

A Class Number Problem in the Cyclotomic \mathbf{Z}_3 -extension of \mathbf{Q}

Takayuki MORISAWA

Waseda University

(Communicated by J. Murakami)

Abstract. Let Ω_n be the n -th layer of the cyclotomic \mathbf{Z}_3 -extension of \mathbf{Q} and h_n the class number of Ω_n . We claim that if ℓ is a prime number less than 10^4 , then ℓ does not divide h_n for any positive integer n .

1. Introduction

Let p be a prime number. It is one of the basic cases of class number problem to ask whether a prime number ℓ divides the class numbers of the intermediate fields of the cyclotomic \mathbf{Z}_p -extension of \mathbf{Q} . In the case $\ell = p$, Iwasawa [4] proved that p does not divide any of the class numbers of the n -th layers of the cyclotomic \mathbf{Z}_p -extension of \mathbf{Q} . In the case $p = 2$, Fukuda and Komatsu [1] showed that ℓ does not divide any of the class numbers of the n -th layers of the cyclotomic \mathbf{Z}_2 -extension of \mathbf{Q} for $\ell < 10^7$.

In this paper, we investigate the case $p = 3$. Put $\Omega_n = \mathbf{Q}(2 \cos(2\pi/3^{n+1}))$. Then Ω_n is a cyclic extension of degree 3^n over \mathbf{Q} and the n -th layer of the cyclotomic \mathbf{Z}_3 -extension of \mathbf{Q} . We denote the class number of Ω_n by h_n . Masley [6] showed $h_1 = h_2 = h_3 = 1$. Linden [5] showed $h_4 = 1$ if GRH (the Generalized Riemann Hypothesis) is valid.

Horie [3] proved the following theorem.

THEOREM 1 (Horie). *Let the notation be as above for $p = 3$ and ℓ a prime number. If $\ell \equiv 2, 4, 5, 7 \pmod{9}$, then ℓ does not divide h_n for any positive integer n .*

In this paper, we prove the following result.

THEOREM 2. *Let $\ell \geq 5$ be a prime number and 3^s the exact power of 3 dividing $\ell^2 - 1$. Put*

$$m_\ell = 3s + 2 + [\log_3(\ell - 1)] + \left[\log_3 \frac{\ell - 1}{2} \right] + [\log_3(2s + 1 + [\log_3(\ell - 1)])],$$

where $[x]$ denotes the greatest integer not exceeding a real number x . If ℓ does not divide h_{m_ℓ} , then ℓ does not divide h_n for any positive integer n .

As a corollary to Theorem 2, we obtained the following result by numerical calculation.

COROLLARY 1. *Let ℓ be a prime number less than 10000. Then ℓ does not divide h_n for any positive integer n .*

We prove Theorem 2 in Section 2. In Section 3, we show a criterion in each of four disjoint cases to determine that a prime number ℓ does not divide h_n .

2. Proof of Theorem 2

Let n be a positive integer, ℓ a prime number with $\ell \geq 5$, χ a character mod ℓ with $\chi(-1) = -1$ and ψ_n an even character mod 3^{n+1} whose order is 3^n . Then the generalized Bernoulli number is defined by

$$B_{1, \chi \psi_n} = \frac{1}{3^{n+1} \ell} \sum_{b=1}^{3^{n+1} \ell} b \chi \psi_n(b).$$

Let s be as in Theorem 2 and ζ_{ψ_n} such a primitive 3^{n+1} -th root of unity as

$$\zeta_{\psi_n}^{3^{n+1-s}} = \psi_n(1 + 3^{n+1-s}).$$

We define a rational function $f_1(T)$ in the rational function field $\mathbf{Q}_\ell(T)$ by

$$f_1(T) = \left(\sum_{\substack{b \equiv 1 \pmod{3^s} \\ 0 < b < 3^s \ell}} \chi(b) T^b \right) (T^{3^s \ell} - 1)^{-1}.$$

We put $d = s + 1 + \lceil \log_3(\ell - 1) \rceil$. We also put $\zeta_\ell = \cos \frac{2\pi}{\ell} + \sqrt{-1} \sin \frac{2\pi}{\ell}$ and $K_{n, \ell} = \Omega_n(\zeta_\ell)$. Let $h_{n, \ell}^-$ be the relative class number of $K_{n, \ell}$. Then we have the following result by [7] p. 387:

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

LEMMA 2. *If $d + s - 1 \leq n$, then the prime number ℓ does not divide $h_{n, \ell}^- / h_{d+s-1, \ell}^-$.*

PROOF. Assume that $d + s - 1 \leq n$. We put

$$g(T) = \frac{(T^{3^s \ell} - 1) f_1(T)}{T}.$$

Since

$$g(T) = \sum_{\substack{b \equiv 1 \pmod{3^s} \\ 0 < b \leq 1+3^s(\ell-1)}} \chi(b)T^{b-1},$$

we have $\deg g(T) \leq 3^s(\ell - 1)$ where $\deg g(T)$ means the degree of the polynomial $g(T)$. Since

$$[\mathbf{Q}_\ell(\zeta) : \mathbf{Q}_\ell] \geq 3^{n+1-s} \geq 3^d > 3^s(\ell - 1) \geq \deg g(T)$$

for a primitive 3^{n+1} -th root of unity $\zeta \in \overline{\mathbf{Q}_\ell}$, we have

$$g(\zeta) \not\equiv 0 \pmod{\bar{\ell}},$$

and hence

$$f_1(\zeta) \not\equiv 0 \pmod{\bar{\ell}}.$$

In particular, we obtain $f_1(\zeta\psi_n) \not\equiv 0 \pmod{\bar{\ell}}$. By Lemma 1, we see $B_{1,\chi\psi_n} \not\equiv 0 \pmod{\bar{\ell}}$. Hence we obtain

$$\frac{h_{n,\ell}^-}{h_{d+s-1,\ell}^-} \not\equiv 0 \pmod{\bar{\ell}}$$

by the class number formula

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

where $Q_{n,\ell} = 1$ or 2 and χ runs over all characters mod ℓ with $\chi(-1) = -1$. □

We denote the plus part and the minus part of the ideal class group of $K_{n,\ell}$ by $C^+(K_{n,\ell})$ and by $C^-(K_{n,\ell})$ respectively. We also denote the ℓ -rank of $C^+(K_{n,\ell})$ and $C^-(K_{n,\ell})$ by $r_{n,\ell}^+$ and by $r_{n,\ell}^-$ respectively. Then Theorem 10.11 in [7] implies

$$r_{n,\ell}^+ \leq r_{n,\ell}^-.$$

LEMMA 3. *Suppose $s + 1 \leq n$. If ℓ divides h_n and if ℓ does not divide h_{n-1} , then $3^{n-s-1} < r_{n,\ell}^-$.*

PROOF. Let r_n be the ℓ -rank of the ideal class group of Ω_n . By Theorem 10.8 in [7], we have $r_n \geq 3^{n-s}$ if $\ell \equiv 1 \pmod{3}$ and $r_n \geq 2 \cdot 3^{n-s}$ if $\ell \equiv 2 \pmod{3}$. Since $r_n \leq r_{n,\ell}^+$, we have $3^{n-s-1} < r_{n,\ell}^-$. □

Now we prove Theorem 2.

Since $|B_{1,\chi\psi_n^b}| \leq 3^{n+1}\ell$, we have

$$\begin{aligned} h_{n,\ell}^- &\leq 2 \cdot 2 \cdot \ell \left(\frac{1}{2} 3^{n+1} \ell \right)^{\frac{\ell-1}{2} 3^n} \\ &< \ell^{3^n(n+1)\frac{\ell-1}{2}+2}. \end{aligned}$$

Hence we obtain

$$r_{n,\ell}^- < 3^n(n+1)\frac{\ell-1}{2} + 2,$$

and then

$$r_{n,\ell}^- < 3^{d+s-1}(d+s)\frac{\ell-1}{2} + 2 \quad (1)$$

by Lemma 2.

Let m_ℓ be as in Theorem 2 and assume that ℓ does not divide h_{m_ℓ} . We also assume that there exists a positive integer n such that ℓ divides h_n but does not divide h_{n-1} . Then we have $m_\ell < n$. By Lemma 3 and (1), we obtain

$$3^{n-s-1} \leq 3^{d+s-1}(d+s)\frac{\ell-1}{2}.$$

Hence we have

$$n-s-1 \leq d+s-1 + \log_3(d+s) + \log_3 \frac{\ell-1}{2};$$

this implies

$$n \leq 3s+1 + [\log_3(\ell-1)] + \log_3(d+s) + \log_3 \frac{\ell-1}{2}.$$

Therefore we have

$$n \leq 3s+2 + [\log_3(\ell-1)] + \left[\log_3 \frac{\ell-1}{2} \right] + [\log_3(2s+1 + [\log_3(\ell-1)])] = m_\ell.$$

This is a contradiction.

3. Calculation

Let $\Delta_n = \text{Gal}(\Omega_n/\mathbf{Q})$ be the Galois group of Ω_n over \mathbf{Q} and A_n the ℓ -part of the ideal class group of Ω_n .

For a character $\chi : \Delta_n \rightarrow \overline{\mathbf{Q}}_\ell$, we define e_χ by

$$e_\chi = \frac{1}{|\Delta_n|} \sum_{\sigma \in \Delta_n} \text{Tr}(\chi^{-1}(\sigma))\sigma \in \mathbf{Z}_\ell[\Delta_n],$$

where Tr is the trace map of $\mathbf{Q}_\ell(\chi(\Delta_n))/\mathbf{Q}_\ell$. We denote by $A_{n,\chi}$ the χ -part $e_\chi A_n$ of A_n . Then we have $A_n = \bigoplus_\chi A_{n,\chi}$ where χ runs over all representatives of \mathbf{Q}_ℓ -conjugacy classes of characters of Δ_n .

In order to prove that ℓ does not divide h_n , it is sufficient to prove that ℓ does not divide the order of $A_{n,\chi}$ for each χ . If χ is not injective, then there exists a positive integer k such that $\Omega_k = \Omega_n^{\text{Ker}\chi}$ and $A_{n,\chi} \cong A_{k,\chi}$. Therefore we may assume χ is injective.

Now, for $n \geq 1$, let ζ_n denote a primitive 3^n -th root of unity in \mathbf{C} and put

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

We fix a truncation $e_{\chi,\ell} \in \mathbf{Z}[\Delta_n]$ of e_χ satisfying

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

in order to consider an action on ξ_n . The following lemma is a special case of Lemma 1 in [2].

LEMMA 4. *If there exists a prime number p which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies*

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

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

Owing to Lemma 4, we may regard χ as a character of Δ_n into $\overline{\mathbf{F}}_\ell$ and define e_χ to be an element of $\mathbf{F}_\ell[\Delta_n]$ where $\overline{\mathbf{F}}_\ell$ is an algebraic closure of the finite field $\mathbf{F}_\ell = \mathbf{Z}/\ell\mathbf{Z}$. Let η_n be a primitive 3^n -th root of unity in $\overline{\mathbf{F}}_\ell$ and put $K = \mathbf{F}_\ell(\eta_n)$. Let ρ be the generator of Δ_n determined by $\zeta_{n+1} \mapsto \zeta_{n+1}^4$ and χ the character of Δ_n defined by $\chi(\rho) = \eta_n^{-1}$. Then

$$e_{\chi^j} = \frac{1}{3^n} \sum_{i=0}^{3^n-1} \text{Tr}_{K/\mathbf{F}_\ell}(\eta_n^{ij}) \rho^i.$$

Let p be a prime number congruent to 1 modulo $3^{n+1}\ell$ and g_p a primitive root of p . Then

$$\zeta_{n+1} \equiv g_p^{\frac{p-1}{3^{n+1}}} \pmod{\mathfrak{p}}$$

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

Therefore, if $e_{\chi^j} = \sum_i a_{ij} \rho^i$, then we have

$$\xi_n^{e_{\chi^j}} = \prod_{i=0}^{3^n-1} (2 - \zeta_{n+1} - \zeta_{n+1}^{-1})^{a_{ij} \rho^i}$$

$$\begin{aligned}
 &= \prod_{i=0}^{3^n-1} (2 - \zeta_{n+1}^{4^i} - \zeta_{n+1}^{-4^i})^{a_{ij}} \\
 &\equiv \prod_{i=0}^{3^n-1} (2 - g_p^{\frac{p-1}{3^{n+1}}4^i} - g_p^{-\frac{p-1}{3^{n+1}}4^i})^{a_{ij}} \pmod{p}.
 \end{aligned}$$

The last product should be calculated modulo p . We fix positive integers z_1 and z_2 satisfying

$$\begin{aligned}
 z_1 &\equiv g_p^{\frac{p-1}{3^{n+1}}} \pmod{p} \\
 z_2 &\equiv z_1^{-1} \pmod{p}.
 \end{aligned}$$

3.1. The case $\ell \equiv 1 \pmod{3}$ and $2 \leq n \leq s$. Since $\eta_n \in \mathbf{F}_\ell$, we have $\text{Tr}_{K/\mathbf{F}_\ell}(\eta_n) = \eta_n$ and

$$e_{\chi^j} = \frac{1}{3^n} \sum_{i=0}^{3^n-1} \eta_n^{ij} \rho^i.$$

Let g_ℓ be a primitive root of ℓ and fix integers a_{ij} satisfying

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{3^n}ij} \pmod{\ell}.$$

There are $2 \cdot 3^{n-1}$ injective characters of Δ_n and none of them is conjugate over \mathbf{F}_ℓ . If we put

$$X = \{j \in \mathbf{Z} \mid 1 \leq j < 3^n, (j, 3) = 1\},$$

then $\{\chi^j \mid j \in X\}$ is the set of all injective characters of Δ_n . Then Lemma 4 implies the following criterion.

CRITERION 1. Put $b = 4$. If there exists a prime number p which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies

$$\left(\prod_{i=0}^{3^n-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p} \quad \text{for each } j \in X,$$

then ℓ does not divide h_n/h_{n-1} .

3.2. The case $\ell \equiv 1 \pmod{3}$ and $s+1 \leq n$. We have $[K : \mathbf{F}_\ell] = 3^{n-s}$. The minimal polynomial of η_n over \mathbf{F}_ℓ is

$$X^{3^{n-s}} - \eta_n^{3^{n-s}}.$$

Therefore $\text{Tr}_{K/\mathbf{F}_\ell}(\eta_n^i) = 0$ if i is not divisible by 3^{n-s} . Hence we have

$$e_{\chi^j} = \frac{1}{3^n} \sum_{i=0}^{3^s-1} \text{Tr}_{K/\mathbf{F}_\ell}(\eta_n^{3^{n-s}ij}) \rho^{3^{n-s}i}$$

$$= \frac{1}{3^s} \sum_{i=0}^{3^s-1} \eta_s^{ij} \rho^{3^{n-s}i}.$$

Since there are $2 \cdot 3^{s-1}$ non-conjugate primitive 3^n -th roots of unity in $\overline{\mathbf{F}}_\ell$, there are the same number of \mathbf{F}_ℓ -conjugacy classes of injective characters of Δ_n . In this case, we put

$$X = \{j \in \mathbf{Z} \mid 1 \leq j < 3^s, (j, 3) = 1\}.$$

Then $\{\chi^j \mid j \in X\}$ is a set of representatives of \mathbf{F}_ℓ -conjugacy classes of injective characters of Δ_n .

Let g_ℓ be a primitive root of ℓ and fix integers a_{ij} satisfying

$$a_{ij} \equiv g_\ell^{\frac{\ell-1}{3^s}ij} \pmod{\ell}.$$

CRITERION 2. Put $b = 4^{3^{n-s}}$. If there exists a prime number p which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies

$$\left(\prod_{i=0}^{3^s-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p} \quad \text{for each } j \in X,$$

then ℓ does not divide h_n/h_{n-1} .

3.3. The case $\ell \equiv -1 \pmod{3}$ and $2 \leq n \leq s$. We have $[K : \mathbf{F}_\ell] = 2$. Since there are 3^{n-1} non-conjugate primitive 3^n -th roots of unity in $\overline{\mathbf{F}}_\ell$, there are the same number of \mathbf{F}_ℓ -conjugacy classes of injective characters of Δ_n . In this case, we put

$$X = \left\{ j \in \mathbf{Z} \mid 1 \leq j \leq \frac{3^n-1}{2}, (j, 3) = 1 \right\}.$$

Then $\{\chi^j \mid j \in X\}$ is a set of representatives of \mathbf{F}_ℓ -conjugacy classes of injective characters of Δ_n .

In this case, we have

$$\begin{aligned} e_{\chi^j} &= \frac{1}{3^n} \sum_{i=0}^{3^n-1} \text{Tr}_{K/\mathbf{F}_\ell}(\eta_n^{ij}) \rho^i \\ &= \frac{1}{3^n} \sum_{i=0}^{3^n-1} \text{Tr}_{\mathbf{F}_\ell(\eta_s)/\mathbf{F}_\ell}(\eta_s^{3^{s-n}ij}) \rho^i. \end{aligned}$$

Fix integers a_{ij} satisfying

$$a_{ij} \equiv t_{3^s-n}ij \pmod{\ell},$$

where t_i is the element of \mathbf{F}_ℓ defined by (2) in 3.4.

CRITERION 3. Put $b = 4$. If there exists a prime number p which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies

$$\left(\prod_{i=0}^{3^n-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p} \quad \text{for each } j \in X,$$

then ℓ does not divide h_n/h_{n-1} .

3.4. The case $\ell \equiv -1 \pmod{3}$ and $s + 1 \leq n$. We have $[K : \mathbf{F}_\ell] = 2 \cdot 3^{n-s}$. Let

$$X^2 - aX + 1$$

be the minimal polynomial of η_s over \mathbf{F}_ℓ . Then the minimal polynomial of η_n over \mathbf{F}_ℓ is

$$X^{2 \cdot 3^{n-s}} - aX^{3^{n-s}} + 1.$$

therefore $\text{Tr}_{K/\mathbf{F}_\ell}(\eta_n^i) = 0$ if i is not divisible by 3^{n-s} . Hence we have

$$\begin{aligned} e_{\chi^j} &= \frac{1}{3^n} \sum_{i=0}^{3^s-1} \text{Tr}_{K/\mathbf{F}_\ell}(\eta_n^{3^{n-s}ij}) \rho^{3^{n-s}i} \\ &= \frac{1}{3^s} \sum_{i=0}^{3^s-1} \text{Tr}_{\mathbf{F}_\ell(\eta_s)/\mathbf{F}_\ell}(\eta_s^{ij}) \rho^{3^{n-s}i}. \end{aligned}$$

We need to calculate

$$t_i = \text{Tr}_{\mathbf{F}_\ell(\eta_s)/\mathbf{F}_\ell}(\eta_s^i). \tag{2}$$

We start from $t_1 = \eta_s + \eta_s^{-1}$ and proceed to

$$\begin{aligned} t_3 &= \eta_s^3 + \eta_s^{3\ell} = (\eta_s + \eta_s^\ell)^3 - 3\eta_s^{(\ell+1)}(\eta_s + \eta_s^\ell) = t_1^3 - 3t_1 \\ t_{3^2} &= \eta_s^{3^2} + \eta_s^{3^2\ell} = (\eta_s^3 + \eta_s^{3\ell})^3 - 3\eta_s^{3(\ell+1)}(\eta_s^3 + \eta_s^{3\ell}) = t_3^3 - 3t_3 \\ &\vdots \\ t_{3^{s-1}} &= \eta_s^{3^{s-1}} + \eta_s^{3^{s-1}\ell} = t_{3^{s-2}}^3 - 3t_{3^{s-2}} = -1, \end{aligned}$$

noting $\eta_s^{\ell+1} = 1$. Reversing this procedure, we obtain t_1 recursively.

LEMMA 5. Let $b_1 = -1 \in \mathbf{F}_\ell$. If $s \geq 2$, we choose $b_i \in \mathbf{F}_\ell$ ($2 \leq i \leq s$) by

$$b_{i+1}^3 - 3b_{i+1} = b_i.$$

Then we have $t_1 = b_s$.

REMARK. For each step, we have three roots. Hence we have just $3^{s-1} t_1$ which correspond to 3^{s-1} non-conjugate primitive 3^s -th roots of unity in $\overline{\mathbf{F}_\ell}$. We fix arbitrary one.

We obtain t_i ($2 \leq i \leq 3^s - 1$) from $t_0 = 2$ and t_1 using the following recurrence formula.

LEMMA 6. *There holds $t_{i+2} = t_{i+1}t_1 - t_i$.*

PROOF. We have

$$\begin{aligned} t_1 t_{i+1} &= (\eta_s + \eta_s^\ell)(\eta_s^{i+1} + \eta_s^{(i+1)\ell}) \\ &= \eta_s^{i+2} + \eta_s^{(i+2)\ell} + \eta_s^{i+\ell+1} + \eta_s^{i\ell+\ell+1} \\ &= (\eta_s^{i+2} + \eta_s^{(i+2)\ell}) + \eta_s^{\ell+1}(\eta_s^i + \eta_s^{i\ell}) \\ &= t_{i+2} + t_i. \end{aligned}$$

□

Since there are 3^{s-1} non-conjugate primitive 3^n -th roots of unity in $\overline{\mathbf{F}}_\ell$, there are the same number of \mathbf{F}_ℓ -conjugacy classes of injective characters of Δ_n . In this case, we put

$$X = \{j \in \mathbf{Z} \mid 1 \leq j \leq \frac{3^s - 1}{2}, (j, 3) = 1\}.$$

Then $\{\chi^j \mid j \in X\}$ is a set of representatives of \mathbf{F}_ℓ -conjugacy classes of injective characters of Δ_n . We fix integers a_{ij} satisfying

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

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

CRITERION 4. Put $b = 4^{3^{n-s}}$. If there exists a prime number p which is congruent to 1 modulo $3^{n+1}\ell$ and satisfies

$$\left(\prod_{i=0}^{3^s-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{p} \quad \text{for each } j \in X,$$

then ℓ does not divide h_n/h_{n-1} .

References

- [1] T. FUKUDA and K. KOMATSU, Weber's Class Number Problem in the Cyclotomic \mathbf{Z}_2 -Extension of \mathbf{Q} , to appear in Experiment. Math.
- [2] M. AOKI and T. FUKUDA, An Algorithm for Computing p -Class Groups of Abelian Number Fields, Algorithmic Number Theory, 56–71, Lecture Notes in Computer Science, vol. 4076, Springer, Berlin, 2006.
- [3] K. HORIE, Certain Primary Components of the Ideal Class Group of the \mathbf{Z}_p -Extension over the Rationals, Tohoku Math. J. **59** (2007), 259–291.
- [4] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.
- [5] F. J. VAN DER LINDEN, Class Number Computations of Real Abelian Number Fields, Math. Comp. **39** (1982), 693–707.
- [6] J. M. MASLEY, Class numbers of real cyclic number fields with small conductor, Compositio Math. **37** (1978), 297–319.

- [7] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, 2nd edition, Graduate Texts in Math. 83, Springer-Verlag, New York, Heidelberg, Berlin, 1997.

Present Address:

DEPARTMENT OF MATHEMATICS, SCHOOL OF SCIENCE AND ENGINEERING,
WASEDA UNIVERSITY,
OKUBO, SHINJUKU, TOKYO, 169-8555 JAPAN.
e-mail: da-vinci-0415@moegi.waseda.jp