RODNEY I. YAGER

A Kummer criterion for imaginary quadratic fields

Compositio Mathematica, tome 47, n° 1 (1982), p. 31-42
<http://www.numdam.org/item?id=CM_1982__47_1_31_0>

COMPOSITIO MATHEMATICA, Vol. 47, Fasc. 1, 1982, pag. 31–42

Printed in the Netherlands

A KUMMER CRITERION FOR IMAGINARY QUADRATIC FIELDS

Rodney I. Yager

Let $\zeta(s)$ denote the Riemann zeta function, and for each even positive integer k, define

$$\zeta_\infty(k) = (k-1)!(2\pi i)^{-k}\zeta(k).$$

Then $\zeta_\infty(k) = -B_k/2k$, where B_k denotes the k-th Bernoulli number, and so $\zeta_\infty(k)$ is rational. Let p be an odd prime. Then it is known that the numbers $\zeta_\infty(k)$ $(1 < k < p-1)$ are p-integral, and so may be regarded as lying in Z_p. Kummer studied the relationship between these numbers and the arithmetic of $\mathbb{Q}(\mu_p)$, and the following theorem is generally known as Kummer's criterion.

THEOREM 1: *Let p be an odd prime. Then the following are equivalent.*

(i) p is regular (i.e., the class number of $\mathbb{Q}(\mu_p)$ is prime to p).

(ii) there is no unramified cyclic extension of $\mathbb{Q}(\mu_p)$ of degree p.

(iii) there is a unique cyclic extension of $\mathbb{Q}(\mu_p)^+$ of degree p which is unramified outside the prime dividing p.

(iv) the numbers $\zeta_\infty(k)$ (k even, $1 < k < p-1$) are units in Z_p.

The aim of this paper is to prove an analagous result in the elliptic case, but before explaining this, we mention the following refinement of Kummer's criterion which is due to Ribet [6].

THEOREM 2: *Let χ denote the canonical character of Gal $(\bar{\mathbb{Q}}/\mathbb{Q})$ with values in $Z_p^\times$ giving the action of Gal $(\bar{\mathbb{Q}}/\mathbb{Q})$ on μ_p, and let k be an even integer with $1 < k < p-1$. Then p divides $\zeta_\infty(k)$ if and only if there is an*

0010–437X/82070031–12$00.20/0

unramified cyclic extension E of $\mathbb{Q}(\mu_p)$ of degree p such that for all $\sigma \in Gal(E/\mathbb{Q})$ and $\tau \in Gal(E/\mathbb{Q}(\mu_p))$,

$$\sigma\tau\sigma^{-1} = \chi^{1-k}(\sigma)\tau.$$

We now turn to the elliptic case. Let K be an imaginary quadratic field with class number 1, and let $\mathcal{O}$ denote the ring of integers of K. Let $\bar{K}$ be an algebraic closure of K, and let E be an elliptic curve defined over K whose ring of endomorphisms is isomorphic to $\mathcal{O}$. Let p be a rational prime, not 2 or 3, which splits in K, and for which E has good reduction at both primes of K dividing p. We fix, for the rest of this paper, one of the primes $\mathfrak{p}$ dividing p, and we write $\mathcal{F}$ for the field $K(E_p)$, where E_p denotes the kernel of the endomorphism p on $E(\bar{K})$. Let F be any Galois extension of K contained in $\mathcal{F}$. We say $\mathfrak{p}$ is irregular for F if there is a cyclic extension of F of degree p which is unramified outside the primes of F dividing $\mathfrak{p}$ and which is distinct from the composition of F and the first layer of the unique $\mathbb{Z}_p$-extension K_∞ of K unramified outside $\mathfrak{p}$.

Coates and Wiles [1] have given a criterion for determining whether $\mathfrak{p}$ is irregular for the ray class field of K modulo $\mathfrak{p}$ in terms of the $\mathfrak{p}$-adic properties of Hurwitz numbers. We shall extend their result, and provide criteria for determining whether $\mathfrak{p}$ is irregular for any Galois extension of K contained in $\mathcal{F}$.

To state our result precisely, we shall need to introduce a little more notation. Choose a Weierstrass model for E

$$y^2 = 4x^3 - g_2x - g_3$$

such that g_2 and g_3 belong to $\mathcal{O}$ and the discriminant is prime to $\mathfrak{p}$ and its conjugate $\mathfrak{p}^*$. As usual, we shall suppose that $\bar{K}$ is embedded the complex field $\mathbb{C}$, and we shall denote by $\mathcal{P}(z)$ the Weierstrass $\mathcal{P}$-function associated to our model. We identify $\mathcal{O}$ with the endomorphism ring of E so that $\alpha \in \mathcal{O}$ corresponds to the endomorphism $\xi(z) \to \xi(\alpha z)$, where $\xi(z) = (\mathcal{P}(z), \mathcal{P}'(z))$. Let L be the period lattice of $\mathcal{P}(z)$, and choose an element $\Omega_\infty \in L$ such that $L = \Omega_\infty\mathcal{O}$. Let ψ be the Grossencharacter attached to the curve E over K by the theory of complex multiplication, and write $L(\bar{\psi}^k, s)$ for the primitive complex Hecke L-function attached to $\bar{\psi}^k$ for each integer $k \geq 1$. Then, if $-d_K$ denotes the discriminant of K, Damerell's Theorem states that the numbers

$$L_\infty(\bar{\psi}^{k+j}, k) = (2\pi/\sqrt{d_K})^j \Omega_\infty^{-(k+j)} L(\bar{\psi}^{k+j}, k) \quad k \geq 1, j \geq 0$$

belong to $\bar{K}$, and, moreover, if $0 \leq j < k$, they belong to K.

We shall be interested in the $\mathfrak{p}$-adic properties of these numbers, and so, for simplicity, we shall fix an embedding of $\bar{K}$ in $\mathbb{C}_{\mathfrak{p}}$, an algebraic closure of the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$. In fact, it has been shown (see [9]) that the numbers $L_{\infty}(\bar{\psi}^{k+j}, k)$ all belong to $K_{\mathfrak{p}}$, and are $\mathfrak{p}$-integral if $0 \leq j \leq p-1$ and $1 < k \leq p$.

Finally, we write χ_1 and χ_2 for the canonical characters with values in $\mathbb{Z}_p^{\times}$ giving the action of $\mathrm{Gal}(\bar{K}/K)$ on the $\mathfrak{p}$ and $\mathfrak{p}^*$-division points of E respectively. Clearly, χ_1 and χ_2 together generate $\mathrm{Hom}(\mathrm{Gal}(\mathcal{F}/K), \mathbb{Z}_p^{\times})$. If F is a subfield of $\mathcal{F}$, we shall say a character χ of $\mathrm{Gal}(\mathcal{F}/K)$ belongs to F if the kernel of χ contains $\mathrm{Gal}(\mathcal{F}/F)$. Our main result is as follows.

THEOREM 3: *Let F be any Galois extension of K contained in $\mathcal{F}$. Then the prime $\mathfrak{p}$ is irregular for F if and only if there exist integers k and j with $0 \leq j < p-1$, $1 < k \leq p$ such that $\chi_1^k \chi_2^{-j}$ is a non-trivial character belonging to F and $L_{\infty}(\bar{\psi}^{k+j}, k)$ is not a unit in $K_{\mathfrak{p}}$.*

As a numerical example, consider the field $K = \mathbb{Q}(i)$ and the elliptic curve E: $y^2 = 4x^3 - 4x$. If p is a prime congruent to 1 modulo 4, and $\mathfrak{p}$ is a prime lying above p, then the characters belonging to $\mathcal{R}_{\mathfrak{p}}$, the ray class field of K modulo $\mathfrak{p}$, are the characters $\chi_1^k \chi_2^{-j}$ for which $j \equiv 0 \bmod (p-1)$ and $k \equiv 0 \bmod 4$, while the characters belonging to $\mathcal{R}_p$, the ray class field of K modulo p, are the characters $\chi_1^k \chi_2^{-j}$ for which $k + j \equiv 0 \bmod 4$. Using the table in Hurwitz [3] together with the formulae in Weil [8] p. 45, it is easy to calculate the following table of values for $(k-1)! L_{\infty}(\bar{\psi}^{k+j}, k)$.

Values of $\pi^j (k-1)! \Omega_{\infty}^{-(k+j)} L(\bar{\psi}^{k+j}, k)$ for the curve $y^2 = 4x^3 - 4x$.

	j			
$k+j$	0	1	2	3
4	$2^{-1} \cdot 5^{-1}$	$2^{-2} \cdot 3^{-1}$	$2^{-2} \cdot 3^{-1}$	$2^{-1} \cdot 5^{-1}$
8	$2^2 \cdot 3 \cdot 5^{-1}$	$2^3 \cdot 7^{-1}$	$2 \cdot 3^{-1}$	2^{-1}
12	$2^7 \cdot 3^3 \cdot 5^{-1} \cdot 7 \cdot 13^{-1}$	$2^7 \cdot 3^2 \cdot 11^{-1}$	2^5	$2^5 \cdot 3^{-1}$
16	$2^9 \cdot 3^4 \cdot 5^{-1} \cdot 7^2 \cdot 11 \cdot 17^{-1}$	$2^{11} \cdot 3^3$	$2^9 \cdot 3^2 \cdot 7^{-1} \cdot 19$	$2^{10} \cdot 3$
20	$2^{15} \cdot 3^6 \cdot 5^{-2} \cdot 7^2 \cdot 11$	$2^{15} \cdot 3^5 \cdot 7 \cdot 19^{-1} \cdot 29$	$2^{13} \cdot 3^3 \cdot 67$	$2^{13} \cdot 3^2 \cdot 37$
24	$2^{18} \cdot 3^6 \cdot 5^{-1} \cdot 7^3 \cdot 11^2 \cdot 13^{-1} \cdot 19$	$2^{19} \cdot 3^6 \cdot 7^2 \cdot 23^{-1} \cdot 389$	$2^{17} \cdot 3^5 \cdot 11^{-1} \cdot 15629$	

It follows from Theorem 3 that $\mathfrak{p}$ is regular for both $\mathcal{R}_{\mathfrak{p}}$, and $\mathcal{R}_p$ when $p = 5$, but that while $\mathfrak{p}$ is regular for $\mathcal{R}_{\mathfrak{p}}$, it is irregular for $\mathcal{R}_p$ when $p = 29$, since 29 divides $L_{\infty}(\bar{\psi}^{20}, 19)$.

Similarly, $\mathfrak{p}$ is irregular for $\mathcal{R}_p$ when $p = 37$, 389 or 15629, since these primes divide $L_\infty(\bar{\psi}^{20}, 17)$, $L_\infty(\bar{\psi}^{24}, 23)$ and $L_\infty(\bar{\psi}^{24}, 22)$ respectively.

Before giving the proof of Theorem 3, we remark that Hida [2] has gone part way towards proving the analogue of Theorem 2. His result is summarized in the following theorem.

THEOREM 4: *Suppose the curve E is defined over $\mathbb{Q}$ and let k be an integer such that $1 < k \leq p$, $k \neq p-1$. Then, if F is any Galois extension of K such that $\chi_1^k\chi_2^{-k}$ belongs to F and $\mathfrak{p}$ divides $L_\infty(\bar{\psi}^{2k}, k)$, there is a cyclic extension of F of degree p unramified outside $\mathfrak{p}$ on which $Gal(F/K)$ acts via $\chi_1^k\chi_2^{-k}$.*

PROOF OF THEOREM 3: Let M denote the maximal abelian p-extension of F unramified outside the primes of F dividing $\mathfrak{p}$, and let F_∞ denote the composition of F and K_∞. It can be shown that for F as in our theorem, $\mathrm{Gal}(M/F_\infty)$ is finite, and it is easy to deduce from this that $\mathfrak{p}$ is irregular for F if and only if $\mathrm{Gal}(M/F_\infty)$ is non-trivial. The idea of our proof is to relate the formula given in Theorem 11 of Coates and Wiles [1] for the order of $\mathrm{Gal}(M/F_\infty)$ to the numbers $L_\infty(\bar{\psi}^{k+j}, k)$.

It will be convenient to do this in two parts. The first is to prove the $\mathfrak{p}$-adic analogue of the well known formula which gives the product of the class number and the regulator of an abelian extension of K in terms of the logarithms of Robert's elliptic units. The $\mathfrak{p}$-adic logarithms of these elliptic units arise in the work of Lichtenbaum [5] as special values of certain Iwasawa functions which he constructs which, as we shall show, are precisely the functions which Katz produced interpolating the numbers $L_\infty(\bar{\psi}^{k+j}, k)$. The congruences which arise from this observation will yield Theorem 3.

For the moment, let us suppose only that F is a finite abelian extension of K of degree d and conductor $\mathfrak{g}$. For each character χ of $\mathrm{Gal}(F/K)$, we let F_χ denote the fixed field of the kernel of χ and we write $\mathfrak{g}_\chi$ for the conductor of F_χ. If we denote by $\mathfrak{R}_{\mathfrak{g}_\chi}$ the ray class field of K modulo $\mathfrak{g}_\chi$, it is clear that we may regard χ as a character of $\mathrm{Gal}(\mathfrak{R}_{\mathfrak{g}_\chi}/K)$, and hence, via the reciprocity map, as a primitive character of the ray class modulo $\mathfrak{g}_\chi$ which we shall denote by $Cl(\mathfrak{g}_\chi)$. Let n_χ be the smallest positive rational integer in $\mathfrak{g}_\chi$ and let $w_{\mathfrak{g}_\chi}$ be the number of roots of unity in K which are congruent to 1 modulo $\mathfrak{g}_\chi$. Let w and w_F be the number of roots of unity in K and F respectively, and let h denote the class number of F. Then, if $\phi_{\mathfrak{g}_\chi}(C)$, $C \in Cl(\mathfrak{g}_\chi)$ is the invariant defined by Robert [7] p. 14, we have the following lemma.

LEMMA 5: *With a suitable choice of the sign of the regulator R of F,*

(1) $$\prod_{\chi\neq 1}\Big(\sum_{C\in Cl(\mathfrak{g}_\chi)}\chi^{-1}(C)\log|\phi_{\mathfrak{g}_\chi}(C)|\Big)\Big/ n_\chi w_{\mathfrak{g}_\chi} = 6^{d-1}whR/w_F,$$

where the product on the left is taken over all non-trivial characters of Gal(F/K).

PROOF: This is Theorem 3(ii) of Robert [7], if we note that the numbers Robert denotes by $\rho(\chi')$ satisfy $(\Pi_{\chi\neq 1}\rho(\chi'))^2 = 1$.

From now on, we fix our choice of the regulator R of F so that equation (1) holds, and we shall now prove a $\mathfrak{p}$-adic analogue of this formula. Let $\log_\mathfrak{p}$ be an extension of the $\mathfrak{p}$-adic logarithm to the whole of $\mathbb{C}_\mathfrak{p}$, and let Δ be the group of values taken by the characters of Gal (F/K). Recall that $\mathcal{R}_\mathfrak{g}$ is the ray class field of K modulo $\mathfrak{g}$, and we extend log | | and $\log_\mathfrak{p}$ to $\mathcal{R}_\mathfrak{g}^\times\otimes\mathbb{Z}[\Delta]$ by defining

(2) $$\log|\alpha\otimes a| = a\log|\alpha|$$

and

(3) $$\log_\mathfrak{p}\alpha\otimes a = a\log_\mathfrak{p}\alpha \text{ for } \alpha\in\mathcal{R}_\mathfrak{g}^\times \text{ and } a\in\mathbb{Z}[\Delta].$$

Let ϕ_χ denote the expression $\Pi_{C\in Cl(\mathfrak{g}_\chi)}(\phi_{\mathfrak{g}_\chi}(C)\otimes\chi^{-1}(C))$, and observe that if $\sigma\in\mathrm{Gal}(F/K)$, then

$$\phi_\chi^\sigma = \phi_\chi\otimes\chi(\sigma).$$

It follows that

(4)
$$\det(\log|\phi_\chi^\sigma|)_{\chi\neq 1,\sigma\neq 1} = \det(\chi(\sigma))_{\chi\neq 1,\sigma\neq 1}\prod_{\chi\neq 1}\Big(\sum_{C\in Cl(\mathfrak{g}_\chi)}\chi^{-1}(C)\log|\phi_{\mathfrak{g}_\chi}(C)|\Big)$$

and that

(5)
$$\det(\log_\mathfrak{p}\phi_\chi^\sigma)_{\chi\neq 1,\sigma\neq 1} = \det(\chi(\sigma))_{\chi\neq 1,\sigma=1}\prod_{\chi\neq 1}\Big(\sum_{C\in Cl(\mathfrak{g}_\chi)}\chi^{-1}(C)\log_\mathfrak{p}\phi_{\mathfrak{g}\chi}(C)\Big).$$

Choose units $e_1,\ldots,e_{d-1}$ in F which generate a subgroup of index

w_F in the group of units of F so that

$$R = 2^{d-1} \det(\log|e_j^\sigma|)_{\sigma\neq 1,\, 1\leq j<d}.$$

We define $\mathfrak{p}$-adic regulator of F, $R_\mathfrak{p}$ by

$$R_\mathfrak{p} = \det(\log_\mathfrak{p} e_j^\sigma)_{\sigma\neq 1,\, 1\leq j<d}.$$

(This definition fixes the sign of $R_\mathfrak{p}$, but otherwise agrees with that used by Coates and Wiles [1].)

Now, if C_0 is a fixed element of $Cl(\mathfrak{g}_\chi)$, $\phi_{\mathfrak{g}_\chi}(C)/\phi_{\mathfrak{g}_\chi}(C_0)$ is a unit in $\mathfrak{R}_\mathfrak{g}$ for all $C \in Cl(\mathfrak{g}_\chi)$, and it is clear that

$$\phi_\chi = \prod_{C\in Cl(\mathfrak{g}_\chi)} (\phi_{\mathfrak{g}_\chi}(C)/\phi_{\mathfrak{g}_\chi}(C_0)) \otimes \chi^{-1}(C).$$

Moreover, since ϕ_χ is fixed by $\mathrm{Gal}(\mathfrak{R}_\mathfrak{g}/F)$, it follows that if W denotes the group of roots of unity in F, there are elements $a_{\chi,j} \in \mathbb{Z}[\Delta]$ and $\mu_\chi \in W \otimes \mathbb{Z}[\Delta]$ such that

$$\phi_\chi = \mu_\chi \prod_{j=1}^{d-1} e_j \otimes a_{\chi,j}.$$

Thus, if $\sigma \in \mathrm{Gal}(F/K)$

$$\phi_\chi^\sigma = \mu_\chi^\sigma \prod_{j=1}^{d-1} e_j^\sigma \otimes a_{\chi,j}$$

and so we conclude that

$$\det(\log|\phi_\chi^\sigma|)_{\chi\neq 1,\, \sigma\neq 1} = \det(a_{\chi,j})_{\chi\neq 1,\, 1\leq j<d}\, R/2^{d-1} \tag{6}$$

and

$$\det(\log_\mathfrak{p} \phi_\chi^\sigma)_{\chi\neq 1,\sigma\neq 1} = \det(a_{\chi,j})_{\chi\neq 1, 1\leq j<d} R_\mathfrak{p}. \tag{7}$$

But, it is easy to see that $\det(\chi(\sigma))_{\chi\neq 1,\, \sigma\neq 1}$ is non-zero (see, for instance, Lemma 10.9 of Lichtenbaum [5]), and so, since $R \neq 0$, we conclude from Lemma 5 and equations (4)–(7) that we have the following $\mathfrak{p}$-adic analogue of Lemma 5.

THEOREM 6: *With our given choice of the sign of* $R_\mathfrak{p}$

$$(8) \qquad \prod_{\chi \neq 1} \Big(\sum_{C \in Cl(\mathfrak{g}_\chi)} \chi^{-1}(C) \log_\mathfrak{p} \phi_{\mathfrak{g}_\chi}(C) \Big) \Big/ n_\chi w_{\mathfrak{g}_\chi} = 12^{d-1} whR_\mathfrak{p}/w_F,$$

where the product on the left is taken over all non-trivial characters of Gal(F/K).

Let $\hat{E}$ be the formal group giving the kernel of reduction modulo $\mathfrak{p}$ on E, and we choose $-2x/y$ as the parameter for $\hat{E}$. Let $\eta : \hat{E} \tilde{\rightarrow} G_m$ be the isomorphism of formal groups defined over $\mathbb{C}_\mathfrak{p}$ between $\hat{E}$ and the formal multiplicative group G_m chosen in [9]. The coefficient of T in the power series expansion of $\eta(T) = \Omega_\mathfrak{p} T + \ldots$, is, of course, a unit in $\mathbb{C}_\mathfrak{p}$. In fact, $\Omega_\mathfrak{p}$ belongs to the maximal unramified extension of $K_\mathfrak{p}$ and, as is shown in [9], the action of Frobenius on $\Omega_\mathfrak{p}$ is given by multiplication by $\bar{\psi}(\mathfrak{p})$.

Recall that if χ is a character of Gal(F/K), we may regard χ as a character of the ray class modulo $\mathfrak{g}_\chi$, and hence as a primitive Dirichlet character of conductor $\mathfrak{g}_\chi$. Suppose $\mathfrak{g}_\chi = \mathfrak{p}^{m_\chi}\mathfrak{c}_\chi$, where $\mathfrak{c}_\chi$ is prime to $\mathfrak{p}$. Then we may express χ uniquely as the product of two primitive Dirichlet characters χ_0 and $\chi_\mathfrak{p}$ of conductor $\mathfrak{c}_\chi$ and $\mathfrak{p}^{m_\chi}$ respectively. Choose generators π of $\mathfrak{p}$, and γ_χ of $\mathfrak{c}_\chi$, and let P_χ be the point of exact order $\mathfrak{g}_\chi$ on the curve given by $P_\chi = P_{\chi_0} + P_{\chi_\mathfrak{p}}$ where $P_{\chi_0} = \xi(\Omega_\infty/\gamma_\chi)$ and $P_{\chi_\mathfrak{p}} = \xi(\Omega_\infty/\pi^{m_\chi})$. The point $P_{\chi_\mathfrak{p}}$ may be regarded as a point of order p^{m_χ} on the formal group $\hat{E}$, and so $\zeta_\chi = \eta(P_{\chi_\mathfrak{p}}) + 1$ is a p^{m_χ}-th root of unity. We write C_χ for the Gauss sum

$$C_\chi = p^{-m_\chi} \sum_{a \bmod p^{m_\chi}} \chi_\mathfrak{p}(a) \zeta_\chi^a.$$

Let $\mathscr{E}$ denote the triple $(E, 2dx/y, \eta^{-1})$ as in §6 of Lichtenbaum [5] and let $L(\mathscr{E}, \chi, P_\chi)$ be the function he defines in §8.1. Then we have the following theorem.

THEOREM 7: *Let $d_{F/K}$ be the relative discriminant of F over K. Then $\Pi_{\chi \neq 1} L(\mathscr{E}, \chi, P_\chi)(1)$, with the product taken over all non-trivial characters of Gal(F/K), has the same $\mathfrak{p}$-adic valuation as*

$$(phR_\mathfrak{p}/w_F \sqrt{d_{F/K}}) \cdot \prod_{\mathfrak{q} | \mathfrak{p}} (1 - (N\mathfrak{q})^{-1}),$$

where the product is taken over the prime ideals of F dividing $\mathfrak{p}$, and $N\mathfrak{q}$ denotes the norm to K of $\mathfrak{q}$.

PROOF: It is easy to see from Corollary 9.4 of Lichtenbaum that, if

χ is non-trivial

(9) $$L(\mathscr{C}, \chi, P_\chi)(1) = (C_\chi/6n_\chi\Omega_\mathfrak{p}) \times (1-\chi(\pi)/p)\chi(\gamma_\chi + \pi^{m_\chi})w \sum_{C\in Cl(\mathfrak{g}_\chi)} \chi^{-1}(C)\log_\mathfrak{p}\phi_{\mathfrak{g}_\chi}(C).$$

Since $\mathfrak{p}$ is prime to 2 and 3, and $\gamma_\chi + \pi^{m_\chi}$ is prime to $\mathfrak{g}_\chi$, it is clear from equations (8) and (9) that it will suffice to prove that $\Pi_{\chi\neq 1} C_\chi(1-\chi(\pi)/p)$ has the same $\mathfrak{p}$-adic valuation as $pd_{F/K}^{-1/2}. \Pi_{\mathfrak{q}|\mathfrak{p}}(1-(N\mathfrak{q})^{-1})$.

Now it is well known that $\pi^{m_\chi}C_\chi C_{\chi-1}$ is a unit in $\mathbb{C}_\mathfrak{p}$, and so the conductor-discriminant theorem shows that $\Pi_{\chi\neq 1} C_\chi$ has the same $\mathfrak{p}$-adic valuation as $d_{F/K}^{-1/2}$. Moreover, if H denotes the maximal abelian extension of K contained in F in which $\mathfrak{p}$ is unramified, it is easy to see that only those characters χ which belong to H contribute to $\Pi_{\chi\neq 1}(1-\chi(\pi)/p)$. We conclude that $\Pi_{\chi\neq 1}(1-\chi(\pi)/p)$ has the same $\mathfrak{p}$-adic valuation as $p^{1-[H:K]}$, which is also the same as the $\mathfrak{p}$-adic valuation of $p. \Pi_{\mathfrak{q}|\mathfrak{p}}(1-(N\mathfrak{q})^{-1})$.

From now on, we suppose, as in Theorem 3, that F is a Galois extension of K contained in $\mathscr{F}$. The importance of the previous theorem can be seen from the following corollary.

COROLLARY 8: *Let F be a Galois extension of K contained in $\mathscr{F}$. Then $\mathfrak{p}$ is regular for F if and only if the number $\Pi_{\chi\neq 1} L(\mathscr{C}, \chi, P_\chi)(1)$, where the product is taken over all non-trivial characters of $Gal(F/K)$, is a unit in $\mathbb{C}_\mathfrak{p}$.*

PROOF: Recall that M denotes the maximal abelian p-extension of F unramified outside the primes of F lying above $\mathfrak{p}$, and that F_∞ denotes the composition of F and K_∞. Since the $\mathfrak{p}$-adic regulator $R_\mathfrak{p}$ is non-zero, it follows from Theorem 11 of Coates and Wiles [1] that $\mathrm{Gal}(M/F_\infty)$ is finite, and that it is trivial if and only if $\Pi_{\chi\neq 1} L(\mathscr{C}, \chi, P_\chi)(1)$ is a unit in $\mathbb{C}_\mathfrak{p}$. But since $\mathrm{Gal}(F_\infty/F)$ has no torsion, we conclude that $\mathfrak{p}$ is regular for F if and only if $\mathrm{Gal}(M/F_\infty)$ is trivial, and the assertion of the corollary is now plain.

To conclude the proof of Theorem 3, we need to relate the numbers $L_\infty(\bar{\psi}^{k+j}, k)$ to the values of $L(\mathscr{C}, \chi, P_\chi)$. Let $\mathfrak{f}$ be the conductor of ψ and let ρ be the Dirichlet character of conductor $\mathfrak{f}$ given by

(10) $$\rho(\alpha) = \psi((\alpha))/\alpha, \quad (\alpha, \mathfrak{f}) = 1,$$

and observe that the character $\chi_1^k\chi_2^{-j}$, when viewed as a primitive Dirichlet character, is given by

(11) $$\chi_1^k\chi_2^{-j}(\alpha) = \omega^k(\alpha)\omega^{-j}(\bar{\alpha})\rho^{k+j}(\alpha),$$

where ω is the usual Teich-Muller character on $Z_p^\times$ (and hence a Dirichlet character of conductor $\mathfrak{p}$ under the obvious identification of $\mathcal{O}_\mathfrak{p}$ with Z_p). By the characters on the right hand side of equation (11) we mean, of course, the associated primitive characters. The following theorem is due to Katz.

THEOREM 9: *For each integer i mod w, there is an integral valued measure μ_i supported on $Z_p^{\times 2}$ such that*

(12) $$\int_{Z_p^2} x^{k-1}y^j d\mu_i = (-1)^{k+j}w(k-1)!\Omega_\mathfrak{p}^{-(k+j)}(1-\psi^{k+j}(\mathfrak{p})/N\mathfrak{p}^{j+1}) \times (1-\bar{\psi}^{k+j}(\mathfrak{p}^*)/N\mathfrak{p}^{*k})L_\infty(\bar{\psi}^{k+j}, k)$$

for all $k \geq 1$, $j \geq 0$ satisfying $k+j \equiv i \bmod w$

and

(13) $$\int_{Z_p^2} x^{k-1}\omega^j(y)d\mu_i = (-1)^k(k-1)!(\Omega_\mathfrak{p}\Omega_\infty)^{-k} \times (1-\omega^{-j}(\bar{\psi}(\mathfrak{p}))\psi^k(\mathfrak{p})/p)\sum_{\substack{\alpha\in\mathcal{O}\\ \alpha\neq 0}} \frac{\rho^{-i}(\alpha)\omega^j(\bar{\alpha})}{\alpha^k}$$

for all $k \geq 3$ and $j \not\equiv 0 \bmod p-1$.

Furthermore, if $a \in Z_p^\times$ there is another integral valued measure $\mu_i^{(a)}$ on $Z_p^\times$ such that

(14)

$$\int_{Z_p} x^{k-1}d\mu_i^{(a)} = (1-a^k)(-1)^k w(k-1)!\Omega_\mathfrak{p}^{-k}(1-\psi^k(\mathfrak{p})/p)L_\infty(\bar{\psi}^k, k)$$

for all $k \geq 1$ such that $k \equiv i \bmod w$.

PROOF: We shall only indicate briefly here how the existence of these measures can be deduced from the results in Katz [4]. For a fuller explanation of how this type of result can be obtained, we refer the reader to our earlier paper [9]. Let N_0 be the smallest positive rational integer belonging to the conductor of the primitive Dirichlet character ρ^{-i}, and let α be any level N_0-structure on E. The isomorphism $\check{\phi}$ fixed by Katz [4] in 8.7.2 is the one corresponding under 8.3.17 to our chosen isomorphism of formal groups η. Thus, the unit defined in 8.3.16 is just $\Omega_{\mathfrak{p}}^{-1}$, and since, as we remarked earlier, Frobenius acts on $\Omega_{\mathfrak{p}}$ by multiplication by $\bar{\psi}(\mathfrak{p})$, it follows that the generator of $\mathfrak{p}$ fixed by Katz in 8.7.3 is, in fact, $\psi(\mathfrak{p})$. Let f_i be the function on $(Z/N_0Z)^2$ given by

$$f_i(u, v) = \sum_{t \bmod N_0} \rho^{-i}(\alpha(t, v))\,(\det \alpha)^{ut}.$$

Then, the function g on $\mathcal{O}/N_0\mathcal{O}$ corresponding to f_i is the primitive Dirichlet character ρ^{-i}, and so the formulae 8.7.5 show that the measure μ_i defined by

$$\int_{Z_p^2} \phi(x, y)d\mu_i = \frac{1}{N_0}\int_{Z_p^{\times 2}\times(Z/N_0Z)^2}\phi(x/N_0, y)f_i(u, v)d\mu_{N_0}$$

satisfies equations (12) and (13).

If b is any integer congruent to 1 modulo N_0, it is a straightforward exercise using the formulae in Katz to show that the measure $\mu_i^{(a)}$ defined by

$$\int_{Z_p} \phi(x)d\mu_i^{(a)} = \frac{1}{N_0}\int_{Z_p^{\times}\times Z_p\times(Z/N_0Z)^2} \phi(x/N_0)f_i(u, v)d\mu_{N_0}^{(a, b)}$$

has the desired properties.

Before proceeding, we observe that it is a consequence of equation (12) and the fact that the numbers $L_\infty(\bar{\psi}^{k+j}, k)$ belong to K provided $0 \le j < k$, that $L_\infty(\bar{\psi}^{k+j}, k)$ belongs to $K_{\mathfrak{p}}$ for all $k \ge 1$ and $j \ge 0$.

Theorem 9 enables us to prove the following theorem.

THEOREM 10: *Let χ be a non-trivial character of $Gal(F/K)$, and let i_1 and i_2 be integers modulo $(p-1)$ such that $\chi = \chi_1^{i_1}\chi_2^{i_2}$. Then $\chi_0 = \chi\omega^{-i_1}$ and $\chi_{\mathfrak{p}} = \omega^{i_1}$. Choose generators π and γ_χ of $\mathfrak{p}$ and the conductor $\mathfrak{c}_\chi$ of χ_0 as before, and let P_χ be the corresponding $\mathfrak{g}_\chi$-division point of E. Then $L(\mathscr{C}, \chi, P_\chi)$ is an Iwasawa function, and if a is primitive $(p-1)$-th root of unity and $u \equiv 1 - i_1 \bmod (p-1)$*

$$L(\mathscr{C}, \chi, P_\chi)(u) = \begin{cases} -\gamma_\chi\Omega_{\mathfrak{p}} \displaystyle\int (\gamma_\chi x)^{-u}\omega^{-i_2}(y)d\mu_{i_1-i_2}, & i_2 \not\equiv 0 \bmod (p-1), \\ (-\gamma_\chi\Omega_{\mathfrak{p}}/(1-a^{i_1})) \displaystyle\int (\gamma_\chi x)^{-u}d\mu_{i_1}^{(a)}, & i_2 \equiv 0 \bmod (p-1). \end{cases}$$

PROOF: Since $L(\mathscr{C}, \chi, P_\chi)$ is a continuous function, it will suffice to prove that if $k \geq 3$ and $k \equiv i_1 \bmod (p-1)$, $L(\mathscr{C}, \chi, P_\chi)\ (1-k)$ is given by the formula in the theorem, since this a dense subset of $\mathbb{Z}_p$. But, for such k, Theorem 8.2 of Lichtenbaum [5] shows that

$$L(\mathscr{C}, \chi, P_\chi)(1-k) = -\Omega_{\mathfrak{p}}^{1-k}(1-\chi_0(\pi)\pi^k/p)E_{k,\chi_0}/k$$

where E_{k,χ_0} is given by Theorem 7.1 and

$$E_{k,\chi_0} = (-1)^k k!(\gamma_\chi/\Omega_\infty)^k \sum_{\substack{\alpha\in\mathcal{O}\\ \alpha\neq 0}} \frac{\rho^{i_2-i_1}(\alpha)\omega^{-i_2}(\bar{\alpha})}{\alpha^k}.$$

Since $\chi_0(\pi)\pi^k = \omega^{i_2}(\bar{\psi}(\mathfrak{p}))\psi^k(\mathfrak{p})$, the theorem follows immediately from equations (13) and (14).

Let χ be a non-trivial character of Gal(F/K) and choose integers k and j with $0 \leq j < p-1$ and $1 < k \leq p$ such that $\chi = \chi_1^k\chi_2^{-j}$. Since $L(\mathscr{C}, \chi, P_\chi)$ is an Iwasawa function, $L(\mathscr{C}, \chi, P_\chi)(1)$ is an integer in $\mathbb{C}_{\mathfrak{p}}$, and it is a unit if and only if $L(\mathscr{C}, \chi, P_\chi)(1-k)$ is a unit. Now, if $j=0$,

$$L(\mathscr{C}, \chi, P_\chi)(1-k) = (-1)^{k-1}w(k-1)!\Omega_{\mathfrak{p}}^{1-k}\gamma_\chi^k(1-\psi^k(\mathfrak{p})/p)L_\infty(\bar{\psi}^k, k)$$

and so we conclude that $L(\mathscr{C}, \chi, P_\chi)(1)$ is a unit if and only if $L_\infty(\bar{\psi}^k, k)$ is a unit in $\mathbb{C}_{\mathfrak{p}}$.

On the other hand, if $j \neq 0$, it follows from the fact that $y^j \equiv \omega^j(y)$ mod p for all $y \in Z_p$ and Theorem 10, that $L(\mathscr{C}, \chi, P_\chi)(1-k)$ is a unit if and only if $\int x^{k-1}y^j d\mu_{k+j}$ is a unit. Again, we deduce from equation (12) that this is the case if and only if $L_\infty(\bar{\psi}^{k+j}, k)$ is a unit in $\mathbb{C}_{\mathfrak{p}}$.

These facts, together with Corollary 8, yield Theorem 3.

REFERENCES

[1] J. COATES and A. WILES: Kummer's criterion for Hurwitz numbers. *Algebraic Number Theory*, papers contributed for the International Symposium, Kyoto 1976, Japan Society for the Promotion of Science (1977) 9–23.

[2] H. HIDA: Kummer's criterion for the special values of Hecke L-functions of imaginary quadratic fields and congruences among cusp forms (to appear).

[3] A. HURWITZ: Über die Entwicklungskoeffizienten der lemniskatischen Funktionen. *Math. Ann. 51* (1899) 196–226 (=Werke II, 342–373).

[4] N. KATZ: p-adic interpolation of real analytic Eisenstein series. *Ann. Math. 104* (1976) 459–571.

[5] S. LICHTENBAUM: On p-adic L-functions associated to elliptic curves. *Invent. Math. 56* (1980) 19–55.

[6] K. RIBET: A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. *Invent. Math. 34* (1976) 151–162.

[7] G. ROBERT: Unités elliptiques, *Bull. Soc. Math.* France Memoire *36* (1973).
[8] A. WEIL: *Elliptic functions according to Eisenstein and Kronecker.* Springer-Verlag, 1976.
[9] R. YAGER: On two variable p-adic L-functions. *Ann. Math. 115* (1982) 411-449.

(Oblatum 26-I-1982)

Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139
U.S.A.