Can. J. Math. Vol. **49** (4), 1997 pp. 749–771.

# TWISTED HASSE-WEIL $L$-FUNCTIONS AND THE RANK OF MORDELL-WEIL GROUPS

LAWRENCE HOWE

ABSTRACT. Following a method outlined by Greenberg, root number computations give a conjectural lower bound for the ranks of certain Mordell-Weil groups of elliptic curves. More specifically, for $\mathrm{PQ}_n$ a $\mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$-extension of $\mathbf{Q}$ and $E$ an elliptic curve over $\mathbf{Q}$, define the motive $E \otimes \rho$, where $\rho$ is any irreducible representation of $\mathrm{Gal}(\mathrm{PQ}_n/\mathbf{Q})$. Under some restrictions, the root number in the conjectural functional equation for the $L$-function of $E \otimes \rho$ is easily computable, and a '$-1$' implies, by the Birch and Swinnerton-Dyer conjecture, that $\rho$ is found in $E(\mathrm{PQ}_n) \otimes \mathbf{C}$. Summing the dimensions of such $\rho$ gives a conjectural lower bound of

$$p^{2n} - p^{2n-1} - p - 1$$

for the rank of $E(\mathrm{PQ}_n)$.

**Introduction.** In [3], Greenberg outlines a method for using root number calculations to give lower bounds for the ranks of Mordell-Weil groups of elliptic curves in certain $\mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$-extensions of $\mathbf{Q}$. This paper pursues those calculations using Silberger's work ([9]) on representations of $\mathrm{PGL}_2(\mathbf{Z}_p)$.

To recall Greenberg's method, let $E$ be an elliptic curve over $\mathbf{Q}$ with conductor $N_E$. Let $p$ be an odd prime, and let $\mathrm{PQ}_n$ be a $\mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$-extension of $\mathbf{Q}$, for some $n$. We assume that no prime factor of $N_E$ ramifies in $\mathrm{PQ}_n$. Such $\mathrm{PQ}_n$ may be constructed by taking an auxiliary elliptic curve $E'$ over $\mathbf{Q}$ without complex multiplication, and whose conductor is coprime with $N_E$. For all but finitely many $p$, the $p$-power division points of $E'$ generate a $\mathrm{GL}_2(\mathbf{Z}_p)$-extension of $\mathbf{Q}$. The fixed field of the centre is thus a $\mathrm{PGL}_2(\mathbf{Z}_p)$-extension PQ of $\mathbf{Q}$. We may then choose $p$ so that no prime in $N_E$ ramifies in PQ. The field $\mathrm{PQ}_n$ appears as the fixed field of the kernel of the reduction map $\mathrm{PGL}_2(\mathbf{Z}_p) \longrightarrow \mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$.

Let $\rho$ be an even dimensional irreducible representation of $\mathrm{Gal}(\mathrm{PQ}_n/\mathbf{Q})$. By twisting the $L$-function of $E$ by $\rho$ a motivic $L$-function is obtained whose associated conjectural functional equation has an $\varepsilon$-factor computable solely in terms of properties of $\rho$ (See Theorem 1 below). Since any complex representation of $\mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$ is isomorphic to its contragredient, the functional equation for the $L$-function with $\Gamma$-factor has the form

$$\Lambda(E \otimes \rho, s) = \varepsilon(E \otimes \rho, s)\Lambda(E \otimes \rho, 2 - s),$$

which makes $\varepsilon(E \otimes \rho, 1) = \pm 1$. The generalized Birch and Swinnerton-Dyer conjecture implies that the order of vanishing at $s = 1$ of the twisted $L$-function is precisely the multiplicity of $\rho$ in $E(\mathrm{PQ}_n) \otimes \mathbf{C}$. Thus, for a particular $\rho$, if $\varepsilon(E \otimes \rho, 1) = -1$, then

Received by the editors August 24, 1995; revised August 1, 1996.
AMS subject classification: 11G05, 14G10.

$\Lambda(E \otimes \rho, 1)$ vanishes. This implies that $\rho$ occurs in $E(\mathrm{PQ}_n) \otimes \mathbf{C}$. Summing the dimensions of all $\rho$ having $\varepsilon(E \otimes \rho, 1) = -1$ gives a lower bound for the rank of $E(\mathrm{PQ}_n)$.

The first two sections fill out the sketch provided above. Section 1 reviews the background of motivic $L$-functions. Section 2 contains a derivation of the conjectural root number formula (Theorem 1)

$$\varepsilon(E \otimes \rho, 1) = (-1)^{d_\rho} \det \rho(N_E),$$

where $\rho$ is an even dimensional irreducible representation of $\mathrm{Gal}(\mathrm{PQ}_n / \mathbf{Q})$ and $d_\rho$ is the dimension of the $(-1)$-eigenspace of complex conjugation under $\rho$. This formula is decades old: in [11], Weil attributes it to Langlands. However, here it is explicitly derived from certain conjectures about motivic $L$-functions. Computing the terms in this formula for the various $\rho$ is done in Section 3, using the catalog of all complex representations of $\mathrm{PGL}_2(\mathbf{Z}_p)$ found in [9].

Applying the results of the computations to obtain a lower bound for the rank of $E(\mathrm{PQ}_n)$ gives the following theorem:

THEOREM 3. *Let $E$ be an elliptic curve defined over $\mathbf{Q}$ with conductor $N_E$, and let $\mathrm{PQ}_n$ be a $\mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$-extension of $\mathbf{Q}$. Suppose that no prime in $N_E$ ramifies in $\mathrm{PQ}_n$ and that $-N_E$ is a quadratic nonresidue modulo $p$. Then,*

$$\mathrm{rank}\big(E(\mathrm{PQ}_n)\big) \geq p^{2n} - p^{2n-1} - p - 1.$$

I would like to thank Michael Harris, Ralph Greenberg, David Rohrlich, and Glenn Stevens for their generous guidance, and the referees for their valuable suggestions and corrections.

Throughout, $\mathrm{PQ}_n$ will be the $\mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$-extension of $\mathbf{Q}$ described above.

## 1. Twisted Hasse-Weil $L$-functions.

Let $E$ is an elliptic curve defined over $\mathbf{Q}$ with conductor $N_E$ and let $\rho$ be an irreducible complex representation of $\mathrm{Gal}(\mathrm{PQ}_n / \mathbf{Q})$ realizable over some number field $K$. The tensor product $E \otimes \rho$ gives a motive with coefficients in $K$. To make the calculations straightforward, we shall assume that no prime in $N_E$ ramifies in $\mathrm{PQ}_n$, so that by the conductor-discriminant product formula ([7], p. 104), $N_E$ is coprime to the conductor of any irreducible representation $\rho$ of $\mathrm{Gal}(\mathrm{PQ}_n / \mathbf{Q})$.

### 1.1. *Motivic L-functions.*

We recall the definition of the $L$-function attached to a motive $M$. For each prime number $p$, let $W_{\mathbf{Q}_p}$ be a Weil group for $\bar{\mathbf{Q}}_p$ over $\mathbf{Q}_p$, where $\bar{\mathbf{Q}}_p$ denotes an algebraic closure of $\mathbf{Q}_p$. We follow Deligne's convention that under the reciprocity law isomorphism,

$$\mathbf{Q}_p^\times \xrightarrow{\sim} W_{\mathbf{Q}_p}^{ab},$$

a uniformizer corresponds to a *geometric* Frobenius element, *i.e.*, one which acts as $x \mapsto x^{p^{-1}}$ on $\bar{\mathbf{F}}_p / \mathbf{F}_p$. We shall always use $\Phi$ to denote a geometric Frobenius element and $I$ to denote the inertia group in $W_{\mathbf{Q}_p}$. Now let $H_\lambda(M)$ be the $\lambda$-adic realization of $M$, where $\lambda$ is a prime of the coefficient field not over $p$. We then set

$$Z_p(M, t) = \det(1 - \Phi t \mid H_\lambda(M)^I)^{-1}, \tag{1}$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

where the superscript $I$ denotes the subspace of inertial invariants. In our case, $Z_p(M,t)$ will always be a polynomial in $t$ with coefficients in the coefficient field of $M$, independent of the choice of $\lambda$.

Setting $L_p(M,s) = Z_p(M,p^{-s})$, define the *L-function* of $M$ to be

$$L(M,s) = \prod_p L_p(M,s), \tag{2}$$

which converges for the real part of $s$ sufficiently large.

The $\Gamma$-factor at infinity $L_\infty(M,s)$ is completely determined by the Hodge decomposition of the 'Betti' realization of $M$. A table of the possibilities is given in [2], Section 5.3. Setting $\Lambda(M,s) = L_\infty(M,s)L(M,s)$, the conjectural functional equation reads

$$\Lambda(M,s) = \varepsilon(M,s)\Lambda(\check{M},1-s), \tag{3}$$

where $\check{M}$ is the dual motive of $M$, and where $\varepsilon(M,s)$, as a function of $s$, is the product of a constant and an exponential function.

1.2. *Three L-functions.*

1. For $M = E$, $L(E,s)$ is the *Hasse-Weil L-function*. In this case $H_\ell(E) = V^\ell$ is the first étale cohomology group of $E$ with coefficients in $\mathbf{Q}_\ell$. For varying $\ell$, the corresponding representations of the Weil-Deligne group ${}'W_{\mathbf{Q}_p}$ are *compatible* and $\Phi$-semisimple (see [1]).

As a representation of the Weil-Deligne group, the $\ell$-adic representation $V^\ell$ of $W_{\mathbf{Q}_p}$ corresponds to a pair $(\sigma, N)$, where $\sigma$ is a representation of $W_{\mathbf{Q}_p}$ in $V^\ell$ trivial on an open subgroup of $I$, and where $N$ is a nilpotent endomorphism of $V^\ell$. With this, the definition of $Z_p(E,t)$ becomes

$$Z_p(E,t) = \det\left(1 - \Phi t \mid \ker(N)^{\sigma(I)}\right)^{-1}.$$

Compatibility ensures that $Z_p(E,t)$ has coefficients in $\mathbf{Q}$.

Since $E$ has a Hodge structure of type $\{(0,1),(1,0)\}$ (see, *e.g.*, [6]) the $\Gamma$-factor $L_\infty(E,s)$ is

$$L_\infty(E,s) = \Gamma_{\mathbf{C}}(s) = 2(2\pi)^s\Gamma(s).$$

Since $\check{E} = E(1)$ and $\Lambda(M(n),s) = \Lambda(M,s+n)$ for any motive $M$, the functional equation for $E$ is usually given in the following form:

$$\Lambda(E,s) = \varepsilon(E,s)\Lambda(E,2-s).$$

Taking series expansions about $s = 1$ shows that $\varepsilon(E,1) = \pm 1$.

2. For $M = \rho$, suppose that $\rho$ has as representation space the $K$-vector space $W$. Then the $\lambda$-adic realization $H_\lambda(\rho)$ is just $K_\lambda \otimes_K W$. From this the compatibility of the $H_\lambda(\rho)$ is clear, as is the fact that $Z_p(\rho,t)$ has coefficients in $K$ independent of $\lambda$. The resulting $L$-function is the *Artin L-function* attached to $\rho$.

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

At $\infty$, $\rho$ has a Hodge structure which is pure of type $(0,0)$, and for which the involution acts as complex conjugation (see [2], Section 6). If $d_\rho$ is the dimension of the $(-1)$-eigenspace of complex conjugation, then

$$L_\infty(\rho, s) = \Gamma_{\mathbf{R}}(s+1)^{d_\rho}\Gamma_{\mathbf{R}}(s)^{\dim(\rho)-d_\rho},$$

where $\Gamma_{\mathbf{R}}(s) = \pi^{-s/2}\Gamma(s/2)$.

Since $\rho \cong \check{\rho}$, the (proven) functional equation reads

$$\Lambda(\rho, s) = \varepsilon(\rho, s)\Lambda(\rho, 1-s).$$

Hence, $\varepsilon(\rho, 1/2) = \pm 1$.

3. For $M = E \otimes \rho$, the $\lambda$-adic realization $H_\lambda(E \otimes \rho)$ is

$$V^\ell \otimes_{\mathbf{Q}_\ell} [K_\lambda \otimes_K W].$$

The resulting $L$-function is a *twisted Hasse-Weil L-function*. By the compatibility of each of the two previous representations, the $H_\lambda(E \otimes \rho)$ are also compatible, and $Z_p(E \otimes \rho, t)$ has coefficients in $K$ independent of $\lambda$. Note, too, that the $H_\lambda(E \otimes \rho)$ are $\Phi$-semisimple, since both $E$ and $\rho$ are.

At $\infty$, the Hodge structure is pure of type $\{(1,0),(0,1)\}$ and hence $L_\infty(E \otimes \rho, s) = \Gamma_{\mathbf{C}}(s)^{\dim \rho}$. As $\check{M} = \check{E} \otimes \check{\rho} = E(1) \otimes \rho$, the conjectural functional equation will be of the form

$$\Lambda(E \otimes \rho, s) = \varepsilon(E \otimes \rho, s)\Lambda(E \otimes \rho, 2-s),$$

from which one concludes that $\varepsilon(E \otimes \rho, 1) = \pm 1$.

The term *root number* will always refer to $\varepsilon(E \otimes \rho, 1)$.

1.3. *A form of the Birch and Swinnerton-Dyer conjecture.* Recall that the Birch and Swinnerton-Dyer conjecture says that the order of vanishing at $s = 1$ of the $L$-function of an elliptic curve $E$ defined over a number field $K$ is the rank of $E(K)$. A generalization of this conjecture also uses the Deligne-Gross conjecture that the order of vanishing of a motivic $L$-function at a critical point is independent of the embedding of the coefficient field in $\mathbf{C}$ (see [2], Conjecture 2.7). The following ([5]) supports assertions made in the introduction:

PROPOSITION 1. *The Birch and Swinnerton-Dyer and Deligne-Gross conjectures together imply that*

$$\operatorname{ord}_{s=1} L(E \otimes \rho, s) = \textit{multiplicity of } \rho \textit{ in } E(\bar{\mathbf{Q}}) \otimes \mathbf{C},$$

*where* $\bar{\mathbf{Q}}$ *denotes an algebraic closure of* $\mathbf{Q}$.

## 2. The root number formula.

2.1. *Local constants.* To compute the root number $\varepsilon(E \otimes \rho, 1)$, we will make use of the conjectural formulae for motivic epsilon factors $\varepsilon(M, s)$ as products over all $p$ of the local factors $\varepsilon_p(M, s, \psi_p, dx_p)$ and of a factor at infinity $\varepsilon_\infty(M, s, \psi_\infty, dx_\infty)$.

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

1. For each prime $p$, set $\psi_p(x) = \exp(-2\pi ix)$, which gives an additive character $\psi_p\colon \mathbf{Q}_p \longrightarrow \mathbf{C}^\times$ via the isomorphism

$$\mathbf{Q}_p/\mathbf{Z}_p \xrightarrow{\sim} p\text{-primary part of } \mathbf{Q}/\mathbf{Z}.$$

Let $dx_p$ be the Haar measure on $\mathbf{Q}_p$ that gives $\int_{\mathbf{Z}_p} dx_p = 1$. Denote by $\omega_s$ the quasi-character $x \longmapsto \|x\|^s$ of $\mathbf{Q}_p^\times$, hence of $W_{\mathbf{Q}_p}$. If the $\lambda$-adic realization $H_\lambda(M)$ of $M$ corresponds to the representation $(\sigma, N)$ of the Weil-Deligne group ${}'W_{\mathbf{Q}_p}$, then define

$$\varepsilon_p(M, s, \psi_p, dx_p) = \varepsilon(\sigma \otimes \omega_s, \psi_p, dx_p) \cdot \det\left(-\Phi p^{-s} \mid H_\lambda(M)^{\sigma(I)} / \ker(N)^{\sigma(I)}\right), \tag{4}$$

where $\varepsilon(\sigma\otimes\omega_s, \psi_p, dx_p)$ is defined by Deligne's theory of local constants ([1], Section 4), since $\sigma \otimes \omega_s$ gives a complex representation of $W_{\mathbf{Q}_p}$ via an embedding $K_\lambda \longrightarrow \mathbf{C}$ over $K$ ($K$ = coefficient field of $M$). Compatibility makes the above definition independent of $\lambda$ and the choice of embedding of $K_\lambda \longrightarrow \mathbf{C}$.

2. At $\infty$, if we set $\psi_\infty = \exp(2\pi ix)$ for $x \in \mathbf{R}$, and $dx_\infty$ to be Lebesgue measure, then $\varepsilon_\infty(M, s, \psi_\infty, dx_\infty)$ is again dependent only on the Hodge structure of $M$, and everything is given in a table in [2], Section 5.3.

2.2. *The formula.*

THEOREM 1. *Assume the formulae for the local epsilon factors given in the preceding section. Let $\rho$ be an irreducible representation of* $\mathrm{Gal}(\mathrm{PQ}_n/\mathbf{Q})$. *If* $\dim(\rho)$ *is even, then*

$$\varepsilon(E \otimes \rho, 1) = (-1)^{d_\rho} \det \rho\big(F(E)\big),$$

*where $N_E$ is the conductor of $E$ and $d_\rho$ is the dimension of the $(-1)$-eigenspace of complex conjugation under $\rho$.*

We first prove the following formula holds for each prime $p$:

$$\varepsilon_p(E \otimes \rho, 1, \psi_p, dx_p) = \varepsilon_p(E, 1, \psi_p, dx_p)^{\dim \rho} \varepsilon_p(\rho, 1/2, \psi_p, dx_p)^2 \det \rho(p^{a(E)}), \tag{5}$$

where $a(E)$ is the exponent of the conductor of $E$.

We distinguish two cases.

CASE 1. *$p$ is a prime of good reduction for $E$.* By the criterion of Néron-Ogg-Shafarevich, $V^\ell$ is unramified, so as a Weil-Deligne group representation we have $N = 0$ for $E$. Therefore, our three motives, $E$, $\rho$, and $E \otimes \rho$, give only complex representations of $W_{\mathbf{Q}_p}$. We can consequently resolve the matter using Deligne's theory of local constants, since the determinant term in Equation (4) is 1.

LEMMA 1. *If $\sigma$ is an unramified, semisimple representation of $W_{\mathbf{Q}_p}$, then*

$$\varepsilon_p(\sigma, s, \psi_p, dx_p) = \varepsilon(\sigma \otimes \omega_s, \psi_p, dx_p) = 1.$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

PROOF. The assumptions show that $\sigma$ is a direct sum of unramified quasi-characters; hence, so is $\sigma \otimes \omega_s$ for any $s$. By the choice of $\psi_p$ and $dx_p$, we have $\varepsilon(\omega, \psi_p, dx_p) = 1$ for any unramified quasi-character, using the definition of the local constants in the abelian case (see [10], Section 3.2.6). The lemma follows easily. ∎

In our case, we know that $\Phi$ acts semisimply on $V^\ell$. Hence, by the lemma, $\varepsilon_p(E, s, \psi_p, dx_p) = 1$ for any $s$. Setting $s = 1$ then gives $\varepsilon_p(E, 1, \psi_p, dx_p) = 1$. Moreover, $a(E) = 0$ since $V^\ell$ is unramified. Therefore the right-hand side of Equation 5 reduces to $\varepsilon_p(\rho, 1/2, \psi_p, dx_p)^2$.

Another useful formula from the theory of local constants is found in [10], Section 3.4.6.

LEMMA 2. *If $U$ and $V$ are $W_{\mathbf{Q}_p}$-representations and $V$ is unramified, then*

$$\varepsilon(U \otimes V, \psi_p, dx_p) = \varepsilon(U, \psi_p, dx_p)^{\dim V} \det V(p^{a(U)}).$$

In our case we have

$$\begin{aligned}\varepsilon_p(E \otimes \rho, 1, \psi_p, dx_p) &= \varepsilon(E \otimes \rho \otimes \omega_1, \psi_p, dx_p) \\ &= \varepsilon(\rho, \psi_p, dx_p)^2 \det V^\ell \otimes \omega_1(p^{a(\rho)}).\end{aligned}$$

Now, $\det V^\ell \otimes \omega_1(p^{a(\rho)}) = \det V^\ell(p^{a(\rho)})\omega_2(p^{a(\rho)})$. As the uniformizer $p$ corresponds to a geometric Frobenius element $\Phi$, and as

$$\det(1 - \Phi t) = 1 - a_p t + pt^2$$

on $V^\ell$, we have $\det V^\ell(p) = \det V^\ell(\Phi) = p$. Therefore, $\det V^\ell \otimes \omega_1(p^{a(\rho)}) = p^{a(\rho)}\|p^{a(\rho)}\| = p^{-a(\rho)}$, and so

$$\begin{aligned}\varepsilon_p(E \otimes \rho, 1, \psi_p, dx_p) &= \varepsilon(\rho, \psi_p, dx_p)^2 p^{-a(\rho)} \\ &= [\varepsilon(\rho, \psi_p, dx_p)\omega_{1/2}(p^{a(\rho)})]^2.\end{aligned}$$

Applying Lemma 2, the last term on the right is

$$\varepsilon(\rho \otimes \omega_{1/2}, \psi_p, dx_p)^2 = \varepsilon_p(\rho, 1/2, \psi_p, dx_p)^2,$$

which establishes Equation 5 in the case of $p$ being a prime of good reduction of $E$.

CASE 2. *$p$ is a prime of bad reduction for $E$.* The $\ell$-adic representation $V^\ell$ gives a representation $(\sigma, N)$ of the Weil-Deligne group ${}'W_{\mathbf{Q}_p}$. Our Galois representation $\rho$ gives the representation $(\rho, 0)$ of ${}'W_{\mathbf{Q}_p}$, and so $V^\ell \otimes \rho$ gives $(\sigma \otimes \rho, N \otimes 1)$. Thus, we need to work with the general formula

$$\begin{aligned}&\varepsilon_p(E \otimes \rho, s, \psi_p, dx_p) \\ &\quad = \varepsilon(\sigma \otimes \rho \otimes \omega_s, \psi_p, dx_p) \cdot \det\left(-\Phi p^{-s} \mid [V^\ell \otimes \rho]^{\sigma \otimes \rho(I)} / \ker(N \otimes 1)^{\sigma \otimes \rho(I)}\right).\end{aligned}$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

Since, by our assumptions, $E$ and $\rho$ have coprime conductors, $\rho$ must be unramified. Hence,

$$[V^\ell \otimes \rho]^{\sigma\otimes\rho(I)} = (V^\ell)^{\sigma(I)} \otimes \rho,$$

and since $\ker(N \otimes 1) = \ker(N) \otimes \rho$, we have

$$\ker(N \otimes 1)^{\sigma\otimes\rho(I)} = \ker(N)^{\sigma(I)} \otimes \rho.$$

Putting the two together, we have the isomorphism

$$[V^\ell \otimes \rho]^{\sigma\otimes\rho(I)} / \ker(N \otimes 1)^{\sigma\otimes\rho(I)} \cong [(V^\ell)^{\sigma(I)} / \ker(N)^{\sigma(I)}] \otimes \rho.$$

As $\Phi$ acts semisimply on both $V^\ell$ and $\rho$, we can then break up the determinant term using the following elementary lemma:

LEMMA 3. *If $S \in \mathrm{End}(U)$ and $T \in \mathrm{End}(V)$ are both semisimple linear transformations, then*

$$\det(S \otimes T) = \det(S)^{\dim V} \det(T)^{\dim U}.$$

Thus, if we abbreviate $\sigma(I)$ by $I$, we have

$$\begin{aligned}\det\left(-\Phi p^{-s} \mid [(V^\ell)^I / \ker(N)^I] \otimes \rho\right) &= (-p^{-s})^{\dim\rho[\dim(V^\ell)^I \dim\ker(N)^I]} \\ &\quad \cdot \det\left(\Phi \mid (V^\ell)^I / \ker(N)^I\right)^{\dim\rho} \cdot \det(\Phi \mid \rho)^{\dim(V^\ell)^I \dim\ker(N)^I}.\end{aligned}$$

The last term on the right is

$$\det\rho(p^{\dim(V^\ell)^I \dim\ker(N)^I}).$$

The first two terms combine to give

$$\det\left(-\Phi p^{-s} \mid (V^\ell)^I / \ker(N)^I\right)^{\dim\rho}.$$

We can now use Lemma 2 on $\varepsilon(\sigma \otimes \rho \otimes \omega_s, \psi_p, dx_p)$ to get

$$\varepsilon(\sigma \otimes \rho \otimes \omega_s, \psi_p, dx_p) = \varepsilon(\sigma \otimes \omega_s, \psi_p, dx_p)^{\dim\rho} \cdot \det\rho(p^{a(\sigma\otimes\omega_s)}).$$

Since $\omega_s$ is unramified, $a(\sigma \otimes \omega_s) = a(\sigma)$.

Combining everything, we have

$$\begin{aligned}\varepsilon_p(E \otimes \rho, s, \psi_p, dx_\rho) &= \left[\varepsilon(\sigma \otimes \omega_s, \psi_p, dx_p) \det\left(-\Phi p^{-s} \mid (V^\ell)^I / \ker(N)^I\right)\right]^{\dim\rho} \\ &\quad \cdot \det\rho(p^{a(\sigma)+\dim(V^\ell)^I - \dim\ker(N)^I}) \\ &= \varepsilon_p(E, s, \psi_p, dx_p)^{\dim\rho} \det\rho(p^{a(E)}),\end{aligned}$$

using the definition of the conductor (see, *e.g.*, [10], Section 4.1.6) to obtain the last term on the right. This proves that Equation 5 holds in this case too, since we have

$$\varepsilon_p(\rho, 1/2, \psi_p, dx_p) = 1$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

because $\rho$ is unramified (Lemma 1).

To complete the proof, we only need to find the constants at $\infty$. From Deligne's table ([2] Section 5.3) we easily read off the following:

$$\begin{aligned}\varepsilon_\infty(E, s, \psi_\infty, dx_\infty) &= -1,\\ \varepsilon_\infty(\rho, s, \psi_\infty, dx_\infty) &= (i)^{d_\rho},\\ \varepsilon_\infty(E \otimes \rho, s, \psi_\infty, dx_\infty) &= (-1)^{\dim \rho} = \varepsilon_\infty(E, s, \psi_\infty, dx_\infty)^{\dim \rho}.\end{aligned}$$

Now, assembling all the pieces, we have

$$\begin{aligned}&\varepsilon(E \otimes \rho, 1)\\ &\quad= \varepsilon_\infty(E \otimes \rho, 1, \psi_\infty, dx_\infty) \prod_p \varepsilon_p(E \otimes \rho, 1, \psi_p, dx_p)\\ &\quad= \varepsilon_\infty(E, 1, \psi_\infty, dx_\infty)^{\dim \rho}\\ &\qquad\cdot \prod_p \Big(\varepsilon_p(E, 1, \psi_p, dx_p)^{\dim \rho} \varepsilon_p(\rho, 1/2, \psi_p, dx_p)^2 \det \rho(p^{a(E)})\Big)\\ &\quad= \varepsilon(E, 1)^{\dim \rho} \varepsilon(\rho, 1/2)^2 \varepsilon_\infty(\rho, 1/2, \psi_\infty, dx_\infty)^{-2} \det \rho[N_E]\\ &\quad= (\pm 1)^{\dim \rho} (\pm 1)^2 (-1)^{d_\rho} \det \rho[N_E].\end{aligned}$$

Since $\dim \rho$ is even by assumption, this completes the proof. ∎

3. **Computation of root numbers.** Throughout, let $O$ denote the ring $\mathbf{Z}_p$, $P$ the maximal ideal of $O$, $O^\times$ the group of units in $O$, and $U^i$ the group $O^\times / 1 + P^i$. To simplify notation, let $G$ be the profinite group $\mathrm{PGL}_2(\mathbf{Z}_p)$, and $G^n$ the finite quotient $\mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$. The kernel of the canonical map $G \longrightarrow G^n$ will be denoted by $G_n$. For $n = 0$, take $G^0 = \{1\}$ and $G_0 = G$.

3.1. *Complex representations of* $\mathrm{PGL}_2(\mathbf{Z}_p)$. Every (continuous) representation $\rho$ of $G$ in a complex vector space has a finite image, hence factors through some $G^n$. If a representation $\rho$ factors through $G^n$, but not through $G^{n-1}$, then $\rho$ is said to be *primitive* modulo $P^n$.

Any representations of $G$ falls into one of four classes: the principal series, the unramified discrete series, or one of the two ramified discrete series. Except for the two one-dimensional characters and two $p$-dimensional representations, all these representations of $G$ are even dimensional. Hence, the root number formula (Theorem 1) is applicable in almost all cases.

A survey of the representation theory of $G$ can be found in [9].

3.2. *Summary of results.* The remaining sections are devoted to proving the following theorem. Recall that we are assuming that $N_E$, the conductor of the elliptic curve $E$, is unramified in $\mathrm{PQ}_n$.

THEOREM 2. *From the root number formula (Theorem 1) it follows that*

$$\varepsilon(E \otimes \rho, 1) = +1$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

*for all even dimensional representations $\rho$ except the representations $\rho = u_\alpha$ of the principal series and $\rho = u_\pi$ of the discrete series. For both of these types,*

$$\varepsilon(E \otimes \rho, 1) = \left(\frac{-N_E}{p}\right),$$

*where the parentheses on the right denote the Legendre symbol.*

Using this theorem, the lower bound for the rank of $E(\mathrm{PQ}_n)$ is a straightforward computation.

THEOREM 3. *If $-N_E$ is a quadratic nonresidue modulo $p$, then*

$$\operatorname{rank}\big(E(\mathrm{PQ}_n)\big) \geq p^{2n} - p^{2n-1} - p - 1.$$

PROOF. The assumption that all primes in $N_E$ are unramified in $\mathrm{PQ}_n$ means that the root number formula applies to all the twists of the $L$-function of $E$ by irreducible even-dimensional representations of $\mathrm{Gal}(\mathrm{PQ}_n / \mathbf{Q})$. In that case, the previous theorem together with our assumption about the quadratic residuacity of $-N_E$ shows that all the $u_\alpha$ and $u_\pi$ above that are primitive modulo $P^i$ for $1 \leq i \leq n$ will occur in $E(\mathrm{PQ}_n) \otimes \mathbf{C}$.

For every character $\alpha$ of $\mathbf{Z}_p^\times$ of conductor $P^i$, $u_\alpha$ is an irreducible representation primitive modulo $P^i$ of dimension $p^i + p^{i-1}$. For $i = 1$, there are $(p-3)/2$ isomorphism classes of such representations, while for $i \geq 2$ there are $p^{i-2}(p-1)^2/2$ distinct classes ([9], Section 3.4).

Given a character $\pi$ on $O_F^\times$ of conductor $P_F^i$ ($F$ = the unramified extension of $\mathbf{Q}_p$, $O_F^\times$ = units in the ring of integers $O_F$, $P_F$ = maximal ideal of $O_F$), if we assume $\pi$ is trivial on $\mathbf{Z}_p^\times$, then $u_\pi$ is an irreducible representation primitive modulo $P^i$ of dimension $p^i - p^{i-1}$. For $i = 1$, there are $(p-1)/2$ such isomorphism classes, while for $i \geq 2$ there are $p^{i-2}(p^2-1)/2$ classes (*loc. cit.*).

Adding gives the result:

$$\begin{aligned}\operatorname{rank}\big(E(K_n)\big) &\geq \left(\frac{p-3}{2}\right)(p+1) + \left(\frac{p-1}{2}\right)(p-1) \\ &\quad + \sum_{i=2}^{n} \frac{1}{2} p^{i-2}(p-1)^2(p^i + p^{i-1}) \\ &\quad + \sum_{i=2}^{n} \frac{1}{2} p^{i-2}(p^2-1)(p^i - p^{i-1})) \\ &= p^{2n} - p^{2n-1} - p - 1,\end{aligned}$$

which was to be shown. ∎

3.3. *The principal series representations.* Let $\alpha$ be a character on $O^\times$ with conductor $P^m$. Any such also gives a character on the subgroup $B$ of upper triangular matrices in $G$. For each such character $\alpha$, the action of $G$ on

$$H_0^\alpha = \{\psi \in L^2(G, \mathbf{C}) \mid \psi(bg) = \alpha(b)\psi(g), \text{ for all } b \in B, g \in G\}$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

by right translation gives a unitary representation $U^\alpha$ of $G$. The sets

$$H_i{}^\alpha = \{\psi \in H_0{}^\alpha \mid \psi \text{ is constant on } G_i - \text{cosets}\}$$

for $i \geq 0$ form an increasing chain of $G$-invariant subspaces. Denote the corresponding representations by $U_i^\alpha$. For $i \geq 1$, let $H_i^\alpha$ be the orthogonal complement of $H_{i-1}{}^\alpha$ in $H_i{}^\alpha$, and let the resulting representation be $u_{\alpha,i}$. Clearly, for $i \geq m$, $U_i^\alpha$ is just the induced representation $\mathrm{Ind}_{B^i}^{G^i}(\alpha)$.

All irreducible representations in the principal series are catalogued in the following theorem.

THEOREM 4 ([9], P. 58). *If $\alpha$ is real-valued, $U_1^\alpha$ decomposes as the sum of a one-dimensional and a p-dimensional irreducible representation. For all other characters $\alpha$, if $\alpha$ has conductor $P^m$, then the representation $u_\alpha = U_m^\alpha$ on $H_m{}^\alpha$ is irreducible, of dimension $p^m + p^{m-1}$. For $i > m$, the representations $u_{\alpha,i}$ are all irreducible, of dimension $p^i - p^{i-2}$.*

Recall the root number formula:

$$\varepsilon(E \otimes \rho, 1) = (-1)^{d_\rho} \det \rho(N_E).$$

Because $\det \rho$ is either the trivial character or the unique quadratic character $\chi$, which, for $g \in \mathrm{PGL}_2(\mathbf{Z}/p^n\mathbf{Z})$, is the map

$$g \longmapsto \det g \in (\mathbf{Z}/p^n\mathbf{Z})^\times / [(\mathbf{Z}/p^n\mathbf{Z})^\times]^2 \cong \{\pm 1\},$$

the root number formula can be simplified.

LEMMA 4. *If $\det \rho$ is the trivial character then $\varepsilon(E \otimes \rho, 1) = +1$. If $\det \rho = \chi$, then*

$$\varepsilon(E \otimes \rho, 1) = \left(\frac{-N_E}{p}\right).$$

PROOF. The parity of $d_\rho$ can be found by evaluating $\det \rho$ at complex conjugation, since the representation space is then the direct sum of the $+1$ and $-1$ eigenspaces. Clearly, if $\det \rho$ is the trivial character $d_\rho$ is even. If $\det \rho$ is $\chi$ then $d_\rho$ is the Legendre symbol

$$\left(\frac{-1}{p}\right),$$

since the $2 \times 2$-determinant of complex conjugation is $-1$, modulo squares. Similarly, $\chi(N_E)$ is also just the Legendre symbol. ∎

To determine $\det \rho$ for the principal series it is sufficient to do it for the representations $U_i^\alpha$, since we have

$$\det u_{\alpha,i} = (\det U_i^\alpha)(\det U_{i-1}^\alpha)^{-1} \tag{6}$$

because $u_{\alpha,i}$ is the orthogonal complement of $U_{i-1}^\alpha$ in $U_i^\alpha$. To check whether $\det U_i^\alpha$ is the trivial character or not, it suffices to evaluate it on the matrix $[\zeta] = \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix}$, where $\zeta \in \mathbf{Z}_p^\times$ is a topological generator. Since $U_i^\alpha \cong \mathrm{Ind}_{B^i}^{G^i}(\alpha)$, we can use the formula for the determinant of an induced representation:

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

LEMMA 5 ([1] P. 508). *If $G$ is a finite group and $\sigma$ a representation of a subgroup $H$, then*

$$\det \operatorname{Ind}_H^G(\sigma) = [\det \operatorname{Ind}_H^G(1)]^{\dim(\sigma)} \cdot (\det \sigma) \circ t_H^G,$$

*where $t_H^G$ denoted the transfer map from the abelianization $G^{ab}$ of $G$ to the abelianization $H^{ab}$ of $H$.*

In our case this yields the formula

$$\det U_i^\alpha = \left(\det \operatorname{Ind}_{B^i}^{G^i}(1)\right)(\alpha \circ t_{B^i}^{G^i}). \tag{7}$$

The second term on the right is taken care of by the following lemma.

LEMMA 6. *The transfer map $t_{B^i}^{G^i}$ is trivial.*

We will make use of the following transversal $\mathbf{T}$ for the coset space $B^i \setminus G^i$. First, set the following notation:

$$M(z) = \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$$
$$M'(z') = \begin{pmatrix} 0 & 1 \\ -1 & z' \end{pmatrix}$$
$$\Delta(a, b) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$$

Now define $\mathbf{T}$ by

$$\mathbf{T} = \{M(z), M'(z') \mid z \in O/P^i, z' \in P/P^i\} \tag{8}$$

PROOF OF LEMMA 6. The transfer map

$$t_{B^i}^{G^i} : (G^i)^{ab} \longrightarrow (B^i)^{ab}$$

can be defined as follows. Let $s : B^i \setminus G^i \longrightarrow G^i$ be any section of the canonical projection; then

$$t_{B^i}^{G^i}\left(g(G^i)^c\right) = \prod_{x \in B^i \setminus G^i} b_{g,x} \pmod{(B^i)^c},$$

where $b_{g,x} \in B^i$ is defined by $s(x)g = b_{g,x}s(xg)$, and where the superscript $c$ denotes the commutator subgroup. Since $(G^i)^{ab} \cong \{\pm 1\}$, it suffices to compute $t_{B^i}^{G^i}$ for $[\zeta]$ to see whether it is trivial or not, since $[\zeta]$ represents the nontrivial element in the group. For the section $s$ take the transversal $\mathbf{T}$.

Now,

$$M(z)\Delta(\zeta, 1) = \Delta(\zeta, 1)M(\zeta z) \tag{9}$$

$$M'(z')\Delta(\zeta, 1) = \Delta(1, \zeta)M'(\zeta^{-1}z'), \tag{10}$$

So, $b_{[\zeta],x} = \Delta(\zeta, 1)$ for $x = M(z)$, and $b_{[\zeta],x} = \Delta(1, \zeta)$ for $x = M'(z')$. Hence,

$$t_{B^i}^{G^i}([\zeta]) = \Delta(\zeta, 1)^{p^i}\Delta(1, \zeta)^{p^{i-1}} = \zeta^{p^{i-1}}\Delta(\zeta^{\phi(p^i)}, 1).$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

| ord($z$) | # in orbit | ord($z'$) | # in orbit |
|---|---|---|---|
| 0 | $p^i - p^{i-1}$ | 1 | $p^{i-1} - p^{i-2}$ |
| 1 | $p^{i-1} - p^{i-2}$ | 2 | $p^{i-2} - p^{i-3}$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $i-1$ | $p-1$ | $i-1$ | $p-1$ |
| $i$ | 1 | $i$ | 1 |

Table 1: Lengths of orbits for action of $[\zeta]$.

But $\zeta^{\phi(p^i)} = 1$ in $(O/P^i)^\times$, so $t_{B^i}^{G^i}$ is indeed trivial. ∎

We now turn to the determination of the character $\det \mathrm{Ind}_{B^i}^{G^i}(1)$. First, consider the following basis for the representation space

$$\{\psi : G^i \longrightarrow \mathbf{C} \mid \psi(bg) = \psi(g), \text{ for all } b \in B^i, g \in G^i\}.$$

For each $x \in B^i \setminus G^i$, define $\psi_x$ by

$$\psi_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{if } y \neq x. \end{cases}.$$

The action of $[\zeta]$ on this basis is easily computed:

$$[\zeta]\psi_x(y) = \psi_x(y[\zeta]) = 1 \Longleftrightarrow y[\zeta] = x \Longleftrightarrow y = x[\zeta^{-1}].$$

This shows that $[\zeta]\psi_x = \psi_{x[\zeta^{-1}]}$. Thus, $[\zeta]$ permutes the basis elements in the same way that right translation by $[\zeta^{-1}]$ permutes the elements of the coset space $B^i \setminus G^i$. The transversal $\mathbf{T}$ can be used to compute the orbits of $[\zeta^{-1}]$ in $B^i \setminus G^i$. From Equation 9 and 10,

$$\begin{aligned} B^i M(z)[\zeta^{-1}] &= B^i M(\zeta^{-1}z), B^i M'(z')[\zeta^{-1}] \\ &= B^i M'(\zeta z'). \end{aligned}$$

So, orbits are formed of all matrices $M(z)$ (resp., $M'(z')$) with $z$ (resp., $z'$) of the same order. The lengths of the orbits are recorded in Table 1. Thus, $[\zeta^{-1}]$ acts as a product of $2i-1$ disjoint cycles of even length. As even cycles are odd permutations, we conclude that $\det U_i^\alpha[\zeta] = (-1)^{2i-1} = -1$, which says that $\det U_i^\alpha$ is the nontrivial character $\chi$ of $G^i$.

By Equation 6 it follows that $\det u_\alpha = \chi$ and $\det u_{\alpha,i} = 1$ for $i > m$. Therefore,

$$\begin{aligned} \varepsilon(E \otimes u_\alpha, 1) &= \left(\frac{-N_E}{p}\right), \\ \varepsilon(E \otimes u_{\alpha,i}, 1) &= +1. \end{aligned}$$

This proves Theorem 2 for $\rho$ an even-dimensional representation in the principal series.

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

3.4. *On the discrete series representations.* Let $F$ be one of the three quadratic extensions $F$ of $\mathbf{Q}_p$, and let $\chi_F$ be the corresponding quadratic character on $\mathbf{Q}_p^\times$. Thus, $\chi_F$ is trivial on $N(F^\times)$, where $N$ denotes the norm map.

Let $O_F$ be the ring of integers of $F$, $P_F$ the maximal ideal of $O_F$, $O_F^\times$ the group of units in $O_F$, and $U_F^i$ the group $O_F^\times/(1+P_F^i)$. The function that gives the order of an element in $O$ (respectively, $O_F$) will be denoted ord (respectively, $\mathrm{ord}_F$). We shall use $\|\cdot\| = \|\cdot\|_F$ to denote the absolute value for which the product formula holds. Finally, the nontrivial automorphism of $F$ over $\mathbf{Q}_p$ will be denoted by $x \longmapsto \bar{x}$. With this notation, $N(x) = x\bar{x}$, for $x \in F^\times$.

Starting with a choice of $F$, the corresponding discrete series can be constructed using a character $\pi = \pi_F$ of $F^\times$ for which $\pi|_{\mathbf{Q}_p^\times} = \chi_F$ and for which $\pi(O_F^\times)$ is not contained in $\mathbf{R}$. Irreducible representations appear as subrepresentations of the space

$$D^\pi = \{\psi \in L^2(\mathbf{Q}_p^\times \times F^\times; \mathbf{C}) \mid \forall t \in \mathbf{Q}_p^\times, \psi(t,x) \text{ is a finite function of } x \\ \text{and } \forall \gamma \in F^\times, \psi(\gamma\bar{\gamma}t, x) = \pi^{-1}(\gamma)\|\gamma\|^{1/2}\psi(t,\gamma x)\},$$

where the term *finite function* in this case means that there are integers $n$, $m$ with $n \le m$ such that $\psi(t,x) = 0$ if $x$ is not in $P_F^n$, and $\psi(t, x+\xi) = \psi(t,x)$ whenever $\xi \in P_F^m$. For future reference the second condition of the definition will be called the *transformation law*:

$$\forall \gamma \in F^\times, \psi(\gamma\bar{\gamma}t, x) = \pi^{-1}(\gamma)\|\gamma\|^{1/2}\psi(t,\gamma x), \tag{11}$$

The action of $G$ on $D^\pi$ is a complicated business in general. (See [9] for details.) But for diagonal matrices it is straightforward: for $[a] = \Delta(a,1)$, $a \in O^\times$, $[a]\psi(t,x) = \psi(at,x)$.

For the computations, it is notationally helpful to distinguish between the ramified and unramified cases.

3.5. *The unramified discrete series representations.* Let $F$ now be the unramified extension of $\mathbf{Q}_p$. Fixing some nonsquare unit $\zeta$ in $O$, say a topological generator, then $F = \mathbf{Q}_p(\sqrt{\zeta})$. Let $\tau$ be a uniformizer. Let $N$ denote the kernel of the norm map. Let $\pi$ have conductor $P_F^m$. Since $\pi$ is not real-valued, $m \ge 1$.

The representation space $D_i^\pi$ can be decomposed as $D_i^\pi = D_{i,\mathrm{even}}^\pi \oplus D_{i,\mathrm{odd}}^\pi$, ([9] p. 72), where

$$D_{i,\mathrm{even}}^\pi = \{\psi \in D^\pi \mid \psi(t,x) = 0 \text{ if ord}(t) \text{ is odd}; \\ \operatorname{supp}\psi(1,\cdot) \subseteq O_F; \psi(1, x+\xi) = \psi(1,x),\ \forall \xi \in P_F^i\} \tag{12}$$

$$D_{i,\mathrm{odd}}^\pi = \{\psi \in D^\pi \mid \psi(t,x) = 0 \text{ if ord}(t) \text{ is even}; \\ \operatorname{supp}\psi(\tau,\cdot) \subseteq O_F; \psi(\tau, x+\xi) = \psi(\tau,x),\ \forall \xi \in P_F^{i-1}\} \tag{13}$$

The map $\psi(t,x) \longmapsto \psi(\tau^{-1}t, x)$ embeds $D_{i-1}^\pi$ into $D_i^\pi$ as a unitary $G$-representation. Let $D_i^\pi$ be the orthogonal complement of $D_{i-1}^\pi$ in $D_i^\pi$.

THEOREM 5 ([9], P. 79). *The representation $u_\pi = D_m^\pi$ is irreducible of dimension $p^m - p^{m-1}$. (In this case $D_{m,\mathrm{odd}}^\pi = \{0\}$.) For $i > m$, $D_i^\pi$ is irreducible of dimension $p^i - p^{i-2}$, giving the representations $u_{\pi,i}$.*

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

We now construct a convenient basis for $D_i^\pi$, $i \geq m$. Note that under the multiplicative action of $N$ on $O_F$ the $P_F^i$ are invariant subgroups. Thus, $N$ acts on all the quotients $O_F/P_F^i$.

PROPOSITION 2. *Let $S_{\text{even}}$ be a set of representatives for the $N$-orbits in*

$$\{\xi \in O_F/P_F^i \mid \text{ord}_F(\xi) \leq i-m\}$$

*and $S_{\text{odd}}$ be the same for*

$$\{\xi \in O_F/P_F^{i-1} \mid \text{ord}_F(\xi) \leq i-1-m\}.$$

*For each $x \in S_{\text{even}}$ set*

$$\psi_x(1,y) = \begin{cases} 1 & y = x, \\ 0 & y \in S_{\text{even}} \setminus \{x\} \end{cases},$$

*and for each $x \in S_{\text{odd}}$ set*

$$\psi_x(\tau,y) = \begin{cases} 1 & y = x, \\ 0 & y \in S_{\text{odd}} \setminus \{x\}. \end{cases}$$

*Then, for each $x \in S_{\text{even}}$ (resp., $x \in S_{\text{odd}}$), $\psi_x$ extends uniquely to a function in $D_{i,\text{even}}^\pi$ (resp., $D_{i,\text{odd}}^\pi$). Moreover,*

$$\{\psi_x \mid x \in S_{\text{even}} \cup S_{\text{odd}}\}$$

*is a basis for $D_i^\pi$.*

PROOF. First we show that any $\psi \in D_{i,\text{even}}^\pi$ (resp., $\psi \in D_{i,\text{odd}}^\pi$) is determined by its values on $S_{\text{even}}$ (resp., $S_{\text{odd}}$). Once this has been established, the result follows by showing that

$$\#(S_{\text{even}} \cup S_{\text{odd}}) = p^i + p^{i-1} - 2p^{m-1} = \dim D_i^\pi.$$

Let $\psi \in D_i^\pi$. According to the transformation law (Equation 11)

$$\psi(\tau^{2n}t,x) = \pi^{-1}(\tau^n)\|\tau^n\|^{1/2}\psi(t,\tau^n x),$$

so once $\psi(t,x)$ is known for $\text{ord}(t) = 0, 1$, it is known for all $t$. Moreover, let $t \in O^\times$ and pick some $\beta \in F^\times$ such that $N(\beta) = t$. Then for $\psi \in D_{i,\text{even}}^\pi$,

$$\psi(t,x) = \pi^{-1}(\beta)\|\beta\|^{1/2}\psi(1,\beta x),$$

so knowing $\psi$ is the same as knowing $\psi(1,x)$ for all $x$. Moreover, by the definition of $D_{i,\text{even}}^\pi$ (Equation 12), one only needs to know the value of $\psi(1,x)$ for $x \in O_F$, and this only up to addition by elements of $P_F^i$. As for $\psi \in D_{i,\text{odd}}^\pi$, a similar result holds: $\psi$ is determined by its values $\psi(\tau,x)$ for $x$ modulo $P_F^{i-1}$ (Equation 13).

Thus, for $\psi \in D_{i,\text{even}}^\pi$, $\psi(1,\cdot)$ can be considered as a function on $O_F/P_F^i$. From the transformation law with $\gamma \in N$, we have

$$\psi(\gamma\bar{\gamma},x) = \psi(1,x) = \pi^{-1}(\gamma)\|\gamma\|^{1/2}\psi(1,\gamma x),$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

or,

$$\forall \gamma \in N\,, \quad \psi(1,\gamma x) = \pi(\gamma)\psi(1,x). \tag{14}$$

In order for $\psi(1,x)$ to be nonzero, $\pi(\gamma)$ must be trivial whenever $\gamma x = x + \xi$ for some $\xi \in P_F^i$, and some $\gamma \in N$. Since $\gamma x = x + \xi$ if and only if $\gamma = 1 + \xi x^{-1}$, this condition is equivalent to $\pi$ being trivial on $N \cap (1 + P_F^{i\,\mathrm{ord}_F(x)})$. Now, the $\pi$ we are using is not arbitrary.

LEMMA 7. *The assumptions on* $\pi$ ($\pi|_{\mathbf{Q}_p^\times} = \chi_F$; $\pi|_{O_F^\times}$ *not real-valued*) *imply that* $\pi$ *is never trivial on* $N \cap (1 + P_F^j)$ *for* $j < m$.

PROOF. If $m = 1$, we need to show $\pi$ is not trivial on $N$. If it were, then since $\pi$ is trivial on norms ($\pi|_{\mathbf{Q}_p^\times} = \chi_F$), we would have $\pi$ being trivial on $N\,O^\times$. But we have the morphism of exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & O_F^\times & \xrightarrow{N} & O^\times & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & N & \longrightarrow & N\,O^\times & \xrightarrow{N} & (O^\times)^2 & \longrightarrow & 1 \end{array}$$

Thus, $[O_F^\times : N\,O^\times] = [O^\times : (O^\times)^2] = 2$. But then this says that the image of $\pi|_{O_F^\times}$ has order 2, *i.e.*, that $\pi|_{O_F^\times}$ is real-valued, contrary to assumption. Therefore the lemma is true for $m = 1$.

Now assume $m > 1$. It suffices to prove the result for $j = m-1$ since the $N \cap (1+P_F^j)$ form a decreasing chain of subgroups. So suppose $\pi$ is trivial on $N \cap (1 + P_F^{m-1})$. Then $\pi$ is surely trivial on $[N \cap (1 + P_F^{m-1})](1 + P^{m-1})$ since $1 + P^{m-1}$ consists of norms. Applying the simple group-theoretic lemma below, we see that $\pi$ must then be trivial on $N\,(1 + P^{m-1}) \cap (1 + P_F^{m-1})$. We again have a diagram of exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & N\,(1 + P_F^{m-1}) & \xrightarrow{N} & 1 + P^{m-1} & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & N & \longrightarrow & N\,(1 + P^{m-1}) & \xrightarrow{N} & (1 + P^{m-1})^2 & \longrightarrow & 1 \end{array}$$

But since $m \geq 2$, $1 + P^{m-1} = (1 + P^{m-1})^2$. So we conclude that the middle vertical arrow is an isomorphism. Hence, $\pi$ us trivial on $N\,(1+P_F^{m-1}) \cap (1+P_F^{m-1}) = 1 + P_F^{m-1}$ contrary to the assumption that $\pi$ has conductor $P_F^m$. This proves the lemma. ∎

The following easy lemma was used in the above proof:

LEMMA 8. *If* $A$, $B$, $C$ *are all subgroups of some larger group, and if* $C \subset B$, *then*

$$[A \cap B]C = AC \cap B.$$

Thus, for $\pi$ to be trivial on $N \cap (1 + P_F^{i-\mathrm{ord}_F(x)})$, we must have $i - \mathrm{ord}_F(x) \geq m$, or equivalently, $\mathrm{ord}_F(x) \leq i - m$. Hence, $\psi(1,\cdot)$, as a function on $O_F/P_F^i$ is determined by its values for $\mathrm{ord}_F(x) \leq i - m$. From Equation 14 it is then clear that one can specify the

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

function by giving its value on a representative of each $N$ -orbit of such $x$-classes. This shows that any $\psi \in D^{\pi}_{i,\text{even}}$ is completely determined by its values on $S_{\text{even}}$.

The $D^{\pi}_{i,\text{odd}}$ case is entirely analogous. Repeating the argument for $\psi(\tau, x)$ as a function on $O_F/P_F^{i-1}$ shows that any $\psi \in D^{\pi}_{i,\text{odd}}$ is determined by its values on $S_{\text{odd}}$.

It remains to count the size of the sets $S_{\text{even}}$ and $S_{\text{odd}}$.

The group of units $O_F^{\times}$ acts transitively on the set of elements of order $j$ in $O_F/P_F^i$. The stabilizer of any element is $1 + P_F^{i-j}$. Thus, the number of such elements is $\#U_F^{i-j}$. The number of elements in each $N$ -orbit is likewise $\#N^{i-j}$, where $N^k = N/[N \cap (1+P_F^k)]$. Dividing, we find that the number of $N$ -orbits is $\#U_F^{i-j}/\#N^{i-j}$. But using the norm map it is easy to see that this is $\#U^{i-j}$, where $U^{i-j} = O^{\times}/(1 + P^{i-j})$. Since $\#U^{i-j} = \phi(p^{i-j})$ (Euler's $\phi$ function), the total number of orbits is

$$\sum_{j=0}^{i-m} \phi(p^{i-j}) = \sum_{k=m}^{i} \phi(p^k) = p^i - p^{m-1}.$$

Thus,

$$\#S_{\text{even}} = p^i - p^{m-1}.$$

The similar calculation for $S_{\text{odd}}$ gives

$$\#S_{\text{odd}} = p^{i-1} - p^{m-1}.$$

Adding the two cardinalities gives $p^i + p^{i-1} - 2p^{m-1}$, which is precisely the dimension of $D_i^{\pi}$. ∎

Again, the root number computations only need be performed on the representations $U_i^{\pi}$, since for $i > m$,

$$\det u_{\pi,i} = (\det U_i^{\pi})(\det U_{i-1}^{\pi})^{-1}.$$

To see whether $\det U_i^{\pi}$ is the trivial character or not, we evaluate it on $[\zeta] = \Delta(\zeta, 1)$, where $\zeta$ is a topological generator in $O^{\times}$. For any $\beta \in O_F^{\times}$ with $N(\beta) = \zeta$, the action of $[\zeta]$ on $\psi \in D_i^{\pi}$ is given by

$$[\zeta]\psi(t, x) = \psi(\zeta t, x) = \pi^{-1}(\beta)\psi(t, \beta x).$$

If we let $O_F^{\times}$ act on $D_i^{\pi}$ by

$$\psi(t, x) \overset{\beta}{\longmapsto} \psi(t, \beta x), \quad \forall \beta \in O_F^{\times},$$

the results of the last section make this representation easily identifiable. Take the case of $D^{\pi}_{i,\text{even}}$. We can define $O_F^{\times}$-invariant subspaces $V_j$, where

$$V_j = \text{Span}\{\psi_x \mid x \in S_{\text{even}}, \text{ord}_F(x) = j.\}$$

Now, $N$ acts on each of these through the character $\pi$, and clearly the $O_F^{\times}$-translates of any one $\psi_x \in V_j$ span that $V_j$. But $O_F^{\times}$ acts on $V_j$ through the quotient $U_F^{i-j}$, which has as exactly $\dim V_j$ elements. We can therefore conclude that

$$V_j \cong \text{Ind}_{N^{i-j}}^{U_F^{ij}}(\pi).$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

Hence, using an analogous argument for $D^{\pi}_{i,\mathrm{odd}}$, we find that as $O_F^{\times}$-representations,

$$D^{\pi}_{i,\mathrm{even}} \cong \bigoplus_{j=0}^{i-m} \mathrm{Ind}_{N^{i-j}}^{U_F^{i-j}}(\pi)$$

$$\cong \bigoplus_{k=m}^{i} \mathrm{Ind}_{N^{k}}^{U_F^{k}}(\pi) \tag{15}$$

(16)

$$D^{\pi}_{i,\mathrm{odd}} \cong \bigoplus_{k=m}^{i-1} \mathrm{Ind}_{N^{k}}^{U_F^{k}}(\pi). \tag{17}$$

Call the representation of $O_F^{\times}$ obtained in this way on $D^{\pi}_{i,\mathrm{even}}$, (respectively, on $D^{\pi}_{i,\mathrm{odd}}$) $\sigma^{\pi}_{i,\mathrm{even}}$, (respectively, $\sigma^{\pi}_{i,\mathrm{odd}}$). To get the action of $[\zeta]$, first choose $\beta$ with $N(\beta) = \zeta$, and then let $\beta$ act through the representations $\pi^{-1} \otimes \sigma^{\pi}_{i,\mathrm{even}}$ and $\pi^{-1} \otimes \sigma^{\pi}_{i,\mathrm{even}}$. Examining these representations,

$$\begin{aligned}
\pi^{-1} \otimes \sigma^{\pi}_{i,\mathrm{even}} &\cong \pi^{-1} \otimes \left\{ \bigoplus_{k=m}^{i} \mathrm{Ind}_{N^{k}}^{U_F^{k}}(\pi) \right\} \\
&\cong \bigoplus_{k=m}^{i} \pi^{-1} \otimes \mathrm{Ind}_{N^{k}}^{U_F^{k}}(\pi) \\
&\cong \bigoplus_{k=m}^{i} \mathrm{Ind}_{N^{k}}^{U_F^{k}}(1) \\
&\cong \bigoplus_{k=m}^{i} r_{U^k} \circ N, \qquad (18)
\end{aligned}$$

where $r_{U^k}$ denotes the regular representation of the group $U^k = O^{\times}/1 + P^k$. Similarly,

$$\pi^{-1} \otimes \sigma^{\pi}_{i,\mathrm{odd}} \cong \bigoplus_{k=m}^{i-1} r_{U^k} \circ N. \tag{19}$$

The determination of the character $\det U_i^{\pi}$ is now straightforward. Since $\zeta$ is primitive modulo $P^i$, its image in each $U^k$ is a generator. So under the regular representation it acts as a cycle of length $\#U^k = (p-1)p^{k-1}$. As this length is even, $[\zeta]$ acts as an odd permutation in each $r_{U^k}$. As there are an odd number of $r_{U^k}$'s, $\det U_i^{\pi}[\zeta] = -1$.

Therefore, $\det u_{\pi}$ is the nontrivial character $\chi$, but all the $\det u_{\pi,i}$ are the trivial character. By Lemma 4 this completes the proof of Theorem 2 in the case of the unramified discrete series.

3.6. *The ramified discrete series representations.* Let $F$ now be one of the two ramified extensions of $\mathbf{Q}_p$. Choose a uniformizer $\tau$ in $O$ such that $\tau = N(\omega)$. Then $\mathrm{ord}_F(\omega) = 1$ and $\mathrm{ord}_F(\tau) = 2$. The norm map $N$ sends $O_F^{\times}$ *onto* $(O^{\times})^2$ and both $1 + P_F^{2i-1}$ and $1 + P_F^{2i}$ *onto* $1 + P^i$, for $i \geq 1$. This latter condition can be rewritten as

$$N(1 + P_F^k) = 1 + P^{[(k+1)/2]} \quad (k \geq 1),$$

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

where $[\cdot]$ denotes the greatest integer function. Again, $N$ will denote the elements of $O_F^\times$ of norm 1.

For the character $\pi$ of $F^\times$ let $m$ be the least positive integer such that $\pi$ is trivial on $1 + P_F^{2m-1}$.

LEMMA 9. *One always has $m \geq 2$.*

PROOF. If $m$ were 1, $\pi$ would be trivial on $1 + P_F$, and hence on $(1 + P_F)(O^\times)^2$ since this latter group consists of norms. But

$$[O_F^\times : (1 + P_F)(O^\times)^2] = [\mathbf{F}_p^\times : (\mathbf{F}_p^\times)^2] = 2,$$

so then $\pi(O_F^\times) \subseteq \mathbf{R}$, contrary to assumption. ∎

Starting with the representation space $D^\pi$ defined in Section 3.4, for each $i$ define the representation $U_i^\pi$ on the space ([9] p. 72)

$$D_i^\pi = \{\psi \in D^\pi \mid \operatorname{supp} \psi(a, \cdot) \subseteq O_F \text{ and } \psi(a, x + \xi) = \psi(a, x),$$
$$\text{for all } a \in O^\times, x \in O_F, \xi \in P_F^{2i-1}\}. \tag{20}$$

The decomposition into irreducibles follows the same pattern as in the unramified case: $\psi(t, x) \longmapsto \psi(\tau^{-1}t, x)$ embeds $D_{i-1}^\pi$ in $D_i^\pi$ as unitary $G$-representations. If $D_i^\pi$ is the orthogonal complement of $D_{i-1}^\pi$ in $D_i^\pi$, then the following theorem holds.

THEOREM 6 ([9], P. 79). *The representation space $D_m^\pi$ gives an irreducible representation $u_\pi$ of $G$ of dimension $p^m - p^{m-2}$. For $i > m$, the space $D_i^\pi$ gives an irreducible representation $u_{\pi,i}$ of dimension $p^i - p^{i-2}$.*

REMARK. The dimension of $D_i^\pi$ is

$$\dim D_i^\pi = p^i + p^{i-1} - p^{m-1} - p^{m-2}, \tag{21}$$

as can be seen by adding the dimensions of the spaces $D_i^\pi$.

We turn to the construction of a basis for $D_i^\pi$. As before, let $\zeta$ be a topological generator for $O^\times$.

PROPOSITION 3. *Let $S$ be a set of representatives for the $N$-orbits in*

$$\{\xi \in O_F / P_F^{2i-1} \mid \operatorname{ord}_F(\xi) \leq 2(i - m) + 1\}.$$

*Define a set of functions*

$$\{\psi_{(1,x)}, \psi_{(\zeta,x)} \mid x \in S\},$$

*where*

$$\psi_{(1,x)}(1, y) = \begin{cases} 1 & \text{if } y = x, \\ 0 & \text{if } y \neq x, y \in S; \end{cases} \tag{22}$$

$$\psi_{(1,x)}(\zeta, y) = 0 \quad \text{for all } y \in S, \tag{23}$$

*and where the $\psi_{(\zeta,x)}$ are defined by switching 1 and $\zeta$ on the lefthand side of the above formulas. Then the $\psi_{(1,x)}$ and $\psi_{(\zeta,x)}$ extend uniquely to functions in $D_i^\pi$ and this set of functions forms a basis.*

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

PROOF. We proceed as in the unramified case. Let $\psi$ be an arbitrary function in $D_i^\pi$. Recalling the transformation law,

$$\psi(t\gamma\bar{\gamma}, x) = \pi^{-1}(\gamma)\|\gamma\|^{1/2}\psi(t, \gamma x),$$

if one knows $\psi(a, x)$ for all $a \in O^\times$, $x \in O_F$, then one knows $\psi$. Indeed, since $\tau = N(\omega)$,

$$\psi(a\tau^n, x) = \psi(a\omega^n\bar{\omega}^n, x) = \pi^{-1}(\omega^n)\|\omega^n\|^{1/2}\psi(a, \omega^n x).$$

Moreover, since all squares in $O^\times$ are norms, it is clear from the transformation law that if one knows $\psi(1, x)$ and $\psi(\zeta, x)$ for all $x \in O_F$, then one knows $\psi$ completely.

Further, the two conditions

$$\psi(a, x + \xi) = \psi(a, x) \quad \text{for all } \xi \in P_F^{2i-1}, \tag{24}$$

$$\psi(a, \gamma x) = \pi(\gamma)\psi(a, x) \quad \text{for all } \gamma \in N, \tag{25}$$

imply that $\pi(\gamma) = 1$ whenever $\gamma x = x + \xi$ for some $\xi \in P_F^{2i-1}$, *i.e.*, we need $\pi$ trivial on $N \cap (1 + P_F^{2i-1-\mathrm{ord}_F(x)})$. The following two lemmas are now useful.

LEMMA 10. *The character $\pi$ is trivial on $1 + P_F^{2m-2}$.*

LEMMA 11. *The character $\pi$ is not trivial on $N \cap (1 + P_F^{2m-3})$.*

Proofs will follow the completion of the proof of the proposition. The two lemmas imply that $\psi(a, x) = 0$ unless $2i - 1 - \mathrm{ord}_F(x) \geq 2m - 2$. Rearranging, $\psi(a, x) = 0$ unless $\mathrm{ord}_F(x) \leq 2(i - m) + 1$. Putting the pieces together, to know some $\psi(t, x)$, it suffices to know its values $\psi(1, x)$, $\psi(\zeta, x)$ for each $x \in S$.

How many values are these?

If we let the number be $c$, by a similar argument as in the unramified case,

$$c = 2\sum_{j=0}^{2(i-m)+1} \frac{\#U_F^{2i-1-j}}{\#N^{2i-1-j}}.$$

Via the norm map, for $k \geq 1$,

$$U_F^k / N^k \cong (O^\times)^2 / (1 + P^{[(k+1)/2]}). \tag{26}$$

Substituting and rearranging gives

$$c = 2\sum_{k=2m-2}^{2i-1} \#(O^\times)^2 / (1 + P^{[(k+1)/2]}).$$

Considering that $\#O^\times / (1 + P^j) = (p - 1)p^{j-1}$,

$$\begin{aligned} c &= 2[(1/2)(p-1)(p^{m-2} + 2p^{m-1} + 2p^m + \cdots + 2p^{i-2} + p^{i-1})] \\ &= p^i + p^{i-1} - p^{m-1} - p^{m-2} \\ &= \dim D_i^\pi, \end{aligned}$$

where we have used Equation 21 for the second last line. This proves the proposition. ∎

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

PROOF OF LEMMA 10. First, two little results:

1. $N \cap (1 + P_F^{2m-1}) = N \cap (1 + P_F^{2m-2})$
2. $N(1 + P^{m-1}) = N(1 + P_F^{2m-2})$

The first follows from the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N \cap (1 + P_F^{2m-2}) & \longrightarrow & 1 + P_F^{2m-2} & \xrightarrow{N} & 1 + P^{m-1} & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & N \cap (1 + P_F^{2m-1}) & \longrightarrow & 1 + P_F^{2m-1} & \xrightarrow{N} & 1 + P^m & \longrightarrow & 1 \end{array}$$

noting that the last two vertical arrows are injections of subgroups of index $p$.

The second follows from the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & N(1 + P_F^{2m-2}) & \xrightarrow{N} & 1 + P^{m-1} & \longrightarrow & 1 \\ & & \| & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & N & \longrightarrow & N(1 + P^{m-1}) & \xrightarrow{N} & (1 + P^{m-1})^2 & \longrightarrow & 1 \end{array}$$

and the fact that $(1 + P^i)^2 = 1 + P^i$ for $i \geq 1$.

Now to prove the lemma. Since $\pi$ is trivial on $N \cap (1 + P_F^{2m-1})$, result 1 implies that $\pi$ is trivial on $N \cap (1 + P_F^{2m-2})$. Then $\pi$ is trivial on

$$[N \cap (1 + P_F^{2m-2})](1 + P^{m-1}),$$

since this latter group consists of norms. Using

$$[A \cap B]C = AC \cap B \quad \text{if } C \subseteq B,$$

this group is $N(1 + P^{m1}) \cap (1 + P_F^{2m-2})$. Now result 2 finishes the proof. ∎

PROOF OF LEMMA 11. Suppose $\pi$ were trivial on $N \cap (1 + P_F^{2m-3})$. Consider the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N \cap (1 + P_F^{2m-3}) & \longrightarrow & 1 + P_F^{2m-3} & \xrightarrow{N} & 1 + P^{m-1} & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \| & & \\ 1 & \longrightarrow & N \cap (1 + P_F^{2m-2}) & \longrightarrow & 1 + P_F^{2m-2} & \xrightarrow{N} & 1 + P^{m-1} & \longrightarrow & 1. \end{array}$$

One must have

$$[1 + P_F^{2m-3} : 1 + P_F^{2m-2}] = [N \cap (1 + P_F^{2m-3}) : N \cap (1 + P_F^{2m-2})],$$

which says that the map

$$N \cap (1 + P_F^{2m-3}) \longrightarrow (1 + P_F^{2m-3})/(1 + P_F^{2m-2}),$$

which has kernel $N \cap (1 + P_F^{2m-2})$, must be surjective. Thus, we have

$$1 + P_F^{2m-3} = [N \cap (1 + P_F^{2m-3})](1 + P_F^{2m-2}).$$

By Lemma 10, $\pi$ is trivial on the second group on the right side. Therefore our hypothesis implies that $\pi$ is also trivial on $1 + P_F^{2m-3}$, contrary to our choice of $m$. This proves the lemma. ∎

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

3.7. *Computations for the ramified discrete series.* As before, it suffices to compute $\det U_i^{\pi}[\zeta]$ for $i \geq m$. To begin, we calculate the action of $[\zeta]$ under $U_i^{\pi}$.

$$[\zeta]\psi(1,x) = \psi(\zeta,x) \tag{27}$$

$$[\zeta]\psi(\zeta,x) = \psi(\zeta^2,x) = \pi^{-1}(\zeta)\psi(1,\zeta x). \tag{28}$$

To determine the action of $[\zeta]$ with respect to our basis, it is helpful to define two subspaces:

$$V_1 = \mathbf{C}\text{-linear span of the } \psi_{(1,x)}$$
$$V_\zeta = \mathbf{C}\text{-linear span of the } \psi_{(\zeta,x)}$$

On each of these subspaces it is helpful to define an $O_F^\times$-representation as in the unramified case:

$$\psi(t,x) \overset{\beta}{\longmapsto} \psi(t,\beta x), \quad \forall \beta \in O_F^\times.$$

Reasoning similarly to the unramified case shows both $V_1$ and $V_\zeta$ are isomorphic to

$$\bigoplus_{j=0}^{2(i-m)+1} \mathrm{Ind}_{N^{2i-1-j}}^{U_F^{2i-1-j}}(\pi) = \bigoplus_{k=2m-2}^{2i-1} \mathrm{Ind}_{N^k}^{U_F^k}(\pi). \tag{29}$$

Let $x, y \in S$. Applying Equations 27 and 28,

$$[\zeta]\psi_{(1,x)}(1,y) = \psi_{(1,x)}(\zeta,y) = 0 \tag{30}$$

$$[\zeta]\psi_{(1,x)}(\zeta,y) = \pi^{-1}(\zeta)\psi_{(1,x)}(1,\zeta y) = \sigma_\zeta\psi_{(1,x)}(1,y) \tag{31}$$

$$[\zeta]\psi_{(\zeta,x)}(1,y) = \psi_{(\zeta,x)}(\zeta,y) = \delta_{xy} \tag{32}$$

$$[\zeta]\psi_{(\zeta,x)}(\zeta,y) = \pi^{-1}(\zeta)\psi_{(\zeta,x)}(1,\zeta y) = 0, \tag{33}$$

where $\sigma_\zeta$ acts on $V_1$ according to the formula

$$\sigma_\zeta\psi(1,\xi) = \pi^{-1}(\zeta)\psi(1,\zeta\xi), \quad \forall \xi \in O_F, \tag{34}$$

and where $\delta_{xy}$ is the Kronecker delta. If $\sigma_\zeta$ has the matrix $\Sigma_\zeta$ with respect to the $\psi_{(1,x)}$, then the matrix of $[\zeta]$ is a block matrix of the form

$$\left(\begin{array}{c|c} 0 & I \\ \hline \Sigma_\zeta & 0 \end{array}\right),$$

where the blocks are square of size $\dim V_1$. The determinant of this matrix is clearly $(-1)^{\dim V_1}\det\Sigma_\zeta$. Since

$$\dim D_i^{\pi} = p^i + p^{i-1}p^{m-1} - p^{m-2} = (p^{m-1} + p^{m-2})(p^{i-m+1} - 1),$$

and since $\dim V_1$ is half this number, $\dim V_1$ must be even. Hence, $(-1)^{dimV_1} = +1$. Thus, we are reduced to calculating the determinant of $\Sigma_\zeta$. To isolate $\Sigma_\zeta$, it is helpful to alter

https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

the action of $[\zeta]$ slightly. If after performing $[\zeta]$, one permutes the basis by interchanging $\psi_{(1,x)}$ and $\psi_{(\zeta,x)}$ for all $x \in S$, then the above calculation shows that the determinant of the new action is the same as that of the old. But now the matrix of the action is

$$\left(\begin{array}{c|c} \Sigma_\zeta & 0 \\ \hline 0 & I \end{array}\right),$$

where again the blocks are square of size $\dim V_1$. So $V_1$ is now an invariant subspace and restricting to this subspace gives $[\zeta]$ the matrix $\Sigma_\zeta$.

It is easy to identify the representation involved. By Equations 29 and 34, we see that $[\zeta]$ acts on $V_1$ through the representation

$$\pi^{-1} \otimes \bigoplus_{k=2m-2}^{2i-1} \mathrm{Ind}_{N^k}^{U_F^k}(\pi) = \bigoplus_{k=2m-2}^{2i-1} \mathrm{Ind}_{N^k}^{U_F^k}(1).$$

Now, $\mathrm{Ind}_{N^k}^{U_F^k}(1)$ is the regular representation of the group

$$U_F^k / N^k \cong (O^\times)^2 / (1 + P^{[(k+1)/2]}),$$

where the isomorphism is given by the norm map (*cf.* Equation 26). Note that $\zeta$ on the left corresponds to $\zeta^2$ on the right.

Since the group $(O^\times)^2/(1+P^{[(k+1)/2]})$ has order $(p-1)p^{[(k-1)/2]}/2$ for the $k$ we are considering, $\zeta^2$ acts as cycle of this length. So the determinant of $[\zeta]$ on $\mathrm{Ind}_{N^k}^{U_F^k}(1)$ is $(-1)^{1+(p-1)p^{[(k-1)/2]}/2}$. Hence, we obtain the result that

$$\det \Sigma_\zeta = \prod_{k=2m-2}^{2i-1} (-1)^{1+(p-1)p^{[(k-1)/2]}/2} = (-1)^e,$$

where

$$e = \sum_{k=2m-2}^{2i-1} \left(1 + (p-1)p^{[(k-1)/2]}/2\right) = 2i - 2m + \dim V_1.$$

As $\dim V_1$ is even, so is $e$, which shows that $\det U_i^\pi$, and hence $\det u_\pi$ and $\det u_{\pi,i}$, are all the trivial character. By Lemma 4, this completes the proof of Theorem 2. ∎

## References


1. P. Deligne, *Les constantes des équations fonctionelles des fonctions L*, Modular Functions of One Variable. II, Lecture Notes in Math. **349**(1973), 501–595.
2. ———, *Valeurs de fonctions L et périodes d'intégrales*, Proc. Sympos. Pure Math. (2) **XXXIII**(1979), 313–346.
3. R. Greenberg, *Non-vanishing of certain values of L-functions*, Analytic Number Theory and Diophantine Problems, Prog. in Math. **70**(1987), 223–235.
4. M. Harris, *Systematic growth of Mordell-Weil groups of abelian varieties in towers of number fields*, Invent. Math. **51**(1979), 123–141.
5. D. Rohrlich, *The vanishing of certain Rankin-Selberg convolutions*, Automorphic Forms and Analytic Number Theory, Publications CRM, Montreal, 1990, 123–133.


https://doi.org/10.4153/CJM-1997-037-7 Published online by Cambridge University Press

**6.** J.-P. Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou, 1969/70, **19**.
**7.** ———, *Local Fields*, Springer-Verlag, New York, 1979.
**8.** ———, *Propriétés des points d'ordre fini des courbes elliptiques*, Invent. Math. **15**(1972), 259–331.
**9.** A. Silberger, $PGL_2$ *over the p-adics*, Lecture Notes in Math. **166**(1970).
**10.** J. Tate, *Number Theoretic Background*, Proc. Sympos. Pure Math. (2) **XXXIII**(1979), 3–26.
**11.** André Weil, *Dirichlet Series and Automorphic Functions*, Lecture Notes in Math. **189**(1971).