation χ', which is trivial on $\mathrm{Gal}(F_m/F_n)$ by assumption. Let $F' \subset F_m^{\chi'}$ denote the fixed field of $\mathrm{Gal}(F_m/F_n)$. One sees from equation (3.1) that there is an exact sequence

$$0 \to \mathrm{Gal}(F'/F_n) \to \mathrm{Gal}(F'/K) \to \mathrm{Gal}(F_n/K) \to 0,$$

where $\mathrm{Gal}(F'/F_n)$ is isomorphic to $\mathrm{Gal}(F_m^{\chi'}/F_m)$. Furthermore, $\mathrm{Gal}(F_n/K)$ acts on $\mathrm{Gal}(F'/F_n)$ via the representation χ'.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

We claim now that F'/F_n is unramified. But this is clear, since $F_m^{\chi'}/F_m$ is unramified, so that any ramification in $F_m^{\chi'}/K$ comes from F_m/K and all the ramification indices must divide the degree of F_m/K, which is prime to ℓ. Since the degree of F'/F_n is a power of ℓ (recall that $\mathrm{Gal}(F_m^{\chi'}/F_m)$ is an ℓ-group) it follows that F'/F_n is unramified. Thus $F' \subset F_n^{\chi'}$, and $F_m^{\chi'}$ descends to F_n. □

3.3. Now let $n(\chi)$ denote the smallest integer such that χ factors through $\mathrm{Gal}(F_n/K)$. Then, in view of the lemma above, we have $A_n^\chi = A_m^\chi$ for all $n, m \geqslant n(\chi)$. In other words, $A_n^\chi = A_m^\chi$ whenever these expressions make sense. Now, letting A_∞ denote the direct limit of the groups A_n, we see that $A_\infty = \mathrm{Gal}(M_\infty/F_\infty)$ where $F_\infty = \cup F_n$, and M_∞ is the maximal abelian unramified ℓ-extension of F_∞. Viewing χ as a character as $\mathrm{Gal}(F_\infty/K)$, it then follows that $A_\infty^\chi = A_n^\chi$ for all $n \geqslant n(\chi)$. In the sequel, we will be concerned with proving that $A_\infty^\chi = 0$ for all but finitely many characters χ, as χ runs over the set of characters of the finite extensions F_n/K, for $n \to \infty$. In view of the above, it suffices to prove that, for all but finitely many χ, we have $A_n^\chi = 0$ for *any* convenient choice of n such that χ factors through F_n/F.

3.4. From now on, we fix the data consisting of a character χ and a base field $F = F_n$, such that $n \geqslant \max\{n(\chi), 1\}$. We put $F = F_n$ and write $\mathfrak{g}$ for $\mathrm{Gal}(F/K)$. The character χ is the primary object here, and as explained above, we may make any convenient choice of F.

Next we fix a factor $\mathfrak{l}$ of ℓ in K. (Recall that ℓ is assumed to be split.) We let $D_\mathfrak{l}$ and $I_\mathfrak{l}$ denote fixed decomposition and inertia groups, respectively. Let $K_\infty^\mathfrak{l}$ denote the unique $\mathbb{Z}_\ell$ extension of K unramified outside $\mathfrak{l}$. We let $F_\infty^\mathfrak{l}/F$ denote the compositum of F with $K_\infty^\mathfrak{l}$. (Here $F_\infty^\mathfrak{l}$ is to be distinguished from $F_\infty = \cup F_n$, which is a p-ramified extension.) Observe here that since F/K has degree prime to ℓ, we have $\mathrm{Gal}(F_\infty^\mathfrak{l}/K) = \mathfrak{g} \times \Gamma$, where $\Gamma \cong \mathbb{Z}_\ell$. Thus we can break up any $\mathrm{Gal}(F_\infty^\mathfrak{l}/K)$-module according to the characters χ of $\mathfrak{g}$. We fix a finite extension $\mathfrak{o}/\mathbb{Z}_l$ containing the values of the given character χ, and put $\Lambda = \mathfrak{o}[\![\Gamma]\!] \cong \mathfrak{o}[\![T]\!]$.

Let $N_\infty^\mathfrak{l}$ denote the maximal abelian pro-ℓ extension of $F_\infty^\mathfrak{l}$ which is unramified outside the primes above $\mathfrak{l}$. Then $X_\infty^\mathfrak{l} = \mathrm{Gal}(N_\infty^\mathfrak{l}/F_\infty^\mathfrak{l}) \otimes_{\mathbb{Z}_\ell} \mathfrak{o}$ is a module over $\mathfrak{o}[\![\mathrm{Gal}(F_\infty^\mathfrak{l}/K)]\!] = \mathfrak{o}[\![\mathfrak{g} \times \Gamma]\!]$. We will put a subscript on the objects $X_{n,\infty}^\mathfrak{l}$, $N_{n,\infty}^\mathfrak{l}$, etc., if we wish to indicate the dependence on the chosen base $F = F_n$.

In the sequel we will drop the superscript of $\mathfrak{l}$ on $X_\infty^\mathfrak{l}$ since the notation will be cumbersome when we consider χ-components, and there is no other X_∞ anywhere. Thus let $X_\infty^\chi = e_\chi(X_\infty)$ denote the χ-isotypic part of X_∞. Then X_∞^χ is a module over Λ. It is well known (see [**dS87**, p. 103]) that X_∞^χ is torsion over Λ.

Now we want to check that the modules X_∞^χ depend only on the character χ, and not on the base field $F = F_n$. Thus suppose that $m \geqslant n$, and view the character χ as a character of F_m. Let $X_{i,\infty}^\chi$ denote the χ-isotypic part of $X_{i,\infty}$, where the dependence on the base F_i is indicated by the subscript i.

Lemma 3.5. *The natural map $X_{n,\infty}^\chi \to X_{m,\infty}^\chi$ is an isomorphism.*

Proof. This follows from an argument similar to that which proved Lemma 3.2, using the fact that $F_{m,\infty}^\mathfrak{l}/F_{n,\infty}^\mathfrak{l}$ is a finite extension of degree prime to ℓ. □

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Now if F' is any subfield of $F_\infty^{\mathfrak{l}}$, we write $U(F')$ for the group of local units in $F' \otimes K_\ell$ which are congruent to 1 modulo primes above $\mathfrak{l}$. Let $C(F')$ denote the group of elliptic units in F' and let $\bar{C}(F')$ denote the closure in $U(F')$ of $C(F') \cap U(F')$. Put $U_\infty = \lim_{F'} U(F')$ and $\bar{C}_\infty = \lim_{F'} \bar{C}(F')$, where the limits are taken over all finite extensions $F' \subset F_\infty^{\mathfrak{l}}$, with respect to the norm maps. It is easy to see that U_∞ and $\bar{C}_\infty$ are finitely generated Λ-modules, and that $U_\infty/\bar{C}_\infty$ is a torsion Λ-module (again, see [**dS87**, p. 103]).

The following theorem is a case of the main conjectures for imaginary quadratic fields, as proven by Rubin.

Theorem 3.6 (Rubin). *Suppose that ℓ does not divide the number of roots of unity in K. Let χ be a character of $\mathfrak{g}$. Then the Λ modules $(U_\infty/C_\infty)^\chi$ and X_∞^χ are both torsion and have the same characteristic ideal.*

Proof. The fact that the modules in question are torsion was already mentioned above. For the equality of the characteristic ideals, we refer to [**Rub94**, Theorem 2 (i)]. Note, however, that the prime p in Rubin's notation corresponds to ℓ in the present situation. □

3.7. The link of Rubin's theorem to the usual statement of the main conjectures comes from the fact that the characteristic ideal of $U_\infty/\bar{C}_\infty$ is known to be generated by a certain ℓ-adic L-function. We now proceed to explain this connection.

Fix an idele class character λ of K, such that $\lambda_\infty : (K \otimes \mathbb{R})^\times \to \mathbb{C}$ satisfies $\lambda_\infty = \iota^2$, where ι is the restriction of a complex place of K. Thus λ has infinity type $(2,0)$. We shall assume further that λ has conductor 1. Such a λ always exists under the hypothesis that $\mathcal{O}_K^\times = \pm 1$ (see [**dS87**, § 1.3, Lemma 1.4 (ii), p. 41]). Then λ defines a character of ideals in K such that $\lambda((\alpha)) = \iota(\alpha)^2$, for a principal ideal (α) of K. Since the class group of K is finite, it is clear that λ takes values in some algebraic extension of K. If we fix an embedding $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_\ell$, and a factor $\mathfrak{l}$ of ℓ in K associated to the given embedding, we can view λ as a Galois character $\lambda_{\mathfrak{l}}$ defined on $\mathrm{Gal}(K_1(\ell^\infty)/K)$, where $K_1(\ell^\infty)$ denotes the compositum of all ray class fields of conductor a power of ℓ. Then we have $\lambda_{\mathfrak{l}}(\mathrm{Frob}(\mathfrak{q})) = \lambda(\mathfrak{q})$ for any prime ideal $\mathfrak{q}$ with $(\mathfrak{q}, \ell) = 1$. Since λ has infinity type $(2,0)$ it follows that in fact $\lambda_{\mathfrak{l}}$ factors through $\mathrm{Gal}(K_1(\mathfrak{l}^\infty)/K)$, where $\mathfrak{l}$ is the prime induced by

$$\iota_{\mathfrak{l}} : K \to \bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_\ell.$$

Then if we identify the inertia group $I_{\mathfrak{l}} \subset \mathrm{Gal}(K_1(\mathfrak{l}^\infty)/K)$ with the image of the local units $U_{\mathfrak{l}}$ via the Artin map, we see that the restriction of $\lambda_{\mathfrak{l}}$ to $U_{\mathfrak{l}}$ is given by $\iota_{\mathfrak{l}}^2$. Since $U_{\mathfrak{l}} \cong (\mathbb{Z}/\ell\mathbb{Z})^\times \times \mathbb{Z}_\ell$ (ℓ is split in K), it follows that $\xi_{\mathfrak{l}} = \lambda_{\mathfrak{l}}^{(\ell-1)/2}$ factors through $\mathrm{Gal}(K_\infty^{\mathfrak{l}}/K)$. We write $\xi = \lambda^{(\ell-1)/2}$ for the complex character corresponding to $\xi_{\mathfrak{l}}$. Then ξ has conductor 1 and infinity type $(\ell-1, 0)$.

Now recall that χ denotes a character of $\mathfrak{g} = \mathrm{Gal}(F/K)$, and that $\mathfrak{g}$ has order prime to ℓ. Then, writing $F_\infty^{\mathfrak{l}}$ for the compositum of F with the $\mathbb{Z}_\ell$-extension $K_\infty^{\mathfrak{l}}/K$ as before, we find that $F_\infty^{\mathfrak{l}}$ is a $\mathbb{Z}_\ell$-extension of F unramified outside $\mathfrak{l}$. Let $\mathcal{G} = \mathrm{Gal}(F_\infty^{\mathfrak{l}}/K) = \mathfrak{g} \times \Gamma$, where $\Gamma \cong \mathbb{Z}_\ell \cong \mathrm{Gal}(K_\infty^{\mathfrak{l}}/K)$. Then we may view the characters of the form $\epsilon_{\mathfrak{l}} = \chi\xi_{\mathfrak{l}}^m$,

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

$m \in \mathbb{Z}$, as characters of $\mathcal{G}$. We will write ϵ for the grossencharacter of K whose $\mathfrak{l}$-adic avatar is $\epsilon_{\mathfrak{l}}$. Note also that the conductor of $\epsilon = \chi\xi^m$ is a power of p, since the original λ was selected to have conductor 1. (But the Galois character $\epsilon_{\mathfrak{l}}$ is of course non-trivial on the inertia group $I_{\mathfrak{l}}$, as is typical with $\mathfrak{l}$-adic representations of Galois groups.)

Our goal is to describe a certain $\mathfrak{l}$-adic L-function associated to the character χ. This L-function is most simply described in terms of a measure on the Galois group $\mathcal{G} = \mathfrak{g} \times \Gamma$, and the integrals of the various characters $\epsilon = \chi\xi^m$. We fix the notation as follows. For each positive integer m, and each character χ of $\mathfrak{g}$, we put

$$\epsilon_{\mathfrak{l}} = \epsilon_{\mathfrak{l}}(\chi, m) = \chi\xi_{\mathfrak{l}}^m = \chi\lambda_{\mathfrak{l}}^{(\ell-1)m/2}.$$

As we have already remarked, each such $\epsilon_{\mathfrak{l}}$ has conductor dividing p^n and has infinity type $(k, 0)$ with $k = (\ell - 1)m > 0$.

With all this notation in mind, the ℓ-adic L-function of interest arises from a measure ϕ on $\mathcal{G}$ satisfying the following formula (see [**dS87**, Theorem 4.12, p. 76], as well as the remarks below):

$$\int_{\mathcal{G}} \epsilon_{\mathfrak{l}} \, \mathrm{d}\phi = G(\epsilon) \cdot (1 - \epsilon(\mathfrak{l})/\ell) \cdot (k-1)! \frac{L^p(\epsilon^{-1}, 0)}{\Omega_\ell^{-k} \Omega_\infty^k}. \tag{3.2}$$

Here $\epsilon_{\mathfrak{l}} = \epsilon_{\mathfrak{l}}(\chi, m)$, and $L^p(\epsilon^{-1}, 0)$ denotes the value of the L-series $\sum_{\mathfrak{a}} \epsilon^{-1}(\mathfrak{a})\mathbb{N}(\mathfrak{a})^{-s}$ at $s = 0$. The sum is taken over ideals $\mathfrak{a} \subset \mathcal{O}_K$ that are relatively prime to p. The numbers Ω_∞ and Ω_ℓ are certain complex and ℓ-adic periods respectively. The number $G(\epsilon)$ is 'the Gauss sum' defined in [**dS87**, p. 75]. Note that $G(\epsilon)$ has complex absolute value equal to $\ell^{n(\epsilon)(k-1)}$, where $n(\epsilon)$ is the exact power of $\mathfrak{l}$ dividing the conductor of ϵ. Furthermore, if $\epsilon = \chi\xi^m$ with χ a character of $\mathfrak{g}$ as above, then $G(\epsilon) = 1$, since ϵ has conductor prime to $\mathfrak{l}$ [**dS87**, Remark (i), p. 75].

Remark 3.8. There is a small misprint in [**dS87**, Theorem 4.12]. The quantity written there as $L_{\infty,\mathfrak{f}}(\epsilon^{-1}, 0)$ should be replaced by

$$(k-1)! L_{\mathfrak{f}}(\epsilon^{-1}, 0) = (2\pi)^k L_{\infty,\mathfrak{f}}(\epsilon^{-1}, 0).$$

Indeed, according to [**dS87**, p. 37], the Euler factor at infinity in $L_{\infty,\mathfrak{f}}(\epsilon^{-1}, s)$ is given by $\Gamma(s+k)/(2\pi^{s+k})$, so that the right-hand side of formula (31) is not even algebraic. I am informed by de Shalit that the extra powers of π were inadvertently absorbed into the period, and that the same error occurs in Theorem 4.14 (p. 80). An accurate formula may be found in Theorem 4.11 (p. 74), which deals with a slightly different situation, or in [**Yag82**, p. 411].

Remark 3.9. We point out also that the measure constructed in [**dS87**] is defined on Galois groups of the form $\mathrm{Gal}(K_1(p^r\mathfrak{l}^\infty)/K)$, where $K_1(p^r\mathfrak{l}^\infty)$ denotes the compositum of the ray class fields $K_1(p^r\mathfrak{l}^t)$, as t tends to infinity. Taking $r = n$ (where $F = F_n$ is our fixed base field) we see that $F_\infty^{\mathfrak{l}} \subset K_1(p^n\mathfrak{l}^\infty)$, and that the characters $\epsilon(\chi, m)$ factor through $\mathcal{G} = \mathrm{Gal}(F_\infty^{\mathfrak{l}}/K)$. Thus de Shalit's measure descends to $\mathcal{G}$ via the natural projection $\mathrm{Gal}(K_1(p^n\mathfrak{l}^\infty)/K) \to \mathcal{G}$.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Remark 3.10. The measure we have defined is imprimitive at p in the sense that it interpolates L-series deprived of the Euler factor at p. This defect is vacuous unless χ is one of the finitely many characters factoring through the Hilbert class field. We are forced to work over the base field F_n for $n \geqslant 1$ by virtue of the fact that the construction of the measures in [**dS87**, Theorem 4.12] requires $\mathfrak{f}$ to be a non-trivial idea, so dealing with characters that are everywhere unramified causes some annoying technicalities. In this paper we are only concerned with results pertaining to almost all χ, so it will be convenient to discard the finitely many unramified χ, thereby avoiding irrelevant complications.

Thus, for each character χ of $\mathfrak{g}$, we deduce that there exists a measure ϕ_χ on Γ such that

$$\int_\Gamma \xi^m \, \mathrm{d}\phi_\chi = (1 - \chi\xi^m(\mathfrak{l})/\ell)(k-1)! \frac{L^p(\chi^{-1}\xi^{-m}, 0)}{\Omega_\ell^{-k}\Omega_\infty^k}. \tag{3.3}$$

Here $k = (\ell - 1)m$ and $m \geqslant 1$. Since $\Gamma \cong \mathbb{Z}_\ell$, we may identify the measure ϕ_χ with a power series $f_\chi \in \mathfrak{o}[\![T]\!]$. The power series f_χ is characterized by $f_\chi(u^m - 1) = \int_\Gamma \xi^m \, \mathrm{d}\phi$, where $u = \xi(\gamma)$, for a fixed topological generator γ of Γ. Note also that formula (3.3) implies that f_χ depends only on χ, but not on the base field $F = F_n$, at least if $n \geqslant 1$.

The following theorem is basically due to Coates and Wiles. Recall that χ is a character of p-power conductor. For technical reasons in the statement, we will exclude the finitely many characters that factor through the Hilbert class field.

Theorem 3.11. *Suppose that χ has conductor divisible by p. Then the characteristic ideal of $(U_\infty/\bar{C}_\infty)^\chi$ is generated by f_χ.*

Proof. This may be found in [**dS87**, Lemma 1.10, p. 105]. Note, however, that de Shalit frames his result in terms of a ray class field $K_1(p^n)$; that everything descends to the subfield $F = F_n$ is a trivial verification, using the fact that the elliptic units in F are norms of those in the ray class field. Note also that we have insisted that χ be ramified at p in order to be consistent with our definition of the p-adic L-function above, which is imprimitive at p if χ is unramified. □

Rubin's theorem may therefore be restated as follows.

Corollary 3.12. *Suppose the conductor of χ is divisible by p. Then the characteristic ideal of X_∞^χ is generated by the p-adic L-function $f_\chi(T)$.*

With all this in mind, we can now approach the key results in this section, which state that the power series f_χ are almost always units. This is a consequence of a theorem due to Hida. Together with the main conjecture due to Rubin, we obtain the fact that the modules X_∞^χ are almost always trivial. Thus, recall that $F_\infty = \cup F_n \subset K(p^\infty)$ is contained in the p-anti-cyclotomic tower, and put $\mathfrak{g}_\infty = \mathrm{Gal}(F_\infty/K)$. Then we have the recently announced theorem of Hida.

Theorem 3.13 (Theorem 1.1 of [Hid03]). *Let ξ denote a grossencharacter of K with conductor* 1, *and with infinity type $(k, 0)$ for some $k > 0$. Let p denote an odd*

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

prime number. If $\ell \neq p$ is an odd prime which splits in K, then, for all but finitely many anti-cyclotomic characters χ of p-power conductor, the number

$$\Gamma(k)\frac{L^p(\chi^{-1}\xi^{-1},0)}{\Omega_\infty^k} = (k-1)!\frac{L^p(\chi^{-1}\xi^{-1},0)}{\Omega_\infty^k}$$

is algebraic and an ℓ-adic unit, for a fixed embedding $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_\ell$. Here $\Gamma(s)$ denotes the Gamma function and L^p denotes the L-series deprived of the Euler factors at p.

Remark 3.14. For the convenience of the reader, we translate Theorem 1.1 of [**Hid03**] into the notation used here. First of all, note that the case of imaginary quadratic fields is indeed included in Hida's results, since the class number of $\mathbb{Q}$ is one (and so $\mathbb{Q}$ cannot satisfy his condition M1). Note also that Hida's ℓ corresponds to our p, and vice versa. Finally, characters of infinity type (r,s) in Hida correspond to infinity types $(-r,-s)$ in this paper and in [**dS87**]. To get the formula given above, observe that $\chi^{-1}\xi^{-1}$ has infinity type $(k,0)$ in Hida's notation, so the formula above is the same as his, with $F = \mathbb{Q}$ and $\kappa = 0$.

Remark 3.15. We would also like to point out here that the paper [**Hid03**] is still in preprint form at the time of writing. While we have tried to ensure that the references to this work are accurate, the reader should always consult the latest version of the manuscript available from Hida's web page.

Our key result may now be stated as follows.

Theorem 3.16. *Let χ run over the set of finite-order characters of $\mathfrak{g}_\infty$. Then, for all but finitely many χ, the power series f_χ is invertible in $\mathfrak{o}[\![T]\!]$.*

Proof. Put $\epsilon = \chi\xi$. Then it suffices to show that

$$f_\chi(u-1) = G(\epsilon)(1-\epsilon(\mathfrak{l})/\ell)(\ell-2)!\frac{L^p(\epsilon^{-1},0)}{\Omega_\ell^{-(\ell-1)}\Omega_\infty^{(\ell-1)}}$$

is an ℓ-adic unit, for all but finitely many χ. Note first of all that the ℓ-adic period Ω_ℓ and the number $G(\epsilon)$ are both units (see [**dS87**, p. 75], both for the definition of the period Ω_ℓ, and a discussion of the Gauss sum; in fact $G(\epsilon) = 1$ under our hypotheses). In view of Hida's theorem above (with $k = \ell - 1$), it suffices to show that the Euler factor at ℓ is an ℓ-adic unit. But this is given explicitly by

$$(1-\epsilon(\mathfrak{l})/\ell) = (1-\chi\xi(\mathfrak{l})/\ell) = (1-\chi(\mathfrak{l})\cdot\xi(\bar{\mathfrak{l}})^{-1}\ell^{\ell-2}),$$

since $\mathfrak{l}\bar{\mathfrak{l}} = \ell$, and $\xi(\ell) = \ell^{\ell-1}$. But now $\xi(\bar{\mathfrak{l}})$ is an $\mathfrak{l}$-adic unit, as follows easily from the facts that $\mathfrak{l}$ is the prime over ℓ singled out by our fixed embedding $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_\ell$, and $\epsilon(\bar{\mathfrak{l}})$ is divisible only by primes above $\bar{\mathfrak{l}}$ (finiteness of the class number). So the Euler factor is a unit as well. □

In order to state the next result, which puts everything together, we recall our various notations.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

(i) χ is any finite order character of $\mathfrak{g}_\infty$, as in the theorem above.

(ii) $n \geqslant 1$ is any integer such that χ factors through $\mathfrak{g} = \mathfrak{g}_n = \mathrm{Gal}(F/K)$ where $F = F_n$. The character χ is the primary object, and we simply choose such an n, depending on χ.

(iii) A_n^χ is the χ-component of the ideal class group of $F = F_n$.

(iv) $F_\infty = \cup F_n$, and $A_\infty = \lim A_n = \mathrm{Gal}(M_\infty/F_\infty)$, where M_∞ is the maximal unramified abelian pro-ℓ extension of F_∞

(v) $F_\infty^{\mathfrak{l}}$ is the unique $\mathbb{Z}_\ell$-extension of F unramified outside primes above $\mathfrak{l}$. This depends on the choice of n.

(vi) $X_\infty = \mathrm{Gal}(N_\infty^{\mathfrak{l}}/F_\infty^{\mathfrak{l}})$, where $N_\infty^{\mathfrak{l}}$ denotes the maximal abelian pro-ℓ extension of $F_\infty^{\mathfrak{l}}$ that is unramified outside primes above $\mathfrak{l}$.

(vii) X_∞^χ is the χ-component of X_∞.

According to Lemmas 3.2 and 3.5, the groups A_∞^χ and X_∞^χ depend only on χ and not on the choice of base field F. We have $A_\infty^\chi = A_n^\chi$ for any choice of n sufficiently large.

Corollary 3.17. *We have $A_\infty^\chi = X_\infty^\chi = 0$ for all but finitely many characters χ of $\mathfrak{g}_\infty$. For all but finitely many χ, we have $A_n^\chi = 0$ for all $n \gg 0$.*

Proof. Without loss of generality, we may exclude the finitely many characters that factor through the Hilbert class field. Then the statement about X_∞^χ follows from the main conjecture. Indeed, the module $(U_\infty/\bar{C}_\infty)^\chi$ is annihilated by f_χ, and the latter is a unit for almost all χ. Thus $(U_\infty/\bar{C}_\infty)^\chi$ is pseudo-null for almost all χ, and by Rubin's theorem, the same is true for X_∞^χ. But Greenberg has shown (see [**Gre78**, end of § 4]) that X_∞ has no non-zero finite Λ-submodule, so that X_∞^χ is zero for almost all χ.

As for A_∞^χ, we know already that $A_\infty^\chi = A_n^\chi$ if n is sufficiently large. So suppose that $A_\infty^\chi = A_n^\chi$ is non-trivial for some choice of n. Let $\chi' = \prod \chi^\sigma$, where χ^σ runs over the conjugates of χ over $\mathbb{Z}_\ell$. Then χ' is an irreducible $\mathbb{Z}_\ell$-representation, and $A_n^{\chi'} \neq 0$. Thus there exists an unramified extension F'/F (here $F = F_n$) with $\mathrm{Gal}(F'/F)$ a finite ℓ-group, such that $\mathrm{Gal}(F/K)$ acts on $\mathrm{Gal}(F'/F)$ via χ'. If $\chi \neq 1$, then $\chi' \neq 1$ as well, so that F' is linearly disjoint from $F_\infty^{\mathfrak{l}}$ over F. Indeed, $F_\infty^{\mathfrak{l}} = FK_\infty^{\mathfrak{l}}$ is abelian over K, so that $\mathrm{Gal}(F_\infty^{\mathfrak{l}}/F)$ is trivial for the action of $\mathfrak{g} = \mathrm{Gal}(F/K)$. Thus $F' \cdot F_\infty^{\mathfrak{l}}$ would be a non-trivial unramified extension of $F_\infty^{\mathfrak{l}}$ contained in $N_\infty^{\mathfrak{l}}$. Since the χ-part of $X_\infty = \mathrm{Gal}(N_\infty^{\mathfrak{l}}/F_\infty^{\mathfrak{l}})$ is zero for almost all χ, the statement about A_∞^χ follows. The last statement results from the fact that $A_n^\chi = A_\infty^\chi$ for all n sufficiently large. □

3.18. We can now transfer everything back to the full ring class field $H_n = K(p^n)$. Thus recall that $F_n \subset H_n$ is the maximal subfield of H_n of degree prime to ℓ. Then $G_n = \mathrm{Gal}(H_n/K) = \Delta \times \mathfrak{g}_n$, where $\mathfrak{g} = \mathfrak{g}_n = \mathrm{Gal}(F_n/K)$ and Δ is an ℓ-group (independent of n). Observe also that H_n/F_n is everywhere unramified, as the degree of H_n/F_n is a power of ℓ. Indeed, only primes above p are ramified in H_n/K, and the ramification index of such primes in H_n is a divisor of $(p \pm 1)p^{n-1}$, which by our hypotheses is prime to ℓ.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Let B_n denote the ℓ-Sylow subgroup of the ideal class group of H_n, and let B_n^χ denote the χ-component, for any character χ of $\mathfrak{g}_n$. Here $\mathfrak{g}_n$ is viewed as a subgroup of G_n. Given a character χ of $\mathfrak{g}_n$, we may as before view it as a character of $\mathfrak{g}_m \subset G_m$, for $m \geqslant n$. Thus we can form the χ component B_m^χ for all $m \geqslant n$. Let B_∞^χ denote the direct limit of the groups B_m^χ, for $m \geqslant n$. Then we claim that B_∞^χ is finite for all χ, and that $B_\infty^\chi = 0$ for all but finitely many χ.

The first of these statements follows from the fact that $B_n^\chi = B_m^\chi$, for $m \geqslant n$, as in Lemma 3.2, since H_m/H_n has degree prime to ℓ. The second follows from the analogous statement for A_∞^χ, but we have to argue carefully, since H_n/F_n may have degree divisible by ℓ.

Thus suppose that B_∞^χ is non-trivial for some χ. Then B_n^χ is non-trivial for some n. Then, defining χ' as in the proof of Lemmas 3.2 and 3.5, we find that there exists an extension H'/H (here put $H = H_n$ and $F = F_n$), such that $\mathrm{Gal}(H'/H)$ is a finite ℓ-group, and such that $\mathfrak{g} = \mathrm{Gal}(F/K)$ acts via the representation χ'. Since Δ is a finite ℓ-group, it follows that there exists a non-trivial quotient of $\mathrm{Gal}(H'/H)$ on which the action of Δ is trivial, and $\mathfrak{g}$ acts via χ'. Let L'/H be the corresponding extension. Then L' is abelian over F, since the action of Δ is trivial. Since H/F is unramified, we see that L'/F is in fact an abelian unramified ℓ-extension. Since $\mathrm{Gal}(F/K)$ acts on the subgroup $\mathrm{Gal}(L'/H) \subset \mathrm{Gal}(L'/F)$ via χ', we find that there is a non-trivial unramified abelian ℓ-extension of F on which the action of $\mathrm{Gal}(F/K)$ is given by χ. But as we have already seen, this can only happen for finitely many χ.

We may summarize these considerations in the following proposition. Let the hypotheses on ℓ and p be as above. Let H_n denote the ring class field of conductor p^n, and let H_n^{un} denote the maximal unramified abelian ℓ-extension of H_n. We put $H_\infty = \bigcup H_n$, and let $H_\infty^{\mathrm{un}} = \bigcup H_n^{\mathrm{un}}$ denote the maximal unramified ℓ-extension of H_∞.

Proposition 3.19. *The extension $H_\infty^{\mathrm{un}}/H_\infty$ is finite. Furthermore, there exists an m such that $H_n^{\mathrm{un}} = H_m^{\mathrm{un}} \cdot H_n$, if $n \geqslant m$.*

For our purposes, it is necessary to have a slightly more general result, where we allow ramification at a finite set of split primes.

Theorem 3.20. *Let Σ denote a finite set of primes of K. Assume that all primes in Σ are split in K, and that Σ does not contain any prime of residue characteristic ℓ. Let M_∞^Σ denote the maximal abelian pro-ℓ extension of H_∞, unramified outside primes in Σ. Then $X_\infty^\Sigma = \mathrm{Gal}(M_\infty^\Sigma/H_\infty)$ has finite ℓ-rank.*

Proof. The maximal *everywhere* unramified pro-ℓ extension of H_∞ is finite, according to the proposition above. Now let $\mathfrak{q}$ denote any prime in Σ. Then $\mathfrak{q}$ is finitely decomposed in H_∞, since H_∞/K is anti-cyclotomic, and $\mathfrak{q}$ is assumed to be split in K. Let $\mathfrak{q}'$ denote any factor of $\mathfrak{q}$ in H_∞. Let M_n^Σ denote the maximal abelian pro-ℓ extension of H_n, unramified outside primes in from Σ, and let $X_n^\Sigma = \mathrm{Gal}(M_n^\Sigma/H_n)$. Then since $\mathfrak{q}'$ has residue characteristic distinct from ℓ by hypothesis, we see that $\mathfrak{q}'$ is *tamely* ramified in M_n^Σ/H_n. Thus the inertia group $I_{n,\mathfrak{q}'}$ at $\mathfrak{q}'$ in X_n^Σ is the image under the reciprocity map of the roots of unity in the completion of H_n at $\mathfrak{q}'$, and this is a cyclic group. Since

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

this holds for every $n \geqslant 0$, it follows that the inertia group of $\mathfrak{q}'$ in X_∞^Σ is the surjective image of the ℓ-power roots of unity in the completion of H_∞ at $\mathfrak{q}'$, which is a pro-cyclic group. Thus each factor $\mathfrak{q}'$ contributes ℓ-rank at most 1, and since there are only finitely many factors of $\mathfrak{q}$ for each $\mathfrak{q} \in \Sigma$, and only finitely many primes in Σ, the statement of the theorem follows. □

The following corollary is an immediate consequence of the theorem.

Corollary 3.21. *Let Σ be as above, and let $r \geqslant 1$ be an integer. For each $n \geqslant 0$, let L_n denote the composite of all abelian extensions of H_n that are of degree dividing ℓ^r and unramified outside Σ. Then there exists an m such that $L_n = L_m \cdot H_n$, for $n \geqslant m$.*

4. The Shimura subgroup

4.1. We can now prove that the Shimura subgroup is maximal. The basic ingredient is a theorem of Ihara. To explain this, we need to introduce various models for the complex curves $\Gamma \setminus \mathcal{H}^*$, where $\Gamma = \Gamma_1(N)$ or $\Gamma_0(N)$, and $\mathcal{H}^*$ denotes the union of the upper half plane and the rational cusps.

Let $S = \mathrm{Spec}(\mathbb{Z}[1/N])$, and let $X_0(N)_S$ denote the coarse moduli space whose R-valued points classify cyclic N-isogenies $E \to E'$ of generalized elliptic curves over R, for any S-scheme R. Similarly, let $X_1(N)_S$ denote the moduli space classifying embeddings $\mu_N \to E$. Note that this variant of $X_1(N)$ is usually written as $X_1(N)^{\mathrm{arith}}$; we will not need to concern ourselves with other models here. The schemes $X_0(N)$ and $X_1(N)$ are smooth and proper over S, and every geometric fibre is a smooth and connected curve.

Let V denote the Shimura subgroup of $J_0(N)(\bar{\mathbb{Q}})$, as defined in the introduction. Our goal is to prove that V is in some sense the maximal multiplicative-type subgroup of $J_0(N)$, at least under some hypotheses. Let $J_0(N)/V$ denote the image of $J_0(N)$ in $J_1(N)$. Then there is an isogeny $J_V = (J_0(N)/V)^{\mathrm{dual}} \to J_0(N)$, whose kernel is the Cartier dual V^* of V. If we embed $X_0(N)$ into its Jacobian by sending the cusp 0 to the origin, then pullback of $J_V \to J_0(N)$ yields a Galois cover $X_V \to X_0(N)$ of curves over $\mathbb{Q}$, with structural group V^*. Then, by definition, the pullback of X_V to $X_1(N)$ via the projection $\pi : X_1(N) \to X_0(N)$ is trivial in the sense that it is isomorphic to a disjoint union of copies of $X_1(N)$. We want to show that in fact this is true for *all* Galois covers of $X_0(N)$ (over $\mathbb{Q}$). While we cannot prove this completely, we can still offer Theorem 1.1 of § 1. For the convenience of the reader, we repeat the statement here.

Theorem 4.2. *Let W denote any finite $\mathbb{Q}$-rational subgroup of $J_0(N)(\bar{\mathbb{Q}})$ such that $W \cong \mu_n$ for some odd integer n, and such that $J_0(N)$ has semi-stable reduction at ℓ for each prime ℓ dividing n. Then W is contained in the Shimura subgroup.*

4.3. To prove the theorem, it suffices to show that the pullback $\pi^*(X_W) \to X_1(N)$ is isomorphic to a finite union of copies of $X_1(N)$. The basic criterion for the triviality of such covers is given by a theorem of Ihara, which we now proceed to explain.

Let q denote a prime with $(N, q) = 1$. Then the non-cuspidal points on $X_0(N)(\bar{\mathbb{F}}_q)$ classify isomorphism classes of cyclic N-isogenies $E \to E'$, with E and E' elliptic curves in characteristic q. A point $x \in X_0(N)(\bar{\mathbb{F}}_q)$ is called *super-singular* if the curves E and

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

E' are super-singular. It is well known that all super-singular points are rational over the field $\mathbb{F}_{q^2}$ with q^2 elements.

Now consider a degree d cover $f : X_q \to X_0(N)$ defined over $\mathbb{F}_q$, where X_q is a smooth and geometrically irreducible curve. A super-singular point $x \in X_0(N)(\mathbb{F}_{q^2})$ is said to split completely in X_q if the fibre of f over x in X_q consists of d distinct points, each rational over $\mathbb{F}_{q^2}$.

Theorem 4.4 (Ihara). *Let $X_q \to X_0(N)$ be an unramified cover over $\mathbb{F}_q$, where X_q is a smooth and absolutely irreducible curve. Suppose that every super-singular point in $X_0(N)$ splits completely. Then $\pi^*(X_q)$ is trivial as a cover of $X_1(N)$.*

Proof. See [**Iha75**, **Rib84**]. A further discussion may also be found in [**Pra95**]. □

4.5. As we have already remarked in § 1, we want to reduce the characteristic zero cover $X_W \to X_0(N)$ to characteristic q, and then apply Ihara's theorem. However, we need to explain what is mean by the reduction, and why triviality of the cover in characteristic q implies triviality of the one in characteristic zero. One way to do this would be to extend the curve X_W to a curve over $\mathbb{Z}_q$, and consider coverings of curves over $\mathbb{Z}_q$, but in practice this is somewhat technical. Instead we shall simplify matters considerably by working with the Jacobians and their Néron models rather than integral models of curves.

To explain this, recall that our cover $X_W \to X_0(N)$ (over $\mathbb{Q}$) is associated by definition to a finite subgroup $W \subset J_0(N)$. Now, if q is any odd prime such that $q \nmid N$, then the Jacobian $J_0(N)$ admits a Néron model $J_0(N)_R$ over $R = \mathbb{Z}_q$ which is an abelian scheme, and the scheme-theoretic closure W_R of W is a finite flat subgroup of $J_0(N)_R$. Writing s for the closed point of R, we deduce that W_s is a finite subgroup of the special fibre $J_0(N)_s$, of order equal to that of W. Similarly, the Shimura subgroup V extends to a finite flat subgroup $V_R \subset J_R$, and by functoriality of the Jacobian (equal to Pic^0 in this setting), the special fibre V_s is precisely the kernel of $J_0(N)_{\mathbb{F}_q} \to J_1(N)_{\mathbb{F}_q}$. To show that $W \subset V$, it suffices to show that $W_s \subset V_s$, since W_R and V_R are both finite flat subgroups of $J_0(N)_R$. Thus if we *define* $X_{W,s}$ to be the cover of $X_0(N)_s = X_0(N)_{\mathbb{F}_q}$ associated to the subgroup $W_s \subset J_0(N)_s$, then it suffices for our purposes to show that $X_{W,s}$ becomes trivial over $X_1(N)_{\mathbb{F}_q}$. Note here that is *not* clear *a priori* that $X_{W,s}$ is related to the special fibre of an integral model of X_W. However, it does follow from functoriality of the Jacobian that the $\mathbb{Q}$-isogeny $J_W \to J_0(N)$ extends to an isogeny of Néron models whose special fibre is precisely the map $J_{W,s} \to J_0(N)_s$ whose pullback gives the cover $X_{W,s} \to X_0(N)_s$. This implies in particular that if T is a scheme over R, and x is a T-valued point of $X_0(N)_R$, then the fibre in $X_{W,s}$ of $x_s \in X_0(N)(T_s)$ is canonically identified with the corresponding fibre in $J_{W,s} \to J_0(N)_s$. Thus, if x_W denotes the fibre over x in the isogeny $J_{W,R} \to J_0(N)_R$, then $x_s = x_{W,s}$ is the special fibre of x_W. Note here that we have avoided any mention of an integral model of X_W, or of Galois coverings of relative curves. This is possible since we are only interested in the fibres of such a cover, and these would be canonically identified with the corresponding fibres of the isogenies in question. In particular, we need not concern ourselves with the precise integral model for X_W, nor the relation between $X_{W,s}$, as defined above, with the special fibre of the integral model.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

We can now prove Theorem 1.1. We keep the notations introduced in the statement and in the discussion above.

4.6. Without loss of generality, we may assume that W has order ℓ^r, where ℓ is an odd prime, and that X is isomorphic to μ_{ℓ^r} as a Galois module. We show that the pullback $X'_W = \pi^*(X_W) \to X_1(N)$ is trivial. Letting $X_{W,q} = X_{W,s}$ denote the 'reduction' of X_W as defined above, it is even enough to show that $X'_{W,q} = \pi^*(X_{W,q})$ is the trivial cover of $X_1(N)_{\mathbb{F}_q}$. As we have mentioned, the main point will be to choose q in such a way as to make Ihara's criterion applicable. We shall achieve this by lifting the super-singular points to CM points in characteristic 0, and controlling the fibres over the CM points by limiting the ramification with the help of Corollary 2.7.

We choose an imaginary quadratic field K of discriminant D such that all primes dividing $N\ell$ are split in K, and such that the roots of unity in K are ± 1. We further choose an odd prime $p \nmid ND\ell$ such that K, p and ℓ satisfy the conditions set out in § 3.1. Then we consider the ring class fields H_n of conductor p^n, and the compositum $H_\infty = \cup H_n$. We will use the notations of § 3 for the ring of integers and Picard groups of the fields H_n. Since all primes dividing N are split in K, we can choose an ideal $\mathfrak{n}$ of K such that $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. Assume that such an $\mathfrak{n}$ is fixed.

Now let C_n denote the set of pairs $(A, \mathfrak{n})$ where A is an elliptic curve with CM by K such that $\mathrm{End}(A) = \mathcal{O}_n$ is the order of conductor p^n. Then $\#C_n = \#G_n$, where $G_n = \mathrm{Pic}(\mathcal{O}_n) \cong \mathrm{Gal}(H_n/K)$. Each pair $(A, \mathfrak{n})$ defines a point $x \in X_0(N)(H_n)$. We want to consider the reduction of x at inert primes of K.

Thus let $q \neq p$ denote any rational prime which remains prime in K (so $q \nmid N\ell$). Then q splits completely in every field H_n. We fix a prime $\mathfrak{q}$ of H_∞ lying over q. Let $S_q(N)$ denote the set of super-singular points on $X_0(N)(\mathbb{F}_{q^2})$. According to [**Vat03**, § 6], there is a reduction mod $\mathfrak{q}$ map

$$r : C_n \to S_q(N),$$

which is surjective for n sufficiently large (depending of course on $\mathfrak{q}$). For another viewpoint on the reduction map, the reader may consult [**Cor02**].

Put $M = N$ if $(N, \ell) = 1$, and $M = N/\ell$ if not. Since ℓ is assumed to be a prime of semi-stable reduction, we have $(M, \ell) = 1$. Let L_n denote the maximal abelian extension of H_n of exponent dividing ℓ^r which is unramified at all primes outside M. Then L_n/H_n is finite, and by Corollary 2.7, we have an m such that $L_n = L_m \cdot H_n$ if $n \geqslant m$. It is clear that L_m is Galois over $\mathbb{Q}$. Let ι denote any embedding of L_m into the complex numbers, and let $c \in \mathrm{Gal}(L_m/\mathbb{Q})$ denote the action of complex conjugation. Note that c induces the non-trivial automorphism of $K/\mathbb{Q}$, and so is non-trivial. We take q to be any prime of K such that $q \nmid ND\ell p$, such that $\mathrm{Frob}(q) = c \in \mathrm{Gal}(L_m/\mathbb{Q})$. Then q is inert in K, and q splits completely in $\mathrm{Gal}(L_m/K)$.

Now choose n sufficiently large that the reduction map $C_n \to S_q(N)$ is surjective. Let $P \in C_n$, so that $P \in X_0(N)(H_n) \subset J_0(N)(H_n)$. Then we consider a point P' lying in the fibre of the cover $X_W \to X_0(N)$ over P. (Note that this fibre is unchanged if we consider P to be a point of $J_0(N)$ instead.) It follows from Corollary 2.7 that P' is rational over an extension H'/H_n of degree dividing ℓ^r, where H' is unramified outside

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

the primes dividing M. Here, as before, M denotes N if $(\ell, N) = 1$, and $M = N/\ell$ if not. Thus $H' \subset L_n = L_m \cdot H_n$, by our choice of m. Since q is inert in K, we see that q splits completely in the anti-cyclotomic field H_n. On the other hand, our choice of q implies that q has degree two in $L_m/\mathbb{Q}$. Thus we see that q has degree two in L_n. It follows that every point in the fibre of $X_{W,q} \to X_0(N)_{\mathbb{F}_q}$ over $r(P) \in S_q(N) \subset X_0(N)_{\mathbb{F}_{q^2}}$ is rational over $\mathbb{F}_{q^2}$, for each $P \in C_n$. Since n was chosen so that the reduction map is surjective, we find that all super-singular points split completely in $X_{W,q} \to X_0(N)_{\mathbb{F}_q}$. It follows now from Ihara's theorem that the cover $X'_{W,q} \to X_1(N)$ is trivial, as required.

5. Stevens's conjecture

In this section we will prove Theorems 1.10, 1.11 and 1.16. We will keep the notation of § 1. Thus $\mathcal{C}$ denotes a fixed isogeny class of elliptic curves over $\mathbb{Q}$ of conductor N. We will write E^* for the curve of minimal height in $\mathcal{C}$, and E_0 and E_1 for the strong Weil curves in $\mathcal{C}$ for $X_0(N)$ and $X_1(N)$, respectively.

5.1. Let $E \in \mathcal{C}$, and let ℓ denote an odd prime. Then E admits a cyclic ℓ-isogeny over $\mathbb{Q}$ if and only if $E[\ell]$ is reducible as a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module. By the work of Mazur [**Maz78**], the list of all possible ℓ is known. Thanks to the further work of Kenku [**Ken82**], we even have a list of all integers M such that there is an elliptic curve over $\mathbb{Q}$ admitting a cyclic isogeny of degree M.

We shall say that the isogeny class $\mathcal{C}$ is *sporadic* if there exists $E \in \mathcal{C}$ such that E admits a cyclic M-isogeny for some M such that the genus of $X_0(M)$ is positive. There are only finitely many sporadic isogeny classes (up to twist), and the j-invariants of the curves in these classes are known (see [**BK75**, p. 79]). Furthermore, one can even write specific curves exhibiting these M-isogenies. This observation will be helpful in what follows (cf. Remark 1.12).

We begin with a series of preliminaries.

Lemma 5.2. *Suppose that $E_{\mathbb{Q}}$ is a semi-stable elliptic curve, and that ℓ is an odd prime such that $E[\ell]$ is reducible as a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module. Then $E[\ell]$ has composition factors isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ. Furthermore, E has ordinary reduction at ℓ.*

Proof. See Proposition 21 and the subsequent Lemma 5 in [**Ser72**, p. 307]. □

The following result is key.

Proposition 5.3. *Let $E_0 \subset J_0(N)$ be the strong Weil curve. Suppose that $E_0[\ell]$ is reducible as a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module, and that E_0 is ordinary at ℓ. Then the following hold.*

(1) *$\ell^2 \nmid N$, for the conductor N.*

(2) *There exists an $E' \in \mathcal{C}$ such that there is an étale isogeny $E_0 \to E'$ of degree ℓ.*

Proof. Let f denote the newform on $\Gamma_0(N)$ associated to E by the Shimura–Taniyama correspondence. Then the ℓth coefficient of the Fourier expansion of f is non-zero, since f is ordinary at ℓ and f is of weight 2. It now follows from [**Miy89**, Theorem 4.6.17] that,

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

if ℓ^r is the exact power of r that divides the level N, then either f has nebentype character with conductor divisible by ℓ^r, or $r \leqslant 1$. Since f has trivial nebentype character, we see that $\ell^2 \nmid N$.

As for the second assertion, observe that ordinariness of E_0 implies that $E_0[\ell]$ has composition factors C and D of order ℓ, where the action of $G_{\mathbb{Q}}$ is given by characters χ and $\chi^{-1}\omega$, respectively, for the Teichmüller character ω and a character χ unramified at ℓ. (Note that $\chi = 1$ if E_0 is semi-stable.) It suffices to show that there is an exact sequence $0 \to C \to E_0[\ell] \to D \to 0$, since C is unramified as a module for the decomposition group D_ℓ and E_0 is semi-stable at ℓ. Indeed, the quotient map $E_0 \to E_0/C$ is étale, as is easy to see (see Lemma 2.2). To construct such a subgroup C, we follow the procedure of [**Ste82**, **Vat99**]. The basic idea is to use an Eisenstein series to produce a subgroup of the cuspidal group, and use a multiplicity one theorem to ensure that this subgroup is contained in E_0. (In this context, the idea goes back to [**Tan97**].)

Let the Fourier expansion of the newform f corresponding to E_0 be given by $f(z) = \sum a_n q^n$. Then one can retrieve the numbers $a_n \pmod{\ell}$ from the Galois module $E_0[\ell]$ as follows. Since f is an eigenform, it suffices to determine a_q, as q runs over all primes. Since $E[\ell]$ is given up to semi-simplification by $\chi \oplus \chi^{-1}\omega$, we get the following.

(i) If $q \nmid N\ell$, then $a_q \equiv \chi(q) + q\chi(q)^{-1} \pmod{\ell}$.

(ii) If $q = \ell$, then $a_q = \chi(q) \pmod{\ell}$, since E_0 is ordinary.

(iii) Finally, if $q \neq \ell$ is such that $q \mid N$, then $a_q = 0$ if $q^2 \mid N$. If q exactly divides N, then either $a_q = \chi(q) \pmod{\ell}$ or $a_q = q/\chi(q) \pmod{\ell}$.

To proceed further, it will be convenient to lift the $\mathbb{F}_\ell$-valued character χ to characteristic zero via the Teichmüller lift. Then χ takes values in the group $\mu_{\ell-1} \subset \mathbb{Z}_\ell^\times$. Picking an embedding $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_\ell$, we may therefore regard χ as taking values in $\bar{\mathbb{Q}}$. Furthermore, the choice of embedding $\bar{\mathbb{Q}} \subset \bar{\mathbb{Q}}_\ell$ determines a prime $\lambda \mid \ell$ of $\bar{\mathbb{Q}}$. Finally, we also pick an embedding $\bar{\mathbb{Q}} \subset \mathbb{C}$.

We now contend that, under the hypotheses of the proposition, there is a holomorphic Eisenstein series $g = \sum b_n q^n$, $b_n \in \mathbb{Q}(\chi)$, on $\Gamma_0(N)$ such that the following hold.

(1) $a_n \equiv b_n \pmod{\lambda}$, for every $n \geqslant 1$.

(2) The constant term of g at every cusp is divisible by λ.

The proof of this is not hard, and follows the lines of similar arguments in [**Vat99**, **GV00**]. However, there are a number of cases to consider, making the argument somewhat lengthy. Note here that we are viewing the coefficients $b_n \in \bar{\mathbb{Q}}$ as complex numbers according to the embedding fixed above.

To prove the contention, it will be convenient first to separate cases depending on whether or not χ is trivial, starting with the latter. Then if M denotes the conductor of χ, we have $M^2 \mid N$, and there is a holomorphic Eisenstein series g' of weight two on $\Gamma_0(M^2)$ such that the L-series $L(g', s)$ is given by $L(g', s) = L(\chi, s)L(\chi^{-1}, s-1)$. For a prime q, the Euler factor at q of $L(g', s)$ is given by the inverse of $(1 - \chi(q)q^{-s})(1 - \chi^{-1}(q)q^{1-s})$.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Stripping away Euler factors from g' as in the proof of Proposition 3.4 in [**Shi78**], we can produce a Eisenstein series $g(z)$ of weight 2 and level N, satisfying the first of the stated conditions. Explicitly, one can take $g(z) = \sum b_n q^n$ to be such that

$$L(g, s) = L_{N_1}(\chi, s) \cdot L_{N_2}(\chi^{-1}, s - 1),$$

is the product of *imprimitive* L-series. Here $L_{N_i}(\xi, s)$ denotes the Dirichlet L-function of the Dirichlet character $\xi = \chi$ or $\xi = \chi^{-1}$, deprived of the Euler factors at primes dividing N_i. (For a general discussion of this type of Eistenstein series, we refer to [**Shi78**, § 3], especially Proposition 3.4 already cited. Alternatively, one could consult [**Miy89**, Chapter 7], but the normalization there is somewhat different.) The integers N_i are square-free, with $N_1 N_2 \mid N$, and may be determined as follows. If q is any prime number, and a_q is the qth Fourier coefficient of the cuspform f, then we require that the following hold.

(i) If $q^2 \mid N$ and $a_q = 0$, then q divides both N_1 and N_2.

(ii) If q exactly divides N, and $a_q \equiv q/\chi(q) \pmod{\ell}$, then $q \mid N_1$.

(iii) If q exactly divides N, and $a_q \equiv \chi(q) \pmod{\ell}$, and $q/\chi(q) \not\equiv \chi(q) \pmod{\ell}$, then $q \mid N_2$. (The last condition is imposed to avoid overlap with the case above.)

(iv) Finally, for $q = \ell$ or $q \nmid N$, we require that $q \nmid N_1 N_2$.

It follows from these conditions that $b_q = a_q \pmod{\ell}$ at *all* primes q. Indeed, if $a_q = 0$, then q divides both N_1 and N_2, so $b_q = 0$. If N is divisible by exactly the first power of q, then a_q is non-zero and q divides precisely one of the N_i, depending on whether $a_q \equiv q/\chi(q) \pmod{\ell}$ or not. So b_q is also non-zero, and one checks (using the previously displayed formulae for a_q) that b_q satisfies $b_q \equiv a_q \pmod{\ell}$. Finally, if $q = \ell$, then we have $a_q \equiv b_q = \chi(q) + q/\chi(q) \pmod{\ell}$. We point out here that according to the result of Shimura mentioned above, the Eisenstein series g has level $N_1 N_2$. Since $(\ell, N_1 N_2) = 1$, we see that the level of g divides N/ℓ if ℓ divides N.

Thus we have found an Eisenstein series g satisfying the first of our desired conditions. The validity of the second condition for g now follows from the fact that χ is non-trivial, together with the q-expansion principle, as in the proof of Theorem 3.11 in [**GV00**]. For the convenience of the reader, we repeat the argument here. Namely, the Eisenstein series $g = \sum b_n q^n$ we have constructed satisfies condition (1) above, so that $a_n - b_n \equiv 0 \pmod{\lambda}$ for $n \geqslant 1$. Since χ is non-trivial, we even have $b_0 = 0$ (because the constant term is equal to the residue of $L(g, s)$ at $s = 1$, and $L(g, s)$ is holomorphic in this case). Since f is a cuspform we have $a_0 = 0$, and so $a_0 - b_0 \equiv 0 \pmod{\lambda}$ as well. Thus the form $f - g = \sum c_n q^n$ is such that $c_n = a_n - b_n \equiv 0 \pmod{\lambda}$ for $n \geqslant 0$. In other words, the q-expansion of $f - g$ at ∞ vanishes identically modulo λ.

If $\ell \nmid N$, this implies that $f - g$ is identically zero modulo λ by the q-expansion principle. Thus the q-expansion of $f - g$ is zero modulo λ at all cusps of $X_0(N)$. In particular, the constant term at any cusp is divisible by λ. But since f is a cuspform, f has no constant

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

term at any cusp, which implies that the constant term of g at every cusp is divisible by λ, as required.

It remains to treat the case where ℓ divides N. In this case, N is divisible by precisely the first power of ℓ, and $c_n = 0 \pmod{\lambda}$, $n \geqslant 0$, implies only that $f - g$ vanishes identically on the component of $X_0(N)_{\mathbb{F}_\ell}$ containing the cusp ∞. Then the same argument as before shows that the constant term of g at any cusp lying on the component containing ∞ of $X_0(N)_{\mathbb{F}_\ell}$, is divisible by λ. As for the remaining cusps, they lie on the component of $X_0(N)_{\mathbb{F}_\ell}$ containing the cusp 0, and an explicit computation with Tate curves shows that such cusps are ramified over $X_0(N/\ell)$ (over $\mathbb{Z}$), with ramification index ℓ. Indeed, one checks using the results of [**DR73**, Chapter V] or the summary in [**DI95**, § 9.3] that the cusps reducing to the 0-component are precisely those corresponding to generalized elliptic curves whose component group has order divisible by ℓ, and that the canonical projection is given in terms of a local coordinate q at such a cusp by $q \mapsto q^\ell$. But as we observed above, our Eisenstein series g has level dividing N/ℓ. Thus it arises via pullback, under the canonical projection from $X_0(N)$ to $X_0(N/\ell)$, from a form on $X_0(N/\ell)$. This implies that the constant term at a ramified cusp is divisible by ℓ, because the constant term is equal to the residue of the associated differential $g(z)\,\mathrm{d}z = g(q^\ell)\,\mathrm{d}(q^\ell)/q^\ell$. This completes the proof when χ is non-trivial.

If χ is trivial, then we have to be more careful. In this case, the composition factors of $E_0[\ell]$ are given by $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ. If $\mathbb{Z}/\ell\mathbb{Z}$ occurs as a subgroup, then the statement of the proposition follows. So we may assume that there is an exact sequence of Galois modules

$$0 \to \mu_\ell \to E_0[\ell] \to \mathbb{Z}/\ell\mathbb{Z} \to 0, \tag{5.1}$$

and our task is to use an Eisenstein series to construct a splitting of this sequence.

Observe that the existence of the sequence (5.1) implies directly that there is a prime r dividing the conductor N such that $r \equiv 1 \pmod{\ell}$. Indeed, we have $\mu_\ell \subset E_0 \subset J_0(N)$, and by Theorem 1.1 we find that $\mu_\ell \subset E_0[\ell]$ must be contained in the Shimura subgroup V. But the formula of Corollary 1 in [**LO91**] shows that the order of V divides $\phi(N)$, for the Euler function ϕ, and since $\ell^2 \nmid N$, this implies our contention.

Thus we fix a prime $r \mid N$ such that $r \equiv 1 \pmod{\ell}$. Since $\mathrm{Frob}(r)$ acts trivially on μ_ℓ, we see that the rth Fourier coefficient $a_r = a_r(f)$ satisfies $a_r \equiv 1 \pmod{\ell}$ if $r^2 \nmid N$, or $a_r = 0$ if $r^2 \mid N$. Here f is the cuspform corresponding to our elliptic curve E_0, as before. Now consider the unique holomorphic Eisenstein series g' of weight 2 on $\Gamma_0(r)$, normalized so that the coefficient of q is equal to 1. Then the constant terms of g' at the two cusps of $\Gamma_0(r)$ are given by $\pm\frac{1}{24}(r-1)$. Note also that the coefficient of q^r is 1, which already matches the coefficient of f, if $r^2 \nmid N$. If $r^2 \mid N$, then we can remove the unique Euler factor of g' at r to match the rth Fourier coefficient of f. Thus, starting from g', we can once again strip Euler factors to produce an Eisenstein series of level M satisfying the first of the two required conditions.

The second condition is clear if $\ell > 3$. Indeed, $r \equiv 1 \pmod{\ell}$, so that the numbers $\pm\frac{1}{24}(r-1)$ are non-units in $\mathbb{Z}_\ell$. Thus the constant terms of the q-expansion of g' at both cusps of $\Gamma_0(r)$ are divisible by ℓ, and it was checked in the proof of Theorem 3.3 in [**Vat99**] that this implies the analogous condition for the form $g(z)$ on $\Gamma_0(N)$.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

It remains to consider the case $\ell = 3$. If $N = r$ is prime, then the results of Mazur [**Maz77**] imply that $r \equiv 1 \pmod 9$. Then $\frac{1}{24}(r-1)$ is divisible by 3, and we obtain the required result as above. Thus we may assume that there exists some prime r' dividing N/r. We want to assume further that we may choose r' so that $r' \neq 3$. Indeed, if this were not possible, then (since $\ell = 3$ is a prime of semi-stable reduction) we must have $N = 3r$, for a prime number r, with $r \equiv 1 \pmod 3$. The existence of the exact sequence (5.1) and Theorem 1.1 shows that the order of the Shimura subgroup is divisible by 3. But looking at the formula for the order of the Shimura subgroup as given in [**LO91**, Corollary 1] we find that $\phi(N) = 2(r-1)$ must be divisible by 9. Thus $r \equiv 1 \pmod 9$, and we may therefore argue as in the case above.

Thus we can assume that $r' \neq 3$ (still assuming $\ell = 3$). If $r' = r$, then $r^2 \mid N$ and $a_r(E_0) = a_r(f) = 0$. Then stripping the remaining Euler factor at r from g' gives the Eisenstein series $g''(z) = g'(z) - g'(rz)$, which has rth coefficient zero, and constant term zero at infinity. Starting from g'', we deduce an Eisenstein series g of level N satisfying the first condition, and such that the constant term at infinity is zero. Note that if $3 \mid N$, then the coefficients of q^3 for g' and f are already congruent. Indeed, the coefficient of q^3 for g' is $\sum_{d|3} d = 4$. On the other hand, the coefficient of q^3 in the expansion of f is determined as the eigenvalue of Frob(3) on the maximal unramified quotient of $E_0[3^\infty]$, and since $E_0[3]$ has the composition series (5.1), we find that $a_3(f) \equiv 1 \pmod 3$. Thus it is not necessary to adjust Euler factors at 3 to achieve the desired congruence, and we may assume that g in fact has level prime to $\ell = 3$. But now that the form $h = f(z) - g(z)$ has q-expansion at infinity that vanishes identically modulo $\lambda \mid 3$, and the same argument used in the case $\chi \neq 1$ above proves our contention.

If $r' \neq r$ and $r' \equiv 1 \pmod 3$, one has $a_{r'}(E_0) = 1$ or 0. Take $g'' = g'(z) - r'g'(r'z)$. Then g'' has constant term divisible by 3 at infinity, and r'th coefficient 1, and we can find $g(z)$ by arguing as before.

If $r' \equiv -1 \pmod 3$, then $a_{r'}(E_0) = -1$ or 0 since if E_0 has multiplicative reduction, it is necessarily non-split. To verify this latter point, we need Theorem 1.1 again. Indeed, we have $\mu_3 \subset X \subset J_0(N)$, since by our ordinariness hypothesis $J_0(N)$ is semi-stable at 3. But then Theorem 6 of [**LO91**] shows that the Hecke operator $T_{r'}$ acts as multiplication by r' on μ_3, and since $r' \equiv -1 \pmod 3$ and $\mu_3 \subset E_0$, we see that the eigenvalue of $T_{r'}$ is -1. Thus we may take $g'' = g'(z) - g'(r'z)$, and argue as before, since the latter has r'th coefficient equal to $r' \equiv -1 \pmod 3$.

In summary, we have shown that there exists an Eisenstein series $g(z)$ of level dividing N satisfying the conditions (1) and (2) above. Let C_g denote the subgroup of the cuspidal group associated to g in [**Ste82**, Definition 1.8.5]. Then we claim that $C_g[\ell]$ is non-zero. In fact, various forms of this result have already been used in [**Ste82**,**Ste85**,**GV00**], but for completeness we spell out the details again. The basic ingredients are condition (2) above, and a theorem of Washington. Namely, by [**Ste82**, Corollary 1.8.7], the group C_g is isomorphic to $\hom(A_g, \mathbb{Q}/\mathbb{Z})$, where $A_g = P_g/C_g$, and A_g and C_g denote the $\mathbb{Z}$-modules generated (in $\mathbb{C}$) by the periods and residues of g, respectively (see [**Ste82**, pp. 40–41]). Then condition (1) states precisely that all residues of g are divisible by λ, and it suffices to exhibit a period of g which is a λ-adic unit. So let $\phi_g \in H^1(X_0(N), A_g)$

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

denote the cohomology class associated to g by Stevens [**Ste82**, bottom of p. 40]. We will show that the 'twisted special value' period $\Lambda(\phi_g, \xi)$ is an ℓ-adic unit, for some Dirichlet character ξ with conductor prime to N. Here we remind the reader that $\Lambda(\phi_g, \xi) = \phi_g \cap \Lambda(\xi) \in A \otimes \mathbb{Z}[\xi]$ is the cap product of ϕ_g with a certain homology class $\Lambda(\xi)$ in $H_1(X_0(N), \mathbb{Z}[\xi])$ defined via modular symbols (see [**Ste82**, Definition 1.6.4]). If we let $P(\xi)$ and $R(\xi)$ denote the $\mathbb{Z}[\xi]$-modules generated respectively by the periods and residues of g, then there is a surjective map $A_g \otimes \mathbb{Z}[\xi] \to A_g(\xi) = R(\xi)/P(\xi)$, and it even suffices to show that $\Lambda(\phi_g, \xi)$ is non-zero in $A_g(\xi)$.

We select ξ to be a Dirichlet character of t-power conductor, where t is some prime with $t \nmid N\ell$ (to be specified later). Then Corollary 3.1.5 in Stevens shows that

$$\Lambda(\phi_g, \xi) = \frac{\tau(\xi)}{2\pi \mathrm{i}} L(g, \xi, 1) \in A_g(\xi),$$

since ξ is non-exceptional at ℓ in Stevens's terminology [**Ste82**, Definition 3.1.3]. Here $\tau(\xi)$ denotes the usual Gauss sum of ξ, and $L(g, \xi, s)$ denotes the ξ-twisted L-function of g. We must therefore unwind the definition of $L(g, \xi, s)$, keeping track of the Euler factors that were removed in the construction. As before, we find that there exist positive integers N_1 and N_2 such that $N_1 N_2$ divides N, and such that

$$L(g, \xi, s) = L_{N_1}(\chi\xi, s) L_{N_2}(\chi^{-1}\xi, s-1).$$

Here again the N_i are prime to ℓ, since our form g has level dividing N/ℓ if $\ell \mid N$. Now applying the functional equation of $L_{N_1}(\chi\xi, s)$ and putting in $s = 1$, we find that

$$\Lambda(\phi_g, \xi) = \text{unit} \cdot \prod_{q \mid N_1} (1 - \chi\xi(q)/q) \cdot \prod_{q \mid N_2} (1 - \chi^{-1}\xi(q)) \cdot L((\chi\xi)^{-1}, 0) \cdot L(\chi^{-1}\xi, 0).$$

But the L-values appearing in the above formula are ℓ-adic units for almost all ξ of t-power conductor according to a theorem of Washington [**Was78**]. Thus one needs only to check that one can choose t and ξ so that the various Euler factors are units, and this is elementary.

Thus $C_g[\ell]$ is non-zero. Furthermore, the eigenvalue of the Hecke operator T_n on C_g is given by $b_n(g) \equiv a_n(E_0) \pmod{\lambda}$. Let $\mathfrak{m}$ denote the maximal ideal of the Hecke ring $\mathbb{T}$ determined by f modulo λ. Then $J_0(N)[\mathfrak{m}]$ contains both $C_g[\ell]$ and $E_0[\ell]$, and all of these are modules for $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Note also that the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on C_g is via the character χ, and that each of the $\pm$-eigenspaces for complex conjugation in $E_0[\ell]$ has dimension 1. But now the multiplicity one theorem of $J_0(N)[\mathfrak{m}]^{et}$ (see [**Vat99**, Theorem 2.7] for a discussion in this context) shows that the α eigenspace for complex conjugation inside $J_0[\mathfrak{m}]$ is one dimensional over $\mathbb{F}_\ell$, where α denotes the parity of χ. It follows that $C_g \cap E[\ell] = E[\ell]^\alpha \neq 0$, and this proves our proposition. □

Lemma 5.4. *Let E_0 be the strong Weil curve for $X_0(N)$. Let $E' \to E_0$ denote an étale isogeny of degree ℓ^r. Suppose that E_0 is ordinary at ℓ. Then $r \leqslant 1$ unless the class $\mathcal{C}$ is sporadic.*

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

Proof. By the previous lemma, there is another étale isogeny $E_0 \to E''$, of degree ℓ. Then the composite $\phi : E' \to E_0 \to E''$ is a composite of étale isogenies, and is therefore étale, and of degree ℓ^{r+1}. Since ϕ is étale, the kernel is necessarily cyclic. Indeed, if this were not the case, then $\ker(\phi)$ would contain a subgroup isomorphic as a group to $\mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z}$. But this means that $E[\ell] \subset \ker(\phi)$, so that ϕ must factor through the multiplication by ℓ, which contradicts the fact that it is étale. Thus ϕ is cyclic of degree ℓ^{r+1}, and by Mazur's theorem again, we must have $r \leqslant 1$ unless $\ell = 3$, in which case $r + 1 = 3$ is possible. Excluding the finitely many curves corresponding to non-cuspidal rational points of $X_0(27)$ (which correspond to sporadic isogeny classes and can be checked by machine as in Remark 1.12), we obtain the conclusion of the lemma. □

5.5. We can now complete the proof of Theorem 1.10. Let $\mathcal{C}$ denote a (non-sporadic) class of semi-stable elliptic curves, and let E_0 denote the strong Weil curve in $\mathcal{C}$. Let $\phi : E^* \to E_0$ be an étale isogeny from the minimal curve E^* to E_0. Let n denote the degree of ϕ. Then, by the lemma above, we have $n = 2^r \prod \ell_i$, where the ℓ_i are distinct odd primes. For each $\ell = \ell_i$ dividing n, we know that the composition factors of $E^*[\ell]$ are $Z/\ell\mathbb{Z}$ and μ_ℓ, by semi-stability of E^*. Let $K_\ell^* \subset E^*[\ell]$ denote the ℓ-part of the kernel of ϕ. Since ϕ is étale, we have $K_\ell^* = \mathbb{Z}/\ell\mathbb{Z}$. Letting $K_\ell \subset E_0$ denote the ℓ-part of the kernel of the dual isogeny ϕ^*, we find that $K_\ell \cong \mu_\ell \subset E_0 \subset J_0(N)$. By Theorem 1.1, we find that $K_\ell \subset J_0(N)$ is contained in the Shimura subgroup V. Now let E_1 denote the analogue of the Weil curve for $X_1(N)$. Then $E_1 \cong E_0/V'$, where $V' = E_0 \cap V$. But now $\prod_\ell K_\ell \subset V'$, and, since V is of multiplicative type, it follows that $\prod K_\ell$ coincides with the prime-to-2 part of $V' = V \cap E_0$ (because any $\mu_\ell^r \subset E_0$ is the kernel of an isogeny with étale dual). But by definition $\prod_\ell K_\ell$ is the prime-to-2 part of the kernel of ϕ^* as well. Thus we get isogenies $E_0 \to E' = E_0/\prod K_\ell \to E_1$, and $E' = E^*$ up to an isogeny of degree a power of 2. This proves the theorem.

5.6. The proof of Theorem 1.11 is straightforward. Let $\ell \geqslant 7$, and consider an isogeny class $\mathcal{C}$ of elliptic curves such that $E[\ell]$ is reducible for $E \in \mathcal{C}$. Then, according to the list of possible rational cyclic isogenies, and excluding finitely many sporadic isogeny classes as explained in Remark 1.12, we may assume that $E[p]$ is irreducible for such E if $p \neq \ell$, and that there are no cyclic isogenies of degree ℓ^2. It follows that the class $\mathcal{C}$ consists of two curves, connected by isogenies of degree ℓ.

Let E_0 denote the strong Weil curve for $X_0(N)$ in $\mathcal{C}$. Then E_0 is ordinary at ℓ by hypothesis. It follows from Proposition 5.3 that there is a subgroup $C \subset E_0[\ell]$ such that C has order ℓ, and the action of $G_\mathbb{Q}$ is via a character χ that is unramified at ℓ. One checks that $E_0 \to E_0/C$ is étale, since C is unramified, and E_0 is semi-stable at ℓ by Proposition 5.3. Thus E_0 is the minimal curve in $\mathcal{C}$. Furthermore, since there are no cyclic isogenies of degree ℓ^2, one sees that the sequence $0 \to C \to E[\ell] \to D \to 0$ is non-split. Then it is clear that E_0 has trivial intersection with the Shimura subgroup, since the action of $G_\mathbb{Q}$ on the latter is cyclotomic. Thus $E_0 \subset J_0(N)$ maps injectively into $J_1(N)$, and we have $E_0 = E_1$ is the strong Weil curve for $X_1(N)$. This proves the theorem.

https://doi.org/10.1017/S147474800500006X Published online by Cambridge University Press

5.7. Finally, we note that Theorem 1.16 follows from the fact that Stevens's conjecture is true at ℓ under the hypotheses of the theorem, by the same argument that proved Theorem 1.10. Indeed, it is clear that the L-function $\mathcal{L}(E_1, T)$ associated to the strong Weil curve for $X_1(N)$ is integral; this was already observed in [**GV00**, Remark 3.5]. The theorem follows from this, together with the formulae of [**Ste89**, Proposition 4.12].

Acknowledgements. It is a pleasure to thank Brian Conrad, Ralph Greenberg and Ken Ribet for some useful exchanges on the subject of this work. I also thank Haruzo Hida and Karl Rubin for answering my many questions about their work. This work was party supported by an NSERC grant, and was written largely while the author was enjoying the hospitality of the University of Paris-7. Finally, we thank the anonymous referees for their careful examination of the manuscript and for their numerous suggestions.

We also point out that a version of our Theorem 1.11 may be found in [**Tan97**], where it was assumed that $\ell \geqslant 13$ and the prime ℓ is a prime of good reduction. The method of proof is similar.

References

[BK75] B. J. Birch and W. Kuyk (eds), *Modular functions of one variable*, IV, Lecture Notes in Mathematics, vol. 476 (Springer, 1975).

[CG96] J. Coates and R. Greenberg, Kummer theory for abelian varieties over local fields, *Invent. Math.* **124** (1996), 129–174.

[Cor02] C. Cornut, Mazur's conjecture on higher Heegner points, *Invent. Math.* **148** (2002), 495–523.

[Cre92] J. Cremona, *Algorithms for elliptic curves* (Cambridge University Press, 1992).

[DR73] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques. Modular functions of one variable, II, in *Proc. Int. Summer School, University of Antwerp, Antwerp, 1972*, pp. 143–316, Lecture Notes in Mathematics, vol. 349 (Springer, 1973).

[dS87] E. de Shalit, *Iwasawa theory of elliptic curves with complex multiplication* (Academic, 1987).

[DI95] F. Diamond and J. Im, Modular curves and modular forms, in *CMS Conf. Proc. Fermat's Last Theorem, Toronto, 1993*, pp. 39–133 (ed. K. Murty) (American Mathematical Society, Providence, RI, 1995).

[Gre78] R. Greenberg, On the structure of certain Galois groups, *Invent. Math.* **47** (1978), 85–99.

[GV00] R. Greenberg and V. Vatsal, Iwasawa invariants of elliptic curves, *Invent. Math.* **142** (2000), 17–63.

[Hid03] H. Hida, *Non-vanishing modulo p of Hecke L-values* (2003) (available at http://www.math.ucla.edu/hida).

[Iha75] Y. Ihara, *On modular curves over finite fields. Discrete subgroups of Lie groups and applications to moduli* (Oxford University Press, 1975).

[Ken82] M. A. Kenku, On the number of **Q**-isomorphism classes of elliptic curves in each **Q**-isogeny class, *J. Number Theory* **15** (1982), 199–202.

[LO91] S. Ling and J. Oesterlé, The Shimura subgroup of $J_0(N)$, *Astérisque* **6** (1991), 171–203.

[Maz] B. Mazur, Courbes elliptiques et symboles modulaires, in *Séminaire Bourbaki, 24ème année, 1971/1972*, Exp. No. 414, pp. 277–294, Lecture Notes in Mathematics, vol. 317 (Springer, 1972).

[Maz77] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33–189.

[Maz78] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.
[Miy89] T. Miyake, *Modular forms* (Springer, 1989).
[Pra95] D. Prasad, Ribet's theorem: Shimura–Taniyama–Weil implies Fermat, in *Seminar on Fermat's Last Theorem, Toronto, ON, 1993/1994*, pp. 155–177 (American Mathematical Society, Providence, RI, 1995).
[Ray74] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$, *Bull. Soc. Math. France* **102** (1974), 241–280.
[Rib84] K. A. Ribet, Congruence relations between modular forms, in *Proc. Int. Congr. Mathematicians*, vols 1, 2, pp. 503–514 (PWN, Warsaw, 1984).
[Rub94] K. Rubin, *More 'main conjectures' for imaginary quadratic fields. Elliptic curves and related topics*, pp. 23–28 (American Mathematical Society, Providence, RI, 1994).
[Ser59] J.-P. Serre, *Groupes algébriques et corps de classes* (Hermann, 1959).
[Ser72] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
[Shi78] G. Shimura, The special values of the zeta functions associated with Hilbert modular forms, *Duke Math. J.* **45** (1978), 637–679.
[Ste82] G. Stevens, *Arithmetic on modular curves*, Progress in Mathematics, vol. 20 (Birkhäuser, 1982).
[Ste85] G. Stevens, The cuspidal group and special values of L-functions, *Trans. Am. Math. Soc.* **291** (1985), 519–550.
[Ste89] G. Stevens, Stickelberger elements and modular parametrizations of elliptic curves, *Invent. Math.* **98** (1989), 75–106.
[Tan97] S.-L. Tang, Congruences between modular forms, cyclic isogenies of modular elliptic curves and integrality of p-adic L-functions, *Trans. Am. Math. Soc.* **349** (1997), 837–856.
[Vat99] V. Vatsal, Canonical periods and congruence formulae, *Duke Math. J.* **98** (1999), 397–419.
[Vat02] V. Vatsal, Uniform distribution of Heegner points, *Invent. Math.* **148** (2002), 1–46.
[Vat03] V. Vatsal, Special values of anticylotomic L-functions, *Duke Math. J.* **116** (2003), 219–261.
[Was78] L. Washington, The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension, *Invent. Math.* **49** (1978), 87–97.
[Yag82] R. Yager, On two variable p-adic L-functions, *Annli Mat.* **115** (1982), 411–449.