ACTA ARITHMETICA
135.2 (2008)

The narrow class groups of some $\mathbb{Z}_p$-extensions over the rationals

by

KUNIAKI HORIE (Hiratsuka) and MITSUKO HORIE (Tokyo)

1. Introduction. Let p be an odd prime number. Let $\mathbb{Z}_p$ denote the ring of p-adic integers, and $\mathbb{B}_\infty$ the $\mathbb{Z}_p$-extension over the rational field $\mathbb{Q}$, that is, the unique abelian extension over $\mathbb{Q}$ in the complex field $\mathbb{C}$ such that the Galois group $\mathrm{Gal}(\mathbb{B}_\infty/\mathbb{Q})$ is topologically isomorphic to the additive group of $\mathbb{Z}_p$. As is well known, the p-class group of $\mathbb{B}_\infty$ is trivial (cf. Iwasawa [I]). Let us choose a prime number l which is a primitive root modulo p^2. It is shown in [H1], through the study of circular units in $\mathbb{B}_\infty$, that the l-class group of $\mathbb{B}_\infty$ is trivial if

$$p = 3 \quad \text{or} \quad l \geq \frac{3}{2\log 2}\,(p-1)\varphi(p-1)\log(p\log p),$$

where φ denotes the Euler function. Furthermore, in case $p = 5$ or $p = 7$, the triviality of the l-class group of $\mathbb{B}_\infty$ is proved in [H2] by arguments similar to and more precise than those of [H1]. In this paper, using some results of [H1, H2], we shall first prove the following result with the help of a personal computer.

THEOREM 1. *Let l be, as above, a prime number which is a primitive root modulo p^2. If $p = 11$ or $p = 13$, then the l-class group of $\mathbb{B}_\infty$ is trivial.*

Now, for any algebraic extension K of $\mathbb{Q}$ in $\mathbb{C}$, we let $\mathfrak{O}$ denote the ring of algebraic integers in K, $\mathcal{I}$ the ideal group of K, and C_+ the ideal class group of K in the narrow sense, that is, the quotient group of $\mathcal{I}$ modulo the group of principal ideals $\alpha\mathfrak{O}$ in $\mathcal{I}$ for all totally positive elements α of K; C_+ is also called the *narrow class group* of K. The natural homomorphism of C_+ onto the ideal class group of K induces, for every odd prime q, an isomorphism of the q-primary component of C_+ onto the q-class group of K. The 2-primary component of C_+ is called the 2-*class group* of K *in the narrow sense* or, simply, the *narrow* 2-*class group* of K. After discussing the parity of certain

2000 *Mathematics Subject Classification*: 11R20, 11R23, 11R29.
Key words and phrases: narrow class group, $\mathbb{Z}_p$-extension.

kinds of class numbers together with a basic criterion by Washington [W1] for such study, we shall secondly prove the following result, still with the help of a (personal) computer in the case $p = 13$.

THEOREM 2. *When $p \leq 13$, the 2-class group of $\mathbb{B}_\infty$ in the narrow sense is trivial.*

The proof of the above theorem, as well as that of Theorem 1, is essentially based upon the analytic class number formula. Most of our computations are done with *Mathematica*.

REMARK 1. A classical theorem of Weber implies the triviality of the narrow 2-class group of the $\mathbb{Z}_2$-extension over $\mathbb{Q}$, $\mathbb{Z}_2$ being the ring of 2-adic integers.

REMARK 2. Apart from our proof of Theorem 2, when $p = 11$ or $p = 13$ so that 2 is a primitive root modulo p, assertion IV of Armitage and Fröhlich [AF] shows that Theorem 1 implies Theorem 2.

At the end of the paper, we shall briefly explain how to show, for $p \leq 487$, the triviality of the narrow 2-class group of the subfield of $\mathbb{B}_\infty$ with degree p.

2. Proof of Theorem 1. For each integer $u \geq 0$, let $\mathbb{B}_u$ denote the subfield of $\mathbb{B}_\infty$ with degree p^u, and h_u the class number of $\mathbb{B}_u$. Let n be any positive integer, which will be fixed throughout the paper. Since the prime ideal of $\mathbb{B}_{n-1}$ dividing p is totally ramified in $\mathbb{B}_n$, we know from class field theory that h_{n-1} divides h_n, i.e., h_n/h_{n-1} is an integer. Now, for each positive integer a, we denote by $\mathbb{K}_a$ the cyclotomic field of ath roots of unity:

$$\mathbb{K}_a = \mathbb{Q}(e^{2\pi i/a}).$$

Let ν be the number of distinct prime divisors of $(p-1)/2$, and let $g_1, \ldots, g_\nu$ be the prime powers > 1 pairwise relatively prime such that

$$\frac{p-1}{2} = g_1 \cdots g_\nu.$$

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

$$e^{\pi i u_1/g_1} \cdots e^{\pi i u_\nu/g_\nu}$$

for all ν-tuples $(u_1, \ldots, u_\nu)$ of integers with $0 \leq u_1 < g_1, \ldots, 0 \leq u_\nu < g_\nu$. It is naturally understood that $V = \{1\}$ if $p = 3$. Taking the ring $\mathbb{Z}$ of (rational) integers, let Ψ denote the set of maps

$$z : V \to \{u \in \mathbb{Z} \mid 0 \leq u \leq 2l\}$$

such that, for some $\xi \in V$,

$$l \nmid z(\xi) \quad \text{or} \quad z(\xi) > 0$$

according to whether $l > 2$ or $l = 2$, and that

$$l \mid z(\xi') \quad \text{for all } \xi' \in V \setminus \{\xi\}.$$

We put

$$M = \max_{z \in \Psi} \mathfrak{N}\Big(\sum_{\xi \in V} z(\xi)\xi - 1\Big),$$

where $\mathfrak{N}$ denotes the norm map from $\mathbb{K}_{p-1} = \mathbb{Q}(e^{2\pi i/(p-1)})$ to $\mathbb{Q}$. We easily see that M is a positive integer.

Lemma 1. *If l divides h_n/h_{n-1}, then*

$$p^n \le M, \quad l < \frac{p-1}{2\log 2}\log\Big(\frac{p^{n+1}}{\pi}\sin\frac{\pi}{p}\Big).$$

Proof. This follows from [H1, Lemma 4] and [H2, Lemma 2]. ∎

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{K}_{p-1}$ dividing p. Let I be the set of positive integers $a < p^{n+1}$ for which $a \equiv \xi \pmod{\mathfrak{p}^{n+1}}$ with some $\xi \in V$. Let $\mathfrak{F}$ denote the family of all maps from I to $\{0, l\}$ and, for each $a \in I$, let $\mathfrak{G}_a$ denote the family of maps $j : I \to \mathbb{Z}$ such that $\min(l-2, 1) \le j(a) < l$ and that $j(b) = 0$ or $j(b) = l$ for every $b \in I \setminus \{a\}$. Given any $u \in \mathbb{Z}$, we then let

$$\mathcal{P}_a(u) = \Big\{(j, y) \in \mathfrak{G}_a \times \mathfrak{F} \;\Big|\; \sum_{b \in I}((p^n+1)j(b) + y(b))b \equiv u \pmod{p^{n+1}}\Big\},$$

$$\mathcal{Q}_a(u) = \Big\{(j, y) \in \mathfrak{F} \times \mathfrak{G}_a \;\Big|\; \sum_{b \in I}((p^n+1)j(b) + y(b))b \equiv u \pmod{p^{n+1}}\Big\}.$$

In the case $l > 2$, we put

$$s(u) = \sum_{a \in I}\Big(\sum_{(j,y) \in \mathcal{Q}_a(u)} (-1)^{\sum_{b \in I}(j(b)+y(b))+y(a)}\widetilde{y(a)} - \sum_{(j,y) \in \mathcal{P}_a(u)} (-1)^{\sum_{b \in I}(j(b)+y(b))+j(a)}\widetilde{j(a)}\Big),$$

where, for each integer r relatively prime to l, $\tilde{r}$ denotes the positive integer smaller than l such that $r\tilde{r} \equiv 1 \pmod{l}$; in the case $l = 2$, we put

$$s(u) = \sum_{a \in I}(|\mathcal{Q}_a(u)| - |\mathcal{P}_a(u)|),$$

where, for each finite set W, $|W|$ denotes the number of elements of W. Lemma 3 of [H2] can now be restated as follows:

Lemma 2. *If there exist integers c and d satisfying*

$$c \equiv d \pmod{p^n}, \qquad s(c) \not\equiv s(d) \pmod{l},$$

then l does not divide h_n/h_{n-1}.

To prove Theorem 1, let us first consider the case $p = 11$. Take any $z \in \Psi$ and put

$$\alpha = \sum_{\xi \in V} z(\xi)\xi - 1, \qquad \alpha' = \sum_{\xi \in V} z(\xi)\xi^3 - 1.$$

Let $\varrho = e^{\pi i/5}$, so that $V = \{1, \varrho, \varrho^2, \varrho^3, \varrho^4\}$. It follows that

$$\alpha = z(1) - 1 - z(\varrho^4) + \sum_{u=1}^{3} (z(\varrho^u) + (-1)^{u-1} z(\varrho^4))\varrho^u,$$
$$|\alpha|^2 \in \mathbb{Z}[\varrho + \varrho^{-1}], \qquad \varrho + \varrho^{-1} = \frac{1+\sqrt{5}}{2}.$$

Let A and B be the integers determined by

$$|\alpha|^2 = A + B(\varrho + \varrho^{-1}).$$

Then

$$\begin{aligned} A &= (z(1)-1)(z(1) - 1 + z(\varrho^3) - z(\varrho^2)) + z(\varrho)z(\varrho^4) \\ &\quad + z(\varrho)^2 - z(\varrho)z(\varrho^3) + z(\varrho^3)^2 + z(\varrho^2)^2 - z(\varrho^2)z(\varrho^4) + z(\varrho^4)^2, \\ \mathfrak{N}(\alpha) &= |\alpha\alpha'|^2 = A^2 + AB - B^2 = \frac{5A^2}{4} - \left(\frac{A}{2} - B\right)^2. \end{aligned}$$

In particular, the former equation above implies $A \geq 0$, because

$$\begin{aligned} A &\geq (z(1)-1)^2 - \frac{(z(1)-1)^2 + z(\varrho^3)^2}{2} - \frac{(z(1)-1)^2 + z(\varrho^2)^2}{2} \\ &\quad + z(\varrho)^2 - \frac{z(\varrho)^2 + z(\varrho^3)^2}{2} + z(\varrho^3)^2 + z(\varrho^2)^2 - \frac{z(\varrho^2)^2 + z(\varrho^4)^2}{2} + z(\varrho^4)^2 \\ &= \frac{z(\varrho)^2 + z(\varrho^4)^2}{2}. \end{aligned}$$

Hence, noting that

$$z(\varrho)^2 - z(\varrho)z(\varrho^3) + z(\varrho^3)^2 \leq 4l^2,$$
$$z(\varrho^2)^2 - z(\varrho^2)z(\varrho^4) + z(\varrho^4)^2 \leq 4l^2,$$

we have

$$\mathfrak{N}(\alpha) < \frac{5}{4}\,(5(4l^2))^2 = 500l^4.$$

This gives

$$M < 500l^4.$$

Let S be the set of the following pairs of integers:

$$
\begin{array}{llllll}
(1,2), & (1,7), & (1,13), & (1,17), & (2,2), & (2,7), \\
(2,13), & (2,17), & (2,19), & (2,29), & (3,2), & (3,7), \\
(3,13), & (3,17), & (3,19), & (3,29), & (3,41), & (4,7), \\
(4,13), & (4,17), & (4,19), & (4,29), & (4,41), & (4,61), \\
(5,7), & (5,13), & (5,17), & (5,19), & (5,29), & (5,41), \\
(5,61), & (5,73), & (5,79), & (5,83), & (6,13), & (6,17), \\
(6,19), & (6,29), & (6,41), & (6,61), & (6,73), & (6,79), \\
(6,83), & (6,101), & (7,17), & (7,19), & (7,29), & (7,41), \\
(7,61), & (7,73), & (7,79), & (7,83), & (7,101), & (7,107), \\
(8,29), & (8,41), & (8,61), & (8,73), & (8,79), & (8,83), \\
(8,101), & (8,107), & (8,127), & (9,61), & (9,73), & (9,79), \\
(9,83), & (9,101), & (9,107), & (9,127), & (9,139), & (9,149), \\
(9,151), & (10,101), & (10,107), & (10,127), & (10,139), & (10,149), \\
(10,151), & (10,167), & (11,167), & (11,173). & &
\end{array}
$$

By simple calculations, we find that the inequalities

$$11^n < 500l^4, \qquad l < \frac{5}{\log 2}\log\left(\frac{11^{n+1}}{\pi}\sin\frac{\pi}{11}\right)$$

hold if and only if $(n,l) \in S$. Hence Lemma 1 implies that $(n,l) \in S$ if l divides h_n/h_{n-1}.

Assume now that $(n,l) \in S$. For each r in $\{1,2,3,4\}$, let b_r denote the integer such that

$$b_r \equiv 2^{11^n r} \pmod{11^{n+1}}, \qquad 0 < b_r < 11^{n+1}.$$

Since 2 is a primitive root modulo 11^{n+1}, we can take as $\mathfrak{p}$ the prime ideal of $\mathbb{K}_{10} = \mathbb{Q}(\varrho)$ generated by 11 and $b_1 - \varrho$. We then have

$$I = \{1, b_1, b_2, b_3, b_4\}.$$

In view of Lemma 2 and [H2, Lemma 1], it suffices for our proof to find integers c and d which satisfy

$$c \equiv d \pmod{11^n}, \qquad s(c) \not\equiv s(d) \pmod{l}.$$

By using a (personal) computer, we have computed $s(u)$ for suitable integers u after the determination of $\mathcal{P}_a(u)$ and $\mathcal{Q}_a(u)$ for all $a \in I$. When $n \geq 4$ but $(n,l) \neq (4,61)$, the computations show that

$$s(1) = 1, \qquad s(1 + 11^n) = -1.$$

Furthermore,

$$
\begin{aligned}
s(1) &= 0, \quad & s(1 + 3\cdot 11^3) &= -1, \qquad & &\text{if } (n,l) = (3,2); \\
s(1) &= 1, \quad & s(1 + 3\cdot 11^3) &= -2, \qquad & &\text{if } (n,l) = (2,2).
\end{aligned}
$$

Results for the other cases of (n, l) are given in the following table:

(n,l)	$s(1)$	$s(1+11^n)$	(n,l)	$s(1)$	$s(1+11^n)$
$(4,61)$	-21	-48	$(2,19)$	69	61
$(3,41)$	-31	-36	$(2,17)$	21	-3
$(3,29)$	24	17	$(2,13)$	-45	21
$(3,19)$	5	52	$(2,7)$	25	-22
$(3,17)$	5	-5	$(1,17)$	-257	203
$(3,13)$	-5	-29	$(1,13)$	-56	12
$(3,7)$	1	-2	$(1,7)$	-23	-32
$(2,29)$	-36	103	$(1,2)$	-2	-9

We thus obtain the conclusion for $p = 11$.

Let us next deal with the case $p = 13$. Take any $z \in \Psi$ and put

$$\alpha = \sum_{\xi \in V} z(\xi)\xi - 1, \qquad \alpha' = \sum_{\xi \in V} z(\xi)\xi^7 - 1.$$

Clearly, $\mathfrak{N}(\alpha) = |\alpha\alpha'|^2$. Let $\varrho = ie^{2\pi i/3}$, so that

$$V = \{1, \varrho, \varrho^2, -\varrho^3, \varrho^4, -\varrho^5\}, \qquad -\varrho^3 = i, \qquad \varrho^4 = e^{2\pi i/3}, \qquad i\varrho^4 = \varrho.$$

Let further

$$\begin{aligned} a_1 &= z(1) - 1 + z(\varrho^2), & a_2 &= z(\varrho^2) + z(\varrho^4), \\ a_3 &= z(i) + z(-\varrho^5), & a_4 &= z(\varrho) + z(-\varrho^5). \end{aligned}$$

Then

$$\begin{aligned} \alpha &= a_1 + a_2\varrho^4 + a_3 i + a_4 i\varrho^4, \\ \alpha' &= a_1 + a_2\varrho^4 - a_3 i - a_4 i\varrho^4. \end{aligned}$$

We therefore see that

$$\begin{aligned} \mathfrak{N}(\alpha) &= |(a_1 + a_2\varrho^4)^2 + (a_3 + a_4\varrho^4)^2|^2 \\ &\le (|a_1 + a_2\varrho^4|^2 + |a_3 + a_4\varrho^4|^2)^2 \\ &= (a_1^2 - a_1a_2 + a_2^2 + a_3^2 - a_3a_4 + a_4^2)^2. \end{aligned}$$

Since $a_1^2 - a_1a_2 + a_2^2 < 16l^2$ and $a_3^2 - a_3a_4 + a_4^2 \le 16l^2$, it follows that

$$\mathfrak{N}(\alpha) < (32l^2)^2 = 2^{10}l^4.$$

Hence we have

$$M < 2^{10}l^4.$$

On the other hand, let S be the set of the following pairs of integers:

$$\begin{array}{llllll}
(1,2), & (1,7), & (1,11), & (2,2), & (2,7), & (2,11), \\
(2,37), & (3,2), & (3,7), & (3,11), & (3,37), & (3,41), \\
(3,59), & (4,7), & (4,11), & (4,37), & (4,41), & (4,59), \\
(4,67), & (4,71), & (5,7), & (5,11), & (5,37), & (5,41), \\
(5,59), & (5,67), & (5,71), & (5,97), & (6,11), & (6,37), \\
(6,41), & (6,59), & (6,67), & (6,71), & (6,97), & (7,37), \\
(7,41), & (7,59), & (7,67), & (7,71), & (7,97), & (7,137), \\
(7,149), & (8,37), & (8,41), & (8,59), & (8,67), & (8,71), \\
(8,97), & (8,137), & (8,149), & (8,163), & (8,167), & (9,59), \\
(9,67), & (9,71), & (9,97), & (9,137), & (9,149), & (9,163), \\
(9,167), & (9,193), & (9,197), & (10,137), & (10,149), & (10,163), \\
(10,167), & (10,193), & (10,197), & (11,223), & (11,227), & (11,241).
\end{array}$$

Simple calculations show that $(n,l) \in S$ if and only if

$$13^n < 2^{10} l^4, \quad l < \frac{6}{\log 2} \log\left(\frac{13^{n+1}}{\pi} \sin\frac{\pi}{13}\right).$$

Lemma 1 therefore implies that $(n,l) \in S$ if l divides h_n/h_{n-1}.

Suppose (n,l) to be in S. Let b_1 be the integer such that

$$b_1 \equiv 2^{13^n} \pmod{13^{n+1}}, \qquad 0 < b_1 < 13^{n+1}.$$

For each $r \in \{2,3,4,5\}$, let b_r denote the integer such that

$$b_r \equiv (-b_1)^r \pmod{13^{n+1}}, \qquad 0 < b_r < 13^{n+1}.$$

Since 2 is a primitive root modulo 13^{n+1}, we take as $\mathfrak{p}$ the prime ideal of $\mathbb{K}_{12} = \mathbb{Q}(\varrho)$ generated by 13 and $b_1 - \varrho$. We then see that

$$I = \{1, b_1, b_2, b_3, b_4, b_5\}.$$

By Lemma 2 and [H2, Lemma 1], it suffices to find integers c and d which satisfy

$$c \equiv d \pmod{13^n}, \qquad s(c) \not\equiv s(d) \pmod{l}.$$

Using a computer as in the case $p = 11$, we have computed $s(u)$ for suitable integers u. When $n \geq 4$ but $(n,l) \neq (5,71),(5,67),(4,71),(4,41)$, the computations yield

$$s(1) = 1, \quad s(1 + 13^n) = -1.$$

Results for the other cases of (n, l) are given in the following tables:

(n,l)	$s(1)$	$s(1+13^n)$
$(5,71)$	-48	-1
$(5,67)$	-31	-1
$(4,71)$	181	-8
$(4,41)$	12	-1
$(3,59)$	84	-133
$(3,41)$	13	-80
$(3,37)$	143	-9
$(3,11)$	-9	3
$(2,37)$	14	266
$(2,11)$	-107	55
$(2,7)$	6	-34
$(1,11)$	16	101
$(1,7)$	48	4

(n,l)	$s(1)$	$s(1+5\cdot 13^n)$
$(3,7)$	1	0
$(3,2)$	0	-5
$(2,2)$	1	2
$(1,2)$	13	26

Thus our proof is completed.

3. Some lemmas. In this section we give some preliminary results for the proof of Theorem 2. Let t be the positive integer such that 2^t is the highest power of 2 dividing $p-1$. Let k be the subfield of $\mathbb{K}_p$ with degree 2^t, whence k is an imaginary abelian extension over $\mathbb{Q}$. For each integer $u \geq 0$, we denote by h_u^- the relative class number of the composite $k\mathbb{B}_u$.

LEMMA 3. *The class number of $\mathbb{B}_n$ in the narrow sense is odd if and only if h_n^- is odd.*

Proof. Let $\mathfrak{p}$ be the unique prime ideal of $\mathbb{B}_n$ dividing p. Since $k\mathbb{B}_n$ is an abelian 2-extension over $\mathbb{B}_n$ and since no prime ideal of $\mathbb{B}_n$ other than $\mathfrak{p}$ is ramified in $k\mathbb{B}_n$ but $\mathfrak{p}$ is fully ramified in $k\mathbb{B}_n$, a well-known argument of [I] tells us that the class number of $k\mathbb{B}_n$ is odd if and only if the class number of $\mathbb{B}_n$ in the narrow sense is odd (cf. the proof of Washington [W2, Theorem 10.4]). On the other hand, $k\mathbb{B}_n$ is a cyclic extension over $\mathbb{Q}$ so that, by Hasse [H, Satz 45], the indivisibility $2 \nmid h_n^-$ means that the class number of $k\mathbb{B}_n$ is odd. Therefore, the lemma follows. ∎

REMARK 3. As is seen from the above proof, Lemma 3 still holds even if one replaces $\mathbb{B}_n$ by any intermediate field of the extension $k\mathbb{B}_n/\mathbb{B}_n$.

Let $\mathfrak{X}$ be the set of primitive Dirichlet characters of order 2^t with conductor p, so that all Dirichlet characters in $\mathfrak{X}$ are odd. Let $\mathfrak{Y}$ be the set of primitive Dirichlet characters of order p^n with conductor p^{n+1}. Since $k\mathbb{B}_n$ does not contain i and since the unit indices of $k\mathbb{B}_n$ and $k\mathbb{B}_{n-1}$ are equal to 1, the analytic class number formula implies that

$$(1)\qquad \frac{h_n^-}{h_{n-1}^-} = \check{p} \prod_{\chi \in \mathfrak{X}} \prod_{\psi \in \mathfrak{Y}} \Big(-\frac{1}{2p^{n+1}} \sum_{a=1}^{p^{n+1}} \chi\psi(a)a \Big),$$

where $\check{p} = p$ or $\check{p} = 1$ according to whether $p-1$ is a power of 2 or not (cf. [H, §36, (3)]). Furthermore, the right hand side of (1) is known to be an integer: $h_{n-1}^- \mid h_n^-$ (cf. [H, Satz 32]).

Let R be a set of positive integers smaller than p such that

$$R \cap \{p-a \mid a \in R\} = \emptyset, \qquad R \cup \{p-a \mid a \in R\} = \{1, \ldots, p-1\}.$$

Given any integer $u \geq 0$, let R_u denote the set of integers b for which $b^{p-1} \equiv 1 \pmod{p^{u+1}}$, $0 < b < p^{u+1}$, and $b \equiv a \pmod{p}$ with some $a \in R$. It then follows that $|R_u| = |R| = (p-1)/2$, because, for each $a \in R$, there exists a unique $b \in R_u$ with $b \equiv a \pmod{p}$. Obviously, $R_0 = R$. Take any positive integer $m \leq (n+1)/2$:

$$n \geq 2m-1 \geq 1, \quad \text{i.e.,} \quad n-m+1 \geq m \geq 1.$$

For each integer a not divisible by p, let a_* denote the integer such that

$$a_* \equiv a \pmod{p^{n-m+1}}, \qquad 0 < a_* < p^{n-m+1},$$

and let a^* denote the integer such that

$$aa^* \equiv 1 \pmod{p^m}, \qquad 0 < a^* < p^m.$$

To state the following lemma, we note that, for any $\psi \in \mathfrak{Y}$, $\psi(1+p^{n-m+1})$ is a primitive p^mth root of unity.

LEMMA 4. *Let ψ be a Dirichlet character in $\mathfrak{Y}$. Assume that $2^{p-1} \not\equiv 1 \pmod{p^{m+1}}$, i.e., $\mathbb{K}_{p^m}$ contains the decomposition field of 2 for the abelian extension $\mathbb{K}_p\mathbb{B}_\infty/\mathbb{Q}$, and that, for some integer c not divisible by p, the algebraic number*

$$\sum_{b \in R_{n-m}} \frac{\psi(c)^{-1}\psi((bc)_*)}{\psi(1+p^{n-m+1})^{(bc)^*} - 1}$$

is relatively prime to 2. Then the integer h_n^-/h_{n-1}^- is odd.

Proof. Let χ be any Dirichlet character in $\mathfrak{X}$. We put

$$\Theta = -\frac{1}{2p^{n+1}} \sum_{a=1}^{p^{n+1}} \chi\psi(a)a, \qquad \omega = \psi(1+p^{n-m+1}).$$

The field in $\mathbb{C}$ generated by the images of χ and ψ over $\mathbb{Q}$ is $\mathbb{K}_{2^t p^n}$ and, by [H, Satz 32], $(\omega-1)\Theta$ is an algebraic integer. Let $\mathfrak{T}$ denote the trace map from $\mathbb{K}_{2^t p^n}$ to $\mathbb{K}_{2^t p^m}$. The argument in the first part of [W1, §IV] then shows that

$$\mathfrak{T}(\psi(c)^{-1}\Theta) = p^{n-m} \sum_{b \in R_{n-m}} \frac{\psi(c)^{-1}\chi\psi((bc)_*)}{\omega^{(bc)^*} - 1}$$

(cf., in particular, [W1, (**)]). Let $\mathfrak{i}$ be the integral ideal of $\mathbb{K}_{2^t p^m}$ generated by $e^{\pi i/2^{t-1}} - 1$, so that, in $\mathbb{K}_{2^t p^n}$,

$$\chi\psi((bc)_*) \equiv \psi((bc)_*) \pmod{\mathfrak{i}}$$

for each $b \in R_{n-m}$. Therefore,

$$\mathfrak{T}(\psi(c)^{-1}(\omega - 1)\Theta) \equiv p^{n-m}(\omega - 1) \sum_{b \in R_{n-m}} \frac{\psi(c)^{-1}\psi((bc)_*)}{\omega^{(bc)^*} - 1} \pmod{\mathfrak{i}}.$$

We see as well that $\mathfrak{i}$ is the product of all prime ideals of $\mathbb{K}_{2^t p^m}$ dividing 2. Hence, by the assumption, any prime ideal of $\mathbb{K}_{2^t p^m}$ dividing 2 does not divide $(\omega-1)\Theta$; indeed, it remains prime in $\mathbb{K}_{2^t p^n}$. Thus the norm of $(\omega-1)\Theta$ for $\mathbb{K}_{2^t p^n}/\mathbb{Q}$ is an odd integer. We can now deduce from (1) that h_n^-/h_{n-1}^- is odd. ∎

We may omit $\psi(c)^{-1}$ in the statement of Lemma 4, while we should note that $\psi(c')^{-1}\psi((bc')_*)$ is a p^mth root of unity for any $(b, c') \in R_{n-m} \times \mathbb{Z}$ with $p \nmid c'$. Further, not only do we have $\{a^* \mid a \in R_{m-1}\} = \{b^* \mid b \in R_{n-m}\}$ but also R may be replaced, from the start, by the set of positive integers $a' < p$ such that $a'a \equiv 1 \pmod{p}$ for some $a \in R$. Thus Lemma 4 gives us the following.

Lemma 5. *Let ζ be any primitive p^mth root of unity. Assume that $2^{p-1} \not\equiv 1 \pmod{p^{m+1}}$ and that, for each map f from R_{m-1} to the set of non-negative integers smaller than p^m,*

$$\sum_{a \in R_{m-1}} \frac{\zeta^{f(a)}}{\zeta^a - 1}$$

is relatively prime to 2. Then h_n^-/h_{n-1}^- is odd.

Let us give one more result.

Lemma 6. *Let ζ be any primitive p^mth root of unity, u any integer, N any positive integer, and μ any map from $\{1, \ldots, N\}$ to $\mathbb{Z}$. Assume that $2^{p-1} \not\equiv 1 \pmod{p^{r+1}}$ with a positive integer $r < m$ and that*

$$\sum_{c=1}^{N} \zeta^{\mu(c)} \equiv 0 \pmod{\mathfrak{l}}$$

with a prime ideal $\mathfrak{l}$ of $\mathbb{K}_{p^r}$ dividing 2. Then

$$\sum_{c'} \zeta^{\mu(c')} \equiv 0 \pmod{\mathfrak{l}},$$

where c' ranges over all positive integers not exceeding N such that $\mu(c') \equiv u \pmod{p^{m-r}}$.

Proof. Let T be the trace map from $\mathbb{K}_{p^m}$ to $\mathbb{K}_{p^r}$. By the hypothesis, $\mathfrak{l}$ remains prime in $\mathbb{K}_{p^m}$ and so

$$T\Big(\sum_{c=1}^{N} \zeta^{\mu(c)-u}\Big)\zeta^u \equiv 0 \pmod{\mathfrak{l}}.$$

However, for each positive integer $c \le N$,

$$T(\zeta^{\mu(c)-u}) = p^{m-r}\zeta^{\mu(c)-u} \quad \text{or} \quad T(\zeta^{\mu(c)-u}) = 0$$

according to whether $\mu(c) \equiv u \pmod{p^{m-r}}$ or not. Thus the lemma is proved. ∎

4. Proof of Theorem 2. To prove Theorem 2, we suppose that $p \le 13$, and hence $2^{p-1} \not\equiv 1 \pmod{p^2}$. The integer m of the preceding section will still be used. For each integer $u \ge 0$, let C_u denote the ideal class group of $\mathbb{B}_u$ in the narrow sense. Then the ideal class group of $\mathbb{B}_\infty$ in the narrow sense is canonically isomorphic to the direct limit of C_u for all integers $u \ge 0$ with respect to the natural homomorphisms $C_u \to C_{u'}$ for all $(u, u') \in \mathbb{Z} \times \mathbb{Z}$ with $0 \le u \le u'$. On the other hand, k is an abelian 2-extension over $\mathbb{Q}$ in which no prime number other than p is ramified. This fact implies by [W2, Theorem 10.4] that the class number of k is odd, whence h_0^-, the relative class number of k, is odd. Therefore, by Lemma 3, it suffices to prove that h_n^-/h_{n-1}^- is always odd.

When $p = 3$ or $p = 5$, the assertion $2 \nmid h_n^-/h_{n-1}^-$ is part of more general results in [W1] but is proved very simply as follows. For $p = 3$, letting $m = 1$ and $R = R_0 = \{1\}$, we obtain the assertion immediately from Lemma 5 (cf. [W1, §IV]). For $p = 5$, we let $m = 1$ and $R = \{1, 2\}$. Let ζ be any primitive 5th root of unity. Then, for any map f from $R = R_0$ to $\{0, 1, 2, 3, 4\}$,

$$(\zeta - 1)\sum_{a\in R} \frac{\zeta^{f(a)}}{\zeta^a - 1} = \zeta^{f(1)}(1 + \zeta^{f(2)-f(1)}(\zeta^4 + \zeta^2 + 1)).$$

Since 2 remains prime in $\mathbb{K}_5$, we easily see that the above algebraic integer is relatively prime to 2. Hence Lemma 5 implies that h_n^-/h_{n-1}^- is odd (cf. [W1, Proposition 3]).

Let us deal with the case $p = 7$. Take $\{1, 2, 4\}$ as R so that $R_1 = \{1, 18, 30\}$. We let $m = 2$ first, and remark that $\mathbb{Q}(\sqrt{-7})$ is the decomposition field of 2 for $\mathbb{K}_7/\mathbb{Q}$. Let ζ be any primitive 49th root of unity. Then

$$\sum_{a\in R_1} \frac{\zeta^{f(a)}}{\zeta^a - 1} = \zeta^{f(1)}\Big(\frac{1}{\zeta - 1} + \frac{\zeta^{f(18)-f(1)}}{\zeta^{18} - 1} + \frac{\zeta^{f(30)-f(1)}}{\zeta^{30} - 1}\Big)$$

for any map $f : R_1 \to \{0, \dots, 48\}$. Assume now that

$$\frac{1}{\zeta - 1} + \frac{\zeta^{c_1}}{\zeta^{18} - 1} + \frac{\zeta^{c_2}}{\zeta^{30} - 1}$$

is not relatively prime to 2 with integers c_1, c_2 in $\{0, \dots, 48\}$, that is,

$$\sum_{a \in Q_0} \zeta^a + \sum_{a \in Q_1} \zeta^a + \sum_{a \in Q_2} \zeta^a$$

is not relatively prime to 2, where

$$Q_0 = \{0, 18, 30, 48\}, \qquad Q_1 = \{c_1, c_1 + 1, c_1 + 30, c_1 + 31\},$$
$$Q_2 = \{c_2, c_2 + 1, c_2 + 18, c_2 + 19\}.$$

It is useful to treat the elements of $Q_0 \cup Q_1 \cup Q_2$ modulo 7; for each pair (u, w) in $\{0, \dots, 6\} \times \{0, 1, 2\}$, we put

$$Q_w(u) = \{a \in Q_w \mid a \equiv u \pmod{7}\}.$$

Since the cardinality of each $Q_w(u)$ is 0 or 1, the above assumption implies by Lemma 6 that

$$\sum_{w=0}^{2} |Q_w(u)| \neq 1, \quad \text{i.e.,} \quad \sum_{w=0}^{2} |Q_w(u)| \in \{0, 2, 3\}$$

for every integer u in $\{0, \dots, 6\}$. This condition is satisfied only when $c_1 \equiv 5 \pmod{7}$ and $c_2 \equiv 4 \pmod{7}$, and then

$$\begin{array}{llll} Q_0(0) = \{0\}, & Q_1(0) = \{c_1 + 30\}, & Q_1(1) = \{c_1 + 31\}, & Q_2(1) = \{c_2 + 18\}, \\ Q_0(2) = \{30\}, & Q_2(2) = \{c_2 + 19\}, & Q_0(4) = \{18\}, & Q_2(4) = \{c_2\}, \\ Q_1(5) = \{c_1\}, & Q_2(5) = \{c_2 + 1\}, & Q_0(6) = \{48\}, & Q_1(6) = \{c_1 + 1\}. \end{array}$$

In particular, we see from Lemma 6 that neither $1 + \zeta^{c_1+30}$ nor $\zeta^{48} + \zeta^{c_1+1}$ is a unit, which means that

$$1 = \zeta^{c_1+30}, \quad \zeta^{48} = \zeta^{c_1+1};$$

but these equalities obviously contradict each other. We therefore find that

$$\sum_{a \in R_1} \frac{\zeta^{f(a)}}{\zeta^a - 1}$$

is relatively prime to 2 for any map $f : R_1 \to \{0, \dots, 48\}$. Hence, by Lemma 5, h_n^-/h_{n-1}^- is odd whenever $n \geq 2m - 1 = 3$.

We next let $m = 1$, still with $R = \{1, 2, 4\}$. Let ψ be a primitive Dirichlet character of order 49 with conductor 7^3, and put $\omega = \psi(50)$. Then ω is a primitive 7th root of unity. In the case $n = 2$, putting $c = 172 = (1 + 7^3)/2$, we have

$$\psi(c)^{-1}\psi(c_*) = \psi(2)\psi(25) = \omega, \qquad \psi(c)^{-1}\psi((18c)_*) = \psi(18) = 1,$$
$$\psi(c)^{-1}\psi((30c)_*) = \psi(30) = \omega^4,$$

so that

$$\sum_{b\in R_1}\frac{\psi(c)^{-1}\psi((bc)_*)}{\omega^{(bc)^*}-1}=-\frac{1}{\omega^2+1}.$$

Therefore Lemma 4 shows that h_2^-/h_1^- is odd. In the case $n=1$, noting that $\omega=\psi^7(8)$, we have

$$\sum_{b\in R}\frac{\psi^7(b_*)}{\omega^{b^*}-1}=-\frac{\omega^3}{\omega+1}$$

and hence Lemma 4 shows as well that h_1^-/h_0^- is odd. The conclusion for $p=7$ is thus proved.

Assertion IV of [AF] implies that, if h_n is odd and the order of 2 modulo p is even, then h_n is also the class number of $\mathbb{B}_n$ in the narrow sense. Hence, as already remarked in the introduction, the conclusion of Theorem 2 follows from Theorem 1 when $p=11$ or $p=13$; nonetheless, for this case, we shall give another proof of Theorem 2 without using Theorem 1 but along the same lines as in the case $p\le 7$.

We now suppose that $p=11$. Let $R=\{1,2,4,5,8\}$ and let ξ be any primitive 11th root of unity. Let us consider the congruence

$$\frac{1}{\xi-1}+\sum_{w=1}^{4}\frac{\xi^{c_w}}{\xi^{2^w}-1}\equiv 0 \pmod 2 \tag{2}$$

with integers c_1, c_2, c_3, c_4 in $\{0,\dots,10\}$. Since

$$\prod_{w=0}^{3}(\xi^{2^w}+1)\equiv\sum_{a=5}^{10}\xi^a \pmod 2,$$

$$\xi^{c_1}\prod_{w=1}^{3}(\xi^{2^w}+1)\equiv\xi^{c_1+5}+\xi^{c_1+7}+\xi^{c_1+9} \pmod 2,$$

we find that (2) is equivalent to the congruence

$$\sum_{a=5}^{10}\xi^a+\xi^{c_1+5}+\xi^{c_1+7}+\xi^{c_1+9}+\xi^{c_2}+\xi^{c_2+1}+\xi^{c_2+4}+\xi^{c_2+8}+\xi^{c_3}+\xi^{c_3+8}+\xi^{c_4}\equiv 0 \pmod 2.$$

Hence, setting $c_2=0,\dots,c_2=10$ successively in the above, we see without difficulty that (2) holds if and only if

$$(c_1,c_2,c_3,c_4)=(5,8,6,7)\quad\text{or}\quad(c_1,c_2,c_3,c_4)=(7,6,1,8). \tag{3}$$

Now, let $m=2$. Let ζ be a primitive 11^2th root of unity such that $\zeta^{11}=\xi$, and note that $R_1=\{1,27,81,112,118\}$. Then, for any map f :

$R_1 \to \{0, \ldots, 120\}$,

$$\sum_{a \in R_1} \frac{\zeta^{f(a)}}{\zeta^{a^*} - 1} = \zeta^{f(1)} \left(\frac{1}{\zeta - 1} + \sum_{w=1}^{4} \frac{\zeta^{f(\hat{w}) - f(1)}}{\zeta^{\hat{w}} - 1} \right),$$

where $(\hat{1}, \hat{2}, \hat{3}, \hat{4}) = (112, 81, 118, 27)$. We assume that there exist integers d_1, d_2, d_3, d_4 in $\{0, \ldots, 120\}$ satisfying

$$\frac{1}{\zeta - 1} + \sum_{w=1}^{4} \frac{\zeta^{d_w}}{\zeta^{\hat{w}} - 1} \equiv 0 \pmod{2}. \tag{4}$$

For each $w \in \{0, 1, 2, 3, 4\}$, define a set Q_w of non-negative integers as follows. Let Q_0 denote the set of

$$\sum_{b \in R_1 \setminus \{1\}} \varepsilon(b) b$$

for all maps $\varepsilon : R_1 \setminus \{1\} \to \{0, 1\}$. If $w \geq 1$, let Q_w denote the set of

$$d_w + \sum_{b \in R_1 \setminus \{\hat{w}\}} \varepsilon(b) b,$$

for all maps $\varepsilon : R_1 \setminus \{\hat{w}\} \to \{0, 1\}$. Given any $u \in \{0, \ldots, 120\}$, we then put

$$Q_w^1(u) = \{a \in Q_w \mid a \equiv u \pmod{11}\},$$
$$Q_w^2(u) = \{a \in Q_w \mid a \equiv u \pmod{11^2}\}.$$

Direct computations show that the cardinality of each $Q_w^2(u)$ is 0 or 1, and that the cardinality of each $Q_w^1(u)$ does not exceed 2, whence

$$\sum_{w=0}^{4} |Q_w^1(u)| \leq 10.$$

Furthermore, 2 remains prime in $\mathbb{K}_{11^2}$, and (4) is equivalent to

$$\sum_{w=0}^{4} \sum_{a \in Q_w} \zeta^a \equiv 0 \pmod{2},$$

which, together with Lemma 6, gives

$$\sum_{w=0}^{4} \sum_{a \in Q_w(u)} \zeta^a \equiv 0 \pmod{2}.$$

Therefore, in view of the form of the 11^2th cyclotomic polynomial, we obtain

$$\sum_{w=0}^{4} |Q_w^2(u)| \equiv 0 \pmod{2}.$$

Consequently,

$$\sum_{w=0}^{4} |Q_w^1(u')| \equiv 0 \pmod 2 \quad \text{for every } u' \in \{0,\dots,10\}.$$

This implies that

$$\sum_{w=0}^{4} \sum_{a\in Q_w} \xi^a \equiv 0 \pmod 2,$$

that is,

$$\frac{1}{\xi-1} + \sum_{w=1}^{4} \frac{\xi^{d_w}}{\xi^{2^w}-1} = \frac{1}{\xi-1} + \sum_{w=1}^{4} \frac{\xi^{d_w}}{\xi^{\hat{w}}-1} \equiv 0 \pmod 2.$$

Hence it follows from (2) that there exist integers c_1', c_2', c_3', c_4' in $\{0,\dots,10\}$ satisfying

$$d_w = 11c_w' + c_w \quad \text{for every } w \in \{1,2,3,4\}.$$

Therefore, by (4),

$$\frac{1}{\xi-1} + \sum_{w=1}^{4} \xi^{c_w'} T\left(\frac{\zeta^{c_w}}{\zeta^{\hat{w}}-1}\right) \equiv 0 \pmod 2; \tag{5}$$

here T denotes the trace map from $\mathbb{K}_{11^2}$ to $\mathbb{K}_{11}$, so that

$$T\left(\frac{1}{\zeta-1}\right) = \frac{11}{\xi-1}$$

and, for each positive integer $a \le 10$,

$$T\left(\frac{\zeta^a}{\zeta-1}\right) = T\left(\sum_{b=0}^{a-1}\zeta^b + \frac{1}{\zeta-1}\right) = \frac{11\xi}{\xi-1}.$$

Since (3) is equivalent to (2), let us first consider the case $(c_1,c_2,c_3,c_4) = (5,8,6,7)$. In this case, (5) is written as

$$\frac{1}{\xi-1} + \frac{\xi^{c_1'-2}}{\xi^2-1} + \frac{\xi^{c_2'+1}}{\xi^4-1} + \frac{\xi^{c_3'}}{\xi^8-1} + \frac{\xi^{c_4'-3}}{\xi^5-1} \equiv 0 \pmod 2.$$

Hence, again by the equivalence of (2) and (3),

$$(c_1',c_2',c_3',c_4') = (7,7,6,10) \quad \text{or} \quad (c_1',c_2',c_3',c_4') = (9,5,1,0).$$

We thus deduce that

$$(d_1,d_2,d_3,d_4) = (82,85,72,117) \quad \text{or} \quad (d_1,d_2,d_3,d_4) = (104,63,17,7).$$

However,

$$\frac{1}{\zeta-1}+\frac{\zeta^{82}}{\zeta^{112}-1}+\frac{\zeta^{85}}{\zeta^{81}-1}+\frac{\zeta^{72}}{\zeta^{118}-1}+\frac{\zeta^{117}}{\zeta^{27}-1} \equiv \Bigl(\prod_{a\in R_1}\frac{1}{\zeta^a-1}\Bigr)\sum_b \zeta^b \pmod 2,$$

$$\frac{1}{\zeta-1}+\frac{\zeta^{104}}{\zeta^{112}-1}+\frac{\zeta^{63}}{\zeta^{81}-1}+\frac{\zeta^{17}}{\zeta^{118}-1}+\frac{\zeta^{7}}{\zeta^{27}-1} \equiv \Bigl(\prod_{a\in R_1}\frac{1}{\zeta^a-1}\Bigr)\sum_{b'} \zeta^{b'} \pmod 2,$$

where b ranges over the integers

$$0,3,4,5,7,14,16,23,25,26,29,32,33,36,37,38,39,42,43,47,48,49,50,58,62,63,$$
$$64,65,67,68,71,73,75,76,79,82,84,85,86,90,92,93,95,96,101,102,106,107,$$

and b' ranges over the integers

$$0,2,11,13,15,17,19,20,21,27,30,31,32,36,41,42,43,44,45,46,51,53,55,$$
$$57,60,62,64,68,69,72,74,75,77,79,80,82,88,89,90,92,97,102,104,107.$$

We are therefore led to a contradiction, whence the case $(c_1,c_2,c_3,c_4)=(5,8,6,7)$ does not occur. In the case $(c_1,c_2,c_3,c_4)=(7,6,1,8)$, as (5) means

$$\frac{1}{\xi-1}+\frac{\xi^{c_1'-1}}{\xi^2-1}+\frac{\xi^{c_2'-3}}{\xi^4-1}+\frac{\xi^{c_3'-1}}{\xi^8-1}+\frac{\xi^{c_4'+2}}{\xi^5-1}\equiv 0 \pmod 2$$

and as (2) is equivalent to (3), it follows that

$$(c_1',c_2',c_3',c_4')=(6,0,7,5) \quad\text{or}\quad (c_1',c_2',c_3',c_4')=(8,9,2,6),$$

so that

$$(d_1,d_2,d_3,d_4)=(73,6,78,63) \quad\text{or}\quad (d_1,d_2,d_3,d_4)=(95,105,23,74);$$

but we have

$$\frac{1}{\zeta-1}+\frac{\zeta^{73}}{\zeta^{112}-1}+\frac{\zeta^{6}}{\zeta^{81}-1}+\frac{\zeta^{78}}{\zeta^{118}-1}+\frac{\zeta^{63}}{\zeta^{27}-1} \equiv \Bigl(\prod_{a\in R_1}\frac{1}{\zeta^a-1}\Bigr)\sum_b \zeta^b \pmod 2,$$

$$\frac{1}{\zeta-1}+\frac{\zeta^{95}}{\zeta^{112}-1}+\frac{\zeta^{105}}{\zeta^{81}-1}+\frac{\zeta^{23}}{\zeta^{118}-1}+\frac{\zeta^{74}}{\zeta^{27}-1} \equiv \Bigl(\prod_{a\in R_1}\frac{1}{\zeta^a-1}\Bigr)\sum_{b'} \zeta^{b'} \pmod 2,$$

where b ranges over the integers

$0, 2, 3, 4, 5, 7, 9, 11, 12, 13, 14, 16, 17, 18, 22, 23, 25, 28, 29, 30, 31, 35, 42, 46, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 60, 61, 63, 65, 66, 68, 73, 74, 75, 81, 82, 83, 86, 90, 93, 94, 97, 98, 99, 100, 104, 105, 106, 109,$

and b' ranges over the integers

$3, 10, 12, 13, 14, 18, 19, 20, 22, 24, 25, 26, 27, 30, 32, 34, 46, 50, 51, 55, 56, 57, 62, 64, 65, 66, 68, 69, 71, 78, 80, 81, 82, 83, 85, 86, 90, 92, 94, 96, 99, 101, 102, 103, 104, 105, 106, 107, 109.$

We thus conclude from the above contradiction that (4) is not satisfied by any 4-tuple (d_1, d_2, d_3, d_4) of integers in $\{0, \ldots, 120\}$. Hence, in virtue of Lemma 5, h_n^-/h_{n-1}^- is odd if $n \geq 3$.

We next let $m = 1$, $R = \{1, 2^*, 4^*, 8^*, 16^*\} = \{1, 3, 6, 7, 9\}$, and so $R_1 = \{1, 3, 9, 40, 94\}$. Let ξ be any primitive 11th root of unity as before, and let ψ be a primitive Dirichlet character of order 121 with conductor 11^3 such that $\xi = \psi(122) = \psi^{11}(12)$. When $n = 2$,

$$\sum_{b\in R_1} \frac{\psi(b_*)}{\xi^{b^*} - 1} = \frac{1}{\xi - 1} + \frac{\psi(94)}{\xi^2 - 1} + \frac{\psi(3)}{\xi^4 - 1} + \frac{\psi(40)}{\xi^8 - 1} + \frac{\psi(9)}{\xi^5 - 1}.$$

Furthermore, whether $n = 1$ or not,

$$\sum_{b\in R} \frac{\psi^{11}(b)}{\xi^{b^*} - 1} = \frac{1}{\xi - 1} + \frac{\psi^{11}(6)}{\xi^2 - 1} + \frac{\psi^{11}(3)}{\xi^4 - 1} + \frac{\psi^{11}(7)}{\xi^8 - 1} + \frac{\psi^{11}(9)}{\xi^5 - 1}.$$

We know, however, that $\psi(3) = 1$. Hence, by the equivalence of (2) and (3), Lemma 4 shows that h_n^-/h_{n-1}^- is odd even if $n = 2$ or $n = 1$.

We finally deal with the case $p = 13$. Let $R = \{1, 2, 3, 4, 6, 8\}$, let ξ_1 be a primitive 13th root of unity, and let U denote the set of the following 5-tuples of integers:

$(5, 6, 5, 1, 4)$,	$(3, 7, 1, 2, 4)$,	$(4, 7, 1, 3, 4)$,	$(5, 7, 2, 3, 4)$,
$(5, 7, 5, 1, 5)$,	$(3, 6, 1, 2, 5)$,	$(4, 6, 1, 3, 5)$,	$(5, 6, 2, 3, 5)$,
$(10, 0, 5, 6, 5)$,	$(9, 10, 7, 6, 5)$,	$(9, 0, 5, 7, 5)$,	$(10, 10, 7, 7, 5)$,
$(12, 8, 0, 2, 6)$,	$(2, 6, 1, 2, 6)$,	$(12, 9, 0, 3, 6)$,	$(11, 9, 0, 4, 6)$,
$(9, 10, 8, 6, 6)$,	$(10, 10, 8, 7, 6)$,	$(12, 10, 0, 3, 7)$,	$(11, 10, 0, 4, 7)$,
$(9, 9, 8, 6, 7)$,	$(10, 9, 8, 7, 7)$,	$(3, 4, 0, 10, 7)$,	$(2, 4, 0, 11, 7)$,
$(8, 9, 8, 6, 8)$,	$(5, 11, 9, 6, 8)$,	$(5, 12, 9, 7, 8)$,	$(4, 12, 9, 8, 8)$,
$(3, 5, 0, 10, 8)$,	$(2, 5, 0, 11, 8)$,	$(2, 6, 0, 12, 8)$,	$(12, 8, 1, 12, 8)$,
$(9, 7, 9, 1, 9)$,	$(8, 7, 9, 2, 9)$,	$(5, 0, 9, 7, 9)$,	$(4, 0, 9, 8, 9)$,
$(10, 8, 1, 11, 9)$,	$(11, 8, 1, 12, 9)$,	$(9, 8, 9, 1, 10)$,	$(8, 8, 9, 2, 10)$,
$(5, 11, 8, 3, 10)$,	$(8, 9, 9, 3, 10)$,	$(10, 7, 1, 11, 10)$,	$(11, 7, 1, 12, 10)$,
$(2, 11, 7, 2, 11)$,	$(3, 11, 8, 2, 11)$,	$(4, 11, 8, 3, 11)$,	$(2, 10, 4, 4, 11)$,
$(10, 7, 2, 11, 11)$,	$(11, 4, 4, 11, 11)$,	$(11, 7, 2, 12, 11)$,	$(10, 4, 4, 12, 11)$,
$(2, 10, 7, 2, 12)$,	$(3, 10, 8, 2, 12)$,	$(4, 10, 8, 3, 12)$,	$(2, 11, 4, 4, 12)$.

Using a computer, we can check that integers c_1, c_2, c_3, c_4, c_5 in $\{0, \ldots, 12\}$ satisfy

$$\frac{1}{\xi_1 - 1} + \sum_{w=1}^{5} \frac{\xi_1^{2^w c_w}}{\xi_1^{2^w} - 1} \equiv 0 \pmod{2}$$

if and only if $(c_1, c_2, c_3, c_4, c_5)$ belongs to U.

Now, let $m = 3$. Let ζ be a primitive 13^3th root of unity such that $\zeta^{13} = \xi_2$, with ξ_2 a primitive 169th root of unity such that $\xi_2^{13} = \xi_1$. We note that 2 remains prime in $\mathbb{K}_{13^3}$, $R_2 = \{1, 418, 1160, 1161, 1540, 1958\}$, and for any map $f : R_2 \to \{0, \ldots, 13^3 - 1\}$,

$$\sum_{a \in R_2} \frac{\zeta^{f(a)}}{\zeta^a - 1} = \zeta^{f(1)} \left(\frac{1}{\zeta - 1} + \sum_{w=1}^{5} \frac{\zeta^{f(\dot{w}) - f(1)}}{\zeta^{\dot{w}} - 1} \right),$$

where $(\dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}) = (418, 1161, 1958, 1160, 1540)$. Assume the congruence

$$\frac{1}{\zeta - 1} + \sum_{w=1}^{5} \frac{\zeta^{\dot{w} d_w}}{\zeta^{\dot{w}} - 1} \equiv 0 \pmod{2} \tag{6}$$

to be satisfied by non-negative integers d_1, d_2, d_3, d_4, d_5 smaller than 13^3. Putting $d_0 = 0$, let Q_w denote for each $w \in \{0, \ldots, 5\}$ the set of the integers

$$d_w + \sum_{b \in R_2 \setminus \{\dot{w}\}} \varepsilon(b) b$$

for all maps $\varepsilon : R_2 \setminus \{\dot{w}\} \to \{0, 1\}$. Let u range over the non-negative integers smaller than 13^3. We then put

$$Q_w^2(u) = \{a \in Q_w \mid a \equiv u \pmod{13^2}\},$$
$$Q_w^3(u) = \{a \in Q_w \mid a \equiv u \pmod{13^3}\}.$$

As in the case $p = 11$, we see that each $|Q_w^3(u)|$ is 0 or 1 and that no $|Q_w^2(u)|$ exceeds 2. Hence not only is (6) equivalent to

$$\sum_{w=0}^{5} \sum_{a \in Q_w} \zeta^a \equiv 0 \pmod{2}$$

but also we have

$$\sum_{w=0}^{5} |Q_w^2(u)| \leq 12.$$

Lemma 6 therefore shows that

$$\sum_{w=0}^{5} |Q_w^3(u)| \equiv 0 \pmod{2},$$

which implies that

$$(7)\qquad \sum_{w=0}^{5}\sum_{a\in Q_w}\xi_2^a\equiv 0 \pmod 2,\qquad \sum_{w=0}^{5}\sum_{a\in Q_w}\xi_1^a\equiv 0 \pmod 2.$$

Since the second congruence above gives

$$\frac{1}{\xi_1-1}+\sum_{w=1}^{5}\frac{\xi_1^{2^w d_w}}{\xi_1^{2^w}-1}=\frac{1}{\xi_1-1}+\sum_{w=1}^{5}\frac{\xi_1^{\dot{w}d_w}}{\xi_1^{\dot{w}}-1}\equiv 0 \pmod 2,$$

there exist integers d_1', d_2', d_3', d_4', d_5', d_1'', d_2'', d_3'', d_4'', d_5'' in $\{0,\dots,12\}$ such that $(d_1',d_2',d_3',d_4',d_5')$ belongs to U and

$$d_w\equiv 13d_w''+d_w' \pmod{13^2}\qquad \text{for every } w\in\{1,\dots,5\}.$$

Hence, by the first congruence of (7),

$$\frac{1}{\xi_2-1}+\sum_{w=1}^{5}\frac{\xi_1^{2^w d_w''}\xi_2^{\dot{w}d_w'}}{\xi_2^{\dot{w}}-1}\equiv 0 \pmod 2.$$

The trace map from $\mathbb{K}_{13^2}$ to $\mathbb{K}_{13}$ transforms the above into

$$\frac{1}{\xi_1-1}+\sum_{w=1}^{5}\frac{\xi_1^{2^w(d_w''+\kappa(d_w'))}}{\xi_1^{2^w}-1}\equiv 0 \pmod 2,$$

where, for each integer c, $\kappa(c)=0$ or $\kappa(c)=1$ according to whether c is divisible by 13 or not. Thus there exists a 5-tuple (c_1,c_2,c_3,c_4,c_5) in U satisfying

$$d_w''+\kappa(d_w')\equiv c_w \pmod{13}\qquad \text{for every } w\in\{1,\dots,5\}.$$

In particular,

$$\frac{1}{\xi_2-1}+\sum_{w=1}^{5}\frac{\xi_2^{\dot{w}(13(c_w-\kappa(d_w'))+d_w')}}{\xi_2^{\dot{w}}-1}\equiv 0 \pmod 2.$$

However, for any given $(c_1',c_2',c_3',c_4',c_5'),(c_1'',c_2'',c_3'',c_4'',c_5'')\in U$, we can check by computer that

$$\frac{1}{\xi_2-1}+\sum_{w=1}^{5}\frac{\xi_2^{\dot{w}(13(c_w''-\kappa(c_w'))+c_w')}}{\xi_2^{\dot{w}}-1}\not\equiv 0 \pmod 2.$$

This contradiction shows that no 5-tuple (d_1,d_2,d_3,d_4,d_5) of integers in $\{0,\dots,13^3-1\}$ satisfies the congruence (6). Hence, by Lemma 5, h_n^-/h_{n-1}^- is odd if $n\ge 5$.

We now let $m=1$, $R=\{1,5,7,9,10,11\}$, and so

$$R_3=\{1,239,5051,7627,7628,23749\}.$$

Let ξ_1 be any primitive 13th root of unity as before. Let ψ be a primitive Dirichlet character of order 13^4 with conductor 13^5 such that $\xi_1=\psi(1+13^4)$,

whence
$$\xi_1 = \psi^{13}(1+13^3) = \psi^{13^2}(1+13^2) = \psi^{13^3}(14).$$
We then see that, in the case $n=4$,
$$\sum_{b\in R_3} \frac{\psi(b_*)}{\xi_1^{b^*}-1} = \frac{1}{\xi_1-1} + \frac{\psi(5051)}{\xi_1^2-1} + \frac{\psi(7628)}{\xi_1^4-1} + \frac{\psi(239)}{\xi_1^8-1} + \frac{\psi(7627)}{\xi_1^{16}-1} + \frac{\psi(23749)}{\xi_1^{32}-1},$$
in the case $n=3$,
$$\sum_{b\in R_2} \frac{\psi^{13}(b_*)}{\xi_1^{b^*}-1} = \frac{1}{\xi_1-1} + \frac{\psi^{13}(657)}{\xi_1^2-1} + \frac{\psi^{13}(1037)}{\xi_1^4-1} + \frac{\psi^{13}(239)}{\xi_1^8-1} + \frac{\psi^{13}(1036)}{\xi_1^{16}-1} + \frac{\psi^{13}(1779)}{\xi_1^{32}-1},$$
in the case $n=2$,
$$\sum_{b\in R_1} \frac{\psi^{13^2}(b_*)}{\xi_1^{b^*}-1} = \frac{1}{\xi_1-1} + \frac{\psi^{13^2}(150)}{\xi_1^2-1} + \frac{\psi^{13^2}(23)}{\xi_1^4-1} + \frac{\psi^{13^2}(70)}{\xi_1^8-1} + \frac{\psi^{13^2}(22)}{\xi_1^{16}-1} + \frac{\psi^{13^2}(89)}{\xi_1^{32}-1},$$
and in any case,
$$\sum_{b\in R} \frac{\psi^{13^3}(b)}{\xi_1^{b^*}-1} = \frac{1}{\xi_1-1} + \frac{\psi^{13^3}(7)}{\xi_1^2-1} + \frac{\psi^{13^3}(10)}{\xi_1^4-1} + \frac{\psi^{13^3}(5)}{\xi_1^8-1} + \frac{\psi^{13^3}(9)}{\xi_1^{16}-1} + \frac{\psi^{13^3}(11)}{\xi_1^{32}-1}.$$
Furthermore,
$$\psi^{13}(1779) = \psi^{13^2}(89) = (\xi_1^{32})^3, \quad \psi(7627) = (\xi_1^{16})^8, \quad \psi(23749) = (\xi_1^{32})^5,$$
$$\psi^{13^3}(9) = (\xi_1^{16})^{12}, \quad \psi^{13^3}(11) = (\xi_1^{32})^7.$$
Therefore, viewing the elements of U, we know from Lemma 4 that h_n^-/h_{n-1}^- is odd if $n \le 4$. Consequently, the theorem is completely proved.

5. Final remark. Let H denote the class number of $\mathbb{B}_1$ in the narrow sense. By class field theory, H must be odd when the narrow 2-class group of $\mathbb{B}_\infty$ is trivial. For each integer a relatively prime to p, we define an integer $v(a)$ by
$$1 - a^{p-1} = pv(a).$$
The following assertion does not need the assumption $2^{p-1} \not\equiv 1 \pmod{p^2}$.

PROPOSITION. *Assume that $m=1$, and take any primitive pth root ζ of unity. Then H is odd if and only if*
$$\sum_{b\in R} \frac{\zeta^{v(b)}}{\zeta^{b^*}-1}$$
is relatively prime to 2.

Proof. Let ψ be a primitive Dirichlet character of order p with conductor p^2 such that $\psi(1+p) = \zeta$. Let χ be any primitive Dirichlet character of order 2^t with conductor p, that is, $\chi \in \mathfrak{X}$. As in the proof of Lemma 4, we have

$$-\frac{1}{2p^2}\sum_{a=1}^{p^2}\chi\psi(a)a \equiv \sum_{b\in R}\frac{\psi(b)}{\zeta^{b^*}-1} \pmod{\mathfrak{i}},$$

where $\mathfrak{i}$ denotes the integral ideal of $\mathbb{K}_{2^t p}$ generated by $e^{\pi i/2^{t-1}} - 1$. Since $\mathfrak{i}$ is the product of all prime ideals of $\mathbb{K}_{2^t p}$ dividing 2, it then follows from (1) that h_1^-/h_0^- is odd if and only if

$$\sum_{b\in R}\frac{\psi(b)}{\zeta^{b^*}-1}$$

is relatively prime to 2. Furthermore, for any $b \in R$, an integer b' with $\zeta^{b'} = \psi(b)$ satisfies $(1+p)^{b'(p-1)} \equiv b^{p-1} \pmod{p^2}$, i.e., $b' \equiv v(b) \pmod{p}$. Hence Lemma 3, together with the fact $2 \nmid h_0^-$, proves the proposition. ∎

By means of the above proposition, we have checked by computer that, if $p \le 487$, then H is odd.

Now, take any prime number q different from p. Let F be the decomposition field of q for the abelian extension $\mathbb{K}_p\mathbb{B}_\infty/\mathbb{Q}$. Note that F is of finite degree and that the case $q = l$ is none other than the case $F = \mathbb{Q}$. It is shown in [H3] that, if q is sufficiently large with the degree of F bounded, then the q-class group of $\mathbb{B}_\infty$ is trivial, whence q does not divide h_n, the class number of $\mathbb{B}_n$. This result implies that the primes q' for which the q'-class group of $\mathbb{B}_\infty$ is trivial distribute with natural density 1 in the set of all prime numbers. On the other hand, we have not found any example of (p, n) such that $h_n > 1$. Hence the question arises whether the ideal class group of $\mathbb{B}_\infty$ is trivial (cf. also J. Buhler, C. Pomerance and L. Robertson [BPR], J. P. Cerri [Ce], H. Cohn [Co], T. Fukuda and K. Komatsu [FK], and [H1]). Moreover, in connection with our results on the narrow class group of $\mathbb{B}_\infty$, it might be an interesting problem to find whether H is always odd.

References

[AF] J. V. Armitage and A. Fröhlich, *Classnumbers and unit signatures*, Mathematika 14 (1967), 94–98.

[BPR] J. Buhler, C. Pomerance and L. Robertson, *Heuristics for class numbers of prime-power real cyclotomic fields*, in: High Primes and Misdemeanours: Lectures in Honor of the Sixtieth Birthday of Hugh Cowie Williams, A. van der Poorten (ed.), Fields Inst. Comm. 41 (2004), 149–157.

[Ce] J.-P. Cerri, *De l'euclidianité de* $\mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ *et* $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ *pour la norme*, J. Théor. Nombres Bordeaux 12 (2000), 103–126.

[Co] H. Cohn, *A numerical study of Weber's real class number calculation I*, Numer. Math. 2 (1960), 347–362.

[FK] T. Fukuda and K. Komatsu, *Weber's class number problem in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$*, Experiment. Math., to appear.

[H] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952; Springer-Verlag, Berlin, 1985.

[H1] K. Horie, *Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field*, J. London Math. Soc. (2) 66 (2002), 257–275 ("$\psi_2^d(b) = 1$" in line 11 on page 260 should be "$\psi_2(b)^d = 1$").

[H2] —, *Primary components of the ideal class group of the $\mathbb{Z}_p$-extension over $\mathbb{Q}$ for typical inert primes*, Proc. Japan Acad. Ser. A Math. Sci. 81 (2005), 40–43.

[H3] —, *The ideal class group of the basic $\mathbb{Z}_p$-extension over an imaginary quadratic field*, Tohoku Math. J. 57 (2005), 375–394 ("$p - 1$" in line 7 on page 391 should be "$\varphi(q)$"; so "$(p - 1)f$" in lines 16, 20 on page 389 and in lines 9, 11 on page 391, along with "$f(p - 1)$" in line 19 on page 391, should be "$\varphi(q)f$" (cf. also [H4, §4])).

[H4] —, *Primary components of the ideal class group of an Iwasawa-theoretical abelian number field*, J. Math. Soc. Japan 59 (2007), 811–824.

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

[W1] L. C. Washington, *Class numbers and $\mathbb{Z}_p$-extensions*, Math. Ann. 214 (1975), 177–193.

[W2] —, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer-Verlag, New York, 1996.

Department of Mathematics
Tokai University
1117 Kitakaname, Hiratsuka
Kanagawa 259-1292, Japan

Department of Mathematics
Ochanomizu University
2-1-1 Otsuka, Bunkyo-ku
Tokyo 112-8610, Japan
E-mail: horie.mitsuko@ocha.ac.jp

Received on 24.1.2008
and in revised form on 31.5.2008 (5619)