ACTA ARITHMETICA
159.4 (2013)

Nonvanishing of a certain Bernoulli number and a related topic

by

Humio Ichimura (Mito)

1. Introduction. Let χ be an odd Dirichlet character of conductor f, and let

$$B_{1,\chi} = \frac{1}{f}\sum_{a=1}^{f-1} a\chi(a)$$

be the generalized Bernoulli number. It is well known that $B_{1,\chi} \neq 0$, which is obtained in an analytic way. Actually, one knows that $L(1,\bar{\chi})$ equals $B_{1,\chi}$ times a nonzero explicit constant and that $L(1,\bar{\chi}) \neq 0$, where $L(s,\bar{\chi})$ denotes the Dirichlet L-function associated to the complex conjugate $\bar{\chi}$ of χ. For these, see Corollary 4.4 and Theorem 4.9 in Washington [13]. It is of interest to search for an algebraic or an elementary proof of the nonvanishing.

In what follows, let p be an odd prime number. We write $p = 1 + 2^{e+1}q$ with an odd integer q. Let δ (resp. φ) be an odd (resp. even) Dirichlet character of conductor p and order 2^{e+1} (resp. order d_φ dividing q), and for an integer $n \geq 0$, let ψ_n be an even Dirichlet character of conductor p^{n+1} and order p^n. We put $\chi = \delta\varphi\psi_n$. At present, algebraic proofs for $B_{1,\chi} \neq 0$ are known for the following three cases:

(i) $n \geq 0$ and $d_\varphi = q$.
(ii) $n = 0$ and $d_\varphi = 1$.
(iii) Under some assumption on a cyclotomic unit of $\mathbb{Q}(\zeta_p)$.

The case (i) is due to Ullom [10] and Miki [9], and the case (ii) is due to [10] and Metsänkylä [8]. The case (iii) was dealt with in Iwasawa [7] and in [9]. (For the case $p = 2$, see Remark 3 at the end of Section 2.)

Let $F = \mathbb{Q}(\zeta_{2^{e+1}}, \zeta_{d_\varphi})$ and $K_n = F(\zeta_{p^n})$ for $n \geq 1$. Here, for an integer $m \geq 2$, ζ_m denotes a primitive mth root of unity. We have $B_{1,\chi} \in K_n$ for $\chi = \delta\varphi\psi_n$. For an element $X \in K_n$, we can uniquely write $X = \sum_u a_u\zeta_{p^n}^u$

2010 *Mathematics Subject Classification*: Primary 11R18; Secondary 11R23.
Key words and phrases: Bernoulli number, class number, $\mathbb{Z}_p$-extension.

DOI: 10.4064/aa159-4-6

where $a_u \in K_1$ and u runs over the integers with $0 \leq u \leq p^{n-1}-1$. Clearly we have $X \neq 0$ if and only if $a_u \neq 0$ for some u. Denote by $\mathrm{Tr}_{n/1}$ the trace map from K_n to K_1. The last condition is equivalent to saying that $\mathrm{Tr}_{n/1}(\xi X) \neq 0$ for some p^nth roots ξ of unity. We thus obtain $\mathrm{Tr}_{n/1}(\xi B_{1,\chi}) \neq 0$ for some ξ. The main purpose of this paper is to prove, with an *algebraic and elementary* manner, the following stronger nonvanishing result for $B_{1,\chi}$ in the extreme cases $d_\varphi = 1$ and q.

Theorem. *Under the above setting, assume that $d_\varphi = 1$ or q, and let $\chi = \delta\varphi\psi_n$. Then, for any $n \geq 1$ and any p^nth root ξ of unity, we have $\mathrm{Tr}_{n/1}(\xi B_{1,\chi}) \neq 0$.*

When $d_\varphi \neq 1$ nor q, no corresponding result seems to be obtained whether in an algebraic or analytic way. Calculation of the traces of Bernoulli numbers played an important role in the study of Washington [11, 12] on the non-p-part of the class numbers in the cyclotomic $\mathbb{Z}_p$-extension over an imaginary abelian field. We prove the Theorem by modifying Washington's calculation and using some combinatorial arguments. Our method is completely different from the previous ones in the above cited papers [7, 8, 9, 10].

Washington's study was taken over by Horie [2, 3]. Let k be the imaginary subfield of $\mathbb{Q}(\zeta_p)$ of degree 2^{e+1} over $\mathbb{Q}$. Let k_n be the nth layer of the cyclotomic $\mathbb{Z}_p$-extension k_∞/k with $k_0 = k$ and h_n^- the relative class number of k_n. Let ℓ be a prime number with $\ell \neq p$. When $p \equiv 3 \bmod 4$ (and hence $k = \mathbb{Q}(\sqrt{-p})$), we see from [3, Theorem 2] that $\ell \nmid h_n^-$ for all n if ℓ is a primitive root modulo p^2 and ℓ is larger than an explicit but very large constant m_p (with $m_p = O(p^p)$). In [4, 5], we obtained the following simple result by carefully looking at the traces of related Bernoulli numbers. When $q > 1$, we denote by d_p the largest divisor of q with $d_p < q$.

Proposition 1. *Let p be a prime number with $p \equiv 3 \bmod 4$ and $p \geq 7$. If ℓ is a primitive root modulo p^2 and $\ell \geq q - 2d_p$, then $\ell \nmid h_n^-$ for all n.*

In the process of showing this proposition, we obtained an assertion [5, Lemma 2] which implies the Theorem for the case where $e = 0$ and $d_\varphi = 1$. We prove the Theorem by generalizing some arguments in [4, 5]. Further, as a by-product, we obtain the following proposition.

Proposition 2. *Let p be a prime number with $p \equiv 5 \bmod 8$ and $p \geq 13$, and ℓ a prime number which is a primitive root modulo p^2. Then $\ell \nmid h_n^-/h_{n-1}^-$ for all $n \geq 1$ if $\ell > 2p(q - 2d_p)^2$.*

It is known that when $p = 3$ (resp. 5), $\ell \nmid h_n^-$ for all n if ℓ is a primitive root modulo p^2 by [2, Proposition 3] (resp. [11, Proposition 3]). When $p = 7$, the same assertion holds by Proposition 1, as $q - 2d_p = 1$. When $p = 11$ or 19, the same is true for $\ell \geq 3$, as $q - 2d_p = 3$. Let $p = 13$. We see that among the primes ℓ with $\ell \leq 2p(q-2d_p)^2 = 26$, ℓ is a primitive root modulo

p^2 when $\ell = 2, 7, 11$. (Note that $\ell = 19$, 23 is a primitive root modulo p but not modulo p^2.) Hence, it follows from Proposition 2 and $h_0^- = 1$ that $\ell \nmid h_n^-$ for all n if ℓ is a primitive root modulo p^2 except for $\ell = 2, 7, 11$. For the case $\ell = 2$, see the following remark.

Remark 1. Let h_n^* be the relative class number of $\mathbb{Q}(\zeta_{p^{n+1}})$. We can easily show that h_n^-/h_{n-1}^- divides h_n^*/h_{n-1}^*. When $p \le 509$, it is shown in [6, Theorem 2] that $2 \nmid h_n^*/h_{n-1}^*$ for *all* $n \ge 1$.

Remark 2. In [3, Theorem 2], Horie worked in a more general setting. Let k be an arbitrary imaginary quadratic field, and h_n^- the same as above. He gave, for each natural number a, an explicit (but large) constant $m_{p,a}$ for which $\ell \nmid h_n^-$ for all n if $\ell > m_{p,a}$ and ℓ satisfies a certain congruence modulo p^a.

2. Proof of Theorem. First, we prepare some lemmas. For an element x of the ring $\mathbb{Z}_p$ of p-adic integers, let

$$x = a_0(x) + a_1(x)p + \cdots + a_n(x)p^n + \cdots$$

be the p-adic expansion of x with $0 \le a_u(x) \le p-1$. Further, denote by $s_n(x)$ the unique integer satisfying $s_n(x) \equiv x \bmod p^{n+1}$ and $0 \le s_n(x) < p^{n+1}$. Clearly, we have $a_n(x) = (s_n(x) - s_{n-1}(x))/p^n$. Let $n \ge 1$. Let δ, φ and ψ_n be as in Section 1, and put $\chi = \delta\varphi\psi_n$. For $\alpha \in \mathbb{Z}_p$ with $\alpha \equiv 1 \bmod p$, we write

$$X = \mathrm{Tr}_{n/1}\bigl(\tfrac{1}{2}\psi_n(\alpha)^{-1}B_{1,\chi}\bigr)$$

for brevity. For an integer r dividing $p-1$, let μ_r be the group of rth roots of unity in $\mathbb{Z}_p$. We choose and fix a generator η of $\mu_{2^{e+1}}$. We put $\zeta_p = \psi_n(1+p^n)$, which is a primitive pth root of unity.

Lemma 1. *Under the above setting, we have*

$$X = \frac{1}{p^2}\sum_{b=0}^{p-1}\Bigl(\sum_{j=0}^{2^e-1}\sum_{\epsilon\in\mu_q} s_n(\epsilon\eta^j\alpha(1+bp^n))\varphi(\epsilon)\delta(\eta)^j\Bigr)\zeta_p^b.$$

Proof. Replacing $\alpha^{-1}a$ with a and noting that $\alpha \equiv 1 \bmod p$, we see that

$$\begin{aligned}\frac{1}{2}\psi_n(\alpha)^{-1}B_{1,\chi} &= \frac{1}{2p^{n+1}}\sum_{a=0}^{p^{n+1}-1} a\delta(a)\varphi(a)\psi_n(\alpha^{-1}a)\\ &= \frac{1}{2p^{n+1}}\sum_{a=0}^{p^{n+1}-1} s_n(a\alpha)\delta(a)\varphi(a)\psi_n(a)\\ &= \frac{1}{2p^{n+1}}\sum_{b=0}^{p^n-1}\sum_{\epsilon\in\mu_{p-1}} s_n(\epsilon\alpha(1+bp))\delta(\epsilon)\varphi(\epsilon)\psi_n(1+bp).\end{aligned}$$

For a p^nth root ξ of unity in K_n, we have $\mathrm{Tr}_{n/1}(\xi) = p^{n-1}\xi$ or 0 according as $\xi^p = 1$ or not. Further, $\psi_n(1+bp)^p = 1$ if and only if p^{n-1} divides b. Hence, noting that $1 + bp^n \equiv (1+p^n)^b \bmod p^{n+1}$, we obtain

$$X = \frac{1}{2p^2}\sum_{b=0}^{p-1} x_b\zeta_p^b \tag{1}$$

with

$$x_b = \sum_{\epsilon\in\mu_{p-1}} s_n(\epsilon\alpha(1+bp^n))\delta(\epsilon)\varphi(\epsilon) = \sum_{\epsilon\in\mu_q}\sum_{j=0}^{2^{e+1}-1} s_n(\epsilon\eta^j\alpha(1+bp^n))\delta(\eta)^j\varphi(\epsilon).$$

We have $\eta^{2^e} = -1$. Hence, as δ is an odd character and $s_n(-x) = p^{n+1} - s_n(x)$ if $p^{n+1} \nmid x$, we see that

$$\begin{aligned} x_b &= \sum_{\epsilon\in\mu_q}\sum_{j=0}^{2^e-1} \big(s_n(\epsilon\eta^j\alpha(1+bp^n)) - s_n(-\epsilon\eta^j\alpha(1+bp^n))\big)\delta(\eta)^j\varphi(\epsilon) \\ &= 2\sum_{\epsilon\in\mu_q}\sum_{j=0}^{2^e-1} s_n(\epsilon\eta^j\alpha(1+bp^n))\delta(\eta)^j\varphi(\epsilon) - p^{n+1}C \end{aligned} \tag{2}$$

with

$$C = \sum_{\epsilon\in\mu_q}\varphi(\epsilon)\sum_{j=0}^{2^e-1}\delta(\eta)^j.$$

Since C is independent of b and $\sum_{b=0}^{p-1}\zeta_p^b = 0$, we now obtain the assertion from (1) and (2). ∎

Lemma 2. *For $\gamma \in \mathbb{Z}_p$ and an integer b with $0 \le b \le p-1$, we have*

$$s_n(\gamma(1+bp^n)) = s_{n-1}(\gamma) + s_0(a_n(\gamma) + a_0(\gamma)b)p^n.$$

Proof. Write $a_n = a_n(\gamma)$ for brevity. Then we obtain the assertion from

$$\begin{aligned} \gamma(1+bp^n) &= a_0 + a_1p + \cdots + a_{n-1}p^{n-1} + (a_n + a_0b)p^n + \cdots \\ &= s_{n-1}(\gamma) + s_0(a_n + a_0b)p^n + \cdots . \end{aligned}$$ ∎

For a while, we assume that $q > 1$. For integers n, b, j and a p-adic integer α with

$$n \ge 1, \quad 0 \le b \le p-1, \quad 0 \le j \le 2^e - 1, \quad \alpha \equiv 1 \bmod p,$$

we put

$$x_{n,b,\alpha,j} = \frac{1}{p^{n+1}}\sum_{\epsilon\in\mu_q} s_n(\epsilon\eta^j\alpha(1+bp^n)) \quad\text{and}\quad z_{n,b,\alpha} = \sum_{j=0}^{2^e-1} x_{n,b,\alpha,j}\delta(\eta)^j.$$

As $q > 1$, we see that $x_{n,b,\alpha,j}$ is an integer.

Lemma 3. *Under the above setting, we have $d_p \le x_{n,b,\alpha,j} \le q - d_p$.*

Proof. Write $d = d_p$ for brevity, and put $r = q/d$. We have $r \geq 3$ since d is the largest divisor of the odd integer q with $d < q$. Further, fixing n, b, α and j, we put $x = x_{n,b,\alpha,j}$ for brevity. Let $\xi_1 = 1, \xi_2, \ldots, \xi_d$ be a complete set of representatives of the quotient μ_q/μ_r. Putting

$$y_u = \frac{1}{p^{n+1}} \sum_{\epsilon \in \mu_r} s_n(\xi_u \epsilon \eta^j \alpha(1 + bp^n)),$$

we have

$$x = \sum_{u=1}^{d} y_u.$$

As $r > 1$, we have $y_u \in \mathbb{Z}$. Then, since

$$1 \leq s_n(\xi_u \epsilon \eta^j \alpha(1 + bp^n)) \leq p^{n+1} - 1,$$

we obtain $1 \leq y_u \leq r - 1$. Therefore,

$$d \leq x \leq d(r-1) = q - d. \ \blacksquare$$

Lemma 4. *Under the above setting, we have*

$$\sum_{b=0}^{p-1} z_{n,b,\alpha} = z_{n-1,0,\alpha} + 2^e q^2 \sum_{j=0}^{2^e-1} \delta(\eta)^j.$$

Proof. Fixing α and j, we abbreviate $x_{n,b} = x_{n,b,\alpha,j}$. From Lemma 2, we see that

$$\begin{aligned}\sum_{b=0}^{p-1} x_{n,b} &= \frac{1}{p^{n+1}} \sum_{\epsilon \in \mu_q} \sum_{b=0}^{p-1} s_n(\epsilon \eta^j \alpha(1 + bp^n)) \\ &= \frac{1}{p^{n+1}} \sum_{\epsilon \in \mu_q} \sum_{b=0}^{p-1} \big(s_{n-1}(\epsilon \eta^j \alpha) + s_0(a_n^\epsilon + a_0^\epsilon b)p^n\big),\end{aligned}$$

where $a_u^\epsilon = a_u(\epsilon \eta^j \alpha)$ with $u = 0$ or n. As $\epsilon \eta^j \alpha \in \mathbb{Z}_p^\times$, $a_0^\epsilon \not\equiv 0 \bmod p$. Therefore, when b runs over $\{0, 1, \ldots, p-1\}$, the integer $s_0(a_n^\epsilon + a_0^\epsilon b)$ runs over the same set. It follows that

$$\sum_{b=0}^{p-1} x_{n,b} = \frac{1}{p^{n+1}} \sum_{\epsilon \in \mu_q} \left(p s_{n-1}(\epsilon \eta^j \alpha) + \frac{(p-1)p^{n+1}}{2} \right) = x_{n-1,0} + 2^e q^2.$$

The assertion follows from this. $\blacksquare$

Lemma 5. *Under the above setting, for each n and α, we have $z_{n,b,\alpha} \neq z_{n,0,\alpha}$ for some b with $1 \leq b \leq p-1$.*

Proof. Fixing α, we abbreviate $z_{n,b} = z_{n,b,\alpha}$ and $x_{n,0} = x_{n,0,\alpha,0}$. Assume that $z_{n,b} = z_{n,0}$ for all b. Then Lemma 4 implies that

$$\sum_{b=0}^{p-1} z_{n,b} = z_{n-1,0} + 2^e q^2 \sum_{j=0}^{2^e-1} \delta(\eta)^j \equiv 0 \bmod p\mathbb{Z}[\zeta_{2^{e+1}}].$$

It follows that

$$x_{n-1,0} + 2^e q^2 \equiv 0 \bmod p \tag{3}$$

because the elements $\delta(\eta)^j$ with $0 \le j \le 2^e - 1$ constitute a free basis of $\mathbb{Z}[\zeta_{2^{e+1}}]$ over $\mathbb{Z}$. We see that

$$2^e q^2 \equiv \frac{p-q}{2} \bmod p \quad \text{and} \quad 0 < \frac{p-q}{2} < p.$$

Lemma 3 gives

$$0 < x_{n-1,0} + \frac{p-q}{2} < q + \frac{p-q}{2} = \frac{p+q}{2} < p = 2^{e+1}q + 1.$$

Thus, the congruence (3) is impossible. ■

Proof of Theorem; the case $d_\varphi = 1$. Under the notation in Lemma 1, it suffices to show that $X \neq 0$ for any n and α. When $q > 1$, we see from Lemma 1 that

$$\begin{aligned} Y &= \frac{1}{p^{n-1}} X = \frac{1}{p^{n-1}} \mathrm{Tr}_{n/1}\big(\tfrac{1}{2}\psi_n(\alpha)^{-1} B_{1,\chi}\big) = \sum_{b=0}^{p-1} z_{n,b,\alpha}\zeta_p^b \\ &= \sum_{b=1}^{p-1} (z_{n,b,\alpha} - z_{n,0,\alpha})\zeta_p^b \in K_1 = \mathbb{Q}(\zeta_{2^{e+1}}, \zeta_p). \end{aligned}$$

Since the elements ζ_p^b with $1 \le b \le p-1$ constitute a basis of K_1 over $F = \mathbb{Q}(\zeta_{2^{e+1}})$, we see immediately from Lemma 5 that $Y \neq 0$.

Next, we deal with the case $q = 1$ (that is, the case where p is a Fermat prime). We see from Lemma 1 that

$$X = \mathrm{Tr}_{n/1}\big(\tfrac{1}{2}\psi_n(\alpha)^{-1} B_{1,\chi}\big) = \frac{1}{p^2} \sum_{b=1}^{p-1} \Big(\sum_{j=0}^{2^e-1} S_{n,b,j}\delta(\eta)^j \Big) \zeta_p^b \tag{4}$$

with

$$S_{n,b,j} = s_n(\eta^j \alpha(1 + bp^n)) - s_n(\eta^j \alpha).$$

It follows from Lemma 2 that

$$\frac{1}{p^n} S_{n,b,j} = s_0\big(a_n(\eta^j\alpha) + a_0(\eta^j\alpha)b\big) - a_n(\eta^j\alpha) \equiv \eta^j \alpha b \not\equiv 0 \bmod p$$

for $1 \le b \le p-1$. Therefore, $S_{n,b,j} \neq 0$ and hence

$$\sum_{j=0}^{2^e-1} S_{n,b,j}\delta(\eta)^j \neq 0$$

since the elements $\delta(\eta)^j$ with $0 \le j \le 2^e - 1$ constitute a basis of F over $\mathbb{Q}$. It follows from (4) that $X \neq 0$. ■

Before going on to the case $d_\varphi = q\,(>1)$, we prove one more lemma. Let $q_1, \ldots, q_s$ be some distinct odd prime numbers dividing $p-1$. We put

$$\mu = \mu_{q_1} \cdots \mu_{q_s} = \{\epsilon_1 \cdots \epsilon_s \mid \epsilon_u \in \mu_{q_u}\ (1 \leq u \leq s)\} \quad (\subseteq \mathbb{Z}_p^\times). \tag{5}$$

Let $f : \mu \to \mathbb{Z}$ be an arbitrary map, and $\tau : \mu \to \mathbb{C}^\times$ an injective homomorphism. Put $S = \{1, \ldots, s\}$. We define a map $g : \mu \to \mathbb{Z}$ by

$$g(\epsilon_1 \cdots \epsilon_s) = \sum_{u=0}^{s} (-1)^{s-u} \sum_{T \subset S}^{(u)} f(\epsilon_{t_1} \cdots \epsilon_{t_u}).$$

Here, in the sum $\sum_{T\subset S}^{(u)}$, $T = \{t_1, \ldots, t_u\}$ runs over the subsets of S with $|T| = u$. Further, when $u = 0$ (and T is empty), we set $\epsilon_{t_1} \cdots \epsilon_{t_u} = 1$.

Lemma 6. *Under the above setting, we have*

$$\sum_{\epsilon\in\mu} f(\epsilon)\tau(\epsilon) = \sum_{\epsilon_1 \neq 1} \cdots \sum_{\epsilon_s \neq 1} g(\epsilon_1 \cdots \epsilon_s)\tau(\epsilon_1) \cdots \tau(\epsilon_s),$$

where in the sum $\sum_{\epsilon_u \neq 1}$, ϵ_u runs over the nontrivial elements of μ_{q_u}.

Proof. Let $\bar{\mu} = \mu_{q_1} \cdots \mu_{q_{s-1}}$ $(\subset \mu)$, and $\bar{S} = S \setminus \{s\}$. As τ is an injective homomorphism, we have

$$\sum_{\epsilon_s \in \mu_{q_s}} \tau(\epsilon_s) = 0,$$

and hence

$$\sum_{\epsilon\in\mu} f(\epsilon)\tau(\epsilon) = \sum_{\epsilon_s \neq 1} \Big(\sum_{\epsilon \in \bar{\mu}} (f(\epsilon\epsilon_s) - f(\epsilon))\tau(\epsilon) \Big) \tau(\epsilon_s).$$

Then, by induction on s,

$$\sum_{\epsilon\in\mu} f(\epsilon)\tau(\epsilon) = \sum_{\epsilon_s \neq 1} \Big(\sum_{\epsilon_1 \neq 1} \cdots \sum_{\epsilon_{s-1} \neq 1} \bar{g}_{\epsilon_s}(\epsilon_1 \cdots \epsilon_{s-1})\tau(\epsilon_1) \cdots \tau(\epsilon_{s-1}) \Big) \tau(\epsilon_s)$$

with

$$\bar{g}_{\epsilon_s}(\epsilon_1 \cdots \epsilon_{s-1}) = \sum_{u=0}^{s-1} (-1)^{s-1-u} \sum_{T \subset \bar{S}}^{(u)} (f(\epsilon_{t_1} \cdots \epsilon_{t_u}\epsilon_s) - f(\epsilon_{t_1} \cdots \epsilon_{t_u})).$$

The right hand side equals

$$\sum_{u=0}^{s-1} (-1)^{s-(1+u)} \sum_{T \subset \bar{S}}^{(u)} f(\epsilon_{t_1} \cdots \epsilon_{t_u}\epsilon_s) + \sum_{u=0}^{s-1} (-1)^{s-u} \sum_{T \subset \bar{S}}^{(u)} f(\epsilon_{t_1} \cdots \epsilon_{t_u}). \tag{6}$$

Putting $s = t_{u+1}$ and changing $1+u$ to u, we see that the first term equals

$$\sum_{u=0}^{s-1} (-1)^{s-(1+u)} \sum_{\substack{T \subset S \\ s \in T}}^{(u+1)} f(\epsilon_{t_1} \cdots \epsilon_{t_u}\epsilon_{t_{u+1}}) = \sum_{u=1}^{s} (-1)^{s-u} \sum_{\substack{T \subset S \\ s \in T}}^{(u)} f(\epsilon_{t_1} \cdots \epsilon_{t_u}),$$

where in the second sum of the left (resp. right) hand side, T runs over the subsets of S such that $|T| = u+1$ (resp. u) and $s \in T$. The second term of (6) equals

$$\sum_{u=0}^{s-1}(-1)^{s-u}\sum_{\substack{T\subset S\\ s\notin T}}^{(u)} f(\epsilon_{t_1}\cdots\epsilon_{t_u}).$$

From these, we see that $\bar{g}_{\epsilon_s}(\epsilon_1\cdots\epsilon_{s-1}) = g(\epsilon_1\cdots\epsilon_s)$, and hence we obtain the assertion. ∎

Proof of Theorem; the case $d_\varphi = q$ (>1). Let $q = q_1^{r_1}\cdots q_s^{r_s}$ be the prime decomposition of q. As in Lemma 1, let X be the trace of $\psi_n(\alpha)^{-1}B_{1,\chi}/2$ to

$$K_1 = \mathbb{Q}(\zeta_{2^{e+1}}, \zeta_{d_\varphi}, \zeta_p) = \mathbb{Q}(\zeta_{2^{e+1}}, \zeta_{q_1^{r_1}}, \ldots, \zeta_{q_s^{r_s}}, \zeta_p).$$

We put

$$K = \mathbb{Q}(\zeta_{2^{e+1}}, \zeta_{q_1}, \ldots, \zeta_{q_s}, \zeta_p).$$

Denote by Tr the trace map from K_1 to K. Let $\mu = \mu_{q_1}\cdots\mu_{q_s}$ be as in (5). For a qth root ϵ of unity in $\mathbb{Z}_p$, we see from $d_\varphi = q$ that $\mathrm{Tr}(\varphi(\epsilon)) = c\varphi(\epsilon)$ or 0 according as $\epsilon \in \mu$ or not, with $c = [K_1 : K]$. Then Lemma 1 yields

$$\begin{aligned}\mathrm{Tr}(X) &= \frac{c}{p^2}\sum_{b=0}^{p-1}\sum_{j=0}^{2^e-1}\sum_{\epsilon\in\mu} s_n(\epsilon\eta^j\alpha(1+bp^n))\varphi(\epsilon)\delta(\eta)^j\zeta_p^b\\ &= \frac{c}{p^2}\sum_{b=1}^{p-1}\sum_{j=0}^{2^e-1}\Big(\sum_{\epsilon\in\mu}(s_n(\epsilon\eta^j\alpha(1+bp^n)) - s_n(\epsilon\eta^j\alpha))\varphi(\epsilon)\Big)\delta(\eta)^j\zeta_p^b.\end{aligned}$$

Assume that $\mathrm{Tr}(X) = 0$. Then, since the elements $\delta(\eta)^j\zeta_p^b$ with $0 \le j \le 2^e-1$ and $1 \le b \le p-1$ constitute a basis of K over $E = \mathbb{Q}(\zeta_{q_1}, \ldots, \zeta_{q_s})$, we observe that

$$\sum_{\epsilon\in\mu}\big(s_n(\epsilon\eta^j\alpha(1+bp^n)) - s_n(\epsilon\eta^j\alpha)\big)\varphi(\epsilon) = 0$$

for all j and b with $1 \le b \le p-1$. Lemma 2 yields

$$\sum_{\epsilon\in\mu}\big(s_0(a_n(\epsilon\eta^j\alpha) + a_0(\epsilon\eta^j\alpha)b) - a_n(\epsilon\eta^j\alpha)\big)\varphi(\epsilon) = 0. \tag{7}$$

Define a map $f : \mu \to \mathbb{Z}$ by

$$f(\epsilon) = s_0\big(a_n(\epsilon\eta^j\alpha) + a_0(\epsilon\eta^j\alpha)b\big) - a_n(\epsilon\eta^j\alpha).$$

Then, from (7) and Lemma 6, we obtain

$$\sum_{\epsilon_1\neq 1}\cdots\sum_{\epsilon_s\neq 1}\Big(\sum_{u=0}^{s}(-1)^{s-u}\sum_{T\subset S}^{(u)} f(\epsilon_{t_1}\cdots\epsilon_{t_u})\Big)\varphi(\epsilon_1)\cdots\varphi(\epsilon_s) = 0$$

because $d_\varphi = q$. We also see that the elements $\varphi(\epsilon_1)\cdots\varphi(\epsilon_s)$ in the above formula constitute a basis of E over $\mathbb{Q}$. Hence,

$$\sum_{u=0}^{s}(-1)^{s-u}\sum_{T\subset S}^{(u)} f(\epsilon_{t_1}\cdots\epsilon_{t_u}) = 0$$

for any $\epsilon_u \in \mu_{q_u}$ with $\epsilon_u \neq 1$ $(1 \leq u \leq s)$. Noting that $f(\epsilon) \equiv b\eta^j\alpha\epsilon \bmod p$, we see that

$$b\eta^j\alpha\sum_{u=0}^{s}(-1)^{s-u}\sum_{T\subset S}^{(u)} \epsilon_{t_1}\cdots\epsilon_{t_u} \equiv 0 \bmod p$$

for any b, j, α, and ϵ_u. It follows that

$$\prod_{u=1}^{s}(\epsilon_u - 1) \equiv 0 \bmod p.$$

This is impossible since each ϵ_u is a primitive q_uth root of unity in $\mathbb{Z}_p$. Thus $\mathrm{Tr}(X) \neq 0$, and hence $X \neq 0$. ∎

Remark 3. Let $p = 2$. Let δ be the quadratic character of conductor 4, ψ_n an even Dirichlet character of conductor 2^{n+2} and order 2^n, and $\chi = \delta\psi_n$. Algebraic proofs for $B_{1,\chi} \neq 0$ for this case are given in [8, 9, 10]. We put $K_n = \mathbb{Q}(\zeta_{2^n})$ $(n \geq 2)$, and denote by $\mathrm{Tr}_{n/2}$ the trace map from K_n to K_2. Then we can easily show the following stronger nonvanishing result:

$$X = \mathrm{Tr}_{n/2}\big(\tfrac{1}{2}\psi_n(\alpha)^{-1}B_{1,\chi}\big) = \pm 2^{n-3}(1 \pm \sqrt{-1}) \neq 0$$

for any integer $n \geq 2$ and $\alpha \in \mathbb{Z}_2$ with $\alpha \equiv 1 \bmod 4$. We give an outline of the proof. We choose a generator η of the multiplicative group $1 + 4\mathbb{Z}_2$ so that $\eta^{2^{n-2}} \equiv 1 + 2^n \bmod 2^{n+2}$. For $x \in \mathbb{Z}_2$, we define $s_n(x)$ and $a_n(x)$ exactly as in the case $p \geq 3$. Since χ is of conductor 2^{n+2}, we have

$$\frac{1}{2}\psi_n(\alpha)^{-1}B_{1,\chi} = \frac{1}{2^{n+3}}\sum_{\epsilon=\pm1}\sum_{b=0}^{2^n-1} s_{n+1}(\epsilon\eta^b\alpha)\delta(\epsilon)\psi_n(\eta)^b.$$

Letting $i = \psi_n(1 + 2^n)$, we see similarly to Lemma 1 that

$$X = \frac{1}{16}\sum_{b=0}^{3} s_{n+1}(\alpha(1 + b2^n))i^b = \frac{1}{16}(x + yi)$$

with

$$\begin{aligned} x &= s_{n+1}(\alpha) - s_{n+1}(\alpha(1 + 2^{n+1})),\\ y &= s_{n+1}(\alpha(1 + 2^n)) - s_{n+1}(\alpha(1 + 2^n)(1 + 2^{n+1})). \end{aligned}$$

For $\gamma \in \mathbb{Z}_2^\times$, we see from Lemma 2 and $a_0(\gamma) = 1$ that

$$s_{n+1}(\gamma(1 + 2^{n+1})) = s_n(\gamma) + s_0(1 + a_{n+1}(\gamma))2^{n+1}.$$

Now, we obtain the assertion noting that $a_{n+1}(\gamma) - s_0(1 + a_{n+1}(\gamma)) = \pm 1$.

3. Proof of Proposition 2. In this section, let $p = 1 + 4q$ with an odd integer $q \geq 3$. We choose $\alpha = 1$, abbreviate

$$x_{n,b} = x_{n,b,1,0}, \qquad y_{n,b} = x_{n,b,1,1}, \qquad z_{n,b} = z_{n,b,1} = x_{n,b} + y_{n,b}i,$$

and put

$$\mathfrak{z}_{n,b} = z_{n,b} - d_p(1+i).$$

Here, $i = \sqrt{-1}$. By Lemma 3, we have

$$\mathfrak{z}_{n,b} \in \Delta = \{x + yi \mid 0 \leq x, y \leq q - 2d_p\} \tag{8}$$

for any n. Let δ (resp. ψ_n) be an odd (resp. even) Dirichlet character of conductor p (resp. p^{n+1}) and order 4 (resp. p^n), and let $\chi = \delta\psi_n$. By Lemma 1 and the relation $\sum_{b=0}^{p-1} \zeta_p^b = 0$, we have

$$X = \mathrm{Tr}_{n/1}\left(\tfrac{1}{2}B_{1,\chi}\right) = p^{n-1}\sum_{b=0}^{p-1} z_{n,b}\zeta_p^b = p^{n-1}\sum_{b=0}^{p-1} \mathfrak{z}_{n,b}\zeta_p^b \in K_1 = \mathbb{Q}(i, \zeta_p).$$

Let N be the norm map from K_1 to $K = \mathbb{Q}(\zeta_p)$. Then

$$Y = N(p^{1-n}X) = \sum_{a=0}^{p-1} w_a\zeta_p^a \tag{9}$$

with

$$w_a = \sum_{(b,c)}^{(a)} \mathfrak{z}_{n,b}\bar{\mathfrak{z}}_{n,c} \in \mathbb{Z}. \tag{10}$$

Here, the sum is taken over the pairs (b, c) of integers b and c with $0 \leq b, c \leq p-1$ and $b + c \equiv a \bmod p$, and $\bar{z}$ is the complex conjugate of $z \in \mathbb{C}$. When $b = c$, we see from (8) that $0 \leq \mathfrak{z}_{n,b}\bar{\mathfrak{z}}_{n,b} \leq 2(q - 2d_p)^2$. When $b \neq c$, we observe that both pairs (b, c) and (c, b) appear in the sum (10), and

$$0 \leq \mathfrak{z}_{n,b}\bar{\mathfrak{z}}_{n,c} + \mathfrak{z}_{n,c}\bar{\mathfrak{z}}_{n,b} \leq 4(q - 2d_p)^2$$

from (8). Since there are exactly $(p-1)/2$ sets of such pairs $\{(b, c), (c, b)\}$, it follows that

$$0 \leq w_a \leq 2p(q - 2d_p)^2. \tag{11}$$

Proof of Proposition 2. It is known that the unit index of the imaginary abelian field k_n equals 1 (cf. Conner and Hurrelbrink [1, Lemma 13.5]). Hence, from the class number formula (cf. [13, Theorem 4.17]),

$$h_n^-/h_{n-1}^- = \prod_{\delta,\psi_n}\left(-\tfrac{1}{2}B_{1,\delta\psi_n}\right)$$

where δ (resp. ψ_n) runs over the Dirichlet characters of conductor p (resp. p^{n+1}) and order 4 (resp. p^n). Let ℓ ($> 2p(q-2d_p)^2$) be a prime number which is a primitive root modulo p^2. Assume that ℓ divides the ratio h_n^-/h_{n-1}^-. We fix δ and ψ_n, and put $\chi = \delta\psi_n$. Then the above formula yields

$$\tfrac{1}{2}B_{1,\chi} \equiv 0 \bmod \mathcal{L}_n$$

for some prime ideal $\mathcal{L}_n$ of $K_n = \mathbb{Q}(i, \zeta_{p^n})$ over ℓ. Since ℓ is a primitive root modulo p^2, the prime ideal $\mathcal{L}_1 = \mathcal{L}_n \cap K_1$ of K_1 remains prime in K_n. It follows that

$$X = \mathrm{Tr}_{n/1}\big(\tfrac{1}{2}B_{1,\chi}\big) \equiv 0 \bmod \mathcal{L}_1,$$

and hence

$$Y = N(p^{1-n}X) \equiv 0 \bmod \mathcal{L}_1 \cap K.$$

Then, since ℓ remains prime in K, we see from (9) that $w_a \equiv w_0 \bmod \ell$ for all a. By the Theorem, we have $X \neq 0$ and hence $Y \neq 0$. Thus, $w_a \neq w_b$ for some a and b. For these a and b, we have $|w_a - w_b| \equiv 0 \bmod \ell$, and $0 < |w_a - w_b| \leq 2p(q - 2d_p)^2$ by (11). However, as $\ell > 2p(q - 2d_p)^2$, this is impossible. ∎

Acknowledgements. The author is grateful to the referee for careful reading and for pointing out a mistake in the original manuscript.

References

[1] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, World Sci., Singapore, 1988.

[2] K. Horie, *Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field*, J. London Math. Soc. 66 (2002), 257–275.

[3] K. Horie, *The ideal class group of the basic $\mathbb{Z}_p$-extension over an imaginary quadratic field*, Tohoku Math. J. 57 (2005), 375–394.

[4] H. Ichimura, *A note on the relative class number of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{-p})$, II*, Proc. Japan Acad. Ser. A Math. Sci. 89 (2013), no. 2, 21–23.

[5] H. Ichimura and S. Nakajima, *A note on the relative class number of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}(\sqrt{-p})$*, Proc. Japan Acad. Ser. A Math. Sci. 88 (2012), no. 1, 16–20.

[6] H. Ichimura and S. Nakajima, *On the 2-part of the class numbers of cyclotomic fields of prime power conductors*, J. Math. Soc. Japan 64 (2012), 317–342.

[7] K. Iwasawa, *A note on cyclotomic fields*, Invent. Math. 36 (1976), 115–123.

[8] T. Metsänkylä, *A short proof for the nonvanishing of a character sum*, J. Number Theory 9 (1977), 507–509.

[9] H. Miki, *On the ℓ-adic expansion of certain Gauss sums and its applications*, in: Galois Representations and Arithmetic Algebraic Geometry, Adv. Stud. Pure Math. 12, North-Holland, Amsterdam, 1987, 87–118.

[10] S. Ullom, *The nonvanishing of certain character sums*, Proc. Amer. Math. Soc. 45 (1974), 164–166.

[11] L. C. Washington, *Class numbers and $\mathbb{Z}_p$-extensions*, Math. Ann. 214 (1975), 177–193.

[12] L. C. Washington, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*, Invent. Math. 49 (1978), 87–97.

[13] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, New York, 1997.

Humio Ichimura
Faculty of Science
Ibaraki University
Bunkyo 2-1-1
Mito, 310-8512, Japan
E-mail: hichimur@mx.ibaraki.ac.jp

Received on 6.10.2012
and in revised form on 10.4.2013 (7221)