Algebra & Number Theory

Volume 4

2010

No. 3

Twisted root numbers of elliptic curves semistable at primes above 2 and 3

Ryota Matsuura

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 4:3(2010)

Twisted root numbers of elliptic curves semistable at primes above 2 and 3

Ryota Matsuura

Let E be an elliptic curve over a number field F, and fix a rational prime p. Put $F^{\infty} = F(E[p^{\infty}])$, where $E[p^{\infty}]$ is the group of p-power torsion points of E. Let τ be an irreducible self-dual complex representation of $\mathrm{Gal}(F^{\infty}/F)$. With certain assumptions on E and p, we give explicit formulas for the root number $W(E, \tau)$. We use these root numbers to study the growth of the rank of E in its own division tower and also to count the trivial zeros of the L-function of E. Moreover, our assumptions ensure that the p-division tower of E is nonabelian.

In the process of computing the root number, we also study the irreducible self-dual complex representations of $\mathrm{GL}(2, \mathcal{O})$, where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$, for p an odd prime. Among all such representations, those that factor through $\mathrm{PGL}(2, \mathcal{O})$ have been analyzed in detail in existing literature. We give a complete description of those irreducible self-dual complex representations of $\mathrm{GL}(2, \mathcal{O})$ that do not factor through $\mathrm{PGL}(2, \mathcal{O})$.

1. Introduction

We study the growth of the Mordell–Weil rank of an elliptic curve in its own division tower. Our approach will be based on root number calculation. Let E an elliptic curve over a number field F, and p a rational prime. Put $F^{\infty} = F(E[p^{\infty}])$, where $E[p^{\infty}]$ is the group of p-power torsion points of E. Given an irreducible self-dual complex representation τ of $\mathrm{Gal}(F^{\infty}/F)$, we define the associated root number $W(E, \tau)$ [Rohrlich 1996, pp. 329 and 336] and the L-function $L(s, E, \tau)$ [Rohrlich 1994, pp. 151 and 156]. Since τ is self-dual, the conjectural functional equation of $L(s, E, \tau)$ relates this function to itself and therefore we obtain

$$W(E, \tau) = (-1)^{\mathrm{ord}_{s=1} L(s,E,\tau)}.$$

The conjectures of Birch–Swinnerton-Dyer and Deligne–Gross [Rohrlich 1990, p. 127], moreover, imply that $\mathrm{ord}_{s=1} L(s, E, \tau)$ is equal to the multiplicity of τ in $\mathbb{C} \otimes_{\mathbb{Z}} E(F^{\infty})$. Thus if we assume the standard conjectures, then $W(E, \tau) = -1$

MSC2000: primary 11G05; secondary 11F80, 11G40.

Keywords: elliptic curves, root number, Mordell–Weil rank.

The author gratefully acknowledges the support of NSF grant EHR 0314692.

lets us conclude that τ occurs in $\mathbb{C} \otimes_{\mathbb{Z}} E(F^\infty)$. Using this observation, we prove, for example, that if E is an elliptic curve over $\mathbb{Q}$ which is semistable at primes 2 and 3, and if p is a sufficiently large prime with $p \equiv 3 \pmod 4$, then the rank of E is unbounded in its p-division tower, provided that the standard conjectures hold.

The goal of this paper is to give explicit formulas for $W(E, \tau)$ under some simplifying assumptions on E and p. These assumptions are the same as in [Rohrlich 2006], except we relax the semistability condition by requiring E to be semistable over F only at primes of F above 2 and 3. In most cases, our formulas are identical to or differ only slightly from those of Rohrlich. However, despite the similarity in the final results, the calculations behind them are quite different, because if an elliptic curve is not semistable at a prime then the twisted local root number depends crucially on the way in which τ decomposes into irreducibles when restricted to the local Galois group. The "semistable part" of our calculation will simply be quoted from Rohrlich's paper, and most of our effort will go into the group theory needed to handle the nonsemistable case. Moreover, we remark that our assumptions ensure that the p-division tower of E is nonabelian.

As another application, we use our root number formulas to count the trivial zeros of the L-function of E over $F(E[p^n])$, where $E[p^n]$ denotes the group of p^n-torsion points of E. By *trivial zeros*, we mean the zeros at $s = 1$ which arise from the functional equation of the L-function. As remarked in [Rohrlich 2008], these trivial zeros are "virtual" in the sense that the functional equations in question are still mostly conjectural.

In the process of computing the root number, we also study the irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$, where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$, for p an odd prime. (In this paper, as was the case in [Rohrlich 2006], a *representation* of a topological group is always meant to be continuous, finite-dimensional, and defined over the complex numbers.) Among all such representations, those that factor through $\mathrm{PGL}(2, \mathcal{O})$ have been analyzed in detail by Silberger [1970]. In the present paper, we will give a complete description of those irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$ that do not factor through $\mathrm{PGL}(2, \mathcal{O})$.

2. Statement of the main theorem

As in the introduction, let F be a number field, E an elliptic curve over F, p a rational prime, and $F^\infty = F(E[p^\infty])$. Let τ be an irreducible self-dual representation of $\mathrm{Gal}(F^\infty/F)$. We will compute the root number $W(E, \tau)$ under the following assumptions:

- E is semistable over F at the primes of F above 2 and 3.
- p is odd.

- The natural embedding of $\mathrm{Gal}(F^\infty/F)$ into $\mathrm{Aut}(T_p(E))$ is an isomorphism.
- If v is a finite place of F, where E has bad reduction, then $v \nmid p$. Furthermore, if $v(j(E)) < 0$, then $p \nmid v(j(E))$.

The third condition allows us to identify $\mathrm{Gal}(F^\infty/F)$ with $\mathrm{GL}(2, \mathbb{Z}_p)$. Since the choice of basis for $T_p(E)$ over $\mathbb{Z}_p$ implicit in such an identification does not affect the resulting correspondence between isomorphism classes of representations, we may view τ as an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$.

2A. ***List of representations.*** In this section (and in Section 3), we consider representations of a slightly more general group. Let p be an odd prime and F_v a finite extension of $\mathbb{Q}_p$. Let $\mathcal{O}$ and $\mathfrak{p}$ denote the ring of integers and the maximal ideal of F_v, respectively. Let q be the order of the residue class field $\mathcal{O}/\mathfrak{p}$, and put $\mathcal{O}^n = \mathcal{O}/\mathfrak{p}^n$ for $n \geq 1$.

Given an irreducible representation τ of $\mathrm{GL}(2, \mathcal{O})$, we define its *central character*

$$\omega_\tau : \mathcal{O}^\times \to \mathbb{C}^\times$$

as follows. Take $a \in \mathcal{O}^\times$ and let I be the 2×2 identity matrix. Schur's Lemma implies that $\tau(a \cdot I)$ is multiplication by $\omega_\tau(a)$. We remark that ω_τ is trivial if and only if τ factors through $\mathrm{PGL}(2, \mathcal{O})$.

We say that τ is *reducible* modulo $\mathfrak{p}^n$ if it factors through $\mathrm{GL}(2, \mathcal{O}^n)$. And we say τ is *primitive* modulo $\mathfrak{p}^n$ if n is the smallest such integer. For $n \geq 1$, let $\mathfrak{T}_n$ be the set of isomorphism classes of irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$ with nontrivial central character that are primitive modulo $\mathfrak{p}^n$. The set $\mathfrak{T}'_n$ is defined in the same way except that the central character is assumed to be trivial. By convention, the characters 1 and λ of $\mathrm{PGL}(2, \mathcal{O})$ defined in the next paragraph are primitive modulo $\mathfrak{p}^0$. Thus we put $\mathfrak{T}'_0 = \{1, \lambda\}$.

2A.1. *Representations of* $\mathrm{PGL}(2, \mathcal{O})$. We begin by giving a complete list, up to isomorphism, of the irreducible representations of $\mathrm{GL}(2, \mathcal{O})$ that factor through $\mathrm{PGL}(2, \mathcal{O})$ [Silberger 1970, pp. 96–100]. Such representations are necessarily self-dual. We let 1 denote the trivial character of $\mathrm{GL}(2, \mathcal{O})$, or of any group. Also, we let λ denote the Legendre symbol on $\mathcal{O}^\times$ or $\mathrm{GL}(2, \mathcal{O})$, that is, the unique quadratic character of these groups. Note that the Legendre symbol on $\mathrm{GL}(2, \mathcal{O})$ is the Legendre symbol on $\mathcal{O}^\times$ composed with the determinant $\mathrm{GL}(2, \mathcal{O}) \to \mathcal{O}^\times$.

Put $G = \mathrm{GL}(2, \mathcal{O})$ and let B be the upper triangular subgroup of G. For an integer $n \geq 1$, let $K(n)$ denote the kernel of reduction modulo $\mathfrak{p}^n$ on G. Given a subgroup H of G, we set $H(n) = HK(n)$; we also set $H(0) = G$. Then we can define a representation σ_n up to isomorphism by writing

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

Here, note that $\operatorname{ind}_{B(n-1)}^{G} 1$ is a subrepresentation of $\operatorname{ind}_{B(n)}^{G} 1$ because $B(n)$ is a subgroup of $B(n-1)$. We remark that $\sigma_1 = \sigma$, the q-dimensional *Steinberg representation* of $\mathrm{GL}(2, \mathcal{O})$, and σ_n has dimension $q^n - q^{n-2}$ for $n \geq 2$. And using σ and λ, we obtain another q-dimensional representation, namely $\sigma \otimes \lambda$.

We introduce a general notation for characters of B. Given characters μ and ν of $\mathcal{O}^\times$, we define a character $\xi_{\mu,\nu}$ of B by

$$\xi_{\mu,\nu}(b) = \mu(b_{11})\nu(b_{22}) \qquad (b \in B), \tag{1}$$

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

Let α be a character of $\mathcal{O}^\times$ of conductor $\mathfrak{p}^n$ and order $|\alpha| > 2$. By a *primitive principal series representation with trivial central character*, we mean a representation of the form $u_\alpha = \operatorname{ind}_{B(n)}^{G} \xi_{\alpha,\alpha^{-1}}$. Such a representation has dimension $q^n + q^{n-1}$. For $m > n$, we define a representation $u_{\alpha,m}$ up to isomorphism by writing

$$\operatorname{ind}_{B(m)}^{G} \xi_{\alpha,\alpha^{-1}} = u_{\alpha,m} \oplus \operatorname{ind}_{B(m-1)}^{G} \xi_{\alpha,\alpha^{-1}}.$$

Then $u_{\alpha,m}$ has dimension $q^m - q^{m-2}$. Also, since $u_{\alpha,m} \cong \sigma_m$ when $m \geq 2n$ [Silberger 1970, p. 59], we will assume that $n < m < 2n$. Thus, in particular, $m \geq 3$.

Let K be the unramified quadratic extension of F_v, and $\mathcal{O}_K$ and $\mathfrak{p}_K$ its ring of integers and the maximal ideal, respectively. Let π be a character of $\mathcal{O}_K^\times$ of order $|\pi| > 2$ such that $\pi\,|\mathcal{O}^\times = 1$. Furthermore, suppose π has conductor $\mathfrak{p}_K^n$. Then u_π^{unr} and $u_{\pi,i}^{\mathrm{unr}}$ $(n < i < 2n)$ will refer to the unramified discrete series representations of $\mathrm{PGL}(2, \mathcal{O})$ as described by Silberger [1970, p. 80]. We remark that $\dim u_\pi^{\mathrm{unr}} = q^n - q^{n-1}$ and $\dim u_{\pi,i}^{\mathrm{unr}} = q^i - q^{i-2}$.

Now let K be a ramified quadratic extension of F_v and π a character of $\mathcal{O}_K^\times$ such that $\pi\,|\mathcal{O}^\times = \lambda$. Also suppose π has conductor $\mathfrak{p}_K^{2n-1}$ for some $n \geq 2$ so that $|\pi| > 2$. Then u_π^{ram} and $u_{\pi,i}^{\mathrm{ram}}$ $(n < i < 2n-1)$ will refer to the ramified discrete series representations of $\mathrm{PGL}(2, \mathcal{O})$ as described by Silberger [1970, p. 80]. Note that $\dim u_\pi^{\mathrm{ram}} = q^n - q^{n-2}$ and $\dim u_{\pi,i}^{\mathrm{ram}} = q^i - q^{i-2}$.

2A.2. *Representations of* $\mathrm{GL}(2, \mathcal{O})$ *with* $\omega_\tau \neq 1$. We now consider the irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$ that do not factor through $\mathrm{PGL}(2, \mathcal{O})$. We remark that if τ is such a representation, then ω_τ is a quadratic character on $\mathcal{O}^\times$. Therefore $\omega_\tau = \lambda$, and τ factors through $\mathrm{GL}(2, \mathcal{O})/(\mathcal{O}^\times)^2$, where we identify $(\mathcal{O}^\times)^2$ with the subgroup

$$\{a^2 \cdot I : a \in \mathcal{O}^\times\} \subset \mathrm{GL}(2, \mathcal{O}).$$

In Section 3, we will define a map $\varphi_n : [\tau'] \mapsto [\tau]$, where $[\tau'] \in \mathfrak{T}'_n$ and $[\tau] \in \mathfrak{T}_n$. Then we will use our knowledge of $\mathfrak{T}'_n$ to characterize the elements of $\mathfrak{T}_n$.

Before proceeding, we mention one family of irreducible self-dual representations of $\mathrm{GL}(2,\mathcal{O})$ with $\omega_\tau \neq 1$ that play a special role in our calculations. With the notations as in (1), let $\mu = 1$ and $\nu = \lambda$, and put

$$\theta_1 = \operatorname{ind}_{B(1)}^{G} \xi_{1,\lambda}.$$

For $n \geq 2$, define a representation θ_n up to isomorphism by writing

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

We remark that $\dim\theta_1 = q+1$ and $\dim\theta_n = q^n - q^{n-2}$ for $n \geq 2$.

2B. ***The main theorem.*** For each finite place v of F, let m_v denote the order of the residue class field of v. If E has bad reduction at v, we have $p \nmid m_v$, so we can classify m_v as either a quadratic residue or a quadratic nonresidue modulo p. Let s denote the number of places v where E has split multiplicative reduction, and 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. Moreover, let u be the number of places v where E has nonsplit multiplicative reduction and m_v is a quadratic nonresidue modulo p. And as usual, let r_1 and $2r_2$ denote the number of real and complex embeddings of F.

Let T^- denote the set of finite places v of F where E has additive reduction and $v(j(E)) < 0$. Define the set T^+ in the same way except with $v(j(E)) \geq 0$. Let t_3^- and t_{nr}^- denote the number of places $v \in T^-$ such that $m_v \equiv 3 \pmod 4$ and m_v is a quadratic nonresidue modulo p, respectively.

Now let $v \in T^+$, that is, E has bad but potentially good reduction at v. Let Δ_v denote the discriminant associated to a minimal Weierstrass equation for E at v, and put

$$e_v = \frac{12}{\gcd(v(\Delta_v), 12)} \ (= 2, 3, 4, \text{ or } 6). \tag{2}$$

Define the following subsets of T^+:

$$\begin{aligned}
T_2^+ &= \{v \in T^+ : e_v = 2 \text{ or } 6, \text{ and } m_v \equiv -1 \pmod 4\},\\
T_3^+ &= \{v \in T^+ : e_v = 3 \text{ and } m_v \equiv -1 \pmod 3\},\\
T_4^+ &= \{v \in T^+ : e_v = 4, \text{ and } m_v \equiv 5 \text{ or } 7 \pmod 8\},\\
T_6^+ &= \{v \in T^+ : e_v = 6 \text{ and } m_v \equiv -1 \pmod 6\}.
\end{aligned}$$

Let $t_{2,4}^+$, t_3^+, and t_6^+ denote the cardinalities of $T_2^+ \cup T_4^+$, T_3^+, and T_6^+, respectively.

Theorem 2.1. *Let τ be an irreducible self-dual representation of* $\mathrm{Gal}(F^\infty/F)$ *and let w be the integer modulo 2 such that $W(E,\tau) = (-1)^w$.*

- *If $\tau = 1$, then $w = r_1 + r_2 + s + t_3^- + t_{2,4}^+ + t_3^+ \pmod 2$.*
- *If $\tau = \lambda$, then $w = r_1(p+1)/2 + r_2 + s_{\mathrm{qr}} + u + t_3^- + t_{2,4}^+ + t_3^+ \pmod 2$.*

- *If* $\tau \cong \sigma$, *then*

$$w = \begin{cases} r_1(p+1)/2 + r_2 + s + t_3^- + t_{2,4}^+ + t_3^+ \pmod 2 & \textit{if } p > 3, \\ r_2 + s + t_3^- + t_{2,4}^+ \pmod 2 & \textit{if } p = 3. \end{cases}$$

- *If* $\tau \cong \sigma \otimes \lambda$, *then*

$$w = \begin{cases} r_1 + r_2 + s_{\mathrm{qr}} + u + t_3^- + t_{2,4}^+ + t_3^+ \pmod 2 & \textit{if } p > 3, \\ r_1 + r_2 + s_{\mathrm{qr}} + u + t_3^- + t_{2,4}^+ \pmod 2 & \textit{if } p = 3. \end{cases}$$

- *If* $\tau \cong \sigma_n$ *with* $n \geq 2$, *then*

$$w = \begin{cases} s_{\mathrm{nr}} + u + t_3^+ \pmod 2 & \textit{if } p = 3 \textit{ and } n = 2, \\ s_{\mathrm{nr}} + u \pmod 2 & \textit{otherwise.} \end{cases}$$

- *If* $\tau \cong u_\alpha$, *where* α *is primitive modulo* p^n $(n \geq 1)$, *then*

$$w = \begin{cases} r_1(p-1)/2 + t_3^+ \pmod 2 & \textit{if } p \equiv 1 \pmod 3 \textit{ and } 3|\alpha| \nmid p^{n-1}(p-1), \\ r_1(p-1)/2 \pmod 2 & \textit{otherwise.} \end{cases}$$

- *If* $\tau \cong u_\pi^{\mathrm{unr}}$, *where* π *is primitive modulo* $\mathfrak{p}_K^n$ $(n \geq 1)$, *then*

$$w = \begin{cases} r_1(p-1)/2 + t_3^+ \pmod 2 & \textit{if } p \equiv -1 \pmod 3 \textit{ and } \pi(1+\sqrt{-3}) \neq 1, \\ r_1(p-1)/2 + t_3^+ \pmod 2 & \textit{if } p = 3 \textit{ and } n = 1, \\ r_1(p-1)/2 \pmod 2 & \textit{otherwise.} \end{cases}$$

- *If* $\tau \cong u_\pi^{\mathrm{ram}}$, *where* π *is primitive modulo* $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, *then*

$$w = \begin{cases} t_3^+ \pmod 2 & \textit{if } p = 3 \textit{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \textit{otherwise.} \end{cases}$$

- *If* $[\tau] = \varphi_n([u_\pi^{\mathrm{ram}}])$, *where* π *is primitive modulo* $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, *then*

$$w = \begin{cases} t_3^+ + t_6^+ \pmod 2 & \textit{if } p = 3 \textit{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \textit{otherwise.} \end{cases}$$

- *If* $\tau \cong \theta_n$ *with* $n \geq 1$, *then*

$$w = \begin{cases} s_{\mathrm{nr}} + u + t_{\mathrm{nr}}^- + t_3^+ + t_6^+ \pmod 2 & \textit{if } p = 3 \textit{ and } 1 \leq n \leq 2, \\ s_{\mathrm{nr}} + u + t_{\mathrm{nr}}^-(p-1)/2 \pmod 2 & \textit{otherwise.} \end{cases}$$

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

Remark. The criterion

$$\pi(1+\sqrt{-3}) \neq 1 \quad \text{when } \tau \cong u_\pi^{\mathrm{unr}}$$

does not depend on the choice of $\sqrt{-3}$, because $\pi(1+\sqrt{-3})\pi(1-\sqrt{-3}) = \pi(4) = 1$ (since $\pi|\mathbb{Z}_p^\times = 1$).

The following proposition serves as an illustrative example. Here we assume the standard conjectures discussed in the introduction.

Proposition 2.2. *Let E be an elliptic curve over $\mathbb{Q}$ which is semistable at* 2 *and* 3*. Choose $p \equiv 3 \pmod 4$ sufficiently large so that our assumptions on E and p are satisfied. Then, assuming the standard conjectures, the rank of E is unbounded in its p-division tower.*

Proof. Consider an integer $n \geq 2$ and choose a character α of $\mathbb{Z}_p^\times$ of conductor p^n. Moreover if $p \equiv 1 \pmod 3$, choose α so that $3|\alpha| \mid p^{n-1}(p-1)$. Put $\tau = u_\alpha$. Since $r_1 = 1$ and $(p-1)/2 \equiv 1 \pmod 2$, Theorem 2.1 implies $W(E, \tau) = -1$. Viewed as a representation of $\mathrm{Gal}(\mathbb{Q}^\infty/\mathbb{Q})$, the map τ factors through $\mathrm{Gal}(\mathbb{Q}^{(n)}/\mathbb{Q})$, where $\mathbb{Q}^{(n)} = \mathbb{Q}(E[p^n])$. Then $W(E, \tau) = -1$, in conjunction with the standard conjectures, implies that the multiplicity of τ in $\mathbb{C} \otimes_{\mathbb{Z}} E(\mathbb{Q}^{(n)})$ is odd, and hence positive. Therefore, we have

$$\mathrm{rank}_{\mathbb{Z}}\, E(\mathbb{Q}^{(n)}) \geq \dim \tau = p^n + p^{n-1}$$

whence the result follows. □

2C. ***Trivial zeros of L-functions.*** For $n \geq 1$, put $F^{(n)} = F(E[p^n])$ so that we can identify $\mathrm{Gal}(F^{(n)}/F)$ with $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. As in [Rohrlich 2008], we let $\mathcal{T}_n$ denote the set of isomorphism classes of irreducible self-dual representations of $\mathrm{Gal}(F^\infty/F)$ which factor through $\mathrm{Gal}(F^{(n)}/F)$. In particular, $\mathcal{T}_n$ is the disjoint union of the sets $\mathfrak{T}'_i$ $(0 \leq i \leq n)$ and $\mathfrak{T}_j$ $(1 \leq j \leq n)$. To measure the "size" of $\mathcal{T}_n$, we define the quantity

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

Silberger [1970, pp. 96–100] lists the number of isomorphism classes of each type of irreducible representations of $\mathrm{PGL}(2, \mathbb{Z}_p)$. And we can find their dimensions using his character tables (pp. 102–107). Moreover we will show in Section 3 that $\#\mathfrak{T}_n = p^{n-1}$ and that for $[\tau] \in \mathfrak{T}_n$,

$$\dim \tau = \begin{cases} p+1 & \text{if } n = 1, \\ p^{n-2}(p^2-1) & \text{if } n \geq 2. \end{cases}$$

Combining all of this, we obtain:

Theorem 2.3. $\vartheta_n = p^{2n} + p^{2n-1} + 2$.

Now let $\mathcal{T}_n^\pm$ be the subsets of $\mathcal{T}_n$ containing those isomorphism classes $[\tau]$ for which $W(E, \tau) = \pm 1$. Then define the quantities

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

Let $\mathcal{T}_n^*$ denote the set of *all* isomorphism classes of irreducible representations of $\mathrm{Gal}(F^{(n)}/F)$ (i.e., not just the self-dual ones). Then we have

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

as a factorization of the L-function of E over $F^{(n)}$. If we assume the conjectural analytic continuation of the L-function, we obtain

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

We restrict the sum on the right-hand side to $\mathcal{T}_n^-$ and note that the standard conjectures imply $\mathrm{ord}_{s=1} L(s, E/F, \tau) \geq 1$ for $[\tau] \in \mathcal{T}_n^-$. Therefore we obtain

$$\mathrm{ord}_{s=1} L(s, E/F^{(n)}) \geq \vartheta_n^- \tag{3}$$

so that the quantity ϑ_n^- gives a lower bound for the number of trivial zeros of $L(s, E/F^{(n)})$ at $s = 1$.

Theorem 2.4. *Suppose* $p \equiv 3 \pmod 4$ *and* $[F : \mathbb{Q}]$ *is odd.*

- *If* $p > 3$, *then* $\vartheta_n^- \sim a(1 - 1/p) \cdot p^{2n}$, *where*

$$a = \begin{cases} 1 & \text{if } t_3^+ \equiv 0 \pmod 2, \\ 2/3 & \text{if } t_3^+ \equiv 1 \pmod 2. \end{cases}$$

- *If* $p = 3$, *then* $\vartheta_n^- \sim a \cdot 3^{2n}$, *where*

$$a = \begin{cases} 2/3 & \text{if } t_3^+ \equiv t_6^+ \equiv 0 \pmod 2, \\ 8/9 & \text{if } t_3^+ \equiv 1 \text{ and } t_6^+ \equiv 0 \pmod 2, \\ 7/9 & \text{otherwise.} \end{cases}$$

Suppose $p \equiv 1 \pmod 4$ *or* $[F : \mathbb{Q}]$ *is even.*

- *Let* $p > 3$. *Then* $\vartheta_n^- = O(p^n)$ (*in fact*, $\vartheta_n^- \leq 4 \cdot p^n$) *when* $t_3^+ \equiv 0 \pmod 2$, *and* $\vartheta_n^- \sim (1/3)(1 - 1/p) \cdot p^{2n}$ *when* $t_3^+ \equiv 1 \pmod 2$.
- *Let* $p = 3$. *If* $t_3^+ \equiv t_6^+ \equiv 0 \pmod 2$, *then* $\vartheta_n^- = O(3^n)$ (*in fact*, $\vartheta_n^- \leq 4 \cdot 3^n$). *Otherwise, we have* $\vartheta_n^- \sim a \cdot 3^{2n}$, *where*

$$a = \begin{cases} 2/9 & \text{if } t_6^+ \equiv 0 \pmod 2, \\ 1/9 & \text{if } t_6^+ \equiv 1 \pmod 2. \end{cases}$$

Remark. An expression such as $\vartheta_n^- \sim a(1 - 1/p) \cdot p^{2n}$ means

$$\lim_{n\to\infty} \frac{\vartheta_n^-}{p^{2n}} = a(1 - 1/p).$$

Proof. Suppose $p \equiv 3 \pmod 4$ and $[F : \mathbb{Q}]$ is odd, or equivalently, $r_1(p-1)/2 \equiv 1 \pmod 2$. Suppose further that $p > 3$ and $t_3^+ \equiv 0 \pmod 2$. From Theorem 2.1, we see that $W(E, \tau) = -1$ for representations τ of the form $\tau = u_\alpha$ and $\tau = u_\pi^{\mathrm{unr}}$. There are $(p-3)/2$ representations (up to isomorphism) of the type $\tau = u_\alpha$ that are primitive modulo p, each with dimension $p+1$ [Silberger 1970, p. 96]. And for $i \geq 2$, there are $p^{i-2}(p-1)^2/2$ representations from this family that are primitive modulo p^i, each with dimension $p^i + p^{i-1}$ [Silberger 1970, pp. 98 and 102]. Thus the contribution to ϑ_n^- from the family of representations u_α is given by

$$\frac{1}{2}\Big((p-3)(p+1) + \sum_{i=2}^{n} p^{i-2}(p-1)^2(p^i + p^{i-1})\Big) = \tfrac{1}{2}(p^{2n} - p^{2n-1} - p - 3). \qquad (*)$$

Similarly, the family u_π^{unr} contributes to ϑ_n^- by the quantity

$$\tfrac{1}{2}(p^{2n} - p^{2n-1} - p + 1). \qquad (**)$$

The representations $1, \lambda, \sigma, \sigma \otimes \lambda, \sigma_i$ $(i \geq 2)$, and θ_i $(i \geq 1)$ can also contribute to ϑ_n^-, but the sum of their contributions would be at most $O(p^n)$, making it negligible. Combining $(*)$ and $(**)$, we get $\vartheta_n^- \sim (1 - 1/p) \cdot p^{2n}$. All the other cases are handled analogously. □

We again assume the standard conjectures. The Birch–Swinnerton-Dyer conjecture states

$$\operatorname{rank}_{\mathbb{Z}} E(F^{(n)}) = \operatorname{ord}_{s=1} L(s, E/F^{(n)}). \qquad (4)$$

Combining (3) and (4) and applying Theorem 2.4, we see that $\operatorname{rank}_{\mathbb{Z}} E(F^{(n)})$ is at least order p^{2n}, provided $p \equiv 3 \pmod 4$ and $[F : \mathbb{Q}]$ is odd. This is stronger than the bound

$$\operatorname{rank}_{\mathbb{Z}} E(F^{(n)}) \geq p^n + p^{n-1} \qquad (5)$$

we found in the proof of Proposition 2.2. Note that this reflects the fact that (5) was obtained using only one irreducible self-dual representation τ of $\mathrm{Gal}(F^{(n)}/F)$ for which $W(E, \tau) = -1$, while ϑ_n^- was computed using *all* such representations up to isomorphism.

3. Characterizations of representations of GL(2, $\mathcal{O}$)

As in Section 2A, let p be an odd prime and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$, let q denote the order of the residue class field $\mathcal{O}/\mathfrak{p}$, and put $\mathcal{O}^n = \mathcal{O}/\mathfrak{p}^n$ for $n \geq 1$. Our goal in this section is to characterize all irreducible self-dual representations of GL(2, $\mathcal{O}$).

3A. ***Cardinalities.*** We begin by proving:

Theorem 3.1. $\#\mathfrak{T}_n = q^{n-1}$.

We introduce some definitions and notations. Let G be a group and c a conjugacy class of G. We put c^{-1} for the class consisting of elements x^{-1}, where $x \in c$. We say that c is *real* if $c = c^{-1}$. Suppose $c = [a]$, that is, the class c is represented by an element $a \in G$. Then one immediately sees that c is real if and only if a is conjugate to a^{-1}. We also remark that if G is finite, then the number of real-valued irreducible characters of G is equal to the number of real conjugacy classes of G [Serre 1977, p. 109, Exercise 13.9(a)].

For $n \geq 1$, put

$$K'_n = \mathrm{PGL}(2, \mathcal{O}^n) = \mathrm{GL}(2, \mathcal{O}^n)/(\mathcal{O}^n)^\times.$$

Let α_n denote the number of irreducible (self-dual) representations of K'_n up to isomorphism, or equivalently, the number of (real) conjugacy classes of K'_n. By [Silberger 1970, p. 101], we have

$$\alpha_n = 2 + q + q^2 + \cdots + q^n.$$

For $n \geq 1$, put

$$K_n = \mathrm{GL}(2, \mathcal{O}^n)/(\mathcal{O}^n)^{\times 2}.$$

Recall that for an irreducible self-dual representation τ of $\mathrm{GL}(2, \mathcal{O})$, $\omega_\tau = 1$ or λ (see Section 2A.2). Thus there is a natural one-to-one correspondence between the isomorphism classes of irreducible self-dual representations of $\mathrm{GL}(2, \mathcal{O})$ that are reducible modulo $\mathfrak{p}^n$ and of irreducible self-dual representations of K_n. Let β_n denote the number of irreducible self-dual representations of K_n up to isomorphism, or equivalently, the number of real conjugacy classes of K_n. To prove Theorem 3.1, we must compute β_n.

Let $K = \mathrm{GL}(2, \mathcal{O})/(\mathcal{O}^\times)^2$ and fix a nonsquare element of $\mathcal{O}^\times$, say ζ.

Lemma 3.2. *Let* $A \in \mathrm{GL}(2, \mathcal{O})$. *If* $\det A \in (\mathcal{O}^\times)^2$, *then* A *is conjugate to* A^{-1} *in* K, *that is*, $[A]$ *is real in* K. *And the converse holds if* $\operatorname{tr} A \neq 0$.

Proof. A calculation shows that if $A \in \mathrm{GL}(2, \mathcal{O})$ and $\det A \in (\mathcal{O}^\times)^2$, then $sAs^{-1} \equiv (A^{-1})^{\mathrm{t}}$, where $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\equiv$ denotes equivalence in K. Since every element of $\mathrm{GL}(2, \mathcal{O})$ is conjugate to its transpose (see [Rohrlich 2006, lemma on p. 364]—the proof is valid for arbitrary $\mathcal{O}$), A is conjugate to A^{-1} in K.

Now suppose $\operatorname{tr} A \neq 0$ and that A is conjugate to A^{-1} in K. Thus, A is conjugate to $x^2 A^{-1}$ in $\mathrm{GL}(2, \mathcal{O})$ for some $x \in \mathcal{O}^\times$. Taking determinants gives $\det A = \pm x^2$. If $\det A = x^2$, we are done. So assume that $\det A = -x^2$. Then a calculation shows that $\operatorname{tr}(x^2 A^{-1}) = -\operatorname{tr} A$. Thus, the fact that A and $x^2 A^{-1}$ are conjugate in $\mathrm{GL}(2, \mathcal{O})$ implies $\operatorname{tr} A = -\operatorname{tr} A$ and hence $\operatorname{tr} A = 0$, a contradiction. □

The following proposition will allow us to compute β_n when $q \equiv 1 \pmod 4$.

Proposition 3.3. *Suppose* $q \equiv 1 \pmod 4$ *and* $A \in \mathrm{GL}(2, \mathcal{O})$.

(1) *$\det A \in (\mathcal{O}^\times)^2$ if and only if A is conjugate to A^{-1} in K.*

(2) *A is not conjugate to ζA in K.*

Proof. Suppose A is conjugate to A^{-1} in K. As in the proof of Lemma 3.2, we have $\det A = \pm x^2$ for some $x \in \mathcal{O}^\times$. And since $q \equiv 1 \pmod 4$, we get $\det A \in (\mathcal{O}^\times)^2$. Combining this with Lemma 3.2 gives the proof of (1).

To prove (2), suppose that A and ζA are conjugate in K. Then

$$\det A \equiv \zeta^2 \det A \pmod{(\mathcal{O}^\times)^4}.$$

Thus $\zeta^2 = x^4$ for some $x \in \mathcal{O}^\times$ so that $\zeta = \pm x^2 \in (\mathcal{O}^\times)^2$, a contradiction. □

From Proposition 3.3(2) above, we can deduce that if

$$\{A_1, A_2, \dots, A_r\}$$

is a set of distinct conjugacy class representatives of K_n' (with $A_i \in \mathrm{GL}(2, \mathcal{O})$), then

$$\{A_1, \zeta A_1, A_2, \zeta A_2, \dots, A_r, \zeta A_r\}$$

is a set of distinct conjugacy class representatives of K_n. Now, Silberger's list of conjugacy class representatives of K_n' [Silberger 1970, p. 101] shows that when $q \equiv 1 \pmod 4$, exactly $(\alpha_n + (q^n - 1)/(q-1))/2$ of the A_i's have $\det A_i \in (\mathcal{O}^n)^{\times 2}$. Hence:

Proposition 3.4. *Let $q \equiv 1 \pmod 4$. Then*

$$\beta_n = \alpha_n + \frac{q^n - 1}{q - 1}.$$

Let us now consider the case $q \equiv 3 \pmod 4$.

Proposition 3.5. *Suppose $q \equiv 3 \pmod 4$ and let $A \in \mathrm{GL}(2, \mathcal{O})$. Then A is conjugate to ζA in K if and only if $\operatorname{tr} A = 0$.*

Proof. Suppose A is conjugate to ζA in K. Thus $x^2 A$ is conjugate to ζA in $\mathrm{GL}(2, \mathcal{O})$ for some $x \in \mathcal{O}^\times$. Taking determinants gives $x^4 = \zeta^2$, and since ζ is a nonsquare element of $\mathcal{O}^\times$ and $q \equiv 3 \pmod 4$, we get $x^2 = -\zeta$. Therefore $-\zeta A$ is conjugate to ζA in $\mathrm{GL}(2, \mathcal{O})$, and taking traces gives $\operatorname{tr} A = 0$.

Conversely, suppose $\operatorname{tr} A = 0$. A calculation shows that $sAs^{-1} = (-A)^{\mathrm{t}}$, where $s = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Recalling that every element of $\mathrm{GL}(2, \mathcal{O})$ is conjugate to its transpose, we see that A is conjugate to $-A$ in $\mathrm{GL}(2, \mathcal{O})$. And since $q \equiv 3 \pmod 4$ (i.e., -1 is a nonsquare element in $\mathcal{O}^\times$), we conclude that A is conjugate to ζA in K. □

From Proposition 3.5 above, we can deduce that if the union

$$\underbrace{\{A_1, \dots, A_r\}}_{\operatorname{tr} A_i \neq 0} \cup \underbrace{\{B_1, \dots, B_s\}}_{\operatorname{tr} B_i = 0}$$

is a set of distinct conjugacy class representatives of K_n', then the union

$$\{A_1, \zeta A_1, \dots, A_r, \zeta A_r\} \cup \{B_1, \dots, B_s\}$$

is a set of distinct conjugacy class representatives of K_n. With $q \equiv 3 \pmod 4$, Silberger's list of conjugacy class representatives of K_n' shows that exactly

$$(\alpha_n + (q^n - 1)/(q-1))/2 - 1$$

of the A_i's with $\operatorname{tr} A_i \neq 0$ have $\det A_i \in (\mathcal{O}^n)^{\times 2}$. Also from the list, the B_i's with $\operatorname{tr} B_i = 0$ are

$$\{B_i\} = \left\{ \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \zeta \\ 1 & 0 \end{smallmatrix}\right) \right\}.$$

And each B_i is conjugate to B_i^{-1} in K_n. Therefore:

Proposition 3.6. *Let* $q \equiv 3 \pmod 4$. *Then*

$$\beta_n = \alpha_n + \frac{q^n - 1}{q - 1}.$$

Thus, the value of β_n is the same regardless of whether q is congruent to 1 or 3 modulo 4. Finally, we obtain

$$\#\mathfrak{T}_n = (\beta_n - \beta_{n-1}) - (\alpha_n - \alpha_{n-1}) = q^{n-1},$$

which proves Theorem 3.1. Note that in contrast, $\#\mathfrak{T}_n' = \alpha_n - \alpha_{n-1} = q^n$.

3B. ***Class functions on finite groups.*** Here we introduce some more notations. Given representations π and τ of a profinite group G, we define their inner product $\langle \pi, \tau \rangle$ by

$$\langle \pi, \tau \rangle = \sum_{[\rho] \in \operatorname{Irr}(G)} (\text{multiplicity of } \rho \text{ in } \pi)(\text{multiplicity of } \rho \text{ in } \tau),$$

where $\operatorname{Irr}(G)$ is the set of isomorphism classes of irreducible representations of G.

For a finite group G, let $\operatorname{Cl}(G)$ denote the space of complex-valued class functions on G. We also define an inner product $\langle \cdot, \cdot \rangle$ on $\operatorname{Cl}(G)$ by

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)}.$$

Note that if π and τ are representations of G so that $\operatorname{tr} \pi, \operatorname{tr} \tau \in \operatorname{Cl}(G)$, we have

$$\langle \pi, \tau \rangle = \langle \operatorname{tr} \pi, \operatorname{tr} \tau \rangle.$$

Moreover, we let $X(G)$ denote the set of those $\chi \in \operatorname{Cl}(G)$ that can be written as a linear combination of irreducible characters of G with *integer* coefficients.

Suppose further that $G = G_1 \times G_2$ is a product of subgroups, and ρ_i a representation of G_i $(i = 1, 2)$. We then define the tensor product representation $\rho_1 \otimes \rho_2$ of G by

$$(\rho_1 \otimes \rho_2)(g_1, g_2) = \rho_1(g_1) \otimes \rho_2(g_2).$$

We note that if each ρ_i is irreducible, then so is their tensor product $\rho_1 \otimes \rho_2$; moreover, every irreducible representation of $G = G_1 \times G_2$ arises in this way [Serre 1977, p. 27, Theorem 10].

Proposition 3.7. *Let G be a finite group, $\zeta \in G$ a central involution, and $S \subset G$ a set of representatives for the distinct cosets in G of the central subgroup of order two generated by ζ. Fix $\chi' \in X(G)$ satisfying two conditions*:

(i) $\chi'(\zeta x) = \chi'(x)$ *for* $x \in G$.

(ii) *If* $s \in S$ *and* $\chi'(s) \neq 0$, *then* $|s|$ *is odd.*

Define a function χ on G by

$$\chi(x) = \begin{cases} \chi'(x) & \textit{if } x \in S, \\ -\chi'(x) & \textit{if } x \notin S. \end{cases}$$

Then $\chi \in X(G)$.

Proof. We begin by showing that χ is a class function on G. Take $g \in G$, $s \in S$, and write $gsg^{-1} = t$ or ζt with $t \in S$. Then $\chi'(s) = \chi'(t)$ because χ' is a class function on G and $\chi'(\zeta t) = \chi'(t)$. Now if $gsg^{-1} = t$, then

$$\chi(gsg^{-1}) = \chi'(t) = \chi'(s) = \chi(s)$$

by the definition of χ. If $gsg^{-1} = \zeta t$, then

$$\chi(gsg^{-1}) = -\chi'(t) = -\chi'(s) = -\chi(s).$$

If either s or t has even order, then by (ii) we conclude that $\chi(gsg^{-1})$ and $\chi(s)$ are both 0, hence equal. If $|s|$ and $|t|$ are both odd, then the equation $gsg^{-1} = \zeta t$ is impossible. Thus in all cases, we have $\chi(gsg^{-1}) = \chi(s)$. On the other hand, the definition of χ shows that $\chi(\zeta x) = -\chi(x)$ for all $x \in G$. Hence

$$\chi(g(\zeta s)g^{-1}) = \chi(\zeta gsg^{-1}) = -\chi(gsg^{-1}) = -\chi(s) = \chi(\zeta s).$$

Thus χ is a class function on G.

Now we will show that $\chi \in X(G)$. By Brauer's characterization of characters [Lang 2002, p. 709, Corollary 10.12], it suffices to show that $\chi|_E \in X(E)$ for every elementary subgroup E of G. But first suppose E is any subgroup of G (not necessarily elementary) such that $\zeta \notin E$. Then we claim that $\chi|_E = \chi'|_E$ and so

$\chi|_E \in X(E)$. For otherwise, there exists $x \in E$ such that $\chi(x) \neq \chi'(x)$. Thus $\zeta x \in S$ and $\chi'(\zeta x) \neq 0$ so that by (ii), $m := |\zeta x|$ is odd. But then

$$\zeta x^m = (\zeta x)^m = 1 \in E$$

so that $\zeta \in E$, a contradiction. Now an elementary subgroup of any finite group can be written in the form $A \times B$, where A is a group of odd order and B is a 2-group. Hence it suffices to show that $\chi|_E \in X(E)$ for every subgroup E of the form $E = A \times B$ with $\zeta \in E$.

Let $\chi^+ = \chi'$ and $\chi^- = \chi$. Suppose $x = ab \in E$ ($a \in A$, $b \in B$) with $\chi^\pm(x) \neq 0$. Writing $x = s$ or $x = \zeta s$ with $s \in S$, we have $\chi'(s) \neq 0$. By (ii), $|s|$ is odd, so $x = a$ (i.e., $b = 1$) or $x = a\zeta$ (i.e., $b = \zeta$). Therefore, we have

$$\chi^\pm|_E(ab) = \begin{cases} \chi^\pm|_A(a) & \text{if } b = 1, \\ \pm\chi^\pm|_A(a) & \text{if } b = \zeta, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\varphi^\pm$ be a class function on B defined by

$$\varphi^\pm(b) = \begin{cases} 1 & \text{if } b = 1, \\ \pm 1 & \text{if } b = \zeta, \\ 0 & \text{otherwise.} \end{cases}$$

so that $\chi^\pm|_E(ab) = \chi^\pm|_A(a) \cdot \varphi^\pm(b)$. Writing

$$\varphi^\pm = \sum_{[\rho] \in \mathrm{Irr}(B)} c_\rho \cdot \operatorname{tr} \rho \qquad (c_\rho \in \mathbb{C})$$

with $c_\rho = \langle \varphi^\pm, \operatorname{tr} \rho \rangle$, we find

$$\varphi^\pm = \frac{2}{\#B} \sum_{[\rho]} \dim \rho \cdot \operatorname{tr} \rho, \tag{$*$}$$

where the sum in $(*)$ runs over all $[\rho] \in \mathrm{Irr}(B)$ such that $\rho(\zeta) = \pm\,\mathrm{id}$. Since $\#A$ is odd, the definition of χ together with (ii) imply that $\chi|_A = \chi'|_A \in X(A)$. Thus write

$$\chi^\pm|_A = \sum_{[\pi_i] \in \mathrm{Irr}(A)} n_i \cdot \operatorname{tr} \pi_i \qquad (n_i \in \mathbb{Z})$$

so that

$$\chi^\pm|_E = \sum_{[\pi_i] \in \mathrm{Irr}(A)} \sum_{[\rho]} \frac{2}{\#B} \dim \rho \cdot n_i \cdot \operatorname{tr}(\pi_i \otimes \rho). \tag{$**$}$$

To show that $\chi|_E \in X(E)$, we must show that the coefficient $(2/\#B) \dim \rho \cdot n_i$ in $(**)$ is an integer for each ordered pair (i, ρ) with $\rho(\zeta) = -\,\mathrm{id}$. Since $\chi'|_E \in X(E)$, we know that $(2/\#B) \dim \rho \cdot n_i$ is an integer for every ordered pair (i, ρ) with $\rho(\zeta) = \mathrm{id}$. In particular, letting ρ be the trivial character of B, we get $\dim \rho = 1$

and so $(2/\#B)n_i$ is an integer for all i. Therefore, $(2/\#B)\dim\rho\cdot n_i$ is an integer regardless of ρ. □

3C. *The map φ_n.* We now describe the set $\mathfrak{T}_n$ for $n\geq 1$. Since $\mathfrak{T}_1=\{[\theta_1]\}$, we may assume that $n\geq 2$. For $n\geq 2$, let $\mathfrak{S}'_n$ be the set consisting of all $[\tau']\in\mathfrak{T}'_n$ *except* for the isomorphism classes of those representations of the form u_α and u_π^{unr}. Using Silberger's classification of irreducible representations of $\mathrm{PGL}(2,\mathcal{O})$ [Silberger 1970, pp. 98–100], we see that the cardinality of $\mathfrak{S}'_n$ is q^{n-1}. In particular, $\#\mathfrak{S}'_n=\#\mathfrak{T}_n$.

Let $\mathrm{Silb}^n\subset\mathrm{GL}(2,\mathcal{O}^n)$ be a set of conjugacy class representatives of K'_n as described by [Silberger 1970, p. 101]. We remark that there are several choices to be made here, including a nonsquare element ζ of $\mathcal{O}^\times$ and a prime element $\mathfrak{s}$ of $\mathcal{O}$. In any case, fix a choice of such a set Silb^n. Also observe that ζ, when viewed as an element of K_n, is a central involution.

Lemma 3.8. *Let $G=K_n$. There exists a set S of representatives for the distinct cosets of $\{1,\zeta\}$ in G which satisfies condition (ii) of Proposition 3.7 simultaneously for all $\chi'=\mathrm{tr}\,\tau'\in X(G)$ with $[\tau']\in\mathfrak{S}'_n$.*

Proof. Let $\chi'=\mathrm{tr}\,\tau'$ with $[\tau']\in\mathfrak{S}'_n$. An inspection of Silberger's tables shows that if $x\in\mathrm{Silb}^n$ and $\chi'(x)\neq 0$, then $|x|$ is odd. (Here, x is being viewed as an element of G.) Given $y\in G$, we can write either $y=gxg^{-1}$ or $y=\zeta gxg^{-1}$ with $x\in\mathrm{Silb}^n$ and $g\in G$, and in either case $\chi'(y)=\chi'(x)$. Hence if $\chi'(y)\neq 0$ then either $|y|$ or $|\zeta y|$ is odd. Now let S_0 be any set of representatives for the distinct cosets of $\{1,\zeta\}$ in G. After replacing each $y\in S_0$ by ζy if necessary, we obtain a set S with the required properties. □

We will now construct a bijection

$$\varphi_n:\mathfrak{S}'_n\to\mathfrak{T}_n.$$

Choose a set S as in Lemma 3.8. Given $[\tau']\in\mathfrak{S}'_n$, put $\chi'=\mathrm{tr}\,\tau'$. Define $\chi\in X(K_n)$ as in Proposition 3.7. Since $\chi(x)=\pm\chi'(x)$ for $x\in K_n$, we have $\langle\chi,\chi\rangle=\langle\chi',\chi'\rangle=1$. Also, $1\in S$ so that $\chi(1)=\chi'(1)=\dim\tau'>0$, and thus $\chi=\mathrm{tr}\,\tau$, where τ is an irreducible self-dual representation of K_n. Moreover, $\chi(\zeta)=-\chi'(1)<0$ so that $\omega_\tau\neq 1$. And by induction on $n\geq 2$, τ is primitive modulo $\mathfrak{p}^n$. Thus $[\tau]\in\mathfrak{T}_n$ and so we define $\varphi_n([\tau'])=[\tau]$. The map φ_n is injective, and since $\#\mathfrak{S}'_n=\#\mathfrak{T}_n$ we conclude that φ_n is a bijection.

We make a few observations. First, with the notations as in the previous paragraph, we have $\chi(x)=\chi'(x)$ for all $x\in\mathrm{Silb}^n$. For, suppose $x\in\mathrm{Silb}^n$ and $\chi'(x)\neq 0$ so that $|x|$ is odd. Now if $x\notin S$, then $\zeta x\in S$ and $\chi'(\zeta x)\neq 0$, and thus $|\zeta x|$ is odd by condition (ii) of Proposition 3.7. But $|x|$ and $|\zeta x|$ can not be both odd, hence $x\in S$ and so $\chi(x)=\chi'(x)$. Moreover, the map φ_n is independent of the choice of Silb^n

or S. And using Silberger's character tables for $[\tau'] \in \mathfrak{S}'_n$ in conjunction with the map φ_n, we can now write down the character tables for all $[\tau] \in \mathfrak{T}_n$. In particular, we have $\dim \tau' = q^{n-2}(q^2-1)$ for all $[\tau'] \in \mathfrak{S}'_n$ so that $\dim \tau = q^{n-2}(q^2-1)$ for $[\tau] \in \mathfrak{T}_n$ with $n \geq 2$.

Example. For $n \geq 2$, the map φ_n sends $[\sigma_n] \in \mathfrak{S}'_n$ to $[\theta_n] \in \mathfrak{T}_n$. This follows from the fact that $\operatorname{tr} \sigma_n(x) = \operatorname{tr} \theta_n(x)$ for all $x \in \mathrm{Silb}^n$. Note that we can compute $\operatorname{tr} \theta_n$ directly using the formula for the trace of an induced representation.

Remark. When $q \equiv 1 \pmod 4$, the map φ_n can be defined more directly using the following fact: Let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathcal{O})$ with $\omega_\tau \neq 1$, and H the kernel of the map $\lambda \circ \det : \mathrm{GL}(2, \mathcal{O}) \to \{\pm 1\}$. Then τ is induced from H (see [Rohrlich 2006, p. 365, Proposition 1]; the proof is valid for arbitrary $\mathcal{O}$).

4. Global multiplicities

Put $G = \mathrm{GL}(2, \mathbb{Z}_p)$ and let U be the open subgroup of $\mathbb{Z}_p^\times$ topologically generated by a fixed rational integer $m \geq 2$ such that $p \nmid m$. Let J denote the subgroup of G which consists of matrices of the form

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

with $u \in U$ and $z \in \mathbb{Z}_p$. Put $J'' = \{\pm I\}J$, and let η'' be the quadratic character of J'' given by $\eta''(b) = b_{22}$. Extend η'' to $J''(n)$ by setting $\eta'' | K(n) = 1$.

Proposition 4.1. *Let τ be an irreducible self-dual representation of G, and choose $n \geq 1$ such that $1 + p^n \in U$ and τ factors through $G/K(n)$. If $p \equiv -1 \pmod 4$, m is a quadratic nonresidue modulo p, and $\tau \cong \theta_i$ with $i \geq 1$, then $\langle \operatorname{ind}_{J''(n)}^G \eta'', \ \tau \rangle$ is odd. Otherwise, $\langle \operatorname{ind}_{J''(n)}^G \eta'', \ \tau \rangle$ is even.*

Proof. As in the proof of [Rohrlich 2006, p. 371, Proposition 7], we have

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

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

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

Thus, we must determine which of the four pairs $(\mu, \nu) = (1, 1)$, (λ, λ), $(1, \lambda)$, $(\lambda, 1)$ satisfy $(**)$.

Write a typical element $b \in J''$ as $b = \epsilon b(u, z)$ with $\epsilon \in \{\pm 1\}$, $u \in U$, and $z \in \mathbb{Z}_p$. Then $\eta''(b) = \epsilon$. If $\mu = \nu = 1$, then $\xi_{\mu,\nu}(b) = 1$. So, $(1, 1)$ does not satisfy $(**)$ and hence does not occur in $(*)$. If $\mu = \nu = \lambda$, then $\xi_{\mu,\nu}(b) = \lambda(u)$. So, (λ, λ)

does not occur in $(*)$ either. We now consider the pairs $(1, \lambda)$ and $(\lambda, 1)$. Note that $\xi_{1,\lambda}(b) = \lambda(\epsilon)$ and $\xi_{\lambda,1}(b) = \lambda(\epsilon)\lambda(u)$.

Suppose $p \equiv 1 \pmod 4$ so that $\lambda(\epsilon) = 1$. In this case, $\xi_{1,\lambda}(b) = 1$ and $\xi_{\lambda,1}(b) = \lambda(u)$. So neither $(1, \lambda)$ nor $(\lambda, 1)$ occurs in $(*)$ and we get

$$\langle \mathrm{ind}_{J''(n)}^{G} \eta'',\ \tau \rangle \equiv 0 \pmod 2.$$

Suppose $p \equiv -1 \pmod 4$ so that $\lambda(\epsilon) = \epsilon$. Thus $\xi_{1,\lambda}|J'' = \eta''$. Furthermore, $\xi_{\lambda,1}|J'' = \eta''$ if and only if $\lambda(m) = 1$. If $\lambda(m) = 1$, then $\langle \mathrm{ind}_{J''(n)}^{G} \eta'',\ \tau \rangle$ is even because the representations induced by $\xi_{1,\lambda}$ and $\xi_{\lambda,1}$ are equivalent [Rohrlich 2006, p. 38, Equation 3.5]. If $\lambda(m) = -1$, then $\xi_{\lambda,1}|J'' \neq \eta''$. We thus get

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

Since

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

and observing that if $\tau \cong \theta_i$, we necessarily have $1 \le i \le n$ because τ factors through $G/K(n)$ by assumption, the proof is complete. □

5. Local multiplicities

We first describe some local identifications and introduce notations. Given a place v of F, we let F_v denote the completion of F at v and $\bar{F}_v$ an algebraic closure of F_v that contains $\bar{F}$. Put $F_v^\infty = F^\infty F_v$, with the compositum taking place inside $\bar{F}_v$. Identify $\mathrm{Gal}(F_v^\infty/F_v)$ with the decomposition subgroup of $\mathrm{Gal}(F^\infty/F)$ that corresponds to the embedding $F^\infty \subset F_v^\infty$. Suppose τ is an irreducible self-dual representation of $\mathrm{Gal}(F^\infty/F)$. Then for each place v of F, we let τ_v denote the restriction of τ to $\mathrm{Gal}(F_v^\infty/F_v)$. Hence τ_v is still self-dual but not necessarily irreducible.

For $n \ge 1$, we let μ_n denote the group of nth roots of unity (inside an algebraically closed field) with a generator ζ_n. Furthermore, any one dimensional character $\chi : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathbb{C}^\times$ factors through $\mathrm{Gal}(K/F_v)$ for some finite abelian subextension K/F_v of $\bar{F}_v/F_v$, allowing us to view χ as a character of $F_v^\times$ via

$$\chi(x) = \chi((x^{-1}, K/F_v)) \qquad (x \in F_v^\times), \tag{6}$$

where $(*, K/F_v)$ is the local Artin map. Moreover, if K/F_v is any finite extension, we let ind_{K/F_v} and res_{K/F_v} denote the induction and restriction functors associated with $\mathrm{Gal}(\bar{F}_v/F_v)$ and its subgroup of finite index $\mathrm{Gal}(\bar{F}_v/K)$.

For the remainder of this section, we will assume $v \in T^+$ so that E/F_v is an elliptic curve having bad but potentially good reduction over F_v. For ease of notation, put $q = m_v$. Also, put $e = e_v$ as defined in (2), and assume that $e = 3$, 4, or 6 and $q \equiv -1 \pmod e$ so that $H = F_v(\zeta_e)$ is the unramified quadratic extension of F_v. Let η denote the unramified quadratic character of $\mathrm{Gal}(\bar{F}_v/F_v)$. Define a representation $\hat{\sigma}_e$ of $\mathrm{Gal}(\bar{F}_v/F_v)$ by

$$\hat{\sigma}_e = \mathrm{ind}_{H/F_v}\,\hat{\varphi}_e = \mathrm{ind}_{H/F_v}\,\hat{\varphi}_e^{-1},$$

where $\hat{\varphi}_e$ is either of the tamely ramified characters of $H^\times$ of exact order e such that $\hat{\varphi}_e|F_v^\times = 1$. Our goal in this section is to compute the parity of the integer

$$s(e, \tau_v) := \langle 1, \tau_v\rangle + \langle \eta, \tau_v\rangle + \langle \hat{\sigma}_e, \tau_v\rangle.$$

5A. *Representations η and $\hat{\sigma}_e$.*

Lemma 5.1. *Let E/F_v be an elliptic curve and suppose E has bad but potentially good reduction at v. Assume $v \mid \ell$, where $5 \le \ell < \infty$. Let Δ denote the discriminant associated to a minimal Weierstrass equation for E over F_v. Put*

$$e = \frac{12}{\gcd(v(\Delta), 12)} \;(= 2, 3, 4, \mathit{or}\ 6).$$

Then any finite Galois extension of F_v over which E acquires good reduction contains $F_v(\zeta_e)$.

Proof. Let K/F_v be a finite Galois extension over which E acquires good reduction. We will show that $F_v(\zeta_e) \subset K$. First, we note that $e \mid e'$, where e' is the ramification index of K/F_v. Let T/F_v and V/F_v denote the maximal unramified and the maximal tamely ramified subextensions of K/F_v, respectively. Thus, we have

$$F_v \subset T \subset V \subset K.$$

Write $e' = m\ell^a$ with $\gcd(m, \ell) = 1$ and $a \ge 0$. Note that $e \mid m$ because $\gcd(e, \ell) = 1$. The extension V/T is totally and tamely ramified of degree m. Since V/T is also Galois, we have $\mu_m \subset V$ and thus $\mu_e \subset V \subset K$ as desired. □

We apply this lemma to the situation at hand. Since $p \ge 3$ and $v \nmid p$, E has good reduction over $F_v(E[p])$ [Silverman 1994, p. 383, Proposition 10.3(b)]. Thus, we have $F_v(\zeta_e) \subset F_v(E[p])$ by Lemma 5.1. Therefore, η may be viewed as a character of $\mathrm{Gal}(F_v(E[p^n])/F_v)$ for all $n \ge 1$.

We state, without proof, a standard fact from group representation theory:

Lemma 5.2. *Let G be a profinite group and $\mathcal{H}$ a normal subgroup of finite index. Let χ be a character of $\mathcal{H}$ such that every conjugate of χ is a power of χ. Put $\rho = \mathrm{ind}_{\mathcal{H}}^{G}\,\chi$. Then* $\ker\rho = \ker\chi$.

Since $\hat{\varphi}_e|F_v^\times = 1$, we have $\hat{\varphi}_e \circ \gamma = \hat{\varphi}_e^{-1}$, where γ is the nontrivial element of $\mathrm{Gal}(H/F_v)$. Hence Lemma 5.2 implies $\ker\hat{\sigma}_e = \ker\hat{\varphi}_e$. Let M' be the fixed field of $\ker\hat{\sigma}_e$.

Next, let π be a uniformizer of F_v and put $M = F_v(\zeta_e, \pi^{1/e})$. We will show that $M' = M$, which will also imply that M is independent of the choice of the uniformizer π. We begin with the following lemma:

Lemma 5.3. *Let e be an integer with $e \geq 3$. Let G be a finite group of order $2e^2$ with subgroups I and C satisfying the following conditions*:

(i) *C is cyclic of order $2e$ whose unique subgroup J of order e is normal in G.*

(ii) *I is cyclic of order e and normal in G. Moreover*, *if c is a generator of C*, *then $cic^{-1} = i^{-1}$ for all $i \in I$.*

Suppose further that $I \cap J$ is trivial and put $K = I \times J$. Then there exists a unique cyclic subgroup N of K which is normal in G and for which G/N is dihedral of order $2e$. Furthermore $N = J$.

Proof. For existence, we take $N = J$. Note that the image of c in G/J is an involution. And since $cic^{-1} = i^{-1}$ for $i \in I$, it follows that G/J is dihedral.

For uniqueness, let N be such a subgroup of K and observe that K/N is the unique cyclic subgroup of G/N of order e. Hence any element of G/N not belonging to K/N is an involution. In particular, the image of c does not belong in K/N because $c \notin K$. So $c^2 = 1$ in G/N, that is, $c^2 \in N$. Thus $J \subset N$, and since $|J| = |N| = e$, we get $N = J$ as desired. □

To apply the lemma, we let H_e^{ab} be the maximal abelian extension of H of exponent e. Write $H_e^{\mathrm{ab}} = H_1 H_2$, where H_1 is the unramified extension of H of degree e and $H_2 = H(\pi^{1/e})$ with a uniformizer π of F_v. Using the notations of Lemma 5.3, put $G = \mathrm{Gal}(H_e^{\mathrm{ab}}/F_v)$, $I = \mathrm{Gal}(H_e^{\mathrm{ab}}/H_1)$, and $C = \mathrm{Gal}(H_e^{\mathrm{ab}}/F_v(\pi^{1/e}))$ so that $J = \mathrm{Gal}(H_e^{\mathrm{ab}}/H_2)$. To see that c acts on I by inversion, it suffices to verify that cic^{-1} and i^{-1} ($i \in I$) agree on $\pi^{1/e}$. And in fact, they both send $\pi^{1/e}$ to $\omega^{-1}\pi^{1/e}$, where ω is the e-th root of unity such that $i(\pi^{1/e}) = \omega\pi^{1/e}$. Finally, recall that M' is the fixed field of $\ker \hat{\sigma}_e = \ker \hat{\varphi}_e$ and note that M'/H is a subextension of H_e^{ab}/H. Putting $N = \mathrm{Gal}(H_e^{\mathrm{ab}}/M')$, we observe that G/N is isomorphic to the image of $\hat{\sigma}_e$, hence dihedral [Rohrlich 1996, pp. 316–317, Proposition 1(ii)]. Thus we can deduce using Lemma 5.3 that $N = J$, or equivalently, $M' = H_2 = F_v(\zeta_e, \pi^{1/e})$.

5B. ***The decomposition subgroup.*** Next, we will determine the structure of the decomposition subgroup $D = \mathrm{Gal}(F_v^{\infty}/F_v)$. Fixing a choice of a $\mathbb{Z}_p$-basis for $T_p(E)$, we obtain an embedding

$$\rho : D \hookrightarrow \mathrm{GL}(2, \mathbb{Z}_p)$$

via the natural action of $\mathrm{Gal}(F_v^{\infty}/F_v)$ on $T_p(E)$. We will also determine the conjugacy class of $\rho(g) \in \mathrm{GL}(2, \mathbb{Z}_p)$ for certain representative elements $g \in D$.

We begin by letting $V_p(E) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(E)$ and $\sigma'_{E/F_v,p}$ the contragradient of the natural action of $\operatorname{Gal}(\bar{F}_v/F_v)$ on $V_p(E)$. Hence $\sigma'_{E/F_v,p}$ is the map

$$\sigma'_{E/F_v,p} : \operatorname{Gal}(\bar{F}_v/F_v) \to \operatorname{GL}(V_p(E)^*),$$

where $V_p(E)^*$ is the dual of $V_p(E)$. Let $\sigma_{E/F_v,p}$ be the restriction of $\sigma'_{E/F_v,p}$ to the Weil group $\mathcal{W}(\bar{F}_v/F_v)$. Fix an embedding $\iota : \mathbb{Q}_p \hookrightarrow \mathbb{C}$, and compose $\sigma_{E/F_v,p}$ with the extension-of-scalars map $\operatorname{GL}(V_p(E)^*) \hookrightarrow \operatorname{GL}(\mathbb{C} \otimes_\iota V_p(E)^*)$ to obtain a homomorphism

$$\sigma_{E/F_v,p,\iota} : \mathcal{W}(\bar{F}_v/F_v) \to \operatorname{GL}(V),$$

where, for ease of notation, we put $V = \mathbb{C} \otimes_\iota V_p(E)^*$. Since E has potential good reduction over F_v, $\sigma_{E/F_v,p,\iota}$ is continuous [Rohrlich 1994, pp. 131 and 148], and hence is a two-dimensional complex representation. Note also that $\sigma_{E/F_v,p,\iota}$ is semisimple and so its isomorphism class is independent of p and ι [Rohrlich 1994, p. 148]. Thus we will simply write σ_{E/F_v} instead of $\sigma_{E/F_v,p,\iota}$.

Let $F_v^{\mathrm{unr}} \subset \bar{F}_v$ denote the maximal unramified extension of F_v and $R \subset \bar{F}_v$ the minimal extension of F_v^{unr} over which E acquires good reduction. Then $\ker \sigma_{E/F_v} = \operatorname{Gal}(\bar{F}_v/R)$ and we may view σ_{E/F_v} as a faithful representation of

$$\mathcal{W}(R/F_v) = \mathcal{W}(\bar{F}_v/F_v)/\operatorname{Gal}(\bar{F}_v/R).$$

Letting $\Phi \in \operatorname{Gal}(\bar{F}_v/F_v)$ denote an inverse Frobenius element, we have

$$\mathcal{W}(R/F_v) = \operatorname{Gal}(R/F_v^{\mathrm{unr}}) \rtimes \langle \Phi|R \rangle. \tag{7}$$

By [Serre 1972, p. 312], we have $\operatorname{Gal}(R/F_v^{\mathrm{unr}}) \cong \mathbb{Z}/e\mathbb{Z}$. And since $e = 3$, 4, or 6, and $q \equiv -1 \pmod{e}$, $\mathcal{W}(R/F_v)$ is nonabelian [Rohrlich 1996, pp. 331–332]. Thus, letting h be a generator of $\operatorname{Gal}(R/F_v^{\mathrm{unr}})$, we have $\Phi h \Phi^{-1} = h^{-1}$.

Since $\mathcal{W}(R/F_v)$ is a dense subgroup of $\operatorname{Gal}(R/F_v)$, (7) implies

$$\operatorname{Gal}(R/F_v) = \operatorname{Gal}(R/F_v^{\mathrm{unr}}) \rtimes \overline{\langle \Phi|R \rangle} = \langle h \rangle \rtimes \overline{\langle \Phi|R \rangle},$$

where the closure is taken in $\operatorname{Gal}(R/F_v)$. Observe that $R = F_v^\infty F_v^{\mathrm{unr}}$. (In fact, since E has good reduction over $F_v(E[p])$, we have $R = F_v(E[p])F_v^{\mathrm{unr}}$.) Therefore we have

$$D = \operatorname{Gal}(F_v^\infty/F_v) = \langle h|F_v^\infty \rangle \rtimes \overline{\langle \Phi|F_v^\infty \rangle},$$

with the closure now taken in D. We still have $\langle h|F_v^\infty \rangle = \mathbb{Z}/e\mathbb{Z}$ because $R = F_v^\infty F_v^{\mathrm{unr}}$. Now our task is to determine the conjugacy classes of $\rho(\Phi)$ and $\rho(h)$ in $\operatorname{GL}(2, \mathbb{Z}_p)$.

The element $(\Phi|R)^2 \in \mathcal{W}(R/F_v)$ is central. And since σ_{E/F_v} is irreducible (because $\mathcal{W}(R/F_v)$ is nonabelian and σ_{E/F_v} is semisimple), Schur's Lemma implies that $\sigma_{E/F_v}((\Phi|R)^2)$ is multiplication by c for some $c \in \mathbb{C}^\times$. Let

$$T = \sigma_{E/F_v}(\Phi|R) \in \operatorname{GL}(V)$$

so that $T^2 = c \cdot \mathrm{id}_V$. We will show that T has distinct eigenvalues $\sqrt{c}$ and $-\sqrt{c}$. Suppose on the contrary that T has a single repeated eigenvalue $\lambda = \sqrt{c}$ or $-\sqrt{c}$. Then the Jordan canonical form of T is either $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$. The latter possibility contradicts $T^2 = c \cdot \mathrm{id}_V$, while the former implies that T is scalar and hence $\Phi|R$ acts trivially on $\mathrm{Gal}(R/F_v^{\mathrm{unr}})$. We conclude that the Jordan canonical form of T is

$$\begin{pmatrix} \sqrt{c} & 0 \\ 0 & -\sqrt{c} \end{pmatrix},$$

as desired. This also means that $\det T = -c$, and since

$$\det T = \det \sigma_{E/F_v}(\Phi|R) = \omega^{-1}(\Phi|R) = q,$$

where ω denotes the p-adic cyclotomic character of $\mathcal{W}(\bar{F}_v/F_v)$ [Rohrlich 1994, p. 150], we get $c = -q$. Therefore, the characteristic polynomial of T is $x^2 + q$. Moreover, since $q \in \mathbb{Q}$ and thus is fixed by the embedding $\imath : \mathbb{Q}_p \hookrightarrow \mathbb{C}$, we conclude that the characteristic polynomial of $\sigma'_{E/F_v,p}(\Phi)$ is also $x^2 + q$.

Recall that h is a generator of $\mathrm{Gal}(R/F_v^{\mathrm{unr}}) \cong \mathbb{Z}/e\mathbb{Z}$. Then

$$\det \sigma_{E/F_v}(h) = \omega^{-1}(h) = 1$$

because ω is trivial on the inertia subgroup $I_v = \mathrm{Gal}(\bar{F}_v/F_v^{\mathrm{unr}})$. One then easily shows that the eigenvalues of $\sigma_{E/F_v}(h)$ are ζ_e and ζ_e^{-1}, so its characteristic polynomial is $x^2 - z_e x + 1$, where

$$z_e = \zeta_e + \zeta_e^{-1} = \begin{cases} -1 & \text{if } e = 3, \\ \ \ 0 & \text{if } e = 4, \\ \ \ 1 & \text{if } e = 6. \end{cases}$$

And since $z_e \in \mathbb{Q}$, the characteristic polynomial of $\sigma'_{E/F_v,p}(h)$ is also $x^2 - z_e x + 1$.

To summarize, we have the following. For a fixed choice of a $\mathbb{Z}_p$-basis for $T_p(E)$, we have a map

$$\sigma'_{E/F_v,p} : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{GL}(2, \mathbb{Q}_p)$$

whose image is in $\mathrm{GL}(2, \mathbb{Z}_p)$. We have shown that

$$\sigma'_{E/F_v,p}(\Phi) \sim \begin{pmatrix} 0 & -q \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \sigma'_{E/F_v,p}(h) \sim \begin{pmatrix} 0 & -1 \\ 1 & z_e \end{pmatrix}, \tag{8}$$

where $\sim$ denotes conjugacy over $\mathbb{Q}_p$.

Lemma 5.4. *Consider $A \in \mathrm{GL}(2, \mathbb{Z}_p)$ whose reduction $\bar{A} \in \mathrm{GL}(2, \mathbb{F}_p)$ is nonscalar. Then A is conjugate in* $\mathrm{GL}(2, \mathbb{Z}_p)$ *to its rational canonical form.*

Proof. Since $\bar{A}$ is nonscalar, there exists

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Z}_p)$$

such that

$$(\bar{B})^{-1} \bar{A} \; \bar{B} = \begin{pmatrix} 0 & * \\ 1 & * \end{pmatrix} \text{ in } \mathrm{GL}(2, \mathbb{F}_p).$$

Let v denote the column vector $v = (a, c)^{\mathrm{t}}$ so that $\bar{A}\bar{v} = (\bar{b}, \bar{d})^{\mathrm{t}}$. Thus, the matrix $U = (v, Av)$ is in $\mathrm{GL}(2, \mathbb{Z}_p)$ because $\bar{U} = \bar{B} \in \mathrm{GL}(2, \mathbb{F}_p)$. Now, $U^{-1}AU$ is the matrix of A with respect to the basis $\{v, Av\}$ so that

$$U^{-1}AU = \begin{pmatrix} 0 & -\det A \\ 1 & \operatorname{tr} A \end{pmatrix},$$

as desired. □

Applying Lemma 5.4, we see that the conjugations in (8) actually occur over $\mathbb{Z}_p$. We summarize the results of this section with the following proposition.

Proposition 5.5. *Let $D = \mathrm{Gal}(F_v^\infty / F_v)$ be the decomposition subgroup and let $\rho : D \hookrightarrow \mathrm{GL}(2, \mathbb{Z}_p)$ be an embedding induced by the natural action of $\mathrm{Gal}(F_v^\infty / F_v)$ on $T_p(E)$. Then*

$$D = \langle h | F_v^\infty \rangle \rtimes \overline{\langle \Phi | F_v^\infty \rangle}$$

with $\langle h | F_v^\infty \rangle \cong \mathbb{Z}/e\mathbb{Z}$ and $\Phi h \Phi^{-1} = h^{-1}$. Moreover,

$$\rho(\Phi) \sim \begin{pmatrix} 0 & (-q)^{-1} \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \rho(h) \sim \begin{pmatrix} z_e & -1 \\ 1 & 0 \end{pmatrix}, \tag{9}$$

where $\sim$ denotes conjugation over $\mathbb{Z}_p$.

Proof. The conjugacy classes of $\rho(\Phi)$ and $\rho(h)$ require some explanation. If we use the same $\mathbb{Z}_p$-basis for $T_p(E)$ in ρ and in $\sigma'_{E/F_v,p}$, we obtain

$$\rho(\Phi) = \sigma'_{E/F_v,p}(\Phi)^{-\mathrm{t}} \sim \begin{pmatrix} 0 & -q \\ 1 & 0 \end{pmatrix}^{-\mathrm{t}} = \begin{pmatrix} 0 & (-q)^{-1} \\ 1 & 0 \end{pmatrix},$$

where the superscript $-\mathrm{t}$ denotes the inverse transpose. Note that $\sigma'_{E/F_v,p}$ is the contragradient of the natural action, and thus we must take the inverse transpose here. The conjugacy class of $\rho(h)$ is obtained analogously. □

5C. ***Images of D.*** We will find the image of D in $K'_n = \mathrm{PGL}(2, \mathbb{Z}/p^n\mathbb{Z})$ and in $K_n = \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})/(\mathbb{Z}/p^n\mathbb{Z})^{\times 2}$. Put $F_v^{(n)} = F_v(E[p^n])$ and $D^n = \mathrm{Gal}(F_v^{(n)}/F_v)$ for $n \geq 1$. Since $\rho(\mathrm{Gal}(F_v^\infty / F_v^{(n)})) \subset K(n)$, ρ induces an embedding (which we also denote by ρ)

$$\rho : D^n \hookrightarrow \mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z}).$$

The group D^n is generated by the elements $h|F_v^{(n)}$ and $\Phi|F_v^{(n)}$ with relations $h^e = 1$, $\Phi h \Phi^{-1} = h^{-1}$, and possibly more. We can obtain further information about D^n by studying its embedded image in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. For example, the rational canonical form of $\rho(\Phi)$ given in (9) implies that $\Phi|F_v^{(n)}$ has order $2d_n$ in D^n, where d_n is the order of $-q$ modulo p^n.

We will also determine whether or not the unramified quadratic character η and the representation $\hat{\sigma}_e$ of $\mathrm{Gal}(\bar{F}_v/F_v)$ factor through the image of D in K'_n and in K_n. Recall from Section 5A that η factors through D^n for all $n \geq 1$ and that $\ker \hat{\sigma}_e = \mathrm{Gal}(\bar{F}_v/M)$, where $M = F_v(\zeta_e, \pi^{1/e})$ for any uniformizer π of F_v. Consequently, the image of $\hat{\sigma}_e$ is isomorphic to $\mathrm{Gal}(M/F_v) \cong \mathbb{Z}/e\mathbb{Z} \rtimes \{\pm 1\}$. Moreover, noting that Φ is an (inverse) Frobenius element of $\mathrm{Gal}(\bar{F}_v/F_v)$ and that $q \equiv -1 \pmod{e}$, we get $\Phi^2|M = \mathrm{id}_M$ so that $\Phi^2 \in \mathrm{Gal}(\bar{F}_v/M)$. We now consider the three cases, $e = 3, 4$, and 6.

Remark. In the discussions to follow, we will often commit a slight abuse of notation (for the sake of brevity) and write Φ to denote both an element of D^n and its image $\rho(\Phi)$ in $\rho(D^n)$. We will do likewise with h. Their meaning should be clear from the context in which they are used.

The case $e = 3$. Let $e = 3$ (that is, $z_e = -1$). Then D^n is a semidirect product

$$D^n = \langle h \rangle \rtimes \langle \Phi \rangle. \tag{10}$$

Let L be the fixed field of $\langle \Phi|F_v^{(1)} \rangle \subset \mathrm{Gal}(F_v^{(1)}/F_v)$ so that L/F_v is totally ramified. In fact, since $\mathrm{Gal}(F_v^{(1)}/F_v) = \mathbb{Z}/3\mathbb{Z} \rtimes \langle \Phi \rangle$ by (10), we see that L/F_v is totally and tamely ramified of degree 3. (Note: The residue characteristic of v is $\ell \geq 5$.) Thus, we may write $L = F_v(\pi^{1/3})$ for some uniformizer π of F_v so that $F_v^{(1)}$ contains $M = F_v(\zeta_3, \pi^{1/3})$. Therefore $\hat{\sigma}_3$ factors through $\mathrm{Gal}(F_v^{(1)}/F_v)$ and so $\hat{\sigma}_3$ may be viewed as a representation of $D^n = \mathrm{Gal}(F_v^{(n)}/F_v)$ for all $n \geq 1$.

Let Z denote the subgroup of all scalar matrices in $\rho(D^n)$. Then $Z = \langle \Phi^2 \rangle$ so that the image of D in K'_n is given by

$$G'_3 := \frac{\rho(D^n)}{Z} = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes \{\pm 1\}$$

for all $n \geq 1$. Moreover, η and $\hat{\sigma}_3$ may both be viewed as representations of G'_3 because they are trivial on Z. The character table of G'_3 is shown in Table 1.

Let $Z^{(2)}$ be the subgroup of $\rho(D^n)$ defined as

$$Z^{(2)} = \left\{ a^2 \cdot I \in \rho(D^n) : a \in (\mathbb{Z}/p^n\mathbb{Z})^\times \right\} \tag{11}$$

so that the image of D in K_n is given by $G_3 := \rho(D^n)/Z^{(2)}$. We remark that the structure of G_3 depends only on the Legendre symbol of $-q$ modulo p. In particular, it is independent of n.

	1	η	$\operatorname{tr}\hat{\sigma}_3$
$\{1\}$	1	1	2
$\{h, h^2\}$	1	1	-1
$\{\Phi, h\Phi, h^2\Phi\}$	1	-1	0

Table 1. Character table of G_3'.

(a) Suppose $\lambda(-q) = 1$. Then $Z^{(2)} = Z$ so that $G_3 = G_3'$. Hence, the character table of G_3 is given by Table 1.

(b) Suppose $\lambda(-q) = -1$. Then $Z^{(2)} = \langle \Phi^4 \rangle$, so $G_3 = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$. Table 2 shows the character table of G_3 ($\psi \cong \chi_i \otimes \hat{\sigma}_3$, where $i = 1$ or 2).

	1	η	χ_1	χ_2	$\operatorname{tr}\hat{\sigma}_3$	$\operatorname{tr}\psi$
$\{1\}$	1	1	1	1	2	2
$\{\Phi^2\}$	1	1	-1	-1	2	-2
$\{h, h^2\}$	1	1	1	1	-1	-1
$\{h\Phi^2, h^2\Phi^2\}$	1	1	-1	-1	-1	1
$\{\Phi, h\Phi, h^2\Phi\}$	1	-1	$\sqrt{-1}$	$-\sqrt{-1}$	0	0
$\{\Phi^3, h\Phi^3, h^2\Phi^3\}$	1	-1	$-\sqrt{-1}$	$\sqrt{-1}$	0	0

Table 2. Character table of G_3 when $\lambda(-q) = -1$.

The case $e = 4$. Let $e = 4$ (i.e., $z_e = 0$). Recall that d_n is the order of $-q$ modulo p^n. The structure of D^n varies according to the parity of d_n. But note that the parity of d_n is independent of n.

If d_n is odd, then D^n is a semidirect product $D^n = \langle h \rangle \rtimes \langle \Phi \rangle$. Moreover, the representation $\hat{\sigma}_4$ factors through D^n for all $n \geq 1$ when d_n is odd, since the same argument from the case $e = 3$ applies here as well.

If $d = d_n$ is even, we have $\rho(\Phi^d) = \rho(h^2) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$. Thus, D^n is generated by h and Φ with relations $h^4 = 1$, $\Phi^d = h^2$, and $\Phi h \Phi^{-1} = h^{-1}$.

Let Z denote the subgroup of all scalar matrices in $\rho(D^n)$. Then

$$Z = \{h^i \Phi^j : i, j \text{ are even}\}.$$

Thus, regardless of the parity of d_n, the image of D in K_n' is given by

$$G_4' := \frac{\rho(D^n)}{Z} = \langle h \rangle \times \langle \Phi \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

for all $n \geq 1$. Since η is trivial on Z, it may be viewed as a character of G_4'. Table 3 shows the character table of G_4'.

	1	η	χ_1	χ_2
1	1	1	1	1
h	1	1	-1	-1
Φ	1	-1	1	-1
$h\Phi$	1	-1	-1	1

Table 3. Character table of G_4'.

Define the subgroup $Z^{(2)}$ of $\rho(D^n)$ as in (11) so that the image of D in K_n is given by $G_4 := \rho(D^n)/Z^{(2)}$. Then the structure of the group G_4 depends only on the Legendre symbols of -1 and $-q$ modulo p.

(a) Suppose $p \equiv 1 \pmod 4$ and $\lambda(-q) = 1$. Then $Z^{(2)} = Z$, so $G_4 = G_4'$, and the character table of G_4 is given by Table 3.

(b) Suppose $p \equiv 1 \pmod 4$ and $\lambda(-q) = -1$. Then $d_n \equiv 0 \pmod 4$ and $Z^{(2)} = \{h^i \Phi^j : 2 \mid i,\ 4 \mid j\}$, so

$$G_4 = \langle h \rangle \times \langle \Phi \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

The character table of G_4 is shown in Table 4.

(c) Suppose $p \equiv -1 \pmod 4$ and $\lambda(-q) = 1$. Then d_n is odd and $Z^{(2)} = \langle \Phi^2 \rangle$, so

$$G_4 = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/4\mathbb{Z} \rtimes \{\pm 1\}.$$

The character table of G_4 is given by Table 5. Because d_n is odd, $\hat{\sigma}_4$ factors through D^n. And since $\hat{\sigma}_4$ is trivial on $Z^{(2)}$, it factors through G_4 as well.

	1	η	χ_1	χ_2	χ_3	χ_4	χ_5	χ_6
1	1	1	1	1	1	1	1	1
h	1	1	1	1	-1	-1	-1	-1
Φ	1	-1	i	$-i$	1	-1	i	$-i$
$h\Phi$	1	-1	i	$-i$	-1	1	$-i$	i
Φ^2	1	1	-1	-1	1	1	-1	-1
$h\Phi^2$	1	1	-1	-1	-1	-1	1	1
Φ^3	1	-1	$-i$	i	1	-1	$-i$	i
$h\Phi^3$	1	-1	$-i$	i	-1	1	i	$-i$

Table 4. Character table of G_4 when $p \equiv 1 \pmod 4$, $\lambda(-q) = -1$. Here $i = \sqrt{-1}$.

	1	η	χ_1	χ_2	$\operatorname{tr}\hat{\sigma}_4$
$\{1\}$	1	1	1	1	2
$\{h^2\}$	1	1	1	1	–2
$\{h, h^3\}$	1	1	–1	–1	0
$\{\Phi, h^2\Phi\}$	1	–1	1	–1	0
$\{h\Phi, h^3\Phi\}$	1	–1	–1	1	0

Table 5. Character table of G_4 when $p \equiv -1 \pmod 4$, $\lambda(-q) = 1$.

(d) Suppose $p \equiv -1 \pmod 4$ and $\lambda(-q) = -1$. Then $d_n \equiv 2 \pmod 4$ and $Z^{(2)} = \langle h^2\Phi^2\rangle$ so that G_4 is generated by h and Φ with relations $h^4 = 1$, $\Phi^2 = h^2$, and $\Phi h \Phi^{-1} = h^{-1}$. In other words, G_4 is the quaternion group of order 8 and its character table is given by Table 6. Note here that $\psi \not\cong \hat{\sigma}_4$, that is, the representation $\hat{\sigma}_4$ does not factor through G_4 because its image is the dihedral group of order 8 which is not a quotient of G_4.

	1	η	χ_1	χ_2	$\operatorname{tr}\psi$
$\{1\}$	1	1	1	1	2
$\{h^2\}$	1	1	1	1	–2
$\{h, h^3\}$	1	1	–1	–1	0
$\{\Phi, h^2\Phi\}$	1	–1	1	–1	0
$\{h\Phi, h^3\Phi\}$	1	–1	–1	1	0

Table 6. Character table of G_4 when $p \equiv -1 \pmod 4$, $\lambda(-q) = -1$.

The case $e = 6$. Let $e = 6$ (i.e., $z_e = 1$). The analysis is very similar to that of the case $e = 4$. Thus, we will omit details and merely present the results.

Let G_6' denote the image of D in K_n'. Then $G_6' = \langle h\rangle \rtimes \langle\Phi\rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes \{\pm 1\}$, and its character table is shown in Table 7. Note that $\psi \not\cong \hat{\sigma}_6$, that is, $\hat{\sigma}_6$ does not factor through G_6' since its image has order 12 and hence is not a quotient of G_6'.

Now let G_6 be the image of D in K_n. As with the case $e = 4$, the group G_6 depends only on the Legendre symbols of -1 and $-q$ modulo p.

	1	η	$\operatorname{tr}\psi$
$\{1\}$	1	1	2
$\{h, h^2\}$	1	1	–1
$\{\Phi, h\Phi, h^2\Phi\}$	1	–1	0

Table 7. Character table of G_6'.

	1	η	χ_1	χ_2	$\mathrm{tr}\,\psi_1$	$\mathrm{tr}\,\psi_2$
$\{1\}$	1	1	1	1	2	2
$\{\Phi^2\}$	1	1	–1	–1	2	–2
$\{h, h^2\}$	1	1	1	1	–1	–1
$\{h\Phi^2, h^2\Phi^2\}$	1	1	–1	–1	–1	1
$\{\Phi, h\Phi, h^2\Phi\}$	1	–1	$\sqrt{-1}$	$-\sqrt{-1}$	0	0
$\{\Phi^3, h\Phi^3, h^2\Phi^3\}$	1	–1	$-\sqrt{-1}$	$\sqrt{-1}$	0	0

Table 8. Character table of G_6 when $p \equiv 1 \pmod 4$, $\lambda(-q) = -1$.

(a) Suppose $p \equiv 1 \pmod 4$ and $\lambda(-q) = 1$. Then $G_6 = G_6'$ and the character table of G_6 is given by Table 7.

(b) Suppose $p \equiv 1 \pmod 4$ and $\lambda(-q) = -1$. Then

$$G_6 = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}.$$

The character table of G_6 is shown in Table 8. Note that $\psi_i \not\cong \hat{\sigma}_6$ $(i = 1, 2)$ because the image of $\hat{\sigma}_6$ is a dihedral group of order 12 and hence is not a quotient of G_6.

(c) Suppose $p \equiv -1 \pmod 4$ and $\lambda(-q) = 1$. Then

$$G_6 = \langle h \rangle \rtimes \langle \Phi \rangle \cong \mathbb{Z}/6\mathbb{Z} \rtimes \{\pm 1\}.$$

The character table of G_6 is shown in Table 9.

(d) Suppose $p \equiv -1 \pmod 4$ and $\lambda(-q) = -1$. Then G_6 is generated by h and Φ with relations

$$h^6 = 1, \;\; \Phi^2 = h^3, \;\; \text{and } \Phi h \Phi^{-1} = h^{-1}.$$

The character table of G_6 is shown in Table 10. Note that $\psi_i \not\cong \hat{\sigma}_6$ $(i = 1, 2)$.

	1	η	χ_1	χ_2	$\mathrm{tr}\,\psi$	$\mathrm{tr}\,\hat{\sigma}_6$
$\{1\}$	1	1	1	1	2	2
$\{h^3\}$	1	1	–1	–1	2	–2
$\{h, h^5\}$	1	1	–1	–1	–1	1
$\{h^2, h^4\}$	1	1	1	1	–1	–1
$\{\Phi, h^2\Phi, h^4\Phi\}$	1	–1	1	–1	0	0
$\{h\Phi, h^3\Phi, h^5\Phi\}$	1	–1	–1	1	0	0

Table 9. Character table of G_6 when $p \equiv -1 \pmod 4$, $\lambda(-q) = 1$.

	1	η	χ_1	χ_2	$\mathrm{tr}\,\psi_1$	$\mathrm{tr}\,\psi_2$
$\{1\}$	1	1	1	1	2	2
$\{h^3\}$	1	1	-1	-1	2	-2
$\{h, h^5\}$	1	1	-1	-1	-1	1
$\{h^2, h^4\}$	1	1	1	1	-1	-1
$\{\Phi, h^2\Phi, h^4\Phi\}$	1	-1	$\sqrt{-1}$	$-\sqrt{-1}$	0	0
$\{h\Phi, h^3\Phi, h^5\Phi\}$	1	-1	$-\sqrt{-1}$	$\sqrt{-1}$	0	0

Table 10. Character table of G_6 when $p \equiv -1 \pmod 4$, $\lambda(-q) = -1$.

5D. ***Computing $s(e, \tau_v)$ when $\omega_\tau = 1$.*** We are now ready to compute the sum

$$s(e, \tau_v) = \langle 1, \tau_v\rangle + \langle \eta, \tau_v\rangle + \langle \hat{\sigma}_e, \tau_v\rangle \pmod 2$$

for representations τ of $G = \mathrm{GL}(2, \mathbb{Z}_p)$ with $\omega_\tau = 1$. Let us consider the individual cases $e = 3$, 4, and 6.

The case $e = 3$. Let $e = 3$ so that $\rho(h) \in \mathrm{GL}(2, \mathbb{Z}_p)$ is conjugate to the matrix $M_h = M_{h,3} = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Let τ be an irreducible representation of $\mathrm{PGL}(2, \mathbb{Z}_p)$ (which, we recall, is necessarily self-dual) so that τ_v may be viewed as a representation of G_3'. Using Table 1, we may write

$$\tau_v \cong 1^{\oplus m_1} \oplus \eta^{\oplus m_2} \oplus \hat{\sigma}_3^{\oplus m_3} \qquad (m_i \geq 0)$$

and obtain the equations $\dim \tau = m_1 + m_2 + 2m_3$ and $\mathrm{tr}\,\tau(M_h) = m_1 + m_2 - m_3$, so

$$s(3, \tau_v) = m_1 + m_2 + m_3 = \tfrac{1}{3}\bigl(2\dim \tau + \mathrm{tr}\,\tau(M_h)\bigr). \tag{12}$$

Thus it suffices to compute the trace $\mathrm{tr}\,\tau(M_h)$, for which we will rely on Silberger's character tables [Silberger 1970, pp. 102 and 107]. Silberger [p. 101] also lists representatives for the conjugacy classes of $\mathrm{PGL}(2, \mathbb{Z}/p^i\mathbb{Z})$. And in order to use his character tables, we must first find the matrix on this list to which M_h is conjugate.

Fix a prime element $\mathfrak{s}$ of $\mathbb{Q}_p$ and a nonsquare element ζ of $\mathbb{Z}_p^\times$. We note that $\mathfrak{s}$ is the same as Silberger's τ.

Proposition 5.6. *Let $M_h = M_{h,3} = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $M_h \sim \alpha A$ in* $\mathrm{GL}(2, \mathbb{Z}/p^i\mathbb{Z})$ $(i > 0)$, *where $\alpha \in \mathbb{Z}_p^\times$ and $A \in$* $\mathrm{GL}(2, \mathbb{Z}_p)$ *are given as follows*:

- *If $p \equiv 1 \pmod 3$, then $\alpha = t$ and $A = \left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $t^2 + t + 1 = 0$. Moreover, $A = \beta B$, where $\beta = (1-b)^{-1}$ and*

$$B = \begin{pmatrix} 1+b & 0 \\ 0 & 1-b \end{pmatrix}$$

with $b = 1 + 2t^{-2}$. In particular, $\mathrm{ord}_p(b) = 0$.

- *If* $p \equiv -1 \pmod 3$, *then* $\alpha = -\frac{1}{2}$ *and*
$$A = \begin{pmatrix} 1 & b\zeta \\ b & 1 \end{pmatrix}$$
with $b^2 = -3/\zeta$. *In particular*, $\operatorname{ord}_p(b) = 0$.
- *Suppose* $p = 3$. *Then*
$$\begin{cases} A = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \textit{ and } \alpha = 1 & \textit{if } i = 1, \\ A = \left(\begin{smallmatrix} 1 & b\mu\mathfrak{s} \\ b & 1 \end{smallmatrix}\right) \textit{ and } \alpha = -\frac{1}{2} & \textit{if } i \geq 2, \end{cases}$$
where $\mu \in \{1, \zeta\}$ *and* $b^2\mu\mathfrak{s} = -3$ *so that* $\operatorname{ord}_3(b) = 0$.

In particular, *the classes of* M_h *and* A (*and* B *when* $p \equiv 1 \pmod 3$) *are conjugate in* $\mathrm{PGL}(2, \mathbb{Z}/p^i\mathbb{Z})$.

Proof. By Lemma 5.4, it suffices to observe that the reduction $\bar{A} \in \mathrm{GL}(2, \mathbb{F}_p)$ is nonscalar and that $\operatorname{tr}(\alpha A) = \operatorname{tr}(M_h) = -1$ and $\det(\alpha A) = \det(M_h) = 1$. In the case $p \equiv 1 \pmod 3$, direct calculation shows $A = \beta B$. □

In view of Proposition 5.6, the following can be read from Silberger's tables.

Proposition 5.7. *Suppose* $e = 3$ *and* τ *an irreducible representation of* $\mathrm{PGL}(2, \mathbb{Z}_p)$.

- *If* $\tau = 1$ *or* λ, *then* $\operatorname{tr}\tau(M_h) = 1$.
- *If* $\tau \cong \sigma$ *or* $\sigma \otimes \lambda$, *then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod 3, \\ -1 & \textit{if } p \equiv -1 \pmod 3, \\ 0 & \textit{if } p = 3. \end{cases}$$
- *If* $\tau \cong \sigma_n$ *with* $n \geq 2$, *then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} -1 & \textit{if } p = 3 \textit{ and } n = 2, \\ 0 & \textit{otherwise.} \end{cases}$$
- *If* $\tau \cong u_\alpha$, *where* α *is a character of* $\mathbb{Z}_p^\times$ *of conductor* p^n *and order* $|\alpha| > 2$, *then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} 2 & \textit{if } p \equiv 1 \pmod 3 \textit{ and } 3|\alpha| \mid p^{n-1}(p-1), \\ -1 & \textit{if } p \equiv 1 \pmod 3 \textit{ and } 3|\alpha| \nmid p^{n-1}(p-1), \\ 0 & \textit{otherwise.} \end{cases}$$
- *Let* K *be the unramified quadratic extension of* $\mathbb{Q}_p$, *and let* π *be a character of* $\mathcal{O}_K^\times$ *of order* > 2 *such that* $\pi|\mathbb{Z}_p^\times = 1$. *Furthermore*, *suppose* π *is primitive*

modulo $\mathfrak{p}_K^n$ $(n \geq 1)$. *If* $\tau \cong u_\pi^{\mathrm{unr}}$, *then*

$$\operatorname{tr}\tau(M_h) = \begin{cases} 2(-1)^n & \textit{if } p \equiv -1 \pmod 3 \textit{ and } \pi(1+\sqrt{-3}) = 1, \\ (-1)^{n+1} & \textit{if } p \equiv -1 \pmod 3 \textit{ and } \pi(1+\sqrt{-3}) \neq 1, \\ -1 & \textit{if } p = 3 \textit{ and } n = 1, \\ 0 & \textit{otherwise.} \end{cases}$$

- *Let* K *be a ramified quadratic extension of* $\mathbb{Q}_p$. *Let* π *be a character of* $\mathcal{O}_K^\times$, *primitive modulo* $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, *such that* $\pi|\mathbb{Z}_p^\times = \lambda$. *Suppose* $\tau \cong u_\pi^{\mathrm{ram}}$.
  - *If* $p > 3$, *then* $\operatorname{tr}\tau(M_h) = 0$.
  - *If* $p = 3$, *then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} 2 & \textit{if } K = \mathbb{Q}_3(\sqrt{3}) \textit{ and } n = 2, \\ 0 & \textit{if } K = \mathbb{Q}_3(\sqrt{3}) \textit{ and } n > 2, \\ -1 & \textit{if } K = \mathbb{Q}_3(\sqrt{-3}) \textit{ and } n = 2, \\ \pm 3 & \textit{if } K = \mathbb{Q}_3(\sqrt{-3}) \textit{ and } n > 2. \end{cases}$$
- *If* $\tau \cong u_{\alpha,m}$, $u_{\pi,i}^{\mathrm{unr}}$, *or* $u_{\pi,i}^{\mathrm{ram}}$, *then* $\operatorname{tr}\tau(M_h) = 0$.

Remark. The character table for the representation u_α is the second table on [Silberger 1970, p. 102]. There is an error in the second row of the table, namely $|t - t^{-1}|$ must be replaced by $|t - 1|$.

The case $e = 4$. Let $e = 4$ so that $\rho(h) \in \mathrm{GL}(2, \mathbb{Z}_p)$ is conjugate to the matrix $M_h = M_{h,4} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Let τ be an irreducible (self-dual) representation of $\mathrm{PGL}(2, \mathbb{Z}_p)$ so that τ_v may be viewed as a representation of G'_4. By Table 3, we can write

$$\tau_v \cong 1^{\oplus m_1} \oplus \eta^{\oplus m_2} \oplus \chi_1^{\oplus m_3} \oplus \chi_2^{\oplus m_4} \qquad (m_i \geq 0)$$

and obtain the equations

$$\dim\tau = m_1 + m_2 + m_3 + m_4 \quad \text{and} \quad \operatorname{tr}\tau(M_h) = m_1 + m_2 - m_3 - m_4$$

so that

$$s(4, \tau_v) = m_1 + m_2 = \tfrac{1}{2}\big(\dim\tau + \operatorname{tr}\tau(M_h)\big). \tag{13}$$

Thus, it again suffices to compute the trace $\operatorname{tr}\tau(M_h)$. As with the case $e = 3$, we will rely on Silberger's character tables so that we must first determine the conjugacy class of M_h. The proof of the following proposition is similar to that of Proposition 5.6. Recall that ζ denotes a nonsquare element of $\mathbb{Z}_p^\times$.

Proposition 5.8. *Let* $M_h = M_{h,4} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. *Then* $M_h \sim \alpha A$ *in* $\mathrm{GL}(2, \mathbb{Z}/p^i\mathbb{Z})$ $(i > 0)$, *where* $\alpha \in \mathbb{Z}_p^\times$ *and* $A \in \mathrm{GL}(2, \mathbb{Z}_p)$ *are given as follows*:

- *If* $p \equiv 1 \pmod 4$, *then* $\alpha^2 = -1$ *and* $A = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
- *If* $p \equiv -1 \pmod 4$, *then* $\alpha^2 = (-\zeta)^{-1}$ *and* $A = \left(\begin{smallmatrix} 0 & \zeta \\ 1 & 0 \end{smallmatrix}\right)$.

In particular, the classes of M_h and A are conjugate in $\mathrm{PGL}(2, \mathbb{Z}/p^i\mathbb{Z})$.

Proposition 5.9. *Suppose $e=4$ and τ an irreducible representation of* $\mathrm{PGL}(2, \mathbb{Z}_p)$.

- *If $\tau = 1$ or λ, then* $\operatorname{tr}\tau(M_h) = 1$.
- *If $\tau \cong \sigma$ or $\sigma \otimes \lambda$, then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} 1 & \textit{if } p \equiv \ \ 1 \pmod 4, \\ -1 & \textit{if } p \equiv -1 \pmod 4. \end{cases}$$
- *If $\tau \cong u_\alpha$, then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} \pm 2 & \textit{if } p \equiv \ \ 1 \pmod 4, \\ 0 & \textit{if } p \equiv -1 \pmod 4. \end{cases}$$
- *If $\tau \cong u_\pi^{\mathrm{unr}}$, then*
$$\operatorname{tr}\tau(M_h) = \begin{cases} 0 & \textit{if } p \equiv \ \ 1 \pmod 4, \\ \pm 2 & \textit{if } p \equiv -1 \pmod 4. \end{cases}$$
- *If $\tau \cong \sigma_n$ with $n \geq 2$, $u_{\alpha,m}$, $u_{\pi,i}^{\mathrm{unr}}$, u_π^{ram}, or $u_{\pi,i}^{\mathrm{ram}}$, then* $\operatorname{tr}\tau(M_h) = 0$.

The case $e=6$. Let $e=6$ so that $\rho(h) \in \mathrm{GL}(2, \mathbb{Z}_p)$ is conjugate to the matrix $M_h = M_{h,6} = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Let τ be an irreducible (self-dual) representation of $\mathrm{PGL}(2, \mathbb{Z}_p)$ so that τ_v may be viewed as a representation of G_6'. Thus by Table 7, we may write

$$\tau_v \cong 1^{\oplus m_1} \oplus \ \eta^{\oplus m_2} \oplus \ \psi^{\oplus m_3} \qquad (m_i \geq 0)$$

and obtain the equations $\dim\tau = m_1 + m_2 + 2m_3$ and $\operatorname{tr}\tau(M_h) = m_1 + m_2 - m_3$, so

$$s(6, \tau_v) = m_1 + m_2 = \tfrac{1}{3}\bigl(\dim\tau + 2\operatorname{tr}\tau(M_h)\bigr). \tag{14}$$

So as before, it suffices to compute the trace $\operatorname{tr}\tau(M_h)$. Moreover, with

$$M_{h,3} = \begin{pmatrix} z_3 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad M_{h,6} = \begin{pmatrix} z_6 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},$$

we have $M_{h,3} = -(M_{h,6})^{\mathrm{t}}$. And since every element of $\mathrm{GL}(2, \mathbb{Z}_p)$ is conjugate to its transpose, we conclude that $M_{h,3}$ and $M_{h,6}$ are in the same conjugacy class of $\mathrm{PGL}(2, \mathbb{Z}_p)$. Thus for a representation τ of $\mathrm{PGL}(2, \mathbb{Z}_p)$, the value of $\operatorname{tr}\tau(M_h)$ is the same for the cases $e=3$ and $e=6$.

5E. *Computing $s(e, \tau_v)$ when $\omega_\tau \neq 1$.*

Let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$ with nontrivial central character ω_τ. We recall that $\omega_\tau = \lambda$, the Legendre symbol on $\mathbb{Z}_p^\times$. By Proposition 5.5, we have $\rho(\Phi^2) = (-q)^{-1} \cdot I$ so that

$$\operatorname{tr}\tau(x\Phi^2) = \lambda(-q)\operatorname{tr}\tau(x) \tag{15}$$

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

In the next three propositions, we derive formulas for $s(e, \tau_v)$ when $\omega_\tau \neq 1$ for the individual cases $e = 3$, 4, and 6.

Proposition 5.10. *Suppose $e = 3$, and let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$ with nontrivial central character.*

- *If $\lambda(-q) = 1$, then $s(3, \tau_v) = \frac{1}{3}\big(2 \dim \tau + \operatorname{tr} \tau(M_h)\big)$.*
- *If $\lambda(-q) = -1$, then $s(3, \tau_v) = 0$.*

Proof. If τ is such a representation, then τ_v may be viewed as a representation of G_3. Suppose $\lambda(-q) = 1$. Then $G_3 = G_3'$ so we may proceed as we did when deriving the formula (12) for the case $\omega_\tau = 1$.

Next suppose $\lambda(-q) = -1$. Then using Table 2, we may write

$$\tau_v \cong 1^{\oplus m_1} \oplus \eta^{\oplus m_2} \oplus \chi_1^{\oplus m_3} \oplus \chi_2^{\oplus m_4} \oplus \hat{\sigma}_3^{\oplus m_5} \oplus \psi^{\oplus m_6} \qquad (m_i \geq 0),$$

and thus we get

$$s(3, \tau_v) = m_1 + m_2 + m_5 = \tfrac{1}{6}\big(2 \dim \tau + 2 \operatorname{tr} \tau(\Phi^2) + \operatorname{tr} \tau(h) + \operatorname{tr} \tau(h\Phi^2)\big). \quad (*)$$

Also, (15) gives $\operatorname{tr} \tau(\Phi^2) = -\dim \tau$ and $\operatorname{tr} \tau(h\Phi^2) = -\operatorname{tr} \tau(h)$, since $\lambda(-q) = -1$. Thus $(*)$ becomes $s(3, \tau_v) = 0$ as desired. □

Similarly, the formulas for $s(4, \tau_v)$ and $s(6, \tau_v)$ are obtained using Tables 3–6 and Tables 7–10, respectively, in conjunction with (15).

Proposition 5.11. *Suppose $e = 4$, and let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$ with nontrivial central character.*

- *If $\lambda(-q) = 1$, then $s(4, \tau_v) = \frac{1}{2}\big(\dim \tau + \operatorname{tr} \tau(M_h)\big)$.*
- *If $\lambda(-q) = -1$, then $s(4, \tau_v) = 0$.*

Proposition 5.12. *Suppose $e = 6$, and let τ be an irreducible self-dual representation of $\mathrm{GL}(2, \mathbb{Z}_p)$ with nontrivial central character.*

- *If $\lambda(-q) = 1$, then*

$$s(6, \tau_v) = \begin{cases} \frac{1}{3}\big(\dim \tau + 2 \operatorname{tr} \tau(M_h)\big) & \text{if } p \equiv 1 \pmod 4, \\ \frac{1}{3}\big(\dim \tau + \operatorname{tr} \tau(M_h)\big) & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

- *If $\lambda(-q) = -1$, then $s(6, \tau_v) = 0$.*

Now we compute the trace values $\operatorname{tr} \tau(M_h)$ for $[\tau] \in \mathfrak{T}_n$. First, recall that $\mathfrak{T}_1 = \{[\theta_1]\}$. And note that if $\tau \cong \theta_1$, $\operatorname{tr} \tau(M_h)$ can be computed directly using the formula for the trace of an induced representation.

Proposition 5.13. *Suppose $\tau \cong \theta_1$.*

- *If* $e = 3$, *then*

$$\operatorname{tr}\tau(M_{h,3}) = \begin{cases} 2 & \textit{if } p \equiv 1 \pmod 3, \\ 0 & \textit{if } p \equiv -1 \pmod 3, \\ 1 & \textit{if } p = 3. \end{cases}$$

- *If* $e = 4$, *then*

$$\operatorname{tr}\tau(M_{h,4}) = \begin{cases} 2 & \textit{if } p \equiv 1 \pmod 8, \\ -2 & \textit{if } p \equiv 5 \pmod 8, \\ 0 & \textit{if } p \equiv -1 \pmod 4. \end{cases}$$

- *If* $e = 6$, *then*

$$\operatorname{tr}\tau(M_{h,6}) = \begin{cases} 2 & \textit{if } p \equiv 1 \pmod{12}, \\ -2 & \textit{if } p \equiv 7 \pmod{12}, \\ 0 & \textit{if } p \equiv -1 \pmod 3, \\ -1 & \textit{if } p = 3. \end{cases}$$

For $n \geq 2$, we use the bijection $\varphi_n : \mathfrak{S}'_n \to \mathfrak{T}_n$ from Section 3C in conjunction with the trace values $\operatorname{tr}\tau'(M_h)$ for $[\tau'] \in \mathfrak{S}'_n$, which we have already computed.

Proposition 5.14. *For* $n \geq 2$, *let* $[\tau'] \in \mathfrak{S}'_n$ *and* $[\tau] = \varphi_n([\tau']) \in \mathfrak{T}_n$. *If* $e = 4$ *or* $p > 3$, *then* $\operatorname{tr}\tau(M_{h,e}) = 0$. *If* $p = 3$, *then*

- $\operatorname{tr}\tau(M_{h,3}) = \operatorname{tr}\tau'(M_{h,3})$;
- $\operatorname{tr}\tau(M_{h,6}) = -\operatorname{tr}\tau(M_{h,3})$.

Proof. If $e = 4$ or $p > 3$, then Propositions 5.7 and 5.9 show that $\operatorname{tr}\tau'(M_{h,e}) = 0$ and hence $\operatorname{tr}\tau(M_{h,e}) = 0$, also. Now suppose $p = 3$. Then by Proposition 5.6,

$$M_{h,3} \sim \alpha A \quad \text{in } \mathrm{GL}(2, \mathbb{Z}/3^n\mathbb{Z})$$

with $\alpha = -\frac{1}{2}$ and $A \in \mathrm{Silb}^n$. And since $-\frac{1}{2}$ is a square in $(\mathbb{Z}/3^n\mathbb{Z})^\times$, we get $M_{h,3} \sim A$ in K_n and hence $\operatorname{tr}\tau(M_{h,3}) = \operatorname{tr}\tau'(M_{h,3})$. Finally, we have seen that $M_{h,6} \sim -1 \cdot M_{h,3}$, where the conjugation occurs in $\mathrm{GL}(2, \mathbb{Z}_p)$. And since -1 is a nonsquare element of $\mathbb{Z}_p^\times$ when $p = 3$, we have $\operatorname{tr}\tau(M_{h,6}) = -\operatorname{tr}\tau(M_{h,3})$ as desired. □

5F. ***Summary of results.*** In the following theorem, we combine the results of the previous sections to compute $s(e, \tau_v)$ in the cases $e = 3$, 4, and 6.

Theorem 5.15. *Let* τ *be an irreducible self-dual representation of* $\mathrm{GL}(2, \mathbb{Z}_p)$.

- *If* $\tau = 1$ *or* $\tau = \lambda$, *then* $s(e, \tau_v) = 1$.
- *If* $\tau \cong \sigma$ *or* $\tau \cong \sigma \otimes \lambda$, *then*

$$s(e, \tau_v) \equiv \begin{cases} 0 \pmod 2 & \textit{if } e = 3 \textit{ and } p = 3, \\ 1 \pmod 2 & \textit{otherwise}. \end{cases}$$

- *If $\tau \cong \sigma_n$ with $n \geq 2$, then*
$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \textit{if } e = 3,\ p = 3, \textit{ and } n = 2, \\ 0 \pmod 2 & \textit{otherwise.} \end{cases}$$
- *If $\tau \cong u_\alpha$, where α is primitive modulo p^n $(n \geq 1)$, then*
$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \textit{if } e = 3,\ p \equiv 1 \pmod 3, \textit{ and } 3|\alpha| \nmid p^{n-1}(p-1), \\ 0 \pmod 2 & \textit{otherwise.} \end{cases}$$
- *If $\tau \cong u_\pi^{\mathrm{unr}}$, where π is primitive modulo $\mathfrak{p}_K^n$ $(n \geq 1)$, then*
$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \textit{if } e = 3,\ p \equiv -1 \pmod 3, \textit{ and } \pi(1+\sqrt{-3}) \neq 1, \\ 1 \pmod 2 & \textit{if } e = 3,\ p = 3, \textit{ and } n = 1, \\ 0 \pmod 2 & \textit{otherwise.} \end{cases}$$
- *If $\tau \cong u_\pi^{\mathrm{ram}}$, where π is primitive modulo $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, then*
$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \textit{if } e = 3,\ p = 3, \textit{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \textit{otherwise.} \end{cases}$$
- *If $[\tau] = \varphi_n([u_\pi^{\mathrm{ram}}])$, where π is primitive modulo $\mathfrak{p}_K^{2n-1}$ $(n \geq 2)$, then*
$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \textit{if } 3 \mid e,\ p = 3, \textit{ and } K = \mathbb{Q}_3(\sqrt{-3}), \\ 0 \pmod 2 & \textit{otherwise.} \end{cases}$$
- *If $\tau \cong \theta_n$ with $n \geq 1$, then*
$$s(e, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \textit{if } 3 \mid e,\ p = 3, \textit{ and } 1 \leq n \leq 2, \\ 0 \pmod 2 & \textit{otherwise.} \end{cases}$$

In all other cases, $s(e, \tau_v) \equiv 0 \pmod 2$.

Proof. If $[\tau] \in \mathfrak{T}_n'$, we compute $s(e, \tau_v)$ by substituting the trace $\operatorname{tr}\tau(M_h)$ from Propositions 5.7 and 5.9 and the dimension $\dim\tau$ from Silberger's tables into Equations (12)–(14). For $[\tau] \in \mathfrak{T}_n$, we substitute $\operatorname{tr}\tau(M_h)$ from Propositions 5.13 and 5.14 and $\dim\tau$ into the formulas for $s(e, \tau_v)$ given in Propositions 5.10–5.12. Note that $\dim\theta_1 = p+1$ and $\dim\tau = p^{n-2}(p^2-1)$ for all $[\tau] \in \mathfrak{T}_n$ with $n \geq 2$. □

6. Proof of the main theorem

We now return to our initial setting. Hence F is a number field and E/F is an elliptic curve semistable at primes of F above 2 and 3. If v is a finite place of F, where E has bad reduction, then $v \nmid p$. If $v(j(E)) < 0$, then $p \nmid v(j(E))$. We also assume that the natural embedding $\mathrm{Gal}(F^\infty/F) \hookrightarrow \mathrm{Aut}(T_p(E))$ is surjective, which allows us to identify $\mathrm{Gal}(F^\infty/F)$ with $\mathrm{GL}(2, \mathbb{Z}_p)$.

Given a finite place v of F such that $v(j(E)) < 0$, let $\mathcal{E}_v$ denote the Tate curve over F_v with $j(\mathcal{E}_v) = j(E)$. Then there exists a unique real-valued character

χ_v of $\mathrm{Gal}(\bar{F}_v/F_v)$ such that E is isomorphic over F_v to the twist of $\mathcal{E}_v$ by χ_v. Furthermore, $\chi_v = 1$, χ_v is the unramified quadratic character of $\mathrm{Gal}(\bar{F}_v/F_v)$, or χ_v is a ramified quadratic character of $\mathrm{Gal}(\bar{F}_v/F_v)$ according as E/F_v has split multiplicative reduction, nonsplit multiplicative reduction, or additive reduction, respectively. In all cases, χ_v factors through $\mathrm{Gal}(F_v^\infty/F_v)$.

Recall that τ is an irreducible self-dual representation of $\mathrm{Gal}(F^\infty/F)$, and for each place v of F, we let τ_v be the restriction of τ to the decomposition subgroup $\mathrm{Gal}(F_v^\infty/F_v)$. Given a finite place v such that $v(j(E)) \geq 0$, we define the local factor $\gamma(E/F_v, \tau_v)$ as follows. If E has good reduction at v, put $\gamma(E/F_v, \tau_v) = 1$. Otherwise, E has bad but potentially good reduction at v (i.e., $v \in T^+$), and $v \mid \ell$, where $5 \leq \ell < \infty$ and $\ell \neq p$. Let Δ_v denote the discriminant associated to a minimal Weierstrass equation for E over F_v, and as in (2) put

$$e_v = \frac{12}{\gcd(v(\Delta_v), 12)} \ (= 2, 3, 4, \text{ or } 6).$$

Let

$$\epsilon_v = \begin{cases} 1 & \text{if } f(F_v/\mathbb{Q}_\ell) \text{ is even,} \\ -1/\ell & \text{if } f(F_v/\mathbb{Q}_\ell) \text{ is odd and } e_v = 2 \text{ or } 6, \\ -3/\ell & \text{if } f(F_v/\mathbb{Q}_\ell) \text{ is odd and } e_v = 3, \\ -2/\ell & \text{if } f(F_v/\mathbb{Q}_\ell) \text{ is odd and } e_v = 4. \end{cases}$$

We then define

$$\gamma(E/F_v, \tau_v) = \\ \begin{cases} \epsilon_v^{\dim \tau} & \text{if } m_v \equiv 1 \pmod{e_v}, \\ (-\epsilon_v)^{\dim \tau} (-1)^{s(e_v, \tau_v)} & \text{if } e_v = 3, 4, \text{ or } 6 \text{ and } m_v \equiv -1 \pmod{e_v}, \end{cases} \tag{16}$$

where we recall that m_v denotes the order of the residue class field of v and that

$$s(e_v, \tau_v) = \langle 1, \tau_v \rangle + \langle \eta, \tau_v \rangle + \langle \hat{\sigma}_{e_v}, \tau_v \rangle.$$

Remark. Recall the following subsets of T^+:

$$\begin{aligned} T_2^+ &= \{v \in T^+ : e_v = 2 \text{ or } 6, \text{ and } m_v \equiv -1 \pmod 4\}, \\ T_3^+ &= \{v \in T^+ : e_v = 3 \text{ and } m_v \equiv -1 \pmod 3\}, \\ T_4^+ &= \{v \in T^+ : e_v = 4, \text{ and } m_v \equiv 5 \text{ or } 7 \pmod 8\}. \end{aligned}$$

Their union constitutes the set of elements $v \in T^+$ for which $\epsilon_v = -1$. We also recall that $t_{2,4}^+$ and t_3^+ denote the cardinalities of $T_2^+ \cup T_4^+$ and T_3^+, respectively.

Given the above notations, we define the root number $W(E, \tau)$ by

$$W(E, \tau) = \prod_v W(E/F_v, \tau_v),$$

where the local factors are given by the following [Rohrlich 1996, pp. 329–330, Theorem 2; p. 332, Proposition 8]:

- If $v \mid \infty$ (that is, if v is an infinite place), then
$$W(E/F_v, \tau_v) = (-1)^{\dim \tau}.$$
- Suppose $v \mid \ell$ with $\ell = 2$ or 3.
  (a) If $v(j(E)) \geq 0$ (good reduction), then
$$W(E/F_v, \tau_v) = \det \tau_v(-1).$$
  Here, we view the one dimensional character $\det \tau_v$ of $\mathrm{Gal}(F_v^\infty/F_v)$ as a character of $F_v^\times$ via the Artin map (6).
  (b) If $v(j(E)) < 0$ (i.e., multiplicative reduction), then
$$W(E/F_v, \tau_v) = \det \tau_v(-1) \cdot (-1)^{\langle \chi_v, \tau_v \rangle}.$$
- Suppose $v \mid \ell$ with $5 \leq \ell < \infty$.
  (a) If $v(j(E)) \geq 0$, then
$$W(E/F_v, \tau_v) = \det \tau_v(-1) \cdot \gamma(E/F_v, \tau_v).$$
  Note that $\gamma(E/F_v, \tau_v) = 1$ if E has good reduction at v.
  (b) If $v(j(E)) < 0$, then
$$W(E/F_v, \tau_v) = \det \tau_v(-1) \cdot (-1)^{\langle \chi_v, \tau_v \rangle} \cdot \chi_v(-1)^{\dim \tau}.$$
  Note that $\chi_v(-1) = 1$ if E has multiplicative reduction at v.

Therefore, we obtain

$$\begin{aligned} W(E, \tau) = \ & (-1)^{(r_1+r_2)\dim \tau} \cdot \prod_{v \nmid \infty} \det \tau_v(-1) \cdot \prod_{\substack{v \nmid \infty \\ v(j(E))<0}} (-1)^{\langle \chi_v, \tau_v \rangle} \\ & \cdot \prod_{v \in T^+} \gamma(E/F_v, \tau_v) \cdot \prod_{v \in T^-} \chi_v(-1)^{\dim \tau}. \end{aligned} \tag{17}$$

As in [Rohrlich 2006, pp. 372–373], we can replace the second factor by $\det \tau(c)^{r_1}$, where c is any element of $\mathrm{GL}(2, \mathbb{Z}_p)$ satisfying $c^2 = 1$ and $\det(c) = -1$. Moreover, we have

$$\prod_{\substack{v \nmid \infty \\ v(j(E))<0}} (-1)^{\langle \chi_v, \tau_v \rangle} = (-1)^{\Sigma + \Sigma' + \Sigma''} \cdot \prod_{v \in T^-} (-1)^{\langle \chi_v, \tau_v \rangle},$$

where Σ, Σ', and Σ'' are as defined in [Rohrlich 2006, p. 375]. Therefore, (17) becomes

$$W(E, \tau) = W_1(E, \tau) \cdot W_2(E, \tau), \tag{18}$$

where

$$W_1(E,\tau)=(-1)^{(r_1+r_2)\dim\tau}\cdot\det\tau(c)^{r_1}\cdot(-1)^{\Sigma+\Sigma'+\Sigma''}$$

and

$$W_2(E,\tau)=\prod_{v\in T^-}(-1)^{\langle\chi_v,\tau_v\rangle}\cdot\prod_{v\in T^-}\chi_v(-1)^{\dim\tau}\cdot\prod_{v\in T^+}\gamma(E/F_v,\tau_v). \tag{19}$$

The term $W_1(E,\tau)$ was computed by [Rohrlich 2006, p. 362, Theorem 1]. We recall his result in the following theorem.

Theorem 6.1 (Rohrlich). *Let τ be an irreducible self-dual representation of*

$$\mathrm{Gal}(F^\infty/F)$$

and let w_1 be the integer modulo 2 such that

$$W_1(E,\tau)=(-1)^{w_1}. \tag{20}$$

- *If $\tau=1$, then $w_1=r_1+r_2+s \pmod 2$.*
- *If $\tau=\lambda$, then $w_1=r_1(p+1)/2+r_2+s_{\mathrm{qr}}+u \pmod 2$.*
- *If $\tau\cong\sigma$, then $w_1=r_1(p+1)/2+r_2+s \pmod 2$.*
- *If $\tau\cong\sigma\otimes\lambda$, then $w_1=r_1+r_2+s_{\mathrm{qr}}+u \pmod 2$.*
- *If $\tau\cong\sigma_n$ with $n\geq 2$ or $\tau\cong\theta_n$ with $n\geq 1$, then $w_1=s_{\mathrm{nr}}+u \pmod 2$.*
- *If $\tau\cong u_\alpha$ or $\tau\cong u_\pi^{\mathrm{unr}}$, then $w_1=r_1(p-1)/2 \pmod 2$.*

In all other cases, $w_1=0 \pmod 2$ so that $W_1(E,\tau)=1$.

In the next two propositions, we recall that t_3^- and t_{nr}^- denote the number of places $v\in T^-$ such that $m_v\equiv 3 \pmod 4$ and m_v is a quadratic nonresidue modulo p, respectively.

Proposition 6.2. *Let τ be an irreducible self-dual representation of* $\mathrm{Gal}(F^\infty/F)$ *and let w_2 be the integer modulo 2 such that*

$$\prod_{v\in T^-}(-1)^{\langle\chi_v,\tau_v\rangle}=(-1)^{w_2}. \tag{21}$$

Then

$$w_2=\begin{cases} t_{\mathrm{nr}}^-(p-1)/2 \pmod 2 & \textit{if } \tau\cong\theta_n \textit{ with } n\geq 1,\\ 0 \pmod 2 & \textit{otherwise}.\end{cases}$$

Proof. We adapt the approach taken in [Rohrlich 2006, pp. 373–375] to the case $v\in T^-$. Thus let $v\in T^-$ and consider the action of $\mathrm{Gal}(\bar F_v/F_v)$ on $T_p(E)$ and $T_p(\mathcal{E}_v)$. We shall regard this action as given by maps

$$\alpha_v:\mathrm{Gal}(\bar F_v/F_v)\to\mathrm{GL}(2,\mathbb{Z}_p)\quad\text{and}\quad\beta_v:\mathrm{Gal}(\bar F_v/F_v)\to\mathrm{GL}(2,\mathbb{Z}_p),$$

respectively, where the implicit choice of bases for the two Tate modules is made as follows. For α_v, we will use the composition of the restriction $\mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{Gal}(F_v^\infty/F_v)$, the inclusion $\mathrm{Gal}(F_v^\infty/F_v) \subset \mathrm{Gal}(F^\infty/F)$, and the isomorphism $\mathrm{Gal}(F^\infty/F) \cong \mathrm{GL}(2, \mathbb{Z}_p)$. And by the theory of Tate curves, we may choose β_v to have the form

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

where $\kappa_v : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathbb{Z}_p^\times$ is the p-adic cyclotomic character.

Since $v \nmid p$, the image of κ_v is the open subgroup $U_v \subset \mathbb{Z}_p^\times$ topologically generated by m_v. Furthermore, the assumption $p \nmid v(j(E))$ implies that the image of β_v is

$$J_v = \left\{ b(u, z) = \begin{pmatrix} u & z \\ 0 & 1 \end{pmatrix} : u \in U_v, z \in \mathbb{Z}_p \right\}.$$

Observe that the fixed fields of the kernels of χ_v and κ_v are linearly disjoint over F_v, because one is totally ramified over F_v while the other is unramified. Thus the image of $\chi_v\beta_v$ is $J_v'' = \{\pm I\} J_v$. And since the maps α_v and $\chi_v\beta_v$ are conjugate, we get

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

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

Put $G = \mathrm{GL}(2, \mathbb{Z}_p)$ and choose $n \geq 1$ such that $1 + p^n \in U_v$ and τ factors through $G/K(n)$. Arguing as in [Rohrlich 2006, pp. 374–375], we get

$$\langle \chi_v, \tau_v \rangle = \langle \mathrm{ind}_{J_v''(n)}^G \eta_v'', \tau \rangle, \tag{$*$}$$

where η_v'' is the quadratic character of Proposition 4.1 with $m = m_v$.

Using ($*$), Proposition 4.1, and the definition of t_{nr}^-, we obtain the desired result. □

Proposition 6.3. *Let τ be an irreducible self-dual representation of* $\mathrm{Gal}(F^\infty/F)$ *and let w_2' be the integer modulo* 2 *such that*

$$\prod_{v \in T^-} \chi_v(-1)^{\dim \tau} = (-1)^{w_2'}. \tag{22}$$

Then

$$w_2' = \begin{cases} t_3^- \pmod 2 & \textit{if } \dim \tau \textit{ is odd}, \\ 0 \pmod 2 & \textit{if } \dim \tau \textit{ is even}. \end{cases}$$

Proof. Let $v \in T^-$ so that χ_v is a ramified quadratic character of $\mathrm{Gal}(\bar{F}_v/F_v)$. We have

$$\chi_v(-1) = \begin{cases} 1 & \text{if } m_v \equiv 1 \pmod 4, \\ -1 & \text{if } m_v \equiv 3 \pmod 4, \end{cases}$$

and thus the result follows. □

Remark. Up to isomorphism, the only irreducible self-dual representations of $\mathrm{GL}(2,\mathbb{Z}_p)$ with odd dimension are 1, λ, σ, and $\sigma\otimes\lambda$ [Rohrlich 2006, p. 366, Proposition 3].

Theorem 6.4. *Let τ be an irreducible self-dual representation of* $\mathrm{Gal}(F^\infty/F)$ *and let w_2'' be the integer modulo* 2 *such that*

$$\prod_{v\in T^+}\gamma(E/F_v,\tau_v)=(-1)^{w_2''}. \tag{23}$$

- *If $\tau=1$ or $\tau=\lambda$, then* $w_2''=t_{2,4}^+ + t_3^+ \pmod 2$.
- *If $\tau\cong\sigma$ or $\tau\cong\sigma\otimes\lambda$, then*

$$w_2''=\begin{cases} t_{2,4}^+ + t_3^+ \pmod 2 & \textit{if } p>3,\\ t_{2,4}^+ \pmod 2 & \textit{if } p=3.\end{cases}$$

- *If $\tau\cong\sigma_n$ with $n\ge 2$, then*

$$w_2''=\begin{cases} t_3^+ \pmod 2 & \textit{if } p=3 \textit{ and } n=2,\\ 0 \pmod 2 & \textit{otherwise.}\end{cases}$$

- *If $\tau\cong u_\alpha$, where α is primitive modulo p^n $(n\ge 1)$, then*

$$w_2''=\begin{cases} t_3^+ \pmod 2 & \textit{if } p\equiv 1 \pmod 3 \textit{ and } \; 3|\alpha|\nmid p^{n-1}(p-1),\\ 0 \pmod 2 & \textit{otherwise.}\end{cases}$$

- *If $\tau\cong u_\pi^{\mathrm{unr}}$, where π is primitive modulo $\mathfrak{p}_K^n$ $(n\ge 1)$, then*

$$w_2''=\begin{cases} t_3^+ \pmod 2 & \textit{if } p\equiv -1 \pmod 3 \textit{ and } \pi(1+\sqrt{-3})\ne 1,\\ t_3^+ \pmod 2 & \textit{if } p=3 \textit{ and } n=1,\\ 0 \pmod 2 & \textit{otherwise.}\end{cases}$$

- *If $\tau\cong u_\pi^{\mathrm{ram}}$, where π is primitive modulo $\mathfrak{p}_K^{2n-1}$ $(n\ge 2)$, then*

$$w_2''=\begin{cases} t_3^+ \pmod 2 & \textit{if } p=3 \textit{ and } K=\mathbb{Q}_3(\sqrt{-3}),\\ 0 \pmod 2 & \textit{otherwise.}\end{cases}$$

- *If $[\tau]=\varphi_n([u_\pi^{\mathrm{ram}}])$, where π is primitive modulo $\mathfrak{p}_K^{2n-1}$ $(n\ge 2)$, then*

$$w_2''=\begin{cases} t_3^+ + t_6^+ \pmod 2 & \textit{if } p=3 \textit{ and } K=\mathbb{Q}_3(\sqrt{-3}),\\ 0 \pmod 2 & \textit{otherwise.}\end{cases}$$

- *If $\tau\cong\theta_n$ with $n\ge 1$, then*

$$w_2''=\begin{cases} t_3^+ + t_6^+ \pmod 2 & \textit{if } p=3 \textit{ and } 1\le n\le 2,\\ 0 \pmod 2 & \textit{otherwise.}\end{cases}$$

In all other cases, $w_2''=0 \pmod 2$.

Proof. Throughout the proof, we assume $v \in T^+$. And whenever $s(e_v, \tau_v)$ is mentioned, we implicitly assume that $e_v = 3$, 4, or 6 and $m_v \equiv -1 \pmod{e_v}$.

Suppose $\tau = 1$, $\tau = \lambda$, $\tau \cong \sigma$ with $p > 3$, or $\tau \cong \sigma \otimes \lambda$ with $p > 3$. Then Theorem 5.15 shows that $s(e_v, \tau_v) \equiv 1 \pmod 2$. Thus, (16) gives $\gamma(E/F_v, \tau_v) = \epsilon_v$ in both cases: (i) $m_v \equiv 1 \pmod{e_v}$ and (ii) $e_v = 3$, 4, or 6 and $m_v \equiv -1 \pmod{e_v}$. And therefore $w_2'' = t_{2,4}^+ + t_3^+ \pmod 2$.

Now suppose $\tau \cong \sigma$ or $\sigma \otimes \lambda$ with $p = 3$. Then Theorem 5.15 shows

$$s(e_v, \tau_v) \equiv \begin{cases} 0 \pmod 2 & \text{if } e_v = 3, \\ 1 \pmod 2 & \text{if } e_v = 4 \text{ or } 6. \end{cases}$$

Therefore, (16) implies

$$\gamma(E/F_v, \tau_v) = \begin{cases} -\epsilon_v & \text{if } v \in T_3^+, \\ \epsilon_v & \text{otherwise,} \end{cases}$$

and thus we get $w_2'' = t_{2,4}^+ \pmod 2$.

Before proceeding, we remark that the remaining representations all have even dimension. And for such representations, (16) simplifies to

$$\gamma(E/F_v, \tau_v) = \begin{cases} 1 & \text{if } m_v \equiv 1 \pmod{e_v}, \\ (-1)^{s(e_v, \tau_v)} & \text{if } e_v = 3, 4, \text{ or } 6 \text{ and } m_v \equiv -1 \pmod{e_v}. \end{cases} \tag{$*$}$$

Suppose $\tau \cong \sigma_n$ with $n \geq 2$. We have by Theorem 5.15

$$s(e_v, \tau_v) \equiv \begin{cases} 1 \pmod 2 & \text{if } e_v = 3,\ p = 3, \text{ and } n = 2, \\ 0 \pmod 2 & \text{otherwise,} \end{cases}$$

so that $(*)$ gives the following:

- If $p = 3$ and $n = 2$, then

$$\gamma(E/F_v, \tau_v) = \begin{cases} -1 & \text{if } v \in T_3^+, \\ 1 & \text{otherwise} \end{cases}$$

  so that $w_2'' = t_3^+ \pmod 2$.
- Otherwise, $\gamma(E/F_v, \tau_v) = 1$ and so $w_2'' = 0 \pmod 2$.

The cases $\tau \cong u_\alpha$, $\tau \cong u_\pi^{\text{unr}}$, $\tau \cong u_\pi^{\text{ram}}$, $[\tau] = \varphi_n([u_\pi^{\text{ram}}])$, and $\tau \cong \theta_n$ follow similarly. And in all other cases, Theorem 5.15 gives $s(e_v, \tau_v) \equiv 0 \pmod 2$ so that $(*)$ implies $\gamma(E/F_v, \tau_v) = 1$ and hence $w_2'' = 0 \pmod 2$. □

Substituting (21), (22), and (23) into (19) yields

$$W_2(E, \tau) = (-1)^{w_2 + w_2' + w_2''}, \tag{24}$$

and then substituting (20) and (24) into (18) gives

$$W(E, \tau) = (-1)^{w_1 + w_2 + w_2' + w_2''}.$$

Theorem 2.1 now follows from combining the values of w_1 (Theorem 6.1), w_2 (Proposition 6.2), w_2' (Proposition 6.3), and w_2'' (Theorem 6.4).

Acknowledgments

This paper is based on the author's Ph.D. thesis at Boston University. He thanks his advisor, David E. Rohrlich, for his generous mentoring, guidance, and support over the years.

References

[Lang 2002] S. Lang, *Algebra*, 3rd ed., Grad. Texts in Math. **211**, Springer, New York, 2002. MR 2003e:00003 Zbl 0984.00001

[Rohrlich 1990] D. E. Rohrlich, "The vanishing of certain Rankin–Selberg convolutions", pp. 123–133 in *Automorphic forms and analytic number theory* (Montréal, 1989), edited by M. Ram Murty, Univ. Montréal, Montreal, QC, 1990. MR 92d:11051 Zbl 0737.11014

[Rohrlich 1994] D. E. Rohrlich, "Elliptic curves and the Weil–Deligne group", pp. 125–157 in *Elliptic curves and related topics*, edited by H. Kisilevsky and M. Ram Murty, CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence, RI, 1994. MR 95a:11054 Zbl 0852.14008

[Rohrlich 1996] D. E. Rohrlich, "Galois theory, elliptic curves, and root numbers", *Compositio Math.* **100**:3 (1996), 311–349. MR 97m:11075 Zbl 0860.11033

[Rohrlich 2006] D. E. Rohrlich, "Root numbers of semistable elliptic curves in division towers", *Math. Res. Lett.* **13**:2-3 (2006), 359–376. MR 2007c:11072 Zbl 1124.11026

[Rohrlich 2008] D. E. Rohrlich, "Scarcity and abundance of trivial zeros in division towers", *J. Algebraic Geom.* **17**:4 (2008), 643–675. MR 2009e:14039 Zbl 05352807

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Serre 1977] J.-P. Serre, *Linear representations of finite groups*, Grad. Texts in Math. **42**, Springer, New York, 1977. MR 56 #8675 Zbl 0355.20006

[Silberger 1970] A. J. Silberger, PGL_2 *over the p-adics: its representations, spherical functions, and Fourier analysis*, Lecture Notes in Math. **166**, Springer, Berlin, 1970. MR 44 #2891 Zbl 0204.44102

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

Communicated by Karl Rubin
Received 2009-01-15 Revised 2009-11-28 Accepted 2009-11-29

matsuura@math.bu.edu *School of Education, Boston University, Two Silber Way, Boston, MA 02215, United States*