Tohoku Math. J.
61 (2009), 551–570

THE IDEAL CLASS GROUP OF THE Z_p-EXTENSION OVER THE RATIONALS

KUNIAKI HORIE AND MITSUKO HORIE

(Received November 4, 2008, revised July 27, 2009)

Abstract. For any prime number p, we study local triviality of the ideal class group of the $\boldsymbol{Z}_p$-extension over the rational field. We improve a known general result in such study by modifying the proof of the result, and pursue known effective arguments on the above triviality with the help of a computer. Some explicit consequences of our investigations are then provided in the case $p \leq 7$.

Introduction. Let p be any prime number. Let $\boldsymbol{Z}_p$ denote the ring of p-adic integers, and $\boldsymbol{B}_\infty$ the $\boldsymbol{Z}_p$-extension over the rational number field $\boldsymbol{Q}$, namely, the unique abelian extension over $\boldsymbol{Q}$ contained in the complex number field $\boldsymbol{C}$ such that the Galois group $\mathrm{Gal}(\boldsymbol{B}_\infty/\boldsymbol{Q})$ is topologically isomorphic to the additive group of $\boldsymbol{Z}_p$. Let

$$q = p \quad \text{or} \quad q = 4$$

according to whether $p > 2$ or $p = 2$. We denote by $\boldsymbol{P}_\infty$ the composite, in $\boldsymbol{C}$, of cyclotomic fields of p^ath roots of unity for all positive integers a, i.e., $\boldsymbol{P}_\infty = \boldsymbol{B}_\infty(e^{2\pi i/q})$. Given any prime number l different from p, let F be the decomposition field of l for the abelian extension $\boldsymbol{P}_\infty/\boldsymbol{Q}$. For each positive integer b, let

$$\xi_b = e^{2\pi i/p^b}\,.$$

It follows that $\boldsymbol{P}_\infty/F(\xi_1)$ is a $\boldsymbol{Z}_p$-extension. We take a unique positive integer ν such that

$$F \subseteq \boldsymbol{Q}(\xi_\nu) \quad \text{and} \quad [\boldsymbol{Q}(\xi_\nu) : F] \mid \varphi(q)\,,$$

where φ denotes the Euler function. Note that $\nu \geq 2$ if $p = 2$. Let $\mathfrak{O}$ denote the ring of algebraic integers in F, and $\boldsymbol{Z}$ the ring of (rational) integers. Let S be the minimal set of non-negative integers less than $\varphi(p^\nu) = p^{\nu-1}(p-1)$ such that

$$\mathfrak{O} \subseteq \sum_{m \in S} \boldsymbol{Z}\xi_\nu^m\,.$$

Evidently, S is not empty, i.e., $0 < |S| \leq \varphi(p^\nu)$. Denoting by D the absolute value of the discriminant of F, put

$$\Theta = \sqrt{D}\left(\frac{[F:\boldsymbol{Q}]}{p^\nu \log 2}\sum_{m\in S}\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m/p^{\nu-1}]+1})\xi_\nu^{-m})\|\right)^{[F:\boldsymbol{Q}]}\,;$$

2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R18, 11R20, 11R23.
Key words and phrases. Ideal class group, $\boldsymbol{Z}_p$-extension.

here, for each finite extension K'/K of subfields of $\boldsymbol{C}$, $T_{K'/K}$ denotes the trace map from K' to K, for each algebraic number θ in $\boldsymbol{C}$, $\|\theta\|$ denotes the maximum of the absolute values of all conjugates of θ over $\boldsymbol{Q}$, and for each real number x, $[x]$ denotes as usual the maximal integer at most equal to x. Now, take any cyclic group Γ of order p^ν, and a generator γ of Γ; $\Gamma = \{\gamma^m\, ;\ m \in \boldsymbol{Z},\ 0 \le m < p^\nu\}$. Let S^* denote the minimal set of non-negative integers less than p^ν such that, in the group ring of Γ over $\boldsymbol{Z}$,

$$(1-\gamma^{p^{\nu-1}})\sum_{m\in S} b_m\gamma^m \in \sum_{w\in S^*} \boldsymbol{Z}\gamma^w$$

for every sequence $\{b_m\}_{m\in S}$ of integers with $\sum_{m\in S} b_m\xi_\nu^m \in \mathfrak{O}$. We easily see that S^* does not depend on the choice of Γ or γ. Further, it follows that $0 < |S^*| \le p^\nu$. Let N denote the set of positive integers n which satisfy

$$p^n \ge \frac{p^{2\nu-1}}{q}\,, \quad \frac{2(qp^{n-\nu})^{1/\varphi(p-1)}}{\varphi(q)|S^*|} < \Theta\left(\frac{\varphi(q)}{2}\log\left(\frac{qp^n}{\pi}\sin\frac{\pi}{p}+\cos\frac{\pi}{p}\right)\right)^{[F:\boldsymbol{Q}]}.$$

Clearly, q divides $p^{2\nu-1}$, and N is a finite set. When $N \ne \emptyset$, we define n_0 to be the maximal integer in N; when $N = \emptyset$, we define an integer $n_0 \ge 0$ by $p^{n_0} = p^{2\nu-1}/q$. For each integer $a \ge 0$, let $\boldsymbol{B}_a$ denote the subfield of $\boldsymbol{B}_\infty$ with degree p^a, and h_a the class number of $\boldsymbol{B}_a$. In this paper, we first prove the following result after some preliminaries.

THEOREM 1. *Assume that $l \nmid h_{\nu-1}$. Then the l-class group of $\boldsymbol{B}_\infty$ is trivial if*

$$l \nmid h_{n_0} \quad or \quad l \ge \Theta\left(\frac{\varphi(q)}{2}\log\left(\frac{qp^{n_0}}{\pi}\sin\frac{\pi}{p}+\cos\frac{\pi}{p}\right)\right)^{[F:\boldsymbol{Q}]}.$$

The proof of the above theorem is based essentially upon arithmetic study in [3, 5] on an algebraic interpretation of the analytic class number formula. The theorem actually improves a main result of [5] in general, while more precise results for certain specific cases are obtained in [4, 6] by pursuing several arguments of [3, 5]. We should add that the p-class group of $\boldsymbol{B}_\infty$ is trivial (cf. Iwasawa [9]). Here we make some corrections for [3, 5]. Insead of defining $f(\chi, u)$ by [3, l. 19 on p. 258], one should define $f(\chi, u)$ as the maximal divisor of $f(\chi)$ relatively prime to u, with the notation $\tilde{u}$ retained; furthermore, "$q_0 = \gcd(q, 2t)$" in [3, l. 3 on p. 260], "$f' = f(\psi_2^d)$" in [3, l. 6 on p. 260] and "$\psi_2^d(b) = 1$" in [3, l. 11 on p. 260] should be "$q_0 = f(\psi_2)/t$", "$f(\psi_2^d) \mid f'$" and "$\psi_2(b)^d = 1$", respectively. Also, "$\tan(\pi/2p^\nu)$" in [5, l. 1 on p. 393] should be "$\tan(\pi/(2p^\nu))$" and "element" in [5, l. 5 on p. 393] should be "elements"; for other corrections, see [7, pp. 822, 823], and [8, p. 180].

It is shown in [3, 6] that, if $p = 3$ and l is congruent to either 2, 4, 5 or 7 modulo 9, then the l-class group of $\boldsymbol{B}_\infty$ is trivial. Theorem 1 implies the following result among others.

PROPOSITION 1. *Assume that $p = 3$ and that $l \equiv 8 \pmod{27}$ or $l \equiv 17 \pmod{27}$. If $l \nmid h_{18}$ or $l > 34681575$, then the l-class group of $\boldsymbol{B}_\infty$ is trivial.*

It is shown in [6] that, if $p = 2$ and if $l \equiv 3 \pmod 8$ or $l \equiv 5 \pmod 8$, then the l-class group of $\boldsymbol{B}_\infty$ is trivial. Theorem 1 also implies the following two results.

PROPOSITION 2. *Assume that* $p = 2$, $l \equiv 9 \pmod{16}$, *and either* $l \nmid h_{36}$ *or* $l > 7150001069$. *Then the* l*-class group of* $\boldsymbol{B}_\infty$ *is trivial.*

PROPOSITION 3. *Assume that* $p = 2$, $l \equiv 7 \pmod{16}$, *and either* $l \nmid h_{39}$ *or* $l > 17324899980$. *Then the* l*-class group of* $\boldsymbol{B}_\infty$ *is trivial.*

In the latter part of the paper, we deduce the following theorem from several results of [6] with the help of a (personal) computer.

THEOREM 2. *Assume that* $p = 5$ *and that*

$$l \equiv g \pmod{25} \quad \textit{for some} \;\; g \in \{2, 3, 4, 8, 9, 12, 13, 14, 17, 19, 22, 23\}\,.$$

Then the l*-class group of* $\boldsymbol{B}_\infty$ *is trivial.*

As to the case where

$$l \equiv g \pmod{25} \quad \text{for some} \;\; g \in \{2, 3, 8, 12, 13, 17, 22, 23\}\,,$$

the above result is already shown in [4]. The final result of the present paper is as follows.

THEOREM 3. *Assume that* $p = 7$ *and that* $l \equiv g \pmod{49}$ *for some integer* g *in*

$$\{2, 3, 4, 5, 9, 10, 11, 12, 16, 17, 23, 24, 25, 26, 32, 33, 37, 38, 39, 40, 44, 45, 46, 47\}\,.$$

Then the l*-class group of* $\boldsymbol{B}_\infty$ *is trivial.*

The proof of this theorem also needs a computer as well as several results of [6]. The theorem is already proved in [4] for the case where

$$l \equiv g \pmod{49} \quad \text{with some} \;\; g \in \{3, 5, 10, 12, 17, 24, 26, 33, 38, 40, 45, 47\}\,.$$

We conclude the present introduction with an optimistic remark. Recently, in the case $p = 2$, Fukuda and Komatsu [1] established a criterion for checking the triviality of the l-class group of $\boldsymbol{B}_\infty$ and, as a consequence, verified that the l-class group of $\boldsymbol{B}_\infty$ is trivial whenever $l < 10^7$. In view of the arguments of [1], it might be possible to improve the propositions stated above. For example, in Proposition 1, there is a possibility of knowing whether the condition that $l \nmid h_{18}$ or $l > 34681575$ is omitted, namely, whether one always has $l \nmid h_{18}$ in the case $l < 34681575$ (for slight improvements, cf. Remarks 1 and 2 in Section 2).

1. Some Lemmas. Let n be any positive integer, which will be fixed in the rest of the paper. Let E denote the group of all units of $\boldsymbol{B}_n$. In the case $p > 2$, we put

$$\eta = \prod_u \frac{\xi_{n+1}^{u} - \xi_{n+1}^{-u}}{\xi_1^u \xi_{n+1}^{u} - \xi_1^{-u} \xi_{n+1}^{-u}} = \prod_u \frac{\sin(2\pi u / p^{n+1})}{\sin(2\pi u (1 + p^n)/p^{n+1})}\,,$$

where u ranges over the positive integers such that

$$u^{p-1} \equiv 1 \pmod{p^{n+1}}\,, \quad u < p^{n+1}/2\,;$$

in the case $p = 2$, we put

$$\eta = \frac{\xi_{n+3} - \xi_{n+3}^{-1}}{i\xi_{n+3} + i\xi_{n+3}^{-1}} = \tan \frac{\pi}{2^{n+2}} .$$

Not only η belongs to E by definition, but also η is a typical example of what is called a circular (or cyclotomic) unit of $\boldsymbol{B}_n$. Let $\mathfrak{R}$ denote the group ring of $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q})$ over $\boldsymbol{Z}$. Naturally, the multiplicative group $\boldsymbol{B}_n^\times$ becomes an $\mathfrak{R}$-module and E an $\mathfrak{R}$-submodule of $\boldsymbol{B}_n^\times$. Now, take an algebraic integer α in $\boldsymbol{Q}(\xi_n)$. Then α is uniquely expressed in the form

$$\alpha = \sum_{m=0}^{\varphi(p^n)-1} a_m \xi_n^m , \quad a_0, \dots, a_{\varphi(p^n)-1} \in \boldsymbol{Z} .$$

For each $\rho \in \mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q})$, we define an element α_ρ of $\mathfrak{R}$ by

$$\alpha_\rho = \sum_{m=0}^{\varphi(p^n)-1} a_m \rho^m .$$

We note as well that h_{n-1} divides h_n, i.e., h_n/h_{n-1} is an integer; indeed this fact follows from class field theory since the prime ideal of $\boldsymbol{B}_{n-1}$ dividing p is totally ramified in $\boldsymbol{B}_n$.

LEMMA 1. *Assume that $n \geq \nu$ and l divides h_n/h_{n-1}. Then*

$$l < \Theta\left(\frac{\varphi(q)}{2} \log\left(\frac{qp^n}{\pi} \sin\frac{\pi}{p} + \cos\frac{\pi}{p}\right)\right)^{[F:\boldsymbol{Q}]} .$$

PROOF. Let σ be a generator of the cyclic group $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q})$. As [5, Lemma 2] implies by the assumption that l divides h_n/h_{n-1}, there exists a prime ideal $\mathfrak{l}$ of F dividing l such that, for any $\beta \in l\mathfrak{l}^{-1}$, η^{β_σ} is an lth power in E. Since the norm of $l\mathfrak{l}^{-1}$ for $F/\boldsymbol{Q}$ is $l^{[F:\boldsymbol{Q}]-1}$, Minkowski's lattice theorem shows that

$$\|\alpha\| \leq (\sqrt{D} l^{[F:\boldsymbol{Q}]-1})^{1/[F:\boldsymbol{Q}]} \quad \text{with some } \alpha \in l\mathfrak{l}^{-1} \setminus \{0\} . \tag{1}$$

There also exist integers a_m for all $m \in S$ which satisfy

$$\alpha = \sum_{m \in S} a_m \xi_\nu^m . \tag{2}$$

Now, given any $m' \in S$, let $S' = \{m \in S ; m \equiv m' \pmod{p^{\nu-1}}\}$. We then see, for any $m \in S'$, that $m \equiv m' \pmod{p^\nu}$ if and only if $m = m'$ and that

$$0 < m - m' + ([m'/p^{\nu-1}] + 1)p^{\nu-1} < p^\nu .$$

Furthermore, for any integer w, we find $T_{\boldsymbol{Q}(\xi_\nu)/\boldsymbol{Q}}(\xi_\nu^w)$ to be either $\varphi(p^\nu)$, $-p^{\nu-1}$ or 0 according to whether the highest power of p dividing w is either greater than $p^{\nu-1}$, equal to $p^{\nu-1}$ or smaller than $p^{\nu-1}$. It therefore follows from (2) that

$$\begin{aligned} &T_{\boldsymbol{Q}(\xi_\nu)/\boldsymbol{Q}}((1 - \xi_1^{[m'/p^{\nu-1}]+1})\xi_\nu^{-m'}\alpha) \\ &\quad = \sum_{m \in S'} a_m T_{\boldsymbol{Q}(\xi_\nu)/\boldsymbol{Q}}(\xi_\nu^{m-m'}) - \sum_{m \in S'} a_m T_{\boldsymbol{Q}(\xi_\nu)/\boldsymbol{Q}}(\xi_\nu^{m-m'+([m'/p^{\nu-1}]+1)p^{\nu-1}}) = p^\nu a_{m'} . \end{aligned}$$

Hence

$$\begin{aligned}|a_{m'}| &= \frac{1}{p^\nu}|T_{F/\boldsymbol{Q}}(T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m'/p^{\nu-1}]+1})\xi_\nu^{-m'})\alpha)| \\ &\le \frac{[F:\boldsymbol{Q}]}{p^\nu}\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m'/p^{\nu-1}]+1})\xi_\nu^{-m'})\|\|\alpha\|\end{aligned}$$

so that, by (1),

$$|a_{m'}| \le \frac{[F:\boldsymbol{Q}]}{p^\nu}(\sqrt{D}l^{[F:\boldsymbol{Q}]-1})^{1/[F:\boldsymbol{Q}]}\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m'/p^{\nu-1}]+1})\xi_\nu^{-m'})\|\,.$$

However, (2) implies that

$$\alpha_\sigma = \sum_{m\in S} a_m \sigma^{p^{n-\nu}m} \quad \text{in } \mathfrak{R}\,,$$

and hence

$$\|\eta^{\alpha_\sigma}\| \le \max(\|\eta\|, \|\eta^{-1}\|)^{\sum_{m\in S}|a_m|}\,.$$

Therefore, putting $L=\log(\max(\|\eta\|,\|\eta^{-1}\|))$, we have

$$\log\|\eta^{\alpha_\sigma}\| \le \frac{[F:\boldsymbol{Q}]L}{p^\nu}(\sqrt{D}l^{[F:\boldsymbol{Q}]-1})^{1/[F:\boldsymbol{Q}]}\sum_{m\in S}\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m/p^{\nu-1}]+1})\xi_\nu^{-m})\|\,.$$

On the other hand, as in the proof of [5, Lemma 6], [5, Lemma 3] gives

$$l\log 2 < \log\|\eta^{\alpha_\sigma}\|\,.$$

Thus

$$\left(\frac{l}{\sqrt{D}}\right)^{1/[F:\boldsymbol{Q}]} < \frac{[F:\boldsymbol{Q}]L}{p^\nu\log 2}\sum_{m\in S}\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m/p^{\nu-1}]+1})\xi_\nu^{-m})\|\,.$$

Since

$$L < \frac{\varphi(q)}{2}\log\left(\frac{qp^n}{\pi}\sin\frac{\pi}{p}+\cos\frac{\pi}{p}\right)$$

by [5, Lemma 4], we then obtain the inequality to be proved. □

In the case $p>2$, let v be the number of distinct prime divisors of $(p-1)/2$, let $g_1,\dots,g_v$ be the prime-powers greater than 1 such that

$$\frac{p-1}{2} = g_1\cdots g_v\,,$$

and let V denote the subset of the cyclic group $\langle e^{2\pi i/(p-1)}\rangle$ consisting of

$$e^{\pi i z_1/g_1}\cdots e^{\pi i z_v/g_v}$$

for all v-tuples $(z_1,\dots,z_v)$ of integers with $0\le z_1<g_1,\dots,0\le z_v<g_v$. We understand that $V=\{1\}$ if $p=3$. In the case $p=2$, we put $V=\{1\}$. It follows that V is a complete set

of representatives of the factor group $\langle e^{2\pi i/\varphi(q)}\rangle/\langle -1\rangle$. Let Φ denote the set of maps from V to $\{u \in \boldsymbol{Z}\,;\ 0 \le u \le |S^*|l\}$. We put

$$M = \max_{\psi\in\Phi}\left|\mathfrak{N}\left(\sum_{\delta\in V}\psi(\delta)\delta - 1\right)\right|,$$

where $\mathfrak{N}$ denotes the norm map from $\boldsymbol{Q}(e^{2\pi i/(p-1)})$ to $\boldsymbol{Q}$. Next, let $\mathfrak{p}$ be a prime ideal of $\boldsymbol{Q}(e^{2\pi i/(p-1)})$ dividing p. Let I denote the set of positive integers smaller than qp^n and congruent to suitable elements of V modulo $\mathfrak{q}\mathfrak{p}^n$. Here

$$\mathfrak{q} = \mathfrak{p} \quad \text{or} \quad \mathfrak{q} = \mathfrak{p}^2$$

according to whether $p > 2$ or $p = 2$. Since the degree of $\mathfrak{p}$ is 1 and $\langle e^{2\pi i/(p-1)}\rangle \cup \{0\}$ is a complete set of representatives of the residue ring $\boldsymbol{Z}[e^{2\pi i/(p-1)}]/\mathfrak{p}$, each $\varepsilon \in V$ gives a unique $u \in I$ with $u \equiv \varepsilon \pmod{\mathfrak{q}\mathfrak{p}^n}$ and the map $\varepsilon \mapsto u$ defines a bijection from V to I. Note that I contains 1. For each pair (m, u) in $S^* \times I$, let $\mathfrak{G}_{m,u}$ denote the set of maps $j : S^* \times I \to \boldsymbol{Z}$ such that $\min(l-2, 1) \le j(m,u) < l$ and $j(m', u') \in \{0, l\}$ for every (m', u') in $S^* \times I \setminus \{(m,u)\}$. We then let

$$\mathfrak{H} = \bigcup_{(m,u)\in S^*\times I} \mathfrak{G}_{m,u}\,.$$

In the case $n \ge \nu$, putting $r = 1 + qp^{n-\nu}$, we define

$$A(j) = \sum_{m\in S^*}\sum_{u\in I} ur^m j(m,u)$$

for each $j \in \mathfrak{H}$, whence

$$A(j) \equiv \sum_{m\in S^*}\sum_{u\in I} uj(m,u) \pmod{qp^{n-\nu}}\,.$$

LEMMA 2. *Assume that $M < qp^{n-\nu}$ and $n \ge \nu$. Take a map j in $\mathfrak{H}$. Then the condition*

$$A(j) \equiv |S^*|l\sum_{u\in I} u - 1 \pmod{qp^{n-\nu}}$$

is equivalent to the condition that

$$j(w,1) = l-1\,, \quad j(m,u) = l$$

for some $w \in S^*$ and every $(m,u) \in S^* \times I \setminus \{(w,1)\}$.

PROOF. The latter condition clearly implies the former. Let us consider the case where $j \in \mathfrak{G}_{w,u_0}$ with $(w, u_0) \in S^* \times I$, under the former condition which can be written as

$$\sum_{u\in I}\left(\sum_{m\in S^*}(l - j(m,u))\right)u - 1 \equiv 0 \pmod{qp^{n-\nu}}\,.$$

In virtue of the bijection $V \to I$ defined above, there exists a unique $\psi \in \Phi$ such that

$$\psi(\varepsilon) = \sum_{m\in S^*}(l - j(m,u))$$

for every $(\varepsilon, u) \in V \times I$ with $\varepsilon \equiv u \pmod{\mathfrak{q}\mathfrak{p}^n}$. We then obtain

$$\sum_{\varepsilon \in V} \psi(\varepsilon)\varepsilon - 1 \equiv 0 \pmod{\mathfrak{q}\mathfrak{p}^{n-\nu}}.$$

This yields

$$\mathfrak{N}\Big(\sum_{\varepsilon \in V} \psi(\varepsilon)\varepsilon - 1\Big) \equiv 0 \pmod{qp^{n-\nu}}.$$

Hence it follows from the assumption $M < qp^{n-\nu}$ that

$$\mathfrak{N}\Big(\sum_{\varepsilon \in V} \psi(\varepsilon)\varepsilon - 1\Big) = 0, \quad \text{i.e.,} \quad \sum_{\varepsilon \in V} \psi(\varepsilon)\varepsilon - 1 = 0.$$

Therefore, by [3, Lemma 7], $\psi(1) = 1$ and $\psi(\varepsilon) = 0$ for all ε in $V \setminus \{1\}$. In particular, we have $u_0 = 1$. We thus find that $j(w, 1) = l - 1$ and $j(m, u) = l$ for all (m, u) in $S^* \times I \setminus \{(w, 1)\}$. □

For each $(m, u) \in S^* \times I$ and each $j \in \mathfrak{G}_{m,u}$, we define an integer $B(j)$ by

$$B(j) = \sum_{(m',u')} \left(1 - \frac{j(m', u')}{l}\right),$$

where (m', u') runs through $S^* \times I \setminus \{(m, u)\}$. This notation will be used in the proof of the following lemma.

LEMMA 3. *Assume that l divides h_n/h_{n-1} and $p^{2\nu}$ divides qp^n. Then*

$$qp^{n-\nu} \leq M.$$

PROOF. The assumption $p^{2\nu} \mid qp^n$ yields

$$n \geq \nu, \quad qp^n \mid (qp^{n-\nu})^2.$$

By the above divisibility, we have

$$r^a \equiv 1 + aqp^{n-\nu} \pmod{qp^n} \tag{3}$$

for every $a \in \boldsymbol{Z}$. Put $\zeta = e^{2\pi i/(qp^n)}$, namely, put

$$\zeta = \xi_{n+1} \quad \text{or} \quad \zeta = \xi_{n+2}$$

according to whether $p > 2$ or $p = 2$. Let s be an integer such that

$$s^{p^{n-\nu}} \equiv r \pmod{qp^n},$$

and let σ be the automorphism of $\boldsymbol{Q}(\zeta)$ mapping ζ to ζ^s. When there is no risk of confusion, we identify $\mathfrak{R}$ with the group ring of $\mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(e^{2\pi i/q}))$ over $\boldsymbol{Z}$ through the natural identification

$$\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q}) = \mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q}(e^{2\pi i/q})) = \langle \sigma \rangle.$$

As [5, Lemma 2] shows under our hypothesis, there exists a prime ideal $\mathfrak{l}$ of $\boldsymbol{Q}(\xi_\nu)$ dividing l such that η^{β_σ} is an lth power in E for every $\beta \in l\mathfrak{l}^{-1}$. Let α be any algebraic integer which is not divisible by l but divisible by $l\mathfrak{l}^{-1}$. Let $\tau = \sigma^{p^{n-1}}$. The definition of S^* then enables us to take the integers a_m, $m \in S^*$, satisfying

$$(1-\tau)\alpha_\sigma = \sum_{m \in S^*} a_m \sigma^{p^{n-\nu} m}\,.$$

It follows that

$$(1-\xi_1)\alpha = \sum_{m \in S^*} a_m \xi_\nu^m\,. \tag{4}$$

In the case $p > 2$, since the disjoint union of I and $\{p^{n+1} - u\,;\ u \in I\}$ is just the set of positive integers $u < p^{n+1}$ satisfying $u^{p-1} \equiv 1 \pmod{p^{n+1}}$ and since $\zeta^\tau = \zeta^{1+p^n} = \xi_1\zeta$, we obtain

$$\eta = \prod_{u \in I} (\zeta^u - \zeta^{-u})^{1-\tau} = \prod_{u \in I} \xi_1^u (\zeta^{2u} - 1)^{1-\tau}\,,$$

so that, by the definition of σ,

$$\eta^{\alpha_\sigma} = \xi_1^{\alpha_\sigma \sum_{u \in I} u} \prod_{m \in S^*} \prod_{u \in I} (\zeta^{2ur^m} - 1)^{a_m}\,.$$

In the case $p = 2$,

$$\eta = i(\zeta - 1)^{1-\tau}\,, \quad \text{whence} \quad \eta^{\alpha_\sigma} = i^{\alpha_\sigma} \prod_{m \in S^*} (\zeta^{r^m} - 1)^{a_m}\,.$$

Consequently, we always find that

$$\prod_{m \in S^*} \prod_{u \in I} (\zeta^{ur^m} - 1)^{a_m}$$

is an lth power in $\mathbf{Z}[\zeta]$. Hence, in $\mathbf{Z}[\zeta]$, [3, Lemma 5] yields

$$\prod_{m \in S^*} \prod_{u \in I} (\zeta^{lur^m} - 1)^{a_m} \equiv \prod_{m \in S^*} \prod_{u \in I} (\zeta^{ur^m} - 1)^{a_m l} \pmod{l^2}\,. \tag{5}$$

We add that the both sides above are relatively prime to l.

Next, let y be an indeterminate. Define a polynomial $J(y)$ in $\mathbf{Z}[y]$ by

$$(y-1)^l = y^l - 1 + lJ(y)\,,$$

namely, let

$$J(y) = \sum_{c=1}^{l-1} \frac{(-1)^{c-1}}{l} \binom{l}{c} y^c \quad \text{or} \quad J(y) = -y + 1 \tag{6}$$

according to whether $l > 2$ or $l = 2$. Then, for each $b \in \mathbf{Z}$ and each $b' \in \mathbf{Z}$ with $\zeta^{b'} \neq 1$,

$$(\zeta^{b'} - 1)^{bl} \equiv (\zeta^{lb'} - 1)^{b-1} (\zeta^{lb'} - 1 + blJ(\zeta^{b'})) \pmod{l^2}\,.$$

Therefore, we see from (5) that

$$\prod_{m \in S^*} \prod_{u \in I} (\zeta^{lur^m} - 1) \equiv \prod_{m \in S^*} \prod_{u \in I} (\zeta^{lur^m} - 1 + a_m lJ(\zeta^{ur^m})) \pmod{l^2}\,.$$

This implies that

$$\sum_{m\in S^*}\sum_{u\in I} a_m J(\zeta^{ur^m}) \prod_{(w,u')} (\zeta^{lu'r^w}-1) \equiv 0 \pmod{l},$$

where (w, u') runs through $S^* \times I \setminus \{(m, u)\}$. Furthermore, for each $(m, u) \in S^* \times I$ and each integer c with $\min(l-2, 1) \le c < l$, we have

$$\zeta^{ur^m c} \prod_{(w,u')} (\zeta^{lu'r^w}-1) = \sum_{j'} (-1)^{B(j')} \zeta^{A(j')},$$

the sum taken over all $j' \in \mathfrak{G}_{m,u}$ with $j'(m, u) = c$. Hence, by (6),

$$\sum_{m\in S^*}\sum_{u\in I}\sum_{j\in\mathfrak{G}_{m,u}} (-1)^{B(j)} a_m b_{m,u}(j) \zeta^{A(j)} \equiv 0 \pmod{l}; \tag{7}$$

here, for each $(m, u) \in S^* \times I$ and each $j \in \mathfrak{G}_{m,u}$,

$$b_{m,u}(j) = \frac{(-1)^{j(m,u)-1}}{l}\binom{l}{j(m,u)} \quad \text{or} \quad b_{m,u}(j) = 1$$

according to whether $l > 2$ or $l = 2$.

Now, contrary to the conclusion of the lemma, we suppose that $M < qp^{n-\nu}$. It follows from [3, Lemma 6] that the partial sum in the left-hand side of (7), under the condition

$$A(j) \equiv |S^*| l \sum_{u\in I} u - 1 \pmod{qp^{n-\nu}},$$

is congruent to 0 modulo l. Therefore, by Lemma 2,

$$\sum_{w\in S^*} a_w \zeta^{A_0 - r^w} \equiv 0 \pmod{l}, \quad \text{with } A_0 = \sum_{m\in S^*}\sum_{u\in I} lur^m.$$

Applying complex conjugation to the above congruence, we have

$$\sum_{w\in S^*} a_w \zeta^{r^w} \equiv 0 \pmod{l}.$$

However, (3) gives $\zeta^{r^w} = \zeta\xi_\nu^w$ for every $w \in S^*$. We thus deduce from (4) that

$$(1-\xi_1)\alpha \equiv 0 \pmod{l}, \quad \text{i.e.,} \quad \alpha \equiv 0 \pmod{l}.$$

This contradiction completes the proof of the lemma. □

2. Proofs of Theorem 1 and Propositions. By means of the lemmas in the preceding section, let us prove the former four results stated in the introduction, as follows.

PROOF OF THEOREM 1. For any $\psi \in \Phi$,

$$\left|\mathfrak{N}\Big(\sum_{\delta\in V}\psi(\delta)\delta - 1\Big)\right| = \prod_{\rho}\left|\sum_{\delta\in V}\psi(\delta)\delta^{\rho} - 1\right|,$$

with ρ ranging over all automorphisms of $\boldsymbol{Q}(e^{2\pi i/(p-1)})$, and

$$\left|\sum_{\delta\in V}\psi(\delta)\delta^{\rho}-1\right|\leq|\psi(1)-1|+\sum_{\delta\in V\setminus\{1\}}\psi(\delta)<\frac{\varphi(q)}{2}\cdot|S^*|l\,.$$

Therefore

$$M<\left(\frac{\varphi(q)|S^*|l}{2}\right)^{\varphi(p-1)}.$$

Now assume that the l-class group of $\boldsymbol{B}_\infty$ is not trivial. Since l does not divide $h_{\nu-1}$, it follows that l divides $h_{n'}/h_{n'-1}$ for some positive integer $n'\geq\nu$. In the case where $p^{n'}<p^{2\nu}/q$ so that $n'\leq n_0$, we have $l\mid h_{n_0}$ and Lemma 1 shows that

$$l<\Theta\left(\frac{\varphi(q)}{2}\log\left(\frac{qp^{n'}}{\pi}\sin\frac{\pi}{p}+\cos\frac{\pi}{p}\right)\right)^{[F:\boldsymbol{Q}]}\leq\Theta\left(\frac{\varphi(q)}{2}\log\left(\frac{qp^{n_0}}{\pi}\sin\frac{\pi}{p}+\cos\frac{\pi}{p}\right)\right)^{[F:\boldsymbol{Q}]}.$$

We next consider the case $p^{n'}\geq p^{2\nu}/q$. Together with the above estimate for M, Lemma 3 yields

$$qp^{n'-\nu}<\left(\frac{\varphi(q)|S^*|l}{2}\right)^{\varphi(p-1)},\quad\text{i.e.,}\quad\frac{2(qp^{n'-\nu})^{1/\varphi(p-1)}}{\varphi(q)|S^*|}<l\,.$$

Furthermore, by Lemma 1,

$$l<\Theta\left(\frac{\varphi(q)}{2}\log\left(\frac{qp^{n'}}{\pi}\sin\frac{\pi}{p}+\cos\frac{\pi}{p}\right)\right)^{[F:\boldsymbol{Q}]}.$$

We therefore obtain

$$\frac{2(qp^{n'-\nu})^{1/\varphi(p-1)}}{\varphi(q)|S^*|}<\Theta\left(\frac{\varphi(q)}{2}\log\left(\frac{qp^{n'}}{\pi}\sin\frac{\pi}{p}+\cos\frac{\pi}{p}\right)\right)^{[F:\boldsymbol{Q}]},$$

which means that n' belongs to N. Hence the definition of n_0 implies $n'\leq n_0$, and consequently,

$$l<\Theta\left(\frac{\varphi(q)}{2}\log\left(\frac{qp^{n_0}}{\pi}\sin\frac{\pi}{p}+\cos\frac{\pi}{p}\right)\right)^{[F:\boldsymbol{Q}]},\quad l\mid h_{n_0}\,.\qquad\square$$

The following lemma is useful to continue our proofs.

LEMMA 4. *Let d be any positive divisor of $p-1$.*

(i) *If $p>2$, then F is an extension of $\boldsymbol{B}_{\nu-1}$, the condition $[F:\boldsymbol{B}_{\nu-1}]=d$ is equivalent to the condition that $l\equiv g_0^{p^{\nu-1}d}\pmod{p^{\nu+1}}$ for some primitive root g_0 modulo p^2, and in the case $[F:\boldsymbol{B}_{\nu-1}]=d$,*

$$\Theta=\frac{1}{p^{((p^{\nu-1}-1)d/(p-1)+1)/2}}\left(\frac{p^{\nu/2}d}{\log 2}\sum_{m\in S}\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m/p^{\nu-1}]+1})\xi_\nu^{-m})\|\right)^{p^{\nu-1}d}.$$

(ii) *If $p=2$, then the condtion $F=\boldsymbol{Q}(\xi_\nu)$ is equivalent to the congruence* $l\equiv 1+2^\nu \pmod{2^{\nu+1}}$, *and implies that*

$$\Theta=\frac{2^{3(\nu-1)2^{\nu-2}}}{(\log 2)^{2^{\nu-1}}}.$$

(iii) *If $p=2$, then the three conditions $[\boldsymbol{Q}(\xi_\nu):F]=2$, $F=\boldsymbol{Q}(\xi_\nu-\xi_\nu^{-1})\neq\boldsymbol{Q}(i)$ and $l\equiv -1+2^{\nu-1}\not\equiv 1 \pmod{2^\nu}$ are equivalent, and imply that*

$$\nu\geq 3\,,\quad \Theta=\frac{2^{(\nu-1)2^{\nu-3}-1/2}}{(\log 2)^{2^{\nu-2}}}\left(1+\sum_{u=2}^{\nu-1}2^{u-2}\cos\frac{\pi}{2^u}\right)^{2^{\nu-2}}.$$

PROOF. We omit most part of the proof which follows from the basic theory of cyclotomic fields. When $p>2$ and $[F:\boldsymbol{B}_{\nu-1}]=d$, F is a cyclic extension over $\boldsymbol{Q}$ of degree $p^{\nu-1}d$ with conductor p^ν, so that the conductor-discriminant formula gives

$$D=p^{\nu p^{\nu-1}d-(p^{\nu-1}-1)d/(p-1)-1}.$$

Combining this with the definition of Θ, we obtain the last conclusion of (i).

We next consider the case where $p=2$ and $F=\boldsymbol{Q}(\xi_\nu)$. Since

$$S=\{0,\dots,2^{\nu-1}-1\}\,,\quad \xi_1=-1\,,$$

it follows that

$$\sum_{m\in S}\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m/2^{\nu-1}]+1})\xi_\nu^{-m})\|=2^\nu.$$

We also have $D=2^{(\nu-1)2^{\nu-1}}$. Hence Θ can be expressed as in the assertion (ii).

We finally consider the case where $p=2$, $F=\boldsymbol{Q}(\xi_\nu-\xi_\nu^{-1})\neq\boldsymbol{Q}(i)$, and hence $\nu\geq 3$. It readily follows that $S=\{0,\dots,2^{\nu-1}-1\}\setminus\{2^{\nu-2}\}$. For any $m\in S\setminus\{0\}$,

$$\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m/2^{\nu-1}]+1})\xi_\nu^{-m})\|=2\|\xi_\nu^{-m}+(-1)^m\xi_\nu^m\|\,;$$

further, when m is odd,

$$\|\xi_\nu^{-m}+(-1)^m\xi_\nu^m\|=2\left\|\sin\frac{\pi}{2^{\nu-1}}\right\|=2\sin\frac{(2^{\nu-2}-1)\pi}{2^{\nu-1}}=2\cos\frac{\pi}{2^{\nu-1}}$$

and, when m is even,

$$\|\xi_\nu^{-m}+(-1)^m\xi_\nu^m\|=2\left\|\cos\frac{m\pi}{2^{\nu-1}}\right\|=2\cos\frac{\gcd(m,2^{\nu-1})\pi}{2^{\nu-1}}.$$

Hence

$$\sum_{m\in S}\|T_{\boldsymbol{Q}(\xi_\nu)/F}((1-\xi_1^{[m/2^{\nu-1}]+1})\xi_\nu^{-m})\|=4+\sum_{u=2}^{\nu-1}2^u\cos\frac{\pi}{2^u}.$$

However, since F is a cyclic extension over $\boldsymbol{Q}$ of degree $2^{\nu-2}$ with conductor 2^ν, we have $D=2^{(\nu-1)2^{\nu-2}-1}$. Therefore Θ is expressed as in (iii). □

PROOF OF PROPOSITION 1. By the hypothesis of the proposition, $l \equiv g_0^3 \pmod{3^3}$ for some primitive root g_0 modulo 3^2, so that $F = \boldsymbol{B}_1 = \boldsymbol{Q}(\xi_2 + \xi_2^{-1})$, $\nu = 2$, $[F : \boldsymbol{Q}] = 3$ (cf. Lemma 4), and

$$\mathfrak{O} = \{a_0 + (a_1 - a_2)\xi_2 + (a_2 - a_1)\xi_2^2 - a_2\xi_2^4 - a_1\xi_2^5\,;\ a_0, a_1, a_2 \in \boldsymbol{Z}\}\,.$$

In particular, $S = \{0, 1, 2, 4, 5\}$. Hence

$$\sum_{m\in S} \|T_{\boldsymbol{Q}(\xi_2)/F}((1 - \xi_1^{[m/3]+1})\xi_2^{-m})\|$$
$$= 3 + 2\left\|2\cos\frac{2\pi}{9} - 2\cos\frac{4\pi}{9}\right\| + \left\|2\cos\frac{8\pi}{9} - 2\cos\frac{4\pi}{9}\right\| + \left\|2\cos\frac{10\pi}{9} - 2\cos\frac{2\pi}{9}\right\|\,.$$

It therefore follows that

$$\Theta = \frac{(3 + 8\cos(2\pi/9) - 8\cos(8\pi/9))^3}{3(\log 2)^3}\,.$$

Furthermore, with the same γ as in the introduction, we have

$$\begin{aligned}(1 - \gamma^3)&(a_0 + (a_1 - a_2)\gamma + (a_2 - a_1)\gamma^2 - a_2\gamma^4 - a_1\gamma^5)\\ &= a_0 + (a_1 - a_2)\gamma + (a_2 - a_1)\gamma^2 - a_0\gamma^3 - a_1\gamma^4 - a_2\gamma^5 + a_2\gamma^7 + a_1\gamma^8\end{aligned}$$

for a_0, a_1, a_2 in $\boldsymbol{Z}$. This gives $S^* = \{0, 1, 2, 3, 4, 5, 7, 8\}$. Hence

$$N = \left\{n' \in \boldsymbol{Z}\,;\ n' \geq 2,\ \frac{3^{n'-1}}{8} < \Theta\left(\log\left(\frac{3^{n'+3/2}}{2\pi} + \frac{1}{2}\right)\right)^3\right\} = \{2, \dots, 18\}, \quad n_0 = 18\,.$$

Since h_1 is known to be 1 and

$$\left[\Theta\left(\log\left(\frac{3^{18+3/2}}{2\pi} + \frac{1}{2}\right)\right)^3\right] = 34681575\,,$$

we then obtain the proposition from Theorem 1.

REMARK 1. Checking the proof of Theorem 1, we actually deduce the following fact from Lemmas 1 and 2: If P denotes the set of pairs (n', l') such that n' is an integer greater than 1, l' is a prime number congruent to 8 or 17 modulo 27, and

$$\frac{3^{n'-1}}{8} < l' < \frac{(3 + 8\cos(2\pi/9) - 8\cos(8\pi/9))^3}{3(\log 2)^3}\left(\log\left(\frac{3^{n'+3/2}}{2\pi} + \frac{1}{2}\right)\right)^3,$$

then not only every (n', l') in P satisfies $n' \leq 18$ and $l' < 34681575$, but the condition $l \nmid h_{18}$ in Proposition 1 can be replaced by the condition that l does not divide $h_{n'}/h_{n'-1}$ for any integer n' with $(n', l) \in P$.

PROOF OF PROPOSITION 2. The hypothesis of the proposition implies that $F = \boldsymbol{Q}(\xi_3)$ and $\nu = 3$. As $S^* = \{0, \dots, 7\}$, (ii) of Lemma 4 yields

$$N = \{n' \in \boldsymbol{Z}\,;\ n' \geq 3,\ 2^{n'-4} < \Theta((n' + 2)\log 2 - \log\pi)^4\} = \{3, \dots, 36\}\,, \quad n_0 = 36\,.$$

Therefore, because of the facts

$$h_2 = 1\,, \quad [\Theta((36 + 2)\log 2 - \log\pi)^4] = 7150001069 = 29 \cdot 8713 \cdot 28297\,,$$

the proposition follows from Theorem 1. $\square$

PROOF OF PROPOSITION 3. Since

$$F = \boldsymbol{Q}(\xi_4 - \xi_4^{-1}), \quad \nu = 4, \quad S = \{0, 1, 2, 3, 5, 6, 7\},$$

we have $S^* = \{0, 1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 13, 14, 15\}$. Hence, by (iii) of Lemma 4,

$$N = \left\{ n' \in \boldsymbol{Z}\,;\ n' \geq 5,\ \frac{2^{n'-3}}{7} < \Theta((n'+2)\log 2 - \log \pi)^4 \right\} = \{5, \ldots, 39\}, \quad n_0 = 39.$$

Furthermore, h_3 is known to be 1 and

$$[\Theta((39+2)\log 2 - \log \pi)^4] = 17324899980.$$

Theorem 1 therefore completes the proof of the proposition. $\square$

REMARK 2. We can weaken the conditions of Propositions 2 and 3, as well as the condition of Proposition 1, in a manner similar to that of Remark 1. Anyhow, once the value of p and the field F are explicitly given, Theorem 1 provides us with a concrete result such as each proposition.

3. Proofs of Theorems 2 and 3. Suppose p to be odd in this section. Let R be the set of positive quadratic residues modulo p smaller than p, i.e.,

$$R = \left\{ m \in \boldsymbol{Z}\,;\ 0 < m < p,\ \left(\frac{m}{p}\right) = 1 \right\}.$$

We let

$$\begin{aligned} R_+ &= \left\{ m \in R\,;\ m \leq p-2,\ \left(\frac{m+1}{p}\right) = -1 \right\}, \\ R_- &= \left\{ m \in R\,;\ 3 \leq m,\ \left(\frac{m-1}{p}\right) = -1 \right\} = R \setminus (\{m+1\,;\ m \in R\} \cup \{1\}). \end{aligned}$$

Putting

$$R_+^* = R_+ \cup \{0\}, \quad R_-^* = R_- \cup \{0\},$$

let $\mathfrak{F}_+$ denote the set of all maps from $R_+^* \times I$ to $\{0, l\}$, and $\mathfrak{F}_-$ the set of all maps from $R_-^* \times I$ to $\{0, l\}$. For each pair (m, u) in $R_+^* \times I$, let $\mathfrak{G}_+^{m,u}$ denote the set of maps $j : R_+^* \times I \to \boldsymbol{Z}$ such that $\min(l-2, 1) \leq j(m, u) < l$ and $j(m', u') \in \{0, l\}$ for every (m', u') in $R_+^* \times I \setminus \{(m, u)\}$. Similarly, for each (m, u) in $R_-^* \times I$, let $\mathfrak{G}_-^{m,u}$ denote the set of maps $j : R_-^* \times I \to \boldsymbol{Z}$ such that $\min(l-2, 1) \leq j(m, u) < l$ and $j(m', u') \in \{0, l\}$ for every (m', u') in $R_-^* \times I \setminus \{(m, u)\}$. We then put

$$\mathfrak{G}_+ = \bigcup_{(m,u) \in R_+^* \times I} \mathfrak{G}_+^{m,u}, \quad \mathfrak{G}_- = \bigcup_{(m,u) \in R_-^* \times I} \mathfrak{G}_-^{m,u}.$$

For each pair (j, j') in $(\mathfrak{G}_+ \times \mathfrak{F}_-) \cup (\mathfrak{F}_+ \times \mathfrak{G}_-)$, we define

$$\hat{A}(j, j') = \sum_{u \in I} u\left(\sum_{m \in R_+^*} (1+p^n)^{m+1} j(m, u) + \sum_{m \in R_-^*} (1+p^n)^m j'(m, u) \right),$$

whence

$$\hat{A}(j, j') \equiv \sum_{u \in I} u\left(\sum_{m \in R_+^*} j(m, u) + \sum_{m \in R_-^*} j'(m, u) \right) \pmod{p^n}.$$

We also define

$$\hat{B}(j, j') = \sum_{u \in I}\left(\sum_{m \in R_+^*} (l - j(m, u)) + \sum_{m \in R_-^*} (l - j'(m, u)) \right).$$

Let d be any integer. For each $(m, u) \in R_+^* \times I$, let $\mathcal{P}_+^{m,u}(d)$ denote the set of (j, j') in $\mathfrak{G}_+^{m,u} \times \mathfrak{F}_-$ such that

$$\hat{A}(j, j') \equiv d \pmod{p^{n+1}}.$$

For each $(m, u) \in R_-^* \times I$, let $\mathcal{P}_-^{m,u}(d)$ denote the set of (j, j') in $\mathfrak{F}_+ \times \mathfrak{G}_-^{m,u}$ such that

$$\hat{A}(j, j') \equiv d \pmod{p^{n+1}}.$$

In the case $l > 2$, we put

$$\begin{aligned} s_+(w_1, w_2\,;\, d) = \sum_{u \in I}\Biggl(& w_1 \sum_{(j,j') \in \mathcal{P}_+^{0,u}(d)} (-1)^{j(0,u) + \hat{B}(j,j')} \widetilde{j(0,u)} \\ & + w_2 \sum_{m \in R_+} \sum_{(j,j') \in \mathcal{P}_+^{m,u}(d)} (-1)^{j(m,u) + \hat{B}(j,j')} \widetilde{j(m,u)} \Biggr), \end{aligned}$$

$$\begin{aligned} s_-(w_1, w_2\,;\, d) = \sum_{u \in I}\Biggl(& w_1 \sum_{(j,j') \in \mathcal{P}_-^{0,u}(d)} (-1)^{j'(0,u) + \hat{B}(j,j')} \widetilde{j'(0,u)} \\ & + w_2 \sum_{m \in R_-} \sum_{(j,j') \in \mathcal{P}_-^{m,u}(d)} (-1)^{j'(m,u) + \hat{B}(j,j')} \widetilde{j'(m,u)} \Biggr) \end{aligned}$$

for each $(w_1, w_2) \in \boldsymbol{Z} \times \boldsymbol{Z}$; here, for each integer g relatively prime to l, $\tilde{g}$ denotes the positive integer smaller than l such that $\tilde{g}g \equiv 1 \pmod{l}$. In the case $l = 2$, we put

$$s_+(w_1, w_2\,;\, d) = \sum_{u \in I}\left(w_1 |\mathcal{P}_+^{0,u}(d)| + w_2 \sum_{m \in R_+} |\mathcal{P}_+^{m,u}(d)| \right),$$

$$s_-(w_1, w_2\,;\, d) = \sum_{u \in I}\left(w_1 |\mathcal{P}_-^{0,u}(d)| + w_2 \sum_{m \in R_-} |\mathcal{P}_-^{m,u}(d)| \right)$$

for each $(w_1, w_2) \in \boldsymbol{Z} \times \boldsymbol{Z}$. Further, put $\iota = 1$ or $\iota = 0$, according to whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. Take a pair (c_1, c_2) of integers for which

$$c_1 > 0\,, \quad 2c_1 \geq c_2 \geq 0\,,$$

and l divides the integer

$$c_1^2 - c_1c_2 + \frac{1-(-1)^{(p-1)/2}p}{4}c_2^2\,.$$

We can now restate [6, Lemma 10] as follows.

LEMMA 5. *Assume that* $[F : \boldsymbol{Q}] = 2$ *and* l *divides* h_n/h_{n-1}. *Take any pair* (d, d') *of integers with* $d \equiv d' \pmod{p^n}$. *Then either*

$$\begin{aligned} s_+(c_1 - c_2, c_2;\ d)\ &- s_-(c_1 - \iota c_2, c_2;\ d) \\ &\equiv s_+(c_1 - c_2, c_2;\ d') - s_-(c_1 - \iota c_2, c_2;\ d') \pmod l \end{aligned}$$

or

$$\begin{aligned} s_+(c_1, -c_2;\ d)\ &- s_-(c_1 + (\iota - 1)c_2, -c_2;\ d) \\ &\equiv s_+(c_1, -c_2;\ d') - s_-(c_1 + (\iota - 1)c_2, -c_2;\ d') \pmod l\,. \end{aligned}$$

PROOF OF THEOREM 2. In virtue of [4, Proposition 1], we may suppose that $l \equiv g \pmod{25}$ for some $g \in \{4, 9, 14, 19\}$, namely, $F = \boldsymbol{Q}(\sqrt{5})$. We then find that

$$\nu = 1\,, \quad \mathfrak{O} = \{a + b\xi_1^2 + b\xi_1^3\,;\ a, b \in \boldsymbol{Z}\}\,,$$

and that, in the group ring of Γ over $\boldsymbol{Z}$,

$$(1-\gamma)(a + b\gamma^2 + b\gamma^3) = a - a\gamma + b\gamma^2 - b\gamma^4 \quad \text{for } a, b \in \boldsymbol{Z}\,.$$

In particular, $|S^*| = 4$. Since $V = \{1, i\}$, it follows that

$$\mathfrak{N}\Big(\sum_{\delta \in V}\psi(\delta)\delta - 1\Big) = (\psi(1) - 1)^2 + \psi(i)^2$$

for every map ψ in Φ. The definition of M therefore gives $M < 32l^2$. Hence Lemma 3 (or [6, Lemma 8]) shows that $5^n < 32l^2$, i.e., $5^{n/2}/(4\sqrt{2}) < l$ if l divides h_n/h_{n-1}. Furthermore, by [6, Lemma 6], we have

$$l < \frac{(\sqrt{5}+1)^4}{2\sqrt{5}}\left(\frac{(n+1)\log 5 - \log\pi + \pi^2/1250}{\log 2}\right)^2$$

if l divides h_n/h_{n-1}. Now, let P be the set of pairs (n', l') such that n' is a positive integer, l' is a prime number congruent to either 4, 9, 14 or 19 modulo 25, and

$$\frac{5^{n'/2}}{4\sqrt{2}} < l' < \frac{(\sqrt{5}+1)^4}{2\sqrt{5}}\left(\frac{(n'+1)\log 5 - \log\pi + \pi^2/1250}{\log 2}\right)^2.$$

Every $(n', l') \in P$ then satisfies

$$n' \leq 14\,, \quad l' \leq 26959\,.$$

Suppose next that (n, l) belongs to P. To complete the present proof, let us see that l does not divide h_n/h_{n-1}. Let u_0 be the positive residue of 2^{5^n} modulo 5^{n+1}. As 2 is a primitive root modulo 25, we can take as $\mathfrak{p}$ the prime ideal of $\boldsymbol{Q}(i)$ generated by 5 and $i - u_0$, so that we have $I = \{1, u_0\}$. In addition, $R_+^* = \{0, 1\}$ and $R_-^* = \{0, 4\}$. Therefore, for each (j, j') in $(\mathfrak{G}_+ \times \mathfrak{F}_-) \cup (\mathfrak{F}_+ \times \mathfrak{G}_-)$,

$$\begin{aligned}\hat{A}(j, j') = {} & (1 + 5^n)(j(0, 1) + u_0 j(0, u_0)) + (1 + 5^n)^2 (j(1, 1) + u_0 j(1, u_0)) \\ & + j'(0, 1) + u_0 j'(0, u_0) + (1 + 5^n)^4 (j'(4, 1) + u_0 j'(4, u_0)) .\end{aligned}$$

Hence, given an integer d, we know for instance that to determine $\mathcal{P}_+^{0,1}(d)$ is none other than to solve the congruence

$$(1+5^n)(y_1+u_0y_2)+(1+5^n)^2(y_3+u_0y_4)+y_5 + u_0y_6+(1+5^n)^4(y_7+u_0y_8) \equiv d \pmod{5^{n+1}}$$

in eight variables $y_1, \ldots, y_8$ under the conditions

$$y_1 \in \{1, \ldots, l-1\}, \quad y_2, \ldots, y_8 \in \{0, l\} .$$

Meanwhile,

$$\begin{aligned}\hat{B}(j, j') \equiv {} & j(0, 1) + j(0, u_0) + j(1, 1) + j(1, u_0) \\ & + j'(0, 1) + j'(0, u_0) + j'(4, 1) + j'(4, u_0) \pmod 2\end{aligned}$$

for each (j, j') in $(\mathfrak{G}_+ \times \mathfrak{F}_-) \cup (\mathfrak{F}_+ \times \mathfrak{G}_-)$. Since 5 is a quadratic residue modulo l, there exist just two positive integers $z < l$ satisfying $z^2 - z - 1 \equiv 0 \pmod{l}$. Let z_0 be the smaller one of such z. We may let $(c_1, c_2) = (z_0, 1)$. Put, for each $d \in \boldsymbol{Z}$,

$$s_1(d) = s_+(z_0 - 1, 1;\ d) - s_-(z_0 - 1, 1;\ d), \quad s_2(d) = s_+(z_0, -1;\ d) - s_-(z_0, -1;\ d) .$$

By Lemma 5, it now suffices for our proof to find a pair (d, d') of integers with $d \equiv d' \pmod{5^n}$ such that

$$s_1(d) \not\equiv s_1(d') \pmod{l}, \quad s_2(d) \not\equiv s_2(d') \pmod{l} .$$

However, using *Mathematica* on a personal computer, we have determined $\mathcal{P}_+^{m,u}(1)$, $\mathcal{P}_+^{m,u}(1 + 5^n)$ for all $(m, u) \in R_+^* \times I$ and $\mathcal{P}_-^{m,u}(1)$, $\mathcal{P}_-^{m,u}(1 + 5^n)$ for all $(m, u) \in R_-^* \times I$; further, with the help of the computer again, we have computed $s_1(1)$, $s_1(1 + 5^n)$, $s_2(1)$, $s_2(1 + 5^n)$, and verified that

$$s_1(1) \not\equiv s_1(1 + 5^n) \pmod{l}, \quad s_2(1) \not\equiv s_2(1 + 5^n) \pmod{l}$$

unless (n, l) is equal to either $(1, 59)$, $(2, 19)$ or $(4, 929)$. Similarly to the above, we have also checked that

$$s_1(2) \not\equiv s_1(2 + 5^n) \pmod{l}, \quad s_2(2) \not\equiv s_2(2 + 5^n) \pmod{l}$$

if (n, l) is equal to either $(1, 59)$, $(2, 19)$ or $(4, 929)$. In passing, when $(n, l) = (1, 59)$,

$$s_1(1) - s_1(1 + 5) \equiv 0 \pmod{59}, \quad s_2(1) - s_2(1 + 5) \equiv 47 \pmod{59},$$

$$s_1(2) - s_1(2 + 5) \equiv 32 \pmod{59}, \quad s_2(2) - s_2(2 + 5) \equiv 46 \pmod{59};$$

when $(n, l) = (2, 19)$,

$$s_1(1) - s_1(1+5^2) \equiv 4 \pmod{19}, \quad s_2(1) - s_2(1+5^2) \equiv 0 \pmod{19},$$

$$s_1(2) - s_1(2+5^2) \equiv 16 \pmod{19}, \quad s_2(2) - s_2(2+5^2) \equiv 15 \pmod{19};$$

when $(n, l) = (4, 929)$,

$$s_1(1) - s_1(1+5^4) \equiv 304 \pmod{929}, \quad s_2(1) - s_2(1+5^4) \equiv 0 \pmod{929},$$

$$s_1(2) - s_1(2+5^4) \equiv 914 \pmod{929}, \quad s_2(2) - s_2(2+5^4) \equiv 360 \pmod{929}.$$

The theorem is thus proved; but we finally add a lemma which is useful in our calculations of $s_1(1) - s_1(1+5^n)$ and $s_2(1) - s_2(1+5^n)$ modulo l. Let Y denote the set of all pairs (x_1, x_2) in

$$(\{1, \ldots, 4l-1\} \setminus \{l, 2l, 3l\}) \times \{0, l, 2l, 3l, 4l\}$$

or in

$$\{0, l, 2l, 3l, 4l\} \times (\{1, \ldots, 4l-1\} \setminus \{l, 2l, 3l\})$$

satisfying

$$x_1 + u_0 x_2 \equiv 1 \pmod{5^n}.$$

Obviously $(1, 0)$ belongs to Y.

LEMMA 6. *Assume that $(n, l) \in P$, and take any integer n' in $\{1, \ldots, 14\}$. Then the condition that $Y = \{(1, 0)\}$ if $n = n'$ implies that*

$$s_1(1) \not\equiv s_1(1+5^n) \pmod{l}, \quad s_2(1) \not\equiv s_2(1+5^n) \pmod{l}$$

whenever $n \geq n'$.

PROOF. Letting

$$\mathcal{P}(d) = \Bigg(\bigcup_{(m,u) \in R_+^* \times I} \mathcal{P}_+^{m,u}(d) \Bigg) \cup \Bigg(\bigcup_{(m,u) \in R_-^* \times I} \mathcal{P}_-^{m,u}(d) \Bigg)$$

for each $d \in \boldsymbol{Z}$, take any $(j_1, j_1') \in \mathcal{P}(1)$ and any $(j_2, j_2') \in \mathcal{P}(1+5^n)$, so that

$$\begin{aligned} &j_1(0,1) + j_1(1,1) + j_1'(0,1) + j_1'(4,1) + u_0(j_1(0,u_0) + j_1(1,u_0) + j_1'(0,u_0) + j_1'(4,u_0)) \\ &\quad \equiv 1 \pmod{5^n}, \\ &j_2(0,1) + j_2(1,1) + j_2'(0,1) + j_2'(4,1) + u_0(j_2(0,u_0) + j_2(1,u_0) + j_2'(0,u_0) + j_2'(4,u_0)) \\ &\quad \equiv 1 \pmod{5^n}. \end{aligned}$$

Assume that $n \geq n'$ and that $Y = \{(1, 0)\}$ if $n = n'$. The definition of Y as well as the choice of u_0 then induces $Y = \{(1, 0)\}$ in the case $n > n'$. Hence we easily see that

$$j_1(R_+^* \times I) = j_1'(R_-^* \times I \setminus \{(0,1)\}) = \{0\}, \quad j_1'(0,1) = 1,$$

$$j_2(0,1) = 1, \quad j_2(R_+^* \times I \setminus \{(0,1)\}) = j_2'(R_-^* \times I) = \{0\},$$

$$\mathcal{P}(1) = \mathcal{P}_{-}^{0,1}(1) = \{(j_1, j_1')\}\,, \quad \mathcal{P}(1+5^n) = \mathcal{P}_{+}^{0,1}(1+5^n) = \{(j_2, j_2')\}\,.$$

Thus

$$s_1(1) = -(z_0-1)(-1)^{1+\hat{B}(j_1,j_1')} = -z_0+1\,, \quad s_1(1+5^n) = (z_0-1)(-1)^{1+\hat{B}(j_2,j_2')} = z_0-1\,,$$

$$s_2(1) = -z_0(-1)^{1+\hat{B}(j_1,j_1')} = -z_0\,, \quad s_2(1+5^n) = z_0(-1)^{1+\hat{B}(j_2,j_2')} = z_0\,.$$

In particular, since $z_0(z_0-1) \equiv 1 \pmod{l}$, both $s_1(1+5^n) - s_1(1) = 2(z_0-1)$ and $s_2(1+5^n) - s_2(1) = 2z_0$ are relatively prime to l. □

REMARK 3. With *Mathematica*, to find whether $Y = \{(1,0)\}$ or not is much easier than to find, for every (j, j') in $(\mathfrak{G}_+ \times \mathfrak{F}_-) \cup (\mathfrak{F}_+ \times \mathfrak{G}_-)$, whether $\hat{A}(j, j') \equiv 1 \pmod{5^{n+1}}$ or not. Moreover, Y almost always coincides with $\{(1,0)\}$ if n is relatively large; for instance, in case $(n,l) \in P$ and $n \geq 12$, one has $Y \neq \{(1,0)\}$ if and only if $(n,l) = (12, 8839)$ or $(n,l) = (13, 8839)$.

PROOF OF THEOREM 3. By [4, Proposition 2], we may only consider the case where $F = \boldsymbol{Q}(\sqrt{-7})$, namely,

$$l \equiv g \pmod{49} \quad \text{for some } g \in \{2, 4, 9, 11, 16, 23, 25, 32, 37, 39, 44, 46\}\,.$$

In this case,

$$\nu = 1\,, \quad \mathfrak{O} = \{a + b\xi_1 + b\xi_1^2 + b\xi_1^4\,;\ a, b \in \boldsymbol{Z}\}\,,$$

and, in the group ring of Γ over $\boldsymbol{Z}$,

$$(1-\gamma)(a + b\gamma + b\gamma^2 + b\gamma^4) = a + (b-a)\gamma - b\gamma^3 + b\gamma^4 - b\gamma^5 \quad \text{for } a, b \in \boldsymbol{Z}\,.$$

Let $\omega = e^{\pi i/3}$, so that $V = \{1, \omega, \omega^2\}$. As $|S^*| = 5$, it follows for any $\psi \in \Phi$ that

$$\begin{aligned}
&\mathfrak{N}\Big(\sum_{\delta\in V} \psi(\delta)\delta - 1\Big) \\
&\quad = (\psi(1)-1+\psi(\omega))^2 - (\psi(1)-1+\psi(\omega))(\psi(\omega)+\psi(\omega^2)) + (\psi(\omega)+\psi(\omega^2))^2 \\
&\quad \leq \frac{1}{2}((\psi(1)-1+\psi(\omega))^2 + (\psi(\omega)+\psi(\omega^2))^2) < 100l^2\,.
\end{aligned}$$

Hence we have $M < 100l^2$. This implies, by Lemma 3 (or [6, Lemma 8]), that $7^n < 100l^2$, i.e., $7^{n/2}/10 < l$ if l divides h_n/h_{n-1}. Let P be the set of pairs (n', l') for which n' is a positive integer, l' is a prime number congruent to some integer in $\{2, 4, 9, 11, 16, 23, 25, 32, 37, 39, 44, 46\}$ modulo 49, and

$$\frac{7^{n'/2}}{10} < l' < \frac{144}{\sqrt{21}}\left(\frac{(n'+1)\log 7 - \log\pi + \pi^2/4802}{\log 2}\right)^2\,.$$

Then each $(n', l') \in P$ satisfies

$$n' \leq 13\,, \quad l' \leq 44543\,,$$

and [6, Lemma 6], together with an argument above, shows that (n,l) belongs to P if l divides h_n/h_{n-1}.

Now, assume (n, l) to be in P. Let u_0 be the positive residue of 3^{7^n} modulo 7^{n+1}. Since 3 is a primitive root modulo 49, we may take as $\mathfrak{p}$ the prime ideal of $\boldsymbol{Q}(\omega)$ generated by 7 and $\omega - u_0$. We then see that $I = \{1, u_0, u_0 - 1\}$. Furthermore, $R_+^* = \{0, 2, 4\}$ and $R_-^* = \{0, 4\}$. Hence, for any (j, j') in $(\mathfrak{G}_+ \times \mathfrak{F}_-) \cup (\mathfrak{F}_+ \times \mathfrak{G}_-)$,

$$\begin{aligned}\hat{A}(j, j') = {} & (1 + 7^n)(j(0, 1) + u_0 j(0, u_0) + (u_0 - 1)j(0, u_0 - 1)) \\ & + (1 + 7^n)^3(j(2, 1) + u_0 j(2, u_0) + (u_0 - 1)j(2, u_0 - 1)) \\ & + (1 + 7^n)^5(j(4, 1) + u_0 j(4, u_0) + (u_0 - 1)j(4, u_0 - 1)) \\ & + j'(0, 1) + u_0 j'(0, u_0) + (u_0 - 1)j'(0, u_0 - 1) \\ & + (1 + 7^n)^4(j'(4, 1) + u_0 j'(4, u_0) + (u_0 - 1)j'(4, u_0 - 1)),\end{aligned}$$

$$\begin{aligned}\hat{B}(j, j') \equiv {} & l + j(0, 1) + j(0, u_0) + j(0, u_0 - 1) + j(2, 1) + j(2, u_0) \\ & + j(2, u_0 - 1) + j(4, 1) + j(4, u_0) + j(4, u_0 - 1) + j'(0, 1) \\ & + j'(0, u_0) + j'(0, u_0 - 1) + j'(4, 1) + j'(4, u_0) + j'(4, u_0 - 1) \pmod 2.\end{aligned}$$

Noting that -7 is a quadratic residue modulo l, we may let $(c_1, c_2) = (z_0, 1)$ where z_0 denotes the smallest positive integer such that $z_0^2 - z_0 + 2 \equiv 0 \pmod l$. Let us put, for each $d \in \boldsymbol{Z}$,

$$s_1(d) = s_+(z_0 - 1, 1;\ d) - s_-(z_0, 1;\ d), \quad s_2(d) = s_+(z_0, -1;\ d) - s_-(z_0 - 1, -1;\ d).$$

As in the proof of Theorem 2, with *Mathematica*, we have computed $s_1(1)$, $s_1(1 + 7^n)$, $s_2(1)$, $s_2(1 + 7^n)$, and checked that

$$s_1(1) \not\equiv s_1(1 + 7^n) \pmod l, \qquad s_2(1) \not\equiv s_2(1 + 7^n) \pmod l$$

unless $(n, l) \in \{(2, 23), (3, 107), (4, 23), (4, 37)\}$. We have also verified that

$$s_1(2) \not\equiv s_1(2 + 7^n) \pmod l, \qquad s_2(2) \not\equiv s_2(2 + 7^n) \pmod l$$

if $(n, l) \in \{(2, 23), (3, 107), (4, 23), (4, 37)\}$. Hence, by Lemma 5, l does not divide h_n/h_{n-1} and consequently the theorem is proved.

Similarly to Lemma 6 for the proof of Theorem 2, the following supplementary lemma is quite useful in our calculations of $s_1(1) - s_1(1 + 7^n)$ and $s_2(1) - s_2(1 + 7^n)$ modulo l; the proof of the lemma is almost the same as that of Lemma 6.

LEMMA 7. *Assume that not only $(n, l) \in P$ but $l > 2$. Let n' be any integer in $\{1, \dots, 13\}$, and let Y' denote the set of triplets (x_1, x_2, x_3) of non-negative integers for which*

$$x_1 + u_0 x_2 + (u_0 - 1)x_3 \equiv 1 \pmod{7^n}$$

and either (x_1, x_2, x_3), (x_2, x_3, x_1) or (x_3, x_1, x_2) belongs to

$$(\{1, \dots, 5l - 1\} \setminus \{l, 2l, 3l, 4l\}) \times \{0, l, 2l, 3l, 4l, 5l\} \times \{0, l, 2l, 3l, 4l, 5l\}.$$

Then the condition that $Y' = \{(1, 0, 0)\}$ if $n = n'$ implies that

$$s_1(1) \not\equiv s_1(1 + 7^n) \pmod l, \quad s_2(1) \not\equiv s_2(1 + 7^n) \pmod l$$

whenever $n \geq n'$.

REMARK 4. In the case $p = 7$, S^* is the union of $\{m+1\,;\ m \in R_+^*\} = \{1, 3, 5\}$ and $R_-^* = \{0, 4\}$, so that

$$A(j) = \hat{A}(j_+, j_-)\,, \quad B(j) \equiv \hat{B}(j_+, j_-) \pmod 2$$

for each $j \in \mathfrak{H}$, where j_+ denotes the restriction of j to $\{1, 3, 5\} \times I$ and j_- the restriction of j to $\{0, 4\} \times I$.

Note added. After the submission of a manuscript of this paper, Professor K. Komatsu informed us that Propositions 2 and 3 hold without our additional assumptions, namely, if $p = 2$ and if $l \equiv 7 \pmod{16}$ or $l \equiv 9 \pmod{16}$, then the l-class group of $\boldsymbol{B}_\infty$ is trivial (for the details, cf. Fukuda and Komatsu [2]).

Acknowledgment. The authors express their thanks to the referee who made helpful comments on the paper.

REFERENCES

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

[2] T. FUKUDA AND K. KOMATSU, Weber's class number problem, preprint.

[3] K. HORIE, Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field, J. London Math. Soc. (2) 66 (2002), 257–275.

[4] K. HORIE, Primary components of the ideal class group of the $\boldsymbol{Z}_p$-extension over $\boldsymbol{Q}$ for typical inert primes, Proc. Japan Acad. Ser. A Math. Sci. 81 (2005), 40–43.

[5] K. HORIE, The ideal class group of the basic $\boldsymbol{Z}_p$-extension over an imaginary quadratic field, Tohoku Math. J. (2) 57 (2005), 375–394.

[6] K. HORIE, Certain primary components of the ideal class group of the $\boldsymbol{Z}_p$-extension over the rationals, Tohoku Math. J. (2) 59 (2007), 259–291.

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

[8] K. HORIE AND M. HORIE, The narrow class groups of some $\boldsymbol{Z}_p$-extensions over the rationals, Acta Arith. 135 (2008), 159–180.

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

DEPARTMENT OF MATHEMATICS
TOKAI UNIVERSITY
HIRATSUKA 259–1292
JAPAN

DEPARTMENT OF MATHEMATICS
OCHANOMIZU UNIVERSITY
2–1–1 OTSUKA, BUNKYO-KU
TOKYO 112–8610
JAPAN

E-mail address: horie.mitsuko@ocha.ac.jp