COMPOSITIO MATHEMATICA

DAVID E. ROHRLICH

Jacobi sums and explicit reciprocity laws

Compositio Mathematica, tome 60, nº 1 (1986), p. 97-114

<http://www.numdam.org/item?id=CM_1986__60_1_97_0>

Compositio Mathematica 60: 97–114 (1986)

JACOBI SUMS AND EXPLICIT RECIPROCITY LAWS

David E. Rohrlich *

Let p be an odd prime and let $q = p^n$, where n is a positive integer. We write μ_q for the group of q-th roots of unity, K for the cyclotomic field $\mathbf{Q}(\mu_q)$, O for the ring of integers of K, and $\mathfrak{p}$ for the prime ideal of O lying above p. If $\mathfrak{l}$ is a nonzero prime ideal of O different from $\mathfrak{p}$ and x is an element of O relatively prime to $\mathfrak{l}$, then the q-th power norm residue symbol $(x/\mathfrak{l})$ is defined by the conditions

$$\left(\frac{x}{\mathfrak{l}}\right) \in \mu_q$$

and

$$\left(\frac{x}{\mathfrak{l}}\right) \equiv x^{(\mathbf{N}\mathfrak{l}-1)/q} \bmod \mathfrak{l},$$

where $\mathbf{N}$ denotes the absolute norm. Note in particular that the value of the symbol depends only on the residue class of x modulo $\mathfrak{l}$. Now let r and s be fixed rational integers; to avoid trivial cases we assume that

$$r,\ s, \text{ and } r+s \not\equiv 0 \bmod q.$$

The Jacobi sum associated to these data is

$$J(\mathfrak{l}) = -\sum_x \left(\frac{x}{\mathfrak{l}}\right)^r \left(\frac{1-x}{\mathfrak{l}}\right)^s,$$

where x runs over the residue classes of O modulo $\mathfrak{l}$, the classes of 0 and 1 being omitted. If $\mathfrak{a}$ is an arbitrary fractional ideal of K relatively prime to $\mathfrak{p}$, then we write $\mathfrak{a}$ as a product over prime ideals

$$\mathfrak{a} = \prod_{\mathfrak{l}} \mathfrak{l}^{n_{\mathfrak{l}}} \quad (n_{\mathfrak{l}} \in \mathbf{Z})$$

and put

$$J(\mathfrak{a}) = \prod_{\mathfrak{l}} J(\mathfrak{l})^{n_{\mathfrak{l}}}.$$

* Partially supported by an N.S.F. grant.

In this way J becomes a homomorphism from the group of fractional ideals of K relatively prime to $\mathfrak{p}$ into the multiplicative group K^* of K.

The fundamental fact about this homomorphism, proved by Weil [9], is that it is a Hecke character of K with conductor equal to a power of $\mathfrak{p}$. The exact value of the conductor is not known in general. Weil's proof shows that the conductor divides q^2, but subsequent work has provided more precise information (cf. Hasse [3], Jensen [5], Schmidt [6]). In particular, Hasse determined the conductor completely in the case $n = 1$ ([3], p. 63, Satz 2) and Jensen proved that the conductor divides $p\mathfrak{p}_1\mathfrak{p}_2$, where

$$\mathfrak{p}_\nu = \mathfrak{p}^{p^{n-\nu}} \quad (1 \leqslant \nu \leqslant n)$$

([5], p. 95, Satz 3a). We shall prove the following.

THEOREM: *The conductor of J divides $\mathfrak{p}_1^2$.*

As we shall see, there is always a pair (r, s) for which the conductor is precisely $\mathfrak{p}_1^2$. Nevertheless, it is possible for the conductor to be a proper divisor of $\mathfrak{p}_1^2$: thus the precise value of the conductor as a function of (r, s) remains to be determined. We return to this point at the end of the paper.

1. Let G denote the Galois group of K over $\mathbf{Q}$ and $\mathbf{Z}[G]$ its integral group ring; let $O_\mathfrak{p}$ be the completion of O at $\mathfrak{p}$ and $O_\mathfrak{p}^*$ the multiplicative group of $O_\mathfrak{p}$. What we need from Weil's paper [9] can be summarized in one sentence: There is an element Φ of $\mathbf{Z}[G]$ and a continuous homomorphism

$$\epsilon \colon O_\mathfrak{p}^* \to \mu_{2q}$$

such that for $\alpha \in K^* \cap O_\mathfrak{p}^*$ we have

$$J((\alpha)) = \epsilon(\alpha)\alpha^\Phi$$

(let (α) denote the principal ideal generated by α). The key point here is that the domain of ϵ is $O_\mathfrak{p}^*$ and that ϵ is continuous: if we were to suppress these features and view ϵ simply as a homomorphism from $K^* \cap O_\mathfrak{p}^*$ into μ_{2q}, then we would be asserting nothing more than a weak form of Stickelberger's theorem (which in its strong form gives an explicit formula for Φ in terms of r and s). Thus from our point of view, the essential content of Weil's theorem is that ϵ is trivial on some subgroup of $K^* \cap O_\mathfrak{p}^*$ of the form

$$K^* \cap \left(1 + \mathfrak{p}^k O_\mathfrak{p}\right) \quad (k \geqslant 1),$$

or equivalently, that ϵ extends to a continuous homomorphism from $O_{\mathfrak{p}}^*$ to μ_{2q}. Now let Ω be the group of roots of unity in $O_{\mathfrak{p}}^*$ of order dividing $p-1$. In view of the decomposition

$$O_{\mathfrak{p}}^* = \Omega \times (1 + \mathfrak{p}O_{\mathfrak{p}}),$$

we may write ϵ as a product

$$\epsilon = \kappa\lambda,$$

with continuous homomorphisms

$$\kappa\colon \Omega \to \mu_2$$

and

$$\lambda\colon 1 + \mathfrak{p}O_{\mathfrak{p}} \to \mu_q.$$

It is easy to see that κ is the Legendre symbol modulo $\mathfrak{p}$, but this fact will not be needed. To prove the theorem stated in the introduction, we must show that λ is trivial on the subgroup $1 + \mathfrak{p}_1^2 O_{\mathfrak{p}}$.

In order to accomplish this, we need two further properties of the Jacobi sum. The first property is the equivariance of the Jacobi sum with respect to the Galois group: for $\mathfrak{a}$ prime to $\mathfrak{p}$ and σ in G we have

$$J(\mathfrak{a}^\sigma) = J(\mathfrak{a})^\sigma,$$

as follows at once from the definitions. The second property is a congruence for the Jacobi sum due to Hasse. Let $\mathfrak{l}$ be a nonzero prime ideal of O different from $\mathfrak{p}$. Since $1-\xi$ is in $\mathfrak{p}$ for any $\xi \in \mu_q$, we have

$$\sum_x \left(1 - \left(\frac{x}{\mathfrak{l}}\right)^r\right)\left(1 - \left(\frac{1-x}{\mathfrak{l}}\right)^s\right) \equiv 0 \bmod \mathfrak{p}^2,$$

where x runs over a set of representatives for the residue classes of O modulo $\mathfrak{l}$, the classes of 0 and 1 being excluded. We write this congruence in the form

$$J(\mathfrak{l}) \equiv \sum_x 1 - \sum_x \left(\frac{x}{\mathfrak{l}}\right)^r - \sum_x \left(\frac{1-x}{\mathfrak{l}}\right)^s \bmod \mathfrak{p}^2$$

and substitute the values

$$\sum_x 1 = \mathbf{N}\mathfrak{l} - 2 \quad \text{and} \quad \sum_x \left(\frac{x}{\mathfrak{l}}\right)^r = \sum_x \left(\frac{1-x}{\mathfrak{l}}\right)^s = -1.$$

(To obtain the latter value, observe that the norm residue symbol ($/\mathfrak{l}$) defines a character of order q on the multiplicative group of $O/\mathfrak{l}$, and recall our assumption $r, s \not\equiv 0 \bmod q$.) Since q divides $\mathbf{N}\mathfrak{l} - 1$ we find

$$J(\mathfrak{l}) \equiv 1 \bmod \mathfrak{p}^2.$$

It follows that

$$J(\mathfrak{a}) \equiv 1 \bmod \mathfrak{p}^2$$

for arbitrary fractional ideals $\mathfrak{a}$ prime to $\mathfrak{p}$. This is Hasse's congruence (cf. [3], p. 61).

From these two properties of the Jacobi sum we deduce corresponding statements about λ.

PROPOSITION 1: *(i) For* $\sigma \in G$ *and* $\alpha \in K^* \cap (1 + \mathfrak{p}O_{\mathfrak{p}})$ *we have* $\lambda(\mathfrak{a}^\sigma) = \lambda(\mathfrak{a})^\sigma$.

(ii) For $\alpha \in K^* \cap (1 + \mathfrak{p}^2 O_{\mathfrak{p}})$ *we have* $\lambda(\alpha)^{p^{n-1}} = 1$.

PROOF: (i) Since $J((\alpha^\sigma)) = J((\alpha))^\sigma$ and $(\alpha^\sigma)^\Phi = (\alpha^\Phi)^\sigma$ we have $\epsilon(\alpha^\sigma) = \epsilon(\alpha)^\sigma$. But $K^* \cap (1 + \mathfrak{p}O_{\mathfrak{p}})$ is invariant under G and ϵ coincides with λ on this subgroup.

(ii) Following Hasse, we observe that his congruence gives

$$\epsilon(\alpha) \equiv \alpha^{-\Phi} \bmod \mathfrak{p}^2$$

for all α in $K^* \cap O_{\mathfrak{p}}^*$. If $\alpha \equiv 1 \bmod \mathfrak{p}$, then $\epsilon(\alpha) = \lambda(\alpha)$. If in addition $\alpha \equiv 1 \bmod \mathfrak{p}^2$, then $\alpha^\Phi \equiv 1 \bmod \mathfrak{p}^2$, whence

$$\lambda(\alpha) \equiv 1 \bmod \mathfrak{p}^2.$$

Now if ζ is a generator of μ_q, then $\zeta \not\equiv 1 \bmod \mathfrak{p}^2$. Hence $\lambda(\alpha)$ is not a generator of μ_q.

2. We now focus on the local aspects of the argument and change our notation accordingly, writing respectively K, O, and $\mathfrak{p}$ for the field $\mathbf{Q}_p(\mu_q)$, the ring of integers of this field, and the latter's maximal ideal. Also, we identify G with the Galois group of K over $\mathbf{Q}_p$, so that

$$\lambda : 1 + \mathfrak{p} \to \mu_q$$

is a continuous G-equivariant homomorphism by Proposition 1 (i).

We define the Hilbert symbol

$$(\ , \ ) : K^* \times K^* \to \mu_q$$

as follows: Given α, $\beta \in K^*$, let $\alpha^{1/q}$ denote an arbitrary q-th root of α, and let

$$\sigma_\beta = \left(\beta,\ K(\alpha^{1/q})/K\right)$$

be the local Artin symbol attached to β. Then

$$(\alpha,\ \beta) = (\alpha^{1/q})^{\sigma_\beta - 1}.$$

This is the normalization of the Hilbert symbol used by Iwasawa [4] (and the inverse of the normalization used by Artin-Tate [1]).

PROPOSITION 2: *There are integers a and b, uniquely determined modulo q, such that*

$$\lambda(\alpha) = \left(\alpha,\ p^a(1+p)^b\right) \quad (\alpha \in 1 + \mathfrak{p}).$$

PROOF: First we shall extend λ to a continuous G-equivariant homomorphism

$$\hat{\lambda}\colon K^* \to \mu_q.$$

Fix a generator ζ of μ_q, put $\pi = \zeta - \zeta^{-1}$, and let Π be the infinite cyclic group generated by π. Then K^* decomposes as a direct product

$$K^* = \Pi \times \Omega \times (1 + \mathfrak{p}),$$

where Ω is the group of roots of unity of order dividing $p-1$. Given $\alpha \in K^*$ with

$$\alpha = \pi^k \omega\beta \quad (k \in \mathbf{Z},\ \omega \in \Omega,\ \beta \in 1 + \mathfrak{p}),$$

we define

$$\hat{\lambda}(\alpha) = \lambda(\beta).$$

We must check that $\hat{\lambda}$ is equivariant. Now $\hat{\lambda}$ is certainly equivariant on O^*, because the decomposition $O^* = \Omega \times (1 + \mathfrak{p})$ is G-invariant. Thus it suffices to check that

$$\hat{\lambda}(\pi^\sigma) = \hat{\lambda}(\pi)^\sigma \quad (\sigma \in G),$$

or in other words, that

$$\hat{\lambda}(\pi^\sigma) = 1 \quad (\sigma \in G).$$

But

$$\hat{\lambda}(\pi^\sigma) = \hat{\lambda}(\pi)\hat{\lambda}(\pi^\sigma/\pi) = \hat{\lambda}(\pi^\sigma/\pi),$$

and π^σ/π belongs to O^*, on which $\hat{\lambda}$ is already known to be equivariant. Letting $\tau \in G$ be the automorphism which takes ζ to ζ^{-1}, we have

$$(\pi^\sigma/\pi)^\tau = \pi^\sigma/\pi$$

and therefore

$$\hat{\lambda}(\pi^\sigma/\pi)^\tau = \hat{\lambda}(\pi^\sigma/\pi).$$

Since $\hat{\lambda}(\pi^\sigma/\pi)$ is a q-th root of unity, it follows that $\hat{\lambda}(\pi^\sigma/\pi) = 1$, as required.

We note in passing that the extension $\hat{\lambda}$ is unique. Indeed, suppose that $\tilde{\lambda}$ is another G-equivariant extension of λ. Since Ω has order prime to p, we see that $\hat{\lambda}$ and $\tilde{\lambda}$ coincide on O^*, and in particular, that

$$\tilde{\lambda}(\pi^\sigma/\pi) = \hat{\lambda}(\pi^\sigma/\pi) = 1 \quad (\sigma \in G).$$

Then the relation

$$\tilde{\lambda}(\pi)^\sigma/\tilde{\lambda}(\pi) = \tilde{\lambda}(\pi^\sigma/\pi) = 1 \quad (\sigma \in G)$$

shows that $\tilde{\lambda}(\pi)$ is invariant under G, whence $\tilde{\lambda}(\pi) = 1$.

Now we apply local class field theory and Kummer theory: every character $K^* \to \mu_q$ has the form $\alpha \mapsto (\alpha, \beta)$ for some $\beta \in K^*$. Writing

$$\hat{\lambda}(\alpha) = (\alpha, \beta)$$

and using the equivariance of $\hat{\lambda}$, we find

$$(\alpha^\sigma, \beta) = (\alpha, \beta)^\sigma = (\alpha^\sigma, \beta^\sigma) \quad (\sigma \in G),$$

whence $(\alpha, \beta^{\sigma-1}) = 1$ for all $\alpha \in K^*$. It follows that $\beta^{\sigma-1}$ is a q-th power in K^*. Choosing σ to be a generator of G and writing

$$\beta^{\sigma-1} = \gamma^q$$

with $\gamma \in K^*$, we see that

$$N_{K/\mathbf{Q}_p}(\gamma)^q = 1,$$

where N denotes norm. Thus

$$N_{K/\mathbf{Q}_p}(\gamma) = 1.$$

Then $\gamma = \delta^{\sigma-1}$ for some $\delta \in K^*$, so that

$$(\beta/\delta^q)^{\sigma-1} = 1$$

and

$$\beta \in \delta^q \mathbf{Q}_p^*.$$

Since $\mathbf{Q}_p^*$ is generated modulo q-th powers by the cosets of p and $1+p$, we conclude that there are integers a and b such that

$$\hat{\lambda}(\alpha) = \left(\alpha,\ p^a(1+p)^b\right).$$

Finally, suppose that for some integers c and d we have

$$\left(\alpha,\ p^c(1+p)^d\right) = 1$$

for all $\alpha \in 1 + \mathfrak{p}$. We must show that q divides c and d. From the uniqueness of the extension $\hat{\lambda}$, we deduce that the above equation holds for all $\alpha \in K^*$, whence $p^c(1+p)^d$ is a q-th power in K^*. Now the natural map

$$\mathbf{Q}_p^*/\mathbf{Q}_p^{*q} \to K^*/K^{*q}$$

is injective (the Galois cohomology group $H^1(G, \mu_q)$ is trivial), and p and $1+p$ represent multiplicatively independent elements of order q in $\mathbf{Q}_p^*/\mathbf{Q}_p^{*q}$. Hence q divides c and d and the proposition is proved.

3. The following proposition completes the proof of the theorem.

PROPOSITION 3: (*i*) *The conductor of the character* $\alpha \mapsto (\alpha, 1+p)$ *divides* $\mathfrak{p}_1^2$.

(*ii*) *The conductor of the character* $\alpha \mapsto (\alpha, p^p)$ *divides* $\mathfrak{p}_1^2$.

(*iii*) *We have* $a \equiv 0 \bmod p$.

PROOF: (i) This statement is a step in the proof of Iwasawa's explicit reciprocity laws (see [4], p. 162, remark following Theorem 2).

(ii) Let ζ be a generator of μ_q and put $\pi = 1 - \zeta$ (note the change in notation). We apply one of Iwasawa's explicit reciprocity laws ([4], p. 162), according to which

$$(\alpha, \beta) = \zeta^{-q^{-1}\operatorname{Tr}(\zeta\alpha^{-1}(d\alpha/d\pi)\log\beta)}$$

for $\alpha \in K^*$ and $\beta \in 1 + \mathfrak{p}_1^2$. Here log is the p-adic logarithm and Tr denotes the trace from K to $\mathbf{Q}_p$. The derivative $d\alpha/d\pi$ stands for $g'(\pi)$, where

$$g(X) = \sum_{m \geqslant k} c_m X^m$$

is any formal Laurent series with the following properties:

(1) $c_m \in \mathbf{Z}_p$ for $m \geqslant k$,
(2) $c_k \in \mathbf{Z}_p^*$,
(3) $g(\pi) = \alpha$.

Of course, the value of $d\alpha/d\pi$ depends on the choice of g. Now if g is an admissible power series for $\alpha = p$, then

$$h(X) = 1 + g(X)$$

is an admissible power series for $\alpha = 1 + p$, and $g'(\pi) = h'(\pi)$. Hence with a suitable interpretation of the derivatives we have

$$p\left(p^{-1}\frac{d}{d\pi}p\right) = (1+p)\left((1+p)^{-1}\frac{d}{d\pi}(1+p)\right).$$

Applying Iwasawa's formula, we see that for $\beta \in 1 + \mathfrak{p}_1^2$,

$$(p, \beta)^p = (1+p, \beta)^{1+p},$$

whence

$$(\beta, p^p) = (\beta, 1+p)^{1+p}.$$

Thus (ii) follows from (i).

(iii) Let ζ and π be as in the proof of (ii). We make the preliminary remark that $(\zeta, p) = 1$. This follows, for example, from the formula

$$(\pi, \beta) = \zeta^{-q^{-1}\operatorname{Tr}(\zeta\pi^{-1}\log\beta)} \quad (\beta \in 1 + \mathfrak{p}),$$

which is one of the explicit reciprocity laws of Artin-Hasse (cf. [4], p.

151). Indeed, since $\log \zeta = 0$, we have $(\pi, \zeta) = 1$, whence $(\pi, \zeta^{\sigma}) = 1$ for every $\sigma \in G$ (every conjugate of ζ is a power of ζ). Then

$$(p, \zeta) = \prod_{\sigma \in G} (\pi^{\sigma}, \zeta) = \prod_{\sigma \in G} \left(\pi, \zeta^{\sigma^{-1}}\right)^{\sigma} = 1,$$

as claimed.

To prove (iii), we note that the character $\alpha \mapsto (\alpha, p)$ on $1 + \mathfrak{p}$ has order q (and not a proper divisor of q): this is implicit in the uniqueness of a modulo q (Proposition 2). Hence there exists $\alpha \in 1 + \mathfrak{p}$ such that (α, p) is a primitive q-th root of unity. Now for some j $(1 \leqslant j \leqslant p)$ we have $\zeta^j \alpha \in 1 + \mathfrak{p}^2$, and in view of our preliminary remark, $(\zeta^j \alpha, p)$ is still a primitive q-th root of unity. Hence without loss of generality, $\alpha \in 1 + \mathfrak{p}^2$.

By Proposition 1 (ii),

$$\left(\alpha, p^a(1+p)^b\right)^{p^{n-1}} = 1,$$

whence

$$(\alpha, p)^{ap^{n-1}} = \left(\alpha^{p^{n-1}}, 1+p\right)^{-b}.$$

Thus by (i) it suffices to show that

$$\alpha^{p^{n-1}} \in 1 + \mathfrak{p}_1^2.$$

Write

$$\alpha = 1 + \pi^2 \beta$$

with β in O. Then

$$\alpha^{p^{n-1}} \equiv 1 + \pi^{2p^{n-1}} \beta^{p^{n-1}} \bmod pO.$$

Since

$$pO = \mathfrak{p}^{(p-1)p^{n-1}} \subset \mathfrak{p}^{2p^{n-1}}$$

we obtain

$$\alpha^{p^{n-1}} \equiv 1 \bmod \mathfrak{p}^{2p^{n-1}},$$

as desired.

4. We would still like to show that there is a pair (r, s) for which the conductor is precisely $\mathfrak{p}_1^2$. In preparation for this we prove the following proposition.

PROPOSITION 4: *If* $n \geqslant 2$, *then the conductor of the character* $\alpha \mapsto (\alpha, p^p)$ *is* $\mathfrak{p}_1^2$.

PROOF: We shall prove the proposition by induction on n, and therefore, for the duration of this proof only, we adjust our notation by adding a subscript n. Thus for $n \geqslant 1$, K_n is the extension of $\mathbf{Q}_p$ obtained by adjoining the p^n-th roots of unity, O_n is the ring of integers of K_n, and $\mathfrak{p}_n$ is the maximal ideal of O_n. The new meaning for $\mathfrak{p}_1$ is essentially compatible with the old, but to be completely consistent, we should reformulate the proposition as follows: If $n \geqslant 2$, then the conductor of the character $\alpha \mapsto (\alpha, p^p)_n$ is $\mathfrak{p}_1^2 O_n$.

Let ζ_n be a primitive p^n-th root of unity and put $\pi_n = 1 - \zeta_n$. Since the conductor of $\alpha \mapsto (\alpha, p^p)_n$ is already known to divide $\mathfrak{p}_1^2 O_n$ (Proposition 3 (ii)), it will suffice to show that for $n \geqslant 2$ there exists $\beta \in O_n$ with

$$\left(\exp\left(\pi_1^2 \pi_n^{-1} \beta\right),\ p^p\right)_n \neq 1,$$

where exp is the p-adic exponential function. Equivalently, we must show that there exists $\beta \in O_n$ with

$$\left(\exp\left(p \pi_1^2 \pi_n^{-1} \beta\right),\ p\right)_n \neq 1.$$

The latter formulation is meaningful even for $n = 1$, and we begin by proving it in this case.

Choose $\alpha \in 1 + \mathfrak{p}_1$ so that $(\alpha, p)_1 \neq 1$. As in the proof of Proposition 3 (iii), after multiplying α by some p-th root of unity, we may assume that $\alpha \in 1 + \mathfrak{p}_1^2$. Let G_1 be the Galois group of K_1 over $\mathbf{Q}_p$, and let

$$\omega\colon G_1 \to \Omega$$

be the character giving the action of G_1 on p-th roots of unity:

$$\zeta_1^\sigma = \zeta_1^{\omega(\sigma)} \quad (\sigma \in G_1).$$

Then

$$(\alpha^\sigma,\ p)_1 = (\alpha,\ p)_1^\sigma = (\alpha,\ p)_1^{\omega(\sigma)}.$$

Therefore, if we put

$$\theta = (p-1)^{-1} \sum_{\sigma \in G_1} \omega(\sigma)^{-1} \sigma \in \mathbf{Z}_p[G_1],$$

then we have

$$(\alpha^{\theta},\ p)_1 = (\alpha,\ p)_1.$$

Hence after replacing α by α^{θ}, we may assume that $(\alpha,\ p)_1 \neq 1$, that $\alpha \in 1 + \mathfrak{p}_1^2$, and in addition, that

$$\alpha^{\sigma} = \alpha^{\omega(\sigma)}$$

for $\sigma \in G_1$.

Now write

$$\alpha = \exp\left(\pi_1^j \gamma\right)$$

with $j \geqslant 2$ and $\gamma \in O_1^*$. The last equation of the preceding paragraph gives

$$\pi_1^{\sigma j} \gamma^{\sigma} = \omega(\sigma) \pi_1^j \gamma,$$

whence

$$(\pi_1^{\sigma}/\pi_1)^j = \omega(\sigma)\gamma/\gamma^{\sigma}$$

and

$$\omega(\sigma)^j \equiv \omega(\sigma) \bmod \mathfrak{p}_1.$$

(Observe that $\gamma^{\sigma} \equiv \gamma \bmod \mathfrak{p}_1$ and that $\pi_1^{\sigma}/\pi_1 = 1 + \zeta_1 + \cdots + \zeta_1^{k-1}$, where k is the smallest positive integer congruent to $\omega(\sigma)$ modulo p.) Choosing σ to be a generator of G_1, we deduce that $j-1$ is a multiple of $p-1$, whence $j \geqslant p$. Thus if we put

$$\beta = \pi_1^{j-1}\gamma/p,$$

then $\beta \in O_1$, and

$$\exp(p\pi_1\beta) = \exp\left(\pi_1^j\gamma\right) = \alpha.$$

So $(\exp(p\pi_1\beta),\ p)_1 \neq 1$, as desired.

Before proving the inductive step, we make some observations. First note that the relative different ideal of K_{n+1} over K_n is generated by p: indeed, the different is multiplicative in towers, and the different of K_{ν} over $\mathbf{Q}_p$ is generated by p^{ν}/π_1. Now let $\mathrm{Tr}_{n+1,n}$ denote the trace from K_{n+1} to K_n. We claim that

$$\mathrm{Tr}_{n+1,n}\left(O_{n+1}\pi_n\pi_{n+1}^{-1}p^{-1}\right) = O_n.$$

Since p generates the relative different of K_{n+1} over K_n, the left-hand side is at least contained in O_n, and is therefore equal to an ideal of O_n. If

$$\mathrm{Tr}_{n+1,n}\left(O_{n+1}\pi_n\pi_{n+1}^{-1}p^{-1}\right)\subset\pi_n O_n,$$

then

$$\mathrm{Tr}_{n+1,n}\left(O_{n+1}\pi_{n+1}^{-1}p^{-1}\right)\subset O_n,$$

and this contradicts the fact that p generates the relative different. Hence $\mathrm{Tr}_{n+1,n}(O_{n+1}\pi_n\pi_{n+1}^{-1}p^{-1})$ is not contained in the maximal ideal of O_n, and equality holds as claimed.

Now we assume the inductive hypothesis: for some integer $n\geqslant 1$ there exists $\beta\in O_n$ such that

$$\left(\exp\left(p\pi_1^2\pi_n^{-1}\beta\right),\ p\right)_n\neq 1.$$

Choosing $\gamma\in O_{n+1}$ so that

$$\mathrm{Tr}_{n+1,n}\left(\gamma\pi_n\pi_{n+1}^{-1}p^{-1}\right)=\beta,$$

and writing $N_{n+1,n}$ for the norm from K_{n+1} to K_n, we have

$$\begin{aligned}\left(\exp\left(p\pi_1^2\pi_{n+1}^{-1}\gamma\right),\ p\right)_{n+1}&=\left(\exp\left(\pi_1^2\pi_{n+1}^{-1}\gamma\right),\ p^p\right)_{n+1}\\&=\left(N_{n+1,n}\left(\exp\left(\pi_1^2\pi_{n+1}^{-1}\gamma\right)\right),\ p\right)_n\\&=\left(\exp\left(\pi_1^2\ \mathrm{Tr}_{n+1,n}\left(\pi_{n+1}^{-1}\gamma\right)\right),\ p\right)_n\\&=\left(\exp\left(p\pi_1^2\pi_n^{-1}\beta\right),\ p\right)_n.\end{aligned}$$

Therefore

$$\left(\exp\left(p\pi_1^2\pi_{n+1}^{-1}\gamma\right),\ p\right)_{n+1}\neq 1,$$

as desired.

5. We return to global considerations and to the corresponding notational conventions. In order to indicate the dependence of J on the pair $(r,\ s)$ we write $J_{r,s}$ instead of J.

PROPOSITION 5: *There is an integer s such that* $J_{1,s}$ *has conductor* $\mathfrak{p}_1^2$. *If* $n=1$ *or* 2, *then s may be chosen to satisfy* $1\leqslant s\leqslant p-2$, *and if* $n\geqslant 3$, *then s may be chosen to satisfy* $1\leqslant s\leqslant p-1$.

PROOF: In the case $n = 1$, this was proved by Hasse ([3], p. 64). Hence we assume that $n \geqslant 2$. We shall deduce the proposition from a well-known relation of Davenport-Hasse, which we write in the form

$$\prod_{k=1}^{p-1} J_{1,p^{n-1}k}(\mathfrak{a}) = \left(\frac{p^p}{\mathfrak{a}}\right) \prod_{k=1}^{p-1} J_{1,k}(\mathfrak{a})$$

(cf. [2], formulas (0.6) and (0.9_2)). Here $\mathfrak{a}$ is an arbitrary fractional ideal of K relatively prime to $\mathfrak{p}$, and $(\ /\mathfrak{a})$ is the q-th power norm residue symbol, defined for prime $\mathfrak{a}$ as in the introduction and extended to arbitrary $\mathfrak{a}$ by complete multiplicativity. Now in the case where $\mathfrak{a}$ is a principal ideal (α), the reciprocity law for the norm residue symbol shows that

$$\left(\frac{p}{(\alpha)}\right) = (\alpha,\ p),$$

(See [1], p. 172, Theorem 14. One consequence, incidentally, is that $(\zeta,\ p) = 1$, as we have already seen by a different method.) In particular, it follows from Proposition 4 that the conductor of the Hecke character $\mathfrak{a} \mapsto (p^p/\mathfrak{a})$ is $\mathfrak{p}_1^2$. On the other hand, the conductor of each $J_{1,s}$ divides $\mathfrak{p}_1^2$. Hence we conclude from the Davenport-Hasse relation that for at least one integer s satisfying

$$s = p^{n-1}k \quad (1 \leqslant k \leqslant p-1) \text{ or } 1 \leqslant s \leqslant p-1,$$

the conductor of $J_{1,s}$ is precisely $\mathfrak{p}_1^2$. To complete the proof of the proposition, it will suffice to show that the conductor of $J_{1,p^{n-1}k}$ is a proper divisor of $\mathfrak{p}_1^2$, and that for $n = 2$, the conductor of $J_{1,p-1}$ is also a proper divisor of $\mathfrak{p}_1^2$. Using an argument of Hasse, we shall prove instead the following statement, which contains both of the preceding ones: If one of the integers r, s and $r + s$ is congruent to 0 modulo p^{n-1}, then the conductor of $J_{r,s}$ divides $\mathfrak{p}_1\mathfrak{p}$.

In proving this assertion we may assume, say, that $s \equiv 0 \bmod p^{n-1}$, because $J_{r,s} = J_{s,r}$ and $J_{r,s} = J_{r,-s-r}$. (To verify these identities write

$$J_{r,s}(\mathfrak{l}) = -\sum_x \left(\frac{x}{\mathfrak{l}}\right)^r \left(\frac{1-x}{\mathfrak{l}}\right)^s$$

with a prime ideal $\mathfrak{l}$, and make the substitutions $x \mapsto 1 - x$ and $x \mapsto -x/(1-x)$ respectively, noting in the latter case that $(-1/\mathfrak{l}) = 1$.) Now for $s \equiv 0 \bmod p^{n-1}$, the congruence of Hasse recalled in Section 1 takes the stronger form

$$J_{r,s}(\mathfrak{a}) \equiv 1 \bmod \mathfrak{p}_1\mathfrak{p}$$

(cf. [3], p. 61): the proof is the same as before, except that now

$$\left(1-\left(\frac{x}{\mathfrak{l}}\right)^{r}\right)\left(1-\left(\frac{1-x}{\mathfrak{l}}\right)^{s}\right)\equiv 0 \bmod \mathfrak{p}_1\mathfrak{p},$$

because $(1-x/\mathfrak{l})^s$ is a p-th root of unity. In particular, for a principal ideal $\mathfrak{a}=(\alpha)$ Hasse's congruence gives

$$\epsilon_{r,s}(\alpha)\equiv\alpha^{-\Phi_{r,s}} \bmod \mathfrak{p}_1\mathfrak{p},$$

and if $\alpha\equiv 1 \bmod \mathfrak{p}_1\mathfrak{p}$, then

$$\lambda_{r,s}(\alpha)\equiv 1 \bmod \mathfrak{p}_1\mathfrak{p}.$$

Since $\lambda_{r,s}(\alpha)$ is a q-th root of unity, it follows that $\lambda_{r,s}(\alpha)=1$. Therefore the conductor of $J_{r,s}$ divides $\mathfrak{p}_1\mathfrak{p}$, as claimed.

6. In conclusion, we would like to draw attention to a problem which we have not discussed so far: the calculation of the integers a and b modulo q.

The calculation of b presents no difficulties. If j is an integer relatively prime to q, let $\sigma(j)$ be the element of G satisfying

$$\xi^{\sigma(j)}=\xi^{j}\quad(\xi\in\mu_q),$$

and for any integer t, let $\langle t\rangle$ be the integer satisfying

$$t\equiv\langle t\rangle \bmod q\quad\text{and } 0\leqslant\langle t\rangle\leqslant q-1.$$

Stickelberger's theorem provides the following explicit formula for the infinity type Φ of J:

$$\Phi=\sum_{j}\left(\left(\langle jr\rangle+\langle js\rangle-\langle j(r+s)\rangle\right)/q\right)\sigma(-j)^{-1},$$

where j runs over a set of representatives for the invertible residue classes modulo q. Let w be an integer satisfying

$$w\equiv-\sum_{j}\left(\left(\langle jr\rangle+\langle js\rangle-\langle j(r+s)\rangle\right)/q\right)j^{-1} \bmod q,$$

and let ζ be a primitive q-th root of unity. Since ζ generates the unit ideal, we have $J((\zeta))=1$; on the other hand,

$$J((\zeta))=\epsilon(\zeta)\zeta^{\Phi}=\lambda(\zeta)\zeta^{\Phi}=\left(\zeta,\ p^{a}(1+p)^{b}\right)\zeta^{w},$$

whence

$$\left(\zeta,\ p^a(1+p)^b\right)=\zeta^{-w}.$$

Now we have already seen in the proofs of Propositions 3 and 5 that $(\zeta,\ p)=1$. We also have, either by the explicit formulas of Artin-Hasse or by the global reciprocity law applied to the extension $\mathbf{Q}(\mu_{q^2})$ over $\mathbf{Q}(\mu_q)$,

$$(\zeta, 1+p)=\zeta^{(p-1)\log(1+p)/p}.$$

(To derive this from the global reciprocity law, use the congruence

$$\left((1+p)^{p^{n-1}(p-1)}-1\right)/q\equiv(p-1)\log(1+p)/p \bmod q,$$

which is elementary.) Putting these facts together, we obtain

$$b\equiv-\frac{pw}{(p-1)\log(1+p)} \bmod q,$$

and thus we have calculated b modulo q.

The calculation of a modulo q probably depends on properties of the curve

$$y^q=x^r(1-x)^s.$$

Here we shall treat only the special case $r=s=1$. Let C be a smooth model over $\mathbf{Q}$ of the hyperelliptic curve

$$y^q=x(1-x),$$

and let A be the Jacobian variety of C; let $A[2]$ be the group of points on A which are annihilated by 2. If we identify A with the group of divisor classes of degree 0 on C, then $A[2]$ is the subgroup of A generated by divisor classes of the form $[P-Q]$, where P and Q run over the fixed points of the hyperelliptic involution of C. Now relative to the equation $y^q=x(1-x)$, the hyperelliptic involution of C has the form $(x,\ y)\mapsto(1-x,\ y)$, and its fixed points are

$$\left(1/2,\ \zeta^j 4^{-1/q}\right),\quad 1\leqslant j\leqslant q, \text{ and } (1,0,0).$$

Putting $K=\mathbf{Q}(\mu_q)$ and $L=K(2^{1/q})$, we conclude that every point of $A[2]$ is rational over L.

The next step is a standard application of ℓ-adic representations. The abelian variety A is of complex multiplication type, and therefore, for every rational prime ℓ, the Tate module $T_\ell(A)$ affords a representation

$$\rho_\ell\colon \mathrm{Gal}(L_{\mathrm{ab}}/L) \to GL(\mathbf{Q}_\ell \otimes T_\ell(A)),$$

where L_{ab} is an abelian closure of L. After choosing a basis for $T_\ell(A)$ over $\mathbf{Z}_\ell$, we may view ρ_ℓ as a map

$$\rho_\ell\colon \mathrm{Gal}(L_{\mathrm{ab}}/L) \to GL_{2g}(\mathbf{Z}_\ell),$$

with $g = (q-1)/2$. Since $A[2]$ is pointwise rational over L, the image of ρ_2 is contained in the subgroup

$$\left\{ S \in GL_{2g}(\mathbf{Z}_2)\colon\ S \equiv \text{identity matrix mod } 2 \right\},$$

and therefore the image of ρ_2^2 is contained in the subgroup

$$\left\{ S \in GL_{2g}(\mathbf{Z}_2)\colon\ S \equiv \text{identity matrix mod } 4 \right\}.$$

In particular, the image of ρ_2^2 is torsion-free. On the other hand, since A has potential good reduction ([7], p. 503), the image under ρ_2^2 of the inertia group of any prime above $\mathfrak{p}$ is finite, and therefore trivial (since torsion-free). We conclude that ρ_2^2 is unramified at the primes above $\mathfrak{p}$.

Let us now return to the Hecke character $\mathfrak{a} \mapsto J(\mathfrak{a})$, with $r = s = 1$. Since J is a Hecke character of K of type A_0, it determines an ℓ-adic representation of $\mathrm{Gal}(K_{\mathrm{ab}}/K)$, and according to theorems of Davenport-Hasse [2] and Weil [8], this representation is a direct summand of the representation of $\mathrm{Gal}(K_{\mathrm{ab}}/K)$ on $\mathbf{Q}_\ell \otimes T_\ell(A)$. It follows that the ℓ-adic representation of $\mathrm{Gal}(L_{\mathrm{ab}}/L)$ determined by $J \circ N_{L/K}$ is a direct summand of the representation ρ_ℓ considered above. In particular, the Hecke character $(J \circ N_{L/K})^2$ is unramified at every prime of L above $\mathfrak{p}$. Let $\mathfrak{P}$ be a prime of L above $\mathfrak{p}$, and let $L_{\mathfrak{P}}$ be the completion of L at $\mathfrak{P}$. Then for every $\alpha \in L_{\mathfrak{P}}$ such that

$$N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha) \in 1 + \mathfrak{p}O_{\mathfrak{p}},$$

we have

$$\lambda\left(N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha)\right) = 1,$$

or in other words,

$$\left(N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha),\ p^a(1+p)^b\right) = 1.$$

At this point we observe that

$$L_{\mathfrak{P}} = K_{\mathfrak{p}}(2^{1/q}) = K_{\mathfrak{p}}(2^{(p-1)/q}) \subset K_{\mathfrak{p}}\big((1+p)^{1/q}\big).$$

(The group $1 + p\mathbf{Z}_p$ is generated by $1+p$ topologically.) Denoting the norm from $K_{\mathfrak{p}}((1+p)^{1/q})$ to $K_{\mathfrak{p}}$ simply by N, we deduce that if $\alpha \in K_{\mathfrak{p}}((1+p)^{1/q})$ satisfies

$$N(\alpha) \in 1 + \mathfrak{p}O_{\mathfrak{p}},$$

then

$$\big(N(\alpha),\ p^a(1+p)^b\big) = 1.$$

Now the kernel of the character $\beta \mapsto (\beta, 1+p)$ (viewed as a character of $1 + \mathfrak{p}O_{\mathfrak{p}}$) is

$$N\big(K_{\mathfrak{p}}\big((1+p)^{1/q}\big)\big) \cap (1 + \mathfrak{p}O_{\mathfrak{p}}),$$

by the local reciprocity law. Hence the kernel of $\beta \mapsto (\beta,\ p^a(1+p)^b)$ contains the kernel of $\beta \mapsto (\beta, 1+p)$, and therefore the former character is a power of the latter. On the other hand, the characters $\beta \mapsto (\beta, p)$ and $\beta \mapsto (\beta, 1+p)$ are multiplicatively independent modulo q-th powers: this is implicit in the uniqueness of a and b modulo q (Proposition 2). It follows that

$$a \equiv 0 \bmod q,$$

and thus we have computed a modulo q in the special case $r = s = 1$.

It remains to compute a modulo q in general. Once this is accomplished, we will have a formula which expresses the value of a Jacobi sum at a principal ideal explicitly in terms of Hilbert symbols. Questions about the conductor will then reduce to questions about the explicit reciprocity laws.

References

[1] A. Artin and J. Tate: *Class Field Theory*. Benjamin (1967).

[2] H. Davenport and H. Hasse: Die Nullstellen der Krongruenzzetafunktionen in gewissen zyklischen Fällen. *J. reine angew. Math.*, 172 (1934) 151–182.

[3] H. Hasse: Zetafunktion und L-Funktionen zu einem arithmetischen Funktionenkörper vom Fermatschen Typus. Abhand. der Deut. Akad. der Wissen. zu Berlin (1955).

[4] K. Iwasawa: On explicit formulas for the norm residue symbol. *J. Math. Soc. Japan*, 20 (1968) 151–165.

[5] C. Jensen: Über die Führer einer Klasse Heckescher Grössencharaktere. *Math. Scand.*, 8 (1960) 81–96.

[6] C.-G. Schmidt: Über die Führer von Gauss'schen Summen als Grössencharaktere. *J. Number Theory*, 12 (1980) 283–310.
[7] J.-P. Serre and J. Tate: Good reduction of abelian varieties. *Ann. of Math.*, 88 (1968) 492–517.
[8] A. Weil: Number of solutions of equations in finite fields. *Bull. AMS*, 55 (1949) 497–508.
[9] A. Weil: Jacobi sums as Grössencharaktere. *Trans. AMS*, 73 (1952) 487–495.

(Oblatum 31-V-1985)

D.E. Rohrlich
Department of Mathematics
Rutgers University
New Brunswick, NJ 08903
USA

Added in proof

A complete solution to the problem has been obtained by R. Coleman and W. McCallum (to appear).