WEBER’S CLASS NUMBER PROBLEM

TAKASHI FUKUDA AND KEIICHI KOMATSU

1. Introduction

Two hundred years ago, Gauss gave the following two conjectures (cf. [2]):

**Conjecture 1.** The imaginary quadratic fields with class number one are as follows:

\[ \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11}), \]
\[ \mathbb{Q}(\sqrt{-19}), \mathbb{Q}(\sqrt{-43}), \mathbb{Q}(\sqrt{-67}), \mathbb{Q}(\sqrt{-163}). \]

**Conjecture 2.** There are infinitely many real quadratic fields with class number one.

Conjecture 1 was settled by Stark. Conjecture 2 is still open. Concerning Conjecture 2, Weber considered the following problem:

**Problem 1.** Are there infinitely many algebraic number fields with class number one?

We are interested in the class number \( h_n \) of the field \( \mathbb{B}_n = \mathbb{Q}(2 \cos(2\pi/2^{n+2})) \) which is a cyclic extension of \( \mathbb{Q} \) with degree \( 2^n \) and constructs the cyclotomic \( \mathbb{Z}_2 \)-extension of \( \mathbb{Q} \). The calculation of \( h_n \) is very difficult even if we use a computer. A technique using root discriminant enabled Linden to conclude \( h_5 = 1 \) (cf. [8]). It is also shown \( h_6 = 1 \) if GRH (Generalized Riemann Hypothesis) is valid. This phenomenon indicates a possibility that \( h_n = 1 \) for all \( n \geq 1 \). But the same technique is no longer applicable for \( h_n \) \( (n \geq 7) \). We need a entirely new technique to calculate \( h_n \) or to show \( h_n = 1 \) for \( n \geq 7 \).

On the other hand, more than one hundred years ago, Weber [10] investigated the even part of \( h_n \) and proved that \( h_n \) is not divisible by 2 for all \( n \geq 1 \). So we are led to study the odd part of \( h_n \). In this aspect, there are preceding works of Horie [4], [5], [6], [7]. He proved that if \( \ell \) satisfies a certain congruence relation and exceeds a certain bound, which is explicitly described, then \( \ell \) does not divide \( h_n \) for all \( n \geq 1 \), namely the \( \ell \)-part of \( h_n \) is trivial for all \( n \geq 1 \). The following is a part of Horie’s results.

**Theorem 1** (Horie). Let \( \ell \) be a prime number.

1. If \( \ell \equiv 3, 5 \pmod{8} \), then \( \ell \) does not divide \( h_n \) for all \( n \geq 1 \).
2. If \( \ell \equiv 9 \pmod{16} \) and \( \ell > 34797970939 \), then \( \ell \) does not divide \( h_n \) for all \( n \geq 1 \).
3. If \( \ell \equiv -9 \pmod{16} \) and \( \ell > 210036365154018 \), then \( \ell \) does not divide \( h_n \) for all \( n \geq 1 \).

1991 Mathematics Subject Classification. 11G15, 11R27, 11Y40.

Key words and phrases. class number, computation.
Although Horie’s results were very striking and very effective, there were many small prime numbers \(\ell\) for which we did not know whether \(\ell\) divides \(h_n\). For example, it was not known whether \(\ell | h_n\) (\(n \geq 6\)) for \(\ell = 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97, \ldots\).

In this talk, we give a criterion for non-divisibility of \(h_n\) for given \(n\) and prove that if \(\ell\) does not divide \(h_m\) for some \(m \geq 1\), then \(\ell\) does not divide \(h_n\) for all \(n \geq 1\). A bound \(m\), which depends on \(\ell\), is explicitly given and is small enough to make it possible to verify computationally that \(\ell\) does not divide \(h_m\). For a real number \(x\), we denote by \([x]\) the largest integer not exceeding \(x\).

**Theorem 2.** Let \(\ell\) be an odd prime number and \(2^c\) the exact power of 2 dividing \(\ell - 1\) or \(\ell^2 - 1\) according as \(\ell \equiv 1 \pmod{4}\) or not. Put

\[
m = 2c - 3 + [\log_2 \ell].
\]

If \(\ell\) does not divide the class number of \(B_m\), then \(\ell\) does not divide the class number of \(B_n\) for all \(n \geq 1\).

Typical values of \(m\) are as follows:

<table>
<thead>
<tr>
<th>(\ell)</th>
<th>7</th>
<th>17</th>
<th>31</th>
<th>257</th>
<th>8191</th>
<th>65537</th>
<th>524287</th>
<th>7340033</th>
<th>39845887</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m)</td>
<td>7</td>
<td>9</td>
<td>14</td>
<td>21</td>
<td>38</td>
<td>45</td>
<td>56</td>
<td>59</td>
<td>66</td>
</tr>
</tbody>
</table>

Theorem 2, together with numerical calculations, allows us to obtain the following corollary.

**Corollary 1.** Let \(\ell\) be a prime number less than \(10^8\). Then \(\ell\) does not divide the class number of \(B_n\) for all \(n \geq 1\).

One more our result is considered a precise version of Horie’s result.

**Theorem 3.** Let \(\ell\) be a prime number. If \(\ell \equiv \pm 9 \pmod{16}\), then \(\ell\) does not divide the class number of \(B_n\) for all \(n \geq 1\).

2. Proof of Theorem

Theorems 2 and 3 are proven by investigating Horie’s techniques carefully and using his lemma in [4, p. 378].

Let \(\zeta_n = \exp(2\pi \sqrt{-1}/2^n)\) and

\[
\eta_n = \frac{\zeta_{n+2} - 1}{\sqrt{-1}(\zeta_{n+2} + 1)} = \frac{\sqrt{2 - 2\cos(2\pi/2^{n+2})}}{\sqrt{2 + 2\cos(2\pi/2^{n+2})}} \in B_n.
\]

Then \(\eta_n\) is a cyclotomic unit of \(B_n\). This special unit played important role in Horie’s works. An element \(\alpha\) in \(\mathbb{Z}[\zeta_n]\) is uniquely expressed in the form

\[
\alpha = \sum_{j=0}^{2^{n-1}-1} a_j \zeta_n^j \quad (a_j \in \mathbb{Z}).
\]
For each such $\alpha$ and each $\rho \in G(\mathbb{Q}(\zeta_{n+2}/\mathbb{Q}(\zeta_2)))$, we define the element $\alpha_\rho$ in the group ring $\mathbb{Z}[G(\mathbb{Q}(\zeta_{n+2}/\mathbb{Q}(\zeta_2)))]$ by

$$\alpha_\rho = \sum_{j=0}^{2^n-1-1} a_j \rho^j.$$ 

Moreover let $F_n$ be the decomposition field of $\ell$ for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Then the following Horie’s lemmas work essentially in our proofs.

**Lemma 1** (cf. [4]). Let $\ell$ be an odd prime number and $\sigma$ a generator of $G(\mathbb{Q}(\zeta_{n+2})/\mathbb{Q}(\zeta_2))$. Then $\ell$ divides $h_n/h_{n-1}$ if and only if there exists a prime ideal $\mathfrak{p}$ of $F_n$ dividing $\ell$ such that $\eta_n^{\sigma}$ is an $\ell$-th power in $\mathbb{B}_n$ for any element $\alpha$ of the ideal $\ell \mathfrak{p}^{-1}$ of $F_n$.

**Lemma 2** (cf. [3]). Let $\ell$ be an odd prime number and $\varphi$ the Frobenius automorphism of $\ell$ in $\mathbb{Q}(\zeta_{n+2})/\mathbb{Q}$. If an element $\alpha$ in $\mathbb{Z}[\zeta_{n+2}]$ is an $\ell$-th power in $\mathbb{Z}[\zeta_{n+2}]$, then $\alpha^\varphi - \alpha \in \ell^2 \mathbb{Z}[\zeta_{n+2}]$.

We prove Theorem 2 using Horie’s lemmas together with the following two lemmas.

**Lemma 3.** Let $a_i$ be elements in $\mathbb{Z}$. If

$$\sum_{i=0}^{2^n+1-1} a_i \zeta_{n+2}^i \equiv 0 \pmod{\ell},$$

then $a_i \in \ell \mathbb{Z}$ for $0 \leq i \leq 2^{n+1} - 1$.

**Lemma 4.** We put

$$S = \{ a_{n-c+2} 2^{n-c+2} + a_{n-c+3} 2^{n-c+3} + \cdots + a_{n+1} 2^{n+1} \mid a_i = 0, 1 \}.$$ 

Let $j$ be a rational integer with $0 \leq j \leq 2^c - 1$, $\nu$ a rational integer with $1 \leq \nu \leq \ell - 1$, $\rho$ an element in $S$ and $\ell$ an odd prime number with $\ell < 2^{n-2^c+3}$. If $\rho(\nu + \ell j) + \nu + \ell j \equiv 2^c \ell - 1 \pmod{2^{n+1}}$, then $j = 2^c - 1$, $\nu = \ell - 1$ and $\rho = 0$ or $2^{n+1}$.

In order to prove Theorem 3, we need the following lemma and calculations based on a computer.

**Lemma 5.** Assume that an odd prime number $\ell$ divides $h_n$.

1. If $\ell \equiv 9 \pmod{16}$, then we have $2^{n-3} < \ell < 12^2(n+1)^4$.
2. If $\ell \equiv -9 \pmod{16}$, then we have $2^{n-5} < \ell < 21^2(n+1)^4$.

Thanks to Lemma 5, we are able to reduce the number of $\ell$ to be checked to about 4 million in the case $\ell \equiv 9 \pmod{16}$ and about 25 million in the case $\ell \equiv -9 \pmod{16}$.

3. Calculation

We briefly explain how to verify numerically that an odd prime number $\ell$ does not divide the class number $h_n$ of $\mathbb{B}_n$. The details are explained in [1]. Let $\Delta_n = G(\mathbb{B}_n/\mathbb{Q})$ be the Galois group of $\mathbb{B}_n$ over $\mathbb{Q}$ and $A_n$ the $\ell$-part of the ideal class group of $\mathbb{B}_n$. For a character $\chi : \Delta_n \to \mathbb{Q}_\ell$, we define the idempotent $e_\chi$ by

$$e_\chi = \frac{1}{|\Delta_n|} \sum_{\sigma \in \Delta_n} \text{Tr}(\chi^{-1}(\sigma)) \sigma \in \mathbb{Z}_\ell[\Delta_n].$$
and the \( \chi \)-part \( A_{n,\chi} \) of \( A_n \) by \( A_{n,\chi} = e_\chi A_n \), where \( \text{Tr} : \mathbb{Q}_\ell(\chi(\Delta_n)) \to \mathbb{Q}_\ell \) is the trace map. Then we have \( A_n = \bigoplus \chi A_{n,\chi} \), where \( \chi \) runs over all representatives of \( \mathbb{Q}_\ell \)-conjugacy classes of characters of \( \Delta_n \). If \( \chi \) is not injective, the intermediate field of \( \mathbb{B}_n \) corresponding to \( \text{Ker} \chi \) is \( \mathbb{B}_k \) for some \( 0 \leq k < n \) and \( A_{n,\chi} \cong A_{k,\chi} \) canonically. So we may assume that \( \chi \) is injective.

Now, let \( \zeta_n = \exp(2\pi i/2^{n+2}) \) as in \( \S 2 \) and put

\[
\xi_n = (\zeta_{n+2} - 1)(\zeta_{n+2}^{-1} - 1) \in \mathbb{B}_n.
\]

Let \( e_{\chi,\ell} \in \mathbb{Z}[\Delta_n] \) be any element satisfying \( e_{\chi,\ell} \equiv e_\chi \mod \ell \). Then the following lemma is a special case of Gras conjecture which is a direct consequence of Iwasawa main conjecture proven by Mazur-Wiles [9].

**Lemma 6.** If there exists a prime number \( p \) which is congruent to 1 modulo \( 2^{n+2}\ell \) and satisfies

\[
(\xi_n^{e_{\chi,\ell}})^{\frac{2^{n+1}}{p-1}} \not\equiv 1 \pmod{p}
\]

for some prime ideal \( p \) of \( \mathbb{B}_n \) lying above \( p \), then we have \( |A_{n,\chi}| = 1 \).

Since \( p \) in Lemma 6 splits completely in \( \mathbb{B}_n/\mathbb{Q} \), we have \( \mathfrak{O}_n/p \cong \mathbb{Z}/p\mathbb{Z} \), where \( \mathfrak{O}_n \) is the integer ring of \( \mathbb{B}_n \). So we are able to show \( |A_n| = 1 \) by calculations of rational integers. Further, taking advantage of a special feature of \( \mathbb{B}_n \), we reduce the amount of calculations for one \( A_{n,\chi} \) from \( \mathcal{O}(2^n) \) to \( \mathcal{O}(2^c) \). Finally we reduce the total amount of calculations from \( \mathcal{O}(4^c) \) to \( \mathcal{O}(c2^c) \) using Fast Fourier Transform.

**References**


**Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan**

*E-mail address:* fukuda@math.cit.nihon-u.ac.jp

**Department of Mathematics, School of Science and Engineering, Waseda University, 3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan**

*E-mail address:* kkomatsu@waseda.jp