JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Takashi FUKUDA et Keiichi KOMATSU

Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, II

Tome 22, nº 2 (2010), p. 359-368.

<http://jtnb.cedram.org/item?id=JTNB_2010__22_2_359_0>

Journal de Théorie des Nombres
de Bordeaux **22** (2010), 359-368

Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, II

par Takashi FUKUDA et Keiichi KOMATSU

Résumé. Soit h_n le nombres de classes du n-ième étage de la $\mathbb{Z}_2$-extension cyclotomique de $\mathbb{Q}$. Weber a prouvé que h_n $(n \geq 1)$ est impair et Horie a prouvé que h_n $(n \geq 1)$ n'est divisible par aucun nombre premier ℓ satisfaisant $\ell \equiv 3, 5 \pmod 8$. Dans un article précédent, les auteurs ont montré h_n $(n \geq 1)$ n'est divisible par aucun nombre premier ℓ inférieur à 10^7. Dans le présent article, en étudiant plus précisément les propriétés d'une unité particulière, nous montrons que h_n $(n \geq 1)$ n'est divisible par aucun nombre premier ℓ inférieur à $1.2 \cdot 10^8$. Notre argument conduit aussi à la conclusion que h_n $(n \geq 1)$ n'est divisible par aucun nombre premier ℓ satisfaisant $\ell \not\equiv \pm 1 \pmod{16}$.

Abstract. Let h_n denote the class number of n-th layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$. Weber proved that h_n $(n \geq 1)$ is odd and Horie proved that h_n $(n \geq 1)$ is not divisible by a prime number ℓ satisfying $\ell \equiv 3, 5 \pmod 8$. In a previous paper, the authors showed that h_n $(n \geq 1)$ is not divisible by a prime number ℓ less than 10^7. In this paper, by investigating properties of a special unit more precisely, we show that h_n $(n \geq 1)$ is not divisible by a prime number ℓ less than $1.2 \cdot 10^8$. Our argument also leads to the conclusion that h_n $(n \geq 1)$ is not divisible by a prime number ℓ satisfying $\ell \not\equiv \pm 1 \pmod{16}$.

1. Introduction

Let $\zeta_n = \exp(2\pi\sqrt{-1}/2^n)$ and $\mathbb{Q}_n = \mathbb{Q}(\zeta_{n+2} + \zeta_{n+2}^{-1})$. Then $\mathbb{Q}_n$, which is n-th layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, is a cyclic extension of $\mathbb{Q}$ with degree 2^n. Weber [14] studied the class number h_n of $\mathbb{Q}_n$ and proved that h_n is odd for all $n \geq 1$. Weber also showed $h_1 = h_2 = h_3 = 1$. We note that h_{n-1} divides h_n because h_{n-1} is odd and $[\mathbb{Q}_n : \mathbb{Q}_{n-1}] = 2$.

Weber conjectured $h_4 > 1$. But Cohn [2], Bauer [1] and Masley [10] showed $h_4 = 1$. Furthermore Linden [11] showed $h_5 = 1$. It is also shown $h_6 = 1$ if GRH (Generalized Riemann Hypothesis) is valid. This phenomenon indicates a possibility that $h_n = 1$ for all $n \geq 1$. But the technique using root discriminant, which enables Masley and Linden to show $h_4 = 1$

Manuscrit reçu le 4 mars 2009, révisé le 4 février 2010.

and $h_5 = 1$ respectively, is no longer applicable for h_n $(n \geq 7)$. We need a entirety new technique to calculate h_n or to show $h_n = 1$ for $n \geq 7$.

The calculation of the whole class number h_n is very difficult even if we use a modern computer. So we are led to study the odd part of h_n. In this aspect, there are preceding works of Washington [12] and [13]. He proved that the ℓ-part of h_n is bounded as n tends to ∞ for a fixed prime number ℓ. Precisely speaking, using the theory of $\mathbb{Z}_p$-extensions, he developed a method which enables us to obtain an explicit bound on n for which the growth of e_n stops, where $h_n = \ell^{e_n} q$ with q not divisible by ℓ.

There is also an approach of Horie [5], [6], [7], [8] which tries to attack h_n from another point of view. He proved that if ℓ satisfies a certain congruence relation and exceeds a certain bound, which is explicitly described, then ℓ does not divide h_n for all $n \geq 1$, namely the ℓ-part of h_n is trivial for all $n \geq 1$. The following is a part of Horie's results.

Proposition 1.1 (Horie, cf. Proposition 3 in [8])**.** *Let ℓ be a prime number such that $\ell \equiv 3, 5 \pmod 8$. Then ℓ does not divide h_n for all $n \geq 1$.*

Horie also obtained the following results which treat higher congruence.

Proposition 1.2 (Horie, cf. Theorem 1 in [5] and Theorem 1 in [7])**.** *Let ℓ be a prime number.*

(1) *If $\ell \equiv 9 \pmod{16}$ and $\ell > 34797970939$, then ℓ does not divide h_n for all $n \geq 1$.*
(2) *If $\ell \equiv -9 \pmod{16}$ and $\ell > 210036365154018$, then ℓ does not divide h_n for all $n \geq 1$.*

Although Horie's results were very striking and very effective, there were many small prime numbers ℓ for which we did not know whether ℓ divides h_n. For example, it was not known whether $\ell \mid h_n$ $(n \geq 6)$ for $\ell = 7, 17, 23, 31, 41, \ldots$.

The main purpose of this paper is to prove the following two theorems. The first,which is proved by investigating the properties of a special unit introduced by Horie, is considered an explicit version of Theorem 3 in [12] and is a refinement of Theorems 1.2 and 5.1 in [3], which were proved by relating the plus part of the class number with the non-divisibility of Bernoulli numbers. For a real number x, we denote by $[x]$ the largest integer not exceeding x.

Theorem 1.1. *Let ℓ be an odd prime number and 2^c the exact power of 2 dividing $\ell - 1$ or $\ell^2 - 1$ according as $\ell \equiv 1 \pmod 4$ or not. Put*

$$m_\ell = 2c - 3 + [\log_2 \ell]$$

and recall h_n denotes the class number of $\mathbb{Q}_n$. Then ℓ does not divide h_n/h_{m_ℓ} for any integer $n \geq m_\ell$.

Typical values of m_ℓ are as follows:

ℓ	7	17	31	257	8191	65537	524287	7340033	39845887
m_ℓ	7	9	14	21	38	45	56	59	66

Theorem 1.1 has a computational application. An algorithm verifying that ℓ does not divide h_n for given ℓ and n was established in [3] and the value of m_ℓ is small enough for this algorithm. So we are able to derive the following corollary which will supersede Corollary 1.3 in [3]. We implemented the algorithms in [3] on a computer with Xeon 2.0 GHz processor and 32 GB memory using TC. The calculating time was three months.

Corollary 1.1. *Let ℓ be a prime number less than $1.2 \cdot 10^8$. Then ℓ does not divide h_n for all $n \geq 1$.*

The second is considered a precise version of Proposition 1.2, which is a direct consequence of Corollary 1.1 and Lemma 2.3 in §2.

Theorem 1.2. *Notations being as in Theorem 1.1, if $\ell \equiv \pm 9 \pmod{16}$, then ℓ does not divide h_n for all $n \geq 1$.*

Remark. After we wrote this manuscript, we were aware of the preprint of K. Horie and M. Horie [9], in which they showed that a prime number ℓ does not divide h_n for all $n \geq 1$ if ℓ satisfies $\ell \equiv 9 \pmod{16}$ and $\ell > 7150001069$ or if $\ell \equiv -9 \pmod{16}$ and $\ell > 17324899980$.

Acknowledgment. The authors would like to express their gratitude to the referee who read the manuscript carefully and suggested computations with simpler formulae.

2. Proofs

We prove our theorems by using Horie's method in [8]. Notations being as in Theorem 1.1, let $\zeta_n = \exp(2\pi\sqrt{-1}/2^n)$ and put

$$\eta_n = \frac{\zeta_{n+2} - 1}{\sqrt{-1}(\zeta_{n+2} + 1)}$$

Then η_n is a unit and contained in $\mathbb{Q}_n$ because $\mathbb{Q}_n$ is the maximal real subfield of $\mathbb{Q}(\zeta_{n+2})$. This special unit, which played important role in Horie's work, takes an active part also in our proofs. First we note

$$N_{\mathbb{Q}_n/\mathbb{Q}_{n-1}}(\eta_n) = \frac{\zeta_{n+2} - 1}{\sqrt{-1}(\zeta_{n+2} + 1)} \, \frac{-\zeta_{n+2} - 1}{\sqrt{-1}(-\zeta_{n+2} + 1)} = -1. \tag{2.1}$$

An element α in $\mathbb{Z}[\zeta_n]$ is uniquely expressed in the form

$$\alpha = \sum_{j=0}^{2^{n-1}-1} a_j \zeta_n^j \quad (a_j \in \mathbb{Z}).$$

For each such α and each $\sigma \in G(\mathbb{Q}(\zeta_{n+2})/\mathbb{Q}(\zeta_2))$, we define the element α_σ in the group ring $\mathbb{Z}[G(\mathbb{Q}(\zeta_{n+2})/\mathbb{Q}(\zeta_2))]$ by

$$\alpha_\sigma = \sum_{j=0}^{2^{n-1}-1} a_j \sigma^j .$$

The following Horie's results are essential in this paper. Following the referee's advice that self-contained paper is convenient for readers, we give proofs here. The idea is due to the referee.

Proposition 2.1 (Horie, cf. Lemma 2 in [5])**.** *Let ℓ be an odd prime number, σ a generator of the Galois group $G(\mathbb{Q}(\zeta_{n+2})/\mathbb{Q}(\zeta_2))$ and F an extension in $\mathbb{Q}(\zeta_n)$ of the decomposition field of ℓ with respect to for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Then ℓ divide h_n/h_{n-1} if and only if there exists a prime ideal $\mathfrak{L}$ of F dividing ℓ such that $\eta_n^{\alpha_\sigma}$ is an ℓ-th power in $\mathbb{Q}_n$ for any element α of the ideal $\ell\mathfrak{L}^{-1}$ of F.*

Proof. We prove "only if part" which is sufficient for our purpose. We take an integer s with $\zeta_{n+2}^\sigma = \zeta_{n+2}^s$ and put

$$\rho = \sigma^{2^{n-1}}, \quad \xi = \frac{\zeta_{n+3} - \zeta_{n+3}^{-1}}{\zeta_{n+3}^s - \zeta_{n+3}^{-s}} .$$

Let E_n be the unit group of $\mathbb{Q}_n$ and C_n the cyclotomic unit group of $\mathbb{Q}_n$, which is generated by $\{ \xi^{\sigma^i} \mid i = 1, 2, \ldots, 2^n \}$. Then $\mathbb{Z}[\zeta_n]$ acts on $E_n^{1-\rho}$ by $(\varepsilon^{1-\rho})^\alpha = (\varepsilon^{1-\rho})^{\alpha_\sigma}$ for $\varepsilon \in E_n$ and $\alpha \in \mathbb{Z}[\zeta_n]$ and we have

$$\mathbb{Z}_\ell \otimes (E_n^{1-\rho}/C_n^{1-\rho}) \cong \prod_j \mathbb{Z}[\zeta_n]/\mathfrak{L}_j^{k_j} ,$$

where $\mathfrak{L}_j$ runs through the prime ideals of $\mathbb{Q}(\zeta_n)$ lying above ℓ and k_j is a non-negative integer. Moreover the order of $E_n^{1-\rho}/C_n^{1-\rho}$ is h_n/h_{n-1} by analytic class number formula.

Now we assume that ℓ divides h_n/h_{n-1}. Then there exists a prime ideal $\mathfrak{L}_j$ of $\mathbb{Q}(\zeta_n)$ lying above ℓ with $k_j > 0$. Hence we have $(\xi^{1-\rho})^{\alpha_\sigma}$ is an ℓ-th power in $\mathbb{Q}_n$ for $\alpha \in (\ell)\mathfrak{L}_j^{-1}$. Since $(\eta_n^{1+\rho})^2 = 1$ by (2.1), we have

$$\eta_n^4 = \eta_n^{2-2\rho} = \eta_n^{2(1-\sigma)(1+\sigma+\cdots+\sigma^{2^{n-1}-1})} .$$

This shows

$$\eta_n^4 = (\xi^{1-\rho})^{2(1+\sigma+\cdots+\sigma^{2^{n-1}-1})}$$

by $\eta_n^{1-\sigma} = \xi^{1-\rho}$, which means $\eta_n^{\alpha_\sigma}$ is an ℓ-th power in $\mathbb{Q}_n$. □

Proposition 2.2 (Horie, cf. Lemma 5 in [4]). *Let ℓ be an odd prime number and φ the Frobenius automorphism of ℓ in $\mathbb{Q}(\zeta_{n+2})/\mathbb{Q}$. If an element β in $\mathbb{Z}[\zeta_{n+2}]$ is an ℓ-th power in $\mathbb{Z}[\zeta_{n+2}]$, then $\beta^\varphi - \beta^\ell \in \ell^2\mathbb{Z}[\zeta_{n+2}]$.*

Proof. Put $\beta = x^\ell$ and $x^\varphi = x^\ell + \ell u$ with $x, u \in \mathbb{Z}[\zeta_{n+2}]$. Then

$$\beta^\varphi = (x^\varphi)^\ell = (x^\ell + \ell u)^\ell = (\beta + \ell u)^\ell \equiv \beta^\ell \pmod{\ell^2}.$$

□

Let ℓ and φ be as in Proposition 2.2, $\zeta = \zeta_{n+2}$, σ a generator of $G(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta_2))$ and put $\eta = \eta_n = (\zeta - 1)/(\sqrt{-1}(\zeta + 1))$. We choose $\mathbb{Q}(\zeta_c)$ as F. We assume $n \geq c$ and ℓ divides h_n/h_{n-1}. Then, by Proposition 2.1, there exists a prime ideal $\mathfrak{L}$ in $\mathbb{Q}(\zeta_c)$ dividing ℓ such that η^{α_σ} is an ℓ-th power of a unit in $\mathbb{Q}_n$ for any element α of the ideal $\ell\mathfrak{L}^{-1}$ of $\mathbb{Q}(\zeta_c)$. let

$$\alpha = \sum_{i=0}^{2^{c-1}-1} a_i (\zeta_n^{2^{n-c}})^i$$

be an element in $\ell\mathfrak{L}^{-1}$ with $a_i \in \mathbb{Z}$. we put $\tau = \sigma^{2^{n-c}}$. Then $\alpha_\sigma = \sum_{i=0}^{2^{c-1}-1} a_i \tau^i$ and $(\zeta^{\tau^i - 1})^{2^c} = 1$. Now, we start computations similar to Lemma 13 in [8]. Noting that

$$\begin{aligned}(\beta + \gamma)^{a\ell} &= \Big(\beta^\ell + \gamma^\ell + \sum_{k=1}^{\ell-1} \binom{\ell}{k} \beta^{\ell-k}\gamma^k\Big)^a \\ &\equiv (\beta^\ell + \gamma^\ell)^a + a(\beta^\ell + \gamma^\ell)^{a-1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \beta^{\ell-k}\gamma^k \pmod{\ell^2}\end{aligned}$$

for $\beta, \gamma \in \mathbb{Z}[\zeta]$ with $\beta + \gamma$ prime to ℓ and for $a \in \mathbb{Z}$, it follows that

$$\begin{aligned}(\zeta^{\tau^i} - 1)^{a_i\ell} &\equiv (\zeta^{\ell\tau^i} - 1)^{a_i} \\ &\quad + a_i(\zeta^{\ell\tau^i} - 1)^{a_i - 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \zeta^{\tau^i(\ell-k)}(-1)^k \pmod{\ell^2}, \\ (\zeta^{\tau^i} + 1)^{-a_i\ell} &\equiv (\zeta^{\ell\tau^i} + 1)^{-a_i} \\ &\quad - a_i(\zeta^{\ell\tau^i} + 1)^{-a_i - 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \zeta^{\tau^i(\ell-k)} \pmod{\ell^2}.\end{aligned}$$

From these congruence relations and a consequence

$$\begin{aligned}\frac{(\eta^{\alpha_\sigma})^\ell - (\eta^{\alpha_\sigma})^\varphi}{\sqrt{-1}^{\,-\ell\alpha^\sigma}} &= \prod_{i=0}^{2^{c-1}-1} \frac{(\zeta^{\tau^i} - 1)^{a_i\ell}}{(\zeta^{\tau^i} + 1)^{a_i\ell}} - \prod_{i=0}^{2^{c-1}-1} \Big(\frac{\zeta^{\ell\tau^i} - 1}{\zeta^{\ell\tau^i} + 1}\Big)^{a_i} \\ &\equiv 0 \pmod{\ell^2}\end{aligned}$$

of Propositions 2.1 and 2.2, we have

$$\sum_{i=0}^{2^{c-1}-1}\Big(\frac{a_i}{\zeta^{\ell\tau^i}-1}\sum_{k=1}^{\ell-1}\binom{\ell}{k}(-1)^k\zeta^{\tau^i(\ell-k)} - \frac{a_i}{\zeta^{\ell\tau^i}+1}\sum_{k=1}^{\ell-1}\binom{\ell}{k}\zeta^{\tau^i(\ell-k)}\Big) \equiv 0 \pmod{\ell^2}$$

because $\zeta^{\ell(\tau^i-1)} \pm \zeta^{-\ell}$ are prime to ℓ. Since

$$\binom{\ell}{k} \equiv \frac{\ell(-1)^{k-1}}{k} \pmod{\ell^2} \quad (1 \le k \le \ell-1)$$

and since

$$\prod_{i=0}^{2^{c-1}-1}(\zeta^{\ell\tau^i}-1)(\zeta^{\ell\tau^i}+1) = \prod_{i=0}^{2^{c-1}-1}(\zeta^{2\ell\tau^i}-1) = 1-\zeta^{2^c\ell},$$

we have

$$\begin{aligned}
(1-\zeta^{2^c\ell}) &\sum_{i=0}^{2^{c-1}-1}\Big(\frac{a_i}{\zeta^{\ell\tau^i}-1}\sum_{k=1}^{\ell-1}\binom{\ell}{k}(-1)^k\zeta^{\tau^i(\ell-k)} - \frac{a_i}{\zeta^{\ell\tau^i}+1}\sum_{k=1}^{\ell-1}\binom{\ell}{k}\zeta^{\tau^i(\ell-k)}\Big)\\
&\equiv \ell\sum_{i=0}^{2^{c-1}-1}a_i\Big(\sum_{j=0}^{2^c-1}-\zeta^{\ell\tau^i(2^c-1-j)}\sum_{k=1}^{\ell-1}\frac{(-1)^{2k-1}}{k}\zeta^{\tau^i(\ell-k)}\\
&\qquad -\sum_{j=0}^{2^c-1}(-1)^{2^c-1-j}\zeta^{\ell\tau^i(2^c-1-j)}\sum_{k=1}^{\ell-1}\frac{(-1)^{k-1}}{k}\zeta^{\tau^i(\ell-k)}\Big)\\
&\equiv 0 \pmod{\ell^2}.
\end{aligned}$$

Hence we have

$$\sum_{i=0}^{2^{c-1}-1}a_i\sum_{j=0}^{2^c-1}\sum_{k=1}^{\ell-1}\Big(\frac{1}{k}+\frac{(-1)^{j+k+1}}{k}\Big)\zeta^{-\tau^i(\ell j+k)} \equiv 0 \pmod{\ell}$$

by $\zeta^{2^c(\tau^i-1)}=1$. Considering the complex conjugate of the left hand side of the above congruence relation, we have the following:

Lemma 2.1. *Let α be in Proposition 2.1 and*

$$\alpha = \sum_{i=0}^{2^{c-1}-1}a_i\Big(\zeta_n^{2^{n-c}}\Big)^i \tag{2.2}$$

with $a_i \in \mathbb{Z}$. *If* ℓ *divides* h_n/h_{n-1}, *then*

$$\sum_{i=0}^{2^{c-1}-1} a_i \sum_{j=0}^{2^c-1} \sum_{k=1}^{\ell-1} \frac{1+(-1)^{j+k+1}}{k} \zeta^{\tau^i(\ell j+k)} \equiv 0 \pmod{\ell}.$$

We put

$$S = \{\, b_0 2^{n-c+2} + b_1 2^{n-c+3} + \cdots + b_{c-1} 2^{n+1} \mid b_j = 0, 1 \text{ for } 0 \le j \le c-1 \,\}$$

and define the subset S' of S by

$$S' = \bigcup_{i=0}^{2^{c-1}-1} \{\, r \in S \mid \zeta^{\tau^i - 1} = \zeta^r \,\}.$$

Lemma 2.2. *Let* j *and* k *be rational integers with* $0 \le j \le 2^c - 1$, $1 \le k \le \ell - 1$ *and* $r \in S'$. *Let* ℓ *be an odd prime number with* $\ell < 2^{n-2c+3}$. *If* $(r+1)(\ell j + k) \equiv 2^{c-1}\ell - 1 \pmod{2^{n+1}}$, *then we have* $j = 2^{c-1} - 1$, $k = \ell - 1$ *and* $r = 0$.

Proof. We have $-2^{n-c+2} < (2^{c-1} - j)\ell - k - 1 < 2^{n-c+2}$ because of $0 \le j \le 2^c - 1$, $1 \le k \le \ell - 1$ and $\ell < 2^{n-2c+3}$. Since $(2^{c-1} - j)\ell - k - 1 \equiv 0 \pmod{2^{n-c+2}}$, we have $(2^{c-1} - j)\ell - k - 1 = 0$. Since $2 \le k+1 = (2^{c-1} - j)\ell \le \ell$, we have $k = \ell - 1$ and $j = 2^{c-1} - 1$, which implies $r \equiv 0 \pmod{2^{n+1}}$. Hence $r = 0$ or $r = 2^{n+1}$. Since $r \in S'$, we have $r = 0$. □

Proof of Theorem 1.1. The assertion of the theorem is trivial when $n = m_\ell$. So we assume that ℓ divides h_n/h_{n-1} for some n greater than m_ℓ. Then ℓ satisfies $\ell < 2^{n-2c+3}$ and Lemma 2.1 yields

$$\sum_{i=0}^{2^{c-1}-1} a_i \sum_{j=0}^{2^c-1} \sum_{k=1}^{\ell-1} \frac{1+(-1)^{j+k+1}}{k} \zeta^{\tau^i(\ell j+k)} \equiv 0 \pmod{\ell},$$

where a_i is the rational integer defined by (2.2). We choose an element α in $\ell\mathfrak{L}^{-1}$ so that $\alpha \notin \ell\mathbb{Z}[\zeta_c]$. Since we may assume $a_0 \not\equiv 0 \pmod{\ell}$, we see that $a_i \dfrac{-1+(-1)^{j+k}}{k} \not\equiv 0 \pmod{\ell}$ for $i = 0$, $j = 2^{c-1} - 1$ and $k = \ell - 1$. This contradicts Lemma 2.2 because $\{\, \zeta^i \mid 0 \le i \le 2^{n+1} - 1 \,\}$ is an integral basis of $\mathbb{Q}(\zeta)$. □

We follow the arguments in [5] to prove Theorem 1.2. For an algebraic number α, let

$$\|\, \alpha \,\| = \max_\rho |\, \alpha^\rho \,|,$$

where ρ runs through all isomorphism of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$. Then

$$\|\, \beta\beta' \,\| \le \|\, \beta \,\| \cdot \|\, \beta' \,\|, \quad \|\, \beta^m \,\| = \|\, \beta \,\|^m$$

for any algebraic numbers β, β' and any positive rational integer m. The following is the key lemma in our proof.

Lemma 2.3. *Assume that an odd prime number ℓ divides h_n/h_{n-1}.*

(1) *If* $\ell \equiv 9 \pmod{16}$, *then we have* $2^{n-3} < \ell < 32(n+1)^4$.

(2) *If* $\ell \equiv -9 \pmod{16}$, *then we have* $2^{n-5} < \ell < 98(n+1)^4$.

Proof. It is known that $h_5 = 1$ by [11]. So we may assume $n \geq 6$. Recall that σ is a generator of $G(\mathbb{Q}(\zeta_{n+2})/\mathbb{Q}(\zeta_2))$. (1) The decomposition field of ℓ with respect to $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $\mathbb{Q}(\zeta_3)$. Proposition 2.1 guarantees the existence of a prime ideal $\mathfrak{L}$ of $\mathbb{Q}(\zeta_3)$ dividing ℓ such that η^{α_σ} is an ℓ-th power in $\mathbb{Q}_n$ for each element α of $\mathbb{Q}(\zeta_3)$ with $\ell\mathfrak{L}^{-1} = (\alpha)$. We write $\alpha = a_0 + a_1\zeta_3 + a_2\zeta_3^2 + a_3\zeta_3^3$ with $a_i \in \mathbb{Z}$ and denote by $\overline{\alpha}$ the complex conjugate of α. Then we have

$$\alpha\overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2 + \sqrt{2}(a_0a_1 + a_1a_2 + a_2a_3 - a_3a_0).$$

We put $a = (a_0^2+a_1^2+a_2^2+a_3^2)/\ell^{3/2}$ and $b = (a_0a_1+a_1a_2+a_2a_3-a_3a_0)/\ell^{3/2}$. Since $N_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(\alpha) = \ell^3$, we have $a^2 - 2b^2 = 1$. Hence there exists a real number x with $a + b\sqrt{2} = (\sqrt{2}+1)^x$ and $a - b\sqrt{2} = (\sqrt{2}-1)^x$. Since $(\alpha) = (\alpha(1+\sqrt{2})^m)$ for $m \in \mathbb{Z}$, we may assume $-1 \leq x < 1$. Hence we have $0 \leq a \leq \sqrt{2}$, which implies $a_0^2 + a_1^2 + a_2^2 + a_3^2 \leq \sqrt{2}\ell^{3/2}$. This shows $|a_0| + |a_1| + |a_2| + |a_3| \leq 2^{5/4}\ell^{3/4}$. Noting that $\eta^{\alpha_\sigma} \neq \pm 1$ (cf. [5, p. 384]), we have

$$2^\ell < \|\, \eta^{\alpha_\sigma} \,\| = \|\, \eta^{a_0 + a_1\sigma^{2^{n-3}} + a_2\sigma^{2\cdot 2^{n-3}} + a_3\sigma^{3\cdot 2^{n-3}}} \,\| \leq \|\, \eta \,\|^{|a_0|+|a_1|+|a_2|+|a_3|} \leq \|\, \eta \,\|^{2^{5/4}\ell^{3/4}} < 2^{2^{5/4}(n+1)\ell^{3/4}} \tag{2.3}$$

by the formula (2.1) and [5, Lemmas 3 and 4]. On the other hand, we have

$$n \leq m_\ell = 3 + [\,\log_2 \ell\,] < 3 + \log_2 \ell \tag{2.4}$$

by Theorem 1.1. Combining (2.3) and (2.4), we derive the desired inequality.

(2) In this case, the decomposition field F of ℓ with respect to $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is $\mathbb{Q}(\sqrt{-1}\sqrt{2-\sqrt{2}})$, which is contained in $\mathbb{Q}(\zeta_4)$. Proposition 2.1 again guarantees the existence of a prime ideal $\mathfrak{L}$ of F dividing ℓ such that η^{α_σ} is an ℓ-th power in $\mathbb{Q}_n$ for each element α of F with $\ell\mathfrak{L}^{-1} = (\alpha)$. We write $\alpha = a_0 + a_1\zeta_4 + \cdots + a_7\zeta_4^7$ with $a_i \in \mathbb{Z}$. For the Frobenius automorphism φ_ℓ of ℓ with respect to $\mathbb{Q}(\zeta_4)/\mathbb{Q}$, we have $\alpha^{\varphi_\ell} = \alpha$, which implies $a_4 = 0$, $a_5 = a_3$, $a_6 = -a_2$ and $a_7 = a_1$. Hence we have

$$\alpha = a_0 + a_1(\zeta_4 + \zeta_4^7) + a_2(\zeta_4^2 - \zeta_4^6) + a_3(\zeta_4^3 + \zeta_4^5).$$

This shows

$$\alpha\overline{\alpha} = a_0^2 + 2a_1^2 + 2a_2^2 + 2a_3^2 + \sqrt{2}(2a_0a_2 - a_1^2 + 2a_1a_3 + a_3^2).$$

We put $a = (a_0^2+2a_1^2+2a_2^2+2a_3^2)/\ell^{3/2}$ and $b = (2a_0a_2-a_1^2+2a_1a_3+a_3^2)/\ell^{3/2}$. Since $N_{F/\mathbb{Q}}(\alpha) = \ell^3$, we have $a^2 - 2b^2 = 1$. Hence there exists a real number

x with $a+b\sqrt{2}=(\sqrt{2}+1)^x$ and $a-b\sqrt{2}=(\sqrt{2}-1)^x$. In a way similar to that in the case $\ell \equiv 9 \pmod{16}$, we have $a_0^2+2(a_1^2+a_2^2+a_3^2) \le \sqrt{2}\ell^{3/2}$, which shows $|a_0|+2(\,|a_1|+|a_2|+|a_3|\,) \le 2^{1/4}\sqrt{7}\ell^{3/4}$. Hence we have

$$
\begin{aligned}
(2.5)\quad 2^\ell &< ||\,\eta^{\alpha_\sigma}\,|| \\
&= ||\,\eta^{a_0+a_1(\sigma^{2^{n-4}}+\sigma^{7\cdot 2^{n-4}})+a_2(\sigma^{2\cdot 2^{n-4}}-\sigma^{6\cdot 2^{n-4}})+a_3(\sigma^{3\cdot 2^{n-4}}+\sigma^{5\cdot 2^{n-4}})}\,|| \\
&\le ||\,\eta\,||^{|a_0|+2(\,|a_1|+|a_2|+|a_3|\,)} \\
&\le ||\,\eta\,||^{2^{1/4}\sqrt{7}\ell^{3/4}} < \left(\frac{2^{n+2}}{\pi}\right)^{2^{1/4}\sqrt{7}\ell^{3/4}} < 2^{2^{1/4}\sqrt{7}(n+1)\ell^{3/4}}.
\end{aligned}
$$

In this case, Theorem 1.1 implies

$$(2.6)\qquad n \le m_\ell = 5+[\,\log_2 \ell\,] < 5+\log_2 \ell$$

and we combine (2.5) and (2.6) to derive the conclusion. □

Proof of Theorem 1.2. Assume that ℓ divides h_n/h_{n-1} for some $n \ge 1$. Then Lemma 2.3 implies $\ell < 32\cdot 28^4 = 19668992$ if $\ell \equiv 9 \pmod{16}$ or $\ell < 98\cdot 32^4 = 102760448$ if $\ell \equiv -9 \pmod{16}$. However this contradicts Corollary 1.1. Hence the proof is completed.

□

Remark. We are also able to prove Theorem 1.2 by combining Proposition 1.2 and Theorem 1.1. Namely, it suffices to verify that ℓ does not divide h_{m_ℓ} for all ℓ not exceeding a certain explicit bound. This bound on ℓ is 34797970939 in the case $\ell \equiv 9 \pmod{16}$ and 210036365154018 in the case $\ell \equiv -9 \pmod{16}$. The calculating time is estimated about one month or one thousand years.

References

[1] H. Bauer, *Numeriche Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper.* J. Number Theory **1** (1969), 161–162.

[2] H. Cohn, *A numerical study of Weber's real class number calculation I.* Numer. Math. **2** (1960), 347–362.

[3] T. Fukuda and K. Komatsu, *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$.* Experimental Math. **18** (2009), 213–222.

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

[5] 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.

[6] K. Horie, *Triviality in ideal class groups of Iwasawa-theoretical abelian number fields.* J. Math. Soc. Japan **57** (2005), 827–857.

[7] K. Horie, *Primary components of the ideal class groups of Iwasawa-theoretical abelian number field.* J. Math. Soc. Japan **59** (2007), 811–824.

[8] K. Horie, *Certain primary components of the ideal class group of the $\mathbb{Z}_p$-extension over the rationals.* Tohoku Math. J. **59** (2007), 259–291.

[9] K. Horie and M. Horie, *The ideal class group of the $\mathbb{Z}_p$-extension over the rationals.* Tohoku Math. J., **61** (2009), 551–570.

[10] J. M. Masley, *Class numbers of real cyclic number fields with small conductor*. Compositio Math. **37** (1978), 297–319.
[11] F. J. van der Linden, *Class Number Computations of Real Abelian Number Fields*. Math. Comp. **39** (1982), 693–707.
[12] L. C. Washington, *Class numbers and $\mathbb{Z}_p$-extensions*. Math. Ann. **214** (1975), 177–193.
[13] L. C. Washington, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*. Inv. Math. **49** (1978), 87–97.
[14] H. Weber, *Theorie der Abel'schen Zahlkörper*. Acta Math. **8** (1886), 193–263.

Takashi Fukuda
Department of Mathematics
College of Industrial Technology
Nihon University
2-11-1 Shin-ei, Narashino, Chiba, Japan
E-mail: fukuda@math.cit.nihon-u.ac.jp

Keiichi Komatsu
Department of Mathematics
School of Science and Engineering
Waseda University
3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan
E-mail: kkomatsu@waseda.jp