VANDIVER'S CONGRUENCE FOR THE RELATIVE CLASS NUMBER OF AN IMAGINARY ABELIAN FIELD

By

Tsuyoshi UEHARA

(Received Oct. 30, 1974)

1. Introduction

Let p be a prime, $\mathbf{Q}$ the rational number field, $\mathbf{Z}$ the ring of rational integers, $\mathbf{Q}_p$ the rational p -adic number field and $\mathbf{Z}_p$ the ring of rational p -adic integers. Let h_0^- be the relative class number of the p -th cyclotomic field $K_0 = \mathbf{Q}(e^{\frac{2\pi i}{p}})$.

Vandiver obtained a congruence for h_0^- to the case $p > 2$ as follows [3], [12]:

$$h_0^- \equiv (-1)^{\frac{p-1}{2}} 2^{-\frac{p-3}{2}} p \prod_m B_{mp^l+1} \pmod{p^l}$$

where m runs over all odd rational integers between 0 and $p-1$ and B_n denotes the n -th Bernoulli number.

Recently generalizations of this formula were given by Shiratani and Slavutsky in [8], [10] and [11].

In this note we shall give a supplement to [8], [10] and [11], i.e. a generalized congruence for the relative class number of a given imaginary abelian field, applying the same method as [3], [10]. Namely we use the theory of p -adic L -functions defined by Kubota-Leopoldt [5] and Iwasawa [4].

The author wishes to thank Professor K. Shiratani for his kind suggestions.

2. Kummer's congruences

In this section we give a slightly variant proof of the results for Kummer's congruences of Shiratani [9] with an improvement to the case $p=2$.

Let χ be a Dirichlet character with its values contained in an algebraic closure $\bar{\mathbf{Q}}_p$. The symbol $B_n(\chi)$ denotes the n -th generalized Bernoulli number with respect to χ in the sense of Leopoldt [7]. Let $q=p$ for $p > 2$ and $q=4$ for $p=2$.

We define ω as a Dirichlet character with conductor q and $\omega(x) \equiv x \pmod{q}$ for $x \in \mathbf{Z}$, $(x, p) = 1$. It is clear that $\omega(x) = \lim_{\rho \rightarrow \infty} x^{p^\rho}$ ($p > 2$) or $\omega(x) = \pm 1$ ($p = 2$) for $x \in \mathbf{Z}$, $(x, p) = 1$. We put $\langle x \rangle = x\omega^{-1}(x)$ for $x \in \mathbf{Z}$, $(x, p) = 1$.

For any given positive integer n , we define $b_n(\chi)$ as follows:

$$b_n(\chi) = (1 - \chi\omega^{-n}(p)p^{n-1}) \frac{B_n(\chi\omega^{-n})}{n}.$$

We remark that the p -adic L -function $L_p(s, \chi)$ is characterized as a continuous function of $s \in \mathbf{Z}_p$ (except $s = 1$ if $\chi = \varepsilon$) which satisfies

$$L_p(1 - n, \chi) = -b_n(\chi)$$

for any positive integer n . This function is determined uniquely because the positive integers are dense in $\mathbf{Z}_p$.

From Witt's formula, we have the following [9]:

$$(1) \quad b_n(\chi) = \lim_{\rho \rightarrow \infty} \frac{1}{nf p^\rho} \sum_{x=1}^{f p^\rho} \chi(x) \langle x \rangle^n$$

where f is the conductor of χ and $*$ means to take sum over all rational integers prime to p in the given range.

Because $\langle x \rangle \in 1 + q\mathbf{Z}_p$ for $x \in \mathbf{Z}$, $(x, p) = 1$, we can find $u_\rho(x)$, $R_\rho(x)$ uniquely for $\rho \geq 0$ which satisfy

$$(2) \quad \langle x \rangle = (1 + q)^{u_\rho(x)} + R_\rho(x) q p^\rho$$

where $R_\rho(x) \in \mathbf{Z}_p$ and $u_\rho(x) \in \mathbf{Z}$, $0 \leq u_\rho(x) < p^\rho$.

Here, let $f = f_0 p^\mu$, $(f_0, p) = 1$, $\mu \geq 0$, then we can have a canonical decomposition $\chi = \chi_0 \omega^h \chi_1$ where the conductor of χ_0 is f_0 and χ_1 is a character of the second kind [4], i.e. the conductor and order of χ_1 are both some powers of p and $\chi_1(x)$ depends upon only $\langle x \rangle$. In this note $\mathfrak{X}_2$ denotes the set of characters of the second kind.

By substituting (2) to (1), we have

$$(3) \quad b_n(\chi) - c_n(\chi) = \lim_{\rho \rightarrow \infty} \frac{1}{f_0} \sum_{x=1}^{f_0 q p^{\mu+\rho}} \chi(x) (1 + q)^{(n-1)u(x)} R(x)$$

where $u(x) = u_{\mu+\rho}(x)$, $R(x) = R_{\mu+\rho}(x)$ and $c_s(\chi)$ is defined for $s \in \mathbf{Z}_p$ (except $s = 0$ if $\chi = \varepsilon$) as follows [9]:

$$c_s(\chi) = \begin{cases} \frac{1-p}{p} \log(1+q) \frac{1}{1-\chi(1+q)(1+q)^s} & \text{in the case } \chi = \varepsilon \text{ or } \chi \in \mathfrak{K}_2 \\ 0 & \text{in the other case.} \end{cases}$$

We transform the right hand side of (3) to the case $p=2$. Let $1 \leq x < 2^{2+\mu+\rho}f_0$, $x \equiv 1 \pmod{4}$ and $y = 2^{2+\mu+\rho}f_0 - x$, then we can easily see $u(x) = u(y)$ and $R(x) = R(y) + f_0$. Hence

$$\begin{aligned} \sum_x^* \chi(x) 5^{(n-1)u(x)} R(x) &= (\chi(1) + \chi(-1)) \sum_x^{**} \chi(x) 5^{(n-1)u(x)} R(x) \\ &\quad - \chi(-1) f_0 \sum_x^{**} \chi(x) 5^{(n-1)u(x)}, \end{aligned}$$

where x runs over the rational integers between 1 and $2^{2+\mu+\rho}f_0$ and $**$ means to take sum over all rational integers congruent to 1 mod 4 in the given range. It holds that

$$\lim_{\rho \rightarrow \infty} \sum_x^{**} \chi(x) 5^{(n-1)u(x)} = 0$$

Thus, in this special case we have

$$(3)' \quad b_n(\chi) - c_n(\chi) = \lim_{\rho \rightarrow \infty} \frac{\chi(1) + \chi(-1)}{f_0} \sum_x^{**} \chi(x) 5^{(n-1)u(x)} R(x).$$

The operator Δ is defined by $\Delta a_n = a_{n+1} - a_n$ for a sequence $\{a_n\}$ in $\bar{\mathbf{Q}}_p$. It holds that

$$\Delta^k(1+q)^{(n-1)u(x)} = (1+q)^{(n-1)u(x)}((1+q)^{u(x)} - 1)^k.$$

Therefore we obtain

PROPOSITION. For $k \geq 0$ and $n \geq 1$, it holds that

$$\Delta^k(b_n(\chi) - c_n(\chi)) \equiv 0 \pmod{q^{k+1}p^{-1}}.$$

By virtue of Proposition the series

$$\sum_{k=0}^{\infty} \binom{-s}{k} \Delta^k(b_1(\chi) - c_1(\chi))$$

is convergent for $s \in \mathbf{Z}_p$ and according to [1], [9] the p -adic L -function can be defined as follows:

$$L_p(s, \chi) = - \sum_{k=0}^{\infty} \binom{-s}{k} \Delta^k (b_1(\chi) - c_1(\chi)) - c_{1-s}(\chi)$$

for $s \in \mathbf{Z}_p$ (except $s=1$ if $\chi=\varepsilon$).

3. Vandiver's formula

Let K be a given imaginary abelian field with degree $2g$, $\mathfrak{X}$ its character group and $\mathfrak{X}^-$ denote the set of odd characters of $\mathfrak{X}$. Then the relative class number h^- of K is expressed as follows [2], [10]:

$$(4) \quad h^- I_K = Q_K w 2^{-g} \prod_{\chi \in \mathfrak{X}^-} L_p(0, \chi \omega)$$

where

$$I_K = \prod_{\chi \in \mathfrak{X}^-} (1 - \chi(p))$$

and

$$Q_K = 2^{g-1} R^+ / R.$$

Herein R, R^+ are the regulators of K , the maximal real subfield of K respectively and w is the number of the roots of unity contained in K .

Now, we obtain from Proposition

$$L_p(0, \chi) \equiv -c_1(\chi) \pmod{qp^{-1}}.$$

Hence,

$$\text{ord}_p L_p(0, \varepsilon) = -1$$

and for $\chi \in \mathfrak{X}_2$,

$$\text{ord}_p L_p(0, \chi) = \text{ord}_p (qp^{-1} (1 - \chi(1+q))^{-1})$$

and for the other case,

$$\text{ord}_p L_p(0, \chi) \geq \text{ord}_p (qp^{-1}).$$

By definition, we have

$$\begin{aligned} L_p(0, \chi) - L_p(s, \chi) \\ = \sum_{k=1}^{\infty} \binom{-s}{k} \Delta^k (b_1(\chi) - c_1(\chi)) + c_{1-s}(\chi) - c_1(\chi) \end{aligned}$$

for $s \in \mathbf{Z}_p$. Let $\text{ord}_p s = l$, then we have the following congruences by investigating the order of $c_{1-s}(\chi) - c_1(\chi)$ at p in detail:

$$L_p(0, \varepsilon) \equiv L_p(s, \varepsilon) \pmod{p^{l-1}}$$

and for $\chi \neq \varepsilon$,

$$L_p(0, \chi) \equiv L_p(s, \chi) \pmod{p^{l-1}q}.$$

Thus, we can see

$$(5) \quad \prod_{\chi \in \mathfrak{X}^-} L_p(0, \chi\omega) \equiv \prod_{\chi \in \mathfrak{X}^-} L_p(s_\chi, \chi\omega) \pmod{p^{l-g}q^{g-1} \prod_{\chi'} (1 - \chi'\omega(1+q))^{-1}}$$

where $s_\chi \in \mathbf{Z}_p$, $\text{ord}_p s_\chi = l$ ($\chi \in \mathfrak{X}^-$) and χ' runs over all characters such that $\chi' \in \mathfrak{X}^-$ and $\chi'\omega \in \mathfrak{X}_2$. If $\omega \notin \mathfrak{X}$, (5) holds modulo $p^{l-g}q^g \prod_{\chi'} (1 - \chi'\omega(1+q))^{-1}$.

Let $\chi_1 = \chi\omega$ be the character of the second kind such that $\chi \in \mathfrak{X}^-$ and order of χ_1 is maximal; this order denotes p^v . If $\omega \in \mathfrak{X}$, then $\{\omega^i \chi_1^i\} \subset \mathfrak{X}$. This implies that $Q(e^{\frac{2\pi i}{qp^v}})$ is contained in K and therefore $2p^{v+1}|w$ and $\prod_{\chi'} (1 - \chi'\omega(1+q)) = p^v$. If $p > 2$, $\omega = \omega^{p^v} = \chi_1^{p^v} \chi^{-p^v} = \chi^{-p^v}$ and therefore $\omega \in \mathfrak{X}$. We assume that $p = 2$ and $\omega \notin \mathfrak{X}$. Then $\prod_{\chi'} (1 - \chi'\omega(5)) = \prod_j (1 - \chi_1^j(5)) = 2$, where j runs over all odd integers between 0 and $2^v - 1$. It is easy to see $2|w$ in general.

Consequently, we have the following theorem by multiplying the both sides of (5) by $Q_K w 2^{-g}$:

THEOREM. For $l \geq 1$ and $s_\chi \in p^l \mathbf{Z}_p$ ($\chi \in \mathfrak{X}^-$), it holds that

$$h^{-1} I_K \equiv Q_K w 2^{-g} \prod_{\chi \in \mathfrak{X}^-} L_p(s_\chi, \chi\omega) \pmod{p^l}.$$

If $p > 2$, we see

$$\begin{aligned} & Q_K w 2^{-g} \prod_{\chi \in \mathfrak{X}^-} L_p(-n_\chi p^l, \chi\omega) \\ &= Q_K w 2^{-g} \prod_{\chi \in \mathfrak{X}^-} -B_{n_\chi p^l + 1}(\chi\omega^{-n_\chi}) \prod_{\chi \in \mathfrak{X}^-} \frac{1 - \chi\omega^{-n_\chi}(p)p^{n_\chi p^l}}{1 + n_\chi p^l} \end{aligned}$$

for positive integers n_χ ($\chi \in \mathfrak{X}^-$). The both sides are p -adic integers. Then, in this case we have

$$(7) \quad h^{-1} I_K \equiv Q_K w 2^{-g} \prod_{\chi \in \mathfrak{X}^-} -B_{n_\chi p^l + 1}(\chi\omega^{-n_\chi}) \pmod{p^l}.$$

If $K = Q(e^{\frac{2\pi i}{p^{v+1}}})$, $p > 2$, then $g = p^v(p-1)/2$, $w = 2p^{v+1}$, $Q_K = I_K = 1$ and $\mathfrak{X} = \{\omega^i \chi_1^j\}$ [2]. We put $n_{\omega^i \chi_1^j} = i$, then it holds that

$$(8) \quad h^- \equiv (-1)^{\frac{p-1}{2}} \cdot 2^{1-p^v \frac{p-1}{2}} \cdot p^{v+1} \prod_i \prod_{j=0}^{p^v-1} B_{ip^i+1}(\chi_1^j) \pmod{p^l}$$

where i runs over all odd integers between 0 and $p-1$.

The congruence (8) is exactly Vandiver's congruence when $v=0$.

Similarly the next congruences hold:

$$(7)' \quad h^- I_K \equiv Q_K w 2^{-g} \prod_{\chi \in \mathfrak{X}^-} -B_{n_\chi 2^l+1}(\chi) \pmod{2^l}$$

and especially, if $K = Q(e^{\frac{2\pi i}{2^{v+2}}})$

$$(8)' \quad h^- \equiv 2^{2+v-2^v} \prod_{j=0}^{2^v-1} B_{n_j 2^l+1}(\chi_1^j \omega) \pmod{2^l}.$$

References

- [1] J. FRESNEL, *Nombres de Bernoulli et fonctions L p-adiques*, Ann. Inst. Fourier, **17** (1967), 281-333.
- [2] H. HASSE, *Über die Klassenzahl abelscher Zahlkörper*, Berlin, 1952.
- [3] H. HASSE, *Vandiver's congruence for the relative class number of the p-th cyclotomic field*, Journ. Math. Anal. Appl., **15** (1966), 87-90.
- [4] K. IWASAWA, *On p-adic L-functions*, Ann. Math., **87** (1969), 198-205.
- [5] T. KUBOTA und H. W. LEOPOLDT, *Eine p-adische Theorie der Zetawerte*, I, Journ. reine u. angew. Math., **214/215** (1964), 328-339.
- [6] A. KUDO, *On a class number relation of imaginary abelian fields*, Journ. of Math. Socie. Japan, (to appear).
- [7] H. W. LEOPOLDT, *Eine Verallgemeinerung der Bernoullischen Zahlen*, Abh. Math. Sem. Univ. Hamburg, **22** (1958), 131-140.
- [8] K. SHIRATANI, *A generalization of Vandiver's congruence*, Mem. Fac. Sci., Kyushu Univ., **25** (1971), 144-151.
- [9] K. SHIRATANI, *Kummer's congruence for generalized Bernoulli number and its application*, Mem. Fac. Sci., Kyushu Univ., **26** (1972), 119-138.
- [10] K. SHIRATANI, *On certain values of p-adic L-functions*, Mem. Fac. Sci., Kyushu Univ., **28** (1974), 59-82.
- [11] И. Ш. СЛАВУТСКИЙ, *Локальные свойства чисел Бернулли и обобщение теоремы Куммера-Вандивера*, И. В. У. З., **118** (1972), 61-69.
- [12] H. S. VANDIVER, *On the first factor of the class number of a cyclotomic field*, Bull. Amer. Math. Soc., **25** (1919), 458-461.