Math. Appl. **1** (2012), 1–12
DOI: 10.13164/ma.2012.01

ON THE RELATIVE CLASS NUMBER OF SPECIAL CYCLOTOMIC FIELDS

TAKASHI AGOH

Dedicated to the memory of Tomihisa Oku

Abstract. Let p be an odd prime, ζ_p be a primitive pth root of unity and h_p^- be the relative class number of the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ over the rationals $\mathbb{Q}$ defined by ζ_p. The main purpose of this paper is to discuss arithmetic properties of factors of h_p^- for an odd prime p of the form $p = 4q + 1$ with q a prime.

1. Introduction

Let p be an odd prime, ζ_p a primitive pth root of unity, $K_p = \mathbb{Q}(\zeta_p)$ the cyclotomic field over the rationals $\mathbb{Q}$ defined ζ_p, h_p the class number of K_p and h_p^+ the real class number of K_p, i.e. the class number of the maximal real subfield $K_p^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \subset K_p$. The relative class number $h_p^- = h_p/h_p^+$ of K_p as well as h_p^+ has been the subject of considerable investigations in connection with the ideal class group of K_p and many kinds of class number formulas have been devised from various viewpoints.

Out of numerous expressions of h_p^-, we first extract the following classical formula established by Kummer in 1851:

$$h_p^- = \frac{(-1)^{(p-1)/2}}{(2p)^{(p-3)/2}} \prod_{\substack{j=1 \\ j:\text{odd}}}^{p-1} f(\zeta_{p-1}^j), \tag{1.1}$$

where $f(x) = \sum_{k=0}^{p-2} g_k x^k$, g is a primitive root (mod p) and g_k is the least positive residue of g^k modulo p. Next, we pick up the well-known

$$h_p^- = 2p \prod_{\chi \in Z^-} \left(-\frac{1}{2} B_{1,\chi} \right), \tag{1.2}$$

where Z^- is the set of all odd Dirichlet characters modulo p and $B_{1,\chi}$ is the generalized Bernoulli number attached to χ, i.e. $B_{1,\chi} = (1/p) \sum_{a=1}^{p-1} a\chi(a)$.

Based on these formulas, we are able to deduce many important arithmetic properties of h_p^- (see, e.g., Ribenboim [14] and Washington [16]).

MSC (2010): primary 11R04, 11R18, 11R29; secondary 11A07, 11R11.
Keywords: cyclotomic fields, class number formulas, relative class number.
The research was supported in part by the Grant-in-Aid for Scientific Research (C), Japan Society for the Promotion of Science.

Concerning prime factors of h_p^- and h_p^+ and their properties, very little is known. By elaborately analysing (1.1), Lehmer [7] obtained the following factorization of h_p^- into rational integers:

$$h_p^- = \prod_{\substack{ed=p-1 \\ d:\text{odd}}} h_p(e), \tag{1.3}$$

where the product is taken over all integers $e > 0$ such that $ed = p-1$ with d odd. The factor $h_p(e)$ is the so-called relative class number of order e. We can consult more details including an explicit formula of $h_p(e)$ in [7].

It is well-known by Kummer's result that $p \mid h_p \Leftrightarrow p \mid h_p^-$, $2 \mid h_p \Leftrightarrow 2 \mid h_p^-$, $p \mid h_p^+ \Rightarrow p \mid h_p^-$ and $2 \mid h_p^+ \Rightarrow 2 \mid h_p^-$. Metsänkylä [11] showed that if p is a prime of the form $p = 2q+1$ with q an odd prime, then $q \nmid h_p^-$. Concerning the parity of h_p^-, Estes [4] proved that if $p = 2q+1$ and 2 is inert in K_q^+, then $2 \nmid h_p^-$. We can find a new proof of this result in [12] based on the formula (1.2). See also the proof by Stevenhagen [15]. The parity of h_p^+ was studied by Davis [3] and it was verified that if $p = 2q+1$ (both p and q are odd primes) and 2 is a primitive root of q, then $2 \nmid h_p^+$. On the one hand, Metsänkylä [13] discussed the case $p = 4q+1$ (q a prime) and proved a similar result to the Davis by making use of the 2-adic class number formula.

In this paper, we focus our attention on the relative class number h_p^- of K_p for an odd prime $p = 4q+1$ with q a prime and discuss arithmetic properties of the factors H_1 and H_2 of h_p^- given in the following theorem.

Theorem 1.1. *Let p be an odd prime of the form $p = 4q+1$ with q a prime. Then h_p^- is factored as $h_p^- = H_1 \cdot H_2$, where H_1 and H_2 can be expressed by using integer pairs (C, D) and (S, T) as, respectively,*

$$H_1 = \frac{C^2 + D^2}{2} \quad \textit{and} \quad H_2 = \frac{S^2 + (-1)^{(q-1)/2} q T^2}{p}. \tag{1.4}$$

Here the integers C, D, S and T are determined uniquely up to the sign.

We note that H_1 and H_2 in (1.4) are corresponding to $h_p(4)$ (with $d = q$) and $h_p(4q)$ (with $d = 1$), respectively, in Lehmer's factorization (1.3).

2. Proof of Theorem 1.1

Throughout this paper, we denote by ζ_n a primitive nth root of unity for $n \geq 1$, $\mathbb{Z}_p$ the ring of p-adic integers, $\mathbb{Q}_p$ the field of p-adic numbers, $\mathcal{O}_K$ the ring of integers in an algebraic number field K over $\mathbb{Q}$ and $\mathcal{N}_{K/F}$ the norm in an extension K/F.

In this Section we first give the proof of Theorem 1.1 based on (1.2) and later we introduce methods how to concretely find the pairs $(C, D), (S, T)$ in (1.4) by making use of (1.1).

Proof. If we sort the odd characters χ according to their orders, then the numbers $\beta_\chi = -\frac{1}{2} B_{1,\chi}$ attached to $\chi \in Z^-$ with $e = \mathrm{ord}(\chi) = (p-1)/d$ for a positive odd integer d dividing $p-1$ form a Galois orbit in K_e. Therefore, letting α be an

element in this orbit, we can write

$$\mathcal{H}_e = \prod_{\mathrm{ord}(\chi)=e} \beta_\chi = \mathcal{N}_{K_e/\mathbb{Q}}(\alpha) \in \mathbb{Q},$$

and hence (1.2) becomes

$$h_p^- = 2p \prod_{\substack{ed=p-1 \\ d:\,\mathrm{odd}}} \mathcal{H}_e. \tag{2.1}$$

This brings us Lehmer's factorization (1.3) if we perceive that the numbers $\beta_\chi = -(1/2p)\sum_{a=1}^{p-1} a\chi(a)$ are elements in $\mathcal{O}_{K_{p-1}}$ except for the following two cases.

(i) When $\mathrm{ord}(\chi) = e = 2^t$ is the highest power of 2 dividing $p-1$, we know that β_χ is not 2-integral.

(ii) When $\mathrm{ord}(\chi) = e = p-1$ and χ is the inverse of the Teichmüller character ω of order $p-1$ after embedding K_{p-1} in a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, we see $\beta_\chi \in (1/p)\mathbb{Z}_p$. Indeed, in this case we have $\beta_{\omega^{-1}} = \beta_{\omega^{p-2}} \equiv -(p-1)/2p \pmod{\mathbb{Z}_p}$, which corresponds to the von Staudt-Clausen theorem on Bernoulli numbers.

Therefore, taking $2\mathcal{H}_{2^t}$ and $p\mathcal{H}_{p-1}$ together in (2.1), we have an actual factorization into rational integers as in (1.3). Now assume that p is an odd prime of the form $p = 4q+1$ with q a prime. Then we have $e = 2^t = 4$ and $e = p-1 = 4q$, and hence (2.1) can be written as $h_p^- = (2\mathcal{H}_4)(p\mathcal{H}_{4q})$.

For the case $e = 4$, we easily see that the number $H_1 = 2\mathcal{H}_4$ can be written as, using a Gaussian integer $C + Di \in \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$,

$$H_1 = 2\prod_{\mathrm{ord}(\chi)=4} \beta_\chi = \frac{1}{2}\mathcal{N}_{\mathbb{Q}(i)/\mathbb{Q}}(2B_{1,\chi}) = \frac{1}{2}\mathcal{N}_{\mathbb{Q}(i)/\mathbb{Q}}(C+Di) = \frac{C^2+D^2}{2}.$$

For the case $e = 4q$, the number $H_2 = p\mathcal{H}_{4q}$ is equal to p times the norm of an algebraic number which is integral in K_{4q} outside a single of the $\varphi(4q) = 2(q-1)$ primes over p of valuation -1, where φ is Euler's totient function. Therefore, it is also p times the norm of an algebraic integer which is integral outside a single of the 2 primes over p of valuation -1 in any quadratic subfield of K_{4q}, for which we may choose $F = \mathbb{Q}(\sqrt{(-1)^\kappa q})$ with $\kappa = (q+1)/2$. Writing H_2 as $1/p$ times the norm of p times that quadratic number which is integral in F, we arrive at the expression of H_2 by means of a pair $(S,T) \in \mathbb{Z}^2$ as follows:

$$H_2 = \frac{1}{p}\mathcal{N}_{F/\mathbb{Q}}\big(S + \sqrt{(-1)^\kappa q}\,T\big) = \frac{S^2 + (-1)^{(q-1)/2} qT^2}{p}.$$

This completes the proof of Theorem 1.1. □

Above proof based on (1.2) tells that there exist pairs (C,D) and (S,T) of integers as stated in (1.4), however it does not show the uniqueness of these pairs. Further, an algorithm how to concretely deduce them does not come in sight. These issues will be resolved when we apply Kummer's formula (1.1). We do not give details because it is rather lengthy and troublesome, but we think that it is better to introduce below only the process how to find explicitly these pairs by making use of (1.1).

As defined in Section 1, let $f(x)=\sum_{k=0}^{p-2} g_k x^k$, where $g^k \equiv g_k \pmod p, 1 \le g_k \le p-1$, for a primitive root $g \pmod p$. Then we have $f(x)=\sum_{k=1}^{4q} kx^{\mathrm{ind}(k)}$ if $p=4q+1$. Since $\{a \in \mathbb{Z} \mid 1 \le a < 4q, (a,4q)=1\} = \{2k+1 \mid 0 \le k < 2q\} \backslash \{q, 3q\}$,

$$\mathcal{N}_{K_{4q}/\mathbb{Q}}(f(\zeta_{4q})) = \prod_{\substack{a=1 \\ (a,4q)=1}}^{4q-1} f(\zeta_{4q}^a).$$

As easily seen, $\zeta_{4q}=i\zeta_q$, $\zeta_{4q}^q = i^q = (-1)^{(q-1)/2}i$, $\zeta_{4q}^{3q} = -i^q = (-1)^{(q+1)/2}i$ and $\{i^q, i^{3q}\} = \{i, -i\}$ for $i=\sqrt{-1}$. Since $K_4=\mathbb{Q}(i)$, we obtain from (1.1)

$$\begin{aligned} h_p^- &= \frac{1}{(2p)^{2q-1}} \prod_{k=0}^{2q-1} f((i\zeta_q)^{2k+1}) \\ &= \frac{1}{(2p)^{2q-1}} \left\{ \mathcal{N}_{K_4/\mathbb{Q}}(f(i)) \cdot \mathcal{N}_{K_{4q}/\mathbb{Q}}(f(i\zeta_q)) \right\}. \end{aligned}$$

Here we write h_p^- as $h_p^- = H_1 \cdot H_2$, where

$$H_1 = \frac{1}{2p^2}\mathcal{N}_{K_4/\mathbb{Q}}(f(i)) \quad \text{and} \quad H_2 = \frac{1}{2^{2(q-1)}p^{2q-3}}\mathcal{N}_{K_{4q}/\mathbb{Q}}(f(i\zeta_q)). \tag{2.2}$$

For an appropriate function ϑ and $a=0,1,2,3$, let write for simplification

$$\sum_k^{(a)} \vartheta(k) = \sum_{\substack{k=1 \\ \mathrm{ind}(k) \equiv a \pmod 4}}^{p-1} \vartheta(k).$$

First we put $U_a = \sum_k^{(a)} k$. Since $\mathrm{ind}(k) \equiv a \pmod 4$ deduces $\mathrm{ind}(p-k) = \mathrm{ind}(-k) \equiv a+2 \pmod 4$, we have $U_{a+2} = \sum_k^{(a+2)} k = \sum_k^{(a)} (p-k) = qp - U_a$ for $a=0,1$. Also since

$$\begin{aligned} f(i) &= \sum_{k=0}^{p-2} g_k i^k = \sum_{k=1}^{4q} k i^{\mathrm{ind}(k)} = \sum_{a=0}^{3} \sum_k^{(a)} k i^{\mathrm{ind}(k)} \\ &= (U_0 - U_2) + i\,(U_1 - U_3) = (2U_0 - pq) + i\,(2U_1 - pq), \end{aligned}$$

we get from (2.2)

$$\begin{aligned} H_1 &= \frac{1}{2p^2} f(i)f(-i) = \frac{1}{2p^2}\left\{(2U_0-pq)^2 + (2U_1-pq)^2\right\} \\ &= \frac{1}{2}\left\{(2U_0/p-q)^2 + (2U_1/p-q)^2\right\}. \end{aligned} \tag{2.3}$$

Noting that $U_a \equiv \sum_k^{(a)} g^{\mathrm{ind}(k)} \equiv \sum_{k=0}^{q-1} g^{a+4k} \equiv g^a(g^{p-1}-1)/(g^4-1) \equiv 0 \pmod p$ by Fermat's little theorem, if we set $C=|2U_0/p-q|$ and $D=|2U_1/p-q|$, then (2.3) leads to $H_1=(C^2+D^2)/2$ with $(C,D) \in \mathbb{Z}^2$ as indicated in (1.4).

Next put $V_a = \sum_k^{(a)} k\zeta_q^{\mathrm{ind}(k)}$ for $a=0,1,2,3$. Then it follows that for $a=0,1$

$$\begin{aligned} V_{a+2} &= \sum_k^{(a+2)} (p-k)\zeta_q^{\mathrm{ind}(p-k)} = \sum_k^{(a)} (p-k)\zeta_q^{\mathrm{ind}(-k)} \\ &= \sum_k^{(a)} (p-k)\zeta_q^{\mathrm{ind}(k)} = p\sum_k^{(a)} \zeta_q^{\mathrm{ind}(k)} - \sum_k^{(a)} k\zeta_q^{\mathrm{ind}(k)} = -V_a. \end{aligned}$$

Thus we have

$$\begin{aligned} f(i\zeta_q) &= \sum_{k=1}^{4q} k(i\zeta_q)^{\mathrm{ind}(k)} = \sum_{a=0}^{3} \sum_{k}^{(a)} k(i\zeta_q)^{\mathrm{ind}(k)} \\ &= (V_0 - V_2) + i\,(V_1 - V_3) = 2\,(V_0 + iV_1)\,. \end{aligned} \tag{2.4}$$

Noting the fact $K_{4q} = K_q(i)$, if we calculate the norm of $f(i\zeta_q)$ in $K_{4q}/\mathbb{Q}$, then

$$\begin{aligned} \mathcal{N}_{K_{4q}/\mathbb{Q}}(f(i\zeta_q)) =& 2^{2(q-1)}\mathcal{N}_{K_{4q}/\mathbb{Q}}\,(V_0 + iV_1) \\ =& 2^{2(q-1)}\mathcal{N}_{K_q/\mathbb{Q}}\left(\mathcal{N}_{K_q(i)/K_q}\,(V_0 + iV_1)\right) \\ =& 2^{2(q-1)}\mathcal{N}_{K_q/\mathbb{Q}}\left(V_0^2 + V_1^2\right). \end{aligned}$$

Putting afresh $\alpha_1 = V_0$ and $\beta_1 = V_1$, we define $\alpha_{j+1} = \Gamma^j(\alpha_1)$ and $\beta_{j+1} = \Gamma^j(\beta_1)$ $(j = 0, 1, ..., q-2)$, where Γ is a generator of $\mathrm{Gal}\,(K_q/\mathbb{Q})$. Consider the recurrence sequences $\{X_n\}_{n\geq 1}$ and $\{Y_n\}_{n\geq 1}$ defined by $X_1 = \alpha_1$, $Y_1 = \beta_1$ and for $k \geq 1$

$$\begin{cases} X_{k+1} = \alpha_{k+1}X_k + \beta_{k+1}Y_k, \\ Y_{k+1} = \beta_{k+1}X_k - \alpha_{k+1}Y_k. \end{cases} \tag{2.5}$$

Then we see $X_{q-1} = \Gamma^j(X_{q-1})$ and $Y_{q-1} = (-1)^j\Gamma^j(Y_{q-1})$ for any $j \geq 0$, which show $X_{q-1} \in \mathbb{Z}$ and $Y_{q-1} \in \mathcal{O}_F$, where $F = \mathbb{Q}(\sqrt{(-1)^\rho q}) \subset K_q$ and $\rho = (q-1)/2$. When we represent Y_{q-1} using the integral basis $\{1, \frac{1}{2}(1+\sqrt{(-1)^\rho q})\}$ of $\mathcal{O}_F$, there exist uniquely $u_q, v_q \in \mathbb{Z}$ such that

$$Y_{q-1} = u_q + v_q\frac{1+\sqrt{(-1)^\rho q}}{2}.$$

We do not mention details, but it can be shown that $Y_{q-1} = -u_q\sqrt{(-1)^\rho q}$ based on the fact $v_q = -2u_q$. Putting anew $X = X_{q-1}$ and $Y = u_q = -Y_{q-1}/\sqrt{(-1)^\rho q}$, we see that $X, Y \in \mathbb{Z}$ and both are divisible by p^{q-2}. Consequently, letting $S = |X/p^{q-2}|$ and $T = |Y/p^{q-2}|$, we realize the following expression of H_2 as desired:

$$\begin{aligned} H_2 &= \frac{1}{2^{2(q-1)}p^{2q-3}}\mathcal{N}_{K_{4q}/\mathbb{Q}}(f(i\zeta_q)) = \frac{1}{p^{2q-3}}\mathcal{N}_{K_q/\mathbb{Q}}(V_0^2 + V_1^2) \\ &= \frac{1}{p^{2q-3}}\prod_{j=0}^{q-2}\Gamma^j(\alpha_1^2 + \beta_1^2) = \frac{1}{p^{2q-3}}\prod_{k=1}^{q-1}(\alpha_k^2 + \beta_k^2) \\ &= \frac{X_{q-1}^2 + Y_{q-1}^2}{p^{2q-3}} = \frac{X^2 + (-1)^{(q-1)/2}qY^2}{p^{2q-3}} \\ &= \frac{S^2 + (-1)^{(q-1)/2}qT^2}{p}. \end{aligned} \tag{2.6}$$

3. Arithmetic properties of H_1 and H_2

In this Section, we discuss arithmetic properties of the factors H_1 and H_2 of h_p^- stated in Theorem 1.1.

First, we shall prove the following

Proposition 3.1. *Let $p = 4q + 1$ be an odd prime with q a prime, H_1, H_2 be as in Theorem 1.1 and $\left(\frac{\cdot}{q}\right)$ be the Legendre symbol. Then we have*

(i) $H_1 \equiv 1 \pmod 4$.

(ii) *If* H_2 *is odd, then* $H_2 \equiv 1 \pmod 4$.

(iii) *If* $q \nmid H_2$, *then* $\left(\frac{H_2}{q}\right) = 1$.

(iv) *If* l *is an odd prime with* $l \neq q$ *and* $l \parallel H_2$, *then* $\left(\frac{l}{q}\right) = (-1)^{(l-1)/2}$.

Proof. (i) Recall the expression $H_1 = (C^2 + D^2)/2$ from Section 2. Since both $C = |2U_0/p - q|$ and $D = |2U_1/p - q|$ are odd, we see $C^2 + D^2 \equiv 2 \pmod 8$ and hence $H_1 \equiv 1 \pmod 4$.

(ii) From the assumption $2 \nmid H_2$ and the expression of H_2 in (2.6), S and T must have different parities. If S is odd and T is even, then $H_2 \equiv S^2 \equiv 1 \pmod 4$. On the one hand, if S is even and T is odd, then $H_2 \equiv (-1)^{(q-1)/2} q T^2 \equiv 1 \pmod 4$, because it always holds that $(-1)^{(q-1)/2} q \equiv 1 \pmod 4$ for an odd prime q.

(iii) Since $p \equiv 1 \pmod q$ and $pH_2 = S^2 + (-1)^{(q-1)/2} q T^2$, we have $H_2 \equiv S^2 \pmod q$ and hence $\left(\frac{H_2}{q}\right) = 1$.

(iv) If $l = p$, then $\left(\frac{l}{q}\right) = \left(\frac{4q+1}{q}\right) = 1$, which proves the assertion. On the other hand, if $l \neq p, q$, then, by the reciprocity and the first complementary laws for the Legendre symbol, it follows that, letting $\kappa = (q+1)/2$,

$$\begin{aligned} l \text{ is inert in } \mathbb{Q}(\sqrt{(-1)^\kappa q}) &\iff \left(\frac{(-1)^\kappa q}{l}\right) = -1 \\ &\iff \left(\frac{l}{q}\right) = (-1)^{(l+1)/2}. \end{aligned} \tag{3.1}$$

If $\left(\frac{l}{q}\right) \neq (-1)^{(l-1)/2}$, i.e. $\left(\frac{l}{q}\right) = (-1)^{(l+1)/2}$, then we know from (3.1) that l is inert in $\mathbb{Q}(\sqrt{(-1)^\kappa q})$. However H_2 can be written as

$$H_2 = \frac{1}{p}\big(S + \sqrt{(-1)^\kappa q}\,T\big)\big(S - \sqrt{(-1)^\kappa q}\,T\big),$$

which implies that if $l \mid H_2$, then $l^2 \mid H_2$. This is contrary to $l \parallel H_2$. □

Combining (i) and (ii) in Proposition 3.1, we know that if h_p^- is odd, then $h_p^- \equiv 1 \pmod 4$.

Proposition 3.2. *Let* $p = 4q+1$ *be an odd prime, where* q *is also a prime with* $q \equiv 3 \pmod 4$. *Then we have* (i) $H_1 \not\equiv 0 \pmod q$ and (ii) $H_2 \not\equiv 0 \pmod q$, and hence $h_p^- \not\equiv 0 \pmod q$.

Proof. (i) We shall first show $H_1 \not\equiv 0 \pmod q$ if $q \equiv 3 \pmod 4$. Let U_a be as in Section 2. Then, since $U_a > 0$, $U_a \equiv 0 \pmod p$ and $U_a + U_{a+2} = pq$, we know $(U_a, q) = 1$ for each $i = 0, 1, 2, 3$. In fact, if $q \mid U_a$, then $U_a/pq + U_{a+2}/pq = 1$, which is impossible because both U_a/pq and U_{a+2}/pq are positive integers. Recall now the expression of H_1 introduced in Section 2 as a consequence of (1.1):

$$H_1 = \frac{C^2 + D^2}{2},$$

where $C = |2U_0/p - q|$ and $D = |2U_1/p - q|$. Since $(U_0, q) = (U_1, q) = 1$, one knows $(C, q) = (D, q) = 1$. This implies that if $H_1 \equiv 0 \pmod{q}$, then $q \equiv 1 \pmod{4}$, which is contrary to the assumption.

(ii) Next, we shall show $H_2 \not\equiv 0 \pmod{q}$ if $q \equiv 3 \pmod{4}$. Let $\alpha_1 = V_0$ and $\beta_1 = V_1$ as defined in Section 2 and put $\mathfrak{q} = (1 - \zeta_q)$ the prime ideal of $\mathcal{O}_{K_q}$ dividing q. Then we have $\alpha_1 \equiv U_0 \pmod{\mathfrak{q}}$ and $\beta_1 \equiv U_1 \pmod{\mathfrak{q}}$, because $U_a - V_a = \sum_k^{(a)} k(1 - \zeta_q^{\mathrm{ind}(k)}) \equiv 0 \pmod{\mathfrak{q}}$ for $a = 0, 1$. Hence, letting $\alpha_{j+1} = \Gamma^j(\alpha_1)$ and $\beta_{j+1} = \Gamma^j(\beta_1)$ for $\Gamma \in \mathrm{Gal}\,(K_q/\mathbb{Q})$, it follows that for $j = 0, 1, ..., q-2$

$$\alpha_{j+1} \equiv U_0 \pmod{\mathfrak{q}}, \quad \beta_{j+1} \equiv U_1 \pmod{\mathfrak{q}}. \tag{3.2}$$

Here reconsider the sequences $\{X_n\}_{n\geq 1}$ and $\{Y_n\}_{n\geq 1}$ defined in (2.5). From (3.2) we deduce for any $k \geq 1$

$$\begin{cases} X_{2k-1} \equiv (U_0^2 + U_1^2)^{k-1} U_0 \pmod{\mathfrak{q}}, \\ Y_{2k-1} \equiv (U_0^2 + U_1^2)^{k-1} U_1 \pmod{\mathfrak{q}}, \end{cases} \quad \begin{cases} X_{2k} \equiv (U_0^2 + U_1^2)^{k} \pmod{\mathfrak{q}}, \\ Y_{2k} \equiv 0 \pmod{\mathfrak{q}}. \end{cases} \tag{3.3}$$

Taking account of the facts $X_{q-1}, Y_{q-1}^2 \in \mathbb{Z}$ and $(q) = \mathfrak{q}^{q-1}$, we get from (3.3)

$$X_{q-1} \equiv (U_0^2 + U_1^2)^{\rho} \pmod{q}, \quad Y_{q-1}^2 \equiv 0 \pmod{q}, \tag{3.4}$$

where $\rho = (q-1)/2$. As mentioned in Section 2, H_2 can be expressed as

$$H_2 = \frac{S^2 + (-1)^{\rho} q T^2}{p},$$

where S, T are rational integers given by

$$S = \left| \frac{X_{q-1}}{p^{q-2}} \right| \quad \text{and} \quad T = \left| \frac{-Y_{q-1}}{p^{q-2}\sqrt{(-1)^{\rho} q}} \right|.$$

If we assume $H_2 \equiv 0 \pmod{q}$ for $q \equiv 3 \pmod{4}$, then $S \equiv 0 \pmod{q}$ since $p \equiv 1 \pmod{q}$. Therefore, from (3.4) we get $X_{q-1} \equiv (U_0^2 + U_1^2)^{\rho} \equiv 0 \pmod{q}$ which implies $U_0^2 + U_1^2 \equiv 0 \pmod{q}$. Also since $(U_0, q) = (U_1, q) = 1$, q must satisfy $q \equiv 1 \pmod{4}$, which is however contrary to the assumption.

By (i) and (ii), we conclude that $h_p^- = H_1 \cdot H_2 \not\equiv 0 \pmod{q}$ if $q \equiv 3 \pmod{4}$. This completes the proof of Proposition 3.2. □

In above proof, we showed independently $H_1 \not\equiv 0 \pmod{q}$ and $H_2 \not\equiv 0 \pmod{q}$ under the assumption $q \equiv 3 \pmod{4}$. However, the second one can be deduced from the first if we apply more general results on Galois extensions and p-groups (see [16, Theorem 10.4 (a)]). Indeed, we have only to know and use the fact that H_1 is the relative class number of the subfield with degree 4 of K_p.

It is possible to discuss the p-divisibility of H_1 by means of Bernoulli numbers defined by the power series expansion

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n \quad (|x| < 2\pi).$$

As easily seen from the von Staudt-Clausen theorem, if p is a prime with $p - 1 \nmid n$, then $B_n \in \mathbb{Z}_p$, and if $p - 1 \mid n$, then $pB_n \in \mathbb{Z}_p$, more precisely $pB_n \equiv -1 \pmod{p}$.

Proposition 3.3. *Let $p = 4q + 1$ be an odd prime with q a prime. Then*

$$H_1 \equiv \frac{1}{2} \cdot \frac{B_{(p+3)/4}}{(p+3)/4} \cdot \frac{B_{(3p+1)/4}}{(3p+1)/4} \pmod{p}. \tag{3.5}$$

Proof. Let ω be the Teichmüller character whose order is $p-1$. Since $\beta_{\omega^n} \equiv \frac{1}{n+1} B_{n+1} \pmod{p}$ for a positive odd integer n with $p - 1 \nmid n + 1$, we know that if $p = 4q + 1$, then

$$\begin{aligned} H_1 =& 2\mathcal{H}_4 = 2(\beta_{\omega^q}\beta_{\omega^{3q}}) = 2\Big(-\frac{1}{2}B_{1,\omega^q}\Big)\Big(-\frac{1}{2}B_{1,\omega^{3q}}\Big) \\ \equiv& \frac{1}{2} \cdot \frac{B_{q+1}}{q+1} \cdot \frac{B_{3q+1}}{3q+1} \pmod{p}, \end{aligned}$$

which completes the proof of (3.5). □

For above proof, we referred to some ideas written in the papers by Carlitz [2] and Metsänkylä [10]. As a matter of fact, there are many different proofs of (3.5) although the above one is very short and smart. It is of course possible to prove it by calculating $\mathcal{N}_{K_4/\mathbb{Q}}(f(i))$, where $f(x) = \sum_{k=0}^{p-2} g_k x^k$ as defined in Section 1.

For this purpose, letting $s_i = (gg_i - g_{i+1})/p \in \mathbb{Z}$, we consider the polynomial

$$s(x) = s_0 + s_1 x + \cdots + s_{p-2}x^{p-2}.$$

A basic relation between $f(x)$ and $s(x)$ is given by

$$\frac{1}{p}(gx - 1)f(x) = xs(x) + \frac{1}{p}(x^{p-1} - 1). \tag{3.6}$$

As easily shown, if $m \geq 2$ is even and $p - 1 \nmid m$, then we have

$$\begin{aligned} \frac{1}{p}f(g^{m-1}) \equiv& \frac{B_m}{m} + \frac{m-1}{g^m - 1}q_p(g) \pmod{p}, \\ s(g^{m-1}) \equiv& \frac{g^m - 1}{g^{m-1}} \cdot \frac{B_m}{m} \pmod{p}, \end{aligned} \tag{3.7}$$

where $q_p(g) = (g^{p-1} - 1)/p$ is the Fermat quotient of p with base g. Indeed, to deduce (3.7) we prepare the well-known congrunece (see, e.g., Agoh [1])

$$\frac{B_m}{m} \equiv \frac{g^m}{g^m - 1}q_p(g) - \sum_{i=1}^{p-1} g^{(m-1)i}\left[\frac{g^i}{p}\right] \pmod{p}, \tag{3.8}$$

where $[g^i/p]$ is the greatest integer $\leq g^i/p$. By the logarithmic property of the Fermat quotient, we have $q_p(g^n) \equiv nq_p(g) \pmod{p}$ for any integer $n \geq 0$. Also since $\big[g^i/p\big] = (g^i - g_i)/p$ and $g_{p-1} = g_0 = 1$, it follows from (3.8) that

$$\begin{aligned} \frac{B_m}{m} \equiv& \frac{g^m}{g^m - 1}q_p(g) - \frac{1}{p}\sum_{i=1}^{p-1} g^{mi} + \frac{1}{p}\sum_{i=1}^{p-1} g^{(m-1)i}g_i \\ \equiv& \frac{g^m}{g^m - 1}q_p(g) - \frac{g^m}{g^m - 1}q_p(p^m) + \frac{1}{p}f(g^{m-1}) + q_p(g^{m-1}) \\ \equiv& -\frac{m-1}{g^m - 1}q_p(g) + \frac{1}{p}f(g^{m-1}) \pmod{p}, \end{aligned}$$

which shows the first congruence in (3.7). The second one can be shown from the first by taking $x = g^{m-1}$ in (3.6).

Now letting $\theta = \zeta_{p-1}$ for brevity, we get immediately from (3.6)

$$\frac{1}{p}\left(g - \frac{1}{\theta}\right) f(\theta) = s(\theta). \tag{3.9}$$

If we set $\mathfrak{p} = (p, g-\theta)$ (the prime ideal of $\mathcal{O}_{K_{p-1}}$), then $g \equiv \theta \pmod{\mathfrak{p}}$ and hence $g^n \equiv \theta^n \pmod{\mathfrak{p}}$ for any $n \geq 0$. Taking this congruence into account, we obtain from (3.7) and (3.9) that, since $i = \theta^{(p-1)/4}$ and $-i = \theta^{3(p-1)/4}$,

$$\begin{aligned} H_1 &= \frac{1}{2p^2}\mathcal{N}_{K_4/\mathbb{Q}}(f(i)) = \frac{1}{2p^2}\left(\frac{p^2}{g^2+1}\mathcal{N}_{K_4/\mathbb{Q}}(s(i))\right) \\ &= \frac{1}{2(g^2+1)} s(i)s(-i) = \frac{1}{2(g^2+1)} s(\theta^{(p-1)/4}) s(\theta^{3(p-1)/4}) \\ &\equiv \frac{1}{2(g^2+1)} s(g^{(p-1)/4}) s(g^{3(p-1)/4}) \\ &\equiv M \cdot \frac{B_{(p+3)/4}}{(p+3)/4} \cdot \frac{B_{(3p+1)/4}}{(3p+1)/4} \pmod{p}, \end{aligned}$$

where M is given by, since $g^{(p-1)/2} \equiv -1 \pmod{p}$,

$$M = \frac{(g^{(p+3)/4}-1)(g^{(3p+1)/4}-1)}{2(g^2+1)} \equiv \frac{1}{2} \pmod{p}.$$

By the congruence (3.5), we can understand that $p \mid H_1$ if and only if at least one of pairs $(p, (p+3)/4)$ and $(p, (3p+1)/4)$ is irregular. However it is unknown whether these pairs are irregular or not as well as the pair $(p, (p-1)/2)$ related to the Ankeny-Artin-Chowla Conjecture on the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \pmod{4}$.

Concerning an upper bound for H_1, we can state

Proposition 3.4. *Let $p = 4q+1$ be an odd prime with q a prime. Then*

$$H_1 < q^2 = \left(\frac{p-1}{4}\right)^2.$$

Proof. As stated in Section 2, $C = |2U_0/p - q|$ and $D = |2U_1/p - q|$, where $U_a = \sum_k^{(a)} k$ for $a = 0, 1$. Here we can calculate U_a by means of a primitive root $g \pmod{p}$ as follows:

$$\begin{aligned} U_a = \sum\nolimits_k^{(a)} k &= \sum_{j=0}^{q-1} g_{4j+a} = \sum_{j=0}^{q-1}\left(g^{4j+a} - \left[\frac{g^{4j+a}}{p}\right]p\right) \\ &= \frac{g^a(g^{4q}-1)}{g^4-1} - p\sum_{j=0}^{q-1}\left[\frac{g^{4j+a}}{p}\right]. \end{aligned}$$

Using this we have

$$\left|\frac{2U_a}{p} - q\right| = 2\left|\frac{g^a}{g^4-1}q_p(g) - \sum_{j=0}^{q-1}\left[\frac{g^{4j+a}}{p}\right] - \frac{q}{2}\right|. \tag{3.10}$$

Since $x-1<[x]\le x$ for a real number x,

$$\sum_{j=0}^{q-1}\left(\frac{g^{4j+a}}{p}-1\right)=\frac{g^a}{g^4-1}q_p(g)-q<\sum_{j=0}^{q-1}\left[\frac{g^{4j+a}}{p}\right]$$
$$\le\sum_{j=0}^{q-1}\frac{g^{4j+a}}{p}=\frac{g^a}{g^4-1}q_p(g),$$

and hence it follows that

$$-\frac{q}{2}<\sum_{j=0}^{q-1}\left[\frac{g^{4j+a}}{p}\right]-\frac{g^a}{g^4-1}q_p(g)+\frac{q}{2}\le\frac{q}{2}.$$

Consequently, from (3.10) we can show $|2U_a/p-q|<q$ for each $a=0,1$ and this leads to $H_1=(C^2+D^2)/2<q^2$ as indicated. □

The size of H_2 is much larger than that of H_1 and it is surmised that H_2 grows more than exponentially with p. In fact, putting for a general prime p

$$G(p)=2p\left(\frac{p}{2\pi^2}\right)^{(p-1)/2},$$

Kummer conjectured in 1851 that asymptotically $h_p^-\sim G(p)$ as $p\to\infty$, i.e. $\lim_{p\to\infty}h_p^-/G(p)=1$. The proof of this assertion is unknown, however Granville expanded heuristic arguments in [6] and proved that the Elliott-Halberstam and the Hardy-Littlewood Conjectures together imply that Kummer's Conjecture is false (see also Fung *et al.* [5]). On the other hand, Lepistö [9] proved the bounds

$$-\frac{1}{2}\log p-4\log\log p-12.93-\frac{4.66}{\log p}$$
$$\le\log\left(\frac{h_p^-}{G(p)}\right)\le 5\log\log p+15.49+\frac{4.66}{\log p},$$

which shows that h_p^- grows rapidly. We cannot adopt the same argument as above because it is still open whether there exist infinitely many pairs (p,q) of primes satisfying $p=4q+1$, but we suppose from Proposition 3.4 that the growth of $H_2=h_p^-/H_1$ will be amazingly fast.

Here we want to enumerate concrete examples of $h_p^-, H_1, H_2, (C,D)$ and (S,T) for a few primes $p=4q+1$ with q a prime.

Examples:

- $(p,q)=(13,3)$: $h_p^-=1$;
  $H_1=1,\ (C,D)=(1,1);\ H_2=1,\ (S,T)=(5,2)$.
- $(p,q)=(29,7)$: $h_p^-=2^3$;
  $H_1=1,\ (C,D)=(1,1);\ H_2=2^3,\ (S,T)=(2\cdot 11,2\cdot 3)$.
- $(p,q)=(53,13)$: $h_p^-=4889$;
  $H_1=1,\ (C,D)=(1,1);\ H_2=4889,\ (S,T)=(2^5\cdot 3\cdot 5,47)$.
- $(p,q)=(149,37)$: $h_p^-=3^2\cdot 149\cdot 5129663838320040805461$;
  $H_1=3^2,\ (C,D)=(3,3);\ H_2=149\cdot 5129663838320040805461$,
  $(S,T)=(3\cdot 149\cdot 14489\cdot 145091, 2\cdot 149\cdot 1788084143)$.

- $(p,q) = (173, 43)$: $h_p^- = 5 \cdot 20297 \cdot 231169 \cdot 72571729362851870621$;
  $H_1 = 5$, $(C, D) = (1, 3)$;
  $H_2 = 20297 \cdot 231169 \cdot 72571729362851870621$,
  $(S, T) = (2 \cdot 3^2 \cdot 2978771 \cdot 14703269237, 131 \cdot 16477 \cdot 55695394459)$.

It seems from numerical tables (e.g., [8]) and other inspections that the following statements hold, although we do not have any definite ideas how to prove them.

(1) $H_1 < p$ and hence $p \nmid H_1$.

(2) $p \mid h_p^- \iff p \mid H_2 \iff p \mid S$ and $p \mid T$.

(3) $2 \nmid h_p^- \implies l^2 \nmid H_2$ for any odd primes l (i.e. H_2 is square-free).

It is possible to give an upper bound for $\log H_1 / \log p$ as a deduction from the Brauer-Siegel Theorem (cf. [16, Chapter 4]). We cannot say exactly now, but such an estimation may be useful to confirm (1).

In this paper, we discussed some arithmetic properties of factors of h_p^- only for the case when p has the form $p = 4q + 1$ with q a prime. It is possible to extend above results to more general cases for primes $p = 2^n q + 1$ where $n \geq 3$ and q is an odd prime.

Acknowledgments. The author would like to express many thanks to Tauno Metsänkylä for his valuable comments and to Tetsuya Taniguchi for his generous help concerning numerical verifications by computer.

References

[1] T. Agoh, *Congruences involving Bernoulli numbers and Fermat-Euler quotients*, J. Number Theory **94** (2002), 1–9.
[2] L. Carlitz, *The first factor of the class number of a cyclic field*, Canad. J. Math. **6** (1954), 23–26.
[3] D. Davis, *Computing the number of totally positive circular units which are squares*, J. Number Theory **10** (1978), 1–9.
[4] D. R. Estes, *On the parity of class number of the field of qth root of unity*, Rocky Mountain J. Math. **19** (1989), 675–682.
[5] G. Fung, A. Granville and H. C. Williams, *Computation of the first factor of the class number of cyclotomic fields*, J. Number Theory **42** (1992), 297–312.
[6] A. Granville, *On the size of the first factor of the class number of a cyclotomic field*, Invent. Math. **100** (1990), 321–338.
[7] D. H. Lehmer, *Prime factors of cyclotomic class numbers*, Math. Comp. **31** (1977), 599–607.
[8] D. H. Lehmer and J. M. Masley, *Table of cyclotomic class number $h^*(p)$ and their factors for $200 < p < 521$*, Math. Comp. **32** (1978), 577–582.
[9] T. Lepistö, *On the growth of the first factor of the class number of the prime cyclotomic field*, Ann. Acad. Sci. Fenn. Ser. AI **577** (1974), 1–21.
[10] T. Metsänkylä, *A congruence for the class number of a cyclic field*, Ann. Acad. Sci. Fenn. Ser. AI **472** (1970), 1–11.
[11] T. Metsänkylä, *On prime factors of the relative class numbers of cyclotomic fields*, Ann. Univ. Turku. Ser. AI **149** (1971), 1–8.
[12] T. Metsänkylä, *Some divisibility results for the cyclotomic class number*, Number Theory (Liptovský Ján, 1995), Tatra Mountains Math. Publ. **11** (1997), 59–68.
[13] T. Metsänkylä, *On the parity of the class number of real abelian fields*, Proc. of the 13th Czech and Slovak International Conference on Number Theory (Ostravice, 1997), Acta Math. Inf. Univ. Ostraviensis **6** (1996), 159–166.

[14] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, Berlin–Heidelberg–New York, 2001.
[15] P. Stevenhagen, *Class number parity for the pth cyclotomic field*, Math. Comp. **63** (1994), 773–784.
[16] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, Berlin–Heidelberg–New York, 1982.

Takashi Agoh, Department of Mathematics, Tokyo University of Science, 2641 Yamazaki, Noda, Chiba 278-8510, Japan
e-mail: agoh_takashi@ma.noda.tus.ac.jp