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

Takashi Fukuda and Keiichi Komatsu


<http://jtnb.cedram.org/item?id=JTNB_2010__22_2_359_0>
Weber’s class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, II

par Takashi FUKUDA et Keiichi KOMATSU

1. Introduction

Let $\zeta_n = \exp(2\pi \sqrt{-1}/2^n)$ and $Q_n = \mathbb{Q}(\zeta_{n+2} + \zeta_{n+2}^{-1})$. Then $Q_n$, 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 $Q_n$ 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 $[Q_n : Q_{n-1}] = 2$.

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 $h_4 = 1$
and $h_5 = 1$ respectively, is no longer applicable for $h_n$ $(n \geq 7)$.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 $\ell$-part of $h_n$ is bounded as $n$ tends to $\infty$ for a fixed prime number $\ell$. 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 $\ell$.

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 $\ell$ satisfies a certain congruence relation and exceeds a certain bound, which is explicitly described, then $\ell$ does not divide $h_n$ for all $n \geq 1$, namely the $\ell$-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 $\ell$ be a prime number such that $\ell \equiv 3, 5 \pmod{8}$. Then $\ell$ 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 $\ell$ be a prime number.

1. If $\ell \equiv 9 \pmod{16}$ and $\ell > 34797970939$, then $\ell$ does not divide $h_n$ for all $n \geq 1$.

2. If $\ell \equiv -9 \pmod{16}$ and $\ell > 210036365154018$, then $\ell$ 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 $\ell$ for which we did not know whether $\ell$ divides $h_n$. For example, it was not known whether $\ell \mid h_n$ $(n \geq 6)$ for $\ell = 7, 17, 23, 31, 41, ...$.

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 $\lfloor x \rfloor$ the largest integer not exceeding $x$.

**Theorem 1.1.** Let $\ell$ 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

$$m_\ell = 2c - 3 + \lceil \log_2 \ell \rceil$$

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

Typical values of $m_\ell$ are as follows:

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>7</th>
<th>17</th>
<th>31</th>
<th>257</th>
<th>8191</th>
<th>65537</th>
<th>524287</th>
<th>7340033</th>
<th>39845887</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m_\ell$</td>
<td>7</td>
<td>9</td>
<td>14</td>
<td>21</td>
<td>38</td>
<td>45</td>
<td>56</td>
<td>59</td>
<td>66</td>
</tr>
</tbody>
</table>

Theorem 1.1 has a computational application. An algorithm verifying that $\ell$ does not divide $h_n$ for given $\ell$ and $n$ was established in [3] and the value of $m_\ell$ 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 $\ell$ be a prime number less than $1.2 \cdot 10^8$. Then $\ell$ 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 $\ell$ 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 $\ell$ does not divide $h_n$ for all $n \geq 1$ if $\ell$ 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 $\eta_n$ 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

$$
(2.1) \quad N_{\mathbb{Q}_n/\mathbb{Q}_{n-1}}(\eta_n) = \frac{\zeta_{n+2} - 1}{\sqrt{-1}(\zeta_{n+2} + 1)} \quad \frac{-\zeta_{n+2} - 1}{\sqrt{-1}(-\zeta_{n+2} + 1)} = -1.
$$
An element $\alpha$ 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 $\alpha$ and each $\sigma \in G(\mathbb{Q}(\zeta_{n+2})/\mathbb{Q}(\zeta_2))$, we define the element $\alpha_\sigma$ 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 $\ell$ be an odd prime number, $\sigma$ 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 $\ell$ with respect to for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Then $\ell$ divide $h_n/h_{n-1}$ if and only if there exists a prime ideal $\mathfrak{L}$ of $F$ dividing $\ell$ such that $\eta_\ell^{\alpha_\sigma}$ is an $\ell$-th power in $\mathbb{Q}_n$ for any element $\alpha$ 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 $\zeta_{n+2}^s = \zeta_{n+2}$ and put
$$\rho = \sigma^{2^{n-1}}, \quad \xi = \frac{\zeta_{n+3} - \zeta_{n+3}^{-1}}{\zeta_{n+3}^\rho - \zeta_{n+3}^{-\rho}}.$$

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 $\{ \xi^i | i = 1, 2, \ldots, 2^n \}$. 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 $\ell$ 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 $\ell$ divides $h_n/h_{n-1}$. Then there exists a prime ideal $\mathfrak{L}_j$ of $\mathbb{Q}(\zeta_n)$ lying above $\ell$ with $k_j > 0$. Hence we have $(\xi^{1-\rho})_{\alpha_\sigma}$ is an $\ell$-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
$$\eta_n^{1-\sigma} = \xi^{1-\rho},$$
by $\eta_n^{1-\sigma} = \xi^{1-\rho}$, which means $\eta_\ell^{\alpha_\sigma}$ is an $\ell$-th power in $\mathbb{Q}_n$. \qed
Proposition 2.2 (Horie, cf. Lemma 5 in [4]). Let $\ell$ be an odd prime number and $\varphi$ the Frobenius automorphism of $\ell$ in $Q(\zeta_{n+2})/Q$. If an element $\beta$ in $Z[\zeta_{n+2}]$ is an $\ell$-th power in $Z[\zeta_{n+2}]$, then $\beta^\varphi - \beta^\ell \in \ell^2Z[\zeta_{n+2}]$.

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

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

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

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

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

$$(\beta + \gamma)^a\ell = \left(\beta^\ell + \gamma^\ell + \sum_{k=1}^{\ell-1} \binom{\ell}{k} \beta^{\ell-k}\gamma^k\right)^a$$

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

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

$$(\zeta^{\ell i} - 1)^{a_i}\ell \equiv (\zeta^{\ell \tau i} - 1)^{a_i}\ell$$

$$+ a_i(\zeta^{\ell \tau i} - 1)^{a_i-1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \zeta^{\tau i(\ell-k)}(-1)^k \pmod{\ell^2},$$

$$(\zeta^{\ell i} + 1)^{-a_i}\ell \equiv (\zeta^{\ell \tau i} + 1)^{-a_i}\ell$$

$$- a_i(\zeta^{\ell \tau i} + 1)^{-a_i-1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \zeta^{\tau i(\ell-k)} \pmod{\ell^2}.$$
of Propositions 2.1 and 2.2, we have
\[
\sum_{i=0}^{2^{c-1}-1} \left( \frac{a_i}{\zeta^{\ell\tau^i}} - \zeta^{\ell\tau^i} \right) \sum_{k=1}^{\ell-1} \binom{\ell}{k} (-1)^k \zeta^{\tau^i(\ell-k)} - \frac{a_i}{\zeta^{\ell\tau^i} + 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \zeta^{\tau^i(\ell-k)} \equiv 0 \pmod{\ell^2}
\]

because \(\zeta^{\ell(\tau^i-1)} \pm \zeta^{-\ell}\) are prime to \(\ell\). Since
\[
\binom{\ell}{k} \equiv \ell(-1)^{k-1} \pmod{\ell^2} \quad (1 \leq k \leq \ell - 1)
\]
and since
\[
\prod_{i=0}^{2^{c-1}-1} (\zeta^{\ell\tau^i} - 1)(\zeta^{\ell\tau^i} + 1) = \prod_{i=0}^{2^{c-1}-1} (\zeta^{2\ell\tau^i} - 1) = 1 - \zeta^{2\ell}
\]
we have
\[
(1 - \zeta^{2\ell}) \sum_{i=0}^{2^{c-1}-1} \left( \frac{a_i}{\zeta^{\ell\tau^i} - 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} (-1)^k \zeta^{\tau^i(\ell-k)} - \frac{a_i}{\zeta^{\ell\tau^i} + 1} \sum_{k=1}^{\ell-1} \binom{\ell}{k} \zeta^{\tau^i(\ell-k)} \right)
\]
\[
\equiv \ell \sum_{i=0}^{2^{c-1}-1} a_i \left( \sum_{j=0}^{2^{c-1}-1} -\zeta^{\ell\tau^i(2^{c-1}-j)} \sum_{k=1}^{\ell-1} \frac{(-1)^{2k-1}}{k} \zeta^{\tau^i(\ell-k)} - \sum_{j=0}^{2^{c-1}-1} (-1)^{2^{c-1}-j} \zeta^{\ell\tau^i(2^{c-1}-j)} \sum_{k=1}^{\ell-1} \frac{(-1)^{k-1}}{k} \zeta^{\tau^i(\ell-k)} \right)
\]
\[
\equiv 0 \pmod{\ell^2}.
\]

Hence we have
\[
\sum_{i=0}^{2^{c-1}-1} a_i \sum_{j=0}^{2^{c-1}-1} \sum_{k=1}^{\ell-1} \binom{1}{k} (-1)^{j+k+1} \zeta^{-\tau^i(\ell j + k)} \equiv 0 \pmod{\ell}
\]
by \(\zeta^{2\ell(\tau^i-1)} = 1\). Considering the complex conjugate of the left hand side of the above congruence relation, we have the following:

**Lemma 2.1.** Let \(\alpha\) be in Proposition 2.1 and
\[
(2.2) \quad \alpha = \sum_{i=0}^{2^{c-1}-1} a_i \left( \zeta_n^{2n-c} \right)^i
\]
Weber’s class number problem

Let \( a_i \in \mathbb{Z} \). If \( \ell \) divides \( h_n / h_{n-1} \), then

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

We put

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

and define the subset \( S' \) of \( S \) by

\[
S' = \bigcup_{i=0}^{2^c-1-1} \{ r \in S \mid \zeta^{r_i-1} = \zeta^{r} \}.
\]

**Lemma 2.2.** Let \( j \) and \( k \) be rational integers with \( 0 \leq j \leq 2^c-1 \), \( 1 \leq k \leq \ell - 1 \) and \( r \in S' \). Let \( \ell \) 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 \(-2^{n-c+2} < (2^c-j)\ell - k - 1 < 2^{n-c+2} \) because of \( 0 \leq j \leq 2^c-1, 1 \leq k \leq \ell - 1 \) and \( \ell < 2^{n-2c+3} \). Since \( (2^c-j)\ell - k - 1 \equiv 0 \pmod{2^{n-c+2}} \), we have \( (2^c-j)\ell - k = 0 \). Since \( 2 \leq k+1 = (2^c-j)\ell \leq \ell \), we have \( k = \ell - 1 \) and \( j = 2^c - 1 \), which implies \( r \equiv 0 \pmod{2^{n+1}} \). Hence \( r = 0 \) or \( r = 2^{n+1} \). Since \( r \in S' \), we have \( r = 0 \). \( \square \)

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

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

where \( a_i \) is the rational integer defined by (2.2). We choose an element \( \alpha \) in \( \ell H^{-1} \) so that \( \alpha \notin \ell \mathbb{Z}[\zeta] \). Since we may assume \( a_0 \neq 0 \pmod{\ell} \), we see that \( a_i \frac{1+(-1)^{j+k}}{k} \neq 0 \pmod{\ell} \) for \( i = 0, j = 2^c - 1, k = \ell - 1 \). This contradicts Lemma 2.2 because \( \{ \zeta^i \mid 0 \leq i \leq 2^{n+1} - 1 \} \) is an integral basis of \( \mathbb{Q}(\zeta) \). \( \square \)

We follow the arguments in [5] to prove Theorem 1.2. For an algebraic number \( \alpha \), let

\[
|| \alpha || = \max_{\rho} | \alpha^\rho |,
\]

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

\[
|| \beta \beta' || \leq || \beta || \cdot || \beta' ||,
\]

\[
|| \beta^m || = || \beta ||^m
\]

for any algebraic numbers \( \beta, \beta' \) and any positive rational integer \( m \). The following is the key lemma in our proof.
Lemma 2.3. Assume that an odd prime number $\ell$ 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 $\sigma$ is a generator of $G(Q(\zeta_n)/Q(\zeta_2))$. (1) The decomposition field of $\ell$ with respect to $Q(\zeta_n)/Q$ is $Q(\zeta_3)$. Proposition 2.1 guarantees the existence of a prime ideal $\mathfrak{p}$ of $Q(\zeta_3)$ dividing $\ell$ such that $\eta^{\sigma_\ell}$ is an $\ell$-th power in $Q_n$ for each element $\alpha$ of $Q(\zeta_3)$ with $\ell\mathfrak{p}^{-1} = (\alpha)$. 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 $\alpha$. 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 $N_{Q(\zeta_3)/Q}(\alpha) = \ell^3$, 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 $\ell = (\alpha(1 + \sqrt{2})^m)$ for $m \in \mathbb{Z}$, we may assume $-1 \leq x < 1$. Hence we have $0 \leq a \leq \sqrt{2}$, which implies $a_1^2 + a_2^2 + a_3^2 \leq \sqrt{2}\ell^{3/2}$. This shows $|a_0| + |a_1| + |a_2| + |a_3| \leq 2^{5/4}\ell^{3/4}$. Noting that $\eta^{\sigma_\ell} \neq \pm 1$ (cf. [5, p. 384]), we have

\[
2^\ell < ||\eta^{\sigma_\ell}|| = ||\eta^{a_0 + a_1\sigma^2 + a_2\sigma^2 - 2n - 3 + a_3\sigma^3 - 2n - 3}||
\]

\[
\leq ||\eta||^{|a_0| + |a_1| + |a_2| + |a_3|}
\]

\[
\leq ||\eta||^{25/4\ell^{3/4}} < 2^{25/4(n+1)\ell^{3/4}}
\]

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

\[
n \leq m_\ell = 3 + \lfloor \log_2 \ell \rfloor < 3 + \log_2 \ell
\]

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

(2) In this case, the decomposition field $F$ of $\ell$ with respect to $Q(\zeta_n)/Q$ is $Q(\sqrt{-1}\sqrt{2} - \sqrt{2})$, which is contained in $Q(\zeta_4)$. Proposition 2.1 again guarantees the existence of a prime ideal $\mathfrak{p}$ of $F$ dividing $\ell$ such that $\eta^{\sigma_\ell}$ is an $\ell$-th power in $Q_n$ for each element $\alpha$ of $F$ with $\ell\mathfrak{p}^{-1} = (\alpha)$. 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 $\varphi_\ell$ of $\ell$ with respect to $Q(\zeta_4)/Q$, 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

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

We put $a = (a_0^2 + 2a_1^2 + 2a_2^2 + 2a_3^2)/\ell^{3/2}$ and $b = (2a_0a_2 - a_1^2 + 2a_1a_3 + a_2^2)/\ell^{3/2}$. Since $N_{F/Q}(\alpha) = \ell^3$, 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 $a_0^2 + 2(\sigma_1^2 + a_2^2 + a_3^2) \leq \sqrt{2}\ell^{3/2}$, which shows $|a_0| + 2(|a_1| + |a_2| + |a_3|) \leq 2^{1/4}\sqrt{\ell}\ell^{3/4}$. Hence we have

$$2^\ell < ||\eta^{a_0}||$$

$$= ||\eta^{a_0+a_1(\sigma_0^{2n-4}+\sigma_7^{2n-4})+a_3(\sigma_3^{2n-4}+\sigma_5^{2n-4})+a_2(\sigma_2^{2n-4}-\sigma_6^{2n-4})}||$$

$$\leq ||\eta||^{2(|a_0|+2(|a_1|+|a_2|+|a_3|))}$$

$$\leq ||\eta||^{2^{1/4}\sqrt{7}\ell^{3/4}} < \left(\frac{2^{n+2}}{\pi}\right)^{2^{1/4}\sqrt{7}\ell^{3/4}} < 2^{2^{1/4}\sqrt{7}(n+1)\ell^{3/4}}.$$  

In this case, Theorem 1.1 implies

$$n \leq m_\ell = 5 + \lceil \log_2 \ell \rceil < 5 + \log_2 \ell$$

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

**Proof of Theorem 1.2.** Assume that $\ell$ divides $h_n/h_{n-1}$ for some $n \geq 1$. 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 $\ell$ does not divide $h_{m_\ell}$ for all $\ell$ not exceeding a certain explicit bound. This bound on $\ell$ 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**


---

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