Weber's Class Number Problem in the Cyclotomic $\mathbb{Z}_2$-Extension of $\mathbb{Q}$

Takashi Fukuda and Keiichi Komatsu

CONTENTS

2000 AMS Subject Classification: 11G15, 11R27, 11Y40

Keywords: Class number, computation

Let h_n denote the class number of $\mathbb{Q}(2\cos(2\pi/2^{n+2}))$. Weber proved that h_n is odd for all $n \geq 1$. We claim that if ℓ is a prime number less than 10^7, then for all $n \geq 1$, ℓ does not divide h_n.

1. INTRODUCTION

Let $\Omega_n = \mathbb{Q}(2\cos(2\pi/2^{n+2}))$. Then Ω_n, the nth layer of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$, is a cyclic extension of $\mathbb{Q}$ of degree 2^n. Let h_n denote the class number of Ω_n. More than one hundred years ago, Weber [Weber 86] proved that h_n is odd for all $n \geq 1$. Later, Iwasawa [Iwasawa 56] gave another beautiful proof in a more general situation.

We are led to investigate the odd part of h_n, or the whole class number h_n. It is very hard to compute h_n. It was shown that $h_1 = h_2 = h_3 = 1$ by Weber; $h_4 = 1$ by Cohn [Cohn 60], Bauer [Bauer 69], and Masley [Masley 78]; and $h_5 = 1$ by van der Linden [Linden 82]. Van der Linden also showed that $h_6 = 1$ if the generalized Riemann hypothesis (GRH) is valid.

On the other hand, concerning the odd part of h_n, there are Washington's results [Washington 75], which claim that the ℓ-part of h_n is bounded as n tends to ∞ for a fixed prime number ℓ. Precisely, he gave explicitly a bound on n for which the growth of e_n stops, where $h_n = \ell^{e_n} q$ with q not divisible by ℓ, using the theory of $\mathbb{Z}_p$-extensions.

The next step is to consider how large e_n is or whether e_n is zero. Washington's techniques also enable us to derive an explicit upper bound for e_n, which unfortunately is very large.

A breakthrough was achieved in successive papers of Horie [Horie 05a, Horie 05b, Horie 07a, Horie 07b]. 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.

Theorem 1.1. Horie *Let ℓ be a prime number.*

(1) *If $\ell \equiv 3, 5 \mod 8$, then ℓ does not divide h_n for all $n \geq 1$.*

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

(3) *If $\ell \equiv 7 \mod 16$ 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 remained 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 $\ell = 7, 17, 23, 31, 41, \ldots$.

In this paper, we give a criterion for nondivisibility of h_n for given n and prove that if ℓ does not divide h_m for some $m \geq 1$, then ℓ does not divide h_n for all $n \geq 1$. A bound m, which depends on ℓ, is explicitly given and is small enough to make it possible to verify computationally that ℓ does not divide h_m. For a real number x, we denote by $[x]$ the largest integer not exceeding x. Let δ_ℓ denote 0 or 1 according as $\ell \equiv 1 \mod 4$ or not.

Theorem 1.2. *Let ℓ be an odd prime number and 2^c the exact power of 2 dividing $\ell - 1$ or $\ell^2 - 1$ according as $\ell \equiv 1 \mod 4$ or not. Put*

$$m = 3c - 1 + 2\left[\log_2(\ell - 1)\right] - 2\delta_\ell.$$

If ℓ does not divide the class number of Ω_m, then ℓ does not divide the class number of Ω_n for all $n \geq 1$.

Typical values of m are as follows:

ℓ	7	17	31	257	8191	65537	524287	7340033
m	13	19	25	39	65	79	95	103

We prove the above theorem using Sinnott and Washington's method [Washington 97, Section 16.3]. Theorem 1.2, together with numerical calculations based on Section 3, allows us to obtain the following corollary.

Corollary 1.3. *Let ℓ be a prime number less than 10^7. Then ℓ does not divide the class number of Ω_n for all $n \geq 1$.*

2. PROOF OF THEOREM 1.2

We begin by explaining our notation. Let K be an algebraic number field of finite degree. We denote by $C(K)$ and $h(K)$ the ideal class group and the class number of K, respectively. If K is an imaginary abelian field, we denote by $C^-(K)$ and $h^-(K)$ the minus part of $C(K)$ and the relative class number of K, respectively. We denote by $\overline{\mathbb{Q}}_\ell$ the algebraic closure of the ℓ-adic number field $\mathbb{Q}_\ell$.

Let c be the integer as in Theorem 1.2, n an integer satisfying $n \geq c$, ℓ an odd prime number, χ a character mod ℓ with $\chi(-1) = -1$, and ψ_n an even character mod 2^{n+2} whose order is 2^n. Note that ψ_n generates the character group of the Galois group $G(\Omega_n/\mathbb{Q})$. Then a generalized Bernoulli number $B_{1,\chi\psi_n}$ is defined by

$$B_{1,\chi\psi_n} = \frac{1}{2^{n+2}\ell} \sum_{b=1}^{2^{n+2}\ell} b\chi\psi_n(b).$$

Let ζ_{ψ_n} be a primitive 2^{n+2}th root of unity with $\zeta_{\psi_n}^{2^{n+2-c}} = \psi_n(1 + 2^{n+2-c})$. Moreover, we define a rational function $f_1(T)$ in the rational function field $\mathbb{Q}_\ell(T)$ by

$$f_1(T) = \Bigl(\sum_{\substack{b \equiv 1 \mod 2^c \\ 0<b<2^{c+1}\ell}} \chi(b)T^b\Bigr)\Bigl(T^{2^{c+1}\ell} - 1\Bigr)^{-1}. \quad (2\text{–}1)$$

Then we have the following by [Washington 97, p. 387]:

Lemma 2.1. *Let χ, ψ_n be as above and $n \geq 2c - 1$. If $B_{1,\chi\psi_n} \equiv 0 \mod \overline{\ell}$ in $\mathbb{Z}_\ell[\zeta_{\psi_n}]$, then $f_1(\zeta_{\psi_n}) \equiv 0 \mod \overline{\ell}$ in $\mathbb{Z}_\ell[\zeta_{\psi_n}]$, where $\overline{\ell}$ is the ideal of $\mathbb{Z}_\ell[\zeta_{\psi_n}]$ generated by ℓ.*

From now on, we assume $n \geq 2c - 1$ and put $d = 2c - 2 + [\log_2(\ell - 1)] - \delta_\ell$. Moreover, we put $\zeta_\ell = \cos(2\pi/\ell) + \sqrt{-1}\sin(2\pi/\ell)$ and work in $K_{n,\ell} = \Omega_n(\zeta_\ell)$. We abbreviate $h^-(K_{n,\ell})$ as $h^-_{n,\ell}$. Then we have the following:

Lemma 2.2. *If $n \geq d$, then ℓ does not divide $h^-_{n,\ell}/h^-_{d,\ell}$.*

Proof: Put

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

Then

$$g(T) = T^{-1}(T^{2^c\ell} + 1)^{-1} \sum_{\substack{b \equiv 1 \mod 2^c \\ 0<b<2^{c+1}\ell}} \chi(b)T^b$$
$$= \sum_{\substack{b \equiv 1 \mod 2^c \\ 0<b\leq 1+2^c(\ell-1)}} \chi(b)T^{b-1}. \quad (2\text{–}2)$$

Hence $g(T)$ is contained in $\mathbb{Q}_\ell[T]$ and

$$\deg g(T) \le 2^c(\ell-1),$$

where $\deg g(T)$ denotes the degree of $g(T)$. The assertion of the lemma is trivially valid for $n = d$. So we assume $n \ge d+1$. Then we have $g(\zeta) \not\equiv 0 \mod \overline{\ell}$ for any primitive 2^{n+2}th root of unity ζ in $\overline{\mathbb{Q}}_\ell$ by

$$[\mathbb{Q}_\ell(\zeta):\mathbb{Q}_\ell] = 2^{n+2-c+\delta_\ell} \ge 2^{d+3-c+\delta_\ell} = 2^{c+1+[\log_2(\ell-1)]} > 2^c(\ell-1).$$

The class number formula (cf. [Washington 97, Theorem 4.17])

$$h^-_{n,\ell} = Q_{n,\ell}2\ell \prod_\chi \prod_{b=1}^{2^n}\left(-\frac{1}{2}B_{1,\chi\psi_n^b}\right) \tag{2–3}$$

yields our assertion by Lemma 2.1, where $Q_{n,\ell}$ is 1 or 2 and χ runs over all characters modulo ℓ with $\chi(-1) = -1$. □

We denote by $r^-_{n,\ell}$ the ℓ-rank of $C^-(K_{n,\ell})$ and abbreviate $h(\Omega_n)$ as h_n. Then the following follows from [Washington 97, Theorems 10.8 and 10.11]:

Lemma 2.3. *If ℓ divides h_n and if ℓ does not divide h_{n-1}, then $2^{n-c+\delta_\ell} \le r^-_{n,\ell}$.*

Proof of Theorem 1.2: Using a rough estimate

$$\left|\frac{1}{2}B_{1,\chi\psi_n}\right| \le \begin{cases} \dfrac{1}{2^{n+3}\ell}\displaystyle\sum_{i=1}^{2^{n+1}\ell}(2i-1) = 2^{n-1}\ell & \text{if } n \ge 1,\\ \dfrac{1}{2\ell}\displaystyle\sum_{i=1}^{\ell-1} i = \dfrac{\ell-1}{4} < 2^{-2}\ell & \text{if } n = 0,\end{cases}$$

and (2–3), we have

$$\begin{aligned} h^-_{n,\ell} &< 2^2\ell(2^{-2}\ell)^{\frac{\ell-1}{2}}\prod_{i=1}^{n}(2^{i-1}\ell)^{2^{i-1}\frac{\ell-1}{2}} \\ &= 4\ell\cdot 2^{(n-2)(\ell-1)2^{n-1}}\ell^{(\ell-1)2^{n-1}}, \end{aligned} \tag{2–4}$$

which implies

$$r^-_{n,\ell} < \log_\ell(4\ell) + (n-2)(\ell-1)2^{n-1}\log_\ell(2) + (\ell-1)2^{n-1}.$$

Hence we have

$$r^-_{n,\ell} < \log_\ell(4\ell) + (d-2)(\ell-1)2^{d-1}\log_\ell(2) + (\ell-1)2^{d-1}$$

for all $n \ge 1$ by Lemma 2.2.

Assume that ℓ does not divide h_m, where m is the integer stated in the theorem. In order to prove the theorem, we assume that there exists n such that ℓ divides h_n and does not divide h_{n-1}, and deduce a contradiction.

Lemma 2.3 shows that

$$\begin{aligned} 2^{n-c+\delta_\ell} &< \log_\ell(4\ell) + (d-2)(\ell-1)2^{d-1}\log_\ell(2) \\ &\quad + (\ell-1)2^{d-1} \\ &= \log_\ell(4\ell) + (\ell-1)2^{2c-3+[\log_2(\ell-1)]-\delta_\ell} \\ &\quad \times\left\{1 + (2c-4+[\log_2(\ell-1)]-\delta_\ell)\log_\ell(2)\right\} \\ &< \log_\ell(4\ell) + (\ell-1)2^{2c-3+[\log_2(\ell-1)]-\delta_\ell} \\ &\quad \times\left\{2 + \frac{1}{\log_2(\ell)}(2c-4)\right\} \\ &< 3 + (\ell-1)2^{2c-1+[\log_2(\ell-1)]-\delta_\ell}. \end{aligned}$$

In the last step, we used the inequality $2^c \le \ell-1$ if $\ell \equiv 1 \mod 4$ and $2^{c-1} \le \ell+1$ if $\ell \equiv 3 \mod 4$. Since the left-hand side of the above inequality is a power of 2 and the right-hand side is of the form $3+64k$ with $k \ge 1$, we have

$$2^{n-c+\delta_\ell} \le (\ell-1)2^{2c-1+[\log_2(\ell-1)]-\delta_\ell}$$

and hence

$$n - c + \delta_\ell \le \log_2(\ell-1) + 2c - 1 + [\log_2(\ell-1)] - \delta_\ell,$$

which means that $n \le m$. This is a contradiction. □

3. CALCULATION

In this section, we explain how to verify numerically that an odd prime number ℓ does not divide the class number h_n of Ω_n for large n.

3.1 General Settings

Let $\Delta_n = G(\Omega_n/\mathbb{Q})$ be the Galois group of Ω_n over $\mathbb{Q}$, and A_n the ℓ-part of the ideal class group of Ω_n. For a character $\chi : \Delta_n \to \overline{\mathbb{Q}}_\ell$, we define the idempotent e_χ by

$$e_\chi = \frac{1}{|\Delta_n|}\sum_{\sigma\in\Delta_n}\mathrm{Tr}(\chi^{-1}(\sigma))\sigma \in \mathbb{Z}_\ell[\Delta_n], \tag{3–1}$$

and the χ-part $A_{n,\chi}$ of A_n by $A_{n,\chi} = e_\chi A_n$ as in [Gras 77], where $\mathrm{Tr} : \mathbb{Q}_\ell(\chi(\Delta_n)) \to \mathbb{Q}_\ell$ is the trace map.

Then we have $A_n = \oplus_\chi A_{n,\chi}$, where χ runs over all representatives of $\mathbb{Q}_\ell$-conjugacy classes of characters of Δ_n. If χ is not injective, the intermediate field of Ω_n corresponding to $\mathrm{Ker}\,\chi$ is Ω_k for some $0 \le k < n$ and $A_{n,\chi} \cong A_{k,\chi}$ canonically. So we may assume that χ is injective.

Now, for $n \geq 1$, let ζ_n denote a primitive 2^nth root of unity in $\mathbb{C}$ and put

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

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

$$e_{\chi,\ell} \equiv e_\chi \mod \ell,$$

in order to consider an action on ξ_n. We note that ξ_n itself is not a unit in Ω_n, but $\xi_n^{e_{\chi,\ell}}$ is a cyclotomic unit of Ω_n if we choose $e_{\chi,\ell}$ such that the sum of coefficients is zero. The following lemma is a special case of [Aoki and Fukuda 06, Lemma 1].

Lemma 3.1. *If there exists a prime number p that is congruent to 1 modulo $2^{n+2}\ell$ and satisfies*

$$(\xi_n^{e_{\chi,\ell}})^{\frac{p-1}{\ell}} \not\equiv 1 \mod \mathfrak{p} \qquad (3\text{–}2)$$

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

Let $s = c - \delta_\ell$ with c as in Theorem 1.2. Then 2^s is the exact power of 2 dividing $\ell - 1$ or $\ell + 1$ according as $\ell \equiv 1 \mod 4$ or not. When $n \leq s$, the calculation of (3–2) is straightforward, so we explain how to reduce the amount of calculation when $n \geq s + 1$.

Owing to Lemma 3.1, we may regard χ as a character of Δ_n into $\overline{\mathbb{F}}_\ell$ and define e_χ to be an element of $\mathbb{F}_\ell[\Delta_n]$, where $\overline{\mathbb{F}}_\ell$ is an algebraic closure of $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$. Let η_n be a primitive 2^nth root of unity in $\overline{\mathbb{F}}_\ell$ and $K = \mathbb{F}_\ell(\eta_n)$. Then $[K : \mathbb{F}_\ell] = 2^{n-s}$ for $n \geq s + 1$. Let ρ be the generator of Δ_n induced by $\zeta_{n+2} \mapsto \zeta_{n+2}^5$, and χ the character of Δ_n defined by $\chi(\rho) = \eta_n$. Then

$$e_{\chi^{-1}} = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^i)\rho^i.$$

The calculation of $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^i)$ divides into two cases according as $\ell \equiv 1 \mod 4$ or not.

3.2 The case $\ell \equiv 1 \mod 4$

Let $n \geq s + 1$. Then the minimal polynomial of η_n over $\mathbb{F}_\ell$ is

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

Namely, $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^i) = 0$ if i is not divisible by 2^{n-s}. Hence we have

$$\begin{aligned} e_{\chi^{-1}} &= \frac{1}{2^n} \sum_{i=0}^{2^s-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{2^{n-s}i})\rho^{2^{n-s}i} \\ &= \frac{1}{2^s} \sum_{i=0}^{2^s-1} \eta_s^i \rho^{2^{n-s}i}. \end{aligned}$$

Since there are 2^{s-1} nonconjugate primitive 2^nth roots of unity in $\overline{\mathbb{F}}_\ell$, there are the same number of $\mathbb{F}_\ell$-conjugacy classes of injective characters of Δ_n. Namely, if we put

$$X = \{j \in \mathbb{Z} \mid 1 \leq j \leq 2^s - 1,\ j \text{ odd}\},$$

then $\{\chi^j \mid j \in X\}$ is a set of representatives of the $\mathbb{F}_\ell$-conjugacy classes of injective characters of Δ_n. Since the choice of η_n is arbitrary, we may assume that

$$\eta_s \equiv g_\ell^{\frac{\ell-1}{2^s}} \mod \ell,$$

where $g_\ell \in \mathbb{Z}$ is a primitive root modulo ℓ.

Let p be a prime number congruent to 1 modulo $2^{n+2}\ell$ and let g_p be a primitive root of p. Then

$$\zeta_{n+2} + \zeta_{n+2}^{-1} \equiv g_p^{\frac{p-1}{2^{n+2}}} + g_p^{-\frac{p-1}{2^{n+2}}} \mod \mathfrak{p}$$

for some prime ideal $\mathfrak{p}$ of Ω_n lying above p.

Now we fix nonnegative integers z_1, z_2, and a_{ij} satisfying

$$z_1 \equiv g_p^{\frac{p-1}{2^{n+2}}} \mod p, \qquad (3\text{–}3)$$

$$z_2 \equiv z_1^{-1} \mod p, \qquad (3\text{–}4)$$

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{2^s}ij} \mod \ell.$$

Then Lemma 3.1 implies the following criterion.

Lemma 3.2. *Put $b = 5^{2^{n-s}}$. If for each $j \in X$, there exists a prime number p congruent to 1 modulo $2^{n+2}\ell$ that satisfies*

$$\left(\prod_{i=0}^{2^s-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}}\right)^{\frac{p-1}{\ell}} \not\equiv 1 \mod p,$$

then ℓ does not divide h_n/h_{n-1}.

We note that b^i should be calculated modulo 2^{n+2}, and the a_{ij} no longer need to satisfy $\sum_i a_{ij} = 0$.

3.3 The Case $\ell \equiv 3 \mod 4$

Let $n \geq s + 1$ and let

$$X^2 - aX - 1$$

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

$$X^{2^{n-s}} - aX^{2^{n-s-1}} - 1.$$

Namely, $\mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^i) = 0$ if i is not divisible by 2^{n-s-1}. Hence we have

$$e_{\chi^{-1}} = \frac{1}{2^n} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{2^{n-s-1}i})\rho^{2^{n-s-1}i}$$
$$= \frac{1}{2^{s+1}} \sum_{i=0}^{2^{s+1}-1} \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^i)\rho^{2^{n-s-1}i},$$

and we need to calculate

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

We start from $t_1 = \eta_{s+1} + \eta_{s+1}^\ell$ and proceed to

$$t_2 = \eta_{s+1}^2 + \eta_{s+1}^{2\ell} = (\eta_{s+1} + \eta_{s+1}^\ell)^2 - 2\eta_{s+1}^{\ell+1} = t_1^2 + 2,$$
$$t_{2^2} = \eta_{s+1}^{2^2} + \eta_{s+1}^{2^2\ell} = (\eta_{s+1}^2 + \eta_{s+1}^{2\ell})^2 - 2\eta_{s+1}^{2(\ell+1)}$$
$$= t_2^2 - 2$$
$$\cdots$$
$$t_{2^{s-1}} = \eta_{s+1}^{2^{s-1}} + \eta_{s+1}^{2^{s-1}\ell} = t_{2^{s-2}}^2 - 2 = 0,$$

noting that $\eta_{s+1}^{\ell+1} = -1$. Reversing this procedure, we obtain the following algorithm for calculating t_1. Note that $t_0 = 2$.

Lemma 3.3. *Let $a_2 = 0$ and define $a_i \in \mathbb{F}_\ell$, $3 \le i \le s+1$, by the recurrence formula*

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

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

Remark 3.4. For each step, we have two square roots. So we have just 2^{s-1} instances of t_1, which correspond to the 2^{s-1} nonconjugate primitive 2^{s+1}th roots of unity in $\overline{\mathbb{F}}_\ell$. We fix an arbitrary such root of unity.

Remark 3.5. Since $\ell \equiv 3 \mod 4$, taking square roots in $\mathbb{F}_\ell$ is easy. Indeed, if $a \in \mathbb{F}_\ell$ and $\sqrt{a} \in \mathbb{F}_\ell$, then $\sqrt{a} = \pm a^{(\ell+1)/4}$.

Lemma 3.3 also determines $t_2, t_{2^2}, \ldots, t_{2^{s-2}}$. But we need t_i, $1 \le i \le 2^s - 1$, and we obtain these from t_0 and t_1 using the following recurrence formula.

Lemma 3.6. *We have $t_{i+2} = t_1 t_{i+1} + t_i$ for $i \ge 0$.*

Proof: We have

$$t_1 t_{i+1} = (\eta_{s+1} + \eta_{s+1}^\ell)(\eta_{s+1}^{i+1} + \eta_{s+1}^{(i+1)\ell})$$
$$= \eta_{s+1}^{i+2} + \eta_{s+1}^{(i+2)\ell} + \eta_{s+1}^{\ell+1}(\eta_{s+1}^i + \eta_{s+1}^{i\ell})$$
$$= t_{i+2} - t_i,$$

yielding the result. □

In this case, we put

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

Then $\{\chi^j \mid j \in X\}$ is a set of representatives of the $\mathbb{F}_\ell$-conjugacy classes of injective characters of Δ_n. Let p be a prime number congruent to 1 modulo $2^{n+2}\ell$ and choose $z_1, z_2, a_{ij} \in \mathbb{Z}$ by (3–3), (3–4), and

$$a_{ij} \equiv t_{ij} \mod \ell.$$

Note that ij on the left-hand side is a subscript with two indices and that on the right is the product of i and j.

Next we make some technical remarks. Let $i' = 2^s + i$ and $b = 5^{2^{n-s-1}}$. Then we have

$$b^{i'} = 5^{2^{n-s-1}(2^s+i)} = 5^{2^{n-1}} b^i \equiv (2^{n+1} + 1)b^i \mod 2^{n+2},$$
$$z_1^{b^{i'}} \equiv g_p^{\frac{p-1}{2^{n+2}}(2^{n+1}+1)b^i} \equiv g_p^{\frac{p-1}{2}} z_1^{b^i} \equiv -z_1^{b^i} \mod p,$$
$$a_{i'j} = \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^{(2^s+i)j}) = \mathrm{Tr}_{\mathbb{F}_\ell(\eta_{s+1})/\mathbb{F}_\ell}(\eta_{s+1}^{2^s j}\eta_{s+1}^{ij})$$
$$= -a_{ij}.$$

Therefore

$$\prod_{i=0}^{2^{s+1}-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}} \equiv \prod_{i=0}^{2^s-1} \left(\frac{2 - z_1^{b^i} - z_2^{b^i}}{2 + z_1^{b^i} + z_2^{b^i}}\right)^{a_{ij}} \mod p.$$

Hence Lemma 3.1 yields the following criterion.

Lemma 3.7. *Put $b = 5^{2^{n-s-1}}$. If for each $j \in X$, there exists a prime number p congruent to 1 modulo $2^{n+2}\ell$ that satisfies*

$$\left(\prod_{i=0}^{2^s-1} \left(\frac{2 - z_1^{b^i} - z_2^{b^i}}{2 + z_1^{b^i} + z_2^{b^i}}\right)^{a_{ij}}\right)^{\frac{p-1}{\ell}} \not\equiv 1 \mod p,$$

then ℓ does not divide h_n/h_{n-1}.

3.4 A Logarithmic Version of Algorithms

When one fixes ℓ and varies n, the running times of Lemmas 3.2 and 3.7 are roughly proportional to n. So we can verify that ℓ does not divide h_n in reasonable time for large n. For example, it takes only 24 minutes on a computer with a Pentium IV 2-GHz processor to verify that 3 does not divide h_{1000}.

On the other hand, if one fixes n and varies ℓ, the running time is proportional to 4^s. For example, an experimental calculation estimates that 40 days are needed to apply Theorem 1.2 to $\ell = 2^{16} + 1$. So we are led to a logarithmic version of Lemmas 3.2 and 3.7 by adapting the idea of [Aoki 02, Corollary 11] or [Aoki 05, Theorem 13].

For $x \in \mathbb{F}_p^\times$, let $\nu_p(x)$ be the unique nonnegative integer less than p that satisfies

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

The calculation of $\nu_p(x)$ is considered hard for large p. But $\nu_p(x) \bmod \ell$ is enough for our purpose. Let $\nu_p(x) = i + j\ell$. Then we can determine i from

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

for small ℓ (e.g., $\ell < 10^7$). Hence we can determine $x_i \in \mathbb{Z}$ that satisfy

$$x_i \equiv \begin{cases} \nu_p(2 - z_1^{b^i} - z_2^{b^i}) \bmod \ell & \text{if } \ell \equiv 1 \bmod 4, \\ \nu_p\left(\dfrac{2 - z_1^{b^i} - z_2^{b^i}}{2 + z_1^{b^i} + z_2^{b^i}}\right) \bmod \ell & \text{if } \ell \equiv 3 \bmod 4. \end{cases}$$

Then Lemmas 3.2 and 3.7 shift to the following form.

Lemma 3.8. *If for each $j \in X$, there exists a prime number p congruent to 1 modulo $2^{n+2}\ell$ that satisfies*

$$\sum_{i=0}^{2^s-1} a_{ij} x_i \not\equiv 0 \bmod \ell, \tag{3–5}$$

then ℓ does not divide h_n/h_{n-1}.

Lemma 3.8 has two advantages. One is, of course, simple multiplication operations, and the other is that all numbers in (3–5) are less than ℓ. A careful implementation of the lemma enables us to verify in 10 hours that $\ell = 2^{16} + 1$ does not divide h_{79}, which is necessary for applying Theorem 1.2.

3.5 Fast Fourier Transform

Lemma 3.8 is faster than Lemmas 3.2 and 3.7 for large s, but it is still an $O(4^s)$ algorithm. The calculating time for $\ell = 2^{19} - 1$ is estimated to be 640 hours. Fortunately, Sumida [Sumida 04] showed that the fast Fourier transform (FFT) provides an efficient method of calculation for this kind of sum.

3.5.1 The case $\ell \equiv 1 \bmod 4$. Since $a_{ij} = \eta_s^{ij}$ in this case and j is odd, putting $j = 2r + 1$ and noting that $2ir = i^2 + r^2 - (r-i)^2$, the expression (3–5) is transformed into

$$\sum_{i=0}^{2^s-1} a_{ij} x_i = \sum_{i=0}^{2^s-1} \eta_s^{i(2r+1)} x_i = \eta_s^{r^2} \sum_{i=0}^{2^s-1} \eta_s^{-(r-i)^2} \eta_s^{i(i+1)} x_i.$$

The last sum is considered a cyclic convolution of $u_i = \eta_s^{-i^2}$ and $v_i = \eta_s^{i(i+1)} x_i$. Hence we can evaluate (3–5) in $O(\log_2(2^s)2^s) = O(s2^s)$ time using FFT.

3.5.2 The case $\ell \equiv 3 \bmod 4$. Putting $j = 2r + 1$, we have

$$\begin{aligned} \sum_{i=0}^{2^s-1} a_{ij} x_i &= \sum_{i=0}^{2^s-1} (\eta_{s+1}^{ij} + \eta_{s+1}^{ij\ell}) x_i \\ &= \sum_{i=0}^{2^s-1} (\eta_{s+1}^{ij} x_i + \eta_{s+1}^{ij\ell} x_i^\ell) \\ &= \sum_{i=0}^{2^s-1} \eta_{s+1}^{ij} x_i + \left(\sum_{i=0}^{2^s-1} \eta_{s+1}^{ij} x_i\right)^\ell \\ &= \mathrm{Tr}\left(\sum_{i=0}^{2^s-1} \eta_{s+1}^{ij} x_i\right) \\ &= \mathrm{Tr}\left(\eta_{s+1}^{r^2} \sum_{i=0}^{2^s-1} \eta_{s+1}^{-(r-i)^2} \eta_{s+1}^{i(i+1)} x_i\right). \end{aligned}$$

First we prepare the table of $\eta_{s+1}^i = a_i + b_i \eta_{s+1}$, $a_i, b_i \in \mathbb{F}_\ell$, $0 \le i \le 2^{s+1} - 1$, using the following formula:

Lemma 3.9. *We have $a_0 = 1$, $b_0 = 0$ and $a_{i+1} = b_i$, $b_{i+1} = a_i + t_1 b_i \quad (i \ge 0)$.*

Proof: We have $a_{i+1} + b_{i+1}\eta_{s+1} = (a_i + b_i \eta_{s+1})\eta_{s+1} = a_i \eta_{s+1} + b_i(1 + t_1 \eta_{s+1}) = b_i + (a_i + t_1 b_i)\eta_{s+1}$. □

Next we calculate

$$\begin{aligned} A_i &= a_{-i^2} \in \mathbb{F}_\ell, \\ B_i &= a_{i+i^2} x_i \in \mathbb{F}_\ell, \\ C_i &= b_{-i^2} \in \mathbb{F}_\ell, \\ D_i &= b_{i+i^2} x_i \in \mathbb{F}_\ell, \end{aligned}$$

$0 \le i \le 2^s - 1$, considering subscripts $-i^2$ and $i + i^2$ modulo 2^{s+1}.

Four convolutions

$$X_r = \sum_{i=0}^{2^s-1} A_{r-i} B_i \in \mathbb{F}_\ell,$$

$$Y_r = \sum_{i=0}^{2^s-1} A_{r-i} D_i \in \mathbb{F}_\ell,$$

$$Z_r = \sum_{i=0}^{2^s-1} C_{r-i} B_i \in \mathbb{F}_\ell,$$

$$W_r = \sum_{i=0}^{2^s-1} C_{r-i} D_i \in \mathbb{F}_\ell,$$

$0 \le r \le 2^s - 1$, are calculated in $O(s2^s)$ time using FFT, and we have

$$\begin{aligned}\sum_{i=0}^{2^s-1} \eta_{s+1}^{-(r-i)^2}\eta_{s+1}^{i(i+1)}x_i &= \sum_{i=0}^{2^s-1}(A_{r-i}+C_{r-i}\eta_{s+1})(B_i+D_i\eta_{s+1}) \\ &= \sum_{i=0}^{2^s-1}\big(A_{r-i}B_i+(A_{r-i}D_i+C_{r-i}B_i)\eta_{s+1} \\ &\qquad + C_{r-i}D_i(1+t_1\eta_{s+1})\big) \\ &= X_r+W_r+(Y_r+Z_r+t_1W_r)\eta_{s+1}.\end{aligned}$$

In order to regard this expression as convolution, we have to consider the subscript $r-i$ not modulo 2^{s+1} but modulo 2^s. We note that our calculation is consistent, because $(2^s+i)^2 = 2^{2s}+2^{s+1}i+i^2 \equiv i^2 \bmod 2^{s+1}$. Therefore we obtain

$$\eta_{s+1}^{r^2}\sum_{i=0}^{2^s-1}\eta_{s+1}^{-(r-i)^2}\eta_{s+1}^{i(i+1)}x_i = E_r + F_r\eta_{s+1},$$

$E_r, F_r \in \mathbb{F}_\ell$, $0 \le r \le 2^s-1$, in $O(s2^s)$ time and hence obtain

$$\begin{aligned} w_r = \sum_{i=0}^{2^s-1} a_{ij}x_i &= E_r + F_r\eta_{s+1} + (E_r+F_r\eta_{s+1})^\ell \\ &= 2E_r + t_1F_r,\end{aligned}$$

$0 \le r \le 2^s-1$, also in $O(s2^s)$ time. It suffices to check $w_r \ne 0$ for $0 \le r \le 2^{s-2}-1$ and $2^{s-1} \le r \le s^{s-1} + 2^{s-2}-1$.

In this manner, we verified $65537 \nmid h_{79}$ in 4 minutes and $524287 \nmid h_{95}$ in 95 minutes. We needed two weeks to derive Corollary 1.3 with three computers combining Lemmas 3.2, 3.7, 3.8 and FFT techniques.

4. APPENDIX

The class number h_6 of Ω_6 is known to be 1 under GRH. It is natural to ask whether Lemmas 3.2 and 3.7 contribute to the derivation of some bound on h_6 without GRH. We have verified that h_6 does not have prime divisors less than 10^{11}. So the following holds:

Theorem 4.1. *If $h_6 > 1$, then $h_6 > 10^{11}$.*

It is possible to reduce the bound m in Theorem 1.2 by investigating carefully the properties of the rational function $f_1(T)$. Namely, the following holds:

Theorem 4.2. *Let ℓ, c, δ_ℓ be the same as in Theorem 1.2 and put*

$$m_1 = 3c + [\log_2(\ell-1)] + \left[\frac{1}{2}\log_2(\ell-1)\right] - \delta_\ell.$$

If ℓ does not divide h_{m_1}, then ℓ does not divide h_n for all $n \ge 1$.

Though our proof is slightly complicated, we write it down because this theorem may be useful if one tries to extend the range of Corollary 1.3. We note that we used Theorem 1.2 to derive Corollary 1.3.

Let $K_{n,\ell} = \Omega_n(\zeta_\ell)$ with $\zeta_\ell = \cos(2\pi/\ell) + \sqrt{-1}\sin(2\pi/\ell)$ as in Section 2 and denote by v_ℓ the additive ℓ-adic valuation normalized by $v_\ell(\ell) = 1$. For a character χ' of $G_n = G(K_{n,\ell}/\mathbb{Q})$, the idempotent $e_{\chi'}$ is defined by replacing Δ_n with G_n in (3–1). Then $e_{\chi'}$ acts on the ℓ-part A'_n of the ideal class group of $K_{n,\ell}$. If χ' is odd, the equality

$$v_\ell(|e_{\chi'}A'_n|) = (\mathbb{Z}_\ell[\chi'(G_n)] : \mathbb{Z}_\ell)v_\ell(B_{1,\chi'^{-1}})$$

holds. This is a direct consequence of Iwasawa's main conjecture proved by Mazur–Wiles [Mazur and Wiles 84, p. 216, Theorem 2]. Let ψ_n be the character stated in Section 2, and ω the Teichmüller character modulo ℓ (i.e., the Teichmüller character of G_0). By definition, e_ω is an element of $\mathbb{Z}_\ell[G_0]$ and acts on A'_0. Further we let e_ω act on A'_n using the isomorphism $G_o \cong G(K_{n,\ell}/\Omega_n)$. By decomposing $e_\omega A'_n$ using ψ_n, we have the following [Gras 77]:

Lemma 4.3. *We have $v_\ell(B_{1,\omega^{-1}\psi_n^{-j}}) \ge 0$ and for $n \ge 1$*

$$v_\ell(|e_\omega A'_n|) - v_\ell(|e_\omega A'_{n-1}|) = \sum_{\substack{j=1 \\ j \text{ odd}}}^{2^n-1} v_\ell(B_{1,\omega^{-1}\psi_n^{-j}}).$$

Now, putting $\chi = \omega^{-1}$ in (2–1), we define

$$f_1(T) = \left(\sum_{\substack{b\equiv 1 \bmod 2^c \\ 0<b<2^{c+1}\ell}} \omega^{-1}(b)T^b\right)\left(T^{2^{c+1}\ell}-1\right)^{-1}.$$

In Lemma 2.1, we considered a congruence relation modulo $\overline{\ell}$ to avoid vagueness. But it is reasonable to use ℓ instead of $\overline{\ell}$ because ℓ is unramified in the field generated by the 2^{n+2}th roots of unity. We rewrite Lemma 2.1 in the following form.

Lemma 4.4. *We suppose that $n \ge 2c-1$. If $f_1(\zeta) \not\equiv 0 \bmod \ell$ for any primitive 2^{n+2}th root of unity in $\overline{\mathbb{Q}}_\ell$, then $B_{1,\omega^{-1}\psi_n^{-j}} \not\equiv 0 \bmod \ell$ for any odd integer j.*

Next we put $g(T) = f_1(T)(T^{2^c\ell} - 1)T^{-1}$ and $h(T) = \sum_{\nu=0}^{\ell-1} \omega^{-1}(1 + 2^c\nu)T^\nu$. Then (2–2) implies

$$\begin{aligned}\left(T^{2^{c+1}\ell} - 1\right) f_1(T) &= T\left(T^{2^c\ell} + 1\right)g(T) \qquad (4\text{–}1)\\ &= T\left(T^{2^c\ell} + 1\right)h(T^{2^c}).\end{aligned}$$

From now on, we assume $n \geq 2c - 1$ and put $u = n - 2c + 2$. Let θ be a primitive 2^cth root of unity in $\overline{\mathbb{Q}}_\ell$. Then $x^{2^u} - \theta \bmod \ell$ is irreducible over $\mathbb{F}_\ell$ or the quadratic extension of $\mathbb{F}_\ell$ according as $\ell \equiv 1 \mod 4$ or not. We put $e = [(\ell - 1)/2^u]$, $f = \ell - 1 - 2^u e$, and

$$a_{ij} = \begin{cases} \omega^{-1}(1 + 2^c(2^u j + i)) & \text{if } 2^u j + i < \ell, \\ 0 & \text{if } 2^u j + i \geq \ell. \end{cases}$$

Assuming $e \geq 1$ for the time being, we put $s_i(\theta) = \sum_{j=0}^{e} a_{ij}\theta^j$. Then there exist polynomials $q(x), r(x) \in \mathbb{Z}_\ell[\theta][x]$ such that $h(x) = (x^{2^u} - \theta)q(x) + r(x)$ with $r(x) = s_0(\theta) + s_1(\theta)x + \cdots + s_{2^u-1}(\theta)x^{2^u-1}$ and such that $\deg r(x) < 2^u$.

Lemma 4.5. *Let α, β, γ be nonzero elements in $\overline{\mathbb{F}}_\ell$ and let ν_i, μ_j be positive integers with $\nu_1 < \nu_2 < \cdots < \nu_k < \ell$ and $\mu_1 < \mu_2 < \cdots < \mu_k < \ell$. Let*

$$S = \begin{pmatrix} \frac{1}{\alpha} & \frac{1}{\alpha+\beta\mu_1} & \cdots & \frac{1}{\alpha+\beta\mu_k} \\ \frac{1}{\alpha+\gamma\nu_1} & \frac{1}{\alpha+\beta\mu_1+\gamma\nu_1} & \cdots & \frac{1}{\alpha+\beta\mu_k+\gamma\nu_1} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{1}{\alpha+\gamma\nu_k} & \frac{1}{\alpha+\beta\mu_1+\gamma\nu_k} & \cdots & \frac{1}{\alpha+\beta\mu_k+\gamma\nu_k} \end{pmatrix}$$

be a matrix of degree $k+1$. We assume that none of the denominators of entries of S are zero. Then the determinant $|S|$ of S is not zero.

Proof: The basic row and column operations yield

$$|S| = \frac{(\beta\gamma)^k \prod_{i=1}^{k}(\mu_i\gamma_i)}{\alpha\left(\prod_{i=1}^{k}(\alpha + \beta\mu_i)(\alpha + \gamma\nu_i)\right)} \times \begin{vmatrix} \frac{1}{\alpha+\beta\mu_1+\gamma\nu_1} & \cdots & \frac{1}{\alpha+\beta\mu_k+\gamma\nu_1} \\ \vdots & \cdots & \vdots \\ \frac{1}{\alpha+\beta\mu_1+\gamma\nu_k} & \cdots & \frac{1}{\alpha+\beta\mu_k+\gamma\nu_k} \end{vmatrix}.$$

We put $\alpha' = \alpha + \beta\mu_1 + \gamma\nu_1, \beta' = \beta, \gamma' = \gamma, \mu'_i = \mu_i - \mu_1$, and $\nu'_i = \nu_i - \nu_1$. Then we have

$$\begin{vmatrix} \frac{1}{\alpha+\beta\mu_1+\gamma\nu_1} & \cdots & \frac{1}{\alpha+\beta\mu_k+\gamma\nu_1} \\ \vdots & \cdots & \vdots \\ \frac{1}{\alpha+\beta\mu_1+\gamma\nu_k} & \cdots & \frac{1}{\alpha+\beta\mu_k+\gamma\nu_k} \end{vmatrix} = \begin{vmatrix} \frac{1}{\alpha'} & \frac{1}{\alpha'+\beta'\mu'_2} & \cdots & \frac{1}{\alpha'+\beta'\mu'_k} \\ \frac{1}{\alpha'+\gamma'\nu'_2} & \frac{1}{\alpha'+\beta'\mu'_2+\gamma'\nu'_2} & \cdots & \frac{1}{\alpha'+\beta'\mu'_k+\gamma'\nu'_2} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{1}{\alpha'+\gamma'\nu'_k} & \frac{1}{\alpha'+\beta'\mu'_2+\gamma'\nu'_k} & \cdots & \frac{1}{\alpha'+\beta'\mu'_k+\gamma'\nu'_k} \end{vmatrix}.$$

Our result follows from inductive arguments. □

Corollary 4.6. *Let u, e and a_{ij} be as above. We put*

$$R = \begin{pmatrix} \overline{a}_{00} & \cdots & \overline{a}_{0e} \\ \overline{a}_{10} & \cdots & \overline{a}_{1e} \\ \vdots & \cdots & \vdots \\ \overline{a}_{2^u-1,0} & \cdots & \overline{a}_{2^u-1,e} \end{pmatrix}$$

with $\overline{a}_{ij} = a_{ij} + \ell\mathbb{Z}_\ell[\theta] \in \mathbb{Z}_\ell[\theta]/\ell\mathbb{Z}_\ell[\theta]$. If $2^u > e$, then the rank of R is greater than or equal to e.

Proof: Note that $a_{ij} \equiv 1/(1 + 2^c(2^u j + i)) \mod \ell$ if $a_{ij} \neq 0$. Remove the last column of R that possibly contains zero entries. Further, remove one row that contains a zero entry and construct the matrix R' of size $(2^u - 1) \times e$ or $2^u \times e$. Then the rank of R' is equal to e by Lemma 4.5. □

Put $d = 2c + \left[\frac{1}{2}\log_2(\ell - 1)\right] - 1$. The following is a precise version of Lemma 2.2.

Proposition 4.7. *If $n \geq d$, then ℓ does not divide $|e_\omega A'_n|/|e_\omega A'_d|$.*

Proof: The argument in the proof of Lemma 2.2 immediately shows that the conclusion holds if

$$n \geq 2c - 1 + [\log_2(\ell - 1)] - \delta_\ell.$$

So we assume

$$d + 1 \leq n \leq 2c - 2 + [\log_2(\ell - 1)] - \delta_\ell.$$

Hence

$$u = n - 2c + 2 \leq [\log_2(\ell - 1)]$$

and $e \geq 1$.

Let ζ be an arbitrary primitive 2^{n+2}th root of unity in $\overline{\mathbb{Q}}_\ell$ and put $\theta = \zeta^{2^{u+c}}$. We assume $f_1(\zeta) \equiv 0 \mod \ell$.

Then we have $h(\zeta^{2^c}) \equiv 0 \mod \ell$ by (4–1). Hence we have $r(\zeta^{2^c}) \equiv 0 \mod \ell$. Since $x^{2^u} - \theta \bmod \ell$ is irreducible in $\mathbb{Z}_\ell[\theta]/\ell\mathbb{Z}_\ell[\theta]$, we have

$$s_i(\theta) \equiv 0 \mod \ell \quad (0 \leq i \leq 2^u - 1). \tag{4–2}$$

From the condition $n \geq d + 1$, it follows that $u > \frac{1}{2}\log_2(\ell - 1) + 1$, which implies $2^{2u} > 4(\ell - 1)$. Hence $2^{u-1} > (\ell - 1)/2^u \geq e$. Let R be the matrix in Corollary 4.5.

First suppose $f \geq 2^{u-1}$, which implies $f + 1 > e + 1$. This shows that the rank of R is equal to $e+1$ by Lemma 4.5. Hence we have $\theta \equiv 0 \mod \ell$ by (4–2), which is a contradiction. Next suppose $f < 2^{u-1}$, which implies $2^u-(f+1) \geq 2^{u-1} > e$. This shows that $\theta \equiv 0 \mod \ell$ by applying Lemma 4.5 to the lowest $2^u - (f+1)$ rows of R, which is again a contradiction. Hence $f_1(\zeta) \not\equiv 0 \mod \ell$ and Lemmas 4.3 and 4.4 yield the conclusion. □

Proof of Theorem 4.2.: Since $v_\ell(|\ e_\omega A'_n\ |) \leq \log_\ell(h^-_{n,\ell})$, (2–4) implies

$$v_\ell(|\ e_\omega A'_n\ |) < \log_\ell(4\ell) + (\ell-1)2^{n-1}\{1 + (n-2)\log_\ell(2)\}$$

for all $n \geq 1$. This inequality remains valid if we replace n on the right-hand side with $d = 2c + [\frac{1}{2}\log_2(\ell - 1)] - 1$ by Proposition 4.7. Namely, we have

$$\begin{aligned} &v_\ell(|\ e_\omega A'_n\ |) \\ &\quad < \log_\ell(4\ell) + (\ell-1)2^{2c+[\frac{1}{2}\log_2(\ell-1)]-2} \\ &\quad\quad \times \left\{1 + \left(2c + \left[\frac{1}{2}\log_2(\ell-1)\right] - 3\right)\log_\ell(2)\right\} \\ &\quad < 3 + (\ell-1)2^{2c+[\frac{1}{2}\log_2(\ell-1)]}. \end{aligned}$$

Now assume that ℓ does not divide h_{m_1}, where m_1 is the integer stated in the theorem. Moreover, we assume that there exists n such that ℓ divides h_n and does not divide h_{n-1}. Then we have

$$\begin{aligned} 2^{n-c+\delta_\ell} &\leq \ell\text{-rank } A_n \leq \ell\text{-rank } e_\omega A'_n \leq v_\ell(|\ e_\omega A'_n\ |) \\ &< 3 + (\ell-1)2^{2c+[\frac{1}{2}\log_2(\ell-1)]}. \end{aligned}$$

The first inequality is what we used implicitly to deduce Lemma 2.3, and the second is a consequence of the reflection theorem. This turns into

$$2^{n-c+\delta_\ell} \leq (\ell-1)2^{2c+[\frac{1}{2}\log_2(\ell-1)]},$$

from which we deduce $n \leq m_1$ and hence a contradiction. □

ACKNOWLEDGEMENTS

We express our gratitude to the referee who read the manuscript very carefully and encouraged us to strive to obtain a better bound m in Theorem 1.2. Owing to the referee's advice, we succeeded in getting a smaller and simpler form of m.

REFERENCES

[Aoki 02] M. Aoki. *Notes on the Structure of the Ideal Class Groups of Abelian Number Fields*, Tokyo Metropolitan Univ. Math. Preprint Series, No. 18, 2002.

[Aoki 05] M. Aoki. "Note on the Structure of the Ideal Class Groups of Abelian Number Fields." *Proc. Japan Acad. Ser. A* 81 (2005), 69–74.

[Aoki and Fukuda 06] M. Aoki and T. Fukuda. "An Algorithm for Computing p-Class Groups of Abelian Number Fields." In *Algorithmic Number Theory*, pp. 56–71, Lecture Notes in Computer Science 4076. New York: Springer, 2006.

[Bauer 69] H. Bauer. "Numeriche Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper." *J. Number Theory* 1 (1969), 161–162.

[Cohn 60] H. Cohn. "A Numerical Study of Weber's Real Class Number Calculation I." *Numer. Math.* 2 (1960), 347–362.

[Gras 77] G. Gras. "Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés." *Ann. Inst. Fourier* 27-1 (1977), 1–66.

[Horie 05a] 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.

[Horie 05b] K. Horie. "Triviality in Ideal Class Groups of Iwasawa-Theoretical Abelian Number Fields." *J. Math. Soc. Japan* 57 (2005), 827–857.

[Horie 07a] K. Horie. "Primary Components of the Ideal Class Groups of Iwasawa-Theoretical Abelian Number Fields." *J. Math. Soc. Japan* 59 (2007), 811–824.

[Horie 07b] 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.

[Iwasawa 56] K. Iwasawa. "A Note on Class Numbers of Algebraic Number Fields." *Abh. Math. Sem. Univ. Hamburg* 20 (1956), 257–258.

[Linden 82] F. J. van der Linden. "Class Number Computations of Real Abelian Number Fields." *Math. Comp.* 39 (1982), 693–707.

[Masley 78] J. M. Masley. "Class Numbers of Real Cyclic Number Fields with Small Conductor." *Compositio Math.* 37 (1978), 297–319.

[Mazur and Wiles 84] B. Mazur and A. Wiles. "Class Fields of Abelian Extensions of $\mathbb{Q}$." *Invent. Math.* 76 (1984), 179–330.

[Sumida 04] H. Sumida. "Computation of Iwasawa Invariants of Certain Real Abelian Fields." *J. Number Theory* 105 (2004), 235–250.

[Washington 75] L. C. Washington. "Class Numbers and $\mathbb{Z}_p$-Extensions." *Math. Ann.* 214 (1975), 177–193.

[Washington 97] L. C. Washington. *Introduction to Cyclotomic Fields*, 2nd edition, Graduate Texts in Math. 83. New York: Springer-Verlag, 1997.

[Weber 86] 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 (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 (kkomatsu@waseda.jp)

Received April 5, 2008; accepted in revised form September 25, 2008.