<table>
<thead>
<tr>
<th>Title</th>
<th>On the strict class number of $\mathbb{Q}(\sqrt{2p})$ modulo 16, $p \equiv 1 \pmod{8}$ prime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Kaplan, Pierre; Williams, Kenneth S.</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Journal of Mathematics. 21(1) P.23-P.29</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1984</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/11094/9288">http://hdl.handle.net/11094/9288</a></td>
</tr>
<tr>
<td>DOI</td>
<td></td>
</tr>
<tr>
<td>Rights</td>
<td></td>
</tr>
</tbody>
</table>
ON THE STRICT CLASS NUMBER OF $\mathbb{Q}(\sqrt{2p})$ 
MODULO 16, $p \equiv 1 \pmod{8}$ PRIME

Pierre Kaplan and Kenneth S. Williams

(Received August 6, 1982)

Let $p \equiv 1 \pmod{8}$ be prime so that there are integers $a, b, c, d, e, f$ with

$$
\begin{align*}
1 & \quad \left\{ \begin{array}{l}
p = a^2 + b^2 = c^2 + 2d^2 = e^2 - 2f^2 \\
a \equiv 1 \pmod{4}, \\b \equiv 0 \pmod{4}, \\c \equiv 1 \pmod{4}, \\d \equiv 0 \pmod{2}, \\
e \equiv 1 \pmod{4}, \\f \equiv 0 \pmod{4}.
\end{array} \right.
\end{align*}
$$

Throughout this note we consider only those primes $p$ for which the strict class number $h^+(8p)$ of the real quadratic field $\mathbb{Q}(\sqrt{2p})$ (of discriminant $8p$) satisfies

$$
(2) \quad h^+(8p) \equiv 0 \pmod{8}.
$$

These primes have been characterized by Kaplan [4]. Indeed such primes must satisfy [5]

$$
(3) \quad \left\{ \begin{array}{l}
p \equiv 1 \pmod{16}, \\a \equiv 1 \pmod{8}, \\b \equiv 0 \pmod{8}, \\c \equiv 1 \pmod{8}, \\
\left( \frac{c}{p} \right) = 1, \\
d \equiv 0 \pmod{4}, \\e \equiv 1 \pmod{8}, \\
\left( \frac{e}{p} \right) = +1.
\end{array} \right.
$$

In this note we give a new determination of $h^+(8p)$ modulo 16, and compare it with the determination given by Yamamoto in [15].

We begin by introducing some notation. We denote the fundamental unit ($>1$) of $\mathbb{Q}(\sqrt{2p})$ by $\eta_{2p}$. As one and only one of the equations $V^2 - 2pW^2 = -1, -2,$ or $+2$ is solvable in integers $V, W$, we define

$$
E_p = \begin{cases} 
-1, & \text{if } V^2 - 2pW^2 = -1 \text{ solvable,} \\
-2, & \text{if } V^2 - 2pW^2 = -2 \text{ solvable,} \\
+2, & \text{if } V^2 - 2pW^2 = +2 \text{ solvable.}
\end{cases}
$$

Clearly the norm $N(\eta_{2p})$ of $\eta_{2p}$ satisfies

$$
N(\eta_{2p}) = \begin{cases} 
+1, & \text{if } E_p = \pm 2, \\
-1, & \text{if } E_p = -1.
\end{cases}
$$
Further we let
\[ \epsilon_2 = 1 + \sqrt{2}, \quad \epsilon_p = T + U\sqrt{p} \]
denote the fundamental units (>1) of \( \mathbb{Q}(\sqrt{2}) \) and \( \mathbb{Q}(\sqrt{p}) \) respectively, and set
\begin{align*}
(4) \quad & e_2 = -\sqrt{2}, \quad e'_2 = -\sqrt{2} (1 - \sqrt{2}) = 2 - \sqrt{2}, \\
(5) \quad & e_p = -\sqrt{p}, \quad e'_p = -\sqrt{p} (T - U\sqrt{p}) = pU - T\sqrt{p}.
\end{align*}
Finally the fundamental unit of \( \mathbb{Q}(\sqrt{2p}) \) of norm +1 is denoted by \( R + S\sqrt{2p} \) so that
\[ R + S\sqrt{2p} = \begin{cases} 
\eta_{2p}, & \text{if } N(\eta_{2p}) = +1, \\
\eta_p^2, & \text{if } N(\eta_{2p}) = -1.
\end{cases} \]

Our starting point is the following result of Bucher [1: p. 8].

**Lemma 1.** If \( p \equiv 1 \pmod{8} \) is a prime such that \( h^+(8p) \equiv 0 \pmod{8} \) then
\begin{align*}
(6) \quad & (-1)^{\lambda(p)} \left( \frac{e_2}{p} \right)_4 \equiv R^{h+(8p)/8} \pmod{p}, \\
(7) \quad & (-1)^{\lambda(p)} \left( \frac{e_p}{2} \right)_4 \equiv R^{h+(8p)/8} \pmod{4},
\end{align*}
where
\[ \lambda(p) = \text{number of quadratic residues of } p \text{ less than } p/8. \]
[In the biquadratic residue symbols \( e_2 \) and \( e_p \) are to be taken modulo \( p \) and 16 respectively.]

It is convenient to set
\[ \alpha = (-1)^{\lambda(p)} \left( \frac{e_2}{2} \right)_4, \quad \beta = (-1)^{\lambda(p)} \left( \frac{e_p}{p} \right)_4. \]

As (see for example [1: p. 4] or [8])
\begin{align*}
E_p = -1 & \Rightarrow R \equiv -1 \pmod{p}, \quad R \equiv -1 \pmod{4}, \\
E_p = -2 & \Rightarrow R \equiv -1 \pmod{p}, \quad R \equiv 1 \pmod{4}, \\
E_p = +2 & \Rightarrow R \equiv 1 \pmod{p}, \quad R \equiv -1 \pmod{4},
\end{align*}
we note that Lemma 1 together with (10) gives immediately the following supplement to the biquadratic reciprocity law of Scholz type proved in [2].

**Corollary 1.** If \( p \equiv 1 \pmod{8} \) is a prime such that \( h^+(8p) \equiv 0 \pmod{8} \) then
\[ \left( \frac{e_2}{p} \right)_4 \left( \frac{e_p}{2} \right)_4 = \begin{cases} 
+1, & \text{if } N(\eta_{2p}) = -1, \\
(-1)^{h+(8p)/8}, & \text{if } N(\eta_{2p}) = +1.
\end{cases} \]
Next we examine each of the three quantities $\lambda(p)$, $\left(\frac{e_2}{p}\right)$, $\left(\frac{e_2}{2}\right)$, which appear in $\alpha$ and $\beta$.

First, from (8), we have

$$\lambda(p) = \frac{1}{2} \sum_{0 < \chi < \sqrt{p}} \left\{ 1 + \left(\frac{x}{p}\right) \right\},$$

that is

$$\lambda(p) = \frac{1}{16} (p-1) + \frac{1}{2} \sum_{0 < \chi < \sqrt{p}} \left(\frac{x}{p}\right).$$

Now it is well-known that for primes $p \equiv 1 \pmod{8}$ (see for example [3: p. 694])

$$\sum_{0 < \chi < \sqrt{p}} \left(\frac{x}{p}\right) = \frac{1}{4} (h(-4p) + h(-8p)),$$

where $h(-4p)$ and $h(-8p)$ are the class numbers of $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{-2p})$ respectively. Hence, from (11) and (12), we obtain

$$\lambda(p) = \frac{1}{16} (p-1+2h(-4p)+2h(-8p)).$$

Then appealing to the easily proved result

$$\frac{p-1}{16} \equiv \frac{a-1}{8} \pmod{2}$$

we have

$$(-1)^{\lambda(p)} = (-1)^{(a+1+h(-4p)+h(-8p))/8}.$$

Secondly, by a theorem of Emma Lehmer [9], we have

$$\left(\frac{e_2}{p}\right) = (-1)^d,$$

and so by (4) we obtain

$$\left(\frac{e_2}{p}\right) = \left(\frac{2}{p}\right)^d (-1)^d.$$

Now by the Reuschle [11]–Western [12] criterion for 2 to be an eighth power (see also [13]), we have

$$\left(\frac{2}{p}\right) = (-1)^{d/8},$$

so
Thirdly, as \( h^+(8p) \equiv 0 \pmod{8} \), we have \( h( -4p) \equiv 0 \pmod{8} \) \[4\], and so \( T \equiv 0 \pmod{8} \) \[6\]. Moreover, as \( p \equiv 1 \pmod{8} \), \( \sqrt{p} \) is defined modulo 16 and is odd, so that \( T \sqrt{p} \equiv T \pmod{16} \), and we have from \( (5) \), as \( p \equiv 1 \pmod{16} \),

\[
\left( \frac{e_p}{2} \right) = (-1)^{(p+T-1)/8} = (-1)^{(T+U-1)/8} .
\]

Appealing to \( (13) \) and the easily-proved result

\[
U \equiv \frac{1}{2} (p+1) \pmod{16} ,
\]
as well as a theorem of Williams \[14\]

\[
h( -4p) \equiv T \pmod{16} ,
\]
we obtain

\[
\left( \frac{e_p}{2} \right) = (-1)^{(e-1+h(-4p))/8} .
\]

From \( (9) \), \( (14) \), \( (15) \), \( (16) \), we see that

\[
\alpha = (-1)^h(-8p)/8, \quad \beta = (-1)^{a-1+b+2d+h(-4p)/8} .
\]

Then by Lemma 1 we obtain the following theorem.

**Theorem.** If \( p \equiv 1 \pmod{8} \) is a prime such that \( h^+(8p) \equiv 0 \pmod{8} \) and \( \alpha \) and \( \beta \) are as given in \( (17) \), then

\[
\alpha = \beta = 1 \quad \Rightarrow h^+(8p) \equiv 0 \pmod{16} ,
\]
\[
\alpha = 1, \beta = -1 \quad \Rightarrow h^+(8p) \equiv 8 \pmod{16} , \quad E_p = -2 ,
\]
\[
\alpha = -1, \beta = 1 \quad \Rightarrow h^+(8p) \equiv 8 \pmod{16} , \quad E_p = +2 ,
\]
\[
\alpha = \beta = -1 \quad \Rightarrow h^+(8p) \equiv 8 \pmod{16} , \quad E_p = -1 .
\]

As an immediate consequence of our Theorem we have the following corollary.

**Corollary 2.** If \( p \equiv 1 \pmod{8} \) is a prime such that \( h^+(8p) \equiv 0 \pmod{8} \) then

\[
\left\{ \begin{array}{ll}
h^+(8p) \equiv T+a+b+2d-1 \pmod{16} , & \text{if } N(\eta_{2p}) = +1 , \\
0 & \text{if } N(\eta_{2p}) = -1 ;
\end{array} \right.
\]

and

\[
\left\{ \begin{array}{ll}
h(-8p) \equiv 0 \pmod{16} , & \text{if } E_p = -2 , \\
h(-8p) \equiv h^+(8p) \pmod{16} , & \text{if } E_p = -1 , +2 .
\end{array} \right.
\]
We remark that the congruences in (18) appear to be new but that those of (19) are contained in [7], [8].

Finally we compare our Theorem with the following result of Yamamoto [15].

**Lemma 2.** If \( p \equiv 1 \pmod{8} \) is a prime such that \( h^+(8p) \equiv 0 \pmod{8} \) then

\[
\left( \frac{e}{p} \right)_4 = \left( \frac{z-2h(p)}{2} \right)_4 = 1 \Rightarrow h^+(8p) \equiv 0 \pmod{16},
\]

\[
\left( \frac{e}{p} \right)_4 = 1, \left( \frac{z-2h(p)}{2} \right)_4 = -1 \Rightarrow h^+(8p) \equiv 8 \pmod{16}, E_p = -2,
\]

\[
\left( \frac{e}{p} \right)_4 = -1, \left( \frac{z-2h(p)}{2} \right)_4 = 1 \Rightarrow h^+(8p) \equiv 8 \pmod{16}, E_p = +2,
\]

\[
\left( \frac{e}{p} \right)_4 = -1, \left( \frac{z-2h(p)}{2} \right)_4 = -1 \Rightarrow h^+(8p) \equiv 8 \pmod{16}, E_p = -1,
\]

where \( h(p) \) is the class number of \( \mathbb{Q}(\sqrt{p}) \) and \( (z, w) \) is a solution of

\[
z^2 - pw^2 = 2^{h(p)+2}, \quad z \equiv 2^{h(p)} + 1 \pmod{4}.
\]

Clearly from our Theorem and Lemma 2 we have the following corollary.

**Corollary 3.** If \( p \equiv 1 \pmod{8} \) is a prime such that \( h^+(8p) \equiv 0 \pmod{8} \) then

\[
(-1)^{h(-8p)/8} = \left( \frac{e}{p} \right)_4.
\]

However corollary 3 is not quite as general as the following result of Leonard and Williams [10: Theorem 2] (since it is possible to have \( h(-8p) \equiv 0 \pmod{8} \) but \( h^+(8p) \equiv 0 \pmod{8} \), for example \( p = 73 \)):

\[
(-1)^{h(-8p)/8} = \left( \frac{e}{p} \right)_4,
\]

if \( p \) is a prime such that \( h(-8p) \equiv 0 \pmod{8} \) and \( e \) is chosen so that \( e \equiv 1 \pmod{8} \). We remark that Yamamoto [15] has shown that \( (-1)^{h(-8p)/8} = \left( \frac{2e}{p} \right)_4 \), if \( p \equiv 1 \pmod{8} \) is a prime such that \( h(-8p) \equiv 0 \pmod{8} \).

We conclude with a few examples.

**Example 1.** \( p = 113 \)
Here \( a = -7, b = 8, c = 9, d = 4, e = 25, f = 16, \)

\[
h(-4p) = 8, \quad h(-8p) = 8,
\]

so

\[
\alpha = -1, \beta = -1.
\]
Hence, by Theorem, \( h^*(8p) \equiv 8 \pmod{16} \) and \( E_p = -1 \).
Indeed \( h^*(8p) = 8 \) and \( 15^2 - 226 \cdot 1^2 = -1 \).

**Example 2.** \( p = 353 \)
Here \( a = 17, \ b = 8, \ c = -15, \ d = 8, \ e = 49, \ f = 32, \)
\[
h(-4p) = 16, \quad h(-8p) = 24,
\]
so
\[
\alpha = -1, \quad \beta = +1.
\]
Hence, by Theorem, \( h^*(8p) \equiv 8 \pmod{16} \) and \( E_p = +2 \).
Indeed \( h^*(8p) = 8 \) and \( 186^2 - 706 \cdot 7^2 = +2 \).

**Example 3.** \( p = 1217 \)
Here \( a = -31, \ b = 16, \ c = 33, \ d = 8, \ e = 97, \ f = 64, \)
\[
h(-4p) = 32, \quad h(-8p) = 32,
\]
so
\[
\alpha = +1, \quad \beta = +1.
\]
Hence, by Theorem, \( h^*(8p) \equiv 0 \pmod{16} \). Indeed \( h^*(8p) = 16 \).

**Example 4.** \( p = 257 \)
Here \( a = 1, \ b = 16, \ c = -15, \ d = 4, \ e = 17, \ f = 4, \)
\[
h(-4p) = 16, \quad h(-8p) = 16,
\]
so
\[
\alpha = +1, \quad \beta = -1.
\]
Hence, by Theorem 1, \( h^*(8p) \equiv 8 \pmod{16} \) and \( E_p = -2 \).
Indeed \( h^*(8p) = 8 \) and \( 68^2 - 514 \cdot 3^2 = -2 \).

**References**


Pierre Kaplan
U.E.R. de Mathématiques
Université de Nancy
Nancy, France

Kenneth S. Williams
Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario
Canada K1S 5B6