Kyungpook Mathematical Journal
Vol.34, No.2, 239-246, December 1994

AN APPLICATION OF p-ADIC ZETA FUNCTIONS TO SOME CYCLOTOMIC CONGRUENCES

Katsumi Shiratani

1. Introduction

Let p be an odd prime and ζ be a fixed primitive p-th root of unity. Then take the number $A^{(r)} = \prod_{i=1}^{p-1}(\frac{1-\zeta^i}{1-\zeta})^{i^r}$ in the prime cyclotomic field $\mathbf{Q}(\zeta)$ over the rational $\mathbf{Q}$, where r is even, $2 \leq r \leq p-3$.

Then Washington [5] proved the following theorem by making use of theory of p-adic L-functions, more precesely speaking, by Leopoldt's formula for $L_p(1,\chi)$. If there exists $q \in \mathbf{Z}$, the rational integer ring, with $A^{(r)} \equiv q \pmod{p}$, then p divides the Bernoulli number B_{p-1-r}. Conversely, if $p|B_{p-1-r}$, then there exists $q \in \mathbf{Z}$ with $A^{(r)} \equiv q^p \pmod{p(1-\zeta)^2}$.

The first half of this assertion was proved by Thaine, as was remarked by Washington. Similarly, another congruence of Thaine was proved by p-adic logarithms in [5].

In the present note we shall show that the congruence of Thaine can be also derived by making use of a formula to $G_p(1,\chi)$, which is a similar one to Leopoldt's formula. Here the function $G_p(s,\chi)$ means the interpolating function for the Euler numbers [2].

Let $B^{(r)} = \prod_{i=1}^{p-1}(a+b\zeta^i)^{i^r}$, where a, b are rational integers. Then the theorem of Thaine is stated as follows. Let $1 \leq r \leq p-3$ and suppose $p \not| ab(a+b)$. If there exists $q \in Z$ with $B^{(r)} \equiv q \pmod{p}$, then

$$\sum_{j=1}^{p-1} j^{p-2-r}(\frac{-b}{a})^j \equiv 0 \pmod{p}.$$

Received July 16, 1993.
Revised April 7, 1994.

Conversely, if this congruence holds, there exists $q \in \mathbf{Z}$ with $B^{(r)} \equiv q^p \pmod{p(1-\zeta)^2}$.

Hasse [1] treated already these numbers above in the left hand side, and indeed used the polynomials

$$f_m(t) = \sum_{j=1}^{p-1} j^{m-1} t^j \quad (m = 2, \cdots, p-2).$$

Thus by Hasse's notation we can rewrite the above congruence such as $f_{p-1-r}(\frac{-b}{a}) \equiv 0 \pmod{p}$. In the following we show that these numbers coincide just with the Euler numbers which were treated in [2], and therefrom a simple proof of the theorem of Thaine can be given by making use of the formula for $G_p(1, \chi)$.

We are able to discuss these cyclotomic congruences from the view point of the classical Kummer's logarithmic differential quotients, namely from the standpoint of explicit reciprocity laws. This method gives us more various assertions.

2. Euler numbers and p-adic zeta functions

Let χ be a Dirichlet character with the conductor f and u be an algebraic number $\neq 0, 1$. Then we define generalized Euler numbers $H_\chi^n(u)$ belonging to u as follows:

$$\frac{1-u^f}{u^f} \sum_{a=0}^{f-1} \frac{\chi(a) e^{aX} u^{f-a}}{e^{fX} - u^f} = e^{H_\chi(u)X}.$$

In the case where χ is the principal character χ^0 the generalized Euler numbers $H_{\chi^0}^n(u)$ are the ordinary Euler numbers $H^n(u)$ belonging to u [2].

Then we have for any $n \geq 0$

$$\frac{u^f}{1-u^f} H_\chi^n(u) = \frac{1}{f} \tau(\chi) \sum_{i=1}^{f} \bar{\chi}(i) \frac{u\zeta_f^i}{1-u\zeta_f^i} H^n(u\zeta_f^i),$$

where ζ_f means a primitive f-th root of unity and $\tau(\chi)$ denotes the Gauss sum, namely $\sum_{i=1}^{f} \chi(i)\zeta_f^i$.

Let $\mathbf{Q}_p(\zeta)$ be the p-adic prime cyclotomic field with the p-adic valuation $|\,|$ so normalized as $|p| = p^{-1}$. The prime ideal in the ring of integers of $\mathbf{Q}_p(\zeta)$ is denoted by $\wp$. Hereafter we assume that the parameter u satisfies the condition $|1-u^{fp^\rho}| \geq 1$ for any $\rho \in \mathbf{N} \cup \{0\}$, the set of natural numbers and 0.

Let f_0 denote the p-free part of the conductor f and define a p-adic measure μ_u on the additive group of the ring

$$X = \lim_{\leftarrow} \mathbf{Z}/fp^{\rho}\mathbf{Z} \cong \mathbf{Z}/f_0\mathbf{Z} \times \mathbf{Z}_p$$

by

$$d\mu_u(a + p^{\rho} f\mathbf{Z}_p) = \frac{u^{fp^{\rho}-a}}{1 - u^{fp^{\rho}}} \quad (0 \leq a \leq fp^{\rho} - 1).$$

Then we have an analytic function on $\mathbf{Z}_p$

$$G_p(s, u, \chi) = \int_{X^*} < x >^{-s} \chi(x) d\mu_u(x),$$

where X^* means the unit group of the ring X and the measure $d\mu_u(x)$ is induced on X^* by the additive measure above, and $< x >$ denotes the principal unit in the canonical decomposition $x = \omega(x) < x >$ with the Teichmüller character ω as usual.

Furthermore, in the case $(f, p) = 1$ it holds that

$$G_p(s, u, \chi) = \frac{\tau(\chi)}{f} \sum_{i=1}^{f} \bar{\chi}(i) G_p(s, u\zeta_f^i).$$

Herein the function $G_p(s, u)$ is the function, which interpolates the ordinary Euler numbers [2]. Thus it yields that for any $n \geq 0$

$$G_p(-n, u, \chi\omega^n) = \frac{u^f}{1 - u^f} H_{\chi}^n(u) - \chi(p)p^n \frac{u^{pf}}{1 - u^{pf}} H_{\chi}^n(u^p).$$

By the way, we know the p-adic zeta functions attached to the Lubin-Tate formal groups defined over $\mathbf{Z}_p$ of height one. Shortly below we give their properties, which we use in the sequel.

Let $F(X, Y) \in \mathbf{Z}_p[[X, Y]]$ be a Lubin-Tate group with height one and $e_F(X)$ the exponential series of F, $\lambda_F(X)$ the logarithm so normalized that their leading coefficients are both equal to one. Let O be the integer ring of the completion of the algebraic closure of the p-adic rationals $\mathbf{Q}_p$. For any meromorphic power series $h(X) \in O((X))^{\times}$ we define a system of numbers $B_n(F, h)$ by

$$\frac{Xh'(e_F(X))}{\lambda'_F(e_F(X))h(e_F(X))} = e^{B(F,h)X} = \sum_{n=0}^{\infty} \frac{B_n(F, h)}{n!} X^n.$$

Then there exists a locally analytic function $\zeta_p(s, F, h)$ such that at any positive integer $m \equiv 0 \pmod{e_0 d}$ we have

$$\zeta_p(1-m, F, h) = -\frac{1}{m}\{B_m(F, h) - p^{m-1}\varepsilon^m B_m(F, Nh)\},$$

where $e_0 = p-1$ or 2 according as p is odd or 2, and d is a certain divisor of $p-1$, and finally N denotes the Coleman's norm operator.

For any Dirichlet character χ with conductor f and for any series $h(X) = \prod_{i=1}^{f} h_i(X)$ with arbitrarily given $h_i(X) \in O((X))^\times$ we can define the most widely generalized Bernoulli numbers and p-adic L-functions by setting

$$e^{B(F,h,\chi)X} = \frac{\chi(-1)}{\tau(\bar{\chi})}\sum_{i=1}^{f}\bar{\chi}(i)e^{B(F,h_i)X},$$

$$L_p(s, F, h, \chi) = \frac{\chi(-1)}{\tau(\bar{\chi})}\sum_{i=1}^{f}\bar{\chi}(i)\zeta_p(s, F, h_i).$$

Because we have, in the case where F is the multiplicative group G_m,

$$\frac{u}{1-u}e^{H(u)X} = \frac{u}{e^X - u} = \frac{1}{X}e^{-B(G_m, h^{(u)})X}$$

with $h^{(u)}(X) = X + 1 - u^{-1}$ we see for any $m \geq 1$

$$\frac{u}{1-u}H^{m-1}(u) = (-1)^m \frac{1}{m} B_m(G_m, h^{(u)}).$$

From the definition of Coleman's norm operator, namely

$$\begin{aligned} Nh^{(u)} \circ [p]_{G_m}(X) &= \prod_{\nu=0}^{p-1}(X +_{G_m} (\zeta^\nu - 1) + 1 - u^{-1}) \\ &= \prod_{\nu=1}^{p}(\zeta^\nu(X+1) - u^{-1}) = (X+1)^p - u^{-p}, \end{aligned}$$

and $[p]_{G_m}(X) = (X+1)^p - 1$ we have

$$Nh^{(u)}(X) = h^{(u^p)}(X), \text{ namely } N(X + 1 - u^{-1}) = X + 1 - u^{-p}.$$

Therefore we have

$$\frac{u^p}{1-u^p}H^{m-1}(u^p) = (-1)^m \frac{1}{m} B_m(G_m, Nh^{(u)}).$$

By noticing $d = 1$ in the case of the multiplicative group G_m we see consequently for any $m \equiv 0 \pmod{e_0}$

$$\zeta_p(1-m, G_m, h^{(u)}) = -\{\frac{u}{1-u}H^{m-1}(u) - p^{m-1}\frac{u^p}{1-u^p}H^{m-1}(u^p)\}.$$

On the other hand the function $-G_p(s, u, \omega^{-1})$ is a continuous function having the same interpolating property, and hence we obtain

$$\zeta_p(s, G_m, h^{(u)}) = -G_p(s, u, \omega^{-1}).$$

In general, from the definition the function $L_p(s, G_m, \prod_{i=1}^{f} h^{(u\zeta_f^i)}, \chi)$ interpolates at $s = 1-m, m \equiv 0 \pmod{e_0}$ the numbers

$$-\frac{u^f}{1-u^f}H_\chi^{m-1}(u) - p^{m-1}\chi(p)\frac{u^{pf}}{1-u^{pf}}H^{m-1}(u^p)$$

and hence we have

$$L_p(s, G_m, (X+1)^f - u^f, \chi) = -G_p(s, u, \chi\omega^{-1}).$$

By making use of the formula for $L_p(1, F, h, \chi)$ [4] we have especially

Theorem 1. *It holds that*

$$G_p(1, u, \chi\omega^{-1}) = \frac{\tau(\chi)}{f}\sum_{i=1}^{f}\bar{\chi}(i)\log(1-u^{-1}\zeta_f^{-i}) - \frac{\tau(\chi)}{f}\sum_{i=1}^{f}\bar{\chi}(i)\frac{1}{p}\log(1-u^{-p}\zeta_f^{-pi}).$$

Proof. We have only to remark the formula

$$L_p(1, G_m, (X+1)^f - u^{-f}, \chi) = \frac{\tau(\chi)}{f}\sum_{i=1}^{f}\bar{\chi}(i)\{\log(1-u^{-1}\zeta_f^{-i}) - \frac{1}{p}\log(1-u^{-p}\zeta_f^{-pi}).\}$$

In particular we see in the case $p|f$

$$G_p(1, u, \chi\omega^{-1}) = \frac{\tau(\chi)}{f}\sum_{i=1}^{f}\bar{\chi}(i)\log(1-u^{-1}\zeta_f^{-i}).$$

Corollary. *In the case where* $\chi = \omega^{-r}$ *with* $r \not\equiv 0$ *(mod* $p-1$*) we have*

$$G_p(1, u, \omega^{-r-1}) = \frac{\tau(\omega^{-r})}{p}\sum_{i=1}^{p}\omega^r(i)\log(1-u^{-1}\zeta^{-i}).$$

Now, we have from the definition

$$\begin{aligned} L_p(1-(p-1-r),G_m,(X+1)^p-u^{-p},\omega^{-r}) &= -G_p(-(p-r-2),u,\omega^{-r-1}) \\ &= -\frac{u}{1-u}H^{p-r-2}(u). \end{aligned}$$

Moreover, from the continuity of the function we see

$$L_p(1,G_m,(X+1)^p-u^{-p},\omega^{-r}) \equiv L_p(1-(p-1-r),G_m,(X+1)^p-u^{-p},\omega^{-r}) \pmod{p},$$

and hence we obtain

$$\frac{\tau(\omega^{-r})}{p}\sum_{i=1}^{p}\omega^r(i)\log(1-u^{-1}\zeta^{-i}) \equiv \frac{u}{1-u}H^{p-r-2}(u) \pmod{p}.$$

Theorem 2. *For any integer $\alpha \in \mathbf{Z}_p$, $\alpha \neq 0,1$ we have*

$$\omega^r(-1)\frac{\tau(\omega^{-r})}{p}\sum_{i=1}^{p}\omega^r(i)\log(1+\alpha(\zeta^{-i}-1)) \equiv (\alpha-1)H^{p-r-2}(\frac{\alpha-1}{\alpha}) \ (mod\ p).$$

Proof. It sufficies to set $u=\frac{\alpha-1}{\alpha}$ in the above.

3. Cyclotomic congruences

As in Introduction we take a number $B^{(r)}(\alpha)=\prod_{i=1}^{p-1}(1+\alpha(\zeta^i-1))^{i^r}$ with the parameter $\alpha \in \mathbf{Z}_p$, $\alpha \neq 0,1$ in the prime cyclotomic field $\mathbf{Q}_p(\zeta)$. Herein r is any rational integer such that $1 \leq r \leq p-3$. Then we see at once that this number is a representative of the coset containing $1+\alpha(\zeta-1)$ in the Takagi decomposition of the unit group U modulo the subgroup U^p of p-th power of it.

Here we know and can easily verify the following congruence, which is a special case of Stickelberger theorem. Let $\wp$ be the prime ideal in the field $\mathbf{Q}_p(\zeta)$ as before, namely $\wp=(\zeta-1)$. Then we have

$$\tau(\omega^{-r}) \equiv -\frac{(\zeta-1)^r}{r!} \pmod{\wp^{r+1}}.$$

By Theorem 2 together with $\log(1+\alpha(\zeta^i-1)) \equiv 0 \pmod{\wp^2}$ we have first

$$\log B^{(r)}(\alpha)=\sum_{i=1}^{p-1}\log(1+\alpha(\zeta^i-1)) \equiv \sum_{i=1}^{p}\omega^r(i)\log(1+\alpha(\zeta^i-1)) \pmod{\wp^{p+1}}.$$

Namely we have

$$\log B^{(r)}(\alpha) \equiv \omega^{-r}(-1)\frac{p}{\tau(\omega^{-r})}(\alpha-1)H^{p-r-2}(\frac{\alpha-1}{\alpha}) \ (\mathrm{mod}\ \wp^{2(p-1)-r}).$$

For $1 \leq r \leq p-3$ we have consequently

$$\log B^{(r)}(\alpha) \equiv \omega^{-r}(-1)\frac{p}{\tau(\omega^{-r})}(\alpha-1)H^{p-r-2}(\frac{\alpha-1}{\alpha}) \ (\mathrm{mod}\ \wp^{p+1}).$$

Therefore we see from these that

$$\log B^{(r)}(\alpha) \equiv 0 \ (\mathrm{mod}\ \wp^{p+1}), \text{ which is equivalent to } B^{(r)}(\alpha) \in U^p,$$

yields $H^{p-r-2}(\frac{\alpha-1}{\alpha}) \equiv 0 \ (\mathrm{mod}\ \wp^{r+2})$. Because the number $H^{p-r-2}(\frac{\alpha-1}{\alpha}) \in \mathbf{Z}_p$ this concludes

$$H^{p-r-2}(\frac{\alpha-1}{\alpha}) \equiv 0 \ (\mathrm{mod}\ p).$$

Conversely, if the last congruence holds then we have directly the congruence $\log B^{(r)}(\alpha) \equiv 0 \ (\mathrm{mod}\ \wp^{p+1})$.

Thus we obtain finally

Theorem 3. *Let $B^{(r)}(\alpha) = \prod_{i=1}^{p-1}(1+\alpha(\zeta^i-1))^{i^r}$ with $\alpha \in \mathbf{Z}_p, \alpha \not\equiv 0,1$ $(\mathrm{mod}\ p)$, $1 \leq r \leq p-3$. It is necessary and sufficient for the number $B^{(r)}(\alpha)$ to be a p-th power, namely $B^{(r)}(\alpha) \equiv 1 \ (\mathrm{mod}\ \wp^{p+1})$ that $H^{p-r-2}(\frac{\alpha-1}{\alpha})$ is divisible by p.*

We remark the numbers $B^{(r)}(\alpha)$ come out from the Fermat equation. As for the number $A^{(r)}$ in Introduction it is also a representative of a coset in the Takagi decomposition of the multiplicative group $\mathbf{Q}_p(\zeta)^\times$ modulo the subgroup $\mathbf{Q}_p(\zeta)^{\times p}$.

From the generating function of the Euler numbers $H^n(u)$ it follows readily that for any $m \geq 1$

$$f_m(u) = \sum_{j=0}^{p-1} j^{m-1}u^j = \frac{u^{p-1}}{1-u^{-1}}\{(H(u^{-1})+p)^{m-1} - u^{-p}H^{m-1}(u^{-1})\}.$$

If the numbers $H^n(u^{-1})$ are p-adic integers for $0 \leq n \leq m-2$ then we have the congruences

$$\begin{aligned} f_m(u) &\equiv \frac{u^p}{u-1}(1-u^{-p})H^{m-1}(u^{-1}) \ (\mathrm{mod}\ p) \\ &\equiv \frac{u^p-1}{u-1}H^{m-1}(u^{-1}) \ (\mathrm{mod}\ p). \end{aligned}$$

In the case where $u \in \mathbf{Z}_p^\times, u \neq 1$ we have $u^p \equiv u \pmod{p}$, and $H^{m-1}(u^{-1})$ $(1 \leq m \leq p-1)$ are all p-adic integers. Hence we obtain for any $m \geq 1$

$$f_m(u) \equiv H^{m-1}(u^{-1}) \pmod{p}.$$

This is what we have mentioned in Introduction.

References

[1] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper II*, Berlin, 1930.

[2] K. Shiratani and S. Yamamoto, *On a p-adic interpolation function for the Euler numbers and its derivatives*, Mem. Fac. Sci., Kyushu Univ., 39(1985), 113-125.

[3] K. Shiratani and T. Imada, *The exponential series of the Lubin-Tate groups and p-adic interpolation*, Mem. Fac. Sci., Kyushu Univ., 46(1992), 351-365.

[4] K. Shiratani, *On p-adic zeta functions of the Lubin-Tate groups*, to appear in Kyushu Jour. of Math., (1993), 1-8.

[5] L.C. Washington, *On some cyclotomic congruences of F. Thaine*, Proc. A.M.S., 93(1985), 10-14.

[6] L.C. Washington, *Kummer's lemma for prime power cyclotomic fields*, Jour. Number Theory, 40(1992), 165-173.

Department of Mathematics, Kyushu University 33, Hakozaki, Fukuoka 812, Japan.