REMARK ON THE CLASS NUMBER
OF $Q(\sqrt{2p})$ MODULO 8 FOR $p \equiv 5 \pmod{8}$ A PRIME

KENNETH S. WILLIAMS AND CHRISTIAN FRIESEN

Abstract. An explicit congruence modulo 8 is given for the class number of the real quadratic field $Q(\sqrt{2p})$, where $p$ is a prime congruent to 5 modulo 8.

Let $Q$ denote the rational number field. Let $Q(\sqrt{d})$ denote the quadratic extension of $Q$ having discriminant $d$. The class number of $Q(\sqrt{d})$ is denoted by $h(d)$. If $d > 0$ the fundamental unit ($> 1$) of $Q(\sqrt{d})$ is denoted by $\epsilon_d$.

If $d = p$, where $p \equiv 5 \pmod{8}$ is a prime, it is a classical result of Gauss that $h(p) \equiv 1 \pmod{2}$ (see for example [4, §3]) and the author [10, Theorem 1] has given an explicit congruence for $h(p)$ modulo 4, namely;

\begin{equation}
\begin{aligned}
\left( 1 \right) \quad h(p) &= \begin{cases} 
\frac{1}{2}(-2t + u + b + 1) \pmod{4}, & \text{if } t = u \equiv 1 \pmod{2}, \\
\frac{1}{2}(t + u + 2b + 2) \pmod{4}, & \text{if } t = u \equiv 0 \pmod{2},
\end{cases}
\end{aligned}
\end{equation}

where

\begin{equation}
\epsilon_p = \frac{1}{2}(t + u\sqrt{p}),
\end{equation}

and $a$ and $b$ are integers given uniquely by

\begin{equation}
p = a^2 + b^2, \quad a \equiv 1 \pmod{4}, \quad b \equiv (\frac{1}{2}(p - 1))!a \pmod{p}.
\end{equation}

In this short note we obtain the corresponding congruence to (1) for $d = 8p$, where $p \equiv 5 \pmod{8}$ is prime. In this case $h(8p) \equiv 2 \pmod{4}$ (see for example [4, Theorem 1(b)]) and we prove

**Theorem.** For $p \equiv 5 \pmod{8}$ a prime we have

\begin{equation}
\begin{aligned}
\left( 4 \right) \quad h(8p) &= 2T + b + 2 \pmod{8},
\end{aligned}
\end{equation}

where $\epsilon_{8p} = T + U\sqrt{2p}$ is the fundamental unit of $Q(\sqrt{2p})$ (of discriminant $8p$) and $b$ is given by (3).

**Proof.** Our starting point is the following congruence given by Gauss [6] in 1828:

\begin{equation}
\begin{aligned}
\left( 5 \right) \quad h(-4p) &\equiv -a + b + 1 \pmod{8}.
\end{aligned}
\end{equation}
A proof by Dedekind is given in Volume 2 of the 1876 edition of Gauss's collected works. In recent years the congruence (5) has been reproved by Barkan [1, Corollary 2, p. 828 (with a misprint corrected)] and Williams and Currie [12, pp. 971–972]. Next we set

\[ S_i = \sum_{x/p = i} \left( \frac{x}{p} \right), \quad i = 0, 1, 2, 3. \]

Dirichlet [5, p. 152] proved in 1840 that

\[ h(-8p) = 2(S_0 - S_3), \]

and Holden [8, p. 130] proved in 1907 that

\[ h(-4p) = -2(S_0 + S_3). \]

Adding (7) and (8) we obtain

\[ h(-4p) + h(-8p) = -4S_3 = 4S_3 \pmod{8} \]

\[ = 4 \sum_{x=(3p+1)/8}^1 1 \pmod{8} \]

\[ = 4 \left( \frac{p + 3}{8} \right) \pmod{8}, \]

that is

\[ h(-4p) + h(-8p) = \frac{1}{2}(p + 3) \pmod{8}. \]

The congruence (9) has been rediscovered many times (see for example [3, p. 282]; [7, p. 188]; [9, p. 188]). Appealing to (3), we have, as \( b = 2 \pmod{4} \),

\[ \frac{1}{2}(p + 3) = a + 3 \pmod{8}. \]

Putting (5), (9) and (10) together we obtain

\[ h(-8p) = 2a - b + 2 = b \pmod{8}. \]

The congruence (11) has been given by Barkan [1, Corollary 1, p. 828]. The required congruence (4) now follows from (11) and the congruence

\[ h(-8p) = h(8p) + 2T + 2 \pmod{8}, \]

which has been established independently by Barkan [2, Lemma 2] and Williams [11, Theorem p. 19].

**Example.** \( p = 2861 \). In this case we have \( a = -19 \), and \( b = -50 \), as \( ((p - 1)/2)! = 1659 \pmod{2861} \). Also \( \varepsilon_{22888} = 15507 + 205\sqrt{5722} \), so \( T = 15507, U = 205 \), and the theorem gives \( h(22888) = 2 \cdot 15507 - 50 = 2 \equiv -2 \pmod{8} \). Indeed \( h(22888) = 6 \).

It appears very unlikely that there is a similar result to (4) for primes \( p = 1 \pmod{8} \) since for the primes 1097 (\( \equiv 9 \pmod{16} \)) and 1481 (\( \equiv 9 \pmod{16} \)) we have

\[ T = 1 \pmod{16}, \quad U = 4 \pmod{16}, \quad a = 13 \pmod{16}, \quad b = 0 \pmod{16}, \]

yet

\[ h(8 \cdot 1097) = 2 \pmod{8}, \quad h(8 \cdot 1481) = 6 \pmod{8}. \]
REFERENCES

7. J. W. L. Glaisher, On the expressions for the number of classes of a negative determinant, and on the numbers of positives in the octants of $P$, Quart. J. Math. 34 (1903), 178–204.
8. H. Holden, On various expressions for $h$, the number of properly primitive classes for a negative determinant not containing a square factor (fifth paper), Messenger Math. 36 (1907), 126–134.
10. Kenneth S. Williams, The class number of $\mathbb{Q}(\sqrt{p})$ modulo 4, for $p \equiv 5 \pmod{8}$ a prime, Pacific J. Math. 92 (1981), 241–248.
11. _____, The class number of $\mathbb{Q}(\sqrt{-2p})$ modulo 8, for $p \equiv 5 \pmod{8}$ a prime, Rocky Mountain J. Math. 11 (1981), 19–26.

DEPARTMENT OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA K1S 5B6

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use