Math. Res. Lett. **13** (2006), *no.* 3, 359–376

ROOT NUMBERS OF SEMISTABLE ELLIPTIC CURVES IN DIVISION TOWERS

David E. Rohrlich

The growth of the Mordell-Weil rank of an elliptic curve in a tower of number fields can be discussed at many levels. On the one hand, the issues raised can be embedded in a broader Iwasawa theory of elliptic curves (Mazur [10]); on the other hand, they can be crystallized in a single easily stated question, namely whether the rank of the elliptic curve over subextensions of finite degree is bounded in the tower. But whatever one's point of view, the case of abelian towers has seen important advances in recent years, including notably the results of Kato on cyclotomic towers, of Cornut [2] and Vatsal [18] on anticyclotomic towers, and of Skinner and Urban on Mazur's conjecture. In the case of nonabelian towers, by contrast, virtually nothing is known, and even a conjectural framework has begun to emerge only recently [1]. However Greenberg [7] observed more than twenty years ago that some insight could already be gained from the classical conjectures about L-functions: They imply that for certain pairs (E_1, E_2) of elliptic curves of relatively prime conductor there exist primes p such that the rank of E_1 is unbounded in the p-division tower of E_2 (which can be chosen not to have complex multiplication, so that the division tower is nonabelian). Greenberg's idea was elaborated further by L. Howe [8], who gave a conjectural lower bound for the growth of the rank of E_1 in the division tower of E_2. The aim of the present note is to show that the standard conjectures also have some bearing on the growth of the rank of an elliptic curve in its own division tower. For example, we shall see that if E is a semistable elliptic curve over $\mathbb{Q}$ and p is a sufficiently large prime congruent to 3 mod 4 then the rank of E should be unbounded in its p-division tower.

As in the papers of Greenberg and Howe, the mechanism for arriving at such conclusions is a root number calculation. Fix a number field F, an elliptic curve E over F, and a prime p, and put $F^\infty = F(E[p^\infty])$, where $E[p^\infty]$ denotes the group of points on E of p-power order. The root numbers at issue here are associated to the L-functions $L(s, E, \tau)$, where τ runs over irreducible self-dual representations of $\mathrm{Gal}(F^\infty/F)$. For a precise definition of $L(s, E, \tau)$ we refer the reader to [12], pp. 151 and 156, or to [1], §5, but we should at least spell out our group-theoretic conventions: First of all, a *representation* of a topological group is understood to be continuous, finite-dimensional, and defined over the complex numbers. In particular, in the case of a profinite group like $\mathrm{Gal}(F^\infty/F)$ a representation is trivial on an open subgroup and hence factors through a finite quotient. It also follows that when the term *character* is used in the sense of "one-dimensional representation" we are

Received by the editors May 25, 2005.
Research partially supported by NSF grant DMS-9396090

talking about a continuous homomorphism to $\mathbb{C}^\times$. On the other hand, if we think of a character as the trace of a representation of arbitrary dimension then in the case of a compact group like $\mathrm{Gal}(F^\infty/F)$ characters provide a criterion for self-duality: a representation τ is self-dual – in other words isomorphic to the contragredient representation $\tau^\vee$ – if and only if $\mathrm{tr}\,\tau$ is real-valued. Returning now to E and F^∞, suppose that τ is an irreducible self-dual representation of $\mathrm{Gal}(F^\infty/F)$, and write $W(E,\tau)$ for the associated root number (cf. [13], pp. 329 and 336). Since $\tau \cong \tau^\vee$, the conjectural functional equation of $L(s,E,\tau)$ relates this function to itself and thus implies that the order of vanishing of $L(s,E,\tau)$ at $s=1$ is even or odd according as $W(E,\tau)$ is 1 or -1. On the other hand, a Galois-equivariant version of the conjecture of Birch and Swinnerton-Dyer (deducible from the usual version plus the Deligne-Gross conjecture; cf. [5], p. 323 and [11], p. 127) asserts that the order of vanishing of $L(s,E,\tau)$ at $s=1$ is the multiplicity of τ in $\mathbb{C}\otimes E(F^\infty)$. The upshot is that if we grant the standard conjectures then for irreducible self-dual τ the condition $W(E,\tau)=-1$ is sufficient for τ to occur in $\mathbb{C}\otimes E(F^\infty)$.

Standing assumptions. This note gives an explicit calculation of $W(E,\tau)$ under some simplifying assumptions on E and p which will henceforth always be in force. The assumptions are as follows:

- E is semistable over F.
- p is odd.
- The natural embedding of $\mathrm{Gal}(F^\infty/F)$ in the group of linear automorphisms of the p-adic Tate module $T_p(E)$ is an isomorphism.
- If v is a finite place of F where E has bad reduction then the residue characteristic of v is not p and $\mathrm{ord}_v j(E) \not\equiv 0 \bmod p$.

Since E is assumed semistable, a bad place is one at which $j(E)$ has negative valuation, so the last assumption can be written symbolically as

$$v(j(E)) < 0 \implies v \nmid p \text{ and } p \nmid v(j(E)).$$

We also remark that while the hypothesis of semistability is severely restrictive, our other assumptions are automatically satisfied if p is sufficiently large relative to E, provided E does not have complex multiplication. Of course it is essential to exclude curves with complex multiplication for the sake of the surjectivity of $\mathrm{Gal}(F^\infty/F) \to \mathrm{Aut}(T_p(E))$ for large p, which is then a theorem of Serre [15].

Notation. Our assumption that $\mathrm{Gal}(F^\infty/F) \to \mathrm{Aut}(T_p(E))$ is surjective enables us to identify $\mathrm{Gal}(F^\infty/F)$ with $\mathrm{GL}(2,\mathbb{Z}_p)$ and hence representations of the former group with representations of the latter. The implicit choice here of a basis for $T_p(E)$ over $\mathbb{Z}_p$ is harmless for our purposes, because changing the basis amounts to composing the given isomorphism $\mathrm{Gal}(F^\infty/F) \cong \mathrm{GL}(2,\mathbb{Z}_p)$ with an inner automorphism of $\mathrm{GL}(2,\mathbb{Z}_p)$, and consequently the correspondence between isomorphism classes of representations of the two groups is unaffected. Thus in the statement of our main result we may view τ simply as an irreducible self-dual representation of $\mathrm{GL}(2,\mathbb{Z}_p)$. Among all such representations certain ones play a special role and will now get a special notation.

First of all, 1 denotes the trivial character of $\mathrm{GL}(2,\mathbb{Z}_p)$, or indeed of any group. Also λ denotes the "Legendre symbol" on $\mathbb{Z}_p^\times$ or $\mathrm{GL}(2,\mathbb{Z}_p)$, in other words the unique

quadratic character of these groups. Note that the Legendre symbol on $\mathrm{GL}(2,\mathbb{Z}_p)$ is the composition of the Legendre symbol on $\mathbb{Z}_p^\times$ with the determinant $\mathrm{GL}(2,\mathbb{Z}_p) \to \mathbb{Z}_p^\times$.

The irreducible p-dimensional *Steinberg representation* of $\mathrm{GL}(2,\mathbb{Z}_p)$ will be denoted σ. It is trivial both on the subgroup of scalar matrices and on the kernel of reduction modulo p and can therefore be viewed as a representation both of $\mathrm{PGL}(2,\mathbb{Z}_p)$ and of $\mathrm{GL}(2,\mathbb{F}_p)$. In the former guise σ appears as the representation u_1 of Silberger's classification (cf. [16], p. 96); in the latter it is the representation of type II with $\mu = 1$ in Lang's table ([9], p. 722, Theorem 12.6).

The Steinberg representation is actually the case $i = 1$ of a family of irreducible representations σ_i ($i \geqslant 1$). Put $G = \mathrm{GL}(2,\mathbb{Z}_p)$, let B be the upper triangular subgroup of G, and for an integer $n \geqslant 1$ let $K(n)$ denote the kernel of reduction modulo p^n on G. Given a subgroup H of G we set $H(n) = HK(n)$. It is also convenient to set $H(0) = G$. Then σ_n can be defined up to equivalence as the complement of one induced representation in another:

$$\mathrm{ind}_{B(n)}^G 1 = \sigma_n \oplus \mathrm{ind}_{B(n-1)}^G 1.$$

The point here is that $B(n)$ is a subgroup of $B(n-1)$ and hence $\mathrm{ind}_{B(n-1)}^G 1$ is a subrepresentation of $\mathrm{ind}_{B(n)}^G 1$. It follows by induction that

$$\mathrm{ind}_{B(n)}^G 1 = 1 \oplus \sigma_1 \oplus \sigma_2 \oplus \cdots \oplus \sigma_n,$$

and referring to [16], pp. 58–59, we find that σ_i coincides with Silberger's $u_{1,i}$ when viewed as a representation of $\mathrm{PGL}(2,\mathbb{Z}_p)$. Thus $\sigma_1 = \sigma$ and σ_i is irreducible of dimension $p^i - p^{i-2}$ for $i \geqslant 2$.

More notation. Before proceeding further with representations of $\mathrm{GL}(2,\mathbb{Z}_p)$, we introduce a general notation for characters of B: If μ and ν are characters of $\mathbb{Z}_p^\times$ then $\xi_{\mu,\nu}$ is the character of B defined by

$$\xi_{\mu,\nu}(b) = \mu(b_{11})\nu(b_{22}) \qquad (b \in B),$$

where b_{ij} is the ij-entry of b. If the conductor of μ and the conductor of ν both divide p^n then $\xi_{\mu,\nu}$ extends uniquely to a character of $B(n)$ trivial on $K(n)$, and we denote the latter character $\xi_{\mu,\nu}$ also.

Now take $\mu = 1$ and $\nu = \lambda$, and put $\theta_1 = \mathrm{ind}_{B(1)}^G \xi_{1,\lambda}$. For $n \geqslant 2$ we define a representation θ_n up to isomorphism by writing

$$\mathrm{ind}_{B(n)}^G \xi_{1,\lambda} = \theta_n \oplus \mathrm{ind}_{B(n-1)}^G \xi_{1,\lambda},$$

so that

$$\mathrm{ind}_{B(n)}^G \xi_{1,\lambda} = \theta_1 \oplus \theta_2 \oplus \cdots \oplus \theta_n.$$

Since θ_i does not factor through $\mathrm{PGL}(2,\mathbb{Z}_p)$ it does not figure in [16], but using the double coset representatives for $B(n)\backslash G/B(n)$ given on p. 60 of [16] and applying the formula for the restriction of an induced representation to the subgroup from which it was induced, one finds that θ_1 is irreducible of dimension $p+1$ and θ_i irreducible of dimension $p^i - p^{i-2}$ for $i \geqslant 2$.

There are two more families requiring special mention. By a *primitive principal series representation with trivial central character* we mean a representation of the form $\mathrm{ind}_{B(n)}^{G}\xi_{\alpha,\alpha^{-1}}$ with α a character of $\mathbb{Z}_p^\times$ of conductor p^n and order > 2. Such a representation factors through $\mathrm{PGL}(2,\mathbb{Z}_p)$ and is isomorphic as a representation of the latter group to Silberger's u_α ([16], p. 59). On the other hand, a *primitive unramified discrete series representation with trivial central character* is one which as a representation of $\mathrm{PGL}(2,\mathbb{Z}_p)$ is isomorphic to Silberger's u_π ([16], p. 80) for some character π of the multiplicative group of the unramified quadratic extension of F. It will be convenient to write Φ for the set of isomorphism classes of all representations which are of one of the two types just mentioned. Given an arbitrary representation τ of $\mathrm{GL}(2,\mathbb{Z}_p)$, we write $[\tau]$ for its isomorphism class, so the notation $[\tau] \in \Phi$ will mean that τ is either a primitive principal series representation with trivial central character or else a primitive unramified discrete series representation with trivial central character.

The main theorem. For each finite place v of F let m_v denote the order of the residue class field of v. Our assumption that $v \nmid p$ whenever $v(j(E)) < 0$ means that if v is a place of bad reduction for E then $p \nmid m_v$. In particular, at a bad place v we can speak of the order o_v of m_v modulo p as well as the index $i_v = (p-1)/o_v$ of the subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ generated by m_v modulo p. We can also classify m_v as either a quadratic residue or a quadratic nonresidue modulo p. In the following theorem we let s denote the number of places v where E has split multiplicative reduction, s_{qr} and s_{nr} the number of such places at which m_v modulo p is a quadratic residue or a quadratic nonresidue respectively, and t the number of places v where E has *nonsplit* multiplicative reduction and i_v is odd. As usual, r_1 and $2r_2$ are the number of real and complex embeddings of F.

Theorem 1. *Let τ be an irreducible self-dual representation of* $\mathrm{Gal}(L/F)$*, and let w be the integer modulo* 2 *such that $W(E,\tau) = (-1)^w$.*

- *If $\tau = 1$ then $w = r_1 + r_2 + s \pmod 2$.*
- *If $\tau = \lambda$ then $w = r_1(p+1)/2 + r_2 + s_{\mathrm{qr}} + t \pmod 2$.*
- *If $\tau \cong \sigma$ then $w = r_1(p+1)/2 + r_2 + s \pmod 2$.*
- *If $\tau \cong \sigma \otimes \lambda$ then $w = r_1 + r_2 + s_{\mathrm{qr}} + t \pmod 2$.*
- *If $\tau \cong \sigma_i$ with $i \geqslant 2$ or $\tau \cong \theta_i$ with $i \geqslant 1$ then $w = s_{\mathrm{nr}} + t \pmod 2$.*
- *If $[\tau] \in \Phi$ then $w = r_1(p-1)/2 \pmod 2$.*

In all other cases $w = 0 \pmod 2$, so that $W(E,\tau) = 1$.

Examples. 1) If $p \equiv 3 \pmod 4$ and r_1 is odd then $W(E,\tau) = -1$ for $[\tau] \in \Phi$. Such τ constitute an infinite family of isomorphism classes.

2) If $F = \mathbb{Q}$ and E is the modular curve $X_0(11)$ then E has split multiplicative reduction at 11 and good reduction elsewhere. Furthermore $j(E) = -2^{12}/11$, and for $p \neq 5$ the natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_p(E)$ gives an isomorphism $\mathrm{Gal}(\mathbb{Q}^\infty/\mathbb{Q}) \cong \mathrm{GL}(2,\mathbb{Z}_p)$ ([15], p. 309). Hence our assumptions are satisfied if $p \neq 2, 5, 11$, and we

find that

$$W(E,\tau)=\begin{cases}\left(\dfrac{p}{11}\right) & \text{if } \tau=\lambda\\ \left(\dfrac{-1}{p}\right) & \text{if } \tau\cong\sigma \text{ or } [\tau]\in\Phi\\ \left(\dfrac{11}{p}\right) & \text{if } \tau\cong\sigma\otimes\lambda \text{ or } \tau\cong\sigma_i\ (i\geqslant 2) \text{ or } \tau\cong\theta_i\ (i\geqslant 1)\end{cases}$$

with $W(E,\tau)=1$ in all other cases.

Organization of the paper. One peculiarity of this note is that our "calculation" of $W(E,\tau)$ is largely a matter of assembling a number of little facts about the group $\mathrm{GL}(2,\mathbb{Z}_p)$ and its representations. Much of what is needed will simply be quoted from Silberger's monograph [16], and it would not be surprising if it turned out that some of the proofs which we do supply could also have been replaced by references to the literature. A possible case in point is our Proposition 4, most of which follows from the determinant calculations of Howe [8]. Be that as it may, the first three sections of the paper are devoted respectively to the dimensions of the irreducible self-dual representations, the determinants of these representations, and the multiplicities with which they occur in certain induced representations. The fourth and final section is devoted to the derivation of a formula from which Theorem 1 is then easily deduced.

Acknowledgments. The problem treated in this note was suggested to me more than a decade ago by Ralph Greenberg and subsequently also by Susan Howson, and I would like to express my thanks to both of them, along with my apologies for taking so long to return to the problem after prematurely setting it aside. I am also indebted to Jerry Tunnell, not only in connection with the present paper but also in connection with several others, for a casual remark at a seminar dinner many years ago to the effect that statements like Rubin's theorem [14] should hold with characters of finite order replaced by arbitrary Artin representations. Finally, I would like to acknowledge the support of the National Science Foundation (grant DMS-9396090) during the first of my two bouts with the problem addressed here.

Postscript. After submitting this paper for publication I learned from Ralph Greenberg and John Coates of some unpublished calculations of Seidai Yasuda, whom I then contacted and who kindly sent me a copy of his work. Yasuda obtains partial results under more general hypotheses, and it is a pleasure to acknowledge his prior discovery of many cases of Theorem 1. I am also grateful to Coates for drawing my attention to a forthcoming paper of Vladimir Dokchitser, who calculates twisted root numbers in the solvable nonabelian towers over $\mathbb{Q}$ afforded by certain radical extensions of cyclotomic extensions.

The referee asks whether the points of infinite order on E, which should exist by Theorem 1, can somehow be accounted for by special points on Shimura curves. My guess is that for $p\geqslant 5$ the nonsolvability of $\mathrm{GL}(2,\mathbb{Z}_p)$ precludes this possibility, but the larger question that the referee raises – where do these points of infinite order come from? – is a natural one. It is even more compelling in light of a remark of Coates, who has informed me that under suitable hypotheses on the relevant Selmer group, the rank of E over the nth layer of the $\mathrm{PGL}(2,\mathbb{Z}_p)$-extension contained in F^∞

is bounded above by a constant times p^{2n}. Coates asked me what one could deduce from Theorem 1 about the order of vanishing at $s = 1$ of the L-function of E over the nth layer. The answer is that in the optimal case (namely r_1 odd and $p \equiv 3$ modulo 4) the lower bound for the order of vanishing which follows from Theorem 1 is in fact asymptotic to p^{2n}. The calculation by which this lower bound is deduced from Theorem 1 is identical to the corresponding calculation in [8].

1. Dimensions

Given $z \in \mathbb{Z}_p^\times$ let $\iota(z)$ denote the scalar matrix $z \cdot I$, where I is the 2×2 identity matrix. By the *central character* of an irreducible representation τ of $\mathrm{GL}(2, \mathbb{Z}_p)$ we mean the character $\omega : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ such that $\tau(\iota(z))$ is multiplication by $\omega(z)$ for $z \in \mathbb{Z}_p^\times$. Of course the existence of ω follows from Schur's lemma, and ω is trivial if and only if τ factors through $\mathrm{PGL}(2, \mathbb{Z}_p)$. Note also that if τ is self-dual then ω takes values in $\{\pm 1\}$. We shall prove that if τ is self-dual and ω nontrivial then τ is induced from an open subgroup of index 2 in $\mathrm{GL}(2, \mathbb{Z}_p)$, whence in particular τ is of even degree.

Lemma. *Every element of* $\mathrm{GL}(2, \mathbb{Z}_p)$ *is conjugate to its transpose.*

Proof. Over a field it is a standard remark that every square matrix is similar to its transpose. Perhaps the lemma can be deduced from this fact, but instead we give the following *ad hoc* argument.

Let $\mathcal{S}$ be the subset of $\mathrm{GL}(2, \mathbb{Z}_p)$ consisting of matrices which are conjugate to their transpose. We wish to prove that $\mathcal{S} = \mathrm{GL}(2, \mathbb{Z}_p)$. A preliminary observation is that $\mathcal{S}$ is closed under transpose and under conjugation by symmetric matrices in $\mathrm{GL}(2, \mathbb{Z}_p)$. (To verify the latter point, suppose that $\gamma A \gamma^{-1} = A^{\mathrm{t}}$ and $U = U^{\mathrm{t}}$; then $\delta U A U^{-1} \delta^{-1} = (U A U^{-1})^{\mathrm{t}}$ with $\delta = U^{-1} \gamma U^{-1}$.) We also remark that any product of two symmetric matrices in $\mathrm{GL}(2, \mathbb{Z}_p)$ belongs to $\mathcal{S}$. Indeed if $A = BC$ with elements $B = B^{\mathrm{t}}$ and $C = C^{\mathrm{t}}$ of $\mathrm{GL}(2, \mathbb{Z}_p)$, then $A^{\mathrm{t}} = CB = CAC^{-1}$, and consequently $A \in \mathcal{S}$.

To prove that an arbitrary element

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

of $\mathrm{GL}(2, \mathbb{Z}_p)$ belongs to $\mathcal{S}$ we may assume that $\mathrm{ord}_p(b) \leqslant \mathrm{ord}_p(c)$, because $\mathcal{S}$ is closed under transpose. We consider three cases:

(i) $b = 0$.
(ii) $b \neq 0$ and $\mathrm{ord}_p(b) \leqslant \mathrm{ord}_p(a - d)$.
(iii) $\mathrm{ord}_p(b) > \mathrm{ord}_p(a - d)$.

In case (i) our hypothesis $\mathrm{ord}_p(b) \leqslant \mathrm{ord}_p(c)$ implies that $b = c = 0$, and the conclusion $A \in \mathcal{S}$ is immediate. In case (ii) we have $A = BC$ with the symmetric matrices

$$B = \begin{pmatrix} b & d \\ d & c - (a-d)d/b \end{pmatrix} \qquad \text{and} \qquad C = \begin{pmatrix} (a-d)/b & 1 \\ 1 & 0 \end{pmatrix},$$

whence again $A \in \mathcal{S}$. Finally, in case (iii) our assumption $\mathrm{ord}_p(b) \leqslant \mathrm{ord}_p(c)$ implies that $\mathrm{ord}_p(c) > \mathrm{ord}_p(a - d)$ also. Putting $A' = UAU^{-1}$ with

$$U = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

and writing

$$A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix},$$

we find that $c' = b$ and $b' = (a-d)-(b-c)$, whence $\mathrm{ord}_p(b') = \mathrm{ord}_p(a-d) < \mathrm{ord}_p(c')$. Thus our standing assumption $\mathrm{ord}_p(b) \leqslant \mathrm{ord}_p(c)$ now holds with A replaced by A'. It also follows that $b' \neq 0$. In fact we are back to case (ii), because $a' - d' = 2b - (a-d)$ and consequently $\mathrm{ord}_p(a'-d') = \mathrm{ord}_p(a-d) = \mathrm{ord}_p(b')$. We conclude that $A' \in \mathcal{S}$. Since $\mathcal{S}$ is invariant under conjugation by symmetric matrices it follows that $A \in \mathcal{S}$ also. □

Proposition 1. *Let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$, and suppose that the central character ω of τ is nontrivial. Let H be the kernel of the map $\omega \circ \det : \mathrm{GL}(2, \mathbb{Z}_p) \to \{\pm 1\}$. Then τ is induced from H.*

Proof. Put

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then

$$s g^{\mathrm{t}} s^{-1} = \iota(\det g) g^{-1}$$

for all $g \in \mathrm{GL}(2, \mathbb{Z}_p)$, and $\mathrm{tr}\,\tau(g^{-1}) = \mathrm{tr}\,\tau(g)$ because τ is self-dual. So the lemma gives

$$\mathrm{tr}\,\tau(g) = \omega(\det g)\,\mathrm{tr}\,\tau(g).$$

But if $g \notin H$ then $\omega(\det g) \neq 1$. Consequently $\mathrm{tr}\,\tau$ vanishes on the complement of H, whence τ is induced from H by Clifford's theorem (cf. [6], p. 64). □

It follows that if $\omega \neq 1$ then $\dim \tau$ is even. The next point is that the stronger hypothesis $\omega(-1) = -1$ leads to the stronger conclusion $\dim \tau \equiv 0 \bmod 4$. The proof will for the first time make use of our standing assumption that p is odd, an assumption which by the way would allow us to replace the hypothesis "$\omega(-1) = -1$" by the equivalent condition "$\omega \neq 1$ and $p \equiv 3 \bmod 4$."

Lemma. *Let Q denote the quaternion group of order 8. Then Q has an embedding in $\mathrm{SL}(2, \mathbb{Z}_p)$, and the image of any such embedding contains the element $-I$.*

Proof. The second assertion follows from the fact that $-I$ is the unique element of order two in $\mathrm{SL}(2, \mathbb{Z}_p)$. For the first assertion we recall that up to isomorphism Q has a unique two-dimensional irreducible representation ρ. Furthermore ρ is faithful, $\det \rho$ is trivial, $\mathrm{tr}\,\rho$ is $\mathbb{Z}$-valued, and the local Schur index of ρ at p, say $m_p(\rho)$, is 1 because p is odd (cf. [3], vol. 2, p. 743). Let $\overline{\mathbb{Q}}$ denote an algebraic closure of $\mathbb{Q}$ which is contained both in $\mathbb{C}$ and in an algebraic closure of $\mathbb{Q}_p$. Then the embedding $Q \to \mathrm{SL}(2, \mathbb{C})$ afforded by ρ can *a priori* be conjugated to an embedding into $\mathrm{SL}(2, \overline{\mathbb{Q}})$, and the triviality of $m_p(\rho)$ implies that ρ can actually be conjugated to an embedding into $\mathrm{SL}(2, \mathbb{Q}_p)$. Finally, the choice of a Q-stable $\mathbb{Z}_p$-lattice in $\mathbb{Q}_p^2$ determines a conjugation of ρ which embeds Q in $\mathrm{SL}(2, \mathbb{Z}_p)$. □

Remark. Another way to prove the lemma is to use the natural embedding of Q in $\mathbb{H}^\times$, where $\mathbb{H} = \mathbb{Q} + \mathbb{Q}\,i + \mathbb{Q}\,j + \mathbb{Q}\,k$ is the standard $\mathbb{Q}$-form of the division algebra of Hamiltonian quaternions. The key point is then that $\mathbb{H}$ splits at p.

Proposition 2. *With notation and hypotheses as in Proposition 1, assume that* $\omega(-1) = -1$. *Then* $\dim \tau \equiv 0$ *modulo* 4.

Proof. Let H be as in Proposition 1, so that τ is induced by a representation π of H. By the lemma we may view Q as a subgroup of H containing $-I$. Thus it is meaningful to ask for a decomposition of $\pi|Q$ into irreducibles, and our assumption on ω implies that any irreducible occurring in $\pi|Q$ sends $-I$ to scalar multiplication by -1. But up to equivalence the irreducible representations of Q consist of the two-dimensional representation ρ and four one-dimensional characters, and the latter are trivial on $-I$. Hence $\pi|Q$ is isomorphic to a direct sum of copies of ρ, and consequently $\dim \pi$ is even. Therefore $\dim \tau$ is divisible by 4. $\square$

Proposition 3. *Let* τ *be an irreducible self-dual representation of* $\mathrm{GL}(2, \mathbb{Z}_p)$ *which is not isomorphic to* 1, λ, σ, *or* $\sigma \otimes \lambda$. *Then* $\dim \tau$ *is even.*

Proof. Let ω be the central character of τ. If $\omega \neq 1$ then the assertion follows from Proposition 1. Otherwise we view τ as a representation of $\mathrm{PGL}(2, \mathbb{Z}_p)$ and appeal to the results of Silberger ([16], pp. 96 – 97), which under our assumptions imply that either $\dim \tau = p^n \pm p^{n-1}$ with $n \geqslant 1$ or $\dim \tau = p^n - p^{n-2}$ with $n \geqslant 2$. $\square$

2. Determinants

The following statement will enable us to compute the determinant of complex conjugation once we return to the Galois setting. The case of trivial central character was treated by Howe [8] using a different method.

Proposition 4. *Let* τ *be an irreducible self-dual representation of* $\mathrm{GL}(2, \mathbb{Z}_p)$, *and let* $c \in \mathrm{GL}(2, \mathbb{Z}_p)$ *be an element satisfying* $c^2 = 1$ *and* $\det(c) = -1$. *If* $\tau = \lambda$ *or* $\tau \cong \sigma$ *or* $[\tau] \in \Phi$ *then* $\det \tau(c) = (-1)^{(p-1)/2}$. *Otherwise* $\det \tau(c) = 1$.

Proof. If $\dim \tau = 1$, or in other words if τ is 1 or λ, then τ is indistinguishable from $\det \tau$ and the assertion is immediate. Henceforth we assume that $\dim \tau > 1$.

The proof will be based on the formula

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

To verify $(*)$, let $d_\pm$ denote the multiplicity of the eigenvalue ± 1 in $\tau(c)$. Then $\dim \tau = d_+ + d_-$ and $\mathrm{tr}\, \tau(c) = d_+ - d_-$, whence $d_- = (\dim \tau - \mathrm{tr}\, \tau(c))/2$.

Let ω be the central character of τ. To apply $(*)$ with $\dim \tau > 1$ we consider five cases:

(i) $\omega \neq 1$.
(ii) $\tau \cong \sigma$ or $\tau \cong \sigma \otimes \lambda$.
(iii) τ is a primitive principal series representation with $\omega = 1$.
(iv) τ is a primitive unramified discrete series representation with $\omega = 1$.
(v) $\omega = 1$ but τ is not as in (ii), (iii), or (iv).

In cases (i) and (v) and in the case of the second alternative in (ii) we must show that $\det \tau(c) = 1$; otherwise we must show that $\det \tau(c) = (-1)^{(p-1)/2}$.

First suppose that (i) holds. If $\det \tau(c) \neq 1$ then $\det \tau$ is a nontrivial one-dimensional real-valued character of $\mathrm{GL}(2, \mathbb{Z}_p)$ and hence coincides with the unique

such, namely λ. Similarly $\omega \circ \det = \lambda$ because $\omega \neq 1$ by assumption. Hence $\det \tau = \omega \circ \det$, and in particular, since $\det \tau(c) \neq 1$, we see that c does not belong to the kernel H of $\omega \circ \det$. But τ is induced from H (Proposition 1) and H is normal in $\mathrm{GL}(2, \mathbb{Z}_p)$, so it follows that $\operatorname{tr} \tau(c) = 0$. Since $\dim \tau \equiv 0 \bmod 4$ by Proposition 2 (applicable here because by assumption $\det \tau(c) \neq 1$ and $\omega \circ \det = \det \tau$, whence $\omega(-1) = \det \tau(c) = -1$) we see from $(*)$ that $\det \tau(c) = 1$.

To handle cases (ii) through (v) we will use the character tables in [16], and in this connection we remark that c is conjugate in $\mathrm{GL}(2, \mathbb{Z}_p)$ to the diagonal matrix with entries -1 and 1. Indeed if we view c as a $\mathbb{Z}_p$-linear automorphism of $\mathbb{Z}_p^2$ then $\mathbb{Z}_p^2$ is the direct sum of its images under the idempotents $(1+c)/2$ and $(1-c)/2$, whence a basis respecting the direct sum decomposition gives the desired diagonalization of c.

Now consider case (ii). The first table on p. 102 of [16] indicates that $\operatorname{tr} \tau(c) = 1$ or $\operatorname{tr} \tau(c) = \lambda(-1)$ according as $\tau \cong \sigma$ or $\tau \cong \sigma \otimes \lambda$. Applying $(*)$, we deduce that if $\tau \cong \sigma$ then $\det \tau(c) = (-1)^{(p-1)/2}$ while if $\tau \cong \sigma \otimes \lambda$ then $\det \tau(c) = (-1)^{(p-\lambda(-1))/2} = 1$.

For case (iii) we consult the second table on p. 102 of [16], taking the parameter t of [16] to be -1 and observing that the p-adic absolute value of $t - t^{-1}$ is 1 since p is odd. We obtain $\operatorname{tr} \tau(c) = \pm 2$. On the other hand, $\dim \tau$ has the form $p^{m-1}(p+1)$ with an integer $m \geqslant 1$. Hence $\operatorname{tr} \tau(c) = (-1)^{(p-1)/2}$ by $(*)$.

In case (iv) the relevant character table is the first table on p. 105, and the conjugacy class of c is missing. By convention, the omission means that $\operatorname{tr} \tau(c) = 0$. Since $\dim \tau$ has the form $p^{m-1}(p-1)$ we obtain $\operatorname{tr} \tau(c) = (-1)^{(p-1)/2}$ once again.

Finally, the conjugacy class of c is missing from all of the tables on pp. 102 – 107 of [16] not already consulted. Hence $\operatorname{tr} \tau(c) = 0$ in the remaining cases. In addition $\dim \tau$ has the form $p^{i-2}(p^2-1)$ with an integer $i \geqslant 2$. We conclude that $\det \tau(c) = 1$ in case (v). $\square$

3. Multiplicities

Given representations π and τ of a profinite group G we define $\langle \pi, \tau \rangle$ by putting

$$\langle \pi, \tau \rangle = \sum_{\rho} (\text{multiplicity of } \rho \text{ in } \pi)(\text{multiplicity of } \rho \text{ in } \tau),$$

where the sum runs over the set of equivalence classes of irreducible representations ρ of G. If H is an open subgroup of G and η a representation of H then in an equation like

$$\langle \eta, \operatorname{res}_H^G \pi \rangle = \langle \operatorname{ind}_H^G \eta, \pi \rangle$$

(Frobenius reciprocity) the brackets on the left and right carry an implicit subscript H and G, the omission of which should cause no confusion.

Henceforth $G = \mathrm{GL}(2, \mathbb{Z}_p)$. Our goal is to compute the parity of the integer $\langle \pi, \tau \rangle$ in three special cases. In all three cases π is monomial, induced either by the trivial character of a subgroup (Proposition 5 below) or by a quadratic character (Propositions 6 and 7). Throughout, U denotes the open subgroup of $\mathbb{Z}_p^\times$ topologically generated by a fixed rational integer $m \geqslant 2$ with $p \nmid m$, and J is the subgroup of G consisting of matrices of the form

$$b(u, z) = \begin{pmatrix} u & z \\ 0 & 1 \end{pmatrix} \tag{3.1}$$

with $u \in U$ and $z \in \mathbb{Z}_p$. We recall that for any subgroup H of G we have put $H(n) = HK(n)$, where $K(n)$ denotes the kernel of reduction mod p^n on G ($n \geqslant 1$).

Proposition 5. *Let τ be an irreducible self-dual representation of G, and choose $n \geqslant 1$ so that $1 + p^n \in U$ and τ factors through $G/K(n)$.*

- *If $\tau = 1$ or $\tau \cong \sigma$ then $\langle \mathrm{ind}_{J(n)}^G 1, \tau \rangle$ is odd.*
- *If $\tau = \lambda$ or $\tau \cong \sigma \otimes \lambda$ then $(-1)^{\langle \mathrm{ind}_{J(n)}^G 1, \tau \rangle} = -\left(\dfrac{m}{p}\right)$.*
- *If $\tau \cong \sigma_i$ with $i \geqslant 2$ or $\tau \cong \theta_i$ with $i \geqslant 1$ then $(-1)^{\langle \mathrm{ind}_{J(n)}^G 1, \tau \rangle} = \left(\dfrac{m}{p}\right)$.*

In all other cases $\langle \mathrm{ind}_{J(n)}^G 1, \tau \rangle$ is even.

Proof. Throughout the proof, μ and ν denote arbitrary characters of $\mathbb{Z}_p^\times$ such that ν is trivial on $1 + p^n\mathbb{Z}_p$ and μ is trivial on U (hence in particular on $1 + p^n\mathbb{Z}_p$). Recall also that B denotes the upper triangular subgroup of G and that $\xi_{\mu,\nu}$ is the character of $B(n)$ which is trivial on $K(n)$ and satisfies $\xi_{\mu,\nu}(b) = \mu(b_{11})\nu(b_{22})$ for $b \in B$. The characters of the abelian group $B(n)/J(n)$ are therefore precisely the characters $\xi_{\mu,\nu}$ with μ and ν as indicated above, and consequently we can write

$$\mathrm{ind}_{J(n)}^{B(n)} 1 = \oplus_{\mu,\nu} \xi_{\mu,\nu}. \tag{3.2}$$

It follows by the transitivity of induction that

$$\mathrm{ind}_{J(n)}^G 1 = \oplus_{\mu,\nu} \mathrm{ind}_{B(n)}^G \xi_{\mu,\nu}. \tag{3.3}$$

Now the orbit of (μ, ν) under $(\mu, \nu) \mapsto (\mu^{-1}, \nu^{-1})$ consists of (μ, ν) alone if and only if $\mu^2 = \nu^2 = 1$. Furthermore induction and dualization commute, and therefore the representation induced by $\xi_{\mu,\nu}$ is dual to the representation induced by the inverse character $\xi_{\mu^{-1},\nu^{-1}}$. Hence after bracketing both sides of (3.3) with the self-dual representation τ we obtain

$$\langle \mathrm{ind}_{J(n)}^G 1, \tau \rangle \equiv \sum_{\mu^2=\nu^2=1} \langle \mathrm{ind}_{B(n)}^G \xi_{\mu,\nu}, \tau \rangle \pmod 2. \tag{3.4}$$

We now consider cases according as m is or is not a square modulo p.

If m is a square mod p then U is contained in $\mathbb{Z}_p^{\times 2}$. Consequently there are two solutions to $\mu^2 = 1$, namely $\mu = 1$ and $\mu = \lambda$, and so there are four terms in the sum on the right-hand side of (3.4), corresponding to $(\mu, \nu) = (1, 1), (\lambda, \lambda), (1, \lambda)$, and $(\lambda, 1)$. But it is a standard remark that

$$\mathrm{ind}_{B(n)}^G \xi_{\mu,\nu} \cong \mathrm{ind}_{B(n)}^G \xi_{\nu,\mu}. \tag{3.5}$$

(Proof: If s is as in the proof of Proposition 1, then the map $g \mapsto s(g^{\mathrm{t}})^{-1}s^{-1}$ is an automorphism of G which stabilizes $B(n)$, interchanges $\xi_{\mu,\nu}$ and $\xi_{\nu^{-1},\mu^{-1}}$, and inverts conjugacy classes, whence the character induced by $\xi_{\mu,\nu}$ is the complex conjugate of the character induced by $\xi_{\nu^{-1},\mu^{-1}}$.) Applying (3.5) with $(\mu, \nu) = (1, \lambda)$, we may rewrite (3.4) simply as

$$\langle \mathrm{ind}_{J(n)}^G 1, \tau \rangle \equiv \langle \mathrm{ind}_{B(n)}^G \xi_{1,1}, \tau \rangle + \langle \mathrm{ind}_{B(n)}^G \xi_{\lambda,\lambda}, \tau \rangle \pmod 2. \tag{3.6}$$

Referring to [16], Theorem (3.3), pp. 58–59, we see that

$$\mathrm{ind}_{B(n)}^{G}\xi_{1,1} = 1 \oplus \sigma \oplus (\cdots)$$

with $(\cdots) = \sigma_2 \oplus \sigma_3 \oplus \cdots \oplus \sigma_n$, and also (note the last line of the cited theorem)

$$\mathrm{ind}_{B(n)}^{G}\xi_{\lambda,\lambda} = \lambda \oplus (\sigma \otimes \lambda) \oplus (\cdots).$$

Hence it follows from (3.6) that

$$\langle \mathrm{ind}_{J(n)}^{G}1, \tau\rangle \equiv \langle 1, \tau\rangle + \langle \sigma, \tau\rangle + \langle \lambda, \tau\rangle + \langle \sigma\otimes\lambda, \tau\rangle \pmod 2. \tag{3.7}$$

This gives the stated result in the case where m is a square mod p, because 1, λ, σ, and $\sigma \otimes \lambda$ are pairwise nonisomorphic and none of these representations is isomorpic to σ_i $(i \geqslant 2)$ or θ_i $(i \geqslant 1)$.

Next suppose that m is a nonsquare mod p. Then λ is not trivial on U, so the only choice for μ in (3.4) is $\mu = 1$. Thus there are just two terms on the right-hand side of (3.4), and consequently

$$\langle \mathrm{ind}_{J(n)}^{G}1, \tau\rangle \equiv \langle \mathrm{ind}_{B(n)}^{G}1, \tau\rangle + \langle \mathrm{ind}_{B(n)}^{G}\xi_{1,\lambda}, \tau\rangle \pmod 2. \tag{3.8}$$

Since

$$\mathrm{ind}_{B(n)}^{G}1 = 1 \oplus (\oplus_{i=1}^{n}\sigma_i)$$

and

$$\mathrm{ind}_{B(n)}^{G}\xi_{1,\lambda} = \oplus_{i=1}^{n}\theta_i$$

we see that the right-hand side of (3.4) is odd if and only if τ is isomorphic to one of the representations 1, σ_i $(i \geqslant 1)$, or θ_i $(i \geqslant 1)$. This is again the desired conclusion when m is a quadratic nonresidue modulo p. □

The next case to consider arises only when the residue class of m modulo p has even order, as we shall now assume. Equivalently, we assume that the image of U in $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is a subgroup of even order, so that U has a unique quadratic character η'. Let J' be the group consisting of all matrices of the form $\eta'(u)b(u,z)$ with $u \in U$, $z \in \mathbb{Z}_p$, and $b(u,z)$ as in (3.1). Since $\eta'(u)$ is the lower right-hand entry of $\eta'(u)b(u,z)$ we may view η' as a character of J' by setting $\eta'(b) = b_{22} = \pm 1$ for $b \in J'$. (Note the identification of $\pm 1 \in \mathbb{Z}_p$ with $\pm 1 \in \mathbb{C}$, which is ultimately traceable to our application: The assignment of a representation of the Weil-Deligne group to an elliptic curve over a nonarchimedean local field involves an embedding of $\mathbb{Q}_p$ in $\mathbb{C}$; cf. [12], p. 147.) We extend η' to $J'(n)$ by the requirement $\eta'|K(n) = 1$.

Proposition 6. *With τ and n as in Proposition 5, assume that the residue class of m modulo p has even order. If $\tau = \lambda$ or $\tau \cong \sigma \otimes \lambda$ or $\tau \cong \sigma_i$ with $i \geqslant 2$ or $\tau \cong \theta_i$ with $i \geqslant 1$ then*

$$\langle \mathrm{ind}_{J'(n)}^{G}\eta', \tau\rangle \equiv [\mathbb{Z}_p^{\times} : U] \pmod 2.$$

Otherwise $\langle \mathrm{ind}_{J'(n)}^{G}\eta', \tau\rangle$ is even.

Proof. The analogue of (3.2) in this case is

$$\mathrm{ind}_{J'(n)}^{B(n)}\eta' = \oplus_{\mu,\nu}\,\xi_{\mu,\nu}, \tag{3.9}$$

where μ and ν are characters of $\mathbb{Z}_p^\times$ which are trivial on $1+p^n\mathbb{Z}_p$ and satisfy

$$\xi_{\mu,\nu}|J' = \eta'. \tag{3.10}$$

Since η' is quadratic, the validity of (3.10) is invariant under $(\mu,\nu)\mapsto(\mu^{-1},\nu^{-1})$, whence it follows as in (3.3) and (3.4) that

$$\langle \mathrm{ind}_{J'(n)}^G \eta', \tau\rangle \equiv \sum_{\mu^2=\nu^2=1} \langle \mathrm{ind}_{B(n)}^G \xi_{\mu,\nu}, \tau\rangle \pmod 2. \tag{3.11}$$

We must determine which of the four pairs $(\mu,\nu)=(1,1),(\lambda,\lambda),(1,\lambda)$, and $(\lambda,1)$ actually satisfies (3.10) and hence occurs on the right-hand side of (3.11). Since every $b\in J'$ has the form $b=\eta'(u)b(u,z)$ with $u\in U$ and $z\in\mathbb{Z}_p$, we may rewrite (3.10) by making the substitutions $b_{11}=\eta'(u)u$ and $b_{22}=\eta'(u)$. The result is

$$\mu(\eta'(u)u)\nu(\eta'(u)) = \eta'(u). \tag{3.12}$$

This condition already shows that the pair $(\mu,\nu)=(1,1)$ does not occur in (3.11), because $\eta'\neq 1$. To decide about $(\lambda,\lambda),(1,\lambda)$, and $(\lambda,1)$ we consider cases according as $[\mathbb{Z}_p^\times : U]$ is even or odd.

Suppose first that $[\mathbb{Z}_p^\times : U]$ is even. Then $p\equiv 1 \bmod 4$, because by assumption the image of U in $(\mathbb{Z}/p\mathbb{Z})^\times$ has even order. Since $\mu,\nu\in\{1,\lambda\}$ it follows that $\mu(\pm1)=\nu(\pm1)=1$. Hence condition (3.12) becomes

$$\mu(u) = \eta'(u). \tag{3.13}$$

But the assumption that $[\mathbb{Z}_p^\times : U]$ is even also implies that $U\subset\mathbb{Z}_p^{\times 2}$, and consequently $\mu|U$ is trivial, whereas η' is nontrivial. Thus none of our pairs (μ,ν) satisfies (3.13), whence the sum in (3.11) is empty and $\langle \mathrm{ind}_{J'(n)}^G\eta',\tau\rangle$ is even. Given that $[\mathbb{Z}_p^\times : U]$ is also even this is the desired conclusion.

Next suppose that $[\mathbb{Z}_p^\times : U]$ is odd. Then $\lambda|U$ is nontrivial and so coincides with the unique quadratic character of U, namely η'. If $(\mu,\nu)=(\lambda,\lambda)$ then (3.12) reduces once again to (3.13), but this time (3.13) is satisfied, because $\lambda|U=\eta'$. Thus (λ,λ) occurs in (3.11). On the other hand, if $(\mu,\nu)=(\lambda,1)$ or $(\mu,\nu)=(1,\lambda)$ then (3.12) reduces to

$$\lambda(\eta'(u)) = 1$$

or to

$$\lambda(\eta'(u)) = \eta'(u)$$

respectively. Since $\eta'(u)=\pm1$ these conditions hold if and only if $p\equiv 1 \bmod 4$ or $p\equiv 3 \bmod 4$ respectively. But the representations induced by $\xi_{\lambda,1}$ and $\xi_{1,\lambda}$ are equivalent (cf. (3.5)), so the cases $p\equiv 1 \bmod 4$ and $p\equiv 3 \bmod 4$ both lead to the same conclusion, namely

$$\langle \mathrm{ind}_{J'(n)}^G\eta',\tau\rangle \equiv \langle \mathrm{ind}_{B(n)}^G\xi_{\lambda,\lambda},\tau\rangle + \langle \mathrm{ind}_{B(n)}^G\xi_{1,\lambda},\tau\rangle \pmod 2.$$

Recalling that

$$\mathrm{ind}_{B(n)}^G\xi_{\lambda,\lambda} = \lambda\oplus(\sigma\otimes\lambda)\oplus(\oplus_{i=2}^n\sigma_i)$$

and

$$\mathrm{ind}_{B(n)}^{G}\xi_{1,\lambda} = \oplus_{i=1}^{n}\theta_i,$$

we deduce that $\langle \mathrm{ind}_{J'(n)}^{G}\eta', \tau\rangle$ is odd if and only if $\tau = \lambda$, $\tau \cong \sigma\otimes\lambda$, $\tau \cong \sigma_i$ $(i \geqslant 2)$, or $\tau \cong \theta_i$ $(i \geqslant 1)$. This is again the desired conclusion, because $[\mathbb{Z}_p^{\times} : U]$ is odd. □

Finally, suppose that the order of m modulo p is odd, put $J'' = \{\pm I\}J$, and let η'' be the quadratic character of J'' defined by $\eta''(b) = b_{22}$. We extend η'' to $J''(n)$ by the requirement $\eta''|K(n) = 1$.

Proposition 7. *With τ and n as in Proposition 5, assume that the residue class of m modulo p has odd order. Then $\langle \mathrm{ind}_{J''(n)}^{G}\eta'', \tau\rangle$ is even.*

Proof. Arguing as in the first paragraph of the proof of Proposition 6, we have

$$\langle \mathrm{ind}_{J''(n)}^{G}\eta'', \tau\rangle \equiv \sum_{\mu^2=\nu^2=1} \langle \mathrm{ind}_{B(n)}^{G}\xi_{\mu,\nu}, \tau\rangle \pmod 2, \tag{3.14}$$

where the analogue of (3.10) is now

$$\xi_{\mu,\nu}|J'' = \eta''. \tag{3.15}$$

As before, we must determine which of the four pairs $(\mu,\nu) = (1,1), (\lambda,\lambda), (1,\lambda)$, and $(\lambda,1)$ satisfy (3.15). Since J'' is now the direct product $\{\pm I\}\times J$, we can write a typical element $b \in J''$ as $b = \epsilon b(u,z)$ with arbitrary $\epsilon \in \{\pm 1\}$, $u \in U$, and $z \in \mathbb{Z}_p$. Furthermore $\mu|U = 1$ because the image of U has odd order in $(\mathbb{Z}/p\mathbb{Z})^{\times}$. Thus the requirement in (3.15) is that $\mu\nu(\epsilon) = \epsilon$; in other words, $\mu\nu$ must be odd. It follows that the pairs $(1,1)$ and (λ,λ) do not occur in (3.14). Furthermore, if $p \equiv 1 \bmod 4$ then neither $(1,\lambda)$ nor $(\lambda,1)$ occurs, while if $p \equiv 3 \bmod 4$ then both occur. However in both cases the parity of $\langle \mathrm{ind}_{J''(n)}^{G}\eta'', \tau\rangle$ is even, because the representations induced by $\xi_{1,\lambda}$ and $\xi_{\lambda,1}$ are equivalent. □

4. Proof of Theorem 1

We return to the setting of the introduction. Thus F is a number field and E is a semistable elliptic curve over F. We assume that if v is a finite place of F such that $v(j(E)) < 0$ then $v \nmid p$ and $p \nmid v(j(E))$, and we also assume that the natural map $\mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(T_p(E))$ is surjective, where $\overline{F}$ denotes a fixed algebraic closure of F. As before, we put $F^{\infty} = F(E[p^{\infty}]) \subset \overline{F}$ and identify $\mathrm{Gal}(F^{\infty}/F)$ with $\mathrm{GL}(2,\mathbb{Z}_p)$.

Locally there are also identifications. Given an arbitrary place v of F, write F_v for the completion of F at v and $\overline{F}_v$ for an algebraic closure of F_v containing $\overline{F}$, and put $F_v^{\infty} = F^{\infty}F_v$, where the compositum is formed inside $\overline{F}_v$. We shall identify $\mathrm{Gal}(F_v^{\infty}/F_v)$ with the decomposition subgroup of $\mathrm{Gal}(F^{\infty}/F)$ corresponding to the embedding $F^{\infty} \subset F_v^{\infty}$. Furthermore, any one-dimensional character δ_v of $\mathrm{Gal}(F_v^{\infty}/F_v)$ factors through $\mathrm{Gal}(K_v/F_v)$ for some finite abelian extension K_v of F_v inside F_v^{∞}, and we shall view δ_v as a character of $F_v^{\times}$ via the formula

$$\delta_v(x) = \delta_v((x^{-1}, K_v/F_v)) \qquad (x \in F_v^{\times}), \tag{4.1}$$

where $(*, K_v/F_v)$ is the local Artin symbol as normalized by Artin. Finally, given a finite place v of F such that $v(j(E)) < 0$, let $\mathcal{E}_v$ denote the Tate curve over F_v satisfying $j(\mathcal{E}_v) = j(E)$. Then there is a unique character $\chi_v : \mathrm{Gal}(\overline{F}_v/F_v) \to \{\pm 1\}$ such that E is isomorphic over F_v to the twist of $\mathcal{E}_v$ by χ_v, and χ_v is unramified. We claim that χ_v factors through $\mathrm{Gal}(F_v^\infty/F_v)$ and can therefore be viewed as a character of the latter group. To verify the claim, recall from the theory of the Tate curve that there is a basis for $T_p(E)$ over $\mathbb{Z}_p$ relative to which the natural map $\mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{Aut}(T_p(E))$ is upper-triangular with χ_v in the lower right-hand corner. Since the natural map factors through $\mathrm{Gal}(F_v^\infty/F_v)$ it follows that χ_v does too.

Now let τ be an irreducible self-dual representation of $\mathrm{Gal}(F^\infty/F)$, and for each place v of F let τ_v be the restriction of τ to the decomposition subgroup $\mathrm{Gal}(F_v^\infty/F_v)$ at v. We begin the calculation of $W(E,\tau)$ by expressing the root number as a product of local factors:

$$W(E,\tau) = \prod_v W(E/F_v, \tau_v). \tag{4.2}$$

Let us write $v|\infty$ or $v \nmid \infty$ according as v is or is not an infinite place. The local factor $W(E/F_v, \tau_v)$ is determined as follows:

- If $v|\infty$ then
$$W(E/F_v, \tau_v) = (-1)^{\dim \tau}$$
(cf. [13], p. 329, Theorem 2, part (i)).
- If $v \nmid \infty$ and $v(j(E)) \geqslant 0$ then
$$W(E/F_v, \tau_v) = \det \tau_v(-1)$$
(cf. [13], p. 332, Proposition 8, part (i)). Here the one-dimensional character $\det \tau_v$ of $\mathrm{Gal}(F_v^\infty/F_v)$ is viewed as a character of $F_v^\times$ using (4.1).
- If $v \nmid \infty$ and $v(j(E)) < 0$ then
$$W(E/F_v, \tau_v) = \det \tau_v(-1)(-1)^{\langle \chi_v, \tau_v \rangle}$$
(cf. [13], p. 329, Theorem 2, part (ii), noting that $\chi_v(-1) = 1$ because χ_v is unramified). The inner product $\langle \chi_v, \tau_v \rangle$ can be interpreted either by viewing χ_v as a character of $\mathrm{Gal}(F_v^\infty/F_v)$ or by inflating τ_v to $\mathrm{Gal}(\overline{F}_v/F_v)$.

Inserting these formulas in (4.2) we obtain

$$W(E,\tau) = (-1)^{(r_1+r_2)\dim \tau} \cdot \prod_{v \nmid \infty} \det \tau_v(-1) \cdot \prod_{\substack{v \nmid \infty \\ v(j(E))<0}} (-1)^{\langle \chi_v, \tau_v \rangle}. \tag{4.3}$$

In the second factor we may replace the condition $v \nmid \infty$ by $v|\infty$, because the product of the characters $\det \tau_v$ over all places v of F is an idele class character, hence trivial on the principal idele -1.

The second factor can be simplified further as follows. If $v|\infty$ then $F_v^\infty \cong \mathbb{C}$, because F^∞ contains the p-power roots of unity. If in addition $F_v \cong \mathbb{C}$ then the Artin symbol $(*, F_v^\infty/F_v)$ is trivial, whence the identification (4.1) gives $\det \tau_v(-1) = 1$. On

the other hand, if $F_v = \mathbb{R}$ then we can speak of complex conjugation at v, which is an element $c_v \in \mathrm{Gal}(F_v^\infty/F_v) \subset \mathrm{GL}(2,\mathbb{Z}_p)$. Since c_v coincides with the Artin symbol $(x, F_v^\infty/F_v)$ for any $x < 0$, this time (4.1) gives $\det \tau_v(-1) = \det \tau(c_v)$. Making the appropriate substitutions in (4.3), or rather in (4.3) as modified at the end of the preceding paragraph, we obtain

$$W(E,\tau) = (-1)^{(r_1+r_2)\dim \tau} \cdot \prod_{v \text{ real}} \det \tau(c_v) \cdot \prod_{\substack{v \nmid \infty \\ v(j(E))<0}} (-1)^{\langle \chi_v, \tau_v \rangle}. \tag{4.4}$$

Now since c_v is a complex conjugation, it satisfies $c_v^2 = 1$ and $c_v(\zeta) = \zeta^{-1}$ for arbitrary p-power roots of unity ζ, and by virtue of the formal properties of the Weil pairing the equations $c_v(\zeta) = \zeta^{-1}$ imply that $\det c_v = -1$. On the other hand, as noted in the proof of Proposition 4, the group $\mathrm{GL}(2,\mathbb{Z}_p)$ has a unique conjugacy class of elements g satisfying $g^2 = 1$ and $\det g = -1$. If c is any fixed member of this conjugacy class then we obtain

$$W(E,\tau) = (-1)^{(r_1+r_2)\dim \tau} \cdot \det \tau(c)^{r_1} \cdot \prod_{\substack{v \nmid \infty \\ v(j(E))<0}} (-1)^{\langle \chi_v, \tau_v \rangle} \tag{4.5}$$

after replacing c_v by c in (4.4).

It remains to elaborate the third factor in (4.5). Let v be a finite place such that $v(j(E)) < 0$. Our point of departure is the action of $\mathrm{Gal}(\overline{F}_v/F_v)$ on $T_p(E)$ and on $T_p(\mathcal{E}_v)$, which can be described by maps $\alpha_v : \mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{GL}(2,\mathbb{Z}_p)$ and $\beta_v : \mathrm{Gal}(\overline{F}_v/F_v) \to \mathrm{GL}(2,\mathbb{Z}_p)$ respectively. In principle these maps depend on a choice of basis for the respective Tate modules, but in the case of $T_p(E)$ we have already specified α_v by the identifications we have made, namely the inclusion of $\mathrm{Gal}(F_v^\infty/F_v)$ in $\mathrm{Gal}(F^\infty/F)$ and the conflation of $\mathrm{Gal}(F^\infty/F)$ with $\mathrm{GL}(2,\mathbb{Z}_p)$. In other words, α_v is just the composite embedding $\mathrm{Gal}(F_v^\infty/F_v) \subset \mathrm{GL}(2,\mathbb{Z}_p)$ inflated to $\mathrm{Gal}(\overline{F}_v/F_v)$. On the other hand, in the case of $T_p(\mathcal{E}_v)$ the theory of the Tate curve assures us that β_v can be chosen to have the form

$$\beta_v(h) = \begin{pmatrix} \kappa_v(h) & z_v(h) \\ 0 & 1 \end{pmatrix} \qquad (h \in \mathrm{Gal}(\overline{F}_v/F_v)), \tag{4.6}$$

where $\kappa_v : \mathrm{Gal}(\overline{F}_v/F_v) \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character. Our goal now is to compute the parity of $\langle \chi_v, \tau_v \rangle$, and the first step is to describe the image of β_v.

By assumption, $v \nmid p$. Hence the p-adic cyclotomic character of $\mathrm{Gal}(\overline{F}_v/F_v)$ is unramified, and therefore its image is topologically generated by its value on a Frobenius element. In other words, if we write $m_v \in \mathbb{Z}_p^\times$ for the order of the residue class field of F_v then the image of κ_v is the open subgroup $U_v \subset \mathbb{Z}_p^\times$ topologically generated by m_v. On the other hand, our assumption that $p \nmid v(j(E))$ implies that the map $h \mapsto (\kappa_v(h), z_v(h))$ is a surjection $\mathrm{Gal}(\overline{F}_v/F_v) \to U_v \ltimes \mathbb{Z}_p$, whence the image of β_v is the group J of Proposition 5 with $m = m_v$. When m is so chosen we denote J by J_v. Thus the image of β_v is J_v.

The remainder of the calculation requires a division into cases. Let o_v denote the order of the image of U_v in $(\mathbb{Z}/p\mathbb{Z})^\times$, or what amounts to the same thing, the order

of the residue class of m_v modulo p. We partition the set of places of F where E has bad reduction into three subsets S, S', and S'' as follows: A place v belongs to S or to $S' \cup S''$ according as E has split or nonsplit multiplicative reduction at v, and if $v \in S' \cup S''$ then $v \in S'$ or $v \in S''$ according as o_v is even or odd.

Suppose first that $v \in S$. Then $\chi_v = 1$ and $E \cong \mathcal{E}_v$ over F_v. Hence α_v is conjugate to β_v, and since the image of β_v is J_v we obtain

$$\mathrm{Gal}(F_v^\infty/F_v) = g_v J_v g_v^{-1} \tag{4.7}$$

for some $g_v \in \mathrm{GL}(2, \mathbb{Z}_p)$.

To bypass the conjugation in (4.7) we insert an elementary remark. Given a profinite group G, an open subgroup H, an element $g \in G$, and a representation π of gHg^{-1}, let us write π_g for the representation of H defined by $\pi_g(h) = \pi(ghg^{-1})$. Then $\langle \rho, \pi \rangle = \langle \rho_g, \pi_g \rangle$ for arbitrary representations ρ of gHg^{-1}. In particular, suppose that π has the form $\pi = \tau | gHg^{-1}$ for some representation τ of G. Then

$$\langle \rho, \tau | gHg^{-1} \rangle = \langle \rho_g, \tau | H \rangle \tag{4.8}$$

because $\tau | H \cong (\tau | gHg^{-1})_g$: indeed $\tau(g)$ is an intertwining operator.

Now take $G = \mathrm{GL}(2, \mathbb{Z}_p)$, $g = g_v$, and $H = J_v(n)$, where n is chosen so that τ factors through $G/K(n)$. Referring to (4.7) and (4.8) we find that

$$\langle 1, \tau_v \rangle = \langle 1, \tau | gHg^{-1} \rangle = \langle 1, \mathrm{res}^G_{J_v(n)} \tau \rangle.$$

But $1 = \chi_v$ for $v \in S$, so we obtain

$$\langle \chi_v, \tau_v \rangle = \langle \mathrm{ind}^G_{J_v(n)} 1, \tau \rangle \qquad (v \in S) \tag{4.9}$$

by Frobenius reciprocity.

Next suppose that $v \in S'$. In this case χ_v is the unramified quadratic character of $\mathrm{Gal}(\overline{F}_v/F_v)$ and α_v is conjugate to the map β' defined by

$$\beta'(h) = \chi_v(h)\beta_v(h) \qquad (h \in \mathrm{Gal}(\overline{F}_v/F_v)).$$

Furthermore, since κ_v is unramified and o_v is even, $\chi_v(h)$ can be expressed as a function of the quantity $u = \kappa_v(h)$. In fact $\chi_v(h) = \omega(u)^{o_v/2}$, where in this equation ω denotes the Teichmüller character. It follows that the image of β' is the group J' of Proposition 6 with $m = m_v$. Writing this group as J'_v, we conclude that

$$\mathrm{Gal}(F_v^\infty/F_v) = g_v J'_v g_v^{-1} \tag{4.10}$$

for some $g_v \in \mathrm{GL}(2, \mathbb{Z}_p)$.

Now put $G = \mathrm{GL}(2, \mathbb{Z}_p)$ as before and choose n so that τ factors through $G/K(n)$. The character η' of Proposition 6 is the unique quadratic character of $J'(n)$, and when $m = m_v$ we denote it η'_v. The uniqueness has the following consequence: If we apply (4.8) with $H = J'_v(n)$, $g = g_v$, and $\rho = \chi_v$ (which we view as a character of

gHg^{-1} by appealing to (4.10) and declaring that $\chi_v|K(n)=1$ then $\rho_g=\eta'_v$. Hence $\langle\chi_v,\tau_v\rangle=\langle\eta'_v,\mathrm{res}^G_{J'_v(n)}\tau\rangle$, and therefore

$$\langle\chi_v,\tau_v\rangle=\langle\mathrm{ind}^G_{J'_v(n)}\eta'_v,\tau\rangle \qquad (v\in S') \tag{4.11}$$

by Frobenius reciprocity.

Finally, suppose that $v\in S''$. Then χ_v is once again the unramified quadratic character of $\mathrm{Gal}(\overline{F}_v/F_v)$ and α_v is again conjugate to the map $\chi_v\beta_v$, which however we denote β'' rather than β'. The key point is that this time $-1\notin U_v$, because o_v is odd. It follows that the fixed fields of the kernels of χ_v and κ_v are linearly disjoint over F_v, whence the image of β'' is the group J'' of Proposition 7 with $m=m_v$. When m is so chosen we denote J'' by J''_v. Thus

$$\mathrm{Gal}(F_v^\infty/F_v)=g_vJ''_vg_v^{-1}$$

for some $g_v\in\mathrm{GL}(2,\mathbb{Z}_p)$. Arguing as before, we conclude that

$$\langle\chi_v,\tau_v\rangle=\langle\mathrm{ind}^G_{J''_v(n)}\eta''_v,\tau\rangle \qquad (v\in S''), \tag{4.12}$$

where η''_v is the quadratic character η'' of Proposition 7 with $m=m_v$.

Now put

$$\Sigma=\sum_{v\in S}\langle\mathrm{ind}^G_{J_v(n)}1,\tau\rangle,$$

$$\Sigma'=\sum_{v\in S'}\langle\mathrm{ind}^G_{J'_v(n)}\eta'_v,\tau\rangle,$$

and

$$\Sigma''=\sum_{v\in S''}\langle\mathrm{ind}^G_{J''_v(n)}\eta''_v,\tau\rangle.$$

Substitution of (4.9), (4.11), and (4.12) in (4.5) gives the following result.

Theorem 2. $W(E,\tau)=(-1)^{(r_1+r_2)\dim\tau}\cdot\det\tau(c)^{r_1}\cdot(-1)^{\Sigma+\Sigma'+\Sigma''}$.

Theorem 1 follows from Theorem 2 on substituting the value of $\dim\tau$ from Proposition 3, the value of $\det\tau(c)$ from Proposition 4, and the value of Σ, Σ', and Σ'' from Propositions 5, 6, and 7 respectively. In applying Proposition 6 we note that if $[\mathbb{Z}_p^\times:U_v]$ is odd then the requirement that o_v be even is automatically satisfied. Hence the omission of this requirement from the definition of the integer t in the introduction is harmless.

References

[1] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, *The GL_2 main conjecture for elliptic curves without complex multiplication* (to appear).

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

[3] C. W. Curtis and I. Reiner, *Methods of representation theory*, 2 vols., John Wiley & Sons, New York, 1981.

[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.
[5] P. Deligne, *Valeurs de fonctions L et périodes d'intégrales*, Automorphic Forms, Representations, and L-Functions, Proc. Symp. Pure Math. Vol. 33 – Part 2, Amer. Math. Soc., Providence, 1979, pp. 313–346.
[6] W. Fulton and J. Harris, *Representation Theory: A First Course*, GTM vol 129 (Readings in Mathematics), Springer-Verlag, New York, 1991.
[7] R. Greenberg, *Non-vanishing of certain values of L-functions*, Analytic Number Theory and Diophantine Problems, Prog. in Math. 70, Birkhauser, Boston, 1987, pp. 223–235.
[8] L. Howe, *Twisted Hasse-Weil L-functions and the rank of Mordell-Weil groups*, Can. J. Math. **49** (1997), 749–771.
[9] S. Lang, *Algebra*, GTM vol. 211, Springer-Verlag, New York, 2002.
[10] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
[11] D. E. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*, Automorphic Forms and Analytic Number Theory, Les publications CRM, Montreal, 1990, pp. 123–133.
[12] D. E. Rohrlich, *Elliptic curves and the Weil-Deligne group*, Elliptic Curves and Related Topics, CRM Proceedings & Lecture Notes Vol. 4, Amer. Math. Soc., Providence, 1994, pp. 125–157.
[13] D. E. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Compos. Math. **100** (1996), 311–349.
[14] K. Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **64** (1981), 455-470.
[15] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.
[16] A. J. Silberger, *PGL_2 over the p-adics: its Representations, Spherical Functions, and Fourier Analysis*, Lect. Notes in Math. 166, Springer-Verlag, 1970.
[17] J. Tate, *Number theoretic background*, Automorphic Forms, Representations, and L-Functions, Proc. Symp. Pure Math. Vol. 33 – Part 2, Amer. Math. Society, Providence, 1979, pp. 3–26.
[18] V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), 219–261.

Department of Mathematics and Statistics, Boston University, Boston, MA 02215
E-mail address: rohrlich@math.bu.edu