GENERALIZED BERNOULLI NUMBERS AND THE BASIC Z_p -EXTENSIONS OF IMAGINARY QUADRATIC NUMBER FIELDS

By

Aichi KUDO

(Received Sept. 1, 1977)

1. Let k_0 be an imaginary quadratic number field and let p be a prime number. For each rational integer $n \geq 0$, let ζ_{qp^n} denote a primitive qp^n -th root of unity, where we set $q=p$ if $p>2$ and $q=4$ if $p=2$. Then the cyclotomic field $Q(\zeta_{qp^n})$ contains uniquely a cyclic subfield P_n of degree p^n over the rational number field Q . The extension k_∞/k_0 , $k_\infty = \bigcup_{n \geq 0} k_0 P_n$, is called the basic Z_p -extension of k_0 . We denote by h_n the class number of the field $k_n = k_0 P_n$, $n \geq 0$.

The purpose of the present note is to deduce a result to a behaviour of the p -part of h_n from the natures of generalized Bernoulli numbers. The result is almost known, and, in fact, will be explained in some different manners. Above all, it is a natural consequence from a construction due to K. Iwasawa [3] of the p -adic L -functions using certain formal power series. Also, R. Gold [1] has shown recently a part of this in another way. In this note, we apply the method used by K. Shiratani [4], [5] to investigate the class number of $Q(\zeta_{qp^n})$ for $p>2$, to the field k_n .

2. Let Q_p be the field of rational p -adic numbers, Z_p the ring of rational p -adic integers and Z the ring of rational integers. For each $n \geq 1$, let ζ_{p^n} be a fixed primitive p^n -th root of unity in an algebraic closure $\bar{Q}_p$ of Q_p . We set $r = \varphi(q)$, where φ is the Euler's function, and denote by ζ_r a fixed primitive r -th root of unity in Q_p .

Throughout this note, the word character will always mean primitive Dirichlet character with values in $\bar{Q}_p$. The character defined modulo a power of p may be considered as a residue class character of Z_p . We then denote by ω the character with conductor q satisfying $\omega(\zeta_r) = \zeta_r$ and $\omega(1+q) = 1$, and by π_n , $n \geq 1$, the character with conductor qp^n satisfying $\pi_n(\zeta_r) = 1$ and $\pi_n(1+q) = \zeta_{p^n}$.

Now, let χ be the odd quadratic character with conductor f_χ corresponding to the extension k_0/Q . Then, for every $m \geq n \geq 1$, the generalized Bernoulli number $B_{\chi\pi_n}^1$ belonging to the character $\chi\pi_n$ is given by the formula

$$B_{\chi\pi_n}^1 = \frac{1}{fq p^m} \sum_{a=1}^{fq p^m} \chi\pi_n(a) a,$$

where f is the rational integer such that $f_\chi = f p^e$, $e \geq 0$ and $(f, p) = 1$.

In the following, we shall assume that $f_\chi = f$ or $f q$ and $f > 1$. Then, as is well-known, the number $\frac{1}{2} B_{\chi\pi_n}^1$ is an integer of the local field $Q_p(\zeta_{p^n})$. Letting $\lambda_n = 1 - \zeta_{p^n}$, for $n \geq 1$, we first give a formula expressing the number $\frac{1}{2} B_{\chi\pi_n}^1$ as a polynomial in λ_n with coefficients in Z_p .

Define for each pair of integers $1 \leq \alpha \leq f-1$, $0 \leq x \leq r-1$ and $0 \leq y \leq p^m-1$ the integer $0 < c_m(\alpha; x, y) < f q p^m$ by

$$c_m(\alpha; x, y) \equiv \begin{cases} \zeta_r^x (1+q)^y & (\text{mod } q p^m) \\ \alpha & (\text{mod } f) \end{cases},$$

and the integers $0 < S_m(x, y) < q p^m$, $0 \leq d_m(\alpha; x, y) \leq f-1$ by

$$c_m(\alpha; x, y) = S_m(x, y) + d_m(\alpha; x, y) q p^m.$$

Also set $i_x = 0$ or $r/2$ according as $f_\chi = f$ or $f q$, so that the character χ may be written as $\chi = \chi_0 \omega^{i_x}$, where χ_0 is a quadratic character with conductor f .

Then we have, by the assumption that $f > 1$,

$$\begin{aligned} \frac{1}{2} B_{\chi\pi_n}^1 &= \frac{1}{2 f q p^m} \sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{x=0}^{r-1} \sum_{y=0}^{p^m-1} c_m(\alpha; x, y) \zeta_r^{i_x x} \zeta_{p^n}^y \\ &= \frac{1}{2 f} \sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{x=0}^{r-1} \sum_{y=0}^{p^m-1} d_m(\alpha; x, y) \zeta_r^{i_x x} \zeta_{p^n}^y \end{aligned}$$

for any $m \geq n$. We see, on the other hand, that

$$\zeta_{p^n}^y = \sum_{k=0}^y (-1)^k \binom{y}{k} \lambda_n^k = \sum_{k=0}^y (-1)^k \lambda_n^k \frac{1}{k!} \sum_{l=0}^k S(k, l) y^l$$

for each rational integer $y \geq 0$, where the numbers $S(k, l)$ are the coefficients of the polynomial

$$X(X-1) \cdots (X-k+1) = \sum_{l=0}^k S(k, l) X^l$$

in $Z[X]$. Hence, if we write

$$B_l^{(m)} = -\frac{1}{2f} \sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{x=0}^{f-1} \sum_{y=0}^{p^m-1} y^l d_m(\alpha; x, y) \zeta_f^{ix^x},$$

for $m \geq 1$ and $l \geq 0$, then the number $\frac{1}{2} B_{\chi^{\pi_n}}^1$ can be expressed for all $m \geq n$ as

$$\frac{1}{2} B_{\chi^{\pi_n}}^1 = \sum_{k=0}^{p^m-1} (-1)^{k-1} \lambda_n^k A_k^{(m)}$$

with

$$A_k^{(m)} = \frac{1}{k!} \sum_{l=0}^k S(k, l) B_l^{(m)}.$$

It can be seen easily that the coefficients $A_k^{(m)}$, $k \geq 0$, $m \geq 1$, are rational p -adic integers. Indeed it is clear if $p > 2$. Then if $p = 2$, since $d_m(\alpha; 1, y) + d_m(f - \alpha; 0, y) = f - 1$ and $\zeta_f^{ix} = (-1)^{ix} = -\chi_0(-1)$, we see

$$B_l^{(m)} = -\frac{1}{f} \sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{y=0}^{p^m-1} y^l d_m(\alpha; 0, y)$$

for all $m \geq 1$ and $l \geq 0$, and therefore for any case $A_k^{(m)}$ are obviously in Z_p . Thus the above formula is the desired expression, which of course is not unique for every fixed m .

For the number $B_{\chi}^1 = \frac{1}{f} \sum_{a=1}^{f-1} \chi(a)a$ ($n=0$), we have by the same argument as above that $\frac{1}{2}(1 - \chi(p))B_{\chi}^1 = -B_0^{(m)} = -A_0^{(m)}$ for all $m \geq 1$. Hence the congruence $\frac{1}{2} B_{\chi^{\pi_n}}^1 \equiv 0 \pmod{\lambda_n}$ holds for every fixed $n \geq 1$ if and only if we have $\frac{1}{2}(1 - \chi(p))B_{\chi}^1 \equiv 0 \pmod{p}$.

Now, we denote by $\text{ord}_{\lambda_n}(a)$, $n \geq 1$, the exponent of the highest power of λ_n dividing the number a in $\mathbb{Q}_p(\zeta_{p^n})$ and by $\text{ord}_p(a)$ the exponent of the highest power of p dividing the number a in $\mathbb{Q}_p$.

PROPOSITION 1. *If $\text{ord}_{\lambda_n}\left(\frac{1}{2} B_{\chi^{\pi_n}}^1\right) = L$ with $0 \leq L < \varphi(p^n)$ for some $n \geq 1$, then $\text{ord}_{\lambda_m}\left(\frac{1}{2} B_{\chi^{\pi_m}}^1\right) = L$ for all $m \geq n$.*

PROOF. By the formula obtained above, the condition that $\text{ord}_{\lambda_n}\left(\frac{1}{2} B_{\chi^{\pi_n}}^1\right) = L < \varphi(p^n)$ is equivalent to that $A_0^{(m)} \equiv \dots \equiv A_{L-1}^{(m)} \equiv 0 \pmod{p}$ and $A_L^{(m)} \not\equiv 0$

(mod p) for all $m \geq n$. Hence, by the same formula, we see that the number $\frac{1}{2}B_{\chi\pi_m}^1$, $m \geq n$, must be divisible exactly by λ_m^L .

PROPOSITION 2. *If $\text{ord}_p\left(\frac{1}{2}(1-\chi(p))B_\chi^1\right)=1$ and $\text{ord}_{\lambda_n}\left(\frac{1}{2}B_{\chi\pi_n}^1\right) > \varphi(p^n)$ for some $n \geq 1$, then $\text{ord}_{\lambda_m}\left(\frac{1}{2}B_{\chi\pi_m}^1\right)=\varphi(p^n)$ for all $m > n$ and $\text{ord}_{\lambda_l}\left(\frac{1}{2}B_{\chi\pi_l}^1\right)=\varphi(p^l)$ for all $0 < l < n$.*

PROOF. From the assumptions, we have $\text{ord}_p(A_0^{(m)})=1$ for all $m \geq 1$ and $\sum_{k=0}^{\varphi(p^n)} (-1)^{k-1} \lambda_n^k A_k^{(m)} \equiv 0 \pmod{\lambda_n^{\varphi(p^n)+1}}$ for all $m \geq n$, and we see that $A_0^{(m)} \equiv \dots \equiv A_{\varphi(p^n)-1}^{(m)} \equiv 0 \pmod{p}$, $A_{\varphi(p^n)}^{(m)} \not\equiv 0 \pmod{p}$ for all $m \geq n$. This implies the first assertion as above. Then the second follows from this and Proposition 1.

3. Next, we shall consider a congruence for $B_{\chi\omega^{-j}}^{j+1}$, $j \geq 0$. We fix a rational integer $h \geq 1$ and define as usual a linear difference operator Δ_h , for any sequence $\{a_j\}$ ($j \geq 0$) of rational p -adic numbers, by $\Delta_h a_j = a_{j+h} - a_j$.

The generalized Bernoulli numbers $B_{\chi\omega^{-j}}^i$, $i \geq 0$, belonging to the character $\chi\omega^{-j}$ satisfy for every $m \geq 0$ the well-known formula

$$\sum_{a=1}^{fqpm} \chi\omega^{-j}(a)a^{j+1} = \frac{1}{j+2} \sum_{k=1}^{j+2} \binom{j+2}{k} B_{\chi\omega^{-j}}^{j+2-k} f^k q^k p^{mk}.$$

We know in our case that the numbers $B_{\chi\omega^{-j}}^i$, $i \geq 0$, are rational p -adic integers, and hence,

$$\sum_{a=1}^{fqpm} \chi\omega^{-j}(a)a^{j+1} \equiv fqp^m B_{\chi\omega^{-j}}^{j+1} \pmod{(j+1)qp^{2m+1}}.$$

Supposing $m \geq 1$, we thus obtain

$$\sum_{\substack{a=1 \\ (a,p)=1}}^{fqpm} \chi\omega^{-j}(a)a^{j+1} \equiv fqp^m(1-\chi\omega^{-j}(p)p^j)B_{\chi\omega^{-j}}^{j+1} \pmod{(j+1)qp^{2m+1}}.$$

On the other hand,

$$\begin{aligned} \sum_{\substack{a=1 \\ (a,p)=1}}^{fqpm} \chi\omega^{-j}(a)a^{j+1} &= \sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{x=0}^{r-1} \sum_{y=0}^{p^m-1} c_m(\alpha; x, y)^{j+1} \zeta_r^{(ix-j)x} \\ &\equiv (j+1)qp^m \sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{x=0}^{r-1} \sum_{y=0}^{p^m-1} S_m(x, y)^j d_m(\alpha; x, y) \zeta_r^{(ix-j)x} \\ &\pmod{(j+1)qp^{2m+1}} \end{aligned}$$

$$\begin{aligned} &\equiv (j+1)qp^m \sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{x=0}^{r-1} \sum_{y=0}^{p^m-1} d_m(\alpha; x, y) \zeta_r^{ix^x} (1+q)^{jy} \\ &\quad (\text{mod } (j+1)qp^{2m+1}) \end{aligned}$$

for every $m \geq 0$. Therefore we have

$$\begin{aligned} &\frac{1}{j+1} (1 - \chi\omega^{-j}(p)p^j) B_{\chi\omega^{-j}}^{j+1} \\ &\equiv \frac{1}{f} \sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{x=0}^{r-1} \sum_{y=0}^{p^m-1} d_m(\alpha; x, y) \zeta_r^{ix^x} (1+q)^{jy} \quad (\text{mod } p^{m+1}) \end{aligned}$$

for every $m \geq 1$.

Now, we operate the Δ_h^l , $l \geq 0$, on the both sides of this congruence with respect to j . Then, since

$$\Delta_h^l (1+q)^{jy} = (1+q)^{jy} \{(1+q)^{yh} - 1\}^l \equiv h^l y^l q^l \quad (\text{mod } h^l p q^l),$$

and we see $\sum_{\alpha=1}^{f-1} \chi_0(\alpha) \sum_{x=0}^{r-1} d_m(\alpha; x, y) \zeta_r^{ix^x}$ lies in $2Z_p$, we obtain

$$\Delta_h^l \frac{1}{2(j+1)} (1 - \chi\omega^{-j}(p)p^j) B_{\chi\omega^{-j}}^{j+1} \equiv -h^l q^l B_l^{(m)} \quad (\text{mod } h^l p q^l)$$

for every m such that $m \geq l \text{ ord}_p(hq)$ and $m \geq 1$.

As the numbers $B_l^{(m)}$ are rational p -adic integers, this congruence clearly amounts to the Kummer's one for the generalized Bernoulli numbers $B_{\chi\omega^{-j}}^{j+1}$, $j \geq 0$, we consider. It namely proves the existence of the p -adic L -function $L_p(s, \chi\omega)$, being continuous on $s \in Z_p$ and satisfying $L_p(-j, \chi\omega) = \frac{-1}{j+1} (1 - \chi\omega^{-j}(p) \cdot p^j) B_{\chi\omega^{-j}}^{j+1}$ for all rational integers $j \geq 0$.

Since m can be considered as arbitrarily large, combining the above result with the formula obtained in section 2, we have the following

PROPOSITION 3. For all $n \geq 1$,

$$\begin{aligned} \frac{1}{2} B_{\chi\pi_n}^1 &\equiv \sum_{k=0}^{p-1} (-1)^{k-1} \lambda_n^k \frac{1}{k!} \sum_{l=0}^k S(k, l) \frac{1}{h^l q^l} \Delta_h^l \frac{-1}{2(j+1)} (1 - \chi\omega^{-j}(p)p^j) B_{\chi\omega^{-j}}^{j+1} \\ &\quad (\text{mod } \lambda_n^p). \end{aligned}$$

Further, since $S(k, l)$, $0 \leq l \leq k$, are rational integers and $S(k, k) = 1$, we can proceed with a similar argument as in [4], [5], and obtain the following

PROPOSITION 4. For $n \geq 1$, let L be such a rational integer that $0 \leq L \leq p-1$

for $n \geq 2$ or $0 \leq L \leq p-2$ for $n=1$. Then it is necessary and sufficient for $\frac{1}{2} B_{\chi\pi_n}^1 \equiv 0 \pmod{\lambda_n^{L+1}}$ that

$$A_h^l \frac{1}{2(j+1)} (1 - \chi\omega^{-j}(p)p^j) B_{\chi\omega^{\frac{1}{2}j}}^{j+1} \equiv 0 \pmod{h^l p q^l}$$

for all $0 \leq l \leq L$.

Now, as is seen clearly from the above discussion, the class $\frac{1}{h^l q^l} A_h^l \frac{1}{2(j+1)} (1 - \chi\omega^{-j}(p)p^j) B_{\chi\omega^{\frac{1}{2}j}}^{j+1}$, modulo p does not depend upon a fixed choice of $j \geq 0$, $h \geq 1$ and a representative $l \geq 1$ modulo $p-1$. So, we shall next consider h as a rational p -adic integer ($\neq 0$), and define the action of A_h , on a function $f(s)$ over Z_p , as $A_h f(s) = f(s+h) - f(s)$. Then the number $\frac{1}{h^l q^l} A_h^l \frac{1}{2} L_p(s, \chi\omega)$ belongs to a fixed class of Z_p modulo p for any s in Z_p , $h (\neq 0)$ in Z_p and for any representative $l \geq 1$ modulo $p-1$. Accordingly, the necessary and sufficient condition for $\frac{1}{2} B_{\chi\pi_n}^1 \equiv 0 \pmod{\lambda_n^{L+1}}$ in Proposition 4 signifies that $A_h^l \frac{1}{2} L_p(s, \chi\omega) \equiv 0 \pmod{h^l p q^l}$ ($0 \leq l \leq L$) for any rational p -adic integers $h \neq 0$ and s . By the way, the condition that $A_h^l \frac{1}{2} L_p(s, \chi\omega) \equiv 0 \pmod{h^l p q^l}$ holds for all integers $l \geq 0$ is equal to that we have $\frac{1}{2} B_{\chi\pi_n}^1 \equiv 0 \pmod{\lambda_n^p}$ for any fixed n such that $n \geq 1$ for $p > 2$ or $n \geq 2$ for $p = 2$.

4. In this section, we shall summarize the above results in the language of the class numbers. Let k_0 , k_n and h_n be as in section 1. As we are concerned with the basic Z_p -extension, we may assume that the field k_0 is of the first kind, namely that the conductor f_χ of the character χ corresponding to the extension k_0/Q can be written as $f_\chi = f$ or $f q$, $(f, p) = 1$. Also we exclude the cases $k_0 = Q(\sqrt{-1})$ for $p=2$ and $k_0 = Q(\sqrt{-3})$ for $p=3$ so that we have $f > 1$. Then, for the first factor h_n^- of h_n , we see that

$$h_n^- = w Q_n \prod_{j=0}^{p^n-1} \left(-\frac{1}{2} B_{\chi\pi_n^j}^1 \right),$$

for all $n \geq 0$, where w and Q_n denote the number of roots of unity in k_0 and the unit index of k_n , respectively. It is well-known that $Q_n = 1$ or 2 . Furthermore, we see in our case that $Q_n = 1$ if $p=2$ [2], because for every $n \geq 0$ the conductors of $\chi\pi_n^j$, $j=0, 1, \dots, p^n-1$, are divisible by $f > 1$, which is odd for $p=2$. Then, since $\text{ord}_p(h_n) = \text{ord}_p(h_n^-)$ for all $n \geq 0$ [3], it follows from the above that $\text{ord}_p(h_n/h_{n-1})$

$$= \text{ord}_{\lambda_n} \left(\frac{1}{2} B_{\chi^n}^1 \right) \text{ for all } n \geq 1.$$

Hence, by the remark before Proposition 1, we see that $h_n/h_{n-1} \equiv 0 \pmod{p}$ for any fixed $n \geq 1$ if and only if $\frac{1}{2}(1 - \chi(p))h_0 \equiv 0 \pmod{p}$.

Propositions 1 and 2 can be stated as the following

THEOREM 1. (i) If $\text{ord}_p(h_n/h_{n-1}) = L$ with $0 \leq L < \varphi(p^n)$ for some $n \geq 1$, then $\text{ord}_p(h_m/h_{m-1}) = L$ for all $m \geq n$.

(ii) If $\text{ord}_p\left(\frac{1}{2}(1 - \chi(p))h_0\right) = 1$ and $\text{ord}_p(h_n/h_{n-1}) > \varphi(p^n)$ for some $n \geq 1$, then $\text{ord}_p(h_m/h_{m-1}) = \varphi(p^n)$ for all $m > n$ and $\text{ord}_p(h_l/h_{l-1}) = \varphi(p^l)$ for all $0 < l < n$.

This result has been utilized to actually determine many examples of Iwasawa invariants $\lambda \geq 0$, $\mu \geq 0$ and ν [1], to which it is known that $\text{ord}_p(h_n) = \lambda n + \mu p^n + \nu$ for all sufficiently large number n .

By the same reason, Proposition 4 proves the following

THEOREM 2. For $n \geq 1$, assume that $h_n/h_{n-1} \equiv 0 \pmod{p^L}$, where L is the integer satisfying $0 \leq L \leq p-1$ for $n \geq 2$ or $0 \leq L \leq p-2$ for $n=1$. Then for $h_n/h_{n-1} \equiv 0 \pmod{p^{L+1}}$, it is necessary and sufficient that

$$\Delta_h^L \frac{1}{2} L_p(s, \chi\omega) \equiv 0 \pmod{h^L p q^L}$$

for arbitrarily chosen rational p -adic integers $h \neq 0$ and s .

Finally we shall state the assertion to $L=1$ in another form when $p=2$ or $p=3$.

Let $K = Q(\sqrt{m})$ for $p=2$ or $K = Q(\sqrt{3m})$ for $p=3$, and let $k_0 = Q(\sqrt{-m})$ be our imaginary quadratic field. In what follows, we assume that $k_0 \neq Q(\sqrt{-1})$ and $Q(\sqrt{-3})$. For the real quadratic field K , let H , D and E denote the class number, the discriminant, and the fundamental unit > 1 , respectively. The quadratic even character corresponding to the extension K/Q is given by $\chi\omega$. Let 'log' mean the p -adic logarithmic function defined on $\bar{Q}_p$.

Then it is well-known that

$$(1 - \chi(p))h_0 = L_p(0, \chi\omega)$$

and

$$\left(1 - \frac{\chi\omega(p)}{p}\right) \frac{H \log E}{\sqrt{D}} = \frac{1}{2} L_p(1, \chi\omega),$$

from which we see that

$$\frac{h_0}{2}(1-\chi(p)) \equiv \frac{H \log E}{\sqrt{D}} \left(1 - \frac{\chi\omega(p)}{p}\right) \pmod{q}$$

because $\frac{1}{2}L_p(0, \chi\omega) \equiv \frac{1}{2}L_p(1, \chi\omega) \pmod{q}$. Similarly, in order that $h_n/h_{n-1} \equiv 0 \pmod{p^2}$, for $n \geq 1$ ($p=3$) or for $n \geq 2$ ($p=2$), it is necessary and sufficient that $\frac{h_0}{2}(1-\chi(p)) \equiv 0 \pmod{p}$ and

$$\frac{h_0}{2}(1-\chi(p)) \equiv \frac{H \log E}{\sqrt{D}} \left(1 - \frac{\chi\omega(p)}{p}\right) \pmod{qp}.$$

References

- [1] R. GOLD, *Examples of Iwasawa invariants*, Acta Arith., **26** (1974), 21–30.
- [2] H. HASSE, *Über die Klassenzahl abelscher Zahlkörper*, Akademie Verlag, Berlin, 1952.
- [3] K. IWASAWA, *Lectures on p -adic L -functions*, Princeton, New Jersey, 1972.
- [4] K. SHIRATANI, *On some relations between Bernoulli numbers and class numbers of cyclotomic fields*, Mem. Fac. Sci. Kyushu Univ., **18** (1964), 127–135.
- [5] K. SHIRATANI, *Ein Satz zu den Relativklassenzahlen der Kreiskörper*, Mem. Fac. Sci. Kyushu Univ., **21** (1967), 132–137.