ON A GENERALIZATION OF A THEOREM OF KUMMER

By

Aichi KUDO

(Received March 18, 1975)

Introduction and theorems

Let p be an odd prime, F a finite totally real extension of the rational number field Q and put $K = F(\zeta_p)$, $K^+ = F(\zeta_p + \zeta_p^{-1})$, where ζ_n denotes a primitive n -th root of unity for every integer $n \geq 1$. Let h and R denote the class number and the regulator of K and h^+ , R^+ the class number, the regulator of K^+ . Then, it is known that $h^+ | h$ and $R/R^+ = 2^e$ for some integer $e \geq 0$. Let w be the number of roots of unity in K and a the number defined by

$$a = \lim_{t \rightarrow 0} \prod_{\substack{p | p \\ \text{in } K}} (1 - Np^{-t}) / \prod_{\substack{p | p \\ \text{in } K^+}} (1 - Np^{-t}), \quad (t: \text{real}),$$

where the products are taken over all primes of K dividing p in the numerator and over that of K^+ in the denominator, and N denotes the absolute norm.

Put $d = [K: F]$. R. Greenberg [3] has derived a congruence to the relative class number $h^- = h/h^+$ for K/K^+ and the values of the Dedekind zeta function $\zeta(s, F)$ of F when $p \nmid [F: Q]$:

$$(1) \quad ah^- \equiv (w/2^{e+1})c \prod_{i=2}^d \zeta(1-i, F) \pmod{p}.$$

Here $\prod''$ means the product over even integers, and the number c is a p -adic unit in Q related to F and p .

In this paper, using the results of J. Coates and W. Sinnott [2], we prove the following

THEOREM 1. *Let F be a finite totally real number field which is abelian over a real quadratic field. Then, it follows that*

$$ah^- \equiv (w/2^{e+1}) \prod_{i=2}^d \zeta(-l_i p^v, F) \pmod{p^v}$$

for any given integer $v \geq 1$, where each l_i denotes a positive integer satisfying $l_i p^v \equiv i-1 \pmod{d}$ for even i , $2 \leq i \leq d$.

We see that the above assertion holds for any totally real F if $p \nmid [F:Q]$. It indeed is verified in the same manner as in [3]. For the case where $v=1$, we obtain in particular the following

THEOREM 1'. *Under the assumption of Theorem 1, it follows that*

$$ah^- \equiv (w/2^{e+1})d \prod_{i=2}^d \zeta(1-i, F) \pmod{p}.$$

In the congruence (1) of Greenberg, it is conjectured that $c=d$ ([1], [3] and [5]).

Now, let p^m denote the highest power of p such that $K=F(\zeta_{p^{m+1}})$, and put $e_2=\dots=e_{d-2}=0$ and $e_d=m+1$. Then, it is true in our case that the rational numbers $p^{e_i}\zeta(1-i, F)$ ($2 \leq i \leq d$, i : even) are all p -integral. Whence, by Theorem 1', we have the following

THEOREM 2. *Assume that no prime of K^+ lying over p splits in K , and that there exists some ramified prime of K for the extension $K(\zeta_{p^{m+2}})/K$. Then, p divides the class number h of K if and only if p divides the numerator of at least one of the rational numbers*

$$p^{e_i}\zeta(1-i, F) \quad (2 \leq i \leq d, i: \text{even}).$$

PROOF. Since no prime of K^+ lying over p splits in K , a is in fact a power of 2, and obviously $w=p^{m+1}w'$ with an integer w' prime to p . Hence, Theorem 1' shows that p divides h^- if and only if p divides the numerator of at least one of the $p^{e_i}\zeta(1-i, F)$, where $2 \leq i \leq d$ and i even. On the other hand, one sees that $p|h$ implies $p|h^-$ applying the theorem of S.-N. Kuroda [4] to the extension K/K^+ , or directly as in [3].

Proof of Theorems 1 and 1'

1. We must state here the results of Coates and Sinnott [2]. First, let k be an arbitrary finite totally real number field. Let Z denote the ring of rational integers and Z_p , Q_p and Ω_p the ring of rational p -adic integers, the field of rational p -adic numbers, and the algebraic closure of Q_p . We define the algebraic number $L^*(-n, \psi)$ and the rational number $\zeta^*(-n, k)$ with $n \in Z$, $n \geq 0$ by

$$\prod_{\substack{p|p \\ \text{in } k}} (1 - \psi(p)Np^n)L(-n, \psi) \quad \text{and} \quad \prod_{\substack{p|p \\ \text{in } k}} (1 - Np^n)\zeta(-n, k)$$

respectively, where $L(s, \psi)$ denotes the usual Hecke L -function to the primitive ray class character ψ of k . They may be considered as contained in Ω_p . Let ω denote the unique Z_p -valued Dirichlet character mod p such that $\omega(x) \equiv x \pmod{p}$ for all $x \in Z$, $(x, p) = 1$. Then, we can define the primitive ray class character ω_k of k belonging to $k(\zeta_p)/k$, putting $\omega_k(\mathfrak{a}) = \omega(N\mathfrak{a})$ for every integral ideal $\mathfrak{a}$ of k prime to p . Recall that every $x \in Z$, $(x, p) = 1$, can be decomposed uniquely in Z_p as $x = \omega(x) \langle x \rangle$, $\langle x \rangle \in 1 + pZ_p$.

Now, assume that k is a real quadratic field. For each character χ of k to any finite abelian extension of k , Coates and Sinnott [2] have constructed the p -adic L -function $L_p(s, \chi)$ for $s \in Z_p$, $s \neq 1$. Let $\mathfrak{o}_\chi$ denote the ring generated by the values of χ over Z_p and $\Lambda_\chi = \mathfrak{o}_\chi[[T]]$ the formal power series ring over $\mathfrak{o}_\chi$. Then, the p -adic L -function $L_p(s, \chi)$ is expressed by the element $f(T, \chi)$ of the quotient field of Λ_χ in the form

$$L_p(s, \chi) = f((1+p)^s - 1, \chi)$$

for all $s \in Z_p$, $s \neq 1$. Accurately, $f(T, \chi)$ is characterized by the equalities $f((1+p)^{1-n} - 1, \chi) = L^*(1-n, \chi\omega_k^{-n})$ for all $n \in Z$, $n \geq 1$. Further, let P_n be the unique cyclic subfield of $Q(\zeta_{p^{n+1}})$ of degree p^n over Q for $n \geq 1$, and put $k_n = kP_n$, $k_\infty = \bigcup_{n \geq 1} k_n$. Then, it is also shown [2] that if χ is not a character of k_∞/k , $f(T, \chi)$ is contained in Λ_χ , and if χ is a character of k_∞/k , putting $\langle Nc \rangle = (1+p)^{\tau(c)}$ with $\tau(c) \in Z_p$ for every integral ideal $c \neq 1$ of k prime to p , $(1 - \langle Nc \rangle \chi(c)(1+T)^{-\tau(c)})f(T, \chi)$ is contained in Λ_χ .

Denote by v_p the exponential valuation of Z_p normalized so that $v_p(p) = 1$ and let $f(T)$ be an element of $\Lambda = \mathfrak{o}[[T]]$, where $\mathfrak{o}$ denotes the ring of integers of a finite extension L of Q_p . Then we see that

$$f((1+p)^s - 1) \equiv f((1+p)^{s'} - 1) \pmod{p^{1+v_p(s-s')}\mathfrak{o}}$$

for all s and s' in Z_p . In fact, since the ring Λ is generated by $1+T$ as a topological $\mathfrak{o}$ -algebra, it is sufficient for the proof to consider the case where $f(T) = 1+T$. By the linearity and by passing to the limit, we can prove the assertion in general cases.

2. Let k be a real quadratic field and F the finite totally real number field which is abelian over k , and put $K = F(\zeta_p)$, $K^+ = F(\zeta_p + \zeta_p^{-1})$ and $d = [K:F]$ as before. Let X , X_1 denote the corresponding group of Ω_p -valued primitive ray

class characters of k for F, K^+ respectively. From the results mentioned above, we see that if $\chi \in X_1$ is not a character of k_∞/k ,

$$(2) \quad L_p(0, \chi) \equiv L_p(-n, \chi) \pmod{p^{1+v_p(n)} \mathfrak{o}_\chi}$$

for all $n \in \mathbb{Z}, n \geq 0$, and if χ is a character of k_∞/k ,

$$(3) \quad (1 - \langle N\mathfrak{c} \rangle \chi(\mathfrak{c})) L_p(0, \chi) \equiv (1 - \langle N\mathfrak{c} \rangle^{n+1} \chi(\mathfrak{c})) L_p(-n, \chi) \pmod{p^{1+v_p(n)} \mathfrak{o}_\chi}$$

for $n \geq 0$ and for any integral ideal $\mathfrak{c} \neq 1$ of k prime to p .

Now, let i be an even integer and suppose that $n \equiv i \pmod{d'}$ for $n \geq 1$, where $d' = [k(\zeta_p): k]$. We have by the definition of $L_p(s, \chi)$ that $L_p(1-n, \chi \omega_k^i) = L^*(1-n, \chi)$. Hence, we obtain for such n ,

$$\prod_{\chi \in X} L_p(1-n, \chi \omega_k^i) = \prod_{\chi \in X} L^*(1-n, \chi) = \zeta^*(1-n, F).$$

On the other hand, let $L_p(s, \omega_F^i)$ denote the Serre p -adic zeta function of F for each even i , i.e., the continuous function of $s \in \mathbb{Z}_p, s \neq 1$ such that

$$L_p(1-n, \omega_F^i) = \zeta^*(1-n, F)$$

for all $n \geq 1, n \equiv i \pmod{d}$. Therefore, by continuity, it must follow that

$$(4) \quad L_p(s, \omega_F^i) = \prod_{\chi \in X} L_p(s, \chi \omega_k^i)$$

for all $s \in \mathbb{Z}_p, s \neq 1$.

Now, let $i \not\equiv 0 \pmod{d}$. Then, we see that there is no character of k_∞/k in $\{\chi \omega_k^i | \chi \in X\}$. Indeed, suppose that $\chi \omega_k^i$ is a character of k_∞/k . Then the order of $\chi \omega_k^i$ is a power of p , say p^n , so we have $\omega_k^i \in X$ from $1 = (\chi \omega_k^i)^{p^n} = \chi^{p^n} \omega_k^i$. This means that $i \equiv 0 \pmod{d}$. Hence, if $i \not\equiv 0 \pmod{d}$, we have from (2) and (4)

$$(5) \quad L_p(0, \omega_F^i) \equiv L_p(-n, \omega_F^i) \pmod{p^{1+v_p(n)}}$$

for all integers $n \geq 0$.

When $i \equiv 0 \pmod{d}$, let m be the greatest positive integer such that $F(\zeta_p) \cong Q(\zeta_{p^{m+1}})$. Because the degree

$$[Q(\zeta_{p^{m+1}}): F \cap Q(\zeta_{p^{m+1}})] = [F(\zeta_{p^{m+1}}): F] = [F(\zeta_p): F]$$

divides $p-1$, $F \cap Q(\zeta_{p^{m+1}})$ and therefore F contains P_m . Hence $X \omega_k^i = X$ contains

all characters of k_m/k , and conversely, it is obvious that the characters of k_∞/k in X is just the ones of k_m/k .

In (3), choose the ideal $\mathfrak{c}$ so that the Artin symbol $(\mathfrak{c}, k_1/k)$ generates the Galois group $G(k_1/k)$ of k_1/k . Then $\langle N\mathfrak{c} \rangle$ is a topological generator of $1 + p\mathbb{Z}_p$ and $\tau(\mathfrak{c})$ is a unit in $\mathbb{Z}_p$. Since $\chi(\mathfrak{c})$ ranges exactly over all p^m -th roots of unity when χ ranges over the group of characters of k_∞/k in X , we have from (2), (3) and (4) that

$$(1 - \langle N\mathfrak{c} \rangle^{p^m})L_p(0, \omega_F^i) \equiv (1 - \langle N\mathfrak{c} \rangle^{(n+1)p^m})L_p(-n, \omega_F^i) \pmod{p^{1+v_p(n)}},$$

for all $n \geq 0$. Now let us consider only $n \geq 0$ such that $v_p(n) \geq 1$. Since

$$\begin{aligned} 1 - \langle N\mathfrak{c} \rangle^{(n+1)p^m} &= 1 - \langle N\mathfrak{c} \rangle^{p^m} \langle N\mathfrak{c} \rangle^{p^m \cdot n} \\ &\equiv 1 - \langle N\mathfrak{c} \rangle^{p^m} \pmod{p^{m+1+v_p(n)}}, \end{aligned}$$

we obtain

$$\frac{1 - \langle N\mathfrak{c} \rangle^{p^m}}{p^{m+1}} p^{m+1} L_p(0, \omega_F^i) \equiv \frac{1 - \langle N\mathfrak{c} \rangle^{p^m}}{p^{m+1}} p^{m+1} L_p(-n, \omega_F^i) \pmod{p^{v_p(n)}}$$

for all $n \geq 0$, $v_p(n) \geq 1$. Dividing the both sides by p -adic unit $(1 - \langle N\mathfrak{c} \rangle^{p^m})/p^{m+1}$, we have

$$(6) \quad p^{m+1} L_p(0, \omega_F^i) \equiv p^{m+1} L_p(-n, \omega_F^i) \pmod{p^{v_p(n)}}$$

for all $n \geq 0$, $v_p(n) \geq 1$, when $i \equiv 0 \pmod{d}$.

3. For any finite totally real number field F , Greenberg [3] has proved the formula

$$(7) \quad ah^- = (w/2^{e+1}) \prod_{i=2}^d L_p(0, \omega_F^i).$$

By the definition of $L_p(s, \omega_F^i)$, we see that $L_p(0, \omega_F^i) = 0$ with even i if and only if there exist such primes $\mathfrak{p}$ of F dividing p that $\omega_F^{i-1}(\mathfrak{p}) = 1$. Hence, if some prime of K^+ lying over p splits in K , the formula (7) means that $0=0$, and each result obtained in the sequel is valid in the sense that the number in the right hand side is congruent to 0.

For each $i=2, \dots, d$ (i : even) and each given $v \geq 1$, let l_i be one of the positive integers such that $l_i p^v \equiv i-1 \pmod{d}$. Then, by a property of the Serre p -adic zeta function, it is obvious that

$$\begin{aligned} p^{e_i} L_p(-l_i p^v, \omega_F^i) &= p^{e_i} L_p(-l_i p^v, \omega_F^{1+l_i p^v}) = p^{e_i} \zeta^*(-l_i p^v, F) \\ &\equiv p^{e_i} \zeta(-l_i p^v, F) \pmod{p^v}. \end{aligned}$$

Hence, from (5) and (6) we have the congruence of p -adic integers

$$(8) \quad p^{e_i} L_p(0, \omega_F^i) \equiv p^{e_i} \zeta(-l_i p^v, F) \pmod{p^v} \quad (2 \leq i \leq d, i: \text{even}).$$

Noticing again that $p^{e_d} \parallel w$, we obtain from (7) and (8)

$$(9) \quad ah^- \equiv (w/2^{e+1}) \prod_{i=2}^d \zeta(-l_i p^v, F) \pmod{p^v}.$$

This completes the proof of Theorem 1.

To the case where $v=1$, we observe that

$$\begin{aligned} 1 - \langle Nc \rangle^{(n+1)p^m} &= 1 - \{1 - (1 - \langle Nc \rangle^{p^m})\}^{n+1} \\ &\equiv (n+1)(1 - \langle Nc \rangle^{p^m}) \pmod{p^{m+2}(n+1)}. \end{aligned}$$

For even i , $2 \leq i \leq d-2$, we know by (5) that

$$L_p(0, \omega_F^i) \equiv L_p(1-i, \omega_F^i) \pmod{p}.$$

For $i=d$, since $d \not\equiv 0 \pmod{p}$, it follows from the fact considered above that

$$p^{m+1} L_p(0, \omega_F^d) \equiv p^{m+1} d \cdot L_p(1-d, \omega_F^d) \pmod{p}.$$

Hence, we obtain in the same manner concluding (9) that

$$\begin{aligned} ah^- &\equiv (w/2^{e+1}) \cdot d \prod_{i=2}^d L_p(1-i, \omega_F^i) \pmod{p} \\ &\equiv (w/2^{e+1}) \cdot d \prod_{i=2}^d \zeta^*(1-i, F) \pmod{p} \\ &\equiv (w/2^{e+1}) \cdot d \prod_{i=2}^d \zeta(1-i, F) \pmod{p}. \end{aligned}$$

Thus, we complete the proof of Theorem 1'.

References

- [1] J. COATES and S. LICHTENBAUM, *On l -adic zeta functions*, Ann. of Math., **98** (1973), 498-550.

- [2] J. COATES and W. SINNOTT, *On p -adic L -functions over real quadratic fields*, Inv. Math., **25** (1974), 253–279.
- [3] R. GREENBERG, *A generalization of Kummer's criterion*, Inv. Math., **21** (1973), 247–254.
- [4] S.-N. KURODA, *Über den allgemeinen Spiegelungssatz für Galoissche Zahlkörper*, J. Number Theory, **2** (1970), 282–297.
- [5] J. P. SERRE, *Formes modulaires et fonctions zêta p -adiques*, Lecture Notes in Math., **350** (1973), 191–268.