TOKYO J. MATH.
VOL. 39, NO. 1, 2016

A Class Number Problem for the Cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}(\sqrt{5})$

Takuya AOKI

Waseda University

(Communicated by M. Kurihara)

Abstract. Let K_n be the n-th layer of the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}(\sqrt{5})$ and h_n the class number of K_n. We prove that, if ℓ is a prime number less than $6 \cdot 10^4$, then ℓ does not divide h_n for any non-negative integer n.

1. Introduction

Let $\mathbf{B}_n$ be the n-th layer of the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$ and $h(\mathbf{B}_n)$ the class number of $\mathbf{B}_n$. Weber [8] showed that $h(\mathbf{B}_n)$ is odd for any non-negative integer n. Iwasawa [3] gave another proof in a more general situation. It is a natural question whether an odd prime number ℓ divides $h(\mathbf{B}_n)$ or not. Fukuda and Komatsu [5] showed that ℓ does not divide $h(\mathbf{B}_n)$ for any non-negative integer n if ℓ is less than 10^9.

Let ℓ be an odd prime number and 2^{c_ℓ} the exact power of 2 dividing $\ell - 1$ or $\ell^2 - 1$ according as $\ell \equiv 1 \pmod 4$ or not. For a real number x, $[x]$ denotes the greatest integer not exceeding x. Let δ_ℓ be 0 or 1 according as $\ell \equiv 1 \pmod 4$ or not. Then the following are the results of Fukuda and Komatsu [4], [5].

THEOREM 1 (Fukuda and Komatsu [4]; Theorem 1.2). *Let ℓ be an odd prime number and put*

$$m := 3c_\ell - 1 + 2[\log_2(\ell - 1)] - 2\delta_\ell .$$

If ℓ does not divide $h(\mathbf{B}_m)$, then ℓ does not divide $h(\mathbf{B}_n)$ for any non-negative integer n.

THEOREM 2 (Fukuda and Komatsu [5]; Theorem 1.1). *Let ℓ be an odd prime number and put*

$$m_0 := 2c_\ell - 1 + \left[\frac{1}{2}\log_2 \ell\right] . \tag{1}$$

Then ℓ does not divide $h(\mathbf{B}_n)/h(\mathbf{B}_{m_0})$ for any $n \geq m_0$.

In this paper, we consider the case that the base field is $\mathbf{Q}(\sqrt{5})$, and investigate the class numbers of the intermediate fields of the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}(\sqrt{5})$. The reason why

Received December 9, 2014; revised June 5, 2015

we study the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}(\sqrt{5})$ is that $\mathbf{Q}(\sqrt{5})$ has the minimal discriminant in all real quadratic fields. Our arguments in this paper can be applied to $\mathbf{Q}(\sqrt{3})$ and $\mathbf{Q}(\sqrt{6})$, but more difficulty occurs when we study quadratic fields with larger discriminant.

We put $K = \mathbf{Q}(\sqrt{5})$ and $K_n = K \cdot \mathbf{B}_n$. Then K_n is the n-th layer of the cyclotomic $\mathbf{Z}_2$-extension of K. We denote by h_n the class number of K_n. It is well known that $h_0 = h_1 = 1$. Applying the result of Iwasawa [3], we obtain the fact that h_n is odd for any non-negative integer n. So we are interested in whether an odd prime number ℓ divides h_n or not. We have the following result.

THEOREM 3. *Let ℓ be an odd prime. Put*

$$m_\ell := \begin{cases} 2c_\ell + [\log_2(5\ell - 1)] - \delta_\ell - 2 & \textit{if } \ell \neq 5\,, \\ 4 & \textit{if } \ell = 5\,. \end{cases}$$

Then ℓ does not divide h_n / h_{m_ℓ} for any $n \geq m_\ell$.

We remark that $m_\ell \geq m_0$ for each odd prime number ℓ. In particular, $m_\ell = m_0 = 4$ for $\ell = 5$. We prove Theorem 3 in Section 2. As a corollary of Theorem 3, we obtain the following result.

COROLLARY 1. *If ℓ is a prime number less than $6 \cdot 10^4$, then ℓ does not divide h_n for any non-negative integer n.*

2. Proof of Theorem 3

Let n be a non-negative integer, ℓ an odd prime number, $\overline{\mathbf{Q}}_\ell$ the algebraic closure of the ℓ-adic number field $\mathbf{Q}_\ell$, v_ℓ the additive ℓ-adic valuation normalized by $v_\ell(\ell) = 1$ and ζ_ℓ a primitive ℓ-th root of unity in $\mathbf{C}$. We put $K'_n = K_n(\zeta_\ell)$. Let A_n and A'_n be the ℓ-Sylow subgroup of the ideal class group of K_n and K'_n, respectively. We abbreviate c_ℓ as c.

Let Γ_n be the Galois group of $\mathbf{B}_n/\mathbf{Q}$, G_n the Galois group of $K_n/\mathbf{Q}$ and G'_n the Galois group of $K'_n/\mathbf{Q}$. We denote by $\widehat{G_n}$ and $\widehat{G'_n}$ the character group of G_n and G'_n, respectively. We also denote by ψ_n an even character mod 2^{n+2} whose order is 2^n. Then ψ_n generates the character group of Γ_n.

For all $\psi \in \widehat{G'_n}$, we define the idempotent $e_\psi \in \mathbf{Z}_\ell[G'_n]$ by

$$e_\psi := \frac{1}{|G'_n|} \sum_{\sigma \in G'_n} \mathrm{Tr}(\psi^{-1}(\sigma))\sigma\,, \tag{2}$$

where Tr is the trace mapping from $\mathbf{Q}_\ell(\psi(G'_n))$ to $\mathbf{Q}_\ell$. Then e_ψ can act on A'_n. We call $A'_{n,\psi} = e_\psi A'_n$ the ψ-part of A'_n.

Let Δ_ℓ be the Galois group of $\mathbf{Q}(\zeta_\ell)/\mathbf{Q}$. Then we have $\Delta_\ell \cong \mathbf{Z}/(\ell - 1)\mathbf{Z}$ and

$$G'_n \cong \begin{cases} G_n \times \Delta_\ell & \text{if } \ell \neq 5\,, \\ \Gamma_n \times \Delta_\ell & \text{if } \ell = 5 \end{cases}$$

for all non-negative integer n. We denote by $\omega_\ell : \Delta_\ell \to \mathbf{Q}_\ell^\times$ the character such that $\zeta_\ell^{\omega_\ell(\delta)} = \zeta_\ell^\delta$ for all $\delta \in \Delta_\ell$. Then ω_5^2 generates the character group of $\mathrm{Gal}(K/\mathbf{Q})$.

If $\psi \in \widehat{G'_n}$ is odd, then the following equality holds by [6].

$$v_\ell(|A'_{n,\psi}|) = (\mathbf{Z}_\ell[\psi(G'_n)] : \mathbf{Z}_\ell)v_\ell(B_{1,\psi^{-1}}),$$

where $B_{1,\psi}$ is the generalized Bernoulli number defined by

$$B_{1,\psi} = \frac{1}{5\ell \cdot 2^{n+2}} \sum_{b=1}^{5\ell \cdot 2^{n+2}} \psi(b)b$$

for all $\psi \in \widehat{G'_n}$. We also define idempotents e_i $(0 \le i \le \ell - 2)$ in $\mathbf{Z}_\ell[\Delta_\ell]$ by

$$e_i := \frac{1}{\ell - 1} \sum_{\delta \in \Delta_\ell} \omega_\ell^{-i}(\delta)\delta .$$

Since

$$\Delta_\ell \cong \begin{cases} \mathrm{Gal}(K'_n/K_n) & \text{if } \ell \neq 5, \\ \mathrm{Gal}(K'_n/\mathbf{B}_n) & \text{if } \ell = 5 \end{cases}$$

canonically, we can act e_i on A'_n. We abbreviate ω_5 as ω. Then we have the following by [2].

LEMMA 1. *Let n be a positive integer.*
(i) *For $\ell \neq 5$, we have*

$$v_\ell(|e_1 A'_n|) - v_\ell(|e_1 A'_{n-1}|) = \sum_{j=1:odd}^{2^n-1} \left(v_\ell(B_{1,\omega_\ell^{-1}\psi_n^{-j}}) + v_\ell(B_{1,\omega_\ell^{-1}\omega^{-2}\psi_n^{-j}}) \right) .$$

(ii) *For $\ell = 5$, we have*

$$v_5(|e_3 A'_n|) - v_5(|e_3 A'_{n-1}|) = \sum_{j=1:odd}^{2^n-1} v_5(B_{1,\omega^{-3}\psi_n^{-j}}) .$$

First, let $\ell \neq 5$. We have the following by [4]; pp. 219–221.

LEMMA 2. *If $n \ge m_0 + 1$, we have $v_\ell(B_{1,\omega_\ell^{-1}\psi_n^{-j}}) = 0$ for all odd integer j with $1 \le j \le 2^n - 1$.*

Since $m_\ell \ge m_0$, Lemma 2 implies that $v_\ell(B_{1,\omega_\ell^{-1}\psi_n^{-j}}) = 0$ for any $n \ge m_\ell + 1$ and any odd integer j with $1 \le j \le 2^n - 1$. Thus we study $B_{1,\omega_\ell^{-1}\omega^{-2}\psi_n^{-j}}$. For $B_{1,\omega_\ell^{-1}\omega^{-2}\psi_n^{-j}}$, we define

$f_1(T) \in \mathbf{Q}_\ell(T)$ by

$$f_1(T) = \left(\sum_{\substack{b \equiv 1 \pmod{2^c} \\ 0<b<5\ell\cdot 2^{c+1}}} \omega_\ell^{-1}\omega^{-2}(b)T^b \right) \left(T^{5\ell\cdot 2^{c+1}} - 1\right)^{-1} . \tag{3}$$

Then we have the following by [7]; pp. 386–387.

LEMMA 3. *Let $n \geq 2c-1$. If $f_1(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any primitive 2^{n+2}-th root of unity η in $\overline{\mathbf{Q}}_\ell$, then $B_{1,\omega_\ell^{-1}\omega^{-2}\psi_n^{-j}} \not\equiv 0 \pmod{\overline{\ell}}$ for any odd integer j, where $\overline{\ell}$ is the ideal of $\mathbf{Z}_\ell[\eta]$ generated by ℓ.*

LEMMA 4. *If $n \geq m_\ell + 1$, then $f_1(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any primitive 2^{n+2}-th root of unity η in $\overline{\mathbf{Q}}_\ell$.*

PROOF. We put

$$g(T) = f_1(T)(T^{5\ell\cdot 2^c} - 1)T^{-1} . \tag{4}$$

For convenience, we put $\chi = \omega_\ell\omega^2$. Since $\chi^{-1}(j) = \chi^{-1}(j+5\ell)$ for any integer j, we have

$$\begin{aligned}
g(T) &= \sum_{\substack{b \equiv 1 \pmod{2^c} \\ 0<b<5\ell\cdot 2^{c+1}}} \chi^{-1}(b)T^bT^{-1}(T^{5\ell\cdot 2^c}+1)^{-1} \\
&= (T^{5\ell\cdot 2^c}+1)^{-1}\Big(\chi^{-1}(1) + \cdots + \chi^{-1}(1+(5\ell-1)2^c)T^{(5\ell-1)2^c} \\
&\quad + \chi^{-1}(1+5\ell\cdot 2^c)T^{5\ell\cdot 2^c} + \cdots + \chi^{-1}(1+(5\ell-1)2^c+5\ell\cdot 2^c)T^{(5\ell-1)2^c+5\ell\cdot 2^c}\Big) \\
&= (T^{5\ell\cdot 2^c}+1)^{-1}\Big(\chi^{-1}(1)(1+T^{5\ell\cdot 2^c}) + \dots \\
&\quad + \chi^{-1}(1+(5\ell-1)2^c)T^{(5\ell-1)2^c}(1+T^{5\ell\cdot 2^c})\Big) \\
&= \sum_{\substack{b \equiv 1 \pmod{2^c} \\ 0<b\leq 1+(5\ell-1)\cdot 2^c}} \chi^{-1}(b)T^{b-1} \in \mathbf{Z}_\ell[T] .
\end{aligned}$$

We denote by $\deg(g)$ the degree of $g(T)$. For all $n \geq m_\ell + 1$ and any primitive 2^{n+2}-th root of unity η in $\overline{\mathbf{Q}}_\ell$, we have

$$\begin{aligned}[\mathbf{Q}_\ell(\eta):\mathbf{Q}_\ell] &= 2^{n+2-c+\delta_\ell} \\ &\geq 2^{c+[\log_2(5\ell-1)]+1} \\ &> 2^c(5\ell-1) \geq \deg(g)\,.\end{aligned}$$

Hence we have $g(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any primitive 2^{n+2}-th root of unity η in $\overline{\mathbf{Q}}_\ell$. Thus we have $f_1(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any η. □

Lemmas 3 and 4 allow us to obtain the following.

LEMMA 5. *If $n \geq m_\ell + 1$, then we have $v_\ell(B_{1,\omega_\ell^{-1}\omega^{-2}\psi_n^{-j}}) = 0$ for all odd integer j with $0 \leq j \leq 2^n - 1$.*

Next, let $\ell = 5$. For $B_{1,\omega^{-3}\psi_n^{-j}}$, we define $f_1(T)$ and $g(T)$ by replacing ω^{-3} with $\omega_\ell^{-1}\omega^{-2}$ and ℓ with 5ℓ in (3) and (4). Then we have the following by [7]; pp. 386–387.

LEMMA 6. *Let $n \geq 2c - 1$. If $f_1(\eta) \not\equiv 0 \pmod{\overline{\ell}}$ for any primitive 2^{n+2}-th root of unity η in $\overline{\mathbf{Q}}_5$, then $B_{1,\omega^{-3}\psi_n^{-j}} \not\equiv 0 \pmod{\overline{\ell}}$ for any odd integer j, where $\overline{\ell}$ is the ideal of $\mathbf{Z}_\ell[\eta]$ generated by 5.*

For $\ell = 5$, we put $d = 2c + [\log_2(\ell-1)] - \delta_\ell - 2 = 4 = m_\ell$. Then we obtain the following by a similar argument in the proof of Lemma 4.

LEMMA 7. *If $n \geq m_\ell + 1$, then we have $v_5(B_{1,\omega^{-3}\psi_n^{-j}}) = 0$ for all odd integer j with $1 \leq j \leq 2^n - 1$.*

Lemmas 1, 2, 5 and 7 allow us to obtain the following lemma.

LEMMA 8. *For all $n \geq m_\ell + 1$, we have*

$$\begin{cases} |e_1 A'_n| = |e_1 A'_{n-1}| & \text{if } \ell \neq 5\,, \\ |e_3 A'_n| = |e_3 A'_{n-1}| & \text{if } \ell = 5\,. \end{cases}$$

Now we prove Theorem 3. Since natural mappings $A_{n-1} \to A_n$ and $A'_{n-1} \to A'_n$ are injective by [7]; Lemma 16.15, we can regard A'_{n-1} as G'_n-submodule of A'_n. Let D_n and D'_n be the kernels of the norm mappings $A_n \to A_{n-1}$ and $A'_n \to A'_{n-1}$, respectively. Then we have $A_n = A_{n-1} \oplus D_n$ and $A'_n = A'_{n-1} \oplus D'_n$ by [7]; Lemma 16.15. Let L'_n be the maximal unramified elementary abelian ℓ-extension of K'_n. Note that $L'_n/\mathbf{Q}$ is a Galois extension since $K'_n/\mathbf{Q}$ is a Galois extension. Since $\mathrm{Gal}(L'_n/K'_n)$ is a normal abelian subgroup of $\mathrm{Gal}(L'_n/\mathbf{Q})$, G'_n can act on $\mathrm{Gal}(L'_n/K'_n)$. Therefore, $\mathrm{Gal}(L'_n/K'_n)$ is isomorphic to $A'_n/\ell A'_n$ as G'_n-module by the Artin mapping. By class field theory, we have $\mathrm{Gal}(L'_n/L'_{n-1}K'_n) \cong D'_n/\ell D'_n$. Since

$$\mathrm{Gal}(L'_n/K'_n) \cong A'_n/\ell A'_n \cong A'_{n-1}/\ell A'_{n-1} \oplus D'_n/\ell D'_n\,,$$

there exists an intermediate field M'_n of L'_n/K'_n such that $\mathrm{Gal}(L'_n/M'_n) \cong A'_{n-1}/\ell A'_{n-1}$ by the Artin mapping. Note that D'_n is a G'_n-submodule of A'_n. Then we have the following;

$$\begin{aligned}
&L'_n = M'_n L'_{n-1}\,,\\
&L'_{n-1}K'_n \cap M'_n = K'_n\,,\\
&\mathrm{Gal}(M'_n/K'_n) \cong D'_n/\ell D'_n\,,\\
&M'_n/\mathbf{Q} \ \text{ is a Galois extension.}
\end{aligned}$$

Since $\zeta_\ell \in K'_n$, M'_n/K'_n is a Kummer extension. Hence there exists a subgroup V of $K'^{\times}_n/(K'^{\times}_n)^\ell$ such that $M'_n = K'_n(\sqrt[\ell]{V})$ in the obvious notation. Let W be the subgroup in $\mathbf{C}^\times$ generated by ζ_ℓ. Then there is a non-degenerate pairing

$$\mathrm{Gal}(M'_n/K'_n) \times V \to W;\, (h, \tilde{b}) \mapsto \langle h, \tilde{b}\rangle\,,$$

which is defined by

$$\langle h, \tilde{b}\rangle = \frac{h(\sqrt[\ell]{b})}{\sqrt[\ell]{b}} \quad \text{for all } h \in \mathrm{Gal}(M'_n/K'_n) \text{ and } \tilde{b} = b(K'^{\times}_n)^\ell$$

and satisfies $\langle h^g, \tilde{b}^g\rangle = \langle h, \tilde{b}\rangle^g$ for all $g \in G'_n$. Then the reflection theorem says $e_j V \cong e_i \mathrm{Gal}(M'_n/K'_n)$ for i, j with $i + j \equiv 1 \pmod{\ell - 1}$. For $\ell \neq 5$, we have

$$e_1 V \cong e_0 \mathrm{Gal}(M'_n/K'_n) \cong D_n/\ell D_n \cong (A_n/A_{n-1})/\ell(A_n/A_{n-1})\,.$$

For $\ell = 5$, noting that the 5-Sylow subgroup of the ideal class group of $\mathbf{B}_n$ is trivial for each non-negative integer n by [4], we have the following;

$$e_3 V \cong e_2 \mathrm{Gal}(M'_n/K'_n) \cong D_n/5D_n \cong (A_n/A_{n-1})/5(A_n/A_{n-1})\,.$$

We can prove the following in a similar method to prove [5]; Proposition 2.2.

LEMMA 9. (i) *Let* $\ell \neq 5$. *If* $e_1(A'_n/A'_{n-1}) = 0$, *then* $A_n = A_{n-1}$.
(ii) *Let* $\ell = 5$. *If* $e_3(A'_n/A'_{n-1}) = 0$, *then* $A_n = A_{n-1}$.

We assume that $n \geq m_\ell + 1$. Then Lemma 8 says that $|e_k A'_n| = |e_k A'_{n-1}| = \cdots = |e_k A'_{m_\ell}|$, where k is 3 or 1 according as $\ell = 5$ or not. Hence we have $|A_n| = |A_{n-1}| = \cdots = |A_{m_\ell}|$ by Lemma 9. Therefore ℓ does not divide h_n/h_{m_ℓ}. □

3. Calculation

In this section, we explain how to verify Corollary 1 numerically. We use notations defined in Section 2 and assume $\ell < 10^9$. For all $\chi \in \widehat{G_n}$, we define the idempotent e_χ by replacing G_n with G'_n in (2). The χ-part $A_{n,\chi}$ of A_n is also defined by $A_{n,\chi} = e_\chi A_n$. Then we have $A_n = \oplus_{\chi'} A_{n,\chi'}$, where χ' runs over all representatives of $\mathbf{Q}_\ell$-conjugacy classes of $\widehat{G_n}$.

For non-negative integer n, let $\zeta_{5\cdot 2^{n+2}}$ be a primitive $5 \cdot 2^{n+2}$-th root of unity in $\mathbf{C}$. We put $\zeta_{2^{n+2}} = \zeta_{5\cdot 2^{n+2}}^5$ and $\zeta_5 = \zeta_{5\cdot 2^{n+2}}^{2^{n+2}}$. We also put

$$\xi_n = (\zeta_5\zeta_{2^{n+2}} - 1)(\zeta_5\zeta_{2^{n+2}}^{-1} - 1)(\zeta_5^{-1}\zeta_{2^{n+2}} - 1)(\zeta_5^{-1}\zeta_{2^{n+2}}^{-1} - 1) \in K_n\,.$$

We define a truncation $e_{\chi,\ell} \in \mathbf{Z}[G_n]$ of e_χ by

$$e_{\chi,\ell} \equiv e_\chi \pmod{\ell}\,.$$

Then we can act $e_{\chi,\ell}$ on ξ_n. The following is the special case of [1]; Lemma 1.

LEMMA 10. *If there exists a prime number p congruent to* 1 *modulo* $5\ell \cdot 2^{n+2}$ *and satisfies*

$$(\xi_n^{e_{\chi,\ell}})^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{\mathfrak{p}} \tag{5}$$

for some prime ideal $\mathfrak{p}$ of K_n lying above p, then we have $|A_{n,\chi}| = 1$.

Let $s = c - \delta_\ell$. Then 2^s is the exact power of 2 dividing $\ell - 1$ or $\ell + 1$ according as $\ell \equiv 1 \pmod 4$ or not.

Owing to Lemma 10, we may regard χ as a character of G_n into $\overline{\mathbf{F}}_\ell$, where $\overline{\mathbf{F}}_\ell$ is the algebraic closure of $\mathbf{F}_\ell = \mathbf{Z}/\ell\mathbf{Z}$. Let η_n be a primitive 2^n-th root of unity in $\overline{\mathbf{F}}_\ell$ and $L = \mathbf{F}_\ell(\eta_n)$. We may also define e_χ to be an element of $\mathbf{F}_\ell[G_n]$. Let ρ be the generator of Γ_n induced by $\zeta_{2^{n+2}} \mapsto \zeta_{2^{n+2}}^5$, σ the generator of $\mathrm{Gal}(K/\mathbf{Q})$ induced by $\zeta_5 \mapsto \zeta_5^2$ and ψ the character of Γ_n defined by $\psi(\rho) = \eta_n^{-1}$. We put $F_n = K_{n+1}^{\mathrm{Ker}\omega^2\psi}$ and $H_n = \mathrm{Gal}(F_n/\mathbf{Q})$. We define $X \subset \mathbf{Z}$ to make $\{\psi^j \mid j \in X\}$ be a set of representatives of injective characters of Γ_n. Then $\{\omega^2\psi^j \mid j \in X\}$ is a set of representatives of injective characters of H_n and we have

$$A_n = A_{n-1} \oplus \bigoplus_{j\in X} A_{n,\psi^j} \oplus \bigoplus_{j\in X} A_{n,\omega^2\psi^j}\,.$$

Note that $A_{n,\chi} \cong A_\chi$, where A_χ is the χ-part of the ℓ-Sylow subgroup of the ideal class group of the subfield of K_n corresponding to $\mathrm{Ker}\chi$. Hence for each $j \in X$, we have $|A_{n,\psi^j}| = 1$ if $\ell < 10^9$ by [5]. By induction, we may assume that $\chi = \omega^2\psi^j$ with $j \in X$. Then we have

$$e_{\omega^2\psi^j} = \frac{1}{2^{n+1}} \sum_{i=0}^{2^n-1} \mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_n^{ij}) \left(\rho^i - \sigma\rho^i\right)\,.$$

Now, let p be a prime number satisfying $p \equiv 1 \pmod{5\ell \cdot 2^{n+2}}$ and g_p a primitive root modulo p. Since p is totally decomposed in $\mathbf{Q}(\zeta_{5\cdot 2^{n+2}})/\mathbf{Q}$, there exists a prime ideal $\mathfrak{P}$ in $\mathbf{Q}(\zeta_{5\cdot 2^{n+2}})$ lying above p which satisfies

$$\zeta_{5\cdot 2^{n+2}} \equiv g_p^{\frac{p-1}{5\cdot 2^{n+2}}} \pmod{\mathfrak{P}}\,.$$

We put $e_{\omega^2\psi^j,\ell} = \sum_{i=0}^{2^n-1} \alpha_{ij}(\rho^i - \sigma\rho^i)$ and fix non-negative integers z_1, z_2, z_3, z_4 satisfying

$$\begin{aligned} z_1 &\equiv g_p^{\frac{p-1}{5}} \pmod p\,, \\ z_2 z_1 &\equiv 1 \pmod p\,, \\ z_3 &\equiv g_p^{\frac{p-1}{2^{n+2}}} \pmod p\,, \\ z_4 z_3 &\equiv 1 \pmod p\,. \end{aligned}$$

Then we have

$$\begin{aligned} \xi_n^{e_{\omega^2\psi^j,\ell}} &= \prod_{i=0}^{2^n-1} \left(\frac{(\zeta_5\zeta_{2^{n+2}}^{5^i}-1)(\zeta_5\zeta_{2^{n+2}}^{-5^i}-1)(\zeta_5^{-1}\zeta_{2^{n+2}}^{5^i}-1)(\zeta_5^{-1}\zeta_{2^{n+2}}^{-5^i}-1)}{(\zeta_5^2\zeta_{2^{n+2}}^{5^i}-1)(\zeta_5^2\zeta_{2^{n+2}}^{-5^i}-1)(\zeta_5^{-2}\zeta_{2^{n+2}}^{5^i}-1)(\zeta_5^{-2}\zeta_{2^{n+2}}^{-5^i}-1)} \right)^{\alpha_{ij}} \\ &\equiv \prod_{i=0}^{2^n-1} \left(\frac{(z_1 z_3^{5^i}-1)(z_1 z_4^{5^i}-1)(z_2 z_3^{5^i}-1)(z_2 z_4^{5^i}-1)}{(z_1^2 z_3^{5^i}-1)(z_1^2 z_4^{5^i}-1)(z_2^2 z_3^{5^i}-1)(z_2^2 z_4^{5^i}-1)} \right)^{\alpha_{ij}} \pmod{\mathfrak{p}} \end{aligned}$$

with $\mathfrak{p} = \mathfrak{P} \cap K_n$. For convenience, we fix $\zeta(b^i) \in \mathbf{Z}$ satisfying $0 \le \zeta(b^i) \le p-1$ and

$$\zeta(b^i) \equiv \frac{(z_1 z_3^{b^i}-1)(z_1 z_4^{b^i}-1)(z_2 z_3^{b^i}-1)(z_2 z_4^{b^i}-1)}{(z_1^2 z_3^{b^i}-1)(z_1^2 z_4^{b^i}-1)(z_2^2 z_3^{b^i}-1)(z_2^2 z_4^{b^i}-1)} \pmod p$$

for each integer $b \ge 1$ and $i \ge 0$. Since $h_1 = 1$, we may assume that $n \ge 2$.

3.1. The case $\ell \equiv 1 \pmod 4$ and $2 \le n \le s$. In this case, we have $L = \mathbf{F}_\ell$. Hence $\mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_n) = \eta_n$. Since the choice of η_n is arbitrary, we may assume that

$$\eta_n \equiv g_\ell^{\frac{\ell-1}{2^n}} \pmod \ell\,,$$

where g_ℓ is a primitive root modulo ℓ. Since there are 2^{n-1} non-conjugate primitive 2^n-th roots of unity in $\overline{\mathbf{F}}_\ell$, there are also 2^{n-1} $\mathbf{F}_\ell$-conjugacy classes of injective characters of H_n. We put

$$X = \{j \in \mathbf{Z} | 1 \le j \le 2^n - 1,\ j \text{ is odd}\}\,.$$

Then $\{\omega^2\psi^j | j \in X\}$ is a set of representatives of the $\mathbf{F}_\ell$-conjugacy classes of injective characters of H_n. We fix non-negative integers a_{ij}'s by

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{2^n}ij} \pmod \ell$$

for each $0 \le i \le 2^n - 1$ and $j \in X$. Then we have the following criterion.

CRITERION 1. If for each $j \in X$, there exists a prime number p congruent to 1 modulo

$5\ell \cdot 2^{n+2}$ satisfying

$$\left(\prod_{i=0}^{2^n-1} \zeta(5^i)^{a_{ij}}\right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p},$$

then ℓ does not divide h_n/h_{n-1}.

3.2. The case $\ell \equiv 1 \pmod 4$ and $s+1 \le n$. In this case, we have $[L : \mathbf{F}_\ell] = 2^{n-s}$. The minimal polynomial of η_n over $\mathbf{F}_\ell$ is

$$T^{2^{n-s}} - \eta_n^{2^{n-s}}.$$

Therefore, if 2^{n-s} does not divide i, then $\mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_n^i) = 0$. So we have

$$\begin{aligned} e_{\omega^2\psi^j} &= \frac{1}{2^{n+1}} \sum_{i=0}^{2^s-1} \mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_n^{2^{n-s}ij}) \left(\rho^{2^{n-s}i} - \sigma\rho^{2^{n-s}i}\right) \\ &= \frac{1}{2^{n+1}} \sum_{i=0}^{2^s-1} \mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_s^{ij}) \left(\rho^{2^{n-s}i} - \sigma\rho^{2^{n-s}i}\right) \\ &= \frac{1}{2^{s+1}} \sum_{i=0}^{2^s-1} \eta_s^{ij} \left(\rho^{2^{n-s}i} - \sigma\rho^{2^{n-s}i}\right). \end{aligned}$$

Since there are 2^{s-1} non-conjugate primitive 2^n-th roots of unity in $\overline{\mathbf{F}}_\ell$, there are also 2^{s-1} $\mathbf{F}_\ell$-conjugacy classes of injective characters of H_n. We put

$$X = \{j \in \mathbf{Z} | 1 \le j \le 2^s - 1, j \text{ is odd}\}.$$

Then $\{\omega^2\psi^j | j \in X\}$ is a set of representatives of the $\mathbf{F}_\ell$-conjugacy classes of injective characters of H_n. We fix non-negative integers a_{ij}'s satisfying

$$a_{ij} \equiv g_\ell^{\frac{p-1}{2^s}ij} \pmod{\ell}$$

for each $0 \le i \le 2^s - 1$ and $j \in X$. Then we have the following criterion.

CRITERION 2. If for each $j \in X$, there exists a prime number p congruent to 1 modulo $5\ell \cdot 2^{n+2}$ satisfying

$$\left(\prod_{i=0}^{2^s-1} \zeta(5^{2^{n-s}i})^{a_{ij}}\right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p},$$

then ℓ does not divide h_n/h_{n-1}.

3.3. The case $\ell \equiv 3 \pmod 4$ and $2 \leq n \leq s$. In this case, we have $[L : \mathbf{F}_\ell] = 2$. Hence we obtain

$$\mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_n) = \eta_n + \eta_n^\ell .$$

Since there are 2^{n-2} non-conjugate primitive 2^n-th roots of unity in $\overline{\mathbf{F}}_\ell$, there are also 2^{n-2} $\mathbf{F}_\ell$-conjugacy classes of injective characters of H_n. We put

$$X = \{j \in \mathbf{Z} | 1 \leq j \leq 2^{n-1} - 1, j \text{ is odd}\} .$$

Then $\{\omega^2\psi^j | j \in X\}$ is a set of representatives of the $\mathbf{F}_\ell$-conjugacy classes of injective characters of H_n. We fix non-negative integers a_{ij}'s satisfying

$$a_{ij} \equiv t_{2^{s+1-n}ij} \pmod \ell$$

for each $0 \leq i \leq 2^n - 1$ and $j \in X$, where t_i's are elements in $\mathbf{F}_\ell$ defined in (6) in subsection 3.4. Then we have the following criterion.

CRITERION 3. If for each $j \in X$, there exists a prime number p congruent to 1 modulo $5\ell \cdot 2^{n+2}$ satisfying

$$\left(\prod_{i=0}^{2^n-1} \zeta(5^i)^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod p ,$$

then ℓ does not divide h_n/h_{n-1}.

3.4. The case $\ell \equiv 3 \pmod 4$ and $s + 1 \leq n$. In this case, we have $[L : \mathbf{F}_\ell] = 2^{n-s}$. Let

$$T^2 - aT - 1$$

be the minimal polynomial of η_{s+1} over $\mathbf{F}_\ell$. Then the minimal polynomial of η_n over $\mathbf{F}_\ell$ is

$$T^{2^{n-s}} - aT^{2^{n-s-1}} - 1 .$$

Thus if 2^{n-s-1} does not divide i, then $\mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_n^i) = 0$. Therefore, we have

$$\begin{aligned}
e_{\omega^2\psi^j} &= \frac{1}{2^{n+1}} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_n^{2^{n-s-1}ij}) \left(\rho^{2^{n-s-1}i} - \sigma\rho^{2^{n-s-1}i}\right) \\
&= \frac{1}{2^{n+1}} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{L/\mathbf{F}_\ell}(\eta_{s+1}^{ij}) \left(\rho^{2^{n-s-1}i} - \sigma\rho^{2^{n-s-1}i}\right) \\
&= \frac{1}{2^{s+2}} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{\mathbf{F}_\ell(\eta_{s+1})/\mathbf{F}_\ell}(\eta_{s+1}^{ij}) \left(\rho^{2^{n-s-1}i} - \sigma\rho^{2^{n-s-1}i}\right) .
\end{aligned}$$

We put

$$t_i = \mathrm{Tr}_{\mathbf{F}_\ell(\eta_{s+1})/\mathbf{F}_\ell}(\eta_{s+1}^i) \,. \tag{6}$$

We need to calculate t_i's. But the calculation of them is done in [4].

LEMMA 11 (Fukuda and Komatsu [4]; Lemma 3.3). *Put $a_2 = 0 \in \mathbf{F}_\ell$ and define $a_i \in \mathbf{F}_\ell$ for all $3 \le i \le s+1$ by the recursive formula*

$$a_i = \sqrt{2 + a_{i-1}} \quad (3 \le i \le s)\,,$$
$$a_{s+1} = \sqrt{-2 + a_s}\,.$$

Then we have $t_1 = a_{s+1}$.

We remark that for each step, we have two square roots. So we have just 2^{s-1} instances of t_1. Since they correspond to the 2^{s-1} non-conjugate primitive 2^{s+1}-th roots of unity in $\overline{\mathbf{F}}_\ell$, we fix an arbitrary one.

LEMMA 12 (Fukuda and Komatsu [4]; Lemma 3.6). *We have $t_{i+2} = t_1 t_{i+1} + t_i$ for all $i \ge 0$.*

Since there are 2^{s-1} non-conjugate primitive 2^n-th roots of unity in $\overline{\mathbf{F}}_\ell$, there are also 2^{s-1} $\mathbf{F}_\ell$-conjugacy classes of injective characters of H_n. We put

$$X = \{j \in \mathbf{Z} : \text{odd} | 1 \le j \le 2^{s-1} \text{ or } 2^s + 1 \le j \le 2^s + 2^{s-1} - 1\}\,.$$

Then $\{\omega^2\psi^j | j \in X\}$ is a set of representatives of the $\mathbf{F}_\ell$-conjugacy classes of injective characters of H_n. We fix non-negative integers a_{ij}'s satisfying

$$a_{ij} \equiv t_{ij} \pmod{\ell}$$

for each $0 \le i \le 2^{s+1} - 1$ and $j \in X$. Then we have the following criterion.

CRITERION 4. If for each $j \in X$, there exists a prime number p congruent to 1 modulo $5\ell \cdot 2^{n+2}$ satisfying

$$\left(\prod_{i=0}^{2^{s+1}-1} \zeta(5^{2^{n-s-1}i})^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p}\,,$$

then ℓ does not divide h_n/h_{n-1}.

3.5. The Logarithmic Algorithm. It takes too much time to verify that an odd prime number ℓ with large s does not divide h_{m_ℓ} with the previous criteria. For example, it takes more than 3 weeks on a computer with Mathematica 9 to verify that $6143 = 3 \cdot 2^{11} - 1$ does not divide h_{35}.

To obtain Corollary 1, we need to verify that $8191 = 2^{13} - 1$ does not divide h_{40}. Thus we are led to a logarithmic version of the previous criteria.

For $x \in \mathbf{F}_p^\times$, let $\nu_p(x)$ be the unique non-negative integer less than p satisfying

$$x = g_p^{\nu_p(x)} .$$

The calculation of $\nu_p(x)$ is considered hard for large p. But $\nu_p(x)$ modulo ℓ is enough for our purpose. Let $\nu_p(x) = i + j\ell$ with $0 \le i < \ell$. Then we can determine i by

$$x^{\frac{p-1}{\ell}} = \left(g_p^{i+j\ell}\right)^{\frac{p-1}{\ell}} = \left(g_p^{\frac{p-1}{\ell}}\right)^i .$$

Hence we can fix $x_i \in \mathbf{Z}$ satisfying $0 \le x_i < \ell$ and

$$x_i \equiv \nu_p(\zeta(b^i)) \pmod{\ell} ,$$

where b is defined by

$$b = \begin{cases} 5 & \text{if } 2 \le n \le s , \\ 5^{2^{n-c}} & \text{if } s+1 \le n . \end{cases}$$

We also put r by

$$r = \begin{cases} n & \text{if } 2 \le n \le s , \\ c & \text{if } s+1 \le n . \end{cases}$$

Then Criteria 1 through 4 shift to the following form.

CRITERION 5. If for each $j \in X$, there exists a prime number p congruent to 1 modulo $5\ell \cdot 2^{n+2}$ satisfying

$$\sum_{i=0}^{2^r-1} a_{ij} x_i \not\equiv 0 \pmod{\ell} ,$$

then ℓ does not divide h_n/h_{n-1}.

Criterion 5 allows us to verify that $8191 = 2^{13} - 1$ does not divide h_n for any non-negative integer n in two days. Moreover, we can verify that, if $10^4 < \ell < 6 \cdot 10^4$, then ℓ does not divide h_n for any non-negative integer n with this criterion.

References

[1] M. AOKI and T. FUKUDA, *An Algorithm for Computing p-Class Groups of Abelian Number Fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., 4076, Springer, Berlin, 2006, 56–71.

[2] G. GRAS, Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, Ann. Inst. Fourier **27**-1 (1977), 1–66.

[3] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

[4] T. FUKUDA and K. KOMATSU, Weber's class number problem in the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$, Experiment. Math. **18**(2) (2009), 213–222.

[5] T. FUKUDA and K. KOMATSU, Weber's class number problem in the cyclotomic $\mathbf{Z}_2$-extension of $\mathbf{Q}$, III, International Journal of Number Theory Vol. 7, No. 6 (2011), 1627–1635.

[6] B. MAZUR and A. WILES, Class fields of abelian extension of $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[7] L. C. WASHINGTON, *Introduction to cyclotomic fields, 2nd ed.*, Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.

[8] H. WEBER, Theorie der Abel'schen Zahlkörper, Acta Math. **8** (1886), 193–263.

Present Address:
DEPARTMENT OF MATHEMATICS, SCHOOL OF FUNDAMENTAL SCIENCE AND ENGINEERING,
WASEDA UNIVERSITY,
3–4–1 OKUBO, SHINJUKU-KU, TOKYO 169–8555, JAPAN.
e-mail: takuya4869aoki@toki.waseda.jp