MATIMYÁS MATEMATIKA Journal of the Mathematical Society of the Philippines
ISSN 0115-6926 Vol. 46 No. 1 (2023) pp. 33-46

Divisibility by powers of 2 of the class number of $\mathbb{Q}(\sqrt{\pm p}, \sqrt{\pm 2})$

Julius M. Basilla
University of the Philippines Diliman
Quezon City, Philippines
jbasilla@math.upd.edu.ph

Christopher F. Santos
University of the Philippines Diliman
Quezon City, Philippines
cfsantos3@up.edu.ph

Abstract

Let K be a bicyclic biquadratic field of the form $\mathbb{Q}(\sqrt{\pm p}, \sqrt{\pm 2})$ where p is an odd prime. Using the class number formula of Herglotz, Gauss genus theory, and results on the divisibility of narrow class numbers of quadratic fields by 2^n where $n \leq 3$, we give necessary and sufficient conditions for the class number of K to be divisible by some power of 2. Our main result subsumes the conditions found by Kucera for $\mathbb{Q}(\sqrt{p}, \sqrt{2})$, $p \equiv 1 \pmod 4$ using the group of circular units.

Keywords: 2-part, bicyclic biquadratic number fields, Herglotz equation
2020 MSC: 11R29, 11R16

1 Introduction

Let p be an odd prime and K be the bicyclic biquadratic field $\mathbb{Q}(\sqrt{\sigma}, \sqrt{\tau})$ with quadratic subfields $k_1 = \mathbb{Q}(\sqrt{\sigma})$, $k_2 = \mathbb{Q}(\sqrt{\tau})$, and $k_3 = \mathbb{Q}(\sqrt{\sigma\tau})$, where $\sigma = \pm p$ and $\tau = \pm 2$. The field K is said to be real if $\sigma > 0$ and $\tau > 0$; otherwise, K is imaginary. Let H be the class number of K and denote by h_i and h_i^+ the class number and the narrow class number of k_i, respectively, for $i = 1, 2, 3$.

For a quadratic field $k = \mathbb{Q}(\sqrt{m})$, where m is a squarefree integer, $h^+ = 2h$ if $m > 0$ and $e > 0$ where e is the norm of the fundamental unit ϵ of k. Otherwise, $h^+ = h$.

For integers a, b, and n where a is not divisible by b, we write $\left(\frac{a}{b}\right)_n = 1$ if $x^n \equiv a \pmod b$ has a solution and $\left(\frac{a}{b}\right)_n = -1$ otherwise. Moreover, we write $2^n || x$ if and only if $x \equiv 2^n \pmod{2^{n+1}}$.

Since $h_2 = 1$, then by Herglotz [7, 13] we have

$$H = \begin{cases} \dfrac{Q}{4} h_1 h_3, & \text{if } K \text{ is real} \\ \\ \dfrac{Q}{2} h_1 h_3, & \text{if } K \text{ is imaginary} \end{cases} \tag{1}$$

where $Q = [\mathcal{O}_K^\times : \mathcal{O}_{k_1}^\times \mathcal{O}_{k_2}^\times \mathcal{O}_{k_3}^\times]$ is the unit index of K over $\mathbb{Q}$ and $\mathcal{O}_L^\times$ is the unit group of the field L. Herglotz further noted that $Q = 1, 2,$ or 4 when K is real and $Q = 1$ or 2 when K is imaginary.

In this paper, we determine the exact value of Q for each of the four bicyclic biquadratic fields under consideration. We also give a summary of the values of e and the divisibility by powers of 2 of the class numbers of $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{2p})$, $\mathbb{Q}(\sqrt{-p})$, and $\mathbb{Q}(\sqrt{-2p})$. For our main result, we find the sufficient and necessary conditions for the class number H of $\mathbb{Q}(\sqrt{\pm p}, \sqrt{\pm 2})$ to be divisible by some power of 2, which is summarized in the tables below.

	$K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$, $k = \mathbb{Q}(\sqrt{2p})$	$K = \mathbb{Q}(\sqrt{-p}, \sqrt{-2})$
$p \equiv 3 \pmod 4$	H odd	H odd
$p \equiv 5 \pmod 8$	H odd	$2 \mid\mid H$
$p \equiv 1 \pmod{16}$	$\begin{cases} H \text{ odd}, & \text{if } \left(\frac{2}{p}\right)_4 = -1 \\ 2 \mid H, & \text{if } \left(\frac{2}{p}\right)_4 = 1, e_k = 1 \\ 4 \mid H, & \text{if } \left(\frac{2}{p}\right)_4 = 1, e_k = -1 \end{cases}$	$\begin{cases} 8 \mid\mid H, & \text{if } \left(\frac{2}{p}\right)_4 = -1 \\ 32 \mid H, & \text{if } \left(\frac{2}{p}\right)_4 = 1 \end{cases}$
$p \equiv 9 \pmod{16}$	$\begin{cases} H \text{ odd}, & \text{if } \left(\frac{2}{p}\right)_4 = 1 \\ 2 \mid H, & \text{if } \left(\frac{2}{p}\right)_4 = -1 \end{cases}$	$\begin{cases} 8 \mid\mid H, & \text{if } \left(\frac{2}{p}\right)_4 = 1 \\ 16 \mid H, & \text{if } \left(\frac{2}{p}\right)_4 = -1 \end{cases}$

Table 1: Divisibility by 2^n of H for $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$ and $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-2})$

	$K = \mathbb{Q}(\sqrt{p}, \sqrt{-2})$	$K = \mathbb{Q}(\sqrt{-p}, \sqrt{2})$
$p \equiv 3 \pmod 4$	$\begin{cases} 2 \mid\mid H, & \text{if } p \equiv 3 \pmod 8 \\ 4 \mid\mid H, & \text{if } p \equiv 7 \pmod{16} \\ 8 \mid H, & \text{if } p \equiv 15 \pmod{16} \end{cases}$	$\begin{cases} H \text{ odd}, & \text{if } p \equiv 3 \pmod 8 \\ 2 \mid\mid H, & \text{if } p \equiv 7 \pmod{16} \\ 4 \mid H, & \text{if } p \equiv 15 \pmod{16} \end{cases}$
$p \equiv 5 \pmod 8$	H odd	$2 \mid\mid H$
$p \equiv 1 \pmod{16}$	$\begin{cases} 2 \mid\mid H, & \text{if } \left(\frac{2}{p}\right)_4 = -1 \\ 4 \mid H, & \text{if } \left(\frac{2}{p}\right)_4 = 1 \end{cases}$	$\begin{cases} 8 \mid\mid H, & \text{if } \left(\frac{2}{p}\right)_4 = -1 \\ 32 \mid H, & \text{if } \left(\frac{2}{p}\right)_4 = 1 \end{cases}$
$p \equiv 9 \pmod{16}$	$\begin{cases} 2 \mid\mid H, & \text{if } \left(\frac{2}{p}\right)_4 = -1 \\ 4 \mid H, & \text{if } \left(\frac{2}{p}\right)_4 = 1 \end{cases}$	$16 \mid H$

Table 2: Divisibility by 2^n of H for $K = \mathbb{Q}(\sqrt{p}, \sqrt{-2})$ and $K = \mathbb{Q}(\sqrt{-p}, \sqrt{2})$

2 Divisibility of the class numbers of $\mathbb{Q}(\sqrt{\pm p})$ and $\mathbb{Q}(\sqrt{\pm 2p})$

Let m be a squarefree integer and k be the quadratic field $\mathbb{Q}(\sqrt{m})$ with discriminant d divisible by exactly two primes and with narrow class number h^+. The conditions for the divisibility of h^+ by 4 were obtained by Rédei and Reichardt [15] in 1934 using class field theory, while the divisibility of h^+ by 8 were obtained by Kaplan [9] in 1973 using properties of quadratic forms. Nemenzo [14] and Basilla [2] were able to verify these results using Ideal Theory and Legendre's theorem on the solvability of the Diophantine equation $ax^2 + by^2 = z^2$ [8].

In this section, we use Gauss genus theory together with the approach of Nemenzo and Basilla to determine the divisibility by powers of 2 of the class number h of the quadratic fields $\mathbb{Q}(\sqrt{\pm p})$ and $\mathbb{Q}(\sqrt{\pm 2p})$, as well as the values of the norm e of the fundamental unit ϵ of real quadratic fields $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{2p})$. Our first theorem is a well-known result from Gauss genus theory [6].

Theorem 1. *Let k be a quadratic number field whose discriminant is divisible by t distinct primes. Then the dimension of the 2-torsion of the narrow class group of k as an $\mathbb{F}_2$-vector space is $t - 1$.*

This implies that $2^{t-1} | h^+$ when $t > 1$ and that h and h^+ are odd when $t = 1$.

The following theorem is a summary of the results of Rédei and Reichardt [15] and Basilla [2] which are related to this paper.

Theorem 2. *Let $k = \mathbb{Q}(\sqrt{m})$ be a quadratic field with narrow class number h^+ and let p be an odd prime.*

1. *For $m = p$, $p \equiv 3 \pmod 4$: 4 does not divide h^+.*
2. *For $m = 2p$: $4 | h^+$ if and only if $p \equiv 1 \pmod 8$ and $8 | h^+$ if and only if $p \equiv 1 \pmod{16}$, $\left(\frac{2}{p}\right)_4 = 1$.*
3. *For $m = -p$, $p \equiv 1 \pmod 4$: $4 | h^+$ if and only if $p \equiv 1 \pmod 8$ and $8 | h^+$ if and only if $p \equiv 1 \pmod 8$, $\left(\frac{-4}{p}\right)_8 = 1$.*
4. *For $m = -2p$: $4 | h^+$ if and only if $p \equiv \pm 1 \pmod 8$ and $8 | h^+$ if and only if $p \equiv 15 \pmod{16}$, or if $p \equiv 1 \pmod 8$, $\left(\frac{2}{p}\right)_4 = 1$.*

The next theorem follows from the approach of Nemenzo [14] and Basilla [2] in their papers. This will be useful for determining e and the relation of h and h^+ in cases where Theorems 1 and 2 are not enough.

Theorem 3. *Let $k = \mathbb{Q}(\sqrt{m})$ be a quadratic field with integer ring $\mathcal{O}_k$, class number h, and narrow class number h^+. If the principal ideal $(\sqrt{m})$ is in the same narrow ideal class as $\mathcal{O}_k$, then $h^+ = h$. Otherwise, $h^+ = 2h$.*

The implication of these three theorems on the divisibility by powers of 2 of the class number h of the four quadratic fields $\mathbb{Q}(\sqrt{\pm p})$ and $\mathbb{Q}(\sqrt{\pm 2p})$ is summarized in Tables 3 and 4.

	$\mathbb{Q}(\sqrt{p})$	$\mathbb{Q}(\sqrt{2p})$
$p \equiv 3 \pmod 4$	h odd, $e = 1$	h odd, $e = 1$
$p \equiv 5 \pmod 8$	h odd, $e = -1$	$2\|\|h$, $e = -1$
$p \equiv 1 \pmod{16}$	h odd, $e = -1$	$\begin{cases} 2\|\|h, e=1 & \text{if } \left(\frac{2}{p}\right)_4 = -1, \\ 4\|h, & \text{if } \left(\frac{2}{p}\right)_4 = 1, e=1 \\ 8\|h, & \text{if } \left(\frac{2}{p}\right)_4 = 1, e=-1 \end{cases}$
$p \equiv 9 \pmod{16}$	h odd, $e = -1$	$\begin{cases} 2\|\|h, e=1 & \text{if } \left(\frac{2}{p}\right)_4 = 1 \\ 4\|\|h, e=-1 & \text{if } \left(\frac{2}{p}\right)_4 = -1 \end{cases}$

Table 3: Value of e and Divisibility by 2^n of h for $K = \mathbb{Q}(\sqrt{p})$ and $K = \mathbb{Q}(\sqrt{2p})$

	$\mathbb{Q}(\sqrt{-p})$	$\mathbb{Q}(\sqrt{-2p})$
$p \equiv 3 \pmod 4$	h odd	$\begin{cases} 2\|\|h, & \text{if } p \equiv 3 \pmod 8 \\ 4\|\|h, & \text{if } p \equiv 7 \pmod{16} \\ 8\|h, & \text{if } p \equiv 15 \pmod{16} \end{cases}$
$p \equiv 5 \pmod 8$	$2\|\|h$	$2\|\|h$
$p \equiv 1 \pmod 8$	$\begin{cases} 4\|\|h, & \text{if } \left(\frac{-4}{p}\right)_8 = -1 \\ 8\|h, & \text{if } \left(\frac{-4}{p}\right)_8 = 1 \end{cases}$	$\begin{cases} 4\|\|h, & \text{if } \left(\frac{2}{p}\right)_4 = -1 \\ 8\|h, & \text{if } \left(\frac{2}{p}\right)_4 = 1 \end{cases}$

Table 4: Divisibility by 2^n of h for $K = \mathbb{Q}(\sqrt{-p})$ and $K = \mathbb{Q}(\sqrt{-2p})$

To illustrate how tables 3 and 4 were constructed, consider the quadratic field $k = \mathbb{Q}(\sqrt{2p})$ where $p \equiv 1 \pmod{16}$. Note that the discriminant $d = 8p$ is divisible by 2 primes. Thus, $2|h^+$ by Theorem 1. For the case where $\left(\frac{2}{p}\right)_4 = -1$, we have $4||h^+$ by #2 of Theorem 2. Furthermore, it was shown in section 4 of the paper of Basilla [2] that $(\sqrt{2p})$ is not in the same narrow ideal class as $\mathcal{O}_k$. Hence, $h^+ = 2h$ by Theorem 3, and it follows that h is odd and $e = 1$. On the other hand, for the case where $\left(\frac{2}{p}\right)_4 = 1$, $8|h^+$ by #2 of Theorem 2. It follows from the relation of h and h^+ that $4|h$ if $e = 1$ while $8|h$ if $e = -1$. The other cases were done similarly.

Notice that our results in Tables 1 and 2, together with the information we summarized in Tables 3 and 4, subsumes the following theorem of Kucera [11].

Theorem 4. *Let p be a prime such that $p \equiv 1 \pmod 4$. Let h and h_1 be the class numbers* *of $k = \mathbb{Q}(\sqrt{p}, \sqrt{2})$ and $k_1 = \mathbb{Q}(\sqrt{2p})$, respectively, and let e be the norm of the fundamental unit of k_1.*

1. *If $p \equiv 5 \pmod 8$, then h is odd, $h_1 \equiv 2 \pmod 4$ and $e = -1$.*
2. *Let us suppose $p \equiv 1 \pmod 8$ and fix $v \in \mathbb{Z}$ such that $v^2 \equiv 2 \pmod p$. Then the following assertions hold true:*
   - *(a) if $\left(\frac{v}{p}\right) \neq (-1)^{\frac{p-1}{8}}$, then h is odd, $h_1 \equiv 2 \pmod 4$ and $e = 1$;*
   - *(b) if $\left(\frac{v}{p}\right) = -1$ and $p \equiv 9 \pmod{16}$, then h is even, $h_1 \equiv 4 \pmod 8$ and $e = -1$;*
   - *(c) if $\left(\frac{v}{p}\right) = 1$ and $p \equiv 1 \pmod{16}$, then h is even and $4|h_1$ (resp. $8|h_1$ whenever $e = -1$).*

Note also that there is a relation between $\left(\frac{-4}{p}\right)_8$ and $\left(\frac{2}{p}\right)_4$ appearing in the last row of Table 4.

Proposition 5. *Let p be a prime such that $p \equiv 1 \pmod 8$. Then*

$$\left(\frac{-4}{p}\right)_8 = \begin{cases} \left(\frac{2}{p}\right)_4, & \text{if } p \equiv 1 \pmod{16} \\ -\left(\frac{2}{p}\right)_4, & \text{if } p \equiv 9 \pmod{16}. \end{cases}$$

This is an implication of the following lemma.

Lemma 6. *Let p be a prime such that $p \equiv 1 \pmod 8$. Then*

$$\left(\frac{-1}{p}\right)_8 = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{16} \\ -1, & \text{if } p \equiv 9 \pmod{16}. \end{cases}$$

Proof. Recall that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

This shows that $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 4$. It follows that

$$\begin{aligned}
\left(\tfrac{-1}{p}\right)_4 = 1 &\iff a^4 \equiv -1 \pmod p \text{ for some integer } a \text{ with } p \nmid a \\
&\iff b^2 \equiv -1 \pmod p \text{ where } b \equiv a^2 \pmod p \text{ for some integers } a \text{ and } b \text{ with } p \nmid ab \\
&\iff \left(\tfrac{-1}{p}\right) = 1, \left(\tfrac{b}{p}\right) = 1 \text{ for some integer } b \text{ with } p \nmid b \text{ such that } b^2 \equiv -1 \pmod p \\
&\iff p \equiv 1 \pmod 4, 1 = \left(\tfrac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \equiv (b^2)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p-1}{4}} \pmod p \\
&\qquad \text{for some integer } b \text{ with } p \nmid b \text{ such that } b^2 \equiv -1 \pmod p \\
&\iff p \equiv 1 \pmod 8, \text{ since } (-1)^{\frac{p-1}{4}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \\ -1, & \text{if } p \equiv 5 \pmod 8. \end{cases}
\end{aligned}$$

This shows that

$$\left(\frac{-1}{p}\right)_4 = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \\ -1, & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

In a very similar manner, it can be shown that

$$\left(\frac{-1}{p}\right)_8 = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{16} \\ -1, & \text{if } p \equiv 9 \pmod{16}. \end{cases}$$

□

Proposition 5 follows from the fact that $\left(\frac{-4}{p}\right)_8 = \left(\frac{-1}{p}\right)_8 \left(\frac{4}{p}\right)_8 = \left(\frac{-1}{p}\right)_8 \left(\frac{2}{p}\right)_4$ and Lemma 6.

In the following three sections, we present a mechanism for determining the value of Q. The bulk of this work was already compiled by Damasco [5].

3 On the integral multiples of the fundamental unit as squares of integers of real quadratic fields

Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic field, for some squarefree integer $m > 0$, and let x and y be integers such that

$$\epsilon = \begin{cases} \frac{1}{2}(x + y\sqrt{m}), x \equiv y \pmod 2, & \text{if } m \equiv 1 \pmod 4 \\ x + y\sqrt{m}, & \text{if } m \equiv 2, 3 \pmod 4 \end{cases}$$

is the fundamental unit of k with norm e. Damasco [5] showed that there exists a squarefree integer $r \notin \{1, m\}$ such that $\sqrt{r\epsilon} \in \mathcal{O}_k$ if and only if $e = 1$. Moreover, Barrucand and Cohn [1, 4] showed that there are exactly two such integers and they are described in the following theorem.

Theorem 7. *Let r_1 and r_2 be distinct squarefree integers such that $\sqrt{r_i \epsilon} \in \mathcal{O}_k$ for $i = 1, 2$.*

1. *If $m \equiv 3 \pmod 4$ and y is odd, then r_i is even and $\frac{r_i}{2} | m$ for $i = 1, 2$ and $r_1 r_2 = 4m$.*
2. *Otherwise, $r_i | m$ for $i = 1, 2$ and $r_1 r_2 = m$.*

4 Determining Q for real bicyclic biquadratic fields

Let K be a real bicyclic biquadratic field and let ϵ_i be the fundamental unit of its quadratic subfields k_i with norm $e_i (i = 1, 2, 3)$. Hence, $Q = 1, 2$, or 4. According to the following theorem of Kuroda [12, 16, 5], we can determine the value of Q by determining the generators for $\mathcal{O}_K^\times$ modulo $\{\pm 1\}$.

Theorem 8. *Up to some permutation of indices, the generators for $\mathcal{O}_K^\times$ modulo $\{\pm 1\}$ is one of the following:*

(a) $\epsilon_1, \epsilon_2, \epsilon_3$

(b) $\epsilon_1, \epsilon_2, \sqrt{\epsilon_3}$

(c) $\epsilon_1, \epsilon_2, \sqrt{\epsilon_1 \epsilon_3}$

(d) $\epsilon_1, \epsilon_2, \sqrt{\epsilon_1 \epsilon_2 \epsilon_3}$

(e) $\epsilon_1, \sqrt{\epsilon_2}, \sqrt{\epsilon_3}$

(f) $\epsilon_1, \sqrt{\epsilon_2}, \sqrt{\epsilon_1 \epsilon_3}$

(g) $\epsilon_1, \sqrt{\epsilon_1 \epsilon_2}, \sqrt{\epsilon_1 \epsilon_3}$

The corresponding values of Q are as follows: $Q = 1$ for case (a), $Q = 2$ for cases (b) to (d), and $Q = 4$ for cases (e) to (g).

Furthermore, we can use the contrapositives of the statements in the following lemma of Kuroda [5, 12, 16] to eliminate some of the possible generators for $\mathcal{O}_K^\times$ modulo $\{\pm 1\}$ listed in Theorem 8.

Lemma 9. *Let $i, j \in \{1, 2, 3\}, i \neq j$.*

1. *If $\sqrt{\epsilon_i} \in K$, then $e_i = 1$.*
2. *If $\sqrt{\epsilon_i \epsilon_j} \in K$, then $e_i = e_j = 1$.*
3. *If $\sqrt{\epsilon_1 \epsilon_2 \epsilon_3} \in K$, then $e_1 = e_2 = e_3 = \pm 1$.*

Moreover, we will use the following lemma of Sime [16] when $e_i = -1$ for each i.

Lemma 10. *Let $k_i = \mathbb{Q}(\sqrt{m_i})$ be the quadratic subfields of the real biquadratic field K with $e_i = -1$ for each $i \in \{1, 2, 3\}$. Then there exists a squarefree integer r dividing $\sqrt{m_1 m_2 m_3}$ such that $\sqrt{r \epsilon_1 \epsilon_2 \epsilon_3} \in K$.*

We now determine the value of Q for the real bicyclic biquadratic field $\mathbb{Q}(\sqrt{p}, \sqrt{2})$.

Proposition 11. *Let $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$. Then*

$$Q = \begin{cases} 2, & \text{if } p \equiv 1 \pmod 4 \\ \\ 4, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. The quadratic subfields of K are $k_1 = \mathbb{Q}(\sqrt{p})$, $k_2 = \mathbb{Q}(\sqrt{2})$, and $k_3 = \mathbb{Q}(\sqrt{2p})$. Moreover, since K is real, then $H = \frac{Q}{4} h_1 h_3$ by Equation (1), where $Q \in \{1, 2, 4\}$. Let us first consider $p \equiv 3 \pmod 4$. Since h_1 and h_3 are odd, it follows that $Q = 4$ and H is odd.

Now, if $p \equiv 1 \pmod 4$, we have $e_1 = e_2 = -1$. It follows from Lemma 9 that $\sqrt{\epsilon_1}$, $\sqrt{\epsilon_2}$, $\sqrt{\epsilon_1\epsilon_2}$, $\sqrt{\epsilon_1\epsilon_3}$, $\sqrt{\epsilon_2\epsilon_3} \notin K$. Hence, we are left with cases (a), (b) and (d) in Theorem 8 as possible generators for $\mathcal{O}_K^\times$ modulo $\{\pm 1\}$. We now show that $Q = 2$ whether $e_3 = 1$ or $e_3 = -1$. First, let us suppose $e_3 = 1$. If r is a squarefree integer such that $\sqrt{r\epsilon_3} \in \mathcal{O}_{k_3}$, then $r | 2p$ and $r \notin \{1, 2p\}$ by Theorem 7. It follows that $r \in \{2, p\}$. In any case, $\sqrt{r} \in K$. Thus, $\sqrt{\epsilon_3} \in K$. Hence, $\epsilon_1, \epsilon_2, \sqrt{\epsilon_3}$ are the generators for $\mathcal{O}_K^\times$ modulo $\{\pm 1\}$ and $Q = 2$. On the other hand, suppose $e_3 = -1$. By Lemma 10, if r is a squarefree integer such that $\sqrt{r\epsilon_1\epsilon_2\epsilon_3} \in K$, then $r | 2p$. It follows that $r \in \{1, 2, p, 2p\}$. In any case, $\sqrt{r} \in K$. Thus, $\sqrt{\epsilon_1\epsilon_2\epsilon_3} \in K$. Hence, $\epsilon_1, \epsilon_2, \sqrt{\epsilon_1\epsilon_2\epsilon_3}$ are the generators for $\mathcal{O}_K^\times$ modulo $\{\pm 1\}$ and $Q = 2$. □

5 Determining Q for imaginary bicyclic biquadratic fields

Let K be an imaginary bicyclic biquadratic field with real quadratic subfield k. Hence, $Q = 1$ or 2. Let ϵ be the fundamental unit of k with norm e. When $e = -1$, the value of Q is determined by the following remark by Brown and Parry [3].

Theorem 12. *If $e = -1$ and $K \neq \mathbb{Q}(\sqrt{-1}, \sqrt{-2})$, then $Q = 1$.*

But when $e = 1$, we use the following result of Kuroda and Kubota [4, 10, 12] to determine Q.

Theorem 13. *Suppose $e = 1$.*

(a) If $\sqrt{-1}$ or $\sqrt{-2}$ is in K, then $Q = 1$ if and only if $\sqrt{2\epsilon} \notin \mathcal{O}_k$.

(b) If $\sqrt{-3}$ is in K and $K \neq \mathbb{Q}(\sqrt{-1}, \sqrt{-3})$, then $Q = 1$ if and only if $\sqrt{3\epsilon} \notin \mathcal{O}_k$.

(c) If none of $\sqrt{-1}, \sqrt{-2}, \sqrt{-3}$ is in K and $\sqrt{-n} \in K$ for some positive squarefree integer n, then $Q = 1$ if and only if $\sqrt{n\epsilon} \notin \mathcal{O}_k$.

In the propositions that will follow, p denotes an odd prime. We now apply the criteria above together with Theorem 7 and Table 3 to determine the value of Q for the imaginary bicyclic biquadratic fields $\mathbb{Q}(\sqrt{-p}, \sqrt{2})$, $\mathbb{Q}(\sqrt{p}, \sqrt{-2})$ and $\mathbb{Q}(\sqrt{-p}, \sqrt{-2})$.

Proposition 14. *Let* $K = \mathbb{Q}(\sqrt{-p}, \sqrt{2})$*. Then* $Q = 1$*.*

Proof. Here, $k = \mathbb{Q}(\sqrt{2})$ with $\epsilon = 1 + \sqrt{2}$. Since $e = -1$, then $Q = 1$ by Theorem 12. □

Proposition 15. *Let* $K = \mathbb{Q}(\sqrt{p}, \sqrt{-2})$*. Then*

$$Q = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ 2, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Here, $k = \mathbb{Q}(\sqrt{p})$. If $p \equiv 1 \pmod 4$, then $e = -1$ by Table 3, and so $Q = 1$ by Theorem 12. On the other hand, if $p \equiv 3 \pmod 4$, then $e = 1$. Since $\sqrt{-2} \in K$, then by Theorem 13(a), $Q = 1$ if and only if $\sqrt{2\epsilon} \notin \mathcal{O}_k$. By Theorem 7, if r is a squarefree integer such that $\sqrt{r\epsilon} \in \mathcal{O}_k$, then $\frac{r}{2} | p$. Since $r \notin \{1, m\}$ and $m = p$ here, then $r \in \{2, 2p\}$. Thus, $\sqrt{2\epsilon}, \sqrt{2p\epsilon} \in \mathcal{O}_k$ and, hence, $Q \neq 1$. □

Proposition 16. *Let* $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-2})$ *and let* ϵ *be the fundamental unit of* $k = \mathbb{Q}(\sqrt{2p})$ *with norm* e*. Then*

$$Q = \begin{cases} 1, & \text{if } e = -1 \\ 2, & \text{if } e = 1. \end{cases}$$

Proof. From Table 3, it can be seen that e may be 1 or -1 for $k = \mathbb{Q}(\sqrt{2p})$. If $e = -1$, then $Q = 1$ by Theorem 12. But if $e = 1$, since $\sqrt{-2} \in K$, it follows from Theorem 13(a) that $Q = 1$ if and only if $\sqrt{2\epsilon} \notin \mathcal{O}_k$. However, by Theorem 7, if r is a squarefree integer such that $\sqrt{r\epsilon} \in \mathcal{O}_k$, then $r | 2p$. Since $r \notin \{1, m\}$ and $m = 2p$ here, then $r \in \{2, p\}$. Thus, $\sqrt{2\epsilon}, \sqrt{p\epsilon} \in \mathcal{O}_k$ and, hence, $Q \neq 1$. □

6 Main Results

We now give the sufficient and necessary conditions for the class number H of the bicyclic biquadratic field $K = \mathbb{Q}(\sqrt{\pm p}, \sqrt{\pm 2})$, p an odd prime, to be divisible by a power of 2. In the propositions that will follow, for $i \in \{1, 2, 3\}$, we denote by e_i the norm of the fundamental unit ϵ_i of the real quadratic subfield k_i of K and by h_i the class number of k_i.

Proposition 17. *Let* $K = \mathbb{Q}(\sqrt{p}, \sqrt{2})$ *with quadratic subfields* $k_1 = \mathbb{Q}(\sqrt{p})$*,* $k_2 = \mathbb{Q}(\sqrt{2})$ *and* $k_3 = \mathbb{Q}(\sqrt{2p})$*.Then 2 divides* H *if and only if* $p \equiv 1 \pmod 8$ *and* $\left(\frac{2}{p}\right)_4 = (-1)^{\frac{p-1}{8}}$*. Equivalently, 2 divides* H *if and only if either*

(i) $p \equiv 1 \pmod{16}$ *and* $\left(\frac{2}{p}\right)_4 = 1$*, or*

(ii) $p \equiv 9 \pmod{16}$ *and* $\left(\frac{2}{p}\right)_4 = -1$*.*

Moreover, if $p \equiv 1 \pmod{16}$, $\left(\frac{2}{p}\right)_4 = 1$ *and* $e_3 = -1$*, then 4 divides* H*.*

Proof. If $p \equiv 3 \pmod 4$, then H is odd (see proof of Proposition 11). For $p \equiv 1 \pmod 4$, we have $H = \frac{1}{2}h_1h_3$ by equation (1) and Proposition 11, and we know that h_1 is odd by Table 3. By knowing the divisibility of h_3 by some power of 2, we will be able to know that of H.

Let us consider two subcases for $p \equiv 1 \pmod 4$: $p \equiv 5 \pmod 8$ and $p \equiv 1 \pmod 8$. If $p \equiv 5 \pmod 8$, then $2||h_3$ by Table 3; thus, H is odd. On the other hand, if $p \equiv 1 \pmod 8$, it follows from Table 3 that $4|h_3$ (hence $2|H$) if and only if either $p \equiv 1 \pmod{16}$, $\left(\frac{2}{p}\right)_4 = 1$ or $p \equiv 9 \pmod{16}$, $\left(\frac{2}{p}\right)_4 = -1$. Moreover, if $p \equiv 1 \pmod{16}$, $\left(\frac{2}{p}\right)_4 = 1$ and $e_3 = -1$, then $8|h_3$ (hence $4|H$). □

Proposition 18. *Let* $K = \mathbb{Q}(\sqrt{-p}, \sqrt{2})$*. Then*

- *(a) 2 divides* H *if and only if either* $p \equiv 1 \pmod 4$ *or* $p \equiv 7 \pmod 8$*,*
- *(b) 4 divides* H *if and only if either* $p \equiv 1 \pmod 8$ *or* $p \equiv 15 \pmod{16}$*.*

Moreover,

- *(c) 8 divides* H *if* $p \equiv 1 \pmod 8$*; in addition, if* $p \equiv 1 \pmod{16}$ *and* $\left(\frac{2}{p}\right)_4 = -1$*, then 16 does not divide* H*,*
- *(d) 16 divides* H *if* $p \equiv 9 \pmod{16}$*,*
- *(e) 32 divides* H *if* $p \equiv 1 \pmod{16}$ *and* $\left(\frac{2}{p}\right)_4 = 1$*.*

Proof. Let $k_1 = \mathbb{Q}(\sqrt{-p})$, $k_2 = \mathbb{Q}(\sqrt{2})$ and $k_3 = \mathbb{Q}(\sqrt{-2p})$. By equation (1) and Proposition 14, we have $H = \frac{1}{2}h_1h_3$. If $p \equiv 3 \pmod 4$, h_1 is odd by Table 4. Also by Table 4, $4|h_3$ (hence $2|H$) if and only if $p \equiv 7 \pmod 8$ and $8|h_3$ (hence $4|H$) if and only if $p \equiv 15 \pmod{16}$.

On the other hand, for $p \equiv 1 \pmod 4$, $2|h_1$ and $2|h_3$ (hence $2|H$) by Table 4. Moreover, $4|h_1$ and $4|h_3$ (hence $8|H$) if and only if $p \equiv 1 \pmod 8$. Furthermore, for $p \equiv 1 \pmod 8$, $8|h_1$ if and only if $\left(\frac{-4}{p}\right)_8 = 1$ and $8|h_3$ if and only if $\left(\frac{2}{p}\right)_4 = 1$. By the relation between $\left(\frac{-4}{p}\right)_8$ and $\left(\frac{2}{p}\right)_4$ in Proposition 5, it can be deduced that $16|H$ if $p \equiv 9 \pmod{16}$, while for $p \equiv 1 \pmod{16}$, we have $8||H$ if $\left(\frac{2}{p}\right)_4 = -1$ but $32|H$ if $\left(\frac{2}{p}\right)_4 = 1$. □

Proposition 19. *Let* $K = \mathbb{Q}(\sqrt{p}, \sqrt{-2})$*. Then*

- *(a) 2 divides* H *if and only if either* $p \equiv 1 \pmod 8$ *or* $p \equiv 3 \pmod 4$*,*
- *(b) 4 divides* H *if and only if either*

(i) $p \equiv 7 \pmod 8$*, or*

(ii) $p \equiv 1 \pmod 8$ *and* $\left(\frac{2}{p}\right)_4 = 1$.

Moreover, if $p \equiv 7 \pmod 8$*, then 8 divides* H *if and only if* $p \equiv 15 \pmod{16}$.

Proof. Let $k_1 = \mathbb{Q}(\sqrt{p})$, $k_2 = \mathbb{Q}(\sqrt{-2})$ and $k_3 = \mathbb{Q}(\sqrt{-2p})$. By equation (1) and Proposition 15, we have

$$H = \begin{cases} \frac{1}{2}h_1h_3, & \text{if } p \equiv 1 \pmod 4 \\ h_1h_3, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Note also that h_1 is odd by Table 3. Thus, we are left to find the divisibility of h_3 by some power of 2 in order to find that of H and we do that by using Table 4.

For $p \equiv 3 \pmod 4$, we have $2|h_3$ (hence $2|H$). Moreover, $4|h_3$ (hence $4|H$) if and only if $p \equiv 7 \pmod 8$, and $8|h_3$ (hence $8|H$) if and only if $p \equiv 15 \pmod{16}$. On the other hand, for $p \equiv 1 \pmod 4$, $4|h_3$ (hence $2|H$) if and only if $p \equiv 1 \pmod 8$, and $8|h_3$ (hence $4|H$) if and only if $p \equiv 1 \pmod 8$ and $\left(\frac{2}{p}\right)_4 = 1$. □

Proposition 20. *Let* $K = \mathbb{Q}(\sqrt{-p}, \sqrt{-2})$*. Then*

(a) 2 divides H *if and only if* $p \equiv 1 \pmod 4$*; in addition, if* $p \equiv 5 \pmod 8$*, then 4 does not divide* H*,*

(b) 8 divides H *if and only if* $p \equiv 1 \pmod 8$*,*

(c) 16 divides H *if and only if* $p \equiv 1 \pmod 8$ *and* $\left(\frac{-4}{p}\right)_8 = 1$.

Moreover, if $p \equiv 1 \pmod{16}$ *and* $\left(\frac{-4}{p}\right)_8 = 1$*, then 32 divides* H.

Proof. Let $k_1 = \mathbb{Q}(\sqrt{-p})$, $k_2 = \mathbb{Q}(\sqrt{-2})$ and $k_3 = \mathbb{Q}(\sqrt{2p})$. By equation (1) and Proposition 16, we have

$$H = \begin{cases} \frac{1}{2}h_1h_3, & \text{if } e_3 = -1 \\ h_1h_3, & \text{if } e_3 = 1. \end{cases}$$

We now use Tables 3 and 4 to find the values of e_3, h_1 and h_3 for each type of primes being considered. First, let us consider $p \equiv 3 \pmod 4$. Here, $e_3 = 1$ and both h_1 and h_3 are odd. Hence, H is odd. Next, let us consider $p \equiv 5 \pmod 8$. Here, $e_3 = -1$, $2||h_1$ and $2||h_3$, and hence $2||H$.

Lastly, consider $p \equiv 1 \pmod 8$. Here, $4||h_1$ if $\left(\frac{-4}{p}\right)_8 = -1$ but $8|h_1$ if $\left(\frac{-4}{p}\right)_8 = 1$. Let us consider its two subcases: $p \equiv 1 \pmod{16}$ and $p \equiv 9 \pmod{16}$. For $p \equiv 1 \pmod{16}$, we have $\left(\frac{-4}{p}\right)_8 = \left(\frac{2}{p}\right)_4$ by Proposition 5. If $\left(\frac{2}{p}\right)_4 = -1$, then $e_3 = 1$, $4||h_1$, $2||h_3$ (hence $8||H$). On the other hand, if $\left(\frac{2}{p}\right)_4 = 1$, then e_3 may be equal to 1 or -1. If $e_3 = 1$, then $8|h_1$, $4|h_3$ (hence $32|H$); while if $e_3 = -1$, then $8|h_1$, $8|h_3$ (hence $32|H$). Now, for the second subcase $p \equiv 9 \pmod{16}$, we have $\left(\frac{-4}{p}\right)_8 = -\left(\frac{2}{p}\right)_4$ by Proposition 5. If $\left(\frac{2}{p}\right)_4 = 1$, then $e_3 = 1$, $4||h_1$, $2||h_3$ (hence $8||H$). On the other hand, if $\left(\frac{2}{p}\right)_4 = -1$, then $e_3 = -1$, $8|h_1$, $4||h_3$ (hence $16|H$). □

7 Acknowledgment

This work was supported by the Institute of Mathematics Computational Research Laboratory Research Grant and part of the second named author's dissertation being completed under the DOST-SEI ASTHRDP scholarship.

References

[1] P. Barrucand, H. Cohn, A rational genus, class number divisibility and unit theory for pure cubic fields, *J. Number Theory* **2** (1970), 7-21.

[2] J.M. Basilla, The quadratic fields with discriminant divisible by exactly two primes and with "narrow" class number divisible by 8, *Proc. Japan Acad.* **80A**(2004), 187-190.

[3] E. Brown, C. J. Parry, The imaginary bicyclic biquadratic fields with class-number 1, *J. Reine Angew. Math.* **266** (1974), 118-120.

[4] D.A. Buell, H.C. Williams, K.S. Williams, On the Imaginary Bicyclic Biquadratic Fields with Class-Number 2. *Mathematics of Computation.* **31** (1977), 1034-1042.

[5] J.R.C.G. Damasco, On Class Numbers of Bicyclic Biquadratic Fields, Master's Thesis, University of the Philippines – Diliman, 2012.

[6] C.F. Gauss, *Disquisitiones Arithmeticae.* Gerhard Fleischer, Leipzig, 1801.

[7] G. Herglotz: Uber einen Dirichletschen Satz. *Math.Zeitschrift.* **12** (1922), 255-261.

[8] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory, second ed., Graduate Texts in Mathematics 84.* Springer-Verlag, New York(1990), 272-275.

[9] P. Kaplan, Divisibilité par 8 du nombr des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique, *J. Math. Soc. Japan,* **25** (4) (1973), 596-608.

[10] T. Kubota, Uber die Beziehung der Klassenzahlen der Unterkorper des bizyklischen biquadratischen Zahlkorpers. *Nagoya Math. J.* **6** (1953), 119-127.

[11] R. Kucera, On the Parity of the Class Number of a Biquadratic Field. *Journal of Number Theory*, **52** (1995), 43-52.

[12] S. Kuroda, Uber den Dirichletschen Korper. *J. Fac. Sci. Imp. Univ. Tokyo Sect. I* **4** (1943), 383-406.

[13] F. Lemmermeyer, Kuroda's class number formula. *Acta Arith.*, LXVI. **3** (1994), 245-260.

[14] F.R. Nemenzo, On a Theorem of Scholz on the class number of quadratic fields. *Proc Japan Acad,* **80A**(2004), 9-11.

[15] L. Rédei, H. Reichardt, Die Anzahl der durch 4 teilbaren invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers. *J. reine angew. Math.*, **170**(1934), 69-74.

[16] P.J. Sime, On the ideal class group of real biquadratic fields, *Transactions of the American Mathematical Society*, **347** (1995), 4855-4876.

This page is intentionally left blank