THE CLASS NUMBER OF \( \mathbb{Q}(\sqrt{p}) \) MODULO 4, FOR \( p \equiv 5 \pmod{8} \) A PRIME

KENNETH S. WILLIAMS

Let \( p \equiv 5 \pmod{8} \) be a prime. Let \( h(p) \) denote the class number of the real quadratic field \( \mathbb{Q}(\sqrt{p}) \). It is well-known that \( h(p) \equiv 1 \pmod{2} \). In this paper the residue of \( h(p) \) modulo 4 is determined.

Let \( p \equiv 5 \pmod{8} \) be a prime. Let \( h = h(p) \) denote the class number of the real quadratic field \( \mathbb{Q}(\sqrt{p}) \). It is well-known (see for example [2; § 3]) that

\[
(1) \quad h = h(p) \equiv 1 \pmod{2}.
\]

In this paper we determine \( h(p) \) modulo 4.

The fundamental unit \( \varepsilon_p (> 1) \) of \( \mathbb{Q}(\sqrt{p}) \) can be written

\[
(2) \quad \varepsilon_p = \frac{1}{2} (t + u\sqrt{p}),
\]

where \( t \) and \( u \) are positive integers satisfying

\[
(3) \quad t \equiv u \pmod{2}.
\]

The norm of \( \varepsilon_p \) is \(-1\) so

\[
(4) \quad t^2 - pu^2 = -4.
\]

If \( t \equiv u \equiv 1 \pmod{2} \) then we have (using (4))

\[
\left(\frac{-1}{u}\right) = \left(\frac{-4}{u}\right) = \left(\frac{t^2 - pu^2}{u}\right) = \left(\frac{t^2}{u}\right) = +1,
\]

so

\[
(5) \quad u \equiv 1 \pmod{4}.
\]

If \( t \equiv u \equiv 0 \pmod{2} \), we define positive integers \( t_i \) and \( u_i \) by \( t = 2t_i \), \( u = 2u_i \). Then, from (4), we have

\[
t_i^2 = pu_i^2 - 1 \equiv 5u_i^2 - 1 \equiv 7, \quad 4 \text{ or } 3 \pmod{8}
\]

according as

\[
u_i^2 \equiv 0, \quad 1 \text{ or } 4 \pmod{8}.
\]

Clearly we must have \( t_i^2 \equiv 4 \pmod{8} \), so that

\[
(6) \quad t_i \equiv 2 \pmod{4}, \quad u_i \equiv 1 \pmod{2}.
\]
Further, we have
\[
\left(\frac{-1}{u_i}\right) = \left(\frac{t_i^2 - pu_i^2}{u_i}\right) = \left(\frac{t_i^2}{u_i}\right) = +1,
\]
so
\[
(7) \quad u_i \equiv 1 \pmod{4}.
\]

Next we define unique integers \(a\) and \(b\) by
\[
(8) \quad p = a^2 + b^2, \quad a \equiv -1 \pmod{4}, \quad b \equiv \left(-\frac{p - 1}{2}\right)! \cdot a \pmod{p},
\]
and we note that (as \(p \equiv 5 \pmod{8}\), \(a\) odd)
\[
(9) \quad b \equiv 2 \pmod{4}.
\]

We prove

**Theorem 1.**

(a) If \(t \equiv u \equiv 1 \pmod{2}\) then
\[
h(p) \equiv \frac{1}{2}(-2t + u + b + 1) \pmod{4}.
\]

(b) If \(t \equiv u \equiv 0 \pmod{2}\) then
\[
h(p) \equiv \frac{1}{2}(t_i + u_i + b + 1) \pmod{4}.
\]

The proof depends upon a number of lemmas.

**Lemma 1.**
\[
\left(\frac{p - 1}{2}\right)! \equiv (-1)^{(k+1)/2} \cdot t \pmod{p}.
\]

This is a result of Chowla [3].

**Lemma 2.**

(a) If \(t \equiv u \equiv 1 \pmod{2}\) then
\[
t + 2(-1)^{(k+1)/2}i \equiv 0 \pmod{a + bi}.
\]

(b) If \(t \equiv u \equiv 0 \pmod{2}\) then
\[
t_i + (-1)^{(k+1)/2}i \equiv 0 \pmod{a + bi}.
\]

**Proof.** From (8) and Lemma 1 we obtain
\[
(10) \quad at + 2b(-1)^{(k+1)/2} \equiv 0 \pmod{p}.
\]

Then (4) and (10) give
THE CLASS NUMBER OF $Q(\sqrt{p})$ MODULO 4, FOR $p \equiv 5 \pmod{8}$ A PRIME

$$t(2a(-1)^{(h+1)/2} - bt) = 2(at + 2b(-1)^{(h+1)/2})(-1)^{(h+1)/2} - bp^u^2$$

$$\equiv 0 \pmod{p}.$$

As $t \not\equiv 0 \pmod{p}$, we deduce

(11) $$2a(-1)^{(h+1)/2} - bt \equiv 0 \pmod{p}.$$  

Using (10) and (11) one easily verifies that $(t + 2(-1)^{(h+1)/2}/(a + bi)$ is a gaussian integer, which completes the proof of (a).

The proof of (b) is similar.

**Lemma 3.** (a) If $t \equiv u \equiv 1 \pmod{2}$ there are integers $r$ and $s$ of opposite parity such that

$$t = a(r^2 - s^2) - b(2rs), \quad u = r^2 + s^2,$$

$$2(-1)^{(h+1)/2} = a(2rs) + b(r^2 - s^2).$$

(b) If $t \equiv u \equiv 0 \pmod{2}$ there are integers $r$ and $s$ of opposite parity such that

$$t_1 = -a(2rs) - b(r^2 - s^2), \quad u_1 = r^2 + s^2,$$

$$(-1)^{(h+1)/2} = a(r^2 - s^2) - b(2rs).$$

**Proof.** (a) The gaussian integers $(t + 2(-1)^{(h+1)/2}/(a + bi)$ and

$(t - 2(-1)^{(h+1)/2}/(a - bi)$ are coprime and their product is $u^2$. Hence there exist integers $r$ and $s$ such that

(12) $$\frac{t + 2(-1)^{(h+1)/2}i}{a + bi} = \varepsilon(r + si)^2,$$

where $\varepsilon = \pm 1, \pm i$. Multiplying both sides of (12) by $a + bi$ and considering the parities of the coefficients of $i$ on both sides of the resulting equation, we see that $\varepsilon = \pm 1$. Replacing $r + si$ by $-s + ri$, if necessary, we can suppose, without loss of generality, that $\varepsilon = +1$ so

(13) $$t + 2(-1)^{(h+1)/2}i = (a + bi)(r + si)^2.$$

Equating coefficients we obtain the required expressions for $t$ and $2(-1)^{(h+1)/2}$. Finally, we have

$$u^2 = \frac{t + 2(-1)^{(h+1)/2}i}{a + bi} \cdot \frac{t - 2(-1)^{(h+1)/2}i}{a - bi}$$

$$= (r + si)^2(r - si)^2$$

$$= (r^2 + s^2)^2,$$

so, as $u > 0, r^2 + s^2 > 0$, we obtain

$$u = r^2 + s^2.$$
Since \( u \) is odd this shows that \( r \) and \( s \) are of opposite parity.

(b) The proof is similar. In this case we obtain

\[
t_i + (-1)^{(k+1)/2}i = i(a + bi)(r + si)\]

**Lemma 4.** (a) If \( t \equiv u \equiv 1 \pmod{2} \) then

\[
u \equiv a + 2\left(\frac{2}{t}\right) \pmod{8}.
\]

(b) If \( t \equiv u \equiv 0 \pmod{2} \) then

\[
u \equiv a + 2 \pmod{8}.
\]

**Proof.** (a) As \( b \equiv 0 \pmod{2} \) and one of \( r \) and \( s \) is even, we have, by Lemma 3(a),

\[
t = a(r^2 - s^2) \pmod{8}.
\]

In particular, as \( a \equiv -1 \pmod{4} \), (15) gives

\[
t \equiv s^2 - r^2 \pmod{4},
\]

so that

\[
\begin{align*}
t &\equiv 1 \pmod{4} \iff r \text{ even, } s \text{ odd,} \\
t &\equiv -1 \pmod{4} \iff r \text{ odd, } s \text{ even.}
\end{align*}
\]

Appealing to Lemma 3(a), (15) and (16), we obtain

\[
u - a \equiv (r^2 + s^2) - t(r^2 - s^2) \pmod{8}
\]

\[
\equiv (1 - t)r^2 + (1 + t)s^2 \pmod{8}
\]

\[
\equiv \begin{cases} 
1 + t & \text{(mod 8), if } r \text{ even, } s \text{ odd,} \\
1 - t & \text{(mod 8), if } s \text{ odd, } s \text{ even,}
\end{cases}
\]

\[
= 2\left(\frac{2}{t}\right) \pmod{8},
\]

as required.

(b) As \( b \equiv 0 \pmod{2} \) and one of \( r \) and \( s \) is even, we have by Lemma 3(b),

\[
(-1)^{(k+1)/2} \equiv a(r^2 - s^2) \pmod{8}.
\]

In particular, as \( a \equiv -1 \pmod{4} \), (17) gives

\[
r^2 - s^2 \equiv (-1)^{(k-1)/2} \pmod{4},
\]

so that

\[
\begin{align*}
h &\equiv 1 \pmod{4} \iff r \text{ odd, } s \text{ even,} \\
h &\equiv 3 \pmod{4} \iff r \text{ even, } s \text{ odd.}
\end{align*}
\]
Appealing to Lemma 3(b), (17) and (18) we obtain
\[
\begin{align*}
   u_i - a &\equiv (r^2 + s^2) - (-1)^{k+1/2}(r^2 - s^2) \pmod{8} \\
   &\equiv (1 + (-1)^{k+1/2})r^2 + (1 + (-1)^{k+1/2})s^2 \pmod{8} \\
   &\equiv 2 \pmod{8},
\end{align*}
\]
as required.

We are now in a position to prove Theorem 1.

**Proof of Theorem 1.** (a) As \( r + s \) is odd, we have, by Lemma 3(a),
\[
2rs = (r + s)^2 - (r^2 + s^2) \equiv 1 - u \pmod{8}.
\]
Hence, by Lemma 3(a), (15) and (19), we have
\[
2(-1)^{(k+1)/2} \equiv a(1 - u) + abt \pmod{8},
\]
so, recalling \( a \equiv -1 \pmod{4}, b \equiv 2 \pmod{4}, t \equiv u \equiv 1 \pmod{2}, \)
\[
h \equiv 2 + (-1)^{(k+1)/2} \pmod{4}
\equiv 2 + a\left(\frac{1 - u}{2}\right) + a\left(\frac{b}{2}\right)t \pmod{4}
\equiv 2 + \left(\frac{u - 1}{2}\right) - \frac{b}{2}t \pmod{4}
\equiv 2 + \left(\frac{u - 1}{2}\right) + \left(\frac{b}{2} - t - 1\right) \pmod{4}
\equiv \frac{1}{2}(-2t + u + b + 1) \pmod{4},
\]
as required.

(b) As \( r + s \) is odd, we have, by Lemma 3(b),
\[
2rs = (r + s)^2 - (r^2 + s^2) \equiv 1 - u_i \pmod{8}.
\]
From Lemma 3(b), (17) and (20), we have
\[
t_i \equiv -a(1 - u_i) - ab(-1)^{(k+1)/2} \pmod{8},
\]
so (as \( a \equiv -1 \pmod{4} \))
\[
\frac{t_i}{2} \equiv \left(\frac{1 - u_i}{2}\right) + \left(\frac{b}{2}\right)(-1)^{(k+1)/2} \pmod{4}.
\]
As \( b \equiv 2 \pmod{4}, \) multiplying both sides by \( b/2 \equiv 1 \pmod{2}, \) we obtain
\[
\frac{b}{2} \cdot \frac{t_i}{2} \equiv \frac{b}{2} \cdot \left(\frac{1 - u_i}{2}\right) + (-1)^{(k+1)/2} \pmod{4},
\]
giving
\[ h = 2 + (-1)^{t+u/2} \pmod{4} \]
\[ = 2 + \frac{b}{2} \left( \frac{t_1 + u_1 - 1}{2} \right) \pmod{4} \]
\[ = 2 + \left( \frac{t_1}{2} - 1 \right) + \left( \frac{u_1 - 1}{2} \right) + \frac{b}{2} \pmod{4} \]
\[ = \frac{1}{2} \left( t_1 + u_1 + b + 1 \right) \pmod{4}, \]
as required.

Using Lemma 4 in conjunction with Theorem 1, we obtain

**Corollary 1.**

(i) If \( t \equiv 1 \) or \( 3 \pmod{8} \) or \( t_1 \equiv 6 \pmod{8} \) then
\[ h(p) \equiv \frac{1}{2} (a + b + 1) \pmod{4}. \]

(ii) If \( t \equiv 5 \) or \( 7 \pmod{8} \) or \( t_1 \equiv 2 \pmod{8} \) then
\[ h(p) \equiv \frac{1}{2} (a + b - 3) \pmod{4}. \]

Reformulating Theorem 1, we obtain

**Corollary 2.**

(a) If \( t \equiv u \equiv 1 \pmod{2} \) then
\[ h(p) = \begin{cases} 
-t + \frac{1}{2} (u + 3) \pmod{4}, & \text{if } b \equiv 2 \pmod{8}, \\
t + \frac{1}{2} (u + 3) \pmod{4}, & \text{if } b \equiv 6 \pmod{8}. 
\end{cases} \]

(b) If \( t \equiv u \equiv 0 \pmod{2} \) then
\[ h(p) = \begin{cases} 
\frac{1}{2} (t_1 + u_1 + 3) \pmod{4}, & \text{if } b \equiv 2 \pmod{8}, \\
\frac{1}{2} (t_1 + u_1 - 1) \pmod{4}, & \text{if } b \equiv 6 \pmod{8}. 
\end{cases} \]

Now Gauss [5] has shown that \( h(-p) \) (the class number of the imaginary quadratic field \( \mathbb{Q}(\sqrt{-p}) \), see also [1: p. 828] satisfies.

**Lemma 5.** \( h(-p) \equiv a + b + 1 \pmod{8} \).

Putting together Corollary 1 and Lemma 5 we obtain

**Corollary 3.**

(i) If \( t \equiv 1 \) or \( 3 \pmod{8} \) or \( t_1 \equiv 6 \pmod{8} \) then
\[ h(-p) \equiv 2h(p) \pmod{8}. \]
(ii) If \( t \equiv 5 \) or \( 7 \pmod{8} \) or \( t \equiv 2 \pmod{8} \) then
\[
h(-p) \equiv 2h(p) + 4 \pmod{8}.
\]

The result corresponding to Corollary 3 for primes \( p \equiv 3 \pmod{4} \) has been given by the author in [4].

Finally we show that there does not exist a result analogous to Theorem 1 for primes \( p \equiv 1 \pmod{8} \). It is easily checked that the above arguments fail to yield such a result in this case, as we do not know the exact power of 2 dividing \( b \) in the representation \( p = a^2 + b^2 \), \( a \) odd, \( b \) even. We prove

**Theorem 2.** Let \( p \equiv 1 \pmod{8} \) be a prime. We define unique integers \( a \) and \( b \) by
\[
p = a^2 + b^2, \quad a \equiv -1 \pmod{4}, \quad b \equiv -(\frac{p-1}{2})! \pmod{p},
\]
so that
\[
b \equiv 0 \pmod{4}.
\]
The fundamental unit \((> 1)\) of the real quadratic field \( \mathbb{Q}(\sqrt{p}) \) is of the form
\[
\varepsilon_p = t_1 + u_1\sqrt{p},
\]
where \( t_1 \) and \( u_1 \) are positive integers such that
\[
t_1^2 - pu_1^2 = -1, \quad t_1 \equiv 0 \pmod{4}, \quad u_1 \equiv 1 \pmod{4}.
\]
Analogous to Lemma 4(b) we have
\[
u_1 \equiv a + 2 \pmod{8}.
\]
Then there do NOT exist integers \( l_1, l_2, l_3, l_4 \) independent of \( p \), such that
\[
h(p) \equiv \frac{1}{2}(l_1a + l_2b + l_3t_1 + l_4) \pmod{4}.
\]
(Note: We remark that it is unnecessary to include multiples of either \( p \) or \( u_1 \) inside the parentheses on the right hand side of (22) since \( p \equiv 1 \pmod{8} \) and \( u_1 \) satisfies (21).)

**Proof.** Suppose that a congruence of the form holds. Taking \( p = 97 \), so that \( t_1 = 5604, \; u_1 = 569, \; a = -9, \; b = +4, \; k = 1 \); and \( p = 257 \), so that \( t_1 = 16, \; u_1 = 1, \; a = -1, \; b = +16, \; k = 3 \); we must have
\[
\begin{align*}
-9l_1 + 4l_2 + 5604l_3 + l_4 & \equiv 2 \pmod{8}, \\
-l_1 + 16l_2 + 16l_3 + l_4 & \equiv 6 \pmod{8}.
\end{align*}
\]
Subtracting the two congruences in (23) we obtain
\[ 8l_1 + 12l_2 - 558l_3 \equiv 4 \pmod{8}, \]
that is
\[ 4l_2 + 4l_3 \equiv 4 \pmod{8}, \]
or
\[ (24) \quad l_2 + l_3 \equiv 1 \pmod{2}. \]
Next taking \( p = 41 \), so that \( t_1 = 32, u_1 = 5, a = -5, b = +4, h = 1; \) and \( p = 73 \), so that \( t_1 = 1068, u_1 = 125, a = 3, b = -8, h = 1; \) we obtain
\[ \begin{cases} -5l_1 + 4l_2 + 32l_3 + l_4 \equiv 2 \pmod{8}, \\ 3l_1 + 8l_2 + 1068l_3 + l_4 \equiv 2 \pmod{8}. \end{cases} \]
Subtracting the congruences in (25) we get
\[ 8l_1 - 12l_2 + 1036l_3 \equiv 0 \pmod{8} \]
that is
\[ 4l_2 + 4l_3 \equiv 0 \pmod{8}, \]
or
\[ (26) \quad l_2 + l_3 \equiv 0 \pmod{2}. \]
(24) and (26) provide the required contradiction.

References

4. Kenneth S. Williams, The class number of \( \mathbb{Q}(\sqrt{-p}) \) modulo 4, for \( p \equiv 3 \pmod{4} \) a prime, Pacific J. Math., 83 (1979), 565-570.

Received May 1, 1979. Research supported by Grant No. A-7233 of the Natural Sciences and Engineering Research Council of Canada.