Tohoku Math. J.
59 (2007), 259–291

CERTAIN PRIMARY COMPONENTS OF THE IDEAL CLASS GROUP OF THE Z_p-EXTENSION OVER THE RATIONALS

KUNIAKI HORIE

(Received December 14, 2005, revised November 21, 2006)

Abstract. We study, for any prime number p, the triviality of certain primary components of the ideal class group of the $\boldsymbol{Z}_p$-extension over the rational field. Among others, we prove that if p is 2 or 3 and l is a prime number not congruent to 1 or -1 modulo $2p^2$, then l does not divide the class number of the cyclotomic field of p^uth roots of unity for any positive integer u.

Introduction. Let p be any prime number. We denote by $\boldsymbol{Z}_p$ the ring of p-adic integers, and by $\boldsymbol{B}_\infty$ the $\boldsymbol{Z}_p$-extension over the rational field $\boldsymbol{Q}$, namely, the unique abelian extension of $\boldsymbol{Q}$, in the complex field $\boldsymbol{C}$, whose Galois group over $\boldsymbol{Q}$ is topologically isomorphic to the additive group of $\boldsymbol{Z}_p$. Let $\boldsymbol{P}_\infty$ denote the composite in $\boldsymbol{C}$ of the cyclotomic fields of p^uth roots of unity for all positive integers u:

$$\boldsymbol{Q} \subset \boldsymbol{B}_\infty \subset \boldsymbol{P}_\infty = \boldsymbol{B}_\infty(e^{\pi i/p}) \subset \boldsymbol{C}\,.$$

Given a prime number l different from p, let F denote the decomposition field of l for the abelian extension $\boldsymbol{P}_\infty/\boldsymbol{Q}$. We have shown in [4], mainly by algebraic investigation of the analytic class number formula, that the l-class group of $\boldsymbol{B}_\infty$, i.e., the l-primary component of the ideal class group of $\boldsymbol{B}_\infty$ is trivial if l is sufficiently large with the degree of F bounded (for the simplest case where $F = \boldsymbol{Q}$ so that $p > 2$, cf. [2, 3]). In this paper, pursuing or refining our arguments of [2, 3, 4], we discuss the triviality of the l-class group of $\boldsymbol{B}_\infty$ more precisely than in [4] for the case where F is a quadratic field. It is verified, as a consequence, that if p is 2 or 3 and $l^2 \not\equiv 1 \pmod{4p^2}$, then the l-class group of $\boldsymbol{P}_\infty$ is trivial, namely, l does not divide the class number of the cyclotomic field of p^uth roots of unity for any positive integer u.

The author expresses here his thanks to the referee for helpful comments.

1. Preliminaries.

To begin with, we give some preliminaries in this brief section.The distinct prime numbers p and l in the introduction will be fixed throughout the paper.

For each integer $m \geq 0$, let $\boldsymbol{B}_m$ denote the subfield of $\boldsymbol{B}_\infty$ with degree p^m, E_m the unit group of $\boldsymbol{B}_m$, and h_m the class number of $\boldsymbol{B}_m$. Note that $\boldsymbol{B}_0 = \boldsymbol{Q}$ and, hence, $h_0 = 1$. Class field theory shows that h_{u-1} divides h_u for every positive integer u, because the prime ideal of

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

$\boldsymbol{B}_{u-1}$ dividing p is totally ramified for the extension $\boldsymbol{B}_u/\boldsymbol{B}_{u-1}$. Furthermore, since $\boldsymbol{B}_\infty/\boldsymbol{Q}$ is a p-extension, we have the following basic result.

LEMMA 1. *The l-class group of $\boldsymbol{B}_\infty$ is trivial if and only if l does not divide h_u/h_{u-1} for any positive integer u.*

In the rest of the paper, we fix a positive integer n under the condition that

$$n \geq 2 \quad \text{if} \quad p = 2$$

and, further,

$$n \geq 3 \quad \text{if} \quad p = 2\,, \quad l \equiv 3 \pmod 8\,.$$

Let

$$t = 1 + p^n \quad \text{or} \quad t = 1 + 2^{n+1}\,,$$

according to whether $p > 2$ or $p = 2$. In the case $p > 2$, put

$$\eta = \prod_u \frac{e^{2\pi iu/p^{n+1}} - e^{-2\pi iu/p^{n+1}}}{e^{2\pi itu/p^{n+1}} - e^{-2\pi itu/p^{n+1}}} = \prod_u \frac{\sin(2\pi u/p^{n+1})}{\sin(2\pi tu/p^{n+1})}\,,$$

with u raging over the positive integers $< p^{n+1}/2$ such that $u^{p-1} \equiv 1 \pmod{p^{n+1}}$; in the case $p = 2$, put

$$\eta = \frac{e^{\pi i/2^{n+2}} - e^{-\pi i/2^{n+2}}}{e^{\pi it/2^{n+2}} - e^{-\pi it/2^{n+2}}} = \tan\frac{\pi}{2^{n+2}}\,.$$

Then η is an element of E_n called a circular (or cyclotomic) unit of $\boldsymbol{B}_n$. Let τ denote the restriction to $\boldsymbol{B}_n$ of the automorphism of $\boldsymbol{Q}(e^{\pi i/p^{n+1}})$ that maps $e^{\pi i/p^{n+1}}$ to $e^{\pi it/p^{n+1}}$. Clearly, τ is a non-trivial element of the Galois group $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{B}_{n-1})$. Let σ denote the restriction to $\boldsymbol{B}_n$ of the automorphism of $\boldsymbol{Q}(e^{\pi i/p^{n+1}})$ that maps $e^{\pi i/p^{n+1}}$ to $e^{\pi i(p+1)/p^{n+1}}$. Then σ generates the cyclic group $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q})$ and satisfies $\sigma^{p^{n-1}} = \tau$:

$$\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q}) = \langle\sigma\rangle \supseteq \langle\tau\rangle = \mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{B}_{n-1})\,.$$

Let $\mathfrak{R}$ denote the group ring of $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{Q})$ over $\boldsymbol{Z}$, the ring of (rational) integers. Note that E_n as well as the multiplicative group of $\boldsymbol{B}_n$ becomes an $\mathfrak{R}$-module in the obvious manner.

Now, to state another basic result, we first deal with the case $p > 2$. Let

$$p^* = (-1)^{(p-1)/2}p\,, \quad \omega = \frac{-1+\sqrt{p^*}}{2}\,,$$

so that $\boldsymbol{Z}[\omega]$ is the ring of algebraic integers in

$$\boldsymbol{Q}(\omega) = \boldsymbol{Q}(\sqrt{p^*})\,,$$

the unique quadratic subfield of $\boldsymbol{P}_\infty$. This coincides with the decomposition field F of l for $\boldsymbol{P}_\infty/\boldsymbol{Q}$ if and only if $l \equiv q^2 \pmod{p^2}$ for some primitive root q modulo p^2. Let R be the set of positive quadratic residues modulo p smaller than p:

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

As is well-known,

$$\omega = \sum_{m \in R} e^{2\pi i m/p} .$$

We define an element $\tilde{\omega}$ of $\mathfrak{R}$ by

$$\tilde{\omega} = \sum_{m \in R} \tau^m .$$

Let a_1 and a_2 be integers such that $a_1 + a_2\omega$ is a non-zero element of a prime ideal of $\boldsymbol{Q}(\sqrt{p^*})$ dividing l. In other words, we are given a pair $(a_1, a_2) \in \boldsymbol{Z} \times \boldsymbol{Z}$ such that l divides

$$a_1^2 - a_1 a_2 + \frac{1 - p^*}{4} a_2^2 = \left(a_1 - \frac{a_2}{2} \right)^2 - \frac{p^* a_2^2}{4} ,$$

the norm of $a_1 + a_2\omega$ for $\boldsymbol{Q}(\sqrt{p^*})/\boldsymbol{Q}$. We may therefore suppose that

$$a_1 > 0 , \quad 2a_1 \geq a_2 \geq 0 .$$

We next deal with the case $p = 2$. Evidently, the quadratic fields contained in $\boldsymbol{P}_\infty$ are

$$\boldsymbol{Q}(i) , \quad \boldsymbol{Q}(\sqrt{-2}) , \quad \boldsymbol{Q}(\sqrt{2}) ;$$

but F cannot be $\boldsymbol{Q}(\sqrt{2})$, since the extension $\boldsymbol{Q}(e^{\pi i/8})/\boldsymbol{Q}(\sqrt{2})$ is not cyclic. The condition $F = \boldsymbol{Q}(i)$ is equivalent to the congruence $l \equiv 5 \pmod 8$, while the condition $F = \boldsymbol{Q}(\sqrt{-2})$ is equivalent to the congruence $l \equiv 3 \pmod 8$. When l is congruent to 5 modulo 8, we put $\omega = i$, put $\tilde{\omega} = \sigma^{2^{n-2}}$ in $\mathfrak{R}$, and take as (a_1, a_2) the pair of positive integers such that

$$l = a_1^2 + a_2^2 , \quad a_1 > a_2 .$$

When l is congruent to 3 modulo 8, we let

$$\omega = \sqrt{-2} = e^{\pi i/4} - e^{-\pi i/4} , \quad \tilde{\omega} = \sigma^{2^{n-3}} - \sigma^{-2^{n-3}} \in \mathfrak{R} ,$$

and take as (a_1, a_2) the pair of positive integers such that

$$l = a_1^2 + 2a_2^2 .$$

LEMMA 2. *Assume that F is a quadratic field and l divides h_n/h_{n-1}. If p is odd, then $\eta^{a_1 + a_2\tilde{\omega}}$ or $\eta^{a_1 - a_2 - a_2\tilde{\omega}}$ is an lth power in E_n. If p is equal to 2, then $\eta^{a_1 + a_2\tilde{\omega}}$ or $\eta^{a_1 - a_2\tilde{\omega}}$ is an lth power in E_n.*

PROOF. Let $f = p^{n-1}(p-1)$. For any $\gamma \in \boldsymbol{Z}[e^{2\pi i/p^n}]$, we put

$$\gamma_\sigma = \sum_{u=1}^{f} c_u \sigma^{u-1} ,$$

where the integers $c_1, \ldots, c_f$ are uniquely determined by

$$\gamma = \sum_{u=1}^{f} c_u e^{2\pi i (u-1)/p^n} .$$

We also put $\dot{\eta} = \eta$ or $\dot{\eta} = \eta^2$, according to whether $p > 2$ or $p = 2$. Since $\dot{\eta}^{\tau^{p-1}+\cdots+\tau+1} = 1$ by the definition of η, it then follows that

$$\dot{\eta}^{(\alpha+\beta)_\sigma} = \dot{\eta}^{\alpha_\sigma+\beta_\sigma}, \quad \dot{\eta}^{(\alpha\beta)_\sigma} = \dot{\eta}^{\alpha_\sigma\beta_\sigma}$$

for every pair (α, β) in $\boldsymbol{Z}[e^{2\pi i/p^n}] \times \boldsymbol{Z}[e^{2\pi i/p^n}]$. In particular, we have

$$\dot{\eta}^{\omega_\sigma} = \dot{\eta}^{\tilde{\omega}}.$$

Now, let $\mathfrak{l}$ be a prime ideal of $\boldsymbol{Q}(\omega)$ containing $\{l, a_1+a_2\omega\}$. By the assumption, $\mathfrak{l}$ and $l\mathfrak{l}^{-1}$ are the prime ideals of $\boldsymbol{Q}(\omega)$ dividing l. Furthermore, $l\mathfrak{l}^{-1}$ contains $a_1 + a_2\omega^\delta$, where δ denotes the non-trivial automorphism of the field $\boldsymbol{Q}(\omega)$. Hence, in the case where $p > 2$ so that $a_1 + a_2\omega^\delta = a_1 - a_2 - a_2\omega$, we obtain our lemma from [4, Lemma 2]. In the case $p = 2$, since $a_1+a_2\omega^\delta = a_1-a_2\omega$, we still deduce from [4, Lemma 2] that $(\eta^{a_1+a_2\tilde{\omega}})^2$ or $(\eta^{a_1-a_2\tilde{\omega}})^2$ is an lth power in E_n; but this conclusion means that $\eta^{a_1+a_2\tilde{\omega}}$ or $\eta^{a_1-a_2\tilde{\omega}}$ is an lth power in E_n. □

2. The minimal $\boldsymbol{Z}_p$-extension with p odd. We suppose that $p > 2$ throughout this section. Let

$$\varDelta = \begin{cases} \dfrac{(\sqrt{p}+1)^4}{2} & \text{if } p \equiv 1 \pmod 4, \\[2ex] \dfrac{(p+1)^2}{\sqrt{3}} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Let

$$\varLambda = \log\left(\frac{\sqrt{\varDelta(p+3)}(p-1)^{3/2}\varphi(p-1)}{(4\log 2)p^{1/4}}\right) + \frac{\log(p/\pi) + \pi^2/(2p^4)}{2\varphi(p-1)},$$

where φ denotes the Euler function as usual. The goal of this section is to prove the following result.

THEOREM 1. *Assume that $F = \boldsymbol{Q}(\sqrt{p^*})$, i.e., $l \equiv q^2 \pmod{p^2}$ for some primitive root q modulo p^2. Then the l-class group of $\boldsymbol{B}_\infty$ is trivial if*

$$l \geq \frac{\varDelta((p-1)\varphi(p-1)\varLambda)^2}{4(\log 2)^2\sqrt{p}}\left(1 + \frac{\log \varLambda}{\varLambda - 1}\right)^2.$$

It should be added that $\varLambda$ exceeds 1 by definition. To prove the above theorem, we start with the following fundamental lemma (cf. Problem 8 for Chapter V of Vinogradov [6]).

LEMMA 3. *Let κ_1 and κ_2 be either 1 or -1. Let T be the number of positive integers $m \leq p-2$ satisfying*

$$\left(\frac{m}{p}\right) = \kappa_1, \quad \left(\frac{m+1}{p}\right) = \kappa_2.$$

Then

$$T = \frac{1}{4}(p - 2 - \kappa_1(-1)^{(p-1)/2} - \kappa_2 - \kappa_1\kappa_2).$$

PROOF. For each integer m relatively prime to p, let $\check{m}$ denote the positive integer less than p such that $m\check{m} \equiv 1 \pmod{p}$. As the set $\{m \in \boldsymbol{Z} \mid 1 \le m \le p-2\}$ is invariant under the map $m \mapsto \check{m}$ of the difference set $\boldsymbol{Z} \setminus p\boldsymbol{Z}$ into itself, we see that

$$\sum_{m=1}^{p-2}\left(\frac{m(m+1)}{p}\right) = \sum_{m=1}^{p-2}\left(\frac{m^2(1+\check{m})}{p}\right) = \sum_{m=1}^{p-2}\left(\frac{1+\check{m}}{p}\right) = \sum_{m'=1}^{p-1}\left(\frac{m'}{p}\right) - \left(\frac{1}{p}\right) = -1\,.$$

Hence,

$$\begin{aligned} T &= \frac{1}{4}\sum_{m=1}^{p-2}\left(1+\kappa_1\left(\frac{m}{p}\right)\right)\left(1+\kappa_2\left(\frac{m+1}{p}\right)\right) \\ &= \frac{1}{4}\sum_{m=1}^{p-2}\left(1+\kappa_1\left(\frac{m}{p}\right)+\kappa_2\left(\frac{m+1}{p}\right)+\kappa_1\kappa_2\left(\frac{m(m+1)}{p}\right)\right) \\ &= \frac{1}{4}\left(p-2-\kappa_1\left(\frac{p-1}{p}\right)-\kappa_2\left(\frac{1}{p}\right)-\kappa_1\kappa_2\right). \end{aligned}$$ □

For each algebraic number α, let $\|\alpha\|$ denote the maximum of the absolute values of all conjugates of α over $\boldsymbol{Q}$. We then find that

$$\|\beta\gamma\| \le \|\beta\|\|\gamma\|\,, \quad \|\beta^m\| = \|\beta\|^m$$

for any algebraic numbers β, γ, and any positive integer m. Let

$$\zeta = e^{2\pi i/p^{n+1}}\,, \quad \theta = \prod_u (\zeta^u - \zeta^{-u})\,,$$

where u ranges over the positive integers less than $p^{n+1}/2$ such that $u^{p-1} \equiv 1 \pmod{p^{n+1}}$. By the definitions of η and τ,

$$\eta = \theta^{1-\tau}\,.$$

We put

$$\Upsilon = \max_m \|\theta^{1-\tau^m}\| = \max_m \left\| \prod_u \frac{\sin(2\pi u/p^{n+1})}{\sin(2\pi t^m u/p^{n+1})} \right\|,$$

where m ranges over the positive integers $< p$. We also put

$$R_+ = \left\{ m \in R \;\middle|\; m \le p-2,\ \left(\frac{m+1}{p}\right) = -1 \right\},$$

$$R_- = \left\{ m \in R \;\middle|\; 3 \le m,\ \left(\frac{m-1}{p}\right) = -1 \right\} = R \setminus (\{m+1 \mid m \in R\} \cup \{1\})\,.$$

As to R_+,

$$\{m+1 \mid m \in R_+\} = \{m+1 \mid m \in R\} \setminus (R \cup \{p\})\,.$$

LEMMA 4. *Assume that $F = \boldsymbol{Q}(\sqrt{p^*})$ and l divides h_n/h_{n-1}.*

(i) *If $p \equiv 1 \pmod 4$, then*

$$l < \left(a_1 + \frac{(p-1)a_2}{4}\right)\frac{\log \Upsilon}{\log 2}\,.$$

(ii) *If* $p \equiv 3 \pmod 4$, *then*

$$l < \left(\max(a_1, a_2) + \frac{(p-3)a_2}{4}\right)\frac{\log \Upsilon}{\log 2}\,.$$

PROOF. It follows from Lemma 2 that either $\theta^{(1-\tau)(a_1+a_2\tilde{\omega})} = \eta^{a_1+a_2\tilde{\omega}}$ or $\theta^{(1-\tau)(a_1-a_2-a_2\tilde{\omega})} = \eta^{a_1-a_2-a_2\tilde{\omega}}$ is an lth power in E_n. Also, it is known that $h_1 = 1$ if $p = 3$. Hence, by [4, Lemma 3],

$$2^l < \max(\|\theta^{(1-\tau)(a_1+a_2\tilde{\omega})}\|, \|\theta^{(1-\tau)(a_1-a_2-a_2\tilde{\omega})}\|)\,. \tag{1}$$

Let us first consider the case $p \equiv 1 \pmod 4$. Since the definitions of $\tilde{\omega}$, R_+, and R_- yield

$$(1-\tau)\tilde{\omega} = \tau + \sum_{m\in R_-}\tau^m - 1 - \sum_{m\in R_+}\tau^{m+1}\,,$$

we see that

$$\begin{aligned}(1-\tau)(a_1+a_2\tilde{\omega}) &= (a_1-a_2)(1-\tau) + a_2\left(\sum_{m\in R_-}\tau^m - \sum_{m\in R_+}\tau^{m+1}\right)\\ &= (a_2-a_1)(\tau-1) + a_2\left(\sum_{m\in R_-}\tau^m - \sum_{m\in R_+}\tau^{m+1}\right),\\ (1-\tau)(a_1-a_2-a_2\tilde{\omega}) &= a_1(1-\tau) + a_2\left(\sum_{m\in R_+}\tau^{m+1} - \sum_{m\in R_-}\tau^m\right).\end{aligned}$$

Furthermore, Lemma 3 yields $|R_-| = |R_+| = (p-1)/4$. Therefore, noting that $|a_1-a_2| \le a_1$ and using (1), we obtain

$$2^l < \Upsilon^{a_1+(p-1)a_2/4}\,.$$

Assume next that $p \equiv 3 \pmod 4$, so that

$$(1-\tau)\tilde{\omega} = \tau + \sum_{m\in R_-}\tau^m - \sum_{m\in R_+}\tau^{m+1}\,.$$

In the case $a_1 \ge a_2$, we have

$$\begin{aligned}(1-\tau)(a_1+a_2\tilde{\omega}) &= (a_1-a_2)(1-\tau) + a_2\left(1 + \sum_{m\in R_-}\tau^m - \sum_{m\in R_+}\tau^{m+1}\right),\\ (1-\tau)(a_1-a_2-a_2\tilde{\omega}) &= (a_1-a_2)(1-\tau) + a_2\left(\sum_{m\in R_+}\tau^{m+1} - \tau - \sum_{m\in R_-}\tau^m\right).\end{aligned}$$

In the case $a_1 < a_2$, we have, for any $c \in R_+$,

$$\begin{aligned}
&(1-\tau)(a_1 + a_2\tilde{\omega}) \\
&\qquad = a_1(1-\tau^{c+1}) + (a_2 - a_1)(\tau - \tau^{c+1}) + a_2\Bigg(\sum_{m \in R_-} \tau^m - \sum_{m \in R_+ \setminus \{c\}} \tau^{m+1}\Bigg), \\
&(1-\tau)(a_1 - a_2 - a_2\tilde{\omega}) \\
&\qquad = (a_2 - a_1)(\tau^{c+1} - 1) + a_1(\tau^{c+1} - \tau) + a_2\Bigg(\sum_{m \in R_+ \setminus \{c\}} \tau^{m+1} - \sum_{m \in R_-} \tau^m\Bigg).
\end{aligned}$$

Lemma 3 implies, however, that $|R_-| = |R_+| - 1 = (p-3)/4$. Therefore, in virtue of (1),

$$2^l < \Upsilon^{a_1 + (p-3)a_2/4} \quad \text{or} \quad 2^l < \Upsilon^{(p+1)a_2/4},$$

according to whether $a_1 \geq a_2$ or $a_1 < a_2$. □

Let a_0 be the ratio, to l, of the absolute value of the norm of $a_1 + a_2\omega$ for $\boldsymbol{Q}(\sqrt{p^*})/\boldsymbol{Q}$:

$$la_0 = \left| a_1^2 - a_1 a_2 + \frac{1-p^*}{4} a_2^2 \right|.$$

Obviously, a_0 is a positive integer. The next lemma is based on Problem 2, Section 26, and Problem 2, Section 30, of Takagi [5].

LEMMA 5. *The integers a_1 and a_2 can be taken as follows*:

$$a_1 + a_2\omega + |a_1 - a_2 - a_2\omega| < \sqrt{2l\sqrt{p}} \quad \textit{when} \ \ p \equiv 1 \pmod 4,$$

$$a_0 \leq \sqrt{\frac{p}{3}} \quad \textit{when} \ \ p \equiv 3 \pmod 4.$$

PROOF. Let $\mathfrak{l}$ be a prime ideal of $\boldsymbol{Q}(\sqrt{p^*})$ dividing l and, as in the proof of Lemma 2, let δ be the non-trivial automorphism of $\boldsymbol{Q}(\sqrt{p^*})$. Take $\lambda_1, \lambda_2 \in \boldsymbol{Z}[\omega]$ such that $\{\lambda_1, \lambda_2\}$ forms a free basis of the additive group of $\mathfrak{l}$. Then

$$|\lambda_1\lambda_2^\delta - \lambda_2\lambda_1^\delta| = l\sqrt{p}.$$

Now assume that $p \equiv 1 \pmod 4$. As

$$|(\lambda_1 + \lambda_1^\delta)(\lambda_2 - \lambda_2^\delta) - (\lambda_1 - \lambda_1^\delta)(\lambda_2 + \lambda_2^\delta)| = 2|\lambda_1^\delta\lambda_2 - \lambda_1\lambda_2^\delta| = 2l\sqrt{p},$$

it follows from Minkowski's lattice theorem that there exists a pair (m_1, m_2) in $\boldsymbol{Z} \times \boldsymbol{Z} \setminus \{(0,0)\}$ for which

$$|(\lambda_1 + \lambda_1^\delta)m_1 + (\lambda_2 + \lambda_2^\delta)m_2| \leq \sqrt{2l\sqrt{p}}, \quad |(\lambda_1 - \lambda_1^\delta)m_1 + (\lambda_2 - \lambda_2^\delta)m_2| < \sqrt{2l\sqrt{p}}.$$

Therefore, by means of the triangle inequality, we have

$$\begin{aligned}
&|\lambda_1 m_1 + \lambda_2 m_2| + |\lambda_1^\delta m_1 + \lambda_2^\delta m_2| \\
&\qquad \leq \frac{1}{2}(|(\lambda_1 + \lambda_1^\delta)m_1 + (\lambda_2 + \lambda_2^\delta)m_2| + |(\lambda_1 - \lambda_1^\delta)m_1 + (\lambda_2 - \lambda_2^\delta)m_2|) \\
&\qquad < \sqrt{2l\sqrt{p}}.
\end{aligned}$$

Obviously, there exists a pair $(u_1, u_2) \in \boldsymbol{Z} \times \boldsymbol{Z}$ such that

$$|u_1 + u_2\omega| = |\lambda_1 m_1 + \lambda_2 m_2|\,, \quad u_1 \geq 0\,.$$

If $u_2 \leq 0$, put

$$b_1 = u_1 - u_2\,, \quad b_2 = -u_2\,;$$

if $u_2 > 0$, put

$$b_1 = \max(u_1, u_2 - u_1)\,, \quad b_2 = u_2\,.$$

It is then easy to check that $b_1 + b_2\omega$ belongs to either $\mathfrak{l}$ or $l^{-1}\mathfrak{l}$ and that

$$b_1 + b_2\omega + |b_1 - b_2 - b_2\omega| < \sqrt{2l\sqrt{p}}\,, \quad 2b_1 \geq b_2 \geq 0\,, \quad b_1 > 0\,.$$

Thus, (b_1, b_2) can be taken as (a_1, a_2) satisfying the condition of the lemma.

Assume next that $p \equiv 3\,(\mathrm{mod}\ 4)$. Replacing λ_1 by $-\lambda_1$ if necessary, we may also assume that the imaginary part of $\lambda_1\lambda_2^{-1}$ is positive:

$$\lambda_1\lambda_2^{\delta} - \lambda_2\lambda_1^{\delta} = l\sqrt{-p}\,.$$

As is well-known, there exist integers c_1, c_2, m_1, m_2 for which

$$c_1 m_2 - c_2 m_1 = 1\,, \quad \frac{c_1\lambda_1\lambda_2^{-1} + c_2}{m_1\lambda_1\lambda_2^{-1} + m_2} \in \left\{ z \in \boldsymbol{C} \;\middle|\; -\frac{1}{2} \leq \mathrm{Re}(z) < \frac{1}{2}, |z| \geq 1 \right\},$$

where $\mathrm{Re}(z)$ denotes the real part of each $z \in \boldsymbol{C}$. We then see that

$$\begin{aligned}
&\frac{c_1\lambda_1\lambda_2^{-1} + c_2}{m_1\lambda_1\lambda_2^{-1} + m_2} \\
&\quad = \frac{(\lambda_1 c_1 + \lambda_2 c_2)(\lambda_1^{\delta} m_1 + \lambda_2^{\delta} m_2)}{(\lambda_1 m_1 + \lambda_2 m_2)(\lambda_1^{\delta} m_1 + \lambda_2^{\delta} m_2)} \\
&\quad = \frac{2(|\lambda_1|^2 c_1 m_1 + |\lambda_2|^2 c_2 m_2) + (\lambda_1\lambda_2^{\delta} + \lambda_1^{\delta}\lambda_2)(c_1 m_2 + c_2 m_1) + \lambda_1\lambda_2^{\delta} - \lambda_1^{\delta}\lambda_2}{2|\lambda_1 m_1 + \lambda_2 m_2|^2}\,.
\end{aligned}$$

Furthermore, the imaginary part of this complex number is not smaller than $\sqrt{3}/2$. Hence,

$$\frac{-i(\lambda_1\lambda_2^{\delta} - \lambda_1^{\delta}\lambda_2)}{2|\lambda_1 m_1 + \lambda_2 m_2|^2} \geq \frac{\sqrt{3}}{2}\,, \quad \text{namely}\,, \quad |\lambda_1 m_1 + \lambda_2 m_2|^2 \leq \frac{l\sqrt{p}}{\sqrt{3}}\,.$$

On taking a pair $(u_1, u_2) \in \boldsymbol{Z} \times \boldsymbol{Z}$ such that

$$u_1 + u_2\omega = \pm(\lambda_1 m_1 + \lambda_2 m_2)\,, \quad u_1 \geq 0\,,$$

we can conclude the proof of the lemma in the same way as in the latter part of the proof for the case $p \equiv 1\,(\mathrm{mod}\ 4)$. □

REMARK 1. One can take a_1 and a_2 satisfying $a_0 = 1$, when the class number of $\boldsymbol{Q}(\sqrt{p^*})$ is equal to 1.

LEMMA 6. *Assume that $F = \boldsymbol{Q}(\sqrt{p^*})$ and l divides h_n/h_{n-1}. Then*

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

PROOF. For each integer m relatively prime to p,

$$\begin{aligned}\|(\zeta-\zeta^{-1})^{1-\tau^m}\| = \|(\zeta-\zeta^{-1})^{\tau^{-m}-1}\| &= \left\|\frac{\sin(2\pi(1-p^n m)/p^{n+1})}{\sin(2\pi/p^{n+1})}\right\| \\ &= \max_u\left|\frac{-\sin(2\pi mu/p)}{\tan(2\pi u/p^{n+1})} + \cos(2\pi mu/p)\right| \\ &\le \max_u\sqrt{\frac{1}{\tan^2(2\pi u/p^{n+1})}+1} = \sqrt{\frac{1}{\tan^2(\pi(p^{n+1}+1)/p^{n+1})}+1}\,,\end{aligned}$$

where u ranges over the positive integers $< p^{n+1}$ relatively prime to p. It then follows from the definition of θ that

$$\|\theta^{1-\tau^m}\| \le \left(\frac{1}{\tan^2(\pi/p^{n+1})}+1\right)^{(p-1)/4} < \left(\frac{p^{2n+2}}{\pi^2}+1\right)^{(p-1)/4} .$$

Since $\log(x+1) < \log x + 1/x$ for any real number $x > 0$, the above inequalities yield

$$\log\Upsilon < \frac{p-1}{2}\left((n+1)\log p - \log\pi + \frac{\pi^2}{2p^4}\right). \tag{2}$$

Now, assume that $p \equiv 1 \pmod 4$, with a_1 and a_2 as in Lemma 5. Then

$$2a_1 - a_2 \le \sqrt{2l\sqrt{p}}\,,\quad a_2\sqrt{p} \le \sqrt{2l\sqrt{p}}\,,$$

so that

$$a_1 + \frac{p-1}{4}a_2 \le \frac{p+2\sqrt{p}+1}{4\sqrt{p}}\sqrt{2l\sqrt{p}}\,.$$

Hence, by (2) and Lemma 4,

$$l < \sqrt{2l\sqrt{p}}\,\frac{(\sqrt{p}+1)^2(p-1)((n+1)\log p - \log\pi + \pi^2/(2p^4))}{(8\log 2)\sqrt{p}}\,,$$

which means that

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

Assume next that $p \equiv 3 \pmod 4$, with a_0 as in Lemma 5. Since

$$(p+1)^2 la_0 - 4p\left(a_1 + \frac{p-3}{4}a_2\right)^2 = ((p-1)a_1 - (3p-1)a_2)^2 \ge 0\,,$$

$$(p+1)^2 la_0 - 4p\left(a_2 + \frac{p-3}{4}a_2\right)^2 = (p+1)^2\left(a_1 - \frac{a_2}{2}\right)^2 \ge 0\,,$$

we have

$$\max(a_1, a_2) + \frac{p-3}{4}a_2 \le \frac{(p+1)\sqrt{la_0}}{2\sqrt{p}} \le \frac{(p+1)}{2\sqrt{p}}\sqrt{l\sqrt{p/3}}\,.$$

Therefore, it follows from (2) and Lemma 4 that

$$l < \sqrt{l\sqrt{p/3}}\,\frac{(p+1)(p-1)((n+1)\log p - \log\pi + \pi^2/(2p^4))}{(4\log 2)\sqrt{p}}\,,$$

namely, that

$$l < \frac{(p+1)^2}{\sqrt{3p}}\left(\frac{(p-1)((n+1)\log p - \log\pi + \pi^2/(2p^4))}{4\log 2}\right)^2. \qquad \square$$

Let ν be the number of distinct prime divisors of $(p-1)/2$, and let

$$\frac{p-1}{2} = q_1 \cdots q_\nu\,,$$

where $q_1, \ldots, q_\nu$ are prime-powers greater than 1 pairwise relatively prime. Let V be the subset of the cyclic group $\langle e^{2\pi i/(p-1)}\rangle$ consisting of

$$e^{\pi i m_1/q_1} \cdots e^{\pi i m_\nu/q_\nu}$$

for all ν-tuples $(m_1, \ldots, m_\nu)$ of integers with $0 \le m_1 < q_1, \ldots, 0 \le m_\nu < q_\nu$. We understand that $V = \{1\}$ if $p = 3$. Denoting by Φ the set of maps from V to the non-negative integers not greater than $(p+3)l/2$, we put

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

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 $< p^{n+1}$ congruent to suitable elements of V modulo $\mathfrak{p}^{n+1}$. Note that I includes 1. Putting

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

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

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

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

$$A(j, j') = \sum_{u\in I} u\left(\sum_{m\in R_+^*} t^{m+1} j(m, u) + \sum_{m\in R_-^*} t^m j'(m, u)\right),$$

whence

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

LEMMA 7. *Assume that $M < p^n$, and take a pair (j, j') in $(\mathfrak{G}_+ \times \mathfrak{F}_-) \cup (\mathfrak{F}_+ \times \mathfrak{G}_-)$. Then the following conditions are equivalent*:

(i) $A(j, j') \equiv \dfrac{(p+3)l}{2} \displaystyle\sum_{u \in I} u - 1 \pmod{p^n}$.

(ii) *Either*

$$\begin{aligned} j(m_1, 1) &= l - 1 \quad \textit{for some } \ m_1 \in R_+^* , \\ j(m, u) &= l \quad \textit{for all } \ (m, u) \in R_+^* \times I \setminus \{(m_1, 1)\} , \\ j'(m, u) &= l \quad \textit{for all } \ (m, u) \in R_-^* \times I , \end{aligned}$$

or

$$\begin{aligned} j(m, u) &= l \quad \textit{for all } \ (m, u) \in R_+^* \times I , \\ j'(m_2, 1) &= l - 1 \quad \textit{for some } \ m_2 \in R_-^* , \\ j'(m, u) &= l \quad \textit{for all } \ (m, u) \in R_-^* \times I \setminus \{(m_2, 1)\} . \end{aligned}$$

PROOF. Since $|R_+^*| + |R_-^*| = (p+3)/2$, (ii) clearly implies (i). Let us consider the case $(j, j') \in \mathfrak{G}_+ \times \mathfrak{F}_-$, under the condition (i). By the definition of $\mathfrak{G}_+$, there exists a pair (m_1, u_1) in $R_+^* \times I$ with $j \in \mathfrak{G}_+^{m_1, u_1}$. Now we can rewrite (i) as

$$\sum_{u \in I} \Biggl(\sum_{m \in R_+^*} (l - j(m, u)) + \sum_{m \in R_-^*} (l - j'(m, u)) \Biggr) u - 1 \equiv 0 \pmod{p^n} .$$

Since $\mathfrak{p}$ splits completely in $\boldsymbol{Q}(e^{2\pi i/(p-1)})$, there exists a unique $\psi \in \Phi$ such that

$$\psi(\xi) = \sum_{m \in R_+^*} (l - j(m, u)) + \sum_{m \in R_-^*} (l - j'(m, u))$$

if $\xi \in V$, $u \in W$, and $\xi \equiv u \pmod{\mathfrak{p}^{n+1}}$. We then obtain

$$\sum_{\xi \in V} \psi(\xi)\xi - 1 \equiv 0 \pmod{\mathfrak{p}^n} ,$$

which induces

$$\mathfrak{N}\Biggl(\sum_{\xi \in V} \psi(\xi)\xi - 1 \Biggr) \equiv 0 \pmod{p^n} .$$

Hence, the assumption of the lemma, together with the definition of M, implies that

$$\sum_{\xi \in V} \psi(\xi)\xi - 1 = 0 .$$

Therefore, by [2, Lemma 7], $\psi(1) = 1$ and $\psi(\xi) = 0$ for all $\xi \in V \setminus \{1\}$, so that $u_1 = 1$ in particular. We thus see that

$$\begin{aligned} j(m_1, 1) &= l - 1 , \\ j(m, u) &= l \quad \text{for all } \ (m, u) \in R_+^* \times I \setminus \{(m_1, 1)\} , \\ j'(m, u) &= l \quad \text{for all } \ (m, u) \in R_-^* \times I . \end{aligned}$$

In the case $(j, j') \in \mathfrak{F}_+ \times \mathfrak{G}_-$, an argument similar to the above enables us to deduce from the condition (i) that

$$\begin{aligned} j(m,u) &= l \quad \text{for all } (m,u) \in R_+^* \times I, \\ j'(m_2, 1) &= l-1 \quad \text{for some } m_2 \in R_-^*, \\ j'(m,u) &= l \quad \text{for all } (m,u) \in R_-^* \times I \setminus \{(m_2,1)\}. \end{aligned} \qquad \square$$

We put $\iota = 1$ or $\iota = 0$, according to whether $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. For each pair (j, j') in $(\mathfrak{G}_+ \times \mathfrak{F}_-) \cup (\mathfrak{F}_+ \times \mathfrak{G}_-)$, we put

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

The notation above will be used in the proof of the following lemma and the rest of the paper.

LEMMA 8. *Assume that $F = \boldsymbol{Q}(\sqrt{p^*})$ and l divides h_n/h_{n-1}. Then*

$$M \geq p^n.$$

PROOF. As the assumption implies by [4, Lemma 2], there exist integers b_1, b_2 such that $b_1 + b_2\omega$ is not divisible by l but belongs to one of the two prime ideals of $\boldsymbol{Q}(\sqrt{p^*})$ dividing l and that $\eta^{b_1 + b_2\tilde{\omega}}$ is an lth power in E_n (cf. also the proof of Lemma 2). In view of the proof of Lemma 4, we obtain

$$(1-\tau)(b_1 + b_2\tilde{\omega}) = b_1 - \iota b_2 + (b_2 - b_1)\tau + b_2 \left(\sum_{m \in R_-} \tau^m - \sum_{m \in R_+} \tau^{m+1} \right).$$

Since $\mathfrak{p}$ splits completely in $\boldsymbol{Q}(e^{2\pi i/(p-1)})$, we further know that

$$\eta = \theta^{1-\tau} = \prod_{u \in I} ((\zeta^u - \zeta^{-u})(\zeta^{ut} - \zeta^{-ut})^{-1}) = \prod_{u \in I} (e^{2\pi i u/p} (\zeta^{2u} - 1)(\zeta^{2tu} - 1)^{-1}).$$

Hence, the image of the lth power $\eta^{b_1 + b_2\tilde{\omega}}$ in E_n under the automorphism of $\boldsymbol{Q}(\zeta)$ sending ζ^2 to ζ is the product of

$$\prod_{u \in I} \left((\zeta^u - 1)^{b_1 - \iota b_2} (\zeta^{ut} - 1)^{b_2 - b_1} \prod_{m \in R_-} (\zeta^{ut^m} - 1)^{b_2} \prod_{m \in R_+} (\zeta^{ut^{m+1}} - 1)^{-b_2} \right)$$

and some pth root of unity. Thus,

$$\prod_{u \in I} \left((\zeta^u - 1)^{b_1 - \iota b_2} (\zeta^{ut} - 1)^{b_2 - b_1} \prod_{m \in R_-} (\zeta^{ut^m} - 1)^{b_2} \prod_{m \in R_+} (\zeta^{ut^{m+1}} - 1)^{-b_2} \right) = \varepsilon^l$$

for some unit ε of $\boldsymbol{Q}(\zeta)$. Lemma 5 of [2] then shows that

$$\begin{aligned}&\prod_{u\in I}\Big((\zeta^{lu}-1)^{b_1-\iota b_2}(\zeta^{lut}-1)^{b_2-b_1}\prod_{m\in R_-}(\zeta^{lut^m}-1)^{b_2}\prod_{m\in R_+}(\zeta^{lut^{m+1}}-1)^{-b_2}\Big)\\ &\quad\equiv\prod_{u\in I}\Big((\zeta^{u}-1)^{l(b_1-\iota b_2)}(\zeta^{ut}-1)^{l(b_2-b_1)}\prod_{m\in R_-}(\zeta^{ut^m}-1)^{lb_2}\\ &\qquad\times\prod_{m\in R_+}(\zeta^{ut^{m+1}}-1)^{-lb_2}\Big)\pmod{l^2}\,.\end{aligned}\tag{3}$$

We add that ζ^w-1 is relatively prime to l for every $w\in\boldsymbol{Z}$ with $\zeta^w\neq 1$. Now, with an indeterminate Y, let $J(Y)$ denote the polynomial in $\boldsymbol{Z}[Y]$ such that

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

namely, let

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

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

$$(\zeta^{w'}-1)^{lw}\equiv(\zeta^{lw'}-1)^{w-1}(\zeta^{lw'}-1+lwJ(\zeta^{w'}))\pmod{l^2}\,.$$

We therefore see that the right-hand side of (3) is congruent, modulo l^2, to

$$\begin{aligned}\prod_{u\in I}\Big(&(\zeta^{lu}-1)^{b_1-\iota b_2-1}(\zeta^{lu}-1+l(b_1-\iota b_2)J(\zeta^u))(\zeta^{lut}-1)^{b_2-b_1-1}\\ &\times(\zeta^{lut}-1+l(b_2-b_1)J(\zeta^{ut}))\\ &\times\prod_{m\in R_-}((\zeta^{lut^m}-1)^{b_2-1}(\zeta^{lut^m}-1+lb_2J(\zeta^{ut^m})))\\ &\times\prod_{m\in R_+}((\zeta^{lut^{m+1}}-1)^{-b_2-1}(\zeta^{lut^{m+1}}-1-lb_2J(\zeta^{ut^{m+1}})))\Big)\,.\end{aligned}$$

Hence, it follows from (3) that

$$\begin{aligned}&\prod_{u\in I}\Big((\zeta^{lu}-1)(\zeta^{lut}-1)\prod_{m\in R_-}(\zeta^{lut^m}-1)\prod_{m\in R_+}(\zeta^{lut^{m+1}}-1)\Big)\\ &\quad\equiv\prod_{u\in I}\Big((\zeta^{lu}-1+l(b_1-\iota b_2)J(\zeta^u))(\zeta^{lut}-1+l(b_2-b_1)J(\zeta^{ut}))\\ &\qquad\times\prod_{m\in R_-}(\zeta^{lut^m}-1+lb_2J(\zeta^{ut^m}))\prod_{m\in R_+}(\zeta^{lut^{m+1}}-1-lb_2J(\zeta^{ut^{m+1}}))\Big)\pmod{l^2},\end{aligned}$$

so that

$$
\begin{aligned}
(4)\qquad & \sum_{u\in I}\Big((b_1-\iota b_2)J(\zeta^u)\Pi^-_{0,u}+(b_2-b_1)J(\zeta^{ut})\Pi^+_{0,u}\\
&\quad + b_2\sum_{m\in R_-}J(\zeta^{ut^m})\Pi^-_{m,u}-b_2\sum_{m\in R_+}J(\zeta^{ut^{m+1}})\Pi^+_{m,u}\Big)\equiv 0 \pmod{l}\,.
\end{aligned}
$$

Here, for each $(m,u)\in R^*_-\times I$,

$$
\Pi^-_{m,u}=(\zeta^{lut^m}-1)^{-1}\prod_{u'\in I}\Big(\prod_{d\in R^*_-}(\zeta^{lu't^d}-1)\prod_{d\in R^*_+}(\zeta^{lu't^{d+1}}-1)\Big)
$$

and, for each $(m,u)\in R^*_+\times I$,

$$
\Pi^+_{m,u}=(\zeta^{lut^{m+1}}-1)^{-1}\prod_{u'\in I}\Big(\prod_{d\in R^*_-}(\zeta^{lu't^d}-1)\prod_{d\in R^*_+}(\zeta^{lu't^{d+1}}-1)\Big).
$$

On the other hand, since

$$
(-1)^{c-1}\binom{l}{c}\equiv\frac{l}{c}\pmod{l^2}
$$

for every positive integer $c<l$, we find in the case $l>2$ that

$$
J(\alpha)\equiv\sum_{c=1}^{l-1}\frac{\alpha^c}{c}\pmod{l}
$$

for each algebraic integer α. Consequently, (4) then means that

$$
\begin{aligned}
(5)\qquad & \sum_{u\in I}\Big(\sum_{j\in\mathfrak{F}_+}\sum_{j'\in\mathfrak{G}^{0,u}_-}\frac{(-1)^{j'(0,u)+B(j,j')}(\iota b_2-b_1)}{j'(0,u)}\zeta^{A(j,j')}\\
&\quad+\sum_{j\in\mathfrak{G}^{0,u}_+}\sum_{j'\in\mathfrak{F}_-}\frac{(-1)^{j(0,u)+B(j,j')}(b_1-b_2)}{j(0,u)}\zeta^{A(j,j')}\\
&\quad+\sum_{m\in R_-}\sum_{j\in\mathfrak{F}_+}\sum_{j'\in\mathfrak{G}^{m,u}_-}\frac{(-1)^{j'(m,u)+B(j,j')}(-b_2)}{j'(m,u)}\zeta^{A(j,j')}\\
&\quad+\sum_{m\in R_+}\sum_{j\in\mathfrak{G}^{m,u}_+}\sum_{j'\in\mathfrak{F}_-}\frac{(-1)^{j(m,u)+B(j,j')}b_2}{j(m,u)}\zeta^{A(j,j')}\Big)\equiv 0\pmod{l}\,.
\end{aligned}
$$

In the case $l = 2$, it is not difficult to transform (4) into

$$\sum_{u\in I}\Bigg(\sum_{j\in\mathfrak{F}_+}\sum_{j'\in\mathfrak{G}_-^{0,u}}(\iota b_2 - b_1)\zeta^{A(j,j')} + \sum_{j\in\mathfrak{G}_+^{0,u}}\sum_{j'\in\mathfrak{F}_-}(b_1 - b_2)\zeta^{A(j,j')} + \sum_{m\in R_-}\sum_{j\in\mathfrak{F}_+}\sum_{j'\in\mathfrak{G}_-^{m,u}}(-b_2)\zeta^{A(j,j')} + \sum_{m\in R_+}\sum_{j\in\mathfrak{G}_+^{m,u}}\sum_{j'\in\mathfrak{F}_-} b_2\zeta^{A(j,j')}\Bigg) \equiv 0 \pmod 2\,. \tag{6}$$

Next, contrary to the conclusion of the lemma, suppose that $M < p^n$. It follows from [2, Lemma 6] that the partial sum in the left-hand side of (5) or (6), under the condition $A(j, j') \equiv ((p+3)l/2)\sum_{u\in I} u - 1 \pmod{p^n}$, is still congruent to 0 modulo l, according to whether $l > 2$ or $l = 2$. Hence, by Lemma 7,

$$\frac{1}{l-1}\Bigg((b_1 - \iota b_2)\zeta^{A_0-1} + (b_2 - b_1)\zeta^{A_0-t} + b_2\sum_{m\in R_-}\zeta^{A_0-t^m} - b_2\sum_{m\in R_+}\zeta^{A_0-t^{m+1}}\Bigg) \equiv 0 \pmod l\,,$$

where $A_0 = \sum_{u\in I} lu(\sum_{m\in R_+} t^{m+1} + \sum_{m\in R_-} t^m)$. On applying complex conjugation to the above congruence, we have

$$b_1 - \iota b_2 + (b_2 - b_1)\zeta^{t-1} + b_2\sum_{m\in R_-}\zeta^{t^m-1} - b_2\sum_{m\in R_+}\zeta^{t^{m+1}-1} \equiv 0 \pmod l\,,$$

namely,

$$b_1 - \iota b_2 + (b_2 - b_1)e^{2\pi i/p} + b_2\sum_{m\in R_-}e^{2\pi i m/p} - b_2\sum_{m\in R_+}e^{2\pi i(m+1)/p} \equiv 0 \pmod l\,.$$

Since

$$(1 - e^{2\pi i/p})\omega = e^{2\pi i/p} + \sum_{m\in R_-}e^{2\pi i m/p} - \iota - \sum_{m\in R_+}e^{2\pi i(m+1)/p}\,,$$

we then see that

$$(1 - e^{2\pi i/p})(b_1 + b_2\omega) \equiv 0 \pmod l\,,$$

which contradicts our choice of b_1 and b_2, however. Thus, the inequality $M < p^n$ turns out to be false. □

To state the following proposition, we note that, in the case $n = 1$, the right-hand side of the inequality in Lemma 6 exceeds

$$\frac{4(p^{1/\varphi(p-1)} + 1)}{(p-1)(p+3)}\,.$$

PROPOSITION 1. *Assume that $F = \boldsymbol{Q}(\sqrt{p^*})$, and let n_0 be the maximal positive integer such that*

$$\frac{4(p^{n_0/\varphi(p-1)}+1)}{(p-1)(p+3)} < \frac{\Delta}{\sqrt{p}}\left(\frac{(p-1)((n_0+1)\log p - \log\pi + \pi^2/(2p^4))}{4\log 2}\right)^2 .$$

If

$$l \geq \frac{\Delta}{\sqrt{p}}\left(\frac{(p-1)((n_0+1)\log p - \log\pi + \pi^2/(2p^4))}{4\log 2}\right)^2 ,$$

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

PROOF. For any $\psi \in \Phi$,

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

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

$$\left|\sum_{\xi\in V}\psi(\xi)\xi^{\rho} - 1\right| \leq |\psi(1)-1| + \sum_{\xi\in V\setminus\{1\}}\psi(\xi) \leq \frac{p-1}{2}\cdot\frac{(p+3)l}{2} - 1 .$$

Therefore,

$$M \leq \left(\frac{(p-1)(p+3)l}{4} - 1\right)^{\varphi(p-1)} .$$

Now assume that the l-class group of $\boldsymbol{B}_\infty$ is not trivial. It then follows from Lemma 1 that l divides $h_{n'}/h_{n'-1}$ for some positive integer n'. Hence, Lemma 8 and the above estimate for M yield

$$p^{n'} \leq \left(\frac{(p-1)(p+3)l}{4} - 1\right)^{\varphi(p-1)} , \quad \text{i.e.,} \quad l \geq \frac{4(p^{n'/\varphi(p-1)}+1)}{(p-1)(p+3)} .$$

Furthermore, by Lemma 6,

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

The definition of n_0 therefore implies $n' \leq n_0$. Consequently, we have

$$l < \frac{\Delta}{\sqrt{p}}\left(\frac{(p-1)((n_0+1)\log p - \log\pi + \pi^2/(2p^4))}{4\log 2}\right)^2 . \qquad \square$$

Let us prove Theorem 1. We put

$$\Theta = \Lambda\left(1 + \frac{\log\Lambda}{\Lambda - 1}\right), \quad C_1 = \frac{2}{\sqrt{(p-1)(p+3)}} , \quad C_2 = \frac{\sqrt{\Delta}(p-1)\varphi(p-1)}{(2\log 2)p^{1/4}} ,$$

$$C_3 = \frac{\sqrt{\Delta}(p-1)(\log(p/\pi) + \pi^2/(2p^4))}{(4\log 2)p^{1/4}} .$$

Naturally, by the fact $\Lambda > 1$, we know that

$$\frac{\log\Lambda}{\Lambda - 1} > 0 , \quad \Theta > 1 .$$

As in Proposition 1, let n_0 denote the maximal positive integer such that

$$C_1^2(p^{n_0/\varphi(p-1)}+1) < (C_2 \log p^{n_0/(2\varphi(p-1))}+C_3)^2 .$$

It then follows that

$$C_1 p^{n_0/(2\varphi(p-1))} - C_2 \log p^{n_0/(2\varphi(p-1))} - C_3 < 0 .$$

On the other hand, since $\Lambda = \log(C_2/C_1) + C_3/C_2$ and since the function $X - \log X$ of a real variable $X \geq 1$ is (strictly) increasing, we see that, for each real number $x \geq C_2\Theta/C_1$,

$$\begin{aligned} C_1 x - C_2 \log x - C_3 &= C_2\left(\frac{C_1 x}{C_2} - \log\frac{C_1 x}{C_2} - \Lambda\right) \geq C_2(\Theta - \log\Theta - \Lambda) \\ &> C_2\left(\Lambda\left(1+\frac{\log\Lambda}{\Lambda-1}\right) - \log\Lambda - \frac{\log\Lambda}{\Lambda-1} - \Lambda\right) = 0 . \end{aligned}$$

Therefore, we have

$$p^{n_0/(2\varphi(p-1))} < \frac{C_2\Theta}{C_1} .$$

Hence, there exists a real number x_0 for which

$$p^{n_0/(2\varphi(p-1))} < x_0 < \frac{C_2\Theta}{C_1} , \quad C_1 x_0 - C_2 \log x_0 - C_3 = 0 ,$$

so that

$$C_2 \log p^{n_0/(2\varphi(p-1))} + C_3 < C_2 \log x_0 + C_3 < C_2\Theta .$$

Proposition 1 states, however, that the l-class group of $\boldsymbol{B}_\infty$ is trivial if

$$l \geq (C_2 \log p^{n_0/(2\varphi(p-1))} + C_3)^2 .$$

We thus obtain Theorem 1.

3. Cyclotomic fields of 3-power conductor. In this section, we prove the following theorem.

THEOREM 2. *Assume that $p = 3$ and l is congruent to either 2, 4, 5, or 7 modulo 9. Then l does not divide the class number of the cyclotomic field of 3^nth roots of unity.*

Henceforth, we assume that p is odd except in the following lemma.

LEMMA 9. *Let m and N be positive integers, and take $2N$ integers $c_1, \dots, c_N, g_1, \dots, g_N$. For each integer d, let $s(d)$ denote the sum of c_u for all positive integers $u \leq N$ with $g_u \equiv d \pmod{p^{m+1}}$. Then*

$$\sum_{u=1}^{N} c_u e^{2\pi i g_u/p^{m+1}} \equiv 0 \pmod{l}$$

if and only if

$$s(d) \equiv s(d') \pmod{l}$$

for all pairs $(d, d') \in \mathbf{Z} \times \mathbf{Z}$ with $d \equiv d' \pmod{p^m}$.

PROOF. The lemma follows from the fact that the p^{m+1}th cyclotomic polynomial in an indeterminate Y is of the form $\sum_{w=0}^{p-1} Y^{p^m w}$. □

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

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

Also, 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

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

Moreover, in the case $l > 2$, we put

$$s_+(w_1, w_2;\ d) = \sum_{u\in I}\Bigg(w_1 \sum_{(j,j')\in\mathcal{P}_+^{0,u}(d)} \frac{(-1)^{j(0,u)+B(j,j')}}{j(0,u)} + w_2 \sum_{m\in R_+}\ \sum_{(j,j')\in\mathcal{P}_+^{m,u}(d)} \frac{(-1)^{j(m,u)+B(j,j')}}{j(m,u)}\Bigg),$$

$$s_-(w_1, w_2;\ d) = \sum_{u\in I}\Bigg(w_1 \sum_{(j,j')\in\mathcal{P}_-^{0,u}(d)} \frac{(-1)^{j'(0,u)+B(j,j')}}{j'(0,u)} + w_2 \sum_{m\in R_-}\ \sum_{(j,j')\in\mathcal{P}_-^{m,u}(d)} \frac{(-1)^{j'(m,u)+B(j,j')}}{j'(m,u)}\Bigg),$$

for each $(w_1, w_2) \in \mathbf{Z} \times \mathbf{Z}$; in the case $l = 2$, we put

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

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

for each $(w_1, w_2) \in \mathbf{Z} \times \mathbf{Z}$. Note that the rational numbers $s_+(w_1, w_2;\ d)$ and $s_-(w_1, w_2;\ d)$ are l-adic integers.

LEMMA 10. *Assume that $F = \mathbf{Q}(\sqrt{p^*})$ and l divides h_n/h_{n-1}. Take any pair $(d, d') \in \mathbf{Z} \times \mathbf{Z}$ with $d \equiv d' \pmod{p^n}$. Then either*

$$\begin{aligned} &s_+(a_1 - a_2, a_2;\ d) - s_-(a_1 - \iota a_2, a_2;\ d) \\ &\qquad \equiv s_+(a_1 - a_2, a_2;\ d') - s_-(a_1 - \iota a_2, a_2;\ d') \pmod{l} \end{aligned}$$

or

$$\begin{aligned} &s_+(a_1, -a_2;\ d) - s_-(a_1 + (\iota - 1)a_2, -a_2;\ d) \\ &\qquad \equiv s_+(a_1, -a_2;\ d') - s_-(a_1 + (\iota - 1)a_2, -a_2;\ d') \pmod{l}. \end{aligned}$$

PROOF. As we know from Lemma 2, $\eta^{a_1+a_2\tilde{\omega}}$ or $\eta^{a_1-a_2-a_2\tilde{\omega}}$ is an lth power in E_n. Suppose that $\eta^{a_1+a_2\tilde{\omega}}$ is an lth power in E_n. Then, by an argument similar to that, in the proof of Lemma 8, which has led us to (5) and (6) through (3) and (4), we are led to the following conclusion: in the case $l > 2$,

$$\sum_{u\in I}\Bigg(\sum_{j\in\mathfrak{F}_+}\sum_{j'\in\mathfrak{G}_-^{0,u}}\frac{(-1)^{j'(0,u)+B(j,j')}(\iota a_2-a_1)}{j'(0,u)}\zeta^{A(j,j')}$$
$$+\sum_{j\in\mathfrak{G}_+^{0,u}}\sum_{j'\in\mathfrak{F}_-}\frac{(-1)^{j(0,u)+B(j,j')}(a_1-a_2)}{j(0,u)}\zeta^{A(j,j')}$$
$$+\sum_{m\in R_-}\sum_{j\in\mathfrak{F}_+}\sum_{j'\in\mathfrak{G}_-^{m,u}}\frac{(-1)^{j'(m,u)+B(j,j')}(-a_2)}{j'(m,u)}\zeta^{A(j,j')}$$
$$+\sum_{m\in R_+}\sum_{j\in\mathfrak{G}_+^{m,u}}\sum_{j'\in\mathfrak{F}_-}\frac{(-1)^{j(m,u)+B(j,j')}a_2}{j(m,u)}\zeta^{A(j,j')}\Bigg)\equiv 0 \pmod{l}\,;$$

in the case $l = 2$,

$$\sum_{u\in I}\Bigg(\sum_{j\in\mathfrak{F}_+}\sum_{j'\in\mathfrak{G}_-^{0,u}}(\iota a_2-a_1)\zeta^{A(j,j')}+\sum_{j\in\mathfrak{G}_+^{0,u}}\sum_{j'\in\mathfrak{F}_-}(a_1-a_2)\zeta^{A(j,j')}$$
$$+\sum_{m\in R_-}\sum_{j\in\mathfrak{F}_+}\sum_{j'\in\mathfrak{G}_-^{m,u}}(-a_2)\zeta^{A(j,j')}+\sum_{m\in R_+}\sum_{j\in\mathfrak{G}_+^{m,u}}\sum_{j'\in\mathfrak{F}_-}a_2\zeta^{A(j,j')}\Bigg)\equiv 0 \pmod{2}\,.$$

Therefore, by the definitions of $s_+(w_1, w_2;\ d'')$, $s_-(w_1, w_2;\ d'')$ for $w_1,\ w_2,\ d'' \in \boldsymbol{Z}$, Lemma 9 shows that

$$s_+(a_1-a_2, a_2;\ d) - s_-(a_1-\iota a_2, a_2;\ d)$$
$$\equiv s_+(a_1-a_2, a_2;\ d') - s_-(a_1-\iota a_2, a_2;\ d') \pmod{l}\,.$$

When $\eta^{a_1-a_2-a_2\tilde{\omega}}$ is an lth power in E_n, replacing (a_1, a_2) by $(a_1-a_2, -a_2)$ in the above, we have

$$s_+(a_1, -a_2;\ d) - s_-(a_1+(\iota-1)a_2, -a_2;\ d)$$
$$\equiv s_+(a_1, -a_2;\ d') - s_-(a_1+(\iota-1)a_2, -a_2;\ d') \pmod{l}\,. \qquad \square$$

We now suppose that $p = 3$ in the following assertion.

PROPOSITION 2. *If l is congruent to either* 2, 4, 5, *or* 7 *modulo* 9, *then the l-class group of the $\boldsymbol{Z}_3$-extension $\boldsymbol{B}_\infty$ over $\boldsymbol{Q}$ is trivial.*

PROOF. When l is congruent to 2 or 5 modulo 9, the proposition holds by [2, Lemma 10]. We assume henceforth that l is congruent to 4 or 7 modulo 9, namely, that $F = \boldsymbol{Q}(\sqrt{-3})$. Assume also that l divides h_n/h_{n-1}, contrary to the assertion of the proposition (cf. Lemma 1). Then Lemma 6 implies that

$$l < \frac{4}{3}\left(\frac{(n+1)\log 3 - \log\pi + \pi^2/162}{\log 2}\right)^2$$

and, since $M = 3l - 1$, Lemma 8 yields $3^{n-1} < l$. Therefore, we know that the pair (l, n) belongs to the set

$$\{(7,2),\ (13,2),\ (13,3),\ (31,4),\ (43,4)\}\,.$$

In the case $l = 43$, we may let $(a_1, a_2) = (7, 1)$. Hence, if $(l, n) = (43, 4)$, then by Lemma 4 and by [4, Lemma 4], we have

$$43 < \frac{7\log\Upsilon}{\log 2} < \frac{7\log(3^5\sqrt{3}/(2\pi) + 1/2)}{\log 2} < 43\,,$$

a contradiction. In the case where $(l, n) = (13, 2)$, we may let $(a_1, a_2) = (4, 1)$ and the same lemmas still give us a contradiction:

$$13 < \frac{4\log\Upsilon}{\log 2} < \frac{4\log(3^3\sqrt{3}/(2\pi) + 1/2)}{\log 2} < 12\,.$$

Thus, (l, n) must be $(7, 2)$, $(13, 3)$, or $(31, 4)$.

Since $|R_-^* \times I| = 1$, it is understood that

$$\mathfrak{F}_- = \{0, l\}, \quad \mathfrak{G}_- = \{1, \ldots, l-1\}\,.$$

When a map $j \in \mathfrak{F}_+$ satisfies $j(0,1) = j(1,1)$, we naturally identify j with the common value of j. Suppose now that $(l, n) = (31, 4)$, so that we may put $(a_1, a_2) = (6, 1)$. We then have

$$\mathcal{P}_+^{0,1}(92) = \emptyset\,, \quad \mathcal{P}_+^{1,1}(92) = \{(j_1, 0)\}, \quad \mathcal{P}_-^{0,1}(92) = \{(31, 30)\}\,,$$
$$\mathcal{P}_+^{0,1}(11) = \{(j_2, 31)\}\,, \quad \mathcal{P}_+^{1,1}(11) = \emptyset, \quad \mathcal{P}_-^{0,1}(11) = \{(0, 11)\}\,,$$

with the maps $j_1 \in \mathfrak{G}_+^{1,1}$, $j_2 \in \mathfrak{G}_+^{0,1}$ defined by

$$j_1(0,1) = 0\,, \quad j_1(1,1) = 11\,, \quad j_2(0,1) = 30\,, \quad j_2(1,1) = 31\,.$$

Hence,

$$s_+(5, 1;\ 92) = -\frac{1}{11}\,, \quad s_-(6, 1;\ 92) = -\frac{1}{5}\,, \quad s_+(5, 1;\ 11) = -\frac{1}{6}\,,$$
$$s_-(6, 1;\ 11) = -\frac{6}{11}\,, \quad s_+(6, -1;\ 92) = \frac{1}{11}\,, \quad s_-(5, -1;\ 92) = -\frac{1}{6}\,,$$
$$s_+(6, -1;\ 11) = -\frac{1}{5}\,, \quad s_-(5, -1;\ 11) = -\frac{5}{11}\,.$$

These imply that

$$
\begin{aligned}
s_+(5, 1;\ 92) - s_-(6, 1;\ 92) &\equiv 8 \pmod{31}\,,\\
s_+(5, 1;\ 11) - s_-(6, 1;\ 11) &\equiv 14 \pmod{31}\,,\\
s_+(6, -1;\ 92) - s_-(5, -1;\ 92) &\equiv 12 \pmod{31}\,,\\
s_+(6, -1;\ 11) - s_-(5, -1;\ 11) &\equiv 29 \pmod{31}\,.
\end{aligned}
$$

Therefore, it follows from Lemma 10 that 31 does not divide h_4/h_3, which is a contradiction. Assume next that $(l, n) = (13, 3)$. Then we have

$$
\begin{gathered}
\mathcal{P}_+^{0,1}(38) = \emptyset\,, \quad \mathcal{P}_+^{1,1}(38) = \{(j_3, 0)\}\,, \quad \mathcal{P}_-^{0,1}(38) = \{(13, 12)\}\,,\\
\mathcal{P}_+^{0,1}(11) = \{(j_4, 13)\}\,, \quad \mathcal{P}_+^{1,1}(11) = \emptyset\,, \quad \mathcal{P}_-^{0,1}(11) = \{(0, 11)\}\,,
\end{gathered}
$$

with the maps $j_3 \in \mathfrak{G}_+^{1,1}$, $j_4 \in \mathfrak{G}_+^{0,1}$ such that

$$
j_3(0, 1) = 0\,, \quad j_3(1, 1) = 11\,, \quad j_4(0, 1) = 12\,, \quad j_4(1, 1) = 13\,.
$$

Therefore

$$
\begin{gathered}
s_+(3, 1;\ 38) = -\frac{1}{11}\,, \quad s_-(4, 1;\ 38) = -\frac{1}{3}\,, \quad s_+(3, 1;\ 11) = -\frac{1}{4}\,,\\
s_-(4, 1;\ 11) = -\frac{4}{11}\,, \quad s_+(4, -1;\ 38) = \frac{1}{11}\,, \quad s_-(3, -1;\ 38) = -\frac{1}{4}\,,\\
s_+(4, -1;\ 11) = -\frac{1}{3}\,, \quad s_-(3, -1;\ 11) = -\frac{3}{11}\,,
\end{gathered}
$$

and, consequently,

$$
\begin{aligned}
s_+(3, 1;\ 38) - s_-(4, 1;\ 38) &\equiv 3 \pmod{13}\,,\\
s_+(3, 1;\ 11) - s_-(4, 1;\ 11) &\equiv 1 \pmod{13}\,,\\
s_+(4, -1;\ 38) - s_-(3, -1;\ 38) &\equiv 3 \pmod{13}\,,\\
s_+(4, -1;\ 11) - s_-(3, -1;\ 11) &\equiv 9 \pmod{13}\,.
\end{aligned}
$$

As we can let $(a_1, a_2) = (4, 1)$, Lemma 10 shows, by the above, that 13 does not divide h_3/h_2, which contradicts our assumption. Suppose, finally, that $(l, n) = (7, 2)$. Then

$$
\begin{gathered}
\mathcal{P}_+^{0,1}(20) = \{(j_5, 0), (j_6, 7)\}\,, \quad \mathcal{P}_+^{1,1}(20) = \emptyset\,, \quad \mathcal{P}_-^{0,1}(20) = \{(j_7, 4), (7, 6)\}\,,\\
\mathcal{P}_+^{0,1}(11) = \{(j_8, 0), (j_9, 7)\}\,, \quad \mathcal{P}_+^{1,1}(11) = \{(j_{10}, 0), (j_{11}, 0)\}\,, \quad \mathcal{P}_-^{0,1}(11) = \emptyset\,,
\end{gathered}
$$

where maps $j_5 \in \mathfrak{G}_+^{0,1}$, $j_6 \in \mathfrak{G}_+^{0,1}$, $j_7 \in \mathfrak{F}_+$, $j_8 \in \mathfrak{G}_+^{0,1}$, $j_9 \in \mathfrak{G}_+^{0,1}$, $j_{10} \in \mathfrak{G}_+^{1,1}$, $j_{11} \in \mathfrak{G}_+^{1,1}$ are defined by

$$
\begin{gathered}
j_5(0, 1) = 2\,, \quad j_5(1, 1) = 0\,, \quad j_6(0, 1) = 4\,, \quad j_6(1, 1) = 0\,, \quad j_7(0, 1) = 7\,,\\
j_7(1, 1) = 0\,, \quad j_8(0, 1) = 4\,, \quad j_8(1, 1) = 7\,, \quad j_9(0, 1) = 6\,, \quad j_9(1, 1) = 7\,,\\
j_{10}(0, 1) = 0\,, \quad j_{10}(1, 1) = 2\,, \quad j_{11}(0, 1) = 7\,, \quad j_{11}(1, 1) = 4\,.
\end{gathered}
$$

Hence,

$$s_+(2,1;\ 20) = -\frac{1}{2}\,, \quad s_-(3,1;\ 20) = \frac{1}{4}\,, \quad s_+(2,1;\ 11) = -\frac{1}{12}\,, \quad s_-(3,1;\ 11) = 0\,,$$
$$s_+(3,-1;\ 20) = -\frac{3}{4}\,, \quad s_-(2,-1;\ 20) = \frac{1}{6}\,, \quad s_+(3,-1;\ 11) = \frac{1}{2}\,, \quad s_-(2,-1;\ 11) = 0\,,$$

so that

$$\begin{aligned} s_+(2,1;\ 20) - s_-(3,1;\ 20) &\equiv 1 \pmod 7\,,\\ s_+(2,1;\ 11) - s_-(3,1;\ 11) &\equiv 4 \pmod 7\,,\\ s_+(3,-1;\ 20) - s_-(2,-1;\ 20) &\equiv 2 \pmod 7\,,\\ s_+(3,-1;\ 11) - s_-(2,-1;\ 11) &\equiv 4 \pmod 7\,. \end{aligned}$$

However, we can put $(a_1, a_2) = (3, 1)$. Lemma 10 therefore shows that 7 does not divide h_2/h_1. This contradiction, together with Lemma 1, completes the proof of the proposition. □

REMARK 2. It is known that $h_3 = 1$ if $p = 3$ (cf. van der Linden [1, Theorem 1]).

We conclude the present section by proving Theorem 2. Let h^* denote the relative class number of the cyclotomic field of 3^nth roots of unity. As is seen in the proof of Proposition 3 of [2], Theorem 1 of [2] shows that l does not divide h^* under the assumption of Theorem 2 (for an original argument, cf. Washington [7, Section IV]). Hence, by Proposition 2, l does not divide $h^* h_{n-1}$, the class number of the cyclotomic field of 3^nth roots of unity.

4. Cyclotomic fields of 2-power conductor. Throughout this section, we suppose that $p = 2$. We eventually prove the following result.

THEOREM 3. *Assume that l is congruent to* 3 *or* 5 *modulo* 8. *Then, for any positive integer u, the class number of the cyclotomic field of 2^uth roots of unity is not divisible by l.*

We put

$$\zeta = e^{\pi i/2^{n+1}}\,,$$

whence

$$\eta = \tan\frac{\pi}{2^{n+2}} = \frac{\zeta - 1}{i(\zeta + 1)}\,.$$

Recall that $n \geq 2$ and that σ is induced by the automorphism of $\boldsymbol{Q}(\zeta)$ sending ζ to ζ^3. We put

$$\sigma_u = \sigma^{2^{n-u-1}}$$

for each positive integer $u < n$.

LEMMA 11. *Assume that l divides h_n/h_{n-1} and is congruent to* 3 *or* 5 *modulo* 8. *Then*

$$l < \frac{a_1 - \iota a_2}{\log 2}\log\left(\cot\frac{\pi}{2^{n+2}}\right) + \frac{a_2}{\log 2}\log\left(\frac{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) + 1}{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) - 1}\right).$$

PROOF. We first prove that

$$\|\eta^{\sigma_1-1}\| = \|\eta^{1-\sigma_1}\| = \frac{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) + 1}{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) - 1} . \tag{7}$$

Since $\eta^\tau = -\eta^{-1}$, we have $\eta^{(1-\sigma_1)\tau} = \eta^{\sigma_1-1}$ which implies that

$$\|\eta^{1-\sigma_1}\| = \|\eta^{\sigma_1-1}\| .$$

Let S be the set of positive odd integers smaller than 2^{n+2}. In the case where $n \geq 3$ so that $3^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+2}}$,

$$\begin{aligned}\eta^{\sigma_1-1} &= \frac{i\zeta - 1}{i(i\zeta+1)} \cdot \frac{i(\zeta+1)}{\zeta-1} = \frac{i\zeta - 1 + i - \zeta^{-1}}{i\zeta + 1 - i - \zeta^{-1}} = \frac{e^{\pi i/4}\zeta - e^{-\pi i/4}\zeta^{-1} + i\sqrt{2}}{e^{\pi i/4}\zeta - e^{-\pi i/4}\zeta^{-1} - i\sqrt{2}} \\ &= \frac{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) + 1}{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) - 1} = 1 + \frac{2}{\sin(\pi/4 + \pi/2^{n+1})/\sin(\pi/4) - 1} ,\end{aligned}$$

$$\begin{aligned}\min_{u\in S}\left|\frac{\sin(\pi u/4 + \pi u/2^{n+1})}{\sin(\pi u/4)} - 1\right| &\geq \min_{u\in S}\left|\frac{|\sin(\pi u/4 + \pi u/2^{n+1})|}{\sin(\pi/4)} - 1\right| \\ &= \min_{u\in S}\left|\frac{|\sin(\pi u/2^{n+1})|}{\sin(\pi/4)} - 1\right| = \frac{\sin(\pi/4 + \pi/2^{n+1})}{\sin(\pi/4)} - 1 ,\end{aligned}$$

and, hence,

$$\|\eta^{\sigma_1-1}\| = \max_{u\in S}\left|1 + \frac{2}{\sin(\pi u/4 + \pi u/2^{n+1})/\sin(\pi u/4) - 1}\right| \leq \eta^{\sigma_1-1} .$$

Similarly, in the case $n = 2$, we easily see that

$$\begin{aligned}\|\eta^{1-\sigma_1}\| = \|\eta^{\sigma_1^{-1}-1}\| &= \max_{u\in S}\left|1 + \frac{2}{\sin(\pi u/4 + \pi u/8)/\sin(\pi u/4) - 1}\right| \\ &\leq 1 + \frac{2}{\sin(\pi/4 + \pi/8)/\sin(\pi/4) - 1} = \frac{\cos(\pi/8) + \sin(\pi/8) + 1}{\cos(\pi/8) + \sin(\pi/8) - 1} = \eta^{\sigma_1^{-1}-1} .\end{aligned}$$

Therefore (7) is proved. On the other hand, Lemma 4 of [4] implies that

$$\|\eta\| = \|\eta^{-1}\| = \cot\frac{\pi}{2^{n+2}} .$$

Now, assume that $l \equiv 5 \pmod 8$. Then, as $\tilde{\omega} = \sigma_1$,

$$\|\eta^{a_1+a_2\tilde{\omega}}\| \leq \|\eta\|^{a_1-a_2}\|\eta^{\sigma_1-1}\|^{a_2} , \quad \|\eta^{a_1-a_2\tilde{\omega}}\| \leq \|\eta\|^{a_1-a_2}\|\eta^{1-\sigma_1}\|^{a_2} .$$

Lemma 3 of [4] shows, however, that

$$2^l < \max(\|\eta^{a_1+a_2\tilde{\omega}}\|, \|\eta^{a_1-a_2\tilde{\omega}}\|) .$$

Hence, it follows from (7) and [4, Lemma 4] that

$$l < \frac{a_1 - a_2}{\log 2}\log\left(\cot\frac{\pi}{2^{n+2}}\right) + \frac{a_2}{\log 2}\log\left(\frac{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) + 1}{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) - 1}\right) .$$

Assume next that $l \equiv 3 \pmod 8$. As $\tilde{\omega} = \sigma_2 - \sigma_2^{-1} = \sigma_2^{-1}(\sigma_1 - 1)$, we then have

$$\|\eta^{a_1+a_2\tilde{\omega}}\| \leq \|\eta\|^{a_1}\|\eta^{\sigma_1-1}\|^{a_2} , \quad \|\eta^{a_1-a_2\tilde{\omega}}\| \leq \|\eta\|^{a_1}\|\eta^{1-\sigma_1}\|^{a_2} .$$

Thus (7), together with [4, Lemmas 3 and 4], proves

$$l < \frac{a_1}{\log 2}\log\left(\cot\frac{\pi}{2^{n+2}}\right) + \frac{a_2}{\log 2}\log\left(\frac{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) + 1}{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) - 1}\right). \qquad \square$$

LEMMA 12. *Assume that l divides h_n/h_{n-1}. Then*

$$l < (n+1)^2 \quad \textit{if } l \equiv 5 \pmod 8\,;$$
$$l < \frac{3}{2}\left(n + \frac{2}{3}\right)^2 \quad \textit{if } l \equiv 3 \pmod 8\,.$$

PROOF. For simplicity, let

$$\gamma_1 = \frac{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) + 1}{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) - 1} = 1 + \frac{2}{\cos(\pi/2^{n+1}) + \sin(\pi/2^{n+1}) - 1}\,,$$
$$\gamma_2 = \cos\frac{\pi}{2^{n+1}} - \sin\frac{\pi}{2^{n+1}} + 1 = 2\sqrt{2}\cos\frac{\pi}{2^{n+2}}\cos\left(\frac{\pi}{4} + \frac{\pi}{2^{n+2}}\right).$$

Since

$$\cos\frac{\pi}{2^{n+1}} + \sin\frac{\pi}{2^{n+1}} - 1 = 2\sqrt{2}\sin\frac{\pi}{2^{n+2}}\cos\left(\frac{\pi}{4} + \frac{\pi}{2^{n+2}}\right)$$
$$> \frac{\sqrt{2}\pi}{2^{n+1}}\cos\frac{\pi}{2^{n+2}}\cos\left(\frac{\pi}{4} + \frac{\pi}{2^{n+2}}\right) = \frac{\pi\gamma_2}{2^{n+2}}\,,$$

it follows that

$$\gamma_1 < 1 + \frac{2^{n+3}}{\pi\gamma_2}\,.$$

Therefore, noting that $\log(1 + 2^{n+3}/(\pi\gamma_2)) < \log(2^{n+3}/(\pi\gamma_2)) + \pi\gamma_2/2^{n+3}$, we obtain

$$\frac{\log\gamma_1}{\log 2} < n + 3 - \frac{\log(\pi\gamma_2)}{\log 2} + \frac{\pi\gamma_2}{2^{n+3}\log 2}\,. \tag{8}$$

We now consider the case $l \equiv 5 \pmod 8$. By Lemma 11,

$$l < \frac{a_1 - a_2}{\log 2}\log\frac{2^{n+2}}{\pi} + \frac{a_2\log\gamma_1}{\log 2}\,.$$

However, simple calculations show that the right-hand side of (8) is smaller than $n+1$. Hence,

$$l < (a_1 - a_2)(n+1) + a_2(n+1) = a_1(n+1) < \sqrt{l}(n+1)\,,$$

and, consequently,

$$l < (n+1)^2\,.$$

We next consider the case where $l \equiv 3 \pmod 8$ so that $n \geq 3$. In this case, the right-hand side of (8) is smaller than $n + 2/3$ and hence, by Lemma 11,

$$l < \frac{a_1}{\log 2}\log\frac{2^{n+2}}{\pi} + a_2\left(n + \frac{2}{3}\right) < (a_1 + a_2)\left(n + \frac{2}{3}\right).$$

Furthermore,

$$\frac{3l}{2} - (a_1 + a_2)^2 = \frac{3(a_1^2 + 2a_2^2)}{2} - (a_1 + a_2)^2 = \frac{(a_1 - 2a_2)^2}{2} \geq 0 .$$

We therefore obtain

$$l < \sqrt{\frac{3l}{2}}\left(n + \frac{2}{3}\right), \quad \text{i.e.,} \quad l < \frac{3}{2}\left(n + \frac{2}{3}\right)^2 . \qquad \square$$

For each positive integer m, let O_m denote the set of all odd positive integers u with $l(m-1) < u < lm$. For each integer u relatively prime to l, let $r(u)$ denote the least positive residue modulo l. If l is congruent to 5 modulo 8 and any integer d is given, let $U_1(d)$ denote the set of all integers u such that

$$u \in O_1 \cup O_2 \cup O_3 \cup O_4 , \quad u \equiv d \pmod{2^{n+2}} ,$$

let $U_2(d)$ denote the set of all integers u such that

$$u - 2^n \in O_1 \cup O_2 \cup O_3 \cup O_4 , \quad u \equiv d \pmod{2^{n+2}} ,$$

and let

$$s_1(d) = a_1 \sum_{u \in U_1(d)} \frac{1}{r(u)} , \quad s_2(d) = a_2 \sum_{u \in U_2(d)} \frac{(-1)^{(u-1)/2}}{r(u - 2^n)} .$$

LEMMA 13. *Assume that l is congruent to 5 modulo 8 and divides h_n/h_{n-1}. Then, for any pair $(d, d') \in \mathbf{Z} \times \mathbf{Z}$ with $d \equiv d' \pmod{2^{n+1}}$, either*

$$s_1(d) + s_2(d) \equiv s_1(d') + s_2(d') \pmod{l}$$

or

$$s_1(d) - s_2(d) \equiv s_1(d') - s_2(d') \pmod{l} .$$

Furthermore,

$$l > 2^{n-1} .$$

PROOF. In the case $n \geq 3$,

$$\eta^{a_1 + a_2\tilde{\omega}} = \frac{(\zeta - 1)^{a_1}(i\zeta - 1)^{a_2}}{i^{a_1}(\zeta + 1)^{a_1} i^{a_2}(i\zeta + 1)^{a_2}} = \frac{(\zeta - 1)^{a_1}(\zeta + i)^{a_2}}{i^{a_1+a_2}(\zeta + 1)^{a_1}(\zeta - i)^{a_2}} ,$$

$$\eta^{a_1 - a_2\tilde{\omega}} = \frac{(\zeta - 1)^{a_1} i^{a_2}(i\zeta + 1)^{a_2}}{i^{a_1}(\zeta + 1)^{a_1}(i\zeta - 1)^{a_2}} = \frac{(\zeta - 1)^{a_1}(\zeta - i)^{a_2}}{i^{a_1-a_2}(\zeta + 1)^{a_1}(\zeta + i)^{a_2}} .$$

In the case $n = 2$,

$$\eta^{a_1 + a_2\tilde{\omega}} = \frac{(\zeta - 1)^{a_1}(\zeta - i)^{a_2}}{i^{a_1+a_2}(\zeta + 1)^{a_1}(\zeta + i)^{a_2}} , \quad \eta^{a_1 - a_2\tilde{\omega}} = \frac{(\zeta - 1)^{a_1}(\zeta + i)^{a_2}}{i^{a_1-a_2}(\zeta + 1)^{a_1}(\zeta - i)^{a_2}} .$$

On the other hand, $\eta^{a_1+a_2\tilde{\omega}}$ or $\eta^{a_1-a_2\tilde{\omega}}$ is an lth power in E_n by Lemma 2, $\zeta^4 - 1$ is relatively prime to l, and $i^l = i$ holds. It therefore follows from [2, Lemma 5] that

$$\begin{aligned}&(\zeta - 1)^{la_1}(\zeta + 1)^{-la_1}(\zeta + i)^{l\kappa a_2}(\zeta - i)^{-l\kappa a_2} \\ &\quad \equiv (\zeta^l - 1)^{a_1}(\zeta^l + 1)^{-a_1}(\zeta^l + i)^{\kappa a_2}(\zeta^l - i)^{-\kappa a_2} \pmod{l^2} ,\end{aligned}$$

where κ is equal to 1 or -1. This implies that

$$(\zeta^l+1)(\zeta^l+i)(\zeta^l-i)a_1\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c(-1)^{l-c}-(\zeta^l-1)(\zeta^l+i)(\zeta^l-i)a_1\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c$$
$$+(\zeta^l-1)(\zeta^l+1)(\zeta^l-i)\kappa a_2\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c i^{l-c}$$
$$-(\zeta^l-1)(\zeta^l+1)(\zeta^l+i)\kappa a_2\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c(-i)^{l-c}$$
$$\equiv 0 \pmod{l^2},$$

because

$$(\zeta+\alpha)^{lw}\equiv(\zeta^l+\alpha^l)^{w-1}\left(\zeta^l+\alpha^l+w\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c\alpha^{l-c}\right) \pmod{l^2}$$

for each $w\in\boldsymbol{Z}$ and each algebraic integer α with $\zeta^l+\alpha^l\neq 0$. Hence, by the relation

$$\binom{l}{c}\equiv\frac{(-1)^{c-1}l}{c} \pmod{l^2}$$

for each positive integer $c<l$, we have

$$a_1(\zeta^{2l}+1)\left((\zeta^l+1)\sum_{c=1}^{l-1}\frac{\zeta^c}{c}-(\zeta^l-1)\sum_{c=1}^{l-1}\frac{(-1)^{c-1}\zeta^c}{c}\right)$$
$$+\kappa a_2(\zeta^{2l}-1)\left((\zeta^l-i)\sum_{c=1}^{l-1}\frac{(-1)^{c-1}i^{l-c}\zeta^c}{c}-(\zeta^l+i)\sum_{c=1}^{l-1}\frac{i^{l-c}\zeta^c}{c}\right)\equiv 0 \pmod{l},$$

namely,

$$a_1(\zeta^{2l}+1)\left(\zeta^l\sum_{b=1}^{(l-1)/2}\frac{\zeta^{2b}}{2b}+\sum_{b=1}^{(l-1)/2}\frac{\zeta^{2b-1}}{2b-1}\right)$$
$$+\kappa a_2(\zeta^{2l}-1)\left(-\zeta^{l+2^n}\sum_{b=1}^{(l-1)/2}\frac{(-1)^b\zeta^{2b}}{2b}+\zeta^{2^n}\sum_{b=1}^{(l-1)/2}\frac{(-1)^b\zeta^{2b-1}}{2b-1}\right)\equiv 0 \pmod{l}.$$

Therefore, in view of the definitions of $s_1(d)$, $s_2(d)$ for $d\in\boldsymbol{Z}$, we know that the first assertion of our lemma is proved by Lemma 9. The second assertion follows from the first. Indeed, if $l<2^{n-1}$, then

$$4l-1<2l-1+2^n<2^{n+1},$$

so that we obtain

$$U_1(2l-1+2^n)=\emptyset,\quad U_2(2l-1+2^n)=\{2l-1+2^n\},$$
$$U_1(2l-1+3\cdot 2^n)=U_2(2l-1+3\cdot 2^n)=\emptyset,$$

which imply that

$$s_1(2l-1+2^n)=0\,,\quad s_2(2l-1+2^n)=\frac{a_2}{l-1}\,,$$

$$s_1(2l-1+3\cdot 2^n)=s_2(2l-1+3\cdot 2^n)=0\,. \qquad \square$$

Next, let

$$O_{3,4}=\{u\in O_3\cup O_4\mid u\equiv 3\pmod 4\}\,.$$

If l is congruent to 3 modulo 8 and d is any integer, let $U_1(d)$ denote the set of integers u for which

$$u\equiv d\pmod{2^{n+2}},\quad u\in O_1\cup O_2\cup O_5\cup O_6\,;$$

let $U_{2,1}(d)$, $U_{2,2}(d)$, and $U_{2,3}(d)$ denote, respectively, the sets of integers u congruent to d modulo 2^{n+2} for which $u-2^{n-1}$ belongs to $O_1\cup O_2$, to $O_{3,4}$, and to $O_5\cup O_6$; let $U_{3,1}(d)$, $U_{3,2}(d)$, and $U_{3,3}(d)$ denote, respectively, the sets of integers u congruent to d modulo 2^{n+2} for which $u-3\cdot 2^{n-1}$ belongs to $O_1\cup O_2$, to $O_{3,4}$, and to $O_5\cup O_6$. We then put

$$s_1(d)=a_1\sum_{u\in U_1(d)}\frac{1}{r(u)}\,,$$

$$\begin{aligned}s_2(d)=a_2\Bigg(&\sum_{u\in U_{2,1}(d)}\frac{(-1)^{[(u+3)/4]}}{r(u-2^{n-1})}+\sum_{u\in U_{2,2}(d)}\frac{2(-1)^{(u+1)/4}}{r(u-2^{n-1})}+\sum_{u\in U_{2,3}(d)}\frac{(-1)^{[(u+1)/4]}}{r(u-2^{n-1})}\\&+\sum_{u\in U_{3,1}(d)}\frac{(-1)^{[(u+3)/4]}}{r(u-3\cdot 2^{n-1})}+\sum_{u\in U_{3,2}(d)}\frac{2(-1)^{(u+1)/4}}{r(u-3\cdot 2^{n-1})}\\&+\sum_{u\in U_{3,3}(d)}\frac{(-1)^{[(u+1)/4]}}{r(u-3\cdot 2^{n-1})}\Bigg)\,,\end{aligned}$$

where, for each real number x, $[x]$ denotes the greatest integer less than or equal to x. We also put

$$U_2(d)=U_{2,1}(d)\cup U_{2,2}(d)\cup U_{2,3}(d)\,,\quad U_3(d)=U_{3,1}(d)\cup U_{3,2}(d)\cup U_{3,3}(d)\,.$$

LEMMA 14. *Assume that* $l\equiv 3\,(\mathrm{mod}\ 8)$, $n\geq 4$, *and* l *divides* h_n/h_{n-1}. *Then, for any pair* $(d,d')\in\mathbf{Z}\times\mathbf{Z}$ *with* $d\equiv d'\,(\mathrm{mod}\ 2^{n+1})$, *either*

$$s_1(d)+s_2(d)\equiv s_1(d')+s_2(d')\pmod l$$

or

$$s_1(d)-s_2(d)\equiv s_1(d')-s_2(d')\pmod l\,.$$

Furthermore,

$$l\geq\frac{2^n+1}{3}\,.$$

PROOF. Let

$$\mu = e^{\pi i/4} = \zeta^{2^{n-1}}$$

for simplicity, and note that

$$\mu^l = -\mu^{-1} = \mu i\,, \quad \mu^2 = i\,.$$

In the case $n \geq 5$, since $3^{2^{n-3}} \equiv 1 + 2^{n-1} + 2^{n+1} \pmod{2^{n+2}}$, we have

$$\begin{aligned}
\eta^{a_1+a_2\tilde{\omega}} &= \frac{(\zeta-1)^{a_1}(-\mu\zeta-1)^{a_2} i^{a_2}(-\mu^{-1}\zeta+1)^{a_2}}{i^{a_1}(\zeta+1)^{a_1} i^{a_2}(-\mu\zeta+1)^{a_2}(-\mu^{-1}\zeta-1)^{a_2}} \\
&= \frac{(\zeta-1)^{a_1}(\zeta+\mu^{-1})^{a_2}(\zeta-\mu)^{a_2}}{i^{a_1}(\zeta+1)^{a_1}(\zeta-\mu^{-1})^{a_2}(\zeta+\mu)^{a_2}}\,, \\
\eta^{a_1-a_2\tilde{\omega}} &= \frac{(\zeta-1)^{a_1} i^{a_2}(-\mu\zeta+1)^{a_2}(-\mu^{-1}\zeta-1)^{a_2}}{i^{a_1}(\zeta+1)^{a_1}(-\mu\zeta-1)^{a_2} i^{a_2}(-\mu^{-1}\zeta+1)^{a_2}} \\
&= \frac{(\zeta-1)^{a_1}(\zeta-\mu^{-1})^{a_2}(\zeta+\mu)^{a_2}}{i^{a_1}(\zeta+1)^{a_1}(\zeta+\mu^{-1})^{a_2}(\zeta-\mu)^{a_2}}\,.
\end{aligned}$$

In the case $n = 4$,

$$\begin{aligned}
\eta^{a_1+a_2\tilde{\omega}} &= \frac{(\zeta-1)^{a_1}(\zeta-\mu^{-1})^{a_2}(\zeta+\mu)^{a_2}}{i^{a_1}(\zeta+1)^{a_1}(\zeta+\mu^{-1})^{a_2}(\zeta-\mu)^{a_2}}\,, \\
\eta^{a_1-a_2\tilde{\omega}} &= \frac{(\zeta-1)^{a_1}(\zeta+\mu^{-1})^{a_2}(\zeta-\mu)^{a_2}}{i^{a_1}(\zeta+1)^{a_1}(\zeta-\mu^{-1})^{a_2}(\zeta+\mu)^{a_2}}\,.
\end{aligned}$$

We also know that $\zeta^8 - 1$ is relatively prime to l. Therefore, by the assumption, Lemma 2 and [2, Lemma 5] give us

$$\begin{aligned}
&(\zeta-1)^{la_1}(\zeta+1)^{-la_1}(\zeta+\mu^{-1})^{l\kappa a_2}(\zeta-\mu^{-1})^{-l\kappa a_2}(\zeta-\mu)^{l\kappa a_2}(\zeta+\mu)^{-l\kappa a_2} \\
&\quad \equiv (\zeta^l-1)^{a_1}(\zeta^l+1)^{-a_1}(\zeta^l-\mu)^{\kappa a_2}(\zeta^l+\mu)^{-\kappa a_2}(\zeta^l+\mu^{-1})^{\kappa a_2}(\zeta^l-\mu^{-1})^{-\kappa a_2} \\
&\qquad \pmod{l^2}\,,
\end{aligned}$$

where κ is equal to -1 or 1. Hence, as in the proof of Lemma 13, we obtain

$$\begin{aligned}
&(\zeta^l+1)(\zeta^{4l}+1)a_1\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c(-1)^{l-c} - (\zeta^l-1)(\zeta^{4l}+1)a_1\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c \\
&\quad + (\zeta^{2l}-1)(\zeta^l+\mu)(\zeta^{2l}+i)\kappa a_2\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c\mu^{c-l} \\
&\quad - (\zeta^{2l}-1)(\zeta^l-\mu)(\zeta^{2l}+i)\kappa a_2\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c(-\mu)^{c-l} \\
&\quad + (\zeta^{2l}-1)(\zeta^l-\mu^{-1})(\zeta^{2l}-i)\kappa a_2\sum_{c=1}^{l-1}\binom{l}{c}\zeta^c(-\mu)^{l-c}
\end{aligned}$$

$$-(\zeta^{2l}-1)(\zeta^{l}+\mu^{-1})(\zeta^{2l}-i)\kappa a_2\sum_{c=1}^{l-1}\binom{l}{c}\zeta^{c}\mu^{l-c}\equiv 0 \pmod{l^2})$$

and, from this, we see that

$$\begin{aligned}(9)\qquad & a_1(\zeta^{4l}+1)\left(\zeta^{l}\sum_{b=1}^{(l-1)/2}\frac{\zeta^{2b}}{2b}+\sum_{b=1}^{(l-1)/2}\frac{\zeta^{2b-1}}{2b-1}\right)\\ &\quad+\kappa a_2(\zeta^{2l}-1)(\zeta^{2l}+i)\left(\zeta^{l}\sum_{b=1}^{(l-1)/2}\frac{\mu i^{b}\zeta^{2b}}{2b}-\sum_{b=1}^{(l-1)/2}\frac{\mu i^{b}\zeta^{2b-1}}{2b-1}\right)\\ &\quad+\kappa a_2(\zeta^{2l}-1)(\zeta^{2l}-i)\left(\zeta^{l}\sum_{b=1}^{(l-1)/2}\frac{\mu i^{1-b}\zeta^{2b}}{2b}-\sum_{b=1}^{(l-1)/2}\frac{\mu i^{1-b}\zeta^{2b-1}}{2b-1}\right)\\ &\equiv 0 \pmod{l}\,.\end{aligned}$$

It further follows that

$$\begin{aligned}&(\zeta^{2l}+i)\left(\zeta^{l}\sum_{b=1}^{(l-1)/2}\frac{\mu i^{b}\zeta^{2b}}{2b}-\sum_{b=1}^{(l-1)/2}\frac{\mu i^{b}\zeta^{2b-1}}{2b-1}\right)\\ &\quad=(\zeta^{2l}+i)\left(\zeta^{l}\sum_{m=1}^{(l-3)/4}\frac{\mu(-1)^{m}\zeta^{4m}}{4m}-\zeta^{l}\sum_{m=1}^{(l+1)/4}\frac{\mu i(-1)^{m}\zeta^{4m-2}}{4m-2}\right.\\ &\qquad\left.-\sum_{m=1}^{(l-3)/4}\frac{\mu(-1)^{m}\zeta^{4m-1}}{4m-1}+\sum_{m=1}^{(l+1)/4}\frac{\mu i(-1)^{m}\zeta^{4m-3}}{4m-3}\right)=\mu D_1+\mu i D_2\,,\end{aligned}$$

where

$$\begin{aligned}D_1&=\sum_{m=1}^{(l+1)/4}\left(\frac{(-1)^{m+1}\zeta^{4m-3}}{4m-3}+\frac{(-1)^{m}\zeta^{l+4m-2}}{4m-2}\right)\\ &\quad+\sum_{m=1}^{(l-3)/4}\left(\frac{(-1)^{m+1}\zeta^{2l+4m-1}}{4m-1}+\frac{(-1)^{m}\zeta^{3l+4m}}{4m}\right),\\ D_2&=\sum_{m=1}^{(l-3)/4}\left(\frac{(-1)^{m+1}\zeta^{4m-1}}{4m-1}+\frac{(-1)^{m}\zeta^{l+4m}}{4m}\right)\\ &\quad+\sum_{m=1}^{(l+1)/4}\left(\frac{(-1)^{m}\zeta^{2l+4m-3}}{4m-3}+\frac{(-1)^{m+1}\zeta^{3l+4m-2}}{4m-2}\right).\end{aligned}$$

We have similarly

$$(\zeta^{2l}-i)\left(\zeta^{l}\sum_{b=1}^{(l-1)/2}\frac{\mu i^{1-b}\zeta^{2b}}{2b}-\sum_{b=1}^{(l-1)/2}\frac{\mu i^{1-b}\zeta^{2b-1}}{2b-1}\right)=\mu i D_1+\mu D_2\,.$$

Hence,

$$(\zeta^{2l}-1)(\zeta^{2l}+i)\left(\zeta^l\sum_{b=1}^{(l-1)/2}\frac{\mu i^b\zeta^{2b}}{2b}-\sum_{b=1}^{(l-1)/2}\frac{\mu i^b\zeta^{2b-1}}{2b-1}\right)$$
$$+(\zeta^{2l}-1)(\zeta^{2l}-i)\left(\zeta^l\sum_{b=1}^{(l-1)/2}\frac{\mu i^{1-b}\zeta^{2b}}{2b}-\sum_{b=1}^{(l-1)/2}\frac{\mu i^{1-b}\zeta^{2b-1}}{2b-1}\right)$$
$$=(\mu+\mu i)(\zeta^{2l}-1)(D_1+D_2)\,.$$

The congruence (9) thus means that

$$a_1\sum_{b=1}^{(l-1)/2}\left(\frac{\zeta^{2b-1}}{2b-1}+\frac{\zeta^{l+2b}}{2b}+\frac{\zeta^{4l+2b-1}}{2b-1}+\frac{\zeta^{5l+2b}}{2b}\right)$$
$$+\kappa a_2(\zeta^{2^{n-1}}+\zeta^{3\cdot 2^{n-1}})\Bigg(\sum_{m=1}^{(l+1)/4}\left(\frac{(-1)^m\zeta^{4m-3}}{4m-3}+\frac{(-1)^{m+1}\zeta^{l+4m-2}}{4m-2}\right)$$
$$+\sum_{m=1}^{(l-3)/4}\left(\frac{(-1)^m\zeta^{4m-1}}{4m-1}+\frac{(-1)^{m+1}\zeta^{l+4m}}{4m}\right)$$
$$+\sum_{m=1}^{(l+1)/4}\left(\frac{2(-1)^{m+1}\zeta^{2l+4m-3}}{4m-3}+\frac{(-1)^m\zeta^{3l+4m-2}}{2m-1}\right)$$
$$+\sum_{m=1}^{(l+1)/4}\left(\frac{(-1)^m\zeta^{4l+4m-3}}{4m-3}+\frac{(-1)^{m+1}\zeta^{5l+4m-2}}{4m-2}\right)$$
$$+\sum_{m=1}^{(l-3)/4}\left(\frac{(-1)^{m+1}\zeta^{4l+4m-1}}{4m-1}+\frac{(-1)^m\zeta^{5l+4m}}{4m}\right)\Bigg)\equiv 0 \pmod{l}\,.$$

Therefore, combined with the definitions of $s_1(d)$, $s_2(d)$ for $d\in\mathbf{Z}$, Lemma 9 proves the first assertion of the present lemma.

Next, let

$$d_1=2l-1+3\cdot 2^{n-1}\,,\quad d_2=\frac{9l-1}{2}=4l+\frac{l-1}{2}\,.$$

If $l<2^{n-2}$, then we easily obtain

$$6l-1+2^{n-1}<d_1<2^{n+1}\,,\quad 6l-1+3\cdot 2^{n-1}<d_1+2^{n+1}\,,$$

which imply that

$$U_1(d_1)=U_2(d_1)=\emptyset\,,\quad U_3(d_1)=U_{3,1}(d_1)=\{d_1\}\,,$$
$$U_1(d_1+2^{n+1})=U_2(d_1+2^{n+1})=U_3(d_1+2^{n+1})=\emptyset\,,$$

so that

$$s_1(d_1)=s_1(d_1+2^{n+1})=s_2(d_1+2^{n+1})=0\,,\quad s_2(d_1)=\frac{a_2}{l-1}\,.$$

If $2^{n-2} < l < (2^n+1)/3$, then

$$s_1(d_2) = \frac{2a_1}{l-1}\,, \quad s_2(d_2) = s_1(d_2+2^{n+1}) = s_2(d_2+2^{n+1}) = 0\,;$$

because

$$2l < d_2 - 2^{n-1} < 3l\,, \quad d_2 \equiv 1 \pmod 4\,, \quad d_2 < 3\cdot 2^{n-1}\,, \quad 6l-1+3\cdot 2^{n-1} < d_2+2^{n+1}\,,$$

and, hence,

$$U_1(d_2) = \{d_2\}\,, \quad U_2(d_2) = U_3(d_2) = \emptyset\,,$$
$$U_1(d_2+2^{n+1}) = U_2(d_2+2^{n+1}) = U_3(d_2+2^{n+1}) = \emptyset\,.$$

Thus, the second assertion of the lemma follows from the first. □

PROPOSITION 3. *If l is congruent to 3 or 5 modulo 8, then the l-class group of the $\boldsymbol{Z}_2$-extension $\boldsymbol{B}_\infty$ over $\boldsymbol{Q}$ is trivial.*

PROOF. Assume that l divides h_n/h_{n-1} contrary to the assertion of the proposition. We first deal with the case $l \equiv 5 \pmod 8$. In this case, Lemmas 12 and 13 yield

$$2^{n-1} < l < (n+1)^2\,,$$

whence we have $n \le 6$. It is known, however, that $h_5 = 1$ (cf. [1, Theorem 1]). Therefore, (l, n) must equal $(37, 6)$. Since

$$(a_1, a_2) = (6, 1)\,, \quad U_1(127) = U_2(127) = \{127\}\,, \quad 127 = 37\cdot 3 + 16 = 2^6 + 37 + 26\,,$$
$$U_1(255) = U_2(255) = \emptyset\,,$$

we see that

$$s_1(127) = \frac{3}{8} \equiv 5 \pmod{37}\,, \quad s_2(127) = -\frac{1}{26} \equiv 27 \pmod{37}\,,$$
$$s_1(255) = s_2(255) = 0\,.$$

Lemma 13 then implies that 37 does not divide h_6/h_5, but this is a contradiction. Thus, the proposition holds whenever $l \equiv 5 \pmod 8$.

Let us next deal with the case $l \equiv 3 \pmod 8$, supposing that $n \ge 6$. In view of Lemmas 12 and 13, we obtain

$$\frac{2^n+1}{3} \le l < \frac{3}{2}\left(n+\frac{2}{3}\right)^2\,.$$

Hence, the pair (l, n) belongs to the set

$$\{(43, 6), (59, 6), (43, 7), (59, 7), (67, 7), (83, 7), (107, 8)\}\,.$$

If $(l, n) = (59, 7)$ so that $(a_1, a_2) = (3, 5)$, then Lemma 11 implies that

$$59 < \frac{3}{\log 2}\log\left(\cot\frac{\pi}{2^9}\right) + \frac{5}{\log 2}\log\left(\frac{\cos(\pi/2^8)+\sin(\pi/2^8)+1}{\cos(\pi/2^8)+\sin(\pi/2^8)-1}\right)\,,$$

but the right-hand side of the above inequality is certainly smaller than 59. Similarly, when (l, n) belongs to $\{(59, 6), (83, 7), (107, 8)\}$, Lemma 11 leads us to one of the following contradictions:

$$59 < \frac{3}{\log 2}\log\left(\cot\frac{\pi}{2^8}\right) + \frac{5}{\log 2}\log\left(\frac{\cos(\pi/2^7)+\sin(\pi/2^7)+1}{\cos(\pi/2^7)+\sin(\pi/2^7)-1}\right) < 51\,,$$
$$83 < \frac{9}{\log 2}\log\left(\cot\frac{\pi}{2^9}\right) + \frac{1}{\log 2}\log\left(\frac{\cos(\pi/2^8)+\sin(\pi/2^8)+1}{\cos(\pi/2^8)+\sin(\pi/2^8)-1}\right) < 74\,,$$
$$107 < \frac{3}{\log 2}\log\left(\cot\frac{\pi}{2^{10}}\right) + \frac{7}{\log 2}\log\left(\frac{\cos(\pi/2^9)+\sin(\pi/2^9)+1}{\cos(\pi/2^9)+\sin(\pi/2^9)-1}\right) < 84\,.$$

Hence, (l, n) must be (43, 6), (43, 7), or (67, 7). Assume now that $(l, n) = (43, 6)$. Because of the facts

$$(a_1, a_2) = (5, 3)\,, \quad U_1(127) = \emptyset\,, \quad 127 = 2^5 + 43\cdot 2 + 9 \in U_{2,2}(127)\,,$$
$$127 = 2^5\cdot 3 + 31 \in U_{3,1}(127)\,, \quad U_2(127) = U_3(127) = \{127\}\,,$$
$$255 = 43\cdot 5 + 40 \in U_1(255)\,, \quad 255 = 2^5 + 43\cdot 5 + 8 \in U_{2,3}(255)\,,$$
$$255 = 2^5\cdot 3 + 43\cdot 3 + 30 \in U_{3,2}(255)\,, \quad U_1(255) = U_2(255) = U_3(255) = \{255\}\,,$$

we have

$$s_1(127) = 0, \quad s_2(127) = \frac{2}{9} + \frac{1}{31} \equiv 30 \pmod{43}\,, \quad s_1(255) = \frac{1}{40} \equiv 14 \pmod{43}\,,$$
$$s_2(255) = \frac{1}{8} + \frac{1}{15} \equiv 7 \pmod{43}\,.$$

Lemma 14 therefore implies that 43 does not divide h_6/h_5, which contradicts our assumption. If $(l, n) = (43, 7)$, then

$$(a_1, a_2) = (5, 3)\,, \quad 255 = 43\cdot 5 + 40 \in U_1(255)\,, \quad 255 = 2^6 + 43\cdot 4 + 19 \in U_{2,3}(255)\,,$$
$$255 = 2^6\cdot 3 + 43 + 20 \in U_{3,1}(255)\,, \quad U_1(255) = U_2(255) = U_3(255) = \{255\}\,,$$
$$U_1(511) = U_2(511) = U_3(511) = \emptyset\,,$$

and, therefore,

$$s_1(255) = \frac{1}{8} \equiv 27 \pmod{43}\,, \quad s_2(255) = \frac{3}{19} + \frac{3}{20} \equiv 14 \pmod{43}\,,$$
$$s_1(511) = s_2(511) = 0\,,$$

but Lemma 14, together with these, shows that 43 does not divide h_7/h_6. Furthermore, if $(l, n) = (67, 7)$, then

$$(a_1, a_2) = (7, 3)\,, \quad 255 = 67\cdot 3 + 54 \in U_1(255)\,, \quad 255 = 2^6 + 67\cdot 2 + 57 \in U_{2,2}(255)\,,$$
$$255 = 2^6\cdot 3 + 63 \in U_{3,1}(255)\,, \quad U_1(255) = U_2(255) = U_3(255) = \{255\}\,,$$
$$U_1(511) = U_2(511) = U_3(511) = \emptyset\,,$$

and, hence,

$$s_1(255) = \frac{7}{54} \equiv 51 \pmod{67}, \quad s_2(255) = \frac{2}{19} + \frac{1}{21} \equiv 2 \pmod{67},$$
$$s_1(511) = s_2(511) = 0.$$

However, together with these, Lemma 14 still shows that 67 does not divide h_7/h_6. Consequently, our assumption that l divides h_n/h_{n-1} turns out to be false. The proof of the proposition is now completed. □

REMARK 3. In the case where $l \equiv 5 \pmod 8$ and $2 \leq n \leq 5$, one can obtain the fact that l does not divide h_n/h_{n-1}, only using Lemmas 11, 12, and 13; also in the case where $l \equiv 3 \pmod 8$ and n is equal to 4 or 5, the same fact can be deduced from Lemmas 11, 12, and 14.

Finally, let us prove Theorem 3. By the assumption, the cyclotomic field of eighth roots of unity contains F. The extension in $\boldsymbol{P}_\infty = \boldsymbol{B}_\infty(i)$ of degree $8^2/2$ over $\boldsymbol{Q}(i)$ is the cyclotomic field of 128th roots of unity, and the relative class number of the cyclotomic field is known to equal $17 \times 21\,121$. It therefore follows from [2, Theorem 1] that, for any positive integer u, l does not divide the relative class number of $\boldsymbol{Q}(e^{\pi i/2^{u-1}})$, the cyclotomic field of 2^uth roots of unity (see also [7, IV]). On the other hand, Proposition 3 means that, for any positive integer u, l does not divide the class number of the maximal real subfield of $\boldsymbol{Q}(e^{\pi i/2^{u-1}})$. Thus, the theorem is proved.

REFERENCES

[1] F. J. VAN DER LINDEN, Class number computations of real abelian number fields, Math. Comp. 39 (1982), 693–707.

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

[3] 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.

[4] 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.

[5] T. TAKAGI, Lectures on elementary theory of numbers (in Japanese), Kyoritsushuppansha, Tokyo, 1971.

[6] I. M. VINOGRADOV, Elements of number theory (English translation), Dover Publishing, New York, 1954.

[7] L. C. WASHINGTON, Class numbers and $\boldsymbol{Z}_p$-extensions, Math. Ann. 214 (1975), 177–193.

DEPARTMENT OF MATHEMATICS
TOKAI UNIVERSITY
HIRATSUKA 259–1292
JAPAN