J. ALGEBRAIC GEOMETRY
17 (2008) 643–675
S 1056-3911(08)00462-1
Article electronically published on February 7, 2008

SCARCITY AND ABUNDANCE OF TRIVIAL ZEROS IN DIVISION TOWERS

DAVID E. ROHRLICH

Abstract

Explicit formulas and asymptotic estimates are derived for twisted root numbers of elliptic curves in division towers. The key assumption on the elliptic curves considered is that the image of the Galois representation afforded by the first layer of the division tower is contained in a Borel subgroup. In [Math. Research Letters **13** (2006), 359–376], by contrast, the Galois representation was assumed to be surjective.

By a *trivial zero* of an L-function one usually means a zero which is forced on the L-function by its functional equation. For example, the negative even integers are trivial zeros of the Riemann zeta function, because the functional equation shows that $\Gamma(s/2)\zeta(s)$ is holomorphic at these points while $\Gamma(s/2)$ has simple poles there. Here we shall be concerned with possible trivial zeros at $s = 1$ of twisted L-functions of an elliptic curve, the twists being self-dual Artin representations of the Galois group of a division tower of the curve. The reason for restricting attention to self-dual representations is that the conjectural functional equation then relates the L-function to itself, so that the issue of trivial zeros arises at $s = 1$ and reduces to a root number calculation as in Greenberg [8] or Howe [9]. The point of the present note is that we carry out the calculation in a case where the Galois representation on the Tate module is *not* surjective. More precisely, we assume that the image of the Galois group of the first layer of the tower is contained in a Borel subgroup. Other hypotheses on the image of this Galois group (for example, that it is contained in the normalizer of a Cartan subgroup, or that it is of projective type A_4, S_4, or A_5) may also be worth investigating but will not be treated here.

To focus on the case at hand, fix a number field F, an algebraic closure $\overline{F}$ of F, an elliptic curve E over F without complex multiplication, and an odd prime p, and let $\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}(2, \mathbb{Z}_p)$ be the representation determined up to isomorphism by the p-adic Tate module of E. We write Γ for the image

Received July 4, 2006.

of ρ, R for the fixed field of its kernel, and $\mathcal{T}$ for the set of isomorphism classes of continuous irreducible complex representations τ of $\mathrm{Gal}(\overline{F}/F)$ which factor through $\mathrm{Gal}(R/F)$ and are self-dual. Given an isomorphism class $[\tau] \in \mathcal{T}$ one defines the associated tensor-product L-function $L(s, E, \tau)$ and root number $W(E, \tau)$ as in [4], [18], [1], [10], and [11]. We shall be concerned with $W(E, \tau)$ only under the following two assumptions, which are henceforth always in force:

- The reduction of Γ modulo p is contained in a Borel subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$.
- Suppose that v is a finite place of F at which E has potential good reduction. If either $p = 3$ or v lies over p, then E attains good reduction at v over an *abelian* extension of F.

We note that the second condition is automatically satisfied if $p \geqslant 5$ and E has good reduction at the places of F over p.

Theorem 1. *If E has potential good reduction, then*

$$W(E, \tau) = \left(\frac{-1}{p}\right)^{[F:\mathbb{Q}]}$$

for $[\tau] \in \mathcal{T}$ with $\dim \tau > 1$.

Thus if $j(E)$ is integral, then for $[\tau] \in \mathcal{T}$ with $\dim \tau > 1$ the root number $W(E, \tau)$ is independent of τ and in fact depends only on the congruence class of $p^{[F:\mathbb{Q}]}$ mod 4. We now ask whether it is possible to remove the hypothesis that E has potential good reduction. Here is an example in which this hypothesis is no longer satisfied, but the conclusion is even starker than in Theorem 1:

Example 1 (Cf. Coates and Sujatha [2], p. 832, Example 4.8)**.** If $F = \mathbb{Q}$, $p = 5$, and E is the curve 150A1 of Cremona's table [3], then $W(E, \tau) = 1$ for all $[\tau] \in \mathcal{T}$. An equation for E is

$$y^2 + xy = x^3 - 3x - 3,$$

and $j(E) = -24389/12$, $N(E) = 2 \cdot 3 \cdot 5^2$, and $\Delta(E) = -2^2 \cdot 3 \cdot 5^3$. (As usual, $N(E)$ and $\Delta(E)$ denote the conductor and minimal discriminant of E.)

On the other hand, the next example shows that we cannot simply omit the hypothesis of Theorem 1 without altering the conclusion in some way.

Example 2 (Cf. Coates and Sujatha [2], p. 831, Example 4.7)**.** If $F = \mathbb{Q}$, $p = 7$, and E is the curve 294B1 of [3], then $W(E, \tau) = -1$ for most $[\tau] \in \mathcal{T}$, but there is a sparse infinite family of exceptional $[\tau]$ for which $W(E, \tau) = 1$.

In this case E is given by the equation

$$y^2 + xy = x^3 - x - 1,$$

and $j(E) = -2401/6$, $N(E) = 2 \cdot 3 \cdot 7^2$, and $\Delta(E) = -2 \cdot 3 \cdot 7^2$.

As it stands, Example 2 is an imprecise statement. To eliminate the imprecision we impose a filtration on $\mathcal{T}$ and describe its growth. For $n \geqslant 1$ let ρ_n and Γ_n be the reduction modulo p^n of ρ and Γ respectively. Write R_n for the fixed field of the kernel of ρ_n and define $\mathcal{T}_n$ to be the subset of $\mathcal{T}$ consisting of isomorphism classes $[\tau]$ such that τ factors through $\mathrm{Gal}(R_n/F)$. The quantity

$$\vartheta_n = \sum_{[\tau] \in \mathcal{T}_n} \dim \tau$$

will serve as our measure of the size of $\mathcal{T}_n$. Its asymptotic behavior is controlled by a constant w defined as follows. Let $\overline{\rho}$ and $\overline{\rho}_n$ denote the projective representations associated to ρ and ρ_n, and let $\overline{\Gamma} \subset \mathrm{PGL}(2, \mathbb{Z}_p)$ and $\overline{\Gamma}_n \subset \mathrm{PGL}(2, \mathbb{Z}/p^n\mathbb{Z})$ be their respective images. Then $w = |\overline{\Gamma}_1|$. We also put $b = |\Gamma_1 \cap \{\pm 1\}|$, where in its second occurrence, 1 denotes the 2×2 identity matrix.

Theorem 2. *If w is even, then $\vartheta_n \sim a \cdot p^{2n}$ for some constant $a > 0$. If w is odd, then $\vartheta_n = b$ for all n.*

The constant a in Theorem 2 depends on E only through Γ; indeed the theorem itself is purely group-theoretic. We shall actually prove a more precise statement (see Proposition 6), but for the moment we merely point out that w is automatically even if F has at least one real place, because any complex conjugation in $\mathrm{Gal}(\overline{F}/F)$ is sent by ρ_1 to a nonscalar involution (recall that an *involution* in a group is simply an element of order two). It follows in particular that w is even if $F = \mathbb{Q}$. Thus $\vartheta_n \sim a \cdot p^{2n}$ in Example 2, and our claim that the exceptional $[\tau]$ in Example 2 are "sparse" is now superseded by the following general statement.

Let $\mathcal{T}_n^{\pm}$ be the set of $[\tau] \in \mathcal{T}_n$ for which $W(E, \tau) = \pm 1$, and put

$$\vartheta_n^{\pm} = \sum_{[\tau] \in \mathcal{T}_n^{\pm}} \dim \tau.$$

Also put

$$\epsilon = \text{ sign of } \left(\frac{-1}{p}\right)^{[F:\mathbb{Q}]},$$

and write $-\epsilon$ for the sign opposite to ϵ.

Theorem 3. *If w is even, then $\vartheta_n^{-\epsilon} = O(p^n)$.*

Since $\vartheta_n = \vartheta_n^{+} + \vartheta_n^{-}$, we deduce:

Corollary 1. *If w is even, then $\vartheta_n \sim \vartheta_n^{\epsilon}$.*

To return to the theme of trivial zeros, let $\mathcal{T}_n^*$ denote the set of *all* isomorphism classes (not just the self-dual classes) of continuous irreducible complex representations of $\mathrm{Gal}(\overline{F}/F)$ which factor through $\mathrm{Gal}(R_n/F)$. Then the L-function of E over R_n has the factorization

$$L(s, E/R_n) = \prod_{[\tau]\in\mathcal{T}_n^*} L(s, E, \tau)^{\dim \tau},$$

whence (granting the analytic continuation to $s = 1$)

$$\mathrm{ord}_{s=1} L(s, E/R_n) = \sum_{[\tau]\in\mathcal{T}_n^*} \dim \tau \cdot \mathrm{ord}_{s=1} L(s, E, \tau).$$

Now if we restrict the summation on the right-hand side to $[\tau] \in \mathcal{T}_n^-$ and replace $\mathrm{ord}_{s=1} L(s, E, \tau)$ by 1, then we obtain ϑ_n^-, which therefore coincides with the contribution of trivial zeros to $\mathrm{ord}_{s=1} L(s, E/R_n)$.

Corollary 2. *If $p \equiv 3 \pmod 4$ and $[F : \mathbb{Q}]$ is odd, then $\vartheta_n^- \sim a \cdot p^{2n}$ with $a > 0$. Otherwise $\vartheta_n^- = O(p^n)$.*

Indeed if $[F : \mathbb{Q}]$ is odd, then F has a real place, whence w is even. Theorem 3 and Corollary 1 are then in force, giving $\vartheta_n^- = O(p^n)$ and $\vartheta_n^- \sim a \cdot p^{2n}$ respectively according as $p \equiv 1$ or $p \equiv 3 \bmod 4$. On the other hand, if $[F : \mathbb{Q}]$ is even, then $\vartheta_n^- = O(p^n)$, either by Theorem 3 (if w is even) or else vacuously by Theorem 2 (if w is odd). It should be added that the trivial zeros counted by ϑ_n^- are strictly speaking "virtual trivial zeros" in the sense that the relevant functional equations are in general still conjectural.

Organization of the paper. After proving Theorems 1, 2, and 3 we will revisit Examples 1 and 2. The point of doing so is that neither example is fully elucidated by our theorems: The theorems give $\vartheta_n^+ \sim \vartheta_n$ in Example 1 and $\vartheta_n^+ = O(p^n)$ in Example 2, but we shall prove the more precise statement $\mathcal{T}_n^+ = \mathcal{T}_n$ in Example 1 and the complementary statement $\vartheta_n^+ \gg p^n$ in Example 2.

1. Proof of Theorem 1. In spite of what the heading might suggest, the arguments in this section are as essential to the proof of Theorem 3 as they are to the proof of Theorem 1. In fact the assumption that E has potential good reduction comes into force only in the final sentence. Until then we use only our two standing assumptions about E, namely that Γ_1 is contained in a Borel subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$ and that at places of potential good reduction which lie over p (and at all places of potential good reduction if $p = 3$) E acquires good reduction over an abelian extension of F. The hypothesis that E does not have complex multiplication is also a part of our framework but is not needed in the proof of Theorem 1.

Let U denote the subgroup of $\mathrm{GL}(2, \mathbb{Z}_p)$ consisting of matrices which reduce modulo p to an upper triangular unipotent matrix. We also write M for the

additive group of 2×2 matrices over $\mathbb{Z}_p$ and put $K(n) = 1 + p^n M$ $(n \geqslant 1)$, so that $K(n)$ is the kernel of reduction modulo p^n on $\mathrm{GL}(2, \mathbb{Z}_p)$.

Lemma. *If $p \geqslant 5$, then U has no nontrivial elements of finite order.*

Proof. It is a standard remark that $K(n)$ has no nontrivial elements of finite order. But if $u \in U$, then $u^p \in K(1)$, so it suffices to see that U has no nontrivial elements of order p. If on the contrary u is such an element, then there is an eigenvalue ζ of u which is a primitive pth root of unity and therefore of degree $p - 1$ over $\mathbb{Q}_p$. On the other hand, ζ satisfies the characteristic polynomial of u, which is a polynomial of degree 2 over $\mathbb{Q}_p$. Hence $p - 1 \leqslant 2$, a contradiction. □

Remark. The lemma fails for $p = 3$, the matrix

$$\begin{pmatrix} 1 & -1 \\ 3 & -2 \end{pmatrix}$$

being a counterexample.

Now let B be the subgroup of $\mathrm{GL}(2, \mathbb{Z}_p)$ consisting of matrices which are upper triangular modulo p, or in other words which reduce modulo p to the standard Borel subgroup of $\mathrm{GL}(2, \mathbb{F}_p)$. By assumption, there is an element $g_1 \in \mathrm{GL}(2, \mathbb{F}_p)$ which conjugates Γ_1 into the standard Borel subgroup, and if $g \in \mathrm{GL}(2, \mathbb{Z}_p)$ is any lift of g_1, then g conjugates Γ into B. Hence after replacing ρ by an equivalent representation we may assume that Γ is itself a subgroup of B. For the proof of the following proposition we also observe that B/U is isomorphic to the subgroup of diagonal matrices in $\mathrm{GL}(2, \mathbb{F}_p)$ and is therefore abelian.

Proposition 1. *Let v be a finite place of F at which E has potential good reduction. There is an abelian extension K of F over which E attains good reduction at v.*

Proof. If $p = 3$ or v lies over p, then the proposition holds by assumption. Henceforth we assume that $p \geqslant 5$ and that the residue characteristic of v is not p. Let $K \subset \overline{F}$ be the fixed field of $\rho^{-1}(U)$. Then $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of B/U and is therefore abelian. If I is the inertia subgroup of $\mathrm{Gal}(\overline{F}/K)$ at a place of $\overline{F}$ above v, then $\rho(I)$ is finite by the criterion of Néron-Ogg-Shafarevich, hence trivial by the lemma. It follows that E has good reduction over K at v. □

Given an arbitrary place v of F, let F_v denote the completion of F at v and $\overline{F}_v$ an algebraic closure of F_v containing $\overline{F}$; write $\mathcal{W}(\overline{F}_v/F_v)$ for the local Weil group. We shall use Proposition 1 to derive a property of the representation σ_{E/F_v} of $\mathcal{W}(\overline{F}_v/F_v)$ associated to E (cf. [10], p. 147). The property at issue involves one-dimensional characters, about which two remarks are in order.

The first remark is that the word *character* will often be used to mean *one-dimensional character*, even though the character $\operatorname{tr}\tau$ associated to a representation τ of dimension > 1 will also make an occasional appearance. The trivial one-dimensional character of any group will be denoted simply 1.

The second remark is number-theoretic. Let F_v^{ab} be the maximal abelian extension of F_v inside $\overline{F}_v$, and write $x \mapsto (x, F_v^{\mathrm{ab}}/F_v)$ for the reciprocity law isomorphism of $F_v^\times$ onto $\mathcal{W}(F_v^{\mathrm{ab}}/F_v)$ as normalized by Artin. We view a character χ of $F_v^\times$ as a character of $\mathcal{W}(F_v^{\mathrm{ab}}/F_v)$, hence as a character of $\mathcal{W}(\overline{F}_v/F_v)$, of which $\mathcal{W}(F_v^{\mathrm{ab}}/F_v)$ is the abelianization, via the formula

$$\chi(x) = \chi((x^{-1}, F_v^{\mathrm{ab}}/F_v)) \qquad (x \in F_v^\times). \tag{1.1}$$

For example, let ω_v be the unramified character of $F_v^\times$ sending the inverse of a uniformizer of F_v to q_v, the order of the residue class field of F_v. Then ω_v also denotes the unramified character of $\mathcal{W}(\overline{F}_v/F_v)$ sending a Frobenius element to q_v.

Proposition 2. *Let v be a place of F where E has potential good reduction. Then*

$$\sigma_{E/F_v} \otimes \omega_v^{1/2} \cong \chi_v \oplus \chi_v^{-1}$$

for some character χ_v of $F_v^\times$.

Proof. The argument is the same as the one at the bottom of p. 331 of [11], but we review it briefly to show that the restriction in [11] to residue characteristic $\geqslant 5$ is unnecessary here. (It is needed in [11] because Proposition 1 above is not universally valid.) Let F_v^{unr} be the maximal unramified extension of F_v inside $\overline{F}_v$. It follows from the criterion of Néron-Ogg-Shafarevich that there is a unique minimal extension L of F_v^{unr} inside $\overline{F}_v$ such that E has good reduction over L: indeed L is the fixed field of the kernel of the natural representation of $\mathrm{Gal}(\overline{F}_v/F_v^{\mathrm{unr}})$ on the ℓ-adic Tate module of E for any prime ℓ different from the residue characteristic of v (cf. Serre-Tate [16], p. 498, Cor. 3). But if $K \subset \overline{F}$ is as in Proposition 1, then E has good reduction over the compositum KF_v^{unr}, so $L \subset KF_v^{\mathrm{unr}}$. In particular L is abelian over F_v. On the other hand, the description of L as a fixed field shows that σ_{E/F_v} factors through $\mathcal{W}(L/F_v)$, whence $\sigma_{E/F_v} \otimes \omega_v^{1/2}$ can be viewed as a representation of $\mathcal{W}(L/F_v)$. The proposition follows, because $\mathcal{W}(L/F_v)$ is abelian while $\sigma_{E/F_v} \otimes \omega_v^{1/2}$ is two-dimensional, semisimple, and of trivial determinant. □

If v is a finite place of F at which E has potential good reduction, then χ_v will henceforth denote a character as in Proposition 2. Since χ_v could be replaced by χ_v^{-1} there is an arbitrary choice here, but it is harmless for our purposes. There is also a character associated to every finite place v of potential multiplicative reduction, namely the unique character χ_v of $F_v^\times$ such that $\chi_v^2 = 1$ and the twist of E by χ_v is a Tate curve over F_v. For example,

if E has split multiplicative reduction over F_v, then $\chi_v = 1$, while if E has nonsplit multiplicative reduction, then χ_v is the unique unramified quadratic character of $F_v^\times$. In summary, by using Proposition 2 and the theory of the Tate curve we associate a character χ_v of $F_v^\times$ to each *finite* place v of F.

Now at *every* place v of F we have chosen an algebraic closure $\overline{F}_v$ of F_v containing $\overline{F}$. This choice determines an extension of v to $\overline{F}$ and hence an identification of $\mathrm{Gal}(\overline{F}_v/F_v)$ with the corresponding decomposition subgroup of $\mathrm{Gal}(\overline{F}/F)$. Thus for $\tau \in \mathcal{T}$ it is meaningful to speak of the restriction τ_v of τ to $\mathrm{Gal}(\overline{F}_v/F_v)$. On the other hand, if v is a place of potential multiplicative reduction, then χ_v is quadratic or trivial, hence in particular of Galois type: we may view χ_v as a character of $\mathrm{Gal}(\overline{F}_v/F_v)$ and can therefore ask for its multiplicity in τ_v. We denote this multiplicity by $\langle \chi_v, \tau_v \rangle$.

If v is a real place of F, then $c_v \in \mathrm{Gal}(\overline{F}_v/F_v)$ denotes complex conjugation. We write r_1 and $2r_2$ for the number of real and complex embeddings of F.

Proposition 3. *For $\tau \in \mathcal{T}$,*

$$W(E,\tau) = (-1)^{(r_1+r_2)\dim\tau} \cdot \prod_{v \text{ real}} \det\tau(c_v) \cdot \prod_{v\nmid\infty} \chi_v(-1)^{\dim\tau} \cdot \prod_{\substack{v \text{ pot.}\\ \text{mult.}}} (-1)^{\langle\chi_v,\tau_v\rangle},$$

where the three products run respectively over the real places of F, the finite places of F, and the finite places of F where E has potential multiplicative reduction.

Proof. By definition,

$$W(E,\tau) = \prod_v W(E/F_v, \tau_v), \tag{1.2}$$

where v runs over the places of F and $W(E/F_v,\tau_v)$ is defined as in [11], p. 329, formula (3.1). We will assemble formulas for the factors $W(E/F_v,\tau_v)$ and then insert them into (1.2).

First of all, if v is an infinite place, then

$$W(E/F_v,\tau_v) = (-1)^{\dim\tau} \qquad (v|\infty) \tag{1.3}$$

(cf. [11], p. 329, Theorem 2, part (i)). Next suppose that v is a finite place where E has potential multiplicative reduction. Then

$$W(E/F_v,\tau_v) = \det\tau_v(-1)\chi_v(-1)^{\dim\tau}(-1)^{\langle\chi_v,\tau_v\rangle} \qquad (v \text{ pot. mult.}) \tag{1.4}$$

(cf. [11], p. 329, Theorem 2, part (ii)). Finally, if v is a finite place where E has potential good reduction, then

$$W(E/F_v,\tau_v) = W(\sigma_{E/F_v} \otimes \tau_v), \tag{1.5}$$

because in the case of potential good reduction σ_{E/F_v} is identifiable with the representation σ'_{E/F_v} of the Weil-Deligne group $\mathcal{W}'(\overline{F}_v/F_v)$ which figures in

formula (3.1) of [11]. Furthermore, since $W(*)$ is insensitive to twists by real powers of ω_v we can combine (1.5) with Proposition 2 to obtain

$$W(E/F_v, \tau_v) = \det \tau_v(-1)\chi_v(-1)^{\dim \tau} \qquad (v \text{ pot. good}) \tag{1.6}$$

([11], p. 328, Proposition 7).

The proposition is now a consequence of (1.2), (1.3), (1.4), (1.6), and the following remark: If $\det \tau$ is regarded as an idele class character of F via the global counterpart to (1.1), then $\det \tau$ is trivial on the principal idele -1. Indeed this remark gives

$$\prod_{v \nmid \infty} \det \tau_v(-1) = \prod_{v \mid \infty} \det \tau_v(-1) = \prod_{v \text{ real}} \det \tau(c_v),$$

the second equality being an instance of (1.1). □

The following lemma enables us to evaluate the quantities $(-1)^{(r_1+r_2)\dim \tau}$, $\det \tau(c_v)$, and $\chi_v(-1)^{\dim \tau}$ appearing in Proposition 3 for most $\tau \in \mathcal{T}$. A subgroup of a group G is *central* if it is contained in the center of G.

Lemma. *Let G be a finite group, Q a central subgroup, and τ an irreducible self-dual complex representation of G of dimension > 1. If there is a normal subgroup P of G of odd order such that $G/(PQ)$ is cyclic, then* $\dim \tau$ *and* $[G : Q]$ *are even and* $\det \tau(c) = (-1)^{[G:Q]/2}$ *for every involution $c \in G$ with $c \notin Q$.*

Proof. We prove the lemma in six steps. If H is a subgroup of G, then ind_H^G and res_H^G denote the associated induction and restriction functors.

Step 1. *The group G/P is abelian.*

Indeed $(PQ)/P$ is a central subgroup of G/P with cyclic quotient.

Step 2. *There is a proper subgroup H of G containing PQ and a representation ξ of H such that $\tau \cong \mathrm{ind}_H^G \xi$.*

Let V be the space of τ and $V = W_1 \oplus W_2 \oplus \cdots \oplus W_r$ the decomposition of $\mathrm{res}_P^G \tau$ into isotypic subspaces for P. Since τ is irreducible the group G/P permutes the spaces W_i transitively, so τ is induced from the stabilizer H of W_1 in G. Furthermore H contains Q because $\mathrm{res}_Q^G \tau$ is scalar by Schur's lemma. It remains to see that H is a *proper* subgroup of G, or in other words that $r > 1$.

Suppose on the contrary that $r = 1$. Then $\mathrm{res}_P^G \tau$ is the direct sum of some number $m \geqslant 1$ of copies of an irreducible representation π of P. If $\pi = 1$ then τ factors through G/P, and since $\dim \tau > 1$ this contradicts the fact that an irreducible representation of an abelian group (Step 1) is one-dimensional. If $\pi \neq 1$, then the fact that the character $\mathrm{tr}\, \pi = m^{-1} \mathrm{tr}\, \tau | P$ is real-valued is also a contradiction, because a finite group of odd order has no nontrivial irreducible self-dual representations.

Step 3. *The subgroup P can be chosen to satisfy $[G : PQ] = 2^n$ with $n \geqslant 1$.*

By Step 1, G/P has a unique complement to its Sylow 2-subgroup. Let P' be the inverse image of this complement in G. After replacing P by P' we may assume that $[G : P]$ (hence also $[G : PQ]$) is a power of 2. If we write $[G : PQ] = 2^n$ with $n \geqslant 0$, then actually $n \geqslant 1$, because H in Step 2 is a proper subgroup of G.

Step 4. *Both $[G : Q]$ and $\dim \tau$ are even.*

That $[G : Q]$ is even follows from Step 3, while Steps 2 and 3 together give $\dim \tau = [G : H] \dim \xi = 2^m \dim \xi$ with $1 \leqslant m \leqslant n$.

Step 5. *A reduction: Let P and n be as in Step 3, and suppose that $c \in G$ is an involution with $c \notin Q$. To prove the stated formula for $\det \tau(c)$ we may assume without loss of generality that there is an element $g \in G$ of order 2^n such that gPQ generates $G/(PQ)$.*

Put $G' = G/Q^2$, $P' = (PQ^2)/Q^2$, and $Q' = Q/Q^2$. Since $\mathrm{res}^G_Q \tau$ is both scalar and self-dual, it maps each element of Q to scalar multiplication by ± 1. Hence τ factors through G' to give an irreducible self-dual representation τ' of G'. Furthermore, if c' denotes the image of c in G', then c' is an involution, $c' \notin Q'$, and $\det \tau'(c') = \det \tau(c)$, while $[G' : Q'] = [G : Q]$. The gain here is that Q' has exponent dividing 2. So returning to G, P, Q, c, and τ, we may assume that $Q^2 = \{1\}$.

Now choose $g \in G$ so that gPQ generates $G/(PQ)$. Then the order of g is divisible by 2^n, and after replacing g by an odd power we may assume that the order of g is a power of 2. In fact since P has odd order we see that $g^{2^n} \in Q$, whence the order of g is either 2^n or 2^{n+1}. Let $\langle g \rangle$ denote the subgroup generated by g. Then the group $S = \langle g \rangle Q$ is a Sylow 2-subgroup of G, and if g has order 2^{n+1}, then the involutions in S are precisely the elements of Q. In view of the conjugacy of Sylow 2-subgroups and the centrality of Q we deduce that if the order of g is 2^{n+1}, then all involutions in G belong to Q, contradicting the existence of c. Therefore g has order 2^n.

Step 6. *If $c \in G \smallsetminus Q$ is an involution, then $\det \tau(c) = (-1)^{[G:Q]/2}$.*

We remark at the outset that $\det \tau$ is trivial on PQ. Indeed as τ is self-dual so is $\det \tau$; thus $(\det \tau)^2 = 1$ and consequently the restriction of $\det \tau$ to the odd-order group P is trivial. On the other hand, $\mathrm{res}^G_Q \tau$ is both scalar and self-dual, whence for any $q \in Q$ we have $\det \tau(q) = (\pm 1)^{\dim \tau}$, which is 1 by Step 4.

We shall use a standard formula for the determinant of an induced representation (cf. [7] or [4], p. 508). With H and ξ as in Step 2, write $\mathrm{sgn}_{G/H}$ for the determinant of the permutation representation of G on the cosets of H. Also let trans^G_H denote the transfer from G^{ab} to H^{ab} (the superscript "ab"

indicates the quotient of the given group by its commutator subgroup). Then

$$\det \tau = (\mathrm{sgn}_{G/H})^{\dim \xi} \cdot (\det \xi \circ \mathrm{trans}_H^G), \tag{1.7}$$

where $\det \tau$ and $\mathrm{sgn}_{G/H}$ are viewed as characters of G^{ab} and $\det \xi$ as a character of H^{ab}.

To compute $\det \tau(c)$ we consider cases according as $c \in H$ or $c \notin H$. Suppose first that $c \in H$. Since $c \notin PQ$ (else $c = c^{|P|} \in Q$) we see that $PQ \subsetneq H$ and hence that $PQ \subsetneq H \subsetneq G$. Therefore $n \geqslant 2$ in Step 3. Thus $4|[G : Q]$ and we must show that $\det \tau(c) = 1$. Now we have already remarked that $\det \tau$ is trivial on PQ, so it suffices to see that $\det \tau(c') = 1$ for some $c' \in cPQ$. Furthermore $\mathrm{sgn}_{G/H}$ factors through G/H and so in particular is trivial on cPQ. Hence by (1.7) it suffices to see that $\mathrm{trans}_H^G(c') = 1$ for some $c' \in cPQ$.

Let g be as in Step 5, and put

$$h = g^{2^{n-1}}.$$

The cosets cPQ and hPQ both generate the unique subgroup of order 2 in $G/(PQ)$; hence they coincide. In other words we may take $c' = h$. Write $[G : H] = 2^m$ with $m \geqslant 1$. Then the elements g^i $(0 \leqslant i \leqslant 2^m - 1)$ form a set of representatives for the distinct cosets of H in G. Since h is a power of g and $m \geqslant 1$ we have

$$\prod_{i=0}^{2^m-1} g^i h g^{-i} = h^{2^m} = 1,$$

which gives the desired result: $\mathrm{trans}_H^G(h) = 1$.

Next suppose that $c \notin H$. Since τ is induced from H and H is normal in G it follows that $\mathrm{tr}\, \tau(c) = 0$. To make efficient use of this fact we will use, in preference to (1.7), an easily verified formula for the determinant of an involution:

$$\det \tau(c) = (-1)^{(\dim \tau - \mathrm{tr}\, \tau(c))/2}. \tag{1.8}$$

Now as $G/(PQ)$ is a cyclic group of order 2^n, its nontrivial subgroups all contain the unique element of order two, namely cPQ. Hence the fact that $c \notin H$ means that $H/(PQ)$ is trivial; in other words, $H = PQ$. Thus $\dim \tau = [G : PQ] \dim \xi$. As $[G : PQ]$ is even and differs from $[G : Q]$ by an odd factor we deduce that $\dim \tau \equiv [G : Q] \dim \xi$ modulo 4, whence the exponent of -1 on the right-hand side of (1.8) can be replaced by $[G : Q](\dim \xi)/2$ (recall that $\mathrm{tr}\, \tau(c) = 0$). Thus to complete Step 6 it suffices to verify that $\dim \xi$ is odd. But ξ is irreducible (for it induces τ), hence so is $\mathrm{res}_P^H \xi$ (because $H = PQ$ and $\mathrm{res}_Q^H \xi$ is scalar). Thus $\dim \xi$ divides $|P|$, which is odd. □

Before applying the lemma we introduce some notation. Let A and Z denote respectively the subgroups of diagonal matrices and of scalar matrices in $\mathrm{GL}(2,\mathbb{Z}_p)$, and write A_n, B_n, U_n, and Z_n for the images of A, B, U, and Z in $\mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$. To avoid confusion, the reader should note that the letters A and Z are consistent with Lie-theoretic notational conventions, but the letters B and U only partially so: B and U are not the standard Borel and unipotent subgroups of $\mathrm{GL}(2,\mathbb{Z}_p)$ but merely the inverse images in $\mathrm{GL}(2,\mathbb{Z}_p)$ of such subgroups of $\mathrm{GL}(2,\mathbb{F}_p)$.

We also recall the notation $w = |\overline{\Gamma}_1|$. It is convenient to set $w_n = |\overline{\Gamma}_n|$ for $n \geqslant 1$, so that $w = w_1$. Then

$$w_n \equiv \pm w \pmod 4, \tag{1.9}$$

because the order of the kernel of reduction $\mathrm{PGL}(2,\mathbb{Z}/p^n\mathbb{Z}) \to \mathrm{PGL}(2,\mathbb{Z}/p\mathbb{Z})$ is p^{3n-3} and hence odd.

Proposition 4. *If $\tau \in \mathcal{T}$ and $\dim \tau > 1$, then $\dim \tau$ and w are even and $\det \tau(c_v) = (-1)^{w/2}$ for each real place v of F.*

Proof. Choose n so that $\tau \in \mathcal{T}_n$, put $G = \mathrm{Gal}(R_n/F)$, and view τ as a representation of G. We may likewise view ρ_n as a representation of G and in fact as an isomorphism of G onto $\Gamma_n \subset B_n$. Since U_n is normal in B_n and of p-power (hence odd) order it follows that the subgroup $P = \rho_n^{-1}(U_n)$ of G is also normal of odd order, while the subgroup $Q = \rho_n^{-1}(Z_n)$ is central because Z_n is central in $\mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$. Furthermore $\rho_n^{-1}(U_nZ_n) = PQ$. Indeed if $\rho_n(g) = uz$ with $g \in G$, $u \in U_n$, $z \in Z_n$, and $z^{p-1} = 1$ (this last condition being satisfied once we replace u and z by uz^{1-p^n} and z^{p^n} respectively), then $\rho_n(g^{p^n}) = z$, whence also $\rho_n(g^{1-p^n}) = u$. Thus ρ_n defines an embedding of $G/(PQ)$ into the group $B_n/(U_nZ_n) \cong A_1/Z_1$, which is isomorphic to $\mathbb{F}_p^\times$ and hence cyclic. It follows that $G/(PQ)$ is cyclic also.

The lemma now implies that $\dim \tau$ and $[G : Q]$ are even. But $\overline{\rho}_n$ induces an isomorphism of G/Q onto $\overline{\Gamma}_n$, so $[G : Q] = w_n$, and thus w is even by (1.9). As for $\det \tau(c_v)$, recall that we are viewing τ as a representation of G. If we likewise treat the involution $c_v \in \mathrm{Gal}(\overline{F}/F)$ as an element of G, then $c_v \notin Q$, because $\rho(c_v)$ has eigenvalues 1 and -1 (hence trace 0) and so does not reduce to a scalar matrix mod p^n. The formula for $\det \tau(c_v)$ now follows from (1.9) and the lemma. □

Proposition 5. *If $\tau \in \mathcal{T}$ and $\dim \tau > 1$, then*

$$W(E,\tau) = (-1)^{(p-1)[F:\mathbb{Q}]/2} \cdot \delta(E,\tau)$$

with $\delta(E,\tau) = \prod_{v \text{ pot. mult.}} (-1)^{\langle \chi_v, \tau_v \rangle}$.

Proof. Propositions 3 and 4 give

$$W(E,\tau) = (-1)^{wr_1/2} \cdot \delta(E,\tau),$$

so it suffices to see that wr_1 and $(p-1)[F:\mathbb{Q}]$ are congruent modulo 4, or equivalently (since w is even and $r_1 \equiv [F:\mathbb{Q}] \bmod 2$) that

$$w[F:\mathbb{Q}] \equiv (p-1)[F:\mathbb{Q}] \pmod 4. \tag{1.10}$$

Let $\overline{B}_1$ denote the image of B_1 in $\mathrm{PGL}(2,\mathbb{F}_p)$. Then $|\overline{B}_1| = p(p-1)$, and since $\overline{\Gamma}_1$ is a subgroup of $\overline{B}_1$ it follows that w divides $p(p-1)$.

Suppose first that $p \equiv 3 \bmod 4$. Then the fact that w is even and divides $p(p-1)$ implies that $w \equiv 2 \bmod 4$, and (1.10) follows. Next suppose that $p \equiv 1 \bmod 4$. We must show that $w[F:\mathbb{Q}] \equiv 0 \bmod 4$. This is immediate if $[F:\mathbb{Q}]$ is even, so we may assume that $[F:\mathbb{Q}]$ is odd. Then the image of the cyclotomic character $\mathrm{Gal}(R_1/F) \to \mathbb{F}_p^\times$ contains the Sylow 2-subgroup of $\mathbb{F}_p^\times$, and therefore the composition of the cyclotomic character with the natural map $\mathbb{F}_p^\times \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ is surjective. Since $\det\rho_1$ is the cyclotomic character we deduce that the determinant induces a surjective map $\overline{\Gamma}_1 \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$. Let $\gamma \in \Gamma_1$ be an element of 2-power order such that $\det\gamma$ is not a square. To complete the proof it suffices to see that the image of γ in $\overline{\Gamma}_1$ has order divisible by 4. Suppose on the contrary that γ^2 is scalar. Then the diagonal entries of the upper triangular matrix γ are λ and $-\lambda$ for some $\lambda \in \mathbb{F}_p^\times$. Then $\det\gamma = -\lambda^2 \in \mathbb{F}_p^{\times 2}$, contradicting the choice of γ. □

Theorem 1 is immediate from Proposition 5, for if E has potential good reduction, then $\delta(E,\tau) = 1$.

2. Proof of Theorem 2. Our assumption that E does not have complex multiplication (unused so far, but henceforth essential) implies that Γ is open in $\mathrm{GL}(2,\mathbb{Z}_p)$ (Serre [13], p. IV-11). However, apart from this point, the proof of Theorem 2 has nothing to do with elliptic curves. In fact one step of the argument forces us to reformulate Theorem 2 so as to eliminate any reference to E. This is the purpose of Proposition 6 below, in which Γ is simply an open subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$ contained in B. As usual, a subscript n on an element or subset of $\mathrm{GL}(2,\mathbb{Z}_p)$ denotes reduction modulo p^n. In particular, Γ_n is the reduction of Γ modulo p^n. Also $\overline{\Gamma}_n$ is the image of Γ_n in $\mathrm{PGL}(2,\mathbb{Z}/p^n\mathbb{Z})$. Put $w = |\overline{\Gamma}_1|$ and $b = |\Gamma_1 \cap \{\pm 1\}|$. As before, A and Z denote the subgroups of diagonal and of scalar matrices in $\mathrm{GL}(2,\mathbb{Z}_p)$.

Throughout this section, *representation* means *complex representation*. Given a finite group G, we put

$$\vartheta(G) = \sum_{[\tau]} \dim\tau, \tag{2.1}$$

where the sum runs over isomorphism classes $[\tau]$ of irreducible self-dual representations τ of G.

Proposition 6. *The asymptotic behavior of $\vartheta(\Gamma_n)$ is as follows:*

(a) *If w is odd then $\vartheta(\Gamma_n) = b$ for all $n \geqslant 1$.*

(b) *If Γ_1 contains a nonscalar involution, then there is a constant $a > 0$ such that $\vartheta(\Gamma_n) = a \cdot p^{2n} + b$ for n sufficiently large.*

(c) *If w is even but Γ_1 does not contain a nonscalar involution, then there is a constant $a > 0$ such that $\vartheta(\Gamma_n) = a \cdot p^{2n}$ for n sufficiently large.*

In the application to elliptic curves, $\mathrm{Gal}(R_n/F) \cong \Gamma_n$, so $\vartheta_n = \vartheta(\Gamma_n)$ and Theorem 2 follows from Proposition 6.

We begin the proof of the proposition by fixing a Sylow 2-subgroup S_1 of Γ_1. Then S_1 is a 2-subgroup of B_1, hence conjugate in B_1 to a subgroup of A_1 (for A_1 contains a Sylow 2-subgroup of B_1). It follows in particular that S_1 is abelian.

More generally, for $n \geqslant 1$ let us define Sylow 2-subgroups S_n of Γ_n so that reduction mod p^n gives isomorphisms $S_{n+1} \cong S_n$. This is possible because the reduction map $\Gamma_{n+1} \to \Gamma_n$ is surjective with kernel of p-power order. Hence any choice of S_{n+1} reduces mod p^n to a conjugate of S_n, and the inverse conjugation can then be lifted to Γ_{n+1}. We put $S = \varprojlim S_n \subset \Gamma$, so that $S \cong S_n$ for all n.

A similar remark pertains to the quantity b. If $b = 2$, then $\gamma \equiv -1 \bmod p$ for some $\gamma \in \Gamma$, and since Γ is closed in $\mathrm{GL}(2, \mathbb{Z}_p)$ it follows that the limit

$$-1 = \lim_{n \to \infty} \gamma^{p^n} \tag{2.2}$$

also belongs to Γ. Thus $b = |\Gamma \cap \{\pm 1\}| = |\Gamma_n \cap \{\pm 1\}|$ for all $n \geqslant 1$.

Part (a) of Proposition 6 is a consequence of the following slightly more precise statement:

Proposition 7. *If w is odd, then an irreducible self-dual representation of Γ_n is a one-dimensional character, and the number of such characters is b.*

Proof. Let Z_n' be the Sylow 2-subgroup of $Z_n \cap \Gamma_n$ and Z_n'' its unique complement, so that $Z_n \cap \Gamma_n = Z_n' \times Z_n''$. If w is odd, then so is the quantity $w_n = |\overline{\Gamma}_n|$ (cf. (1.9), which is still valid in the present context) and therefore $|\Gamma_n / Z_n'|$ is odd too. Hence $H^2(\Gamma_n/Z_n', Z_n') = 0$, and consequently

$$\Gamma_n \cong (\Gamma_n / Z_n') \times Z_n'.$$

With respect to this decomposition any irreducible representation τ of Γ_n has the form of an external tensor product, $\tau \cong \pi \boxtimes \psi$, with irreducible representations π and ψ of Γ_n/Z_n' and Z_n' respectively. Furthermore, τ is self-dual if and only if π and ψ are. But Γ_n/Z_n' has odd order, so a self-dual π is trivial. Furthermore, Z_n' is cyclic of order 2^m for some m, so ψ is one-dimensional, and ψ is self-dual if and only if $\psi^2 = 1$. The number of such ψ is 1 or 2 according as $m = 0$ or $m > 0$, and these conditions are equivalent to $b = 1$ and $b = 2$ respectively. □

Henceforth we assume that w is even. For a finite group G define quantities $\vartheta_{\mathrm{orth}}(G)$ and $\vartheta_{\mathrm{symp}}(G)$ by restricting the summation in (2.1) to orthogonal and symplectic τ respectively. Then

$$\vartheta(G) = \vartheta_{\mathrm{orth}}(G) + \vartheta_{\mathrm{symp}}(G). \tag{2.3}$$

On the other hand, the Frobenius-Schur theorem gives

$$\mathrm{FS}(G) = \vartheta_{\mathrm{orth}}(G) - \vartheta_{\mathrm{symp}}(G), \tag{2.4}$$

where $\mathrm{FS}(G)$ is the number of solutions $x \in G$ to the equation $x^2 = 1$ (cf. [15], p. 110, Ex. 13.11). To compute $\vartheta(\Gamma_n)$ we first compute $\mathrm{FS}(\Gamma_n)$.

Let C be the set of nonscalar involutions in S. Then the image of C under reduction modulo p^n is the set of nonscalar involutions in S_n. In particular, Γ_1 contains a nonscalar involution if and only if $C \neq \emptyset$, so that cases (b) and (c) of Proposition 6 correspond respectively to $C \neq \emptyset$ and $C = \emptyset$. We claim that

$$\mathrm{FS}(\Gamma_n) = b + \sum_{c \in C} |\mathrm{Conj}(c_n)|, \tag{2.5}$$

where $\mathrm{Conj}(c_n)$ denotes the conjugacy class of c_n in Γ_n.

Before verifying (2.5), we remark that the sum on the right-hand side has at most two terms. Indeed we have seen that S is isomorphic to a subgroup of A_1 (via an isomorphism sending -1 to -1), so it suffices to observe that A_1 has just two nonscalar involutions: they are ι_1 and $-\iota_1$, where we define $\iota \in A$ by

$$\iota = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.6}$$

It should be added that ι_n and $-\iota_n$ are nonconjugate in B_n, so that if $|C| = 2$ then the two elements of C are *a fortiori* nonconjugate in Γ_n.

We can now verify (2.5). The number of scalar solutions to $x^2 = 1$ in Γ_n is b, and if $x \in \Gamma_n$ is a nonscalar solution then by the Sylow theorems x is conjugate to a nonscalar involution in S_n. In other words, $x \in \mathrm{Conj}(c_n)$ for some $c \in C$, and in fact for a unique c by virtue of the remark at the end of the previous paragraph. This completes the proof of (2.5).

Lemma. *Let c be a nonscalar involution in $\mathrm{GL}(2, \mathbb{Z}_p)$. Then there is an element $g \in \mathrm{GL}(2, \mathbb{Z}_p)$ such that the centralizer of c_n in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is $g_n A_n g_n^{-1}$ for $n \geqslant 1$.*

Proof. Let us identify a linear automorphism of $\mathbb{Z}_p^2$ with its matrix relative to the standard basis. Then $\mathbb{Z}_p^2$ is the direct sum of the respective images of $(1 + c)/2$ and $(1 - c)/2$, which are both nonzero submodules and therefore both free of rank one. Hence there is an element $g \in \mathrm{GL}(2, \mathbb{Z}_p)$ such that $c = g\iota g^{-1}$ with ι as in (2.5), and then $c_n = g_n \iota_n g_n^{-1}$ for all n. An elementary

calculation shows that the centralizer of ι_n is A_n, whence the centralizer of c_n is $g_n A_n g_n^{-1}$. □

Recall that M denotes the additive group of 2×2 matrices over $\mathbb{Z}_p$ and that $K(n) = 1 + p^n M$ for $n \geqslant 1$. Since Γ is open in $\mathrm{GL}(2, \mathbb{Z}_p)$ there is an integer $n_0 \geqslant 1$ such that Γ contains $K(n_0)$.

Proposition 8. *If $C \neq \emptyset$ then there is a constant $a > 0$ such that*

$$\mathrm{FS}(\Gamma_n) = a \cdot p^{2n} + b$$

for n sufficiently large. If $C = \emptyset$ then $\mathrm{FS}(\Gamma_n) = b$ for all n.

Proof. The second statement is immediate from (2.5). Suppose now that $c \in C$ is given. We will show that there is a constant $a(c) > 0$ such that

$$|\mathrm{Conj}(c_n)| = a(c) p^{2n} \tag{2.7}$$

if n is sufficiently large. In view of (2.5) this will prove the proposition.

As noted above, there is an integer $n_0 \geqslant 1$ such that Γ contains $K(n_0)$. Thus for $n \geqslant n_0$ we can write

$$|\Gamma_n| = [\Gamma : K(n_0)][K(n_0) : K(n)].$$

As $[K(n_0) : K(n)] = [(1 + p^{n_0} M) : (1 + p^n M)] = p^{4(n-n_0)}$ we deduce that

$$|\Gamma_n| = a_0 p^{4n} \tag{2.8}$$

with $a_0 = [\Gamma : K(n_0)]/p^{4n_0}$. On the other hand, let $\mathrm{Cent}(c_n)$ denote the centralizer of c_n in Γ_n. We claim that there is a constant $a_1 > 0$ such that

$$|\mathrm{Cent}(c_n)| = a_1 p^{2n} \tag{2.9}$$

for n sufficiently large. Verification of the claim will complete the proof, for (2.8) and (2.9) give (2.7) with $a(c) = a_0/a_1$.

By the lemma there exists $g \in \mathrm{GL}(2, \mathbb{Z}_p)$ such that

$$\mathrm{Cent}(c_n) = (g_n A_n g_n^{-1}) \cap \Gamma_n \tag{2.10}$$

for all $n \geqslant 1$. Let $D \subset M$ be the additive group of 2×2 diagonal matrices over $\mathbb{Z}_p$, and let D_n be the reduction of D modulo p^n. If $n \geqslant n_0$, then Γ_n contains the image of $K(n_0)$ in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, and consequently $\mathrm{Cent}(c_n)$ contains $g_n(1 + p^{n_0} D_n) g_n^{-1}$. Now reduction modulo p^{n_0} defines a map

$$r_n : \mathrm{Cent}(c_n)/g_n(1 + p^{n_0} D_n) g_n^{-1} \longrightarrow \mathrm{Cent}(c_{n_0}),$$

and it follows from (2.10) that r_n is an embedding. Since r_{n+1} factors through r_n while $\mathrm{Cent}(c_{n_0})$ is a finite group we deduce that if n is sufficiently large, then the image of r_n is independent of n. Thus if n is sufficiently large, then the first factor on the right-hand side of the equation

$$|\mathrm{Cent}(c_n)| = [\mathrm{Cent}(c_n) : g_n(1 + p^{n_0} D_n) g_n^{-1}] |1 + p^{n_0} D_n|$$

is a constant a_2 independent of n. Since the second factor is $p^{2(n-n_0)}$ we obtain (2.9) with $a_1 = a_2 p^{-2n_0}$. □

Part (b) of Proposition 6 is now a consequence of (2.3), (2.4), Proposition 8, and the following result:

Proposition 9. *If $C \neq \emptyset$, then every irreducible self-dual representation of Γ_n is orthogonal.*

As with so many other arguments involving the Schur index, the proof of Proposition 9 is a reduction to a statement about hyperelementary subgroups. More specifically, we shall reduce Proposition 9 to a statement about subgroups H which are $\mathbb{R}$-*elementary at* 2, or in other words which have the form $H \cong O \rtimes T$ with a 2-group T and a cyclic group O of odd order satisfying the following condition: Given elements o and o' of O conjugate in H, we have $o' = o$ or $o' = o^{-1}$ (cf. [5], p. 71). It follows from the Brauer-Witt theory of virtual characters that if a finite group G has an irreducible symplectic representation, then there is a subgroup H of G which is $\mathbb{R}$-elementary at 2 and has an irreducible symplectic representation also; cf. [5], p. 85, (16.1). (To deduce our assertion from [5], note that a character ξ is symplectic if and only only if its Schur index $m_{\mathbb{R}}(\xi)$ with respect to $\mathbb{R}$ is 2. Furthermore, a group H is $\mathbb{C}$-*elementary at* 2 provided it is a direct product $O \times T$ with O and T as above. Hence such a group is also $\mathbb{R}$-elementary at 2.)

In the following proposition we fix $n \geqslant 1$ and put $G = \Gamma_n / W^2$ with $W = S_n \cap Z_n$. If τ is an irreducible self-dual representation of Γ_n, then $\tau | W$ is scalar multiplication by a character $W \to \{\pm 1\}$. Hence τ factors through G, and it suffices to prove Proposition 9 with Γ_n replaced by G. The previous paragraph provides a further reduction to the following statement:

Proposition 10. *Assume that $C \neq \emptyset$, and let H be a subgroup of G which is $\mathbb{R}$-elementary at 2. Then every irreducible self-dual representation of H is orthogonal.*

Proof. Write $H = O \rtimes T$ as above. Since S_n / W^2 is a Sylow 2-subgroup of G there exists $g \in G$ such that gTg^{-1} is contained in S_n / W^2, and after replacing H by gHg^{-1} we may assume that T itself is contained in S_n / W^2. In particular, T is a subquotient of S_n and is therefore abelian. Hence if the semidirect product $O \rtimes T$ is actually direct, then H is abelian and the proposition follows. We may therefore assume that the map $f : T \to \mathrm{Aut}(O)$ underlying the semidirect product is nontrivial. Furthermore, since O is cyclic an automorphism of O is determined by its effect on a generator. We conclude that the image of f consists of two elements: the identity and the automorphism $o \mapsto o^{-1}$. Put $K = \mathrm{Ker}\, f$; then $[T : K] = 2$.

Suppose now that τ is an irreducible self-dual representation of H. If $\dim \tau = 1$, then the orthogonality of τ is immediate, so suppose that $\dim \tau >$

1. Then the fact that H is a semidirect product $O \rtimes T$ with O and T abelian implies that we can write τ as an induced representation of the form $\tau = \mathrm{ind}_I^H \xi$, where I is a proper subgroup of H containing the centralizer of O in H and ξ is a one-dimensional character of I (cf. [15], p. 62, Prop. 25). But the centralizer of O in H is precisely the subgroup $O \times K$ of index 2 in H. Hence $I = O \times K$.

We claim that there is an involution $t \in T$ which represents the nonidentity coset of K in T and hence also the nonidentity coset of I in H. Granting this claim temporarily, we complete the proof of the proposition as follows. Let $\mathrm{sgn}_{H/I}$ be the permutation representation of H on the cosets of I, and let trans_I^H be the transfer from H^{ab} to I^{ab}. Then

$$\det \tau = \mathrm{sgn}_{H/I} \cdot (\xi \circ \mathrm{trans}_I^H)$$

(cf. (1.7)). Furthermore $\mathrm{sgn}_{H/I}(t) = -1$ (because t represents the nontrivial coset of I in H) and $\mathrm{trans}_I^H(t) = \mathrm{trans}_K^T(t) = 1$ (because, in addition, t is an involution). Therefore $\det \tau(t) = -1$. Since a symplectic representation has trivial determinant we conclude that τ is orthogonal.

It remains to prove the claim. We will show more generally that *any* $t \in T \smallsetminus K$ is an involution. Since $T \subset S_n/W^2$ by assumption, given $t \in T \smallsetminus K$ we can write $t = s_n W^2$ with $s \in S$, where s_n is the reduction of s modulo p^n. Note in particular that the order of s is a power of 2. We must show that $s_n^2 \in W^2$.

Choose $y \in \Gamma_n$ so that yW^2 is a nonidentity element of O. Then yW^2 has odd order > 1, and after replacing y by y^{2^m} for some integer $m \geqslant 0$ we may assume that y itself has odd order > 1. Now as $t \notin K$ the automorphism $f(t)$ is not the identity, and therefore $s_n y s_n^{-1} W^2 = y^{-1} W^2$. But W is a central 2-group, whereas y has odd order, so we get $s_n y s_n^{-1} = y^{-1}$. Thus

$$s_n(y - y^{-1})s_n^{-1} = -(y - y^{-1}), \tag{2.11}$$

where $y - y^{-1}$ is now viewed as a nonzero element of the additive group M_n of 2×2 matrices over $\mathbb{Z}/p^n\mathbb{Z}$.

Let $\nu \geqslant 0$ be the integer $\leqslant n-1$ for which $y - y^{-1} \in p^\nu M_n$ but $y - y^{-1} \notin p^{\nu+1} M_n$. Put $X = p^\nu M$ and define a $\mathbb{Z}_p$-linear automorphism $\mathrm{Ad}(s)$ of X by $\mathrm{Ad}(s)(x) = sxs^{-1}$ for $x \in X$. Then $\mathrm{Ad}(s)$ modulo p is an $\mathbb{F}_p$-linear automorphism of X/pX, and according to (2.11) the image of $y - y^{-1}$ under the natural map $p^\nu M_n \to X/pX$ is a nonzero eigenvector of $\mathrm{Ad}(s)$ mod p with eigenvalue -1 mod p.

On the other hand, s is an element of Γ of 2-power order, and it is nonscalar (else $\mathrm{Ad}(s)$ is the identity). Hence s is semisimple with distinct eigenvalues, say ω, ω', both roots of unity of 2-power order. It follows that the eigenvalues

of $\mathrm{Ad}(s)$ are $\omega^{-1}\omega'$, $(\omega')^{-1}\omega$, and 1 (with multiplicity 2). Reducing the characteristic polynomial of $\mathrm{Ad}(s)$ mod p we see that one of these eigenvalues is congruent to -1 mod p. It may appear *a priori* that the congruence should be taken modulo $\mathfrak{p}$, the maximal ideal of the ring of integers of an algebraic closure of $\mathbb{Q}_p$, but it is easy to see directly that $\omega, \omega' \in \mathbb{Q}_p$, and this will actually follow from the remainder of the argument. In any case, since $1 \not\equiv -1$ mod p we deduce that $\omega' \equiv -\omega$, and the congruence can be replaced by an equality because reduction mod $\mathfrak{p}$ is injective on roots of unity of order prime to p. Now $s \in S$ by construction, and by hypothesis there is also a nonscalar involution $c \in S$. As S is abelian it follows that s (with eigenvalues ω and $-\omega$) and c (with eigenvalues 1 and -1) are simultaneously diagonalizable. Regardless of the order in which each pair of eigenvalues is listed, we deduce that the element $sc \in S$ is scalar and that $(sc)^2 = s^2$. Thus $s_n c_n$ belongs to the subgroup $S_n \cap Z_n = W$ and $(s_n c_n)^2 = s_n^2$, so $s_n^2 \in W^2$. □

Remark. As far as the application to elliptic curves is concerned, if the base field F has at least one real place, then $C \neq \emptyset$, and hence the proof of Theorem 2 is completed by Proposition 10.

It remains to prove part (c) of Proposition 6. We have seen that $b = |\Gamma \cap \{\pm 1\}| = |\Gamma_n \cap \{\pm 1\}|$ for all $n \geqslant 1$, and the same argument (with p replaced by a power of p in (2.2)) shows that $|S \cap Z| = |S_n \cap Z_n|$. Hence the isomorphism $S \to S_n$ afforded by reduction modulo p^n determines an isomorphism $S/(S \cap Z) \to S_n/(S_n \cap Z_n)$, and since w is even we can choose an element $s \in S$ such that $s^2 \in Z$ but $s \notin Z$. Furthermore $s^2 \neq 1$ because $C = \emptyset$. The eigenvalues of s are then ω and $-\omega$ for some 2-power root of unity $\omega \neq \pm 1$. We claim that $\omega \in \mathbb{Q}_p$. Indeed $s_1 \in \Gamma_1 \subset B_1$, so the eigenvalues of s_1 belong to $\mathbb{F}_p$, and reduction mod $\mathfrak{p}$ defines a Galois-equivariant isomorphism on roots of unity of order prime to p.

The fact that $\omega \in \mathbb{Q}_p$ allows us to define a scalar matrix $\tilde{s} \in \mathrm{GL}(2, \mathbb{Z}_p)$ by $\tilde{s} = \omega \cdot 1$. We also put

$$\widetilde{\Gamma} = \Gamma \cup \tilde{s}\,\Gamma. \tag{2.12}$$

This is a subgroup of B because $\tilde{s}$ is scalar and $\tilde{s}^2 = s^2 \in \Gamma$. Note also that the element $s^{-1}\tilde{s} \in \widetilde{\Gamma}$ is a nonscalar involution.

Proposition 11. *Let τ be an irreducible self-dual representation of Γ_n. The following are equivalent:*

(i) $\tau(s_n^2) = 1$.
(ii) *There is an extension of τ to an irreducible self-dual representation $\tilde{\tau}$ of $\widetilde{\Gamma}_n$.*
(iii) *τ is orthogonal.*

Furthermore, if these equivalent conditions hold, then there are exactly two distinct isomorphism classes $[\tilde{\tau}]$ *of extensions of* τ *in* (ii).

Before proving Proposition 11 let us see how part (c) of Proposition 6 follows from it. As we have already noted, $\widetilde{\Gamma}$ contains a nonscalar involution, namely $s^{-1}\tilde{s}$, and therefore Proposition 9 and part (b) of Proposition 6 are applicable with Γ replaced by $\widetilde{\Gamma}$ and b replaced by $\tilde{b} = |\widetilde{\Gamma} \cap \{\pm 1\}|$. Furthermore the fact that s^2 is a nonidentity scalar matrix in Γ of 2-power order gives $b = 2$ and *a fortiori* $\tilde{b} = 2$. Hence there is a constant $\tilde{a} > 0$ such that

$$\vartheta_{\mathrm{orth}}(\widetilde{\Gamma}_n) = \vartheta(\widetilde{\Gamma}_n) = \tilde{a} \cdot p^n + 2 \tag{2.13}$$

for n sufficiently large. On the other hand, if $\tilde{\tau}$ is an irreducible orthogonal representation of $\widetilde{\Gamma}_n$, then the restriction $\tau = \tilde{\tau}|\Gamma_n$ is also irreducible orthogonal, the irreducibility being a consequence of (2.12) and the fact that $\tilde{\tau}(\tilde{s})$ is scalar by Schur's lemma. Proposition 11 then tells us that the resulting function $[\tilde{\tau}] \mapsto [\tau]$ is a two-to-one map from the set of isomorphism classes of irreducible orthogonal representations of $\widetilde{\Gamma}_n$ onto the corresponding set for Γ_n. (We are also using Proposition 9 here: for $\tilde{\tau}$, orthogonal is the same as self-dual.) Returning to (2.13), we see that

$$\vartheta_{\mathrm{orth}}(\Gamma_n) = (\tilde{a}/2) \cdot p^n + 1 \tag{2.14}$$

for n sufficiently large. On the other hand, recalling that $b = 2$ we have

$$\vartheta_{\mathrm{orth}}(\Gamma_n) - \vartheta_{\mathrm{symp}}(\Gamma_n) = 2 \tag{2.15}$$

by Proposition 8. Combining (2.3), (2.14), and (2.15) we obtain part (c) of Proposition 6 with $a = \tilde{a}$.

We turn now to the proof of Proposition 11. The implication (ii) $\Rightarrow$ (iii) is immediate from the fact that an irreducible self-dual representation of $\widetilde{\Gamma}_n$ is orthogonal. The implication (i) $\Rightarrow$ (ii) is also straightforward: Given τ with $\tau(s_n^2) = 1$, we define $\tilde{\tau}$ by the requirements $\tilde{\tau}|\Gamma_n = \tau$ and $\tilde{\tau}(\tilde{s}_n) = \pm 1$ (cf. (2.12)). That $\tilde{\tau}$ is a representation follows from the fact that $\tilde{s}_n$ is central and $\tilde{s}_n^2 = s_n^2$, while the irreducibility of $\tilde{\tau}$ follows from that of τ and the self-duality likewise: given $g \in \Gamma_n$ we have $\operatorname{tr}\tilde{\tau}(g) = \operatorname{tr}\tau(g) \in \mathbb{R}$ and $\operatorname{tr}\tilde{\tau}(\tilde{s}_n g) = \pm\operatorname{tr}\tau(g) \in \mathbb{R}$. The two choices inherent in writing $\tilde{\tau}(\tilde{s}_n) = \pm 1$ yield distinct central characters of $\tilde{\tau}$ and hence distinct isomorphism classes $[\tilde{\tau}]$, and these two choices are the only ones possible given that $\tau(s_n^2) = 1$ and that $\tilde{\tau}(\tilde{s}_n)$ must be scalar by Schur's lemma. Hence there are indeed exactly two distinct isomorphism classes $[\tilde{\tau}]$ in (ii).

It remains to prove the implication (iii) $\Rightarrow$ (i). If $\dim\tau = 1$, then τ is a character $\Gamma_n \to \{\pm 1\}$ and (i) is immediate. Hence we may assume that $\dim\tau > 1$. Then $\dim\tau$ is even by Proposition 4 (or strictly speaking by the lemma preceding Proposition 4, which can be applied with $P = \Gamma_n \cap U_n$ and

$Q = \Gamma_n \cap Z_n$). The crux of the argument will once again be a reduction to the case of hyperelementary subgroups.

Fix n and put $G = \Gamma_n/W^2$ with $W = S_n \cap Z_n$, as before. Then τ factors through G, also as before, and the subgroup $L = W/W^2$ of G contains the element $s_n^2 W$. Hence it suffices to prove the following:

Proposition 12. *Let τ be an irreducible orthogonal representation of G of even dimension. Then τ is trivial on L.*

Proof. The group L is a central subgroup of G of order 2, for it is the quotient W/W^2 of the cyclic 2-group $W = S_n \cap Z_n$, and W is central in Γ_n. It follows that $\tau|L$ is scalar. Thus either $\tau|L$ is trivial or $\tau|L$ is λ-isotypic, where λ is the unique nontrivial character of L. The goal of the proof is to exclude the latter possibility.

Write [1] for the isomorphism class of the trivial one-dimensional representation of G. There is an odd integer d such that in the Grothendieck group of virtual representations of G we have

$$d \cdot [1] = \sum_{(H,\eta)\in\mathcal{H}} r_{H,\eta} \cdot \left[\mathrm{ind}_H^G \eta\right] \tag{2.16}$$

(cf. [5], p. 83, (15.11)), where the meaning of the notation is as follows: First of all, $\mathcal{H}$ is a finite set consisting of ordered pairs (H, η). Second, H denotes a subgroup of G which is $\mathbb{R}$-elementary at 2 and η is an orthogonal representation of H. Finally, $r_{H,\eta} \in \mathbb{Z}$. Now for any $(H, \eta) \in \mathcal{H}$ the group $H' = HL$ is still $\mathbb{R}$-elementary at 2 (because L is central of order 2) and the representation $\eta' = \mathrm{ind}_H^{H'} \eta$ is still orthogonal (because orthogonality is equivalent to realizability over $\mathbb{R}$), and furthermore $\mathrm{ind}_H^G \eta = \mathrm{ind}_{H'}^G \eta'$. Hence after replacing (H, η) by (H', η') we may assume that the subgroups H appearing on the right-hand side of (2.16) contain L. Taking the tensor product of both sides of (2.16) with $[\tau]$, we can write

$$d \cdot [\tau] = \sum_{(H,\theta)} r_{H,\theta} \cdot \left[\mathrm{ind}_H^G \theta\right], \tag{2.17}$$

where each θ is the tensor product of an orthogonal representation η of H and the orthogonal representation $\mathrm{res}_H^G \tau$ and is therefore itself orthogonal.

Next a point of notation: $\langle *, * \rangle$ denotes the usual $\mathbb{Z}$-valued symmetric bilinear pairing on the Grothendieck group of virtual representations of G. Thus if π and π' are irreducible representations of G then $\langle \pi, \pi' \rangle$ $(= \langle [\pi], [\pi'] \rangle)$ is 1 or 0 according as π is or is not isomorphic to π'. We do not bother to adorn $\langle *, * \rangle$ with a subscript G, and therefore the notation is universal, applicable in particular to the subgroups H of G. Hence applying the map $* \mapsto \langle *, \tau \rangle$ to

both sides of (2.17) we obtain

$$d = \sum_{(H,\theta)} r_{H,\theta} \langle \theta, \mathrm{res}^G_H \tau \rangle \tag{2.18}$$

by Frobenius reciprocity, where res^G_H is restriction to H.

To prove that $\tau|L$ is trivial suppose on the contrary that $\tau|L$ is λ-isotypic. Under this assumption we shall prove that the integers $\langle \theta, \mathrm{res}^G_H \tau \rangle$ in (2.18) are all even, contradicting the fact that d is odd.

Fix a pair (H, θ). Since θ is orthogonal it can be written as a direct sum of irreducible orthogonal representations of H and representations of the form $\pi \oplus \pi^\vee$, where π is an arbitrary representation of H and $\pi^\vee$ its dual. But the integer $\langle \pi \oplus \pi^\vee, \mathrm{res}^G_H \tau \rangle$ is even because $\mathrm{res}^G_H \tau$ is self-dual. Hence without loss of generality we may assume that θ is irreducible as well as orthogonal.

It follows in particular that the restriction of θ to L (which is contained in H by construction) is scalar. If $\theta|L$ is trivial, then we immediately deduce that $\langle \theta, \mathrm{res}^G_H \tau \rangle = 0$, because by assumption, $\tau|L$ is λ-isotypic. Henceforth we assume that $\theta|L$ is also λ-isotypic.

Write $H = O \rtimes T$ with O cyclic of odd order and T a 2-group. Since L is central and of order 2 it is contained in every Sylow 2-subgroup of H; in particular, $L \subset T$. We consider cases according as $L = T$ or $L \subsetneq T$.

First suppose that $L = T$. Then H is abelian; hence θ is one-dimensional. But θ is also self-dual, so it is a homomorphism $H \to \{\pm 1\}$. Thus θ is trivial on O, and among extensions of λ to one-dimensional characters of H it is the unique one which is trivial on O. The other such extensions come in pairs, a character and its conjugate, so we can write

$$\mathrm{ind}^H_T(\lambda) = \theta \oplus (\pi \oplus \pi^\vee), \tag{2.19}$$

where π is a direct sum of $(|O| - 1)/2$ characters of H. Applying the function $\langle *, \mathrm{res}^G_H \tau \rangle$ to both sides of (2.19), we find that

$$\langle \lambda, \mathrm{res}^G_T \tau \rangle \equiv \langle \theta, \mathrm{res}^G_H \tau \rangle \pmod 2, \tag{2.20}$$

because $\mathrm{res}^G_H \tau$ is self-dual. Since the left-hand side of (2.20) is $\dim \tau$ we conclude that the right-hand side is even, as desired.

Next suppose that $L \subsetneq T$. In this case we shall prove that θ is symplectic, contradicting the fact that θ is irreducible orthogonal. Alternatively, we can ignore the latter contradiction and simply deduce from the theory of the Schur index that $\langle \theta, \mathrm{res}^G_H \tau \rangle$ is even (an irreducible symplectic representation has even multiplicity in any orthogonal representation).

To prove that θ is symplectic it suffices to show that for some $g \in G$ the representation $y \mapsto \theta(g^{-1} y g)$ of gHg^{-1} is symplectic. Now as T is a 2-subgroup of G and S_n/W^2 a Sylow 2-subgroup we can choose g so that

$gTg^{-1} \subset S_n/W^2$. Hence after replacing H by gHg^{-1} we may assume that T itself is contained in S_n/W^2.

As a first step toward showing that θ is symplectic, choose $t \in T$ such that $t^2 \in L$ but $t \notin L$. We claim that t^2 is the nontrivial element of L. If not, then $t^2 = 1$. Since $T \subset S_n/W^2$ by assumption, and since the natural map $S \to S_n$ is an isomorphism identifying $S \cap Z$ with $S_n \cap Z_n = W$, the hypothesis that $t^2 = 1$ has the following consequence: there are elements $x \in S \smallsetminus (S \cap Z)$ and $z \in S \cap Z$ such that $t = x_n W^2$ and $x^2 = z^2$. Then $xz^{-1} \in \Gamma$ is a nonscalar involution, contrary to our hypothesis that $C = \emptyset$. It follows that t^2 is the nonidentity element of L, as claimed. Thus if θ is one-dimensional, then $\theta(t)^2 = -1$, contradicting the fact that θ is orthogonal. We conclude that $\dim \theta > 1$. In particular, H is nonabelian.

As in the proof of Proposition 10, the fact that $\dim \theta > 1$ and that H is a semidirect product $O \rtimes T$ with O and T abelian has the following consequence: there is a proper subgroup I of H containing the centralizer of O in H such that $\theta = \mathrm{ind}_I^H \xi$ for some one-dimensional character ξ of I. Now since H is both nonabelian and $\mathbb{R}$-elementary at 2, the centralizer of O in T is a subgroup K of index 2 in T (necessarily containing the central subgroup L), so that I contains $O \times K$. As I is a proper subgroup of H it follows that $I = O \times K$, whence $[H : I] = 2$ and therefore $\dim \theta = 2$.

The symplectic group in dimension two is simply $\mathrm{SL}(2, \mathbb{C})$, so to show that θ is symplectic it suffices to see that $\det \theta$ is trivial. Before doing so we observe that K is central in H, so that $\theta|K$ is scalar multiplication by $\xi|K$. It follows that $\xi|L = \lambda$ and consequently that $t \notin K$: for otherwise we have $\xi(t)^2 = \lambda(t^2) = -1$, contradicting the self-duality of $\theta|K$. We conclude that t represents the nontrivial coset of K in T.

We are now ready to show that $\det \theta$ is trivial. The triviality of $\det \theta|O$ is immediate from the fact that O has odd order while $\det \theta$ (being the determinant of a self-dual representation) takes values in $\{\pm 1\}$. To see that $\det \theta$ is trivial on T we once again use the standard formula for the determinant of an induced representation (cf. (1.7)), which in the present context gives

$$\det \theta|T = \mathrm{sgn}_{T/K} \cdot (\xi \circ \mathrm{trans}_K^T).$$

Now $\mathrm{sgn}_{T/K}$ is trivial on K, while trans_K^T sends an element of T to its square (true for the transfer from any abelian group to a subgroup of index 2). Thus $\det \theta(k) = \xi(k^2)$ for $k \in K$. But $\theta|K$ is $(\xi|K)$-isotypic and self-dual, so $\xi|K$ takes values in $\{\pm 1\}$ and we deduce that $\det \theta$ is trivial on K. Finally, $\mathrm{sgn}_{T/K}(t) = -1$ while $\mathrm{trans}_K^T(t) = t^2$. Since $\xi(t^2) = \lambda(t^2) = -1$ we conclude that $\det \theta$ is trivial. □

3. Proof of Theorem 3. We return to the setting of the introduction. Thus Γ is the image of the representation ρ of $\mathrm{Gal}(\overline{F}/F)$ on the p-adic Tate module of E. Let $\mathcal{T}_n^{\dim=1}$ be the set of $[\tau] \in \mathcal{T}_n$ such that $\dim \tau = 1$.

Proposition 13. $|\mathcal{T}_n^{\dim=1}| \leqslant 4$.

Proof. If $[\tau] \in \mathcal{T}_n^{\dim=1}$, then τ can be viewed as a character $\mathrm{Gal}(R_n/F) \to \{\pm 1\}$ and is therefore determined by its restriction to a Sylow 2-subgroup. As already noted, a Sylow 2-subgroup of $\mathrm{Gal}(R_n/F)$ is isomorphic to a subgroup of A_1 ($\cong \mathbb{F}_p^\times \times \mathbb{F}_p^\times$) and so has at most four characters with values in $\{\pm 1\}$. $\square$

Combining Propositions 5 and 13, we see that

$$\vartheta_n^{-\epsilon} = \sum_{\substack{[\tau]\in\mathcal{T}_n \\ \dim\tau>1 \\ \delta(E,\tau)=-1}} \dim\tau \quad + \quad O(1) \tag{3.1}$$

with $|O(1)| \leqslant 4$. On the other hand, $\delta(E,\tau) = -1$ only if there is a finite place v of F such that E has potential multiplicative reduction at v and the integer $\langle \chi_v, \tau_v \rangle$ is odd. Hence

$$\sum_{\substack{[\tau]\in\mathcal{T}_n \\ \dim\tau>1 \\ \delta(E,\tau)=-1}} \dim\tau \leqslant \sum_{v \text{ pot. mult.}} \vartheta_n^v \tag{3.2}$$

with

$$\vartheta_n^v = \sum_{\substack{[\tau]\in\mathcal{T}_n \\ \langle\chi_v,\tau_v\rangle \text{ odd}}} \dim\tau. \tag{3.3}$$

Henceforth v denotes a fixed place of F at which E has potential multiplicative reduction. Combining (3.1) and (3.2), we see that Theorem 3 has been reduced to the following assertion:

Proposition 14. $\vartheta_n^v = O(p^n)$.

Proposition 14 will be proved via a further reduction to Proposition 15 below, but first a review of notation is in order. The key point to recall is that if $\tau \in \mathcal{T}$ is given, then τ_v denotes the restriction of τ to $\mathrm{Gal}(\overline{F}_v/F_v)$, the latter group being identified with the decomposition subgroup of $\mathrm{Gal}(\overline{F}/F)$ at some fixed place of $\overline{F}$ over v. Furthermore χ_v is the character $\mathrm{Gal}(\overline{F}_v/F_v) \to \{\pm 1\}$ such that the twist of E over F_v by χ_v is a Tate curve, and $\langle \chi_v, \tau_v \rangle$ is the multiplicity of χ_v in τ_v. In fact we have already applied the notation $\langle *, * \rangle$ more generally to the semisimple representations of other groups, the essential properties of $\langle *, * \rangle$ being that it is symmetric, that it is bilinear with respect to direct sums, and that if π is irreducible, then $\langle \pi, \pi' \rangle$ is the multiplicity of π in π'.

Now take $n \geqslant 1$ and suppose that $[\tau] \in \mathcal{T}_n$. We may think of τ as a representation of the finite group $G_n = \mathrm{Gal}(R_n/F)$. Hence after forming the

compositum $R_{n,v} = R_n F_v$ inside $\overline{F}_v$ we can view τ_v as the restriction of τ to our chosen decomposition subgroup $D_n = \mathrm{Gal}(R_{n,v}/F_v)$ of G_n at v. We claim that χ_v can likewise be regarded as a representation of D_n. To see this, write $\rho_{1,v}$ for the restriction of ρ_1 to $\mathrm{Gal}(\overline{F}_v/F_v)$. Then $\rho_{1,v} \otimes \chi_v$ is equivalent to the representation afforded by the points of order p on a Tate curve over F_v, and consequently the semisimplification of $\rho_{1,v} \otimes \chi_v$ is the direct sum of two one-dimensional characters, one of which is trivial. Hence the semisimplification of $\rho_{1,v}$ is also the direct sum of two one-dimensional characters, one of which is χ_v. It follows that χ_v factors through $\mathrm{Gal}(R_{1,v}/F_v)$ and *a fortiori* through $D_n = \mathrm{Gal}(R_{n,v}/F_v)$, as claimed. We may therefore view χ_v as a character of D_n. When χ_v is so viewed we write C_n for its kernel.

Proposition 15. *There is a subgroup H_n of G_n containing D_n such that*

(i) *C_n is normal in H_n with abelian quotient,*
(ii) *H_n/C_n can be generated by $\leqslant 2$ elements, and*
(iii) *$[G_n : H_n] = O(p^n)$.*

Before proving Proposition 15 let us see how Proposition 14 follows. Let Λ_n be the set of one-dimensional characters of H_n which restrict to χ_v on D_n. By part (i) of the proposition,

$$\mathrm{ind}_{D_n}^{H_n} \chi_v = \bigoplus_{\lambda \in \Lambda_n} \lambda.$$

But as χ_v is real-valued we have $\lambda \in \Lambda_n$ if and only if $\lambda^{-1} \in \Lambda_n$, and consequently there is a subset Λ_n' of Λ_n such that

$$\mathrm{ind}_{D_n}^{H_n} \chi_v = \Big(\bigoplus_{\lambda \in \Lambda_n'} \lambda \oplus \lambda^{-1}\Big) \oplus \Big(\bigoplus_{\substack{\lambda \in \Lambda_n \\ \lambda^2 = 1}} \lambda\Big).$$

Next we use the fact that $\mathrm{res}_{H_n}^{G_n} \tau$ is self-dual, which gives

$$\langle \mathrm{ind}_{D_n}^{H_n} \chi_v, \mathrm{res}_{H_n}^{G_n} \tau \rangle \equiv \sum_{\substack{\lambda \in \Lambda_n \\ \lambda^2 = 1}} \langle \lambda, \mathrm{res}_{H_n}^{G_n} \tau \rangle \pmod 2$$

and hence

$$\langle \chi_v, \tau_v \rangle \equiv \sum_{\substack{\lambda \in \Lambda_n \\ \lambda^2 = 1}} \langle \mathrm{ind}_{H_n}^{G_n} \lambda, \tau \rangle \pmod 2$$

by Frobenius reciprocity. It follows that if the integer $\langle \chi_v, \tau_v \rangle$ is odd, then there exists $\lambda \in \Lambda_n$ with $\lambda^2 = 1$ such that the nonnegative integer $\langle \mathrm{ind}_{H_n}^{G_n} \lambda, \tau \rangle$ is positive. Thus if we put

$$\vartheta_n^\lambda = \sum_{\tau \in \mathcal{T}_n} \langle \mathrm{ind}_{H_n}^{G_n} \lambda, \tau \rangle \dim \tau, \tag{3.4}$$

then a glance at (3.3) shows that

$$\vartheta_n^v \leqslant \sum_{\substack{\lambda\in\Lambda_n\\ \lambda^2=1}} \vartheta_n^\lambda. \tag{3.5}$$

To exploit this bound, we replace "=" by "$\leqslant$" in (3.4) while replacing $\mathcal{T}_n$ by $\mathcal{T}_n^*$, the set of isomorphism classes of all irreducible Artin representations of $\mathrm{Gal}(\overline{F}/F)$ which factor through $G_n = \mathrm{Gal}(R_n/F)$:

$$\vartheta_n^\lambda \leqslant \sum_{\tau\in\mathcal{T}_n^*} \langle \mathrm{ind}_{H_n}^{G_n}\lambda, \tau\rangle \dim\tau. \tag{3.6}$$

As $\langle \mathrm{ind}_{H_n}^{G_n}\lambda, \tau\rangle$ is the multiplicity of τ in $\mathrm{ind}_{H_n}^{G_n}\lambda$ we see that the right-hand side of (3.6) is just the dimension of $\mathrm{ind}_{H_n}^{G_n}\lambda$, or in other words $[G_n : H_n]$. Hence $\vartheta_n^\lambda = O(p^n)$ by part (iii) of Proposition 15. But it follows from part (ii) of the proposition that the sum over λ in (3.5) has at most four terms, whence $\vartheta_n^v = O(p^n)$ also. This completes the reduction of Proposition 14 to Proposition 15.

Proof of Proposition 15. Put $G = \mathrm{Gal}(R/F)$ and view ρ and ρ_n as representations of G and G_n respectively. Then ρ and ρ_n are injective, and since Z is central in $\mathrm{GL}(2,\mathbb{Z}_p)$ it follows that $\rho^{-1}(Z)$ is central in G. Set

$$H = \rho^{-1}(Z)D, \tag{3.7}$$

where D is our chosen decomposition subgroup of G at v (thus $D = \mathrm{Gal}(R_v/F_v)$, the compositum $R_v = RF_v$ being formed inside $\overline{F}_v$). We define H_n to be the image of H under the natural map $G \to G_n$.

To verify (i) and (ii), let C denote the kernel of χ_v when χ_v is viewed as a character of D. Then C is a subgroup of index $\leqslant 2$ in D, hence normal. Since $\rho^{-1}(Z)$ is central in G we deduce from (3.7) that C is normal in H with abelian quotient, and applying the surjective map $G \to G_n$ we obtain (i). In fact (ii) also follows, because Z is procyclic.

It remains to prove (iii). Write J for the subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$ consisting of the matrices

$$b(u,z) = \begin{pmatrix} u & z \\ 0 & 1 \end{pmatrix} \tag{3.8}$$

with $u \in \mathbb{Z}_p^\times$ and $z \in \mathbb{Z}_p$. As E is the twist of a Tate curve over F_v we know that $\rho(D)$ is conjugate in $\mathrm{GL}(2,\mathbb{Z}_p)$ to an open subgroup of $\pm J$. On the other hand, the group $\Gamma = \rho(G)$ is open in $\mathrm{GL}(2,\mathbb{Z}_p)$ and therefore $\Gamma \cap Z$ is open in Z. It follows that $\rho(H)$ is conjugate to an open subgroup of ZJ. Writing J_n for the reduction of J modulo p^n, we conclude that the ratio $|Z_nJ_n|/|\rho_n(H_n)|$

is a constant c_1 for large n. But $Z_n J_n$ is the subgroup of upper triangular matrices in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$, which is of index $(p+1)p^{n-1}$. Thus for large n,

$$[\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}) : \rho_n(H_n)] = c_2 \cdot p^n$$

with $c_2 = c_1(p+1)/p$. As the index $[\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}) : \rho_n(G_n)]$ is a constant c_3 for large n we deduce that $[\rho_n(G_n) : \rho_n(H_n)] = (c_2/c_3) \cdot p^n$ for large n, and property (iii) follows. □

4. Example 1 revisited. We must still verify that if $F = \mathbb{Q}$, $p = 5$, and E is the curve 150A1 of [3], then $W(E, \tau) = 1$ for all $\tau \in \mathcal{T}$. But first we should check that our two standing assumptions are satisfied in this case. That $\Gamma_1 \subset B$ follows by inspection from the tables in [3], according to which 150A1 is 5-isogenous to an elliptic curve over $\mathbb{Q}$. As for the behavior of E at primes of potential good reduction, there is a unique such prime of bad reduction, namely 5, and $\mathrm{ord}_5 \Delta(E) = 3$. Thus $\Delta(E)$ has valuation 12 relative to a uniformizer of $\mathbb{Q}_5(\Delta(E)^{1/4})$, whence E has good reduction over $\mathbb{Q}_5(\Delta(E)^{1/4})$. But the latter field is abelian over $\mathbb{Q}_5$, because $\mathbb{Q}_5$ contains the fourth roots of unity. As any local abelian extension is realized by some global abelian extension (a weak form of the Grunwald-Wang theorem), we conclude that E does attain good reduction at 5 over some abelian extension of $\mathbb{Q}$.

To see that $W(E, \tau) = 1$ for all $\tau \in \mathcal{T}$, it suffices to prove two formulas, namely

$$W(E, \tau) = (-1)^{\langle 1, \tau_2 \rangle + \langle 1, \tau_3 \rangle} \tag{4.1}$$

and

$$\langle 1, \tau_2 \rangle = \langle 1, \tau_3 \rangle. \tag{4.2}$$

Here and elsewhere, we conflate a prime number with the place of $\mathbb{Q}$ determined by it. For instance τ_2 is really τ_v with v equal to the standard 2-adic place of $\mathbb{Q}$.

Let us begin the proof of (4.1). The primes of potential multiplicative reduction for E are 2 and 3, and E has split multiplicative reduction at these primes, so if $\dim \tau > 1$, then (4.1) is immediate from Proposition 5. Suppose now that $\dim \tau = 1$. To verify (4.1) in this case we proceed as in the proof of Proposition 3. First of all, (1.2) becomes

$$W(E, \tau) = \prod_{v \leqslant \infty} W(E/\mathbb{Q}_v, \tau_v), \tag{4.3}$$

and (1.3) becomes

$$W(E/\mathbb{R}, \tau_\infty) = -1 \tag{4.4}$$

because $\dim \tau = 1$. For this same reason τ and $\det \tau$ are indistinguishable, and consequently (1.4) gives

$$W(E/\mathbb{Q}_2, \tau_2)W(W/\mathbb{Q}_3, \tau_3) = \tau_2(-1)\tau_3(-1) \cdot (-1)^{\langle 1,\tau_2\rangle + \langle 1,\tau_3\rangle} \tag{4.5}$$

(recall that if E has split multiplicative reduction at v then $\chi_v = 1$). Finally,

$$W(E/\mathbb{Q}_5, \tau_5) = -\tau_5(-1) \tag{4.6}$$

and if $v \neq 2, 3, 5, \infty$, then

$$W(E/\mathbb{Q}_v, \tau_v) = \tau_v(-1). \tag{4.7}$$

The reference for (4.6) and (4.7) is [11], p. 330, Theorem 2, part (iii). In the case of (4.6) the invariant e of [11] is 4 (because $\mathrm{ord}_5\Delta = 3$), and hence the invariant ϵ is -1 (because -2 is a quadratic nonresidue mod 5). The quantity q defined by the first displayed formula on p. 329 of [11] is 5, so we choose the first of the two formulas for the local root number on p. 330, obtaining (4.6). In the case of (4.7), on the other hand, $e = 1$, whence $q \equiv 1 \bmod e$ and $\epsilon = 1$. Thus the first of the two formulas on p. 330 is again in force, and the result is (4.7).

To complete the proof of (4.1), we insert (4.4), (4.5), (4.6), and (4.7) in (4.3), obtaining

$$W(E, \tau) = (-1)^{\langle 1,\tau_2\rangle + \langle 1,\tau_3\rangle} \cdot \prod_{v<\infty} \tau_v(-1),$$

and hence

$$W(E, \tau) = \tau_\infty(-1)(-1)^{\langle 1,\tau_2\rangle + \langle 1,\tau_3\rangle}.$$

Let μ_5 be the group of fifth roots of unity in $\overline{\mathbb{Q}}$, and let $E[5]$ be the group of 5-division points on E. Then μ_5 is a Galois submodule of $E[5]$ (cf. [6], p. 197, Table 1). It follows that $\mathrm{Gal}(R/\mathbb{Q}(\mu_5))$ is a pro-5-group and hence that the one-dimensional real-valued character τ is trivial on $\mathrm{Gal}(R/\mathbb{Q}(\mu_5))$ when τ is viewed as a representation of $\mathrm{Gal}(R/\mathbb{Q})$. Thus τ factors through $\mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ and so coincides as a Dirichlet character either with the trivial character or with the Legendre symbol modulo 5. In either case, $\tau_\infty(-1) = 1$, and (4.1) follows.

We turn now to (4.2). View τ as a representation of $\mathrm{Gal}(R/\mathbb{Q})$, and let D and D' denote the decomposition subgroups of $\mathrm{Gal}(R/\mathbb{Q})$ at our chosen place of R above 2 and 3 respectively. The statement to be proved is that the multiplicity of the trivial one-dimensional representation of D in $\tau|D$ equals the multiplicity of the trivial one-dimensional representation of D' in $\tau|D'$. Thus it will suffice to see that D is conjugate to D' in $\mathrm{Gal}(R/\mathbb{Q})$. Equivalently, if we set $\Delta = \rho(D)$ and $\Delta' = \rho(D')$, then it suffices to see that Δ is conjugate to Δ' in Γ, because ρ is an isomorphism of $\mathrm{Gal}(R/\mathbb{Q})$ onto Γ.

First we show that Δ is conjugate to Δ' in $\mathrm{GL}(2,\mathbb{Z}_5)$. Let U and U' be the open subgroups of $\mathbb{Z}_5^\times$ topologically generated by 2 and 3 respectively. Since 2 and 3 are primitive roots mod 5 while neither 2^4 nor 3^4 is congruent to 1 mod 5^2, we see that $U = U' = \mathbb{Z}_5^\times$. Furthermore $\mathrm{ord}_p j(E) \not\equiv 0 \bmod 5$ for $p = 2, 3$. Recalling that E is a Tate curve over $\mathbb{Q}_2$ and $\mathbb{Q}_3$, we deduce that Δ and Δ' are both conjugate in $\mathrm{GL}(2,\mathbb{Z}_5)$ to the subgroup J consisting of the matrices $b(u,z)$ in (3.8). The proof of (4.2) is now completed by the following proposition:

Proposition 16. *Let Γ be an open subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$, and let Δ and Δ' be subgroups of Γ which are both conjugate to J in $\mathrm{GL}(2,\mathbb{Z}_p)$. Then Δ is conjugate to Δ' in Γ.*

For an integer $n \geqslant 0$ let $P(n)$ denote the subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$ consisting of matrices which are upper triangular modulo p^n, with the understanding that $P(0) = \mathrm{GL}(2,\mathbb{Z}_p)$. Our proof of Proposition 16 depends on the following lemma. Recall that Z is the group of scalar matrices in $\mathrm{GL}(2,\mathbb{Z}_p)$.

Lemma. *Let Γ be an open subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$ containing J. Then $Z\Gamma = P(n_0)$ for some $n_0 \geqslant 0$.*

Proof. For $z \in \mathbb{Z}_p$ let $\ell(z)$ be the 2×2 lower triangular unipotent matrix with z as lower left-hand entry. The set $\{z \in \mathbb{Z}_p : \ell(z) \in Z\Gamma\}$ is an open subgroup of $\mathbb{Z}_p$, hence of the form $p^{n_0}\mathbb{Z}_p$ for some $n_0 \geqslant 0$, and consequently $Z\Gamma$ contains both $\ell(p^{n_0}\mathbb{Z}_p)$ and ZJ. Note that ZJ is the group of upper triangular matrices in $\mathrm{GL}(2,\mathbb{Z}_p)$. If $n_0 = 0$, then the lemma follows from the identities

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a^{-1}c & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d - a^{-1}bc \end{pmatrix} \quad (a \in \mathbb{Z}_p^\times) \tag{4.8}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ (a')^{-1}c & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & d - (a')^{-1}b'c \end{pmatrix} \quad (a \in p\mathbb{Z}_p), \tag{4.9}$$

where $a' = a + c$ and $b' = b + d$ in (4.9). Assume now that $n_0 \geqslant 1$. Then the relation $P(n_0) \subset Z\Gamma$ follows from (4.8) on taking $c \in p^{n_0}\mathbb{Z}_p$. For the reverse inclusion we argue by contradiction: suppose that for some $c \in p^n\mathbb{Z}_p^\times$ with $0 \leqslant n < n_0$ the left-hand side of (4.8) or (4.9) belongs to $Z\Gamma$. Then $\ell(a^{-1}c) \in Z\Gamma$ (if $a \in \mathbb{Z}_p^\times$) or $\ell((a+c)^{-1}c) \in Z\Gamma$ (if $a \in p\mathbb{Z}_p$), contradicting the definition of n_0. □

Proof of Proposition 16. Write $\Delta' = hJh^{-1}$ with $h \in \mathrm{GL}(2,\mathbb{Z}_p)$. After replacing Γ by $h^{-1}\Gamma h$ we may assume that $\Delta' = J$. It will suffice to see that Δ is conjugate to J in $Z\Gamma$, because Z is central in $\mathrm{GL}(2,\mathbb{Z}_p)$.

By hypothesis, $\Delta = gJg^{-1}$ for some $g \in \mathrm{GL}(2,\mathbb{Z}_p)$, and by the lemma, $Z\Gamma = P(n_0)$ for some $n_0 \geqslant 0$ (and in fact for some $n_0 \geqslant 1$, else $Z\Gamma =$

$\mathrm{GL}(2,\mathbb{Z}_p)$ and there is nothing to prove). It follows that $gJg^{-1} \subset P(n_0)$. In particular, $gb(1,1)g^{-1} \in P(n_0)$ and $gb(2,1)g^{-1} \in P(n_0)$ with $b(*,*)$ as in (3.8). After a straightforward calculation the first of these relations implies that $g \in P([(n_0+1)/2])$ (whence in particular the lower left-hand entry of g has positive valuation) and then the second relation implies that $g \in P(n_0) = Z\Gamma$. □

5. Example 2 revisited. Finally, suppose that $F = \mathbb{Q}$, $p = 7$, and E is the curve 294B1 of [3]. The verification that our two standing assumptions are satisfied in this case is similar to the corresponding verification in Example 1. We will show that $\vartheta_n^+ \gg 7^n$.

As in Example 1, the primes 2 and 3 are precisely the primes of potential multiplicative reduction for E, and E has split multiplicative reduction at these primes. Hence for $\tau \in \mathcal{T}$ with $\dim \tau > 1$ Proposition 5 gives

$$W(E,\tau) = -(-1)^{\langle 1,\tau_2\rangle + \langle 1,\tau_3\rangle}, \tag{5.1}$$

where as before, a prime number is conflated with the place of $\mathbb{Q}$ it determines. If we choose $n \geqslant 1$ so that $\tau \in \mathcal{T}_n$, then we may view τ as a representation of $\mathrm{Gal}(R_n/\mathbb{Q})$ and τ_v as the restriction of τ to $\mathrm{Gal}(R_{n,v}/\mathbb{Q}_v)$, where $R_{n,v} = R_n\mathbb{Q}_v \subset \overline{\mathbb{Q}}_v$.

We claim that $\langle 1,\tau_2\rangle$ is even. To see this, view ρ_n as a representation of $\mathrm{Gal}(R_n/\mathbb{Q})$ and consider the image of the subgroup $\mathrm{Gal}(R_{n,2}/\mathbb{Q}_2)$. Since E is a Tate curve over $\mathbb{Q}_2$, the image of $\mathrm{Gal}(R_{n,2}/\mathbb{Q}_2)$ is conjugate in $\mathrm{GL}(2,\mathbb{Z}/7^n\mathbb{Z})$ to a subgroup of J_n, the reduction modulo 7^n of J. Write

$$g\rho_n(\mathrm{Gal}(R_{n,2}/\mathbb{Q}_2))g^{-1} \subset J_n \tag{5.2}$$

with $g \in \mathrm{GL}(2,\mathbb{Z}/7^n\mathbb{Z})$. With notation as in (3.8), if $b(u,z) \bmod 7^n$ belongs to the left-hand side of (5.2), then u is a value of the 7-adic cyclotomic character of $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$, and since 2 mod 7 has order 3 we deduce that u mod 7 has order dividing 3. It follows that the left-hand side of (5.2), hence $\mathrm{Gal}(R_{n,2}/\mathbb{Q})$ itself, is a group of odd order. But a group of odd order has no nontrivial irreducible self-dual representations, whereas τ_2 is self-dual. Thus the nontrivial irreducible representations of $\mathrm{Gal}(R_{n,2}/\mathbb{Q})$ occurring in τ_2 occur in pairs, each with the same multiplicity as its dual. Since $\dim\tau$ is even (Proposition 4) we conclude that the multiplicity of 1 in τ_2 is also even, as claimed.

It follows that the term $\langle 1,\tau_2\rangle$ can be removed from the exponent on the right-hand side of (5.1). Hence to see that $\vartheta_n^+ \gg 7^n$ it suffices to see that for large n there is an isomorphism class $[\tau] \in \mathcal{T}_n$ with $\dim\tau \gg 7^n$ and $\langle 1,\tau_3\rangle = 1$. We shall deduce this fact from the following proposition. As usual, a subscript n on a subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$ denotes the reduction of the subgroup modulo p^n.

Proposition 17. *Let Γ be an open subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$ and Δ a subgroup of Γ which is conjugate in $\mathrm{GL}(2,\mathbb{Z}_p)$ to J. If n is sufficiently large, then there exists an irreducible self-dual complex representation σ of Γ which factors through Γ_n and satisfies $\dim\sigma \gg p^n$ and $\langle 1,\sigma|\Delta\rangle = 1$.*

To apply the proposition in the case at hand, view ρ as an isomorphism of $\mathrm{Gal}(R/\mathbb{Q})$ onto Γ and put $\Delta = \rho(D)$, where $D \subset \mathrm{Gal}(R/\mathbb{Q})$ is the decomposition subgroup at our chosen place above 3. Since E is a Tate curve over $\mathbb{Q}_3$ we know that Δ is conjugate in $\mathrm{GL}(2,\mathbb{Z}_7)$ to an open subgroup of J. But in fact Δ is conjugate to J itself, because 3 is a primitive root mod 7 and $3^6 \not\equiv 1 \bmod 49$ while $\mathrm{ord}_7 j(E) \not\equiv 0 \bmod 7$. Hence for large n we obtain a representation σ as in the proposition. The representation $\tau = \sigma\circ\rho$ then satisfies $\dim\tau \gg 7^n$ and $\langle 1,\tau|D\rangle = 1$, and if we view ρ as a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then $[\tau] \in \mathcal{T}_n$.

The proof of Proposition 17 is routine, but we nonetheless supply the details.

Lemma. *Let G and G' be finite groups, $f : G \to G'$ a surjective group homomorphism, and H and H' subgroups of G and G' respectively, with $H' = f(H)$. Assume that the following conditions hold:*

(i) $[G:H] > [G':H']$,

(ii) $|H\backslash G/H| = 1 + |H'\backslash G'/H'|$.

Then there exists an irreducible self-dual complex representation σ of G such that $\dim\sigma = [G:H] - [G':H']$ and $\langle 1, \mathrm{res}^G_H\sigma\rangle = 1$.

Proof. Write $(\mathrm{ind}^{G'}_{H'}1)\circ f$ for the representation of G obtained from $\mathrm{ind}^{G'}_{H'}1$ via composition with f. Then $(\mathrm{ind}^{G'}_{H'}1)\circ f$ is naturally a subrepresentation of $\mathrm{ind}^G_H 1$, so we can write

$$\mathrm{ind}^G_H 1 \cong \sigma \oplus (\mathrm{ind}^{G'}_{H'}1)\circ f$$

with a self-dual representation σ of G of dimension $[G:H] - [G':H']$. We must show that σ is irreducible and does not occur in $(\mathrm{ind}^{G'}_{H'}1)\circ f$. Both conclusions will follow if we prove that

$$\langle \mathrm{ind}^G_H 1, \mathrm{ind}^G_H 1\rangle - \langle \mathrm{ind}^{G'}_{H'}1, \mathrm{ind}^{G'}_{H'}1\rangle = 1, \tag{5.3}$$

for the left-hand side is the sum of the positive integer $\langle\sigma,\sigma\rangle$ and the nonnegative integer $2\langle\sigma, (\mathrm{ind}^{G'}_{H'}1)\circ f\rangle$, which must then be 1 and 0 respectively.

To prove (5.3) we apply the standard formula for the restriction of an induced representation to a subgroup (cf. [15], p. 58, Proposition 22). Let S be a set of representatives in G for the distinct double cosets of H, and for $s \in S$ put $H_s = H \cap sHs^{-1}$; then

$$\mathrm{res}^G_H(\mathrm{ind}^G_H 1) = \bigoplus_{s\in S} \mathrm{ind}^H_{H_s} 1. \tag{5.4}$$

Applying Frobenius reciprocity to both sides of (5.4), we obtain

$$\langle \mathrm{ind}_H^G 1, \mathrm{ind}_H^G 1\rangle = \sum_{s\in S} \langle \mathrm{res}_{H_s}^H 1, 1\rangle$$

and therefore

$$\langle \mathrm{ind}_H^G 1, \mathrm{ind}_H^G 1\rangle = |S|. \tag{5.5}$$

By (ii), the analogous statement for G' and H' is

$$\langle \mathrm{ind}_{H'}^{G'} 1, \mathrm{ind}_{H'}^{G'} 1\rangle = |S| - 1. \tag{5.6}$$

Subtracting (5.6) from (5.5) yields (5.3). □

Proof of Proposition 17. After replacing Γ by a conjugate we may assume that $\Delta = J$. Then $Z\Delta$ coincides with ZJ, which is the upper triangular subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$. Hence

$$[\mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z}) : Z_n\Delta_n] = (p+1)p^{n-1}.$$

On the other hand, $[\mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z}) : Z_n\Gamma_n]$ is independent of n for large n, because $Z\Gamma$ is open in $\mathrm{GL}(2,\mathbb{Z}_p)$. It follows that for large n we have

$$[Z_n\Gamma_n : Z_n\Delta_n] = c\cdot p^n \tag{5.7}$$

with a constant $c > 0$.

Next recall that $Z\Gamma = P(n_0)$ for some $n_0 \geqslant 0$ (see the lemma used in the proof of Proposition 16). Hence $Z_n\Gamma_n = P(n_0)_n$. On the other hand, we have already noted that $Z\Delta$ is the upper triangular subgroup of $\mathrm{GL}(2,\mathbb{Z}_p)$, and consequently $Z_n\Delta_n$ is the upper triangular subgroup of $\mathrm{GL}(2,\mathbb{Z}/p^n\mathbb{Z})$. Using these descriptions of $Z_n\Delta_n$ and $Z_n\Gamma_n$ one can check that for $n > n_0$ the identity matrix and the matrices

$$\gamma_i = \begin{pmatrix} 1 & 0 \\ p^i & 1 \end{pmatrix} \qquad (n_0 \leqslant i \leqslant n-1)$$

together constitute a set of representatives for the distinct double cosets of $Z_n\Delta_n$ in $Z_n\Gamma_n$. (In fact given $\gamma \in Z_n\Gamma_n$ with lower left-hand entry $c \not\equiv 0 \bmod p^n$, choose i so that $c \equiv 0 \bmod p^i$ but $c \not\equiv 0 \bmod p^{i+1}$; then γ belongs to the double coset represented by γ_i.) Thus

$$|(Z_n\Delta_n)\backslash(Z_n\Gamma_n)/(Z_n\Delta_n)| = n + 1 - n_0 \tag{5.8}$$

for $n \geqslant n_0$.

Now take n large and apply the lemma with $G = \overline{\Gamma}_n$, $G' = \overline{\Gamma}_{n-1}$, $H = \overline{\Delta}_n$, and $H' = \overline{\Delta}_{n-1}$, where the bar denotes the projective image (thus $G = (Z_n\Gamma_n)/Z_n$, $H = (Z_n\Delta_n)/Z_n$, and so on). Let $f : G \to G'$ be reduction modulo p^{n-1}. Conditions (i) and (ii) of the lemma follow from (5.7) and (5.8) respectively, and we deduce that there is a representation σ of G as in the

lemma. But $G \cong \Gamma_n/(Z_n \cap \Gamma_n)$, so we may view σ as a representation of Γ which factors through Γ_n. Furthermore $\dim \sigma = c(p^n - p^{n-1})$ by (5.7), so $\dim \sigma \gg p^n$. Finally, the assertion that $\langle 1, \mathrm{res}^G_H \sigma \rangle = 1$ when σ is viewed as a representation of G amounts to the assertion that $\langle 1, \sigma|\Delta \rangle = 1$ when σ is viewed as a representation of Γ. □

Acknowledgments

It is a pleasure to acknowledge my large debt to John Coates, without whose inquiries and encouragement this paper would never have been written. I am particularly grateful to Coates for suggesting that I look at Examples 1 and 2, which were the genesis of this project, and also for drawing my attention to the work of Michael Shuter [17] on Selmer groups, which influenced the final formulation. I would also like to thank R. Sujatha and Tom Fisher for their comments.

References

1. J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication*, Publ. Math. IHES **101** (2005), 163–208. MR2217048 (2007b:11172)
2. J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann. **331** (2005), 809–839. MR2148798 (2006g:11219)
3. J. E. Cremona, *Algorithms for elliptic curves*, Cambridge University Press, 1992. MR1201151 (93m:11053)
4. P. Deligne, *Les constantes des équations fonctionelles des fonctions L*, Modular Functions of One Variable, II, SLN 349, Springer-Verlag, New York, 1973, pp. 501–595. MR0349635 (50:2128)
5. W. Feit, *Characters of Finite Groups*, W. A. Benjamin, New York, 1967. MR0219636 (36:2715)
6. T. Fisher, *Some examples of 5 and 7 descents for elliptic curves over $\mathbb{Q}$*, Jour. Eur. Math. Soc. **3** (2001), 169–201. MR1831874 (2002m:11045)
7. P. X. Gallagher, *Determinants of representations of finite groups*, Abh. Math. Sem. Univ. Hamburg **28** (1965), 162–167. MR0185017 (32:2487)
8. R. Greenberg, *Non-vanishing of certain values of L-functions*, Analytic Number Theory and Diophantine Problems, Prog. in Math. 70, Birkhäuser, Boston, 1987, pp. 223–235. MR1018378 (90j:11124)
9. L. Howe, *Twisted Hasse-Weil L-functions and the rank of Mordell-Weil groups*, Can. J. Math. **49** (1997), 749–771. MR1471055 (98h:11087)
10. D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic Curves and Related Topics, CRM Proceedings & Lecture Notes, Vol. 4, Amer. Math. Society, Providence, 1994, pp. 125–157. MR1260960 (95a:11054)
11. D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compos. Math. **100** (1996), 311–349. MR1387669 (97m:11075)

12. D. E. Rohrlich, *Root numbers of semistable elliptic curves in division towers*, Math. Research Letters **13** (2006), 359–376. MR2231124 (2007c:11072)
13. J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, written with the collaboration of W. Kuyk and J. Labute, W. A. Benjamin, New York, 1968. MR0263823 (41:8422)
14. J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331. MR0387283 (52:8126)
15. J.-P. Serre, *Linear Representations of Finite Groups*, translated from the French by L. S. Scott, Springer-Verlag, New York, 1977. MR0450380 (56:8675)
16. J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. Math. **88** (1968), 492–517. MR0236190 (38:4488)
17. M. Shuter, *Rational points of elliptic curves in p-division fields* (to appear).
18. J. Tate, *Number theoretic background*, Automorphic Forms, Representations, and *L*-Functions, Proc. Sympos. Pure Math. Vol. 33 – Part 2, Amer. Math. Society, Providence, 1979, pp. 3–26. MR546607 (80m:12009)

Department of Mathematics and Statistics, Boston University, Boston, Massachusetts 02215

E-mail address: rohrlich@math.bu.edu