COMPOSITIO MATHEMATICA

RALPH GREENBERG

On the jacobian variety of some algebraic curves

Compositio Mathematica, tome 42, nº 3 (1980), p. 345-359

<http://www.numdam.org/item?id=CM_1980__42_3_345_0>

COMPOSITIO MATHEMATICA, Vol. 42, Fasc. 3, 1981, pag. 345–359

ON THE JACOBIAN VARIETY OF SOME ALGEBRAIC CURVES

Ralph Greenberg*

1. Introduction

Let p be a prime and let F be a field of characteristic different from p. We will assume throughout this paper that $p \geq 5$ and that F contains a primitive p-th root of unity. For any integer a such that $1 \leq a \leq p-2$, let J_a denote the Jacobian variety of the curve $y^p = x^a(1-x)$ over F. In this paper we will prove several results about the points of p-power order on J_a. Our most interesting results will concern the case when F is $\boldsymbol{Q}(\sqrt[p]{1})$ or $\boldsymbol{Q}_p(\sqrt[p]{1})$, where $\boldsymbol{Q}$ denotes the rational numbers and $\boldsymbol{Q}_p$ the p-adic numbers. However, we will begin by stating two general results. We let $\bar{F}$ denote a fixed algebraic closure of F.

THEOREM 1: *The group $J_a(F)$ of F-rational points on J_a contains a subgroup isomorphic to $(\boldsymbol{Z}/(p))^3$.*

THEOREM 2: *Let $F_\infty^{(a)}$ denote the field generated by all points of p-power order on $J_a(\bar{F})$. Then $\mathrm{Gal}(F_\infty^{(a)}/F) \cong \boldsymbol{Z}_p^{d_a}$, where $0 \leq d_a \leq \frac{p+1}{2}$ and $\boldsymbol{Z}_p$ denotes the additive group of p-adic integers.*

We have a number of remarks to make about these theorems. If F is a finite field of characteristic $\ell (\neq p)$, then the fact that $J_a(F)$ contains a subgroup of order p^3 was noticed by Iwasawa. It follows quite simply from the fact that the roots of the zeta function of $y^p = x^a(1-x)$ are certain Jacobi sums over F by using an elementary congruence for these Jacobi sums which Iwasawa proves in [6]. Our

* Supported in part by a National Science Foundation grant.

0010-437X/81/03345-15$00.20/0

proof of theorem 1 provides another, somewhat more conceptual proof of this congruence. By a similar approach, congruences for other Jacobi sums can also be derived. Also, as our arguments will show, the result that $\mathrm{Gal}(F_\infty^{(a)}/F)$ is torsion-free is quite closely related to Iwasawa's congruence.

The value of d_a depends on the nature of the field F. Let $\tilde{F}$ denote the composite of all $\boldsymbol{Z}_p$-extensions (contained in $\bar{F}$) of F. Theorem 2 of course shows that $F_\infty^{(a)} \subseteq \tilde{F}$. If F is either a finite field or a finite extension of the field $\boldsymbol{Q}_\ell$ of ℓ-adic numbers, then $\mathrm{Gal}(\tilde{F}/F) \cong \boldsymbol{Z}_p$ and one can see easily that we must have $F_\infty^{(a)} = \tilde{F}$ and hence $d_a = 1$ in this case. On the other hand, if $F = Q_p(\sqrt[p]{1})$, then it follows from local class field theory that $\mathrm{Gal}(\tilde{F}/F) \cong \boldsymbol{Z}_p^p$ and therefore $F_\infty^{(a)}$ is considerably smaller than $\tilde{F}$. The most interesting case to consider is when F is the field $K = \boldsymbol{Q}(\sqrt[p]{1})$. Then one can show by class field theory (using Leopoldt's conjecture which is valid for K) that $\mathrm{Gal}(\tilde{K}/K) \cong \boldsymbol{Z}_p^{(p+1)/2}$. (See [2] and [4].) It turns out that "usually" $K_\infty^{(a)} = \tilde{K}$. However, for certain values of a and p, $K_\infty^{(a)}$ is a proper subfield of $\tilde{K}$. This occurs for example whenever $p \equiv 1 \pmod 3$ and a is either of the two solutions to the congruence $x^2 + x + 1 \equiv 0 \pmod p$. (This can be explained by the fact that, for these values of a, J_a is not a simple abelian variety. See [8].) There are also other cases where $K_\infty^{(a)} \neq \tilde{K}$ which we will describe at the end of Section 3.

In contrast, it is conceivable that the group $J_a(K)$ never contains more than p^3 points of p-power order. In section 5, we will give a necessary and sufficient condition (involving cyclotomic units) for the p-primary subgroup of $J_a(K)$ to be just $(\boldsymbol{Z}/(p))^3$. Our condition is satisfied if p does not divide the class number of the maximal real subfield of K. Despite extensive calculations, there are no known p that do divide this class number. (See [7] and [10].)

Our approach to proving the above theorems is to study the p-adic representation of $\mathrm{Gal}(\bar{F}/F)$ on the Tate module for J_a for the prime p, using the fact that J_a is of CM-type. In the case $F = K$, this p-adic representation can be described explicitly in terms of certain Jacobi sums. Our final results depend on this explicit description of the above p-adic representation. By following some of the arguments in Iwasawa's paper [6] (which depend on Stickelberger's theorem on the factorization of Jacobi sums), we can determine precisely the field generated by points of order p on J_a over $\boldsymbol{Q}_p$ and over $\boldsymbol{Q}$. (For $\boldsymbol{Q}$, we also need to use an explicit reciprocity law proved by Artin and Hasse.) For simplicity, we will just state our results for $J = \prod_{a=1}^{p-2} J_a$. Let L and L_p denote the fields generated over $\boldsymbol{Q}$ and $\boldsymbol{Q}_p$ respectively by the points of order p on J. Then it is well-known that $K \subseteq L$ and that

$K_p = \boldsymbol{Q}_p(\sqrt[p]{1})$, the completion of K at the prime over p. It turns out that $\mathrm{Gal}(L/K)$ and $\mathrm{Gal}(L_p/K_p)$ are both elementary abelian p-groups and therefore one can consider them as representation spaces over $\boldsymbol{Z}/(p)$ for the group $\Delta = \mathrm{Gal}(K/\boldsymbol{Q}) \cong \mathrm{Gal}(K_p/\boldsymbol{Q}_p)$. (If $x \in \mathrm{Gal}(L/K)$ or $\mathrm{Gal}(L_p/K_p)$ and $\delta \in \Delta$, the action of δ is $x \to \bar{\delta} x \bar{\delta}^{-1}$, where $\bar{\delta}$ is any automorphism of L or L_p extending δ.) The irreducible representations of Δ over $\boldsymbol{Z}/(p)$ are one-dimensional and correspond to the powers $\omega^i (i = 1, \ldots, p-1)$ of the character $\omega : \Delta \to (\boldsymbol{Z}/(p))^x$ defined by $\omega(\delta) = c \mod p$ if $\delta(\zeta_p) = \zeta_p^c$ for a primitive p-th root of unity ζ_p in K(and K_p). If V is any representation space for Δ over $\boldsymbol{Z}/(p)$, we let

$$V_i = \{v \in V \mid \delta(v) = \omega^i(\delta)v \quad \text{for all } \delta \in \Delta\}.$$

We will also regard ω and its powers as characters of Δ with values in $\boldsymbol{Z}_p^x$ by using the canonical isomorphism of $(\boldsymbol{Z}/(p))^x$ into $\boldsymbol{Z}_p^x$. We can then define V_i whenever V is a $\boldsymbol{Z}_p$-module on which Δ acts. We can now state our main results.

THEOREM 3: *Let $i + j = p$. Then $\mathrm{Gal}(L_p/K_p)_i \cong \{0\}$ or $\boldsymbol{Z}/(p)$. It is isomorphic to $\boldsymbol{Z}/(p)$ if and only if i is odd, $\neq 1$, and p does not divide the numerator of the j-th Bernoulli number B_j.*

THEOREM 4: *Let C denote the group of cyclotomic units in the maximal real subfield K^+ of K. Then $L = K(\{\sqrt[p]{\eta} \mid \eta \in C\})$.*

We want to add a few remarks concerning these theorems. First of all, it is not hard to see from local class field theory that theorem 3 actually does determine L_p uniquely. One needs to know only the so-called "indices of irregularity." Also, theorem 4 implies immediately that $\mathrm{Gal}(L/K) \cong (\boldsymbol{Z}/(p))^t$ where $t \leq \dfrac{p-3}{2}$, since this is the rank of C and the torsion subgroup of C has order prime to p. If we let E^+ denote the full unit group of K^+, then it is well-known that $[E^+ : C]$ is equal to the class number h^+ of K^+ and from this one finds that $t = \dfrac{p-3}{2}$ precisely when $p \nmid h^+$. Now the action of Δ on C is such that $(C/C^p)_j$ is isomorphic to $\boldsymbol{Z}/(p)$ when j is even but $\neq p-1$ and is otherwise trivial. Thus one can find a set of generators $\{\eta_j\}$, where j is even and $2 \leq j \leq p-3$, such that $\eta_j C^p$ generates $(C/C^p)_j$. It is not hard to show that Δ acts on $\mathrm{Gal}(K(\sqrt[p]{\eta_j})/K)$ by the character ω^i (where $i + j = p$). Thus $\mathrm{Gal}(L/K)_i$ is isomorphic to $\boldsymbol{Z}/(p)$ when $\eta_j \notin (K^x)^p$ and

is trivial otherwise. If we let $(E^+/C)_p$ denote the p-primary subgroup of E^+/C, then η_j is a p-th power in $K^\times$ if and only if the ω^j-th component $(E^+/C)_{p,j}$ is non-trivial. Thus the structure of $(E^+/C)_p$ as a Δ-module completely determines the structure of $\mathrm{Gal}(L/K)$. The field L itself is actually determined also, as we can see by using the fact that $L \subseteq \tilde{K}$.

We also want to point out that theorem 3 could be derived from theorem 4 by using the classical result that η_j is a p-th power in K_p if and only if p divides the numerator of B_j together with the observation that L_p is the completion of L for any prime dividing p. However, we will give a simpler, direct proof of theorem 3.

2. Generalities

Let ϵ_p denote a fixed primitive p-th root of unity in F. We begin by considering the curve $y^p = f(x)$, where $f(x)$ is a non-constant polynomial over F whose irreducible factors occur with multiplicity not divisible by p. In much of this section, we won't need to assume that $p \neq 2$ or 3. We will study the divisor classes on the above curve from two points of view – namely by using genus theory for the cyclic extension $F(x, y)/F(x)$ and also by using the fact that the Jacobian variety J_p of the above curve has $A = \boldsymbol{Z}[\zeta_p]$ as a ring of endomorphisms, where ζ_p is a fixed primitive p-th root of unity in K.

We can determine the group of divisor classes for the above curve which are defined over F and invariant under the action of $\mathrm{Gal}(F(x, y)/F(x))$ by the following standard genus-theoretic arguments. To avoid a slight complication, we assume that $f(x)$ has at least one linear factor over F. Let $\phi \in \mathrm{Gal}(F(x, y)/F(x))$ be defined by $\phi(y) = \epsilon_p y$. Assume that D is a divisor of degree zero for $F(x, y)$ such that $\phi(D) - D$ is a principal divisor, $\phi(D) - D = (z)$, say. Clearly, $N(z) \in F^\times$, where N is the norm map for the above cyclic extension. In fact, our assumption about $f(x)$ implies that $N(z) \in (F^\times)^p$ as one can see by just noting that every residue class for a ramified prime of $F(x, y)$ corresponding to a linear factor of $f(x)$ has a representative from F and that z must be a unit at the ramified primes. Hence, we may assume that $N(z) = 1$. Thus $z = \phi(w)/w$ for some non-zero element w of $F(x, y)$ and therefore $D - (w)$ is invariant under ϕ and in the same divisor class as D. Let $P_1, P_2, \ldots, P_t$ denote the primes of $F(x, y)$ ramified in the extension $F(x, y)/F(x)$. It follows that every divisor class of degree zero invariant under ϕ contains a sum of the P_i's. These divisor classes have order dividing

p. The only non-trivial principal divisors formed from the P_i's are multiples of (y) (up to divisors from $F(x)$). Thus we see that the group of invariant divisor classes of degree zero for $F(x, y)/F(x)$ is isomorphic to $(\boldsymbol{Z}/(p))^{t-2}$. If e denotes the number of distinct irreducible factors of $f(x)$ over F and if $d = \deg(f(x))$, $t = e + 1$ if $p \nmid d$ since in this case the infinite prime is ramified. If $p \mid d$, then $t = e$.

The curve $y^p = f(x)$ has a birational automorphism $(x, y) \to (x, \epsilon_p y)$ (corresponding to ϕ) which induces an endomorphism Z of J_f defined over F. Since $1 + Z + Z^2 + \ldots + Z^{p-1}$ is the zero-endomorphism, we obtain a homomorphism of $A = \boldsymbol{Z}[\zeta_p]$ into $\mathrm{End}_F(J_f)$ by mapping ζ_p to Z. If the genus of the above curve is positive, then this is an isomorphism and, to simplify notation, we will identify A with its image.

The Tate module T_f of J_f for the prime p can be viewed as a module over A and therefore over $A_p = A \otimes_{\boldsymbol{Z}} \boldsymbol{Z}_p$. Of course, A_p is just the ring of integers in $K_p = \boldsymbol{Q}_p(\zeta_p)$. Now A_p is a principal ideal domain and hence T_f must be a free A_p-module of rank $r = \dfrac{2g}{p-1}$, where g is the genus of $y^p = f(x)$. One could easily determine g by Hurwitz' formula but one can also do this as follows. Let $\pi = \zeta_p - 1$, a generator of the maximal ideal of A_p. Then r is equal to the dimension of $T_f/\pi T_f$ over $\boldsymbol{Z}/(p)$. If $\alpha \in A$, we will let $J_f[\alpha]$ denote the kernel of the endomorphism of J_f corresponding to α. The group $J_f[p]$ of p-division points on J_f defined over $\bar{F}$ is isomorphic to T_f/pT_f as an A_p-module and contains $J_f[\pi]$. Hence we can see that $p^r = |J_f[\pi]|$. But $J_f[\pi]$ is isomorphic to the group of divisor classes of degree zero of $\bar{F}(x, y)$ invariant under $\mathrm{Gal}(\bar{F}(x, y)/\bar{F}(x))$ and this just depends on the number of distinct roots of $f(x)$ and its degree d. In particular, if p is odd and if $f(x) = x^a(1-x)$ which $1 \le a \le p-2$, then $g = \dfrac{p-1}{2}$ and the corresponding Tate module T_a is a free A_p-module of rank 1.

From now on we will assume that p is odd and that $f(x)$ is such that $g = \dfrac{p-1}{2}$. If $\sigma \in \mathrm{Gal}(\bar{F}/F)$, then the action of σ on T_f commutes with that of A_p. Since T_f is a free A_p-module of rank 1, we have $\sigma(t) = \rho(\sigma)t$ for all $t \in T_f$, where ρ is a homomorphism of $\mathrm{Gal}(\bar{F}/F)$ into $U = A_p^x$. Let F_∞ denote the subfield of $\bar{F}$ generated by the coordinates of all p-power division points on J_f. Then $\mathrm{Gal}\,(F_\infty/F)$ is of course isomorphic to the image of ρ. The image of ρ also determines the structure of the p-primary subgroup of $J_f(F)$; it must be precisely $J_f[\pi^{s_f}]$, where s_f is the largest integer such that $\rho(\sigma) \equiv 1 \pmod{\pi^{s_f}}$ for all $\sigma \in \mathrm{Gal}(\bar{F}/F)$. One simple consequence of this is that $J_f(F)$ will

contain $J_f[p^n]$ if and only if $s_f \geq n(p-1)$, since $\pi^{p-1}A = pA$. This would occur for example if $J_f(F)$ contained a point of order p^{n+1}.

We will assume from here on that $f(x)$ factors into linear factors over F. The genus theoretic arguments described above make it clear that $J_f(F)$ contains at least $J_f[\pi]$. It follows that $\mathrm{Im}(\rho) \subseteq U_1$, where we are using the notation U_s for $\{u \in V \mid u \equiv 1 \pmod{\pi^s}\}$ when $s \geq 1$. We can say more. Let $\tau \in \Delta$ be defined by $\tau(\zeta_p) = \zeta_p^{-1}$. If $\alpha \in A_p$, we will usually write $\tau(\alpha)$ as $\bar{\alpha}$. We let $U^* = \{u \in U_1 \mid u\bar{u} \in \boldsymbol{Z}_p^x\}$. Then we will show that $\mathrm{Im}(\rho) \subseteq U^*$. This in fact follows easily from Weil's pairing. Let $M = \varprojlim \mu_{p^n}$ as $n \to \infty$, where μ_{p^n} is the group of p^n-th roots of unity in $\bar{F}$ and the inverse limit is defined by means of the p-th power map from $\mu_{p^{n+1}}$ to μ_{p^n}. Then $M \cong \boldsymbol{Z}_p$ and the action of $\mathrm{Gal}(\bar{F}/F)$ on M is given by a homomorphism $\kappa: \mathrm{Gal}(\bar{F}/F) \to \boldsymbol{Z}_p^x$. Now if C_1, C_2 are divisor classes for $\bar{F}(x, y)$ of order dividing p^n, choose D_i and $f_i (i = 1, 2)$ such that $D_i \in C_i$, D_1 and D_2 are disjoint, and $p^n D_i = (f_i)$ where $f_i \in \bar{F}(x, y)$. Then $(C_1, C_2) \to f_1(D_2)/f_2(D_1)$ defines a non-degenerate pairing $J_f[p^n] \times J_f[p^n] \to \mu_{p^n}$. Here $f(D)$ is defined for $f \in \bar{F}(x, y)$ and for a prime divisor D disjoint from (f)) in the obvious way and extended multiplicatively to non-prime divisors. It is clear that for $\sigma \in \mathrm{Gal}(\bar{F}/F)$, $(\sigma(C_1), \sigma(C_2)) = \sigma((C_1, C_2))$. Also, if $\phi \in \mathrm{Gal}(\bar{F}(x, y)/\bar{F}(x))$ is the generator defined by $\phi(y) = \epsilon_p y$, then $(\phi(C_1), \phi(C_2)) = (C_1, C_2)$. The Weil pairing $T_f \times T_f \to M$, which we denote by $\langle \cdot, \cdot \rangle$, will then have the properties: $\langle \sigma(t_1), t_2 \rangle = \langle t_1, \kappa(\sigma)\sigma^{-1}(t_2) \rangle$ and $\langle Z(t_1), t_2 \rangle = \langle t_1, Z^{-1}(t_2) \rangle$ for all $t_1, t_2 \in T_f$. By using $\boldsymbol{Z}_p$-bilinearity, we find that $\langle \alpha t_1, t_2 \rangle = \langle t_1, \bar{\alpha} t_2 \rangle$ for $\alpha \in A_p$. If $\alpha = \rho(\sigma)$, it follows that $\bar{\alpha} = \kappa(\sigma)\rho(\sigma)^{-1}$, i.e. $\rho(\sigma)\overline{\rho(\sigma)} = \kappa(\sigma)$. This proves that $\mathrm{Im}(\rho) \subseteq U^*$. We also mention in passing that if F is a finite field of order ℓ^r and if σ is the Frobenius automorphism over F, then $\kappa(\sigma) = \ell^r$ and therefore, since $\rho(\sigma)$ and its conjugates over $\boldsymbol{Q}_p$ are the roots of the zeta function for $y^p = f(x)$ over F, the above statement is just the Riemann Hypothesis in this very special case.

The fact that $\mathrm{Im}(\rho) \subseteq U^*$ has a few consequences that we want to mention. First, if $J_f(F)$ contains a point of order p^n, then $s_f > (n-1)(p-1)$ and so $\kappa(\sigma) \equiv 1 \pmod{p^{n-1}\pi}$ and therefore $\equiv 1 \pmod{p^n}$ for all $\sigma \in \mathrm{Gal}(\bar{F}/F)$. It follows that $\mu_{p^n} \subseteq F$. Secondly, it is easy to see that Δ acts on U_s/U_{s+1} by the character ω^s. In particular, J acts as $(-1)^s$. Now if $s \not\equiv 0 \pmod{p-1}$ and $\alpha \in U_s \cap U^*$ but $\notin U_{s+1}$, then clearly $\alpha\bar{\alpha} \in U_{s+1}$ and hence s must be odd. Therefore we see that either s_f is odd or $s_f \equiv 0 \pmod{p-1}$. For example, if we knew that $J_f(F)$ did not contain all the p-division points of J_f, then it would follow that the p-primary subgroup of $J_f(F)$ is isomorphic to $(\boldsymbol{Z}/(p))^s$, where $s = s_f$ is odd. We have one final general remark to make. Let F_1

denote the field generated by all points of order p on J_f. As a Galois module and as an A_p-module, we have $J_f[p] \cong T_f/pT_f$. It follows that $\mathrm{Gal}(\bar{F}/F_1) = \rho^{-1}(U_{p-1})$ and hence that $\mathrm{Gal}(F_1/F)$ is isomorphic to a subgroup of U_1/U_{p-1}. We see easily from this that $\mathrm{Gal}(F_1/F)$ is an elementary abelian p-group, as we mentioned in the introduction.

3. The curves $y^p = x^a(1-x)$

We just assume p is odd at first and that $1 \leq a \leq p-2$. Let p_0, p_1, and p_∞ denote the primes of $F(x)$ corresponding to x, $1-x$, and $1/x$. These primes are ramified in the extension $F(x, y)/F(x)$. Let P_0, P_1 and P_∞ be the primes of $F(x, y)$ lying above p_0, p_1, and p_∞. Let c denote the divisor class containing $D = P_0 - P_\infty$. Then c is invariant under the action of ϕ and the corresponding point on $J_a(F)$ is a generator of $J_a[\pi]$. We will show that $J_a(F)$ contains $J_a[\pi^2]$. This is equivalent to finding a divisor class c_1 of $F(x, y)$ such that $\phi(c_1) - c_1 = c$. We begin by showing that such a c_1 exists if and only if one can find a $z \in F(x, y)$ such that $N(z) = x$, where N is the norm map for the cyclic extension $F(x, y)/F(x)$. The existence of c_1 amounts to the existence of a divisor $D' \in c$ with $N(D') = 0$. If $N(z) = x$, then $D' = D - (z)$ has this property since $N(D) = p_0 - p_\infty = (x)$. Conversely if such a D' exists, then we must at least be able to find a $z' \in F(x, y)$ with $N(z') = \alpha x$ where $\alpha \in F^x$. But by considering residue classes modulo P_1, we easily see that $\alpha = \beta^p$ where $\beta \in F^x$ and hence $z = \beta^{-1}z'$ has the required property.

We will now show that x is in fact a norm for the extension $F(x, y)/F(x)$. This is a consequence of the following rather well-known lemma since both x and $1-x$ and therefore $x^a(1-x)$ are clearly norms for the extension $F(\sqrt[p]{x})/F(x)$.

LEMMA 1: *Let $\mathcal{F}$ be any field containing a primitive p-th root of unity. Let $u, v \in \mathcal{F}^x$. Then u is a norm for the extension $\mathcal{F}(\sqrt[p]{v})/\mathcal{F}$ if and only if v is a norm for $\mathcal{F}(\sqrt[p]{u})/\mathcal{F}$.*

PROOF: Let ϵ_p be a primitive p-th root of unity in $\mathcal{F}$. If either u or v is a p-th power in $\mathcal{F}$, the lemma is trivial. Assuming that this is not the case, let $\phi_u \in \mathrm{Gal}(\mathcal{F}(\sqrt[p]{u})/\mathcal{F})$ be defined by $\phi_u(\sqrt[p]{u}) = \epsilon_p \sqrt[p]{u}$. Define ϕ_v similarly. Consider the cyclic algebra $\mathcal{A} = [\mathcal{F}(\sqrt[p]{u}), \phi_u, v]$. Let $V = \sqrt[p]{u}$. The field $\mathcal{F}(U)$ can be considered as a subalgebra of $\mathcal{A}$. As a vector space over $\mathcal{F}(U)$, $\mathcal{A}$ has a basis 1, V, $V^2, \ldots, V^{p-1}$ where $V\alpha V^{-1} = \phi_u(\alpha)$ for all $\alpha \in \mathcal{F}(U)$ and $V^p = v$. Furthermore, v is

a norm for the extension $\mathcal{F}(U)/\mathcal{F}$ if and only if $\mathcal{A}$ is isomorphic to the algebra of $p \times p$ matrices over $\mathcal{F}$. But we can clearly identify $\mathcal{F}(\sqrt[p]{v})$ with the subalgebra $\mathcal{F}(V)$. Also $UVU^{-1} = \phi_v^{-1}(V)$ so that the inner automorphism of $\mathcal{A}$ by V restricts to ϕ_v^{-1} on $\mathcal{F}(V)$. Since 1, U, $U^2, \ldots, U^{p-1}$ is a basis for $\mathcal{A}$ over $\mathcal{F}(V)$, we see that $\mathcal{A}$ is isomorphic to the cyclic algebra $[\mathcal{F}(\sqrt[p]{v}), \phi_v^{-1}, u]$. Since this is the $p \times p$ matrix algebra if and only if u is a norm for $\mathcal{F}(\sqrt[p]{v})/\mathcal{F}$, lemma 1 is proved.

The following proposition follows immediately from what we have said above and at the end of section 2. Theorem 1 of course follows from this.

PROPOSITION 1: *If* $p = 3$, $J_a[\pi^2] \subseteq J_a(F)$. *If* $p > 3$, $J_a[\pi^3] \subseteq J_a(F)$.

Theorem 2 also follows quickly. Letting ρ_a denote the p-adic representation of $\mathrm{Gal}(\bar{F}/F)$ on the Tate module T_a for J_a, we have $\mathrm{Gal}(F_\infty^{(a)}/F) \cong \mathrm{Im}(\rho_a)$. But $U^* \cong \boldsymbol{Z}_p^{(p+1)/2} \times \boldsymbol{Z}/(p)$ as a topological group and $U^* \cap U_2 \cong \boldsymbol{Z}_p^{(p+1)/2}$. Since $\mathrm{Im}(\rho_a) \subseteq U^* \cap U_2$, we obtain theorem 2.

In the case where F is a finite field of order ℓ^r(with $\ell^r \equiv 1 \pmod{p}$ since we are assuming that F contains a primitive p-th root of unity), proposition 1 immediately gives a congruence for the roots of the zeta function of $y^p = x^a(1-x)$ over F. If σ denotes the Frobenius automorphisms of $\bar{F}/F$, then these roots are precisely the conjugates of $\rho_a(\sigma)$ over $\boldsymbol{Q}_p$ and they must be $\equiv 1 (\mathrm{mod}\ \pi^2)$ and even mod π^3 if $p > 3$. The fact that σ actually gives an endomorphism of J_a which commutes with Z together with the fact that A is a maximal commutative subring of $\mathrm{End}(J_a)$ shows that $\rho_a(\sigma)$ is in A and not just A_p. Let us assume that F is the residue class field $A/\mathfrak{P}$, where $\mathfrak{P}$ is a prime ideal dividing ℓ. We also assume that ϵ_p is ζ_p mod $\mathfrak{P}$. Now the roots of the zeta function are known to be the conjugates over Q of the Jacobi sum

$$\alpha_{\mathfrak{P}} = -\sum_{\substack{x \in F \\ x \neq 0, 1}} \phi(x)\phi^a(1-x) = \frac{g(1)g(a)}{g(1+a)},$$

where ϕ is the p-th power residue character mod $\mathfrak{P}$ and $g(t)$ is the Gaussian sum for F corresponding to the character ϕ^t. It is not essential for our arguments to know which conjugate of $\alpha_{\mathfrak{P}}$ is $\rho_a(\sigma)$. But this could be found as follows. Because of the above congruence $\rho_a(\sigma)$ is determined by its factorization. The CM-type of J_a is known to be $K_a = \{\delta \in \Delta \mid [\omega(\delta)] + [a\omega(\delta)] < p\}$, where [ ] denotes the first digit in the p-adic expansion, and thus we have $(\rho_a(\sigma)) = \prod_{\delta \in K_a} \mathfrak{P}^{\delta^{-1}}$. (See [3].) On the other hand, by a theorem of Stickelberger we have $(g(1)^p) = \mathfrak{P}^R$, where $R = \sum_{c=1}^{p-1} c\delta_{-c}^{-1}$, where $\delta_c \in \Delta$ is determined by

$\delta_c(\zeta_p) = \zeta_p^c$. It follows that $(\alpha_{\mathfrak{P}}) = \mathfrak{P}^{S_a}$, with $S_a = \frac{1}{p}(\delta_1 + \delta_a - \delta_{1+a})R$. By comparing, one finds that $\rho_a(\sigma) = \alpha_{\mathfrak{P}}$.

Now we come to the case $F = K = \boldsymbol{Q}(\zeta_p)$. Let $G = G_a = \mathrm{Gal}(K_\infty^{(a)}/K)$ and let $H = H_a$ be the inertia subgroup of G corresponding to the prime (π) of K, which is the only ramified prime in $K_\infty^{(a)}/K$ since $K_\infty^{(a)} \subseteq \tilde{K}$. Letting I denote the group of fractional ideals of K prime to p, the Artin symbol $\sigma_{\mathfrak{a}} = \left(\frac{K_\infty^{(a)}/K}{\mathfrak{a}}\right)$ defines a homomorphism $\mathfrak{a} \to \sigma_{\mathfrak{a}}$ of I to G. The image of I is dense in G by the Tchebotarev density theorem. If $\mathfrak{P}$ is a prime ideal of $K(\neq(\pi))$, then $\sigma_{\mathfrak{P}}$ is just the corresponding Frobenius automorphisms and we have $\rho_a(\sigma_{\mathfrak{P}}) = \alpha_{\mathfrak{P}}$. The image $\rho_a(G)$ is clearly just the closure of the subgroup generated by the $\alpha_{\mathfrak{P}}$'s for all $\mathfrak{P}$. We will follow Iwasawa [6] to study this image. Let I_0 be the subgroup of I of principal ideals. The image of I_0 in G under the Artin map is a dense subgroup of H. If $\mathfrak{a} \in I$, then obviously $(\rho_a(\sigma_{\mathfrak{a}})) = \mathfrak{a}^{S_a}$ and if $\mathfrak{a} \in I_0$, then $\rho_a(\sigma_{\mathfrak{a}}) = \alpha^{S_a}$ where α is any generator of $\mathfrak{a}$ such that $\alpha \equiv 1 \pmod{\pi^2}$. It follows easily that $\rho_a(H) = U_2^{S_a}$.

We will conclude this section by determining $d_a = d_a(K) = \mathrm{rank}_{Z_p}(G)$. Since H has finite index in G, this amounts to finding $\mathrm{rank}_{Z_p}(U_2^{S_a})$.

It is easy to determine this rank by decomposing U_2 by the action of Δ. If $\chi = \omega^i$, $1 \le i \le p-1$, then the χ-component of U_2 is isomorphic to Z_p and S_a acts as multiplication by

$$\chi(S_a) = \pm(1 + \chi(a) - \chi(a+1))B_{1,\chi^{-1}}.$$

Now $B_{1,\chi}$ is non-zero precisely when χ is odd or χ is the principal character. If $e_a = \frac{p+1}{2} - d_a$, then it is clear that e_a is the number of odd χ's such that $\chi(a+1) = 1 + \chi(a)$. It is easy to see that this holds only when $\chi(a)$ is a primitive 6-th root of unity and $\chi(a+1) = \chi(a)^2$. Obviously, if $p \equiv 2 \pmod 3$, then $e_a = 0$. On the other hand, if $p \equiv 1 \pmod 3$ and if $a^2 + a + 1 \equiv 0 \pmod p$, then $\chi(a+1) = 1 + \chi(a)$ whenever $\chi(a) \neq 1$. Thus $d_a = \frac{p-1}{6} + 1$ and one can see that $K_\infty^{(a)} = K\tilde{K}'$, where K' is the subfield of K fixed by $\{1, \delta_a, \delta_a^2\}$. For such a, J_a turns out to be isogenous over K to $(J_a')^3$ where J_a' is an abelian variety of dimension $\frac{p-1}{6}$ with the ring of integers of K' as a ring of endomorphisms. (See [8].)

There are many other pairs (a, p) for which e_a is non-zero. The first exceptional pairs occur for $p = 67$. In addition to the values of a

discussed in the last paragraph ($a = 29$ and 37 for $p = 67$), we have $e_a = 2$ for $a = 6$, 10, 19, 47, 56, and 60. (Note the easily explained symmetry $a \leftrightarrow p - 1 - a$.) The exceptional characters in these cases are the two characters of Δ of order 6. The following remark due to Lenstra shows that similar exceptional pairs (a, p) occur for all sufficiently large p such that $p \equiv 7 \pmod{12}$. A character χ of order 6 of Δ will then correspond to an odd character mod p. Let g be a primitive root mod p. We have $\chi(a+1) = 1 + \chi(a)$ if $a \equiv gx^6$ and $a + 1 \equiv g^2y^6 \pmod{p}$ with $(x, p) = (y, p) = 1$. But the Riemann Hypothesis for the curve $gx^6 + 1 = g^2y$ over $\boldsymbol{Z}/(p)$ provides many such values of a. (The genus of this curve is 10.) More generally, if $p \equiv 6r + 1 \pmod{12r}$ and if χ is any character of Δ of order $6r$, then χ will again be odd and the existence of a's satisfying $\chi(a+1) = 1 + \chi(a)$ for sufficiently large p follows by considering the curve $g^r x^{6r} + 1 = g^{2r} y^{6r}$ over $\boldsymbol{Z}/(p)$. One can make e_a arbitrarily large in this way. We also want to remark that for any fixed value of $a > 1$, one can prove the existence of infinitely many primes p such that $e_a = e_a(p)$ is non-zero by using the Tchebotarev density theorem. We will omit the details.

Finally, we want to point out here that the field $K_\infty^{(a)}$ is actually completely determined by the exceptional χ's. By class field theory, it is not difficult to show that if χ is either an odd character or the principal character of Δ, then there exists a unique Z_p-extension $\tilde{K}_\chi$ of K such that $\tilde{K}_\chi/\boldsymbol{Q}$ is a Galois extension and such that Δ acts on $\mathrm{Gal}(\tilde{K}_\chi/K)$ by means of χ. By noting that ρ_a induces a Δ-isomorphism of G with $\mathrm{Im}(\rho_a)$, one can see that $K_\infty^{(a)}$ is precisely the composite of the $\tilde{K}_\chi$'s for those χ such that $\chi(a+1) \neq 1 + \chi(a)$.

4. The local field of p-division points

Let $K_p = \boldsymbol{Q}_p(\zeta_p)$ and let $L_p^{(a)}$ denote the extension of K_p generated by the points of order p on J_a. Now H_a can be identified with $\mathrm{Gal}(K_{p,\infty}^{(a)}/K_p)$. We will then have $\mathrm{Gal}(K_{p,\infty}^{(a)}/L_p) = \{h \in H_a \mid \rho_a(h) \equiv 1 \pmod{pA_p}\}$ and hence $\mathrm{Gal}(L_p^{(a)}/K_p)$ will be isomorphic to the corresponding quotient group of H_a. Using the fact that $\rho_a(H_a) = U_2^{S_a}$, we find that as Δ-modules $\mathrm{Gal}(L_p^{(a)}/K_p) \cong V^{S_a}$, where $V = U_2/U_{p-1}$. Now as mentioned earlier U_i/U_{i+1} is isomorphic to $\boldsymbol{Z}/(p)$ with Δ acting by ω^i. Thus, considering V as a representation space for Δ over $\boldsymbol{Z}/(p)$, each character χ of Δ occurs with multiplicity one in V except for $\omega^{p-1} = \omega^0$ and ω^1, which don't occur in V at all. If $\chi = \omega^i$, $2 \leq i \leq p-2$, then S_a acts on V_χ as multiplication by $\chi(S_a) = \pm(1 + \chi(a) - \chi(a+1))\, B_{1,\chi^{-1}}$. For these χ's, the χ-component of $\mathrm{Gal}(L_p^{(a)}/K_p)$ is non-trivial precisely when $\chi(S_a) \not\equiv 0 \pmod{p\boldsymbol{Z}_p}$. It is well-known that p divides $B_{1,\chi^{-1}}$ if and only if p

divides the Bernoulli number B_j, where $i+j=p$. (Up to p-adic units, both occur as values of the same p-adic L-function $L_p(s, \omega^j)$.) Therefore, if $p \mid B_j$ then $\mathrm{Gal}(L_p^{(a)}/K_p)_i$ will be trivial for every a. It is also possible that $1+\chi(a)-\chi(a+1)$ is divisible by p for certain values of a. Obviously this cannot occur for every a since then one would have $\chi=\omega$ which has been excluded. Also we note that only odd χ's can occur non-trivially in $\mathrm{Gal}(L_p^{(a)}/K_p)$.

The above remarks allow us to determine $L_p^{(a)}$ completely. By local class field theory, K_p has a unique cyclic extension L_χ of degree p such that $L_\chi/\boldsymbol{Q}_p$ is Galois and such that Δ acts on $\mathrm{Gal}(L_\chi/K_p)$ by the character χ, where $\chi=\omega^i$ with $2 \le i \le p-2$. (This is not true for $\chi=\omega^0$ and ω^1!) We see that $L_p^{(a)}$ is just the composite of those L_χ's for which $\chi(S_a) \not\equiv 0 \pmod{p\boldsymbol{Z}_p}$. Obviously L_χ will be contained in $L_p^{(a)}$ for some a if and only if $p \nmid B_j$. Theorem 3 follows immediately from these considerations.

It is interesting to examine the structure of the p-primary subgroup of $J_a(K_p)$. Of course, $J_a[\pi^3]$ is contained in $J_a(K_p)$. (We are assuming here that $p \ge 5$.) In order to have more than this, we would have to have $\rho_a(H_a) \subseteq U_4$. Hence a necessary and sufficient condition for having $J_a[\pi^4] \subseteq J_a(K_p)$ is that $\omega^3(S_a) \equiv 0 \pmod{p\boldsymbol{Z}_p}$. Now it is easy to see that $1+\chi(a) \not\equiv \chi(a+1) \pmod p$ for $\chi=\omega^3$ and $1 \le a \le p-2$. Therefore $\omega^3(S_a) \equiv 0 \pmod{p\boldsymbol{Z}_p}$ if and only if p divides B_{p-3}. The first such prime (and the only one less than 125,000) is $p=16843$. (See [7] and [10].) Of course, for this p we actually have $J_a[\pi^5] \subseteq J_a(K_p)$ for every $a (1 \le a \le p-2)$. Now $p \nmid B_{p-5}$ for this p and hence the p-primary subgroup of $J_a(K_p)$ will be precisely $J_a[\pi^5]$ unless $\omega^5(a+1) \equiv \omega^5(a)+1 \pmod p$. There are just two values of a within the range $1 \le a \le p-2$ for which this congruence holds – the two solutions of $a^2+a+1 \equiv 0 \pmod p$. In fact, for these two values of a, we have $\chi(a+1)=\chi(a)+1$ whenever $\chi=\omega^i$ with $i \not\equiv 0 \pmod 3$. Since $p \nmid B_{p-9}$ for the above p, we can see that, for these two values of a, the p-primary subgroup of $J_a(K_p)$ is $J_a[\pi^9]$, an elementary abelian p-group of order p^9. In general, for $p \ge 5$, one can at least say that $J_a(K_p)$ never contains all the p-division points on J_a. This follows by an easy argument using the trivial fact that B_2 and B_4 are not divisible by p.

5. The global field of p-division points

Let $L^{(a)}$ denote the extension of $K=\boldsymbol{Q}(\zeta_p)$ generated by the points of order p on J_a. The field L generated by the p-division points on J is of course just the composite of the $L^{(a)}$'s. Now $\mathrm{Gal}(L^{(a)}/K)$ is a

quotient group of $\mathrm{Gal}(K_\infty^{(a)}/K)$ and the representation ρ_a induces an isomorphism $\bar{\rho}_a$ of $\mathrm{Gal}(L^{(a)}/K)$ with a subgroup of $V = U_2/U_{p-1}$. In fact, since $\mathrm{Im}(\rho_a) \subseteq U^*$, it follows that $\mathrm{Im}(\bar{\rho}_a) \subseteq V^* = \{v \in V \mid v^{1+\tau} = 1\}$. Noticing that V_i^* is isomorphic to $\boldsymbol{Z}/(p)$ if i is odd and $3 \leq i \leq p-2$ (and is trivial otherwise), we can see that $L^{(a)}$ can be expressed as a composite of certain fields $L_i^{(a)}$, where i varies through the values just mentioned and where $L_i^{(a)}$ is a cyclic extension of K of degree 1 or p which is Galois over $\boldsymbol{Q}$ with the action of Δ on $\mathrm{Gal}(L_i^{(a)}/K)$ given by the character ω^i. Now if i is as above and if $i+j=p$, then j will be even and satisfy $2 \leq j \leq p-3$ and so we can define another field $L_i' = K(\sqrt[p]{\eta_j})$, where η_j is the cyclotomic unit in the introduction. We will prove that $L_i^{(a)} = L_i'$ whenever $\omega^i(a+1) \not\equiv \omega^i(a)+1 \pmod{p\boldsymbol{Z}_p}$ and $L_i^{(a)} = K$ otherwise. Theorem 4 follows at once from this because $\omega^i(a+1) \equiv \omega^i(a)+1 \pmod{p\boldsymbol{Z}_p}$ cannot hold for all a unless $i \equiv 1 \pmod{p-1}$ and this has been excluded.

To prove the above result, we use Bauer's well-known theorem that a Galois extension is determined by the set of primes which split completely in it. Let $\mathfrak{P}$ be a prime of $K(\neq(\pi))$ and let $\sigma_{\mathfrak{P}}$ denote the Frobenius automorphism for $\mathfrak{P}$ in the extension $K_\infty^{(a)}/K$. Then it is clear that $\mathfrak{P}$ splits in the extension $L_i^{(a)}/K$ if and only if the projection of $\bar{\rho}_a(\sigma_{\mathfrak{P}})$ onto the ω^i-th component V_i^* is trivial. Now let $\rho_a(\sigma_{\mathfrak{P}}) = \alpha \in U^*$. Of course α is just the Jacobi sum $\alpha_{\mathfrak{P}}$ and depends on both $\mathfrak{P}$ and a. Let e_i denote the indempotent $\frac{1}{p-1}\Sigma_{\delta\in\Delta}\,\omega^{-i}(\delta)\delta$ corresponding to ω^i in the group ring $\boldsymbol{Z}_p[\Delta]$. The projection of α onto the ω^i-th component U_i^* is just α^{e_i}. Thus we see that $\mathfrak{P}$ splits in $L_i^{(a)}/K$ if and only if α^{e_i} is a p-th power in U_i^* (or equivalently in U). Choose an element $e_i' \in \boldsymbol{Z}[\Delta]$ whose coefficients are close enough to those of e_i p-adically to make all of the following arguments work. It will always be clear that this is possible. We also assume that the coefficients of e_1' have sum equal to zero. We must examine when $\alpha^{e_i'}$ (which is now in K) is a p-th power in U. We have the factorization $(\alpha^{e_i'}) = \mathfrak{P}^{e_i' S_a}$. It will be convenient to restrict attention to primes $\mathfrak{P}$ whose ideal class is in the p-primary subgroup P of the ideal class group of K. It is not hard to see that a Galois p-extension of K is still determined by the set of such primes that split completely in it.

The ideal class of $\mathfrak{P}^{e_i'}$ will be a typical element of P_i. So we see that P_i is annihilated by $\omega^i(S_a) = (1+\omega^i(a)-\omega^i(a+1))\ B_{1,\omega^{-1}}$ and therefore by $B_{1,\omega^{-1}}$ (since $i \not\equiv 1 \pmod{p-1}$ and a can be varied). This of course is just the usual proof of this simple consequence of Stickelberger's theorems. For $i = 3, 5, \ldots, p-2$, let p^{n_i} be the largest power of p dividing $B_{1,\omega^{-i}}$. Then P_i has exponent dividing p^{n_i}.

Now $e_i' S_a$ is close to $e_i' \omega^i(S_a)$ in the p-adic topology on $Z_p[\Delta]$. If p divides $1 + \omega^i(a) - \omega^i(a+1)$, then we will have $(\alpha^{e_i'})$ equal to a p-th power of a principal ideal in K. It is not hard to see from this that $\alpha^{e_i'}$ is in $(K^x)^p$ and hence $\mathfrak{P}$ splits in $L_i^{(a)}$. In this case, we see that $L_i^{(a)} = K$ as we stated above. Similarily, if P_i has exponent smaller than p^{n_i}, then we actually have $L_i^{(a)} = K$ for all a.

We assume now that $1 + \omega^i(a) \not\equiv \omega^i(a+1) \pmod{pZ_p}$. Our result will follow if we show that $\alpha^{e_i'}$ is a p-th power in K_p if and only if $\left(\frac{\eta_j}{\mathfrak{P}}\right)_0 = 1$, where $(\div)_0$ is the p-th power residue symbol for K. This is proved in [5] and we essentially are just going to reproduce his argument here. If $\pi = \zeta_p - 1$ as before, then we can take η_j to be $\pi^{e_j'}$. (This is a unit since the coefficients of the "approximate" idempotent e_j' have sum zero.) Using elementary properties of the power residue symbol, we find that

$$\left(\frac{\eta_j}{\mathfrak{P}}\right)_0 = \left(\frac{\pi^{e_j'}}{\mathfrak{P}}\right)_0 = \left(\frac{\pi}{\mathfrak{P}^{e_i}}\right)_0.$$

Consider the cyclotomic field $K_n = \boldsymbol{Q}(\zeta_n)$ where ζ_n is a primitive p^{n+1}-st root of unity and $n \geq 0$. (A slight change in notation – ζ_p will now be written as ζ_0.) We may assume that $\zeta_n^{p^n} = \zeta_0$. Then if $\pi_n = \zeta_n - 1$, we have that $N_{n,0}(\pi_n) = \pi_0 = \pi$. Therefore, we see that

$$\left(\frac{\pi}{\mathfrak{a}}\right)_0 = \left(\frac{\pi_n}{\mathfrak{a}}\right)_{0,n},$$

where $(—)_{0,n}$ denotes the p-th power residue symbol in K_n. Here $\mathfrak{a}$ is an arbitrary ideal of K prime to (π). If $(—)_n$ is the p^{n+1}-th power residue symbol in K_n, then $(—)_n^{p^n} = (—)_{0,n}$. Applying these elementary facts to $\mathfrak{a} = \mathfrak{P}^{e_i'}$ and $n = n_i$, we have

$$\left(\frac{\pi}{\mathfrak{P}^{e_i'}}\right)_0 = \left(\frac{\pi_n}{\mathfrak{P}^{e_i' p^n}}\right)_n = \left(\frac{\pi}{\alpha^{e_i'}}\right)_n^b,$$

where b is some integer prime to p.

We recall the following result of Artin and Hasse [1]. Let $\beta \in K_n$ satisfy $\beta \equiv 1 \pmod{\pi_n}$. Then

$$\left(\frac{\pi_n}{\beta}\right)_n = \zeta_n^{r(\beta)},$$

where

$$r(\beta) = \frac{1}{p^{n+1}} T_n\left(\frac{\zeta_n}{\pi_n} \log_p \beta\right),$$

where T_n denotes the trace from $\boldsymbol{Q}_p(\zeta_n)$ to $\boldsymbol{Q}_p$. Now a simple calculation shows that the trace of $\frac{\zeta_n}{\pi_n}$ from K_n to K is $p^n \frac{\zeta_0}{\pi_0}$. Hence if $\beta \in K$, then $r(\beta) = \frac{1}{p} T_0\left(\frac{\zeta_0}{\pi_0} \log_p \beta\right)$. If we view K_p as a representation space for Δ over $\boldsymbol{Q}_p$, then we can decompose it into a direct sum of the one dimensional spaces $e_i K_p$, $1 \leq i \leq p-1$. The Gaussian sum $g_i = e_i \zeta_0 = \Sigma_{a=1}^{p-1} \omega^{-i}(a) \zeta_0^a$ spans $e_i K_p$ over $\boldsymbol{Q}_p$. If $A \in e_{i_1} K_p$ and $B \in e_{i_2} K_p$, then it is easy to see that $AB \in e_{i_1+i_2} K_p$ and that

$$T_0(AB) = \begin{cases} 0 \text{ if } i_1 + i_2 \not\equiv 0 \pmod{p-1} \\ (p-1)AB \text{ if } i_1 + i_2 \equiv 0 \pmod{p-1}. \end{cases}$$

Now, letting $\beta = \alpha^{e_i'}$, we obviously have

$$r(\beta) = \frac{1}{p} T_0\left(\frac{\zeta_0}{\pi_0} e_i' \log_p \alpha\right) \equiv \frac{1}{p} T_0\left(\frac{\zeta_0}{\pi_0} e_i \log_p(\alpha)\right) \pmod{p^{n+1} \boldsymbol{Z}_p}$$

if e_i' is close enough p-adically to e_i. To evaluate this, we must find the projection $e_{-i} \frac{\zeta_0}{\pi_0}$ on the ω^{-i}-th component of K_p. This is easily found from the elementary identity

$$\frac{\zeta_0}{\pi_0} = 1 + \frac{1}{\pi_0} = \frac{1}{p}(1 + \zeta_0 + 2\zeta_0^2 + 3\zeta_0^3 + \cdots + (p-1)\zeta_0^{p-1})$$

which can be derived by differentiating $x^p - 1 = (x-1)(1 + x + x^2 + \cdots + x^{p-1})$. We obtain

$$e_{-i} \frac{\zeta_0}{\pi_0} = B_{1,\omega^{-i}} g_{-i}$$

On the other hand, $e_i \log_p(\alpha) = \ell_i(\alpha) g_i$, where $\ell_i(\alpha) \in \boldsymbol{Z}_p$ and we will have $\ell_i(\alpha) \equiv 0 \pmod{p\boldsymbol{Z}_p}$ if and only if α^{e_i} is a p-th power in U. From all of these remarks, we find that

$$\frac{1}{p} T_0\left(\frac{\zeta_0}{\pi_0} e_i \log_p(\alpha)\right) = \pm (p-1) B_{1,\omega^{-i}} \ell_i(\alpha).$$

It follows that $r(\alpha^i) \equiv 0 \pmod{p^{n+1}}$ if and only if $\ell_i(\alpha) \equiv 0 \pmod{pZ_p}$, providing what we needed.

We conclude this paper by coming back to the question of the structure of the p-primary subgroup of $J_a(K)$. It would be larger than $J_a[\pi^3]$ if and only if $\rho_a(\sigma_\mathfrak{s}) = \alpha_\mathfrak{s} \equiv 1 \pmod{\pi^4 A}$ holds for all $\mathfrak{s}$. This means that the projection of $\alpha_\mathfrak{s}$ onto the ω^3-component of V^* is trivial. Since we have $\omega^3(a+1) \not\equiv \omega^3(a) + 1 \pmod{pZ_p}$, our arguments show that η_{p-3} must be a p-th power in K. Hence $J_a(K)$ contains $J_a[\pi^4]$ (and therefore $J_a[\pi^5]$) if and only if $(E^+/C)_{p-3}$ is non-trivial. We also want to point out how to describe the structure of the p-primary subgroup of $J_a(K)$ as a representation space (over $Z/(p)$) for the natural action of Δ. First note that $J_a[\pi] \subseteq J_a(Q)$. Thus Δ acts on $J_a[\pi]$ by the character ω^0. Now multiplication by π gives a group theoretic isomorphisms $J_a[\pi^{t+1}]/J_a[\pi^t]$ onto $J_a[\pi^t]/J_a[\pi^{t-1}]$ for $t \geq 1$. Using the fact that $\delta(\pi) \equiv \omega(\delta)\pi \pmod{\pi^2 Z_p}$, one finds inductively that $\mathrm{Gal}(\bar{Q}/Q)$ acts on $J_a[\pi^{t+1}]/J_a[\pi^t]$ through its quotient group Δ by the character ω^{-t}. Thus the semisimple action of Δ on $J_a[\pi^3] \subseteq J_a(K)$ has the characters ω^0, ω^{-1}, and ω^{-2} as its constituents. One simple consequence is that $J_a(K^+)$ has a subgroup isomorphic to $(Z/(p))^2$, where K^+ is the maximal real subfield of K.

REFERENCES

[1] E. ARTIN and H. HASSE: Die beiden Erganzungssatze zum Reziprozitatsgesetz der ℓ^n-ten Potenzreste im Korper der $\mathfrak{s}^n$-ten Finheitswurzeln. *Abh. Math. Sem. Univ. Hamburg 6* (1928) 146–162.

[2] A. BRUMER: On the units of algebraic number fields. *Mathematika 14* (1967) 121–124.

[3] B. GROSS and D. ROHRLICH: Some Results on the Mordell–Weil Group of the Jacobian of the Fermat Curve. *Inventiones, Math. 44* (1978) 201–224.

[4] K. IWASAWA: On Z_ℓ-extensions of algebraic number fields. *Ann. of Math. 98* (1973) 246–326.

[5] K. IWASAWA: A note on cyclotomic fields. *Inventiones Math. 36* (1976) 115–123.

[6] K. IWASAWA: A note on Jacobi sums, Symposia Mathematica, Vol. *15* (1975), 447–459.

[7] W. JOHNSON: Irregular primes and cyclotomic invariants. *Math. Comp. 29* (1975) 113–120.

[8] N. KOBLITZ and D. ROHRLICH: Simple Factors in the Jacobian of a Fermat curve, (to appear in Canadian Journ. of Math.).

[9] G. SHIMURA and Y. TANIYAMA: *Complex Multiplication of Abelian Varieties and its Applications to Number Theory.* Tokyo, Math. Soc. Japan 1961.

[10] S. WAGSTAFF: The Irregular Primes to 125000. *Math. Comp. 32* (1978) 583–591.

(Oblatum 19-IX-1979)

Department of Mathematics
University of Washington
Seattle, Washington 98195,
U.S.A.