On the class numbers of $\mathbb{Q} \left( \sqrt{-2p} \right)$ modulo 16, for $p \equiv 1 \pmod{8}$ a prime

by

PIERRE KAPLAN (Nancy, France) and KENNETH S. WILLIAMS* (Ottawa, Canada)

1. Introduction. This paper is a sequel to the paper [4] of the second author and should be read in conjunction with it. For the prime $p = 8l + 1$, we consider the ideal class number $h(-2p)$ of $\mathbb{Q} \left( \sqrt{-2p} \right)$ and the ideal class number $h(2p)$ in the narrow sense of $\mathbb{Q} \left( \sqrt{2p} \right)$. It is well known that $h(-2p) = h(2p) = 0 \pmod{4}$. Let $\eta_{2p} = R + S \sqrt{2p} > 1$ be the fundamental unit of norm +1 of the real quadratic field $\mathbb{Q} \left( \sqrt{2p} \right)$, so that

$$R^2 - 2pS^2 = 1.$$  

Clearly $R$ is odd and $S$ is even. Our aim is to prove the following theorem.

**Theorem.**

$$h(-2p) + S \cdot h(2p) + p - 1 \equiv 0 \pmod{16}.$$  

This theorem establishes a conjecture of the first author given in [3], p. 285.

It is known (see for example [1], p. 600) that exactly one of the three equations $x^2 - 2py^2 = -1, -2, +2$ is solvable in integers $x$ and $y$. We set $E_p = -1, -2, +2$ accordingly, so that

$$V^2 - 2pW^2 = E_p$$

has rational integral solutions $V, W$. The following congruences involving $h(2p), h(-2p)$ and $h(-p)$ modulo 8 are known (see for example [1]):

$$h(-2p) \equiv h(-p) + 4l \pmod{8},$$  

$$h(2p) \equiv 0 \pmod{8} \iff h(-p) \equiv 0 \pmod{8} \text{ and } p \equiv 1 \pmod{16},$$

* Research supported by grant no. A-7233 of the Natural Sciences and Engineering Research Council Canada.
\[ h(-p) = 0 \pmod{8}, \quad p = 9 \pmod{16} \Rightarrow E_p = -1, \]
\[ h(-p) = 4 \pmod{8}, \quad p = 1 \pmod{16} \Rightarrow E_p = +2, \]
\[ h(-p) = 4 \pmod{8}, \quad p = 9 \pmod{16} \Rightarrow E_p = -2. \]

In fact (1.5), (1.6), (1.7) are parts of Lemma 5 in [4], and (1.3) follows from (7.5) in [4], as \( h(-p) + h(-2p) = 4S_b \), and \( S_b = l \pmod{2} \). We will reprove (1.4), and then make use of it to prove the theorem.

Next we consider (1.1), written in the form
\[ (R+1)(R-1) = 2pS^2. \]

As \( \gcd(R+1, R-1) = 2 \), there exist positive integers \( V \) and \( W \) such that one of the following four alternatives holds:

\[
\begin{align*}
R+1 & = 2pW^2, & R-1 & = V^2; \\
R+1 & = p(2W)^2, & R-1 & = 2W^2; \\
R+1 & = 2pW^2, & R-1 & = p(2V)^2;
\end{align*}
\]

where \( W \) is odd. The last alternative is impossible, as then \( W^2 - 2pV^2 = 1 \) with \( W < R \) and \( V < S \). The three first possibilities give respectively:

\[ 2 = V^2 - 2pW^2, \quad R = 1 + V^2, \quad S = WV, \quad V = S = 0 \pmod{4}, \]

\[ 2 = V^2 - 2pW^2, \quad R = V^2 - 1, \quad S = WV, \quad V = S = 2 \pmod{4}, \]

\[ -1 = V^2 - 2pW^2, \quad R = 1 + 2V^2, \quad S = 2VW, \quad W = 1 \pmod{4}, \quad S = 2 \pmod{4}. \]

We note that \((V, W)\) is the smallest positive solution of \( V^2 - 2pW^2 = E_p \) and that

\[ S = 0 \pmod{4} \Leftrightarrow E_p = -2. \]

2. **Evaluation of \( F_n(a) \).** In this section we make use of the following class number formulae of Dirichlet (see for example [2], p. 196):

\[ h(-p) = \frac{2}{\pi} V^2 \sum_{n=1}^{\infty} \frac{1}{n} \left( -\frac{4p}{n} \right), \]

\[ h(-2p) = \frac{2}{\pi} V^2 \sum_{n=1}^{\infty} \frac{1}{n} \left( -\frac{8p}{n} \right), \]

\[ h(2p) \log n_{2p} = 2V^2 \sum_{n=1}^{\infty} \frac{1}{n} \left( \frac{8p}{n} \right). \]
One finds easily from the definition of $F_-(x)$ given in [4], (1.9), that

$$F_-(x) = (-1)^{[p-1]/8} \prod_{j=1}^{p-1} (1 + \omega^j x^j),$$

where $\omega = (1 + \sqrt{2})/2 = \exp(2\pi i/8)$, $\phi = \exp(2\pi i/p)$, and the minus ($-$) indicates that $j$ is restricted to those $j$ satisfying $(j/p) = -1$. Hence we have

$$(-1)^{[p-1]/8} F_-(x) = \phi^{S_1},$$

where

$$S_1 = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} \omega^3 \phi^{n/2}}{n} = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} \omega^{3n}}{n} \sum_{j=1}^{p-1} \phi^{nj},$$

Using the familiar Gauss sum (expressed so that the case $n = 0 \pmod{p}$ is included)

$$\sum_{j=1}^{p-1} \phi^{nj} = \frac{1}{2} \left(1 - \frac{n}{p}\right)^2 - \frac{1}{2},$$

we obtain

$$S_1 = \frac{1}{2} p^{1/2} \sum_{n=1}^{\infty} \frac{(-1)^n \omega^{3n}}{n} \left(\frac{n}{p}\right).$$

Collecting terms on the right-hand side of (2.6) having the same residue modulo 4, we obtain

$$2p^{1/2} S_1 = T_0 + T_1 \omega + T_2 \omega^3 + T_3 \omega^5,$$

where

$$T_j = \sum_{k=1}^{\infty} \frac{(-1)^k \left(\frac{4k-j}{p}\right)}{4k-j} \quad (j = 0, 1, 2, 3).$$

Now

$$4T_0 + \sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{k}{p}\right) = \sum_{k=1}^{\infty} \frac{(-1)^k}{k} \left(\frac{k}{p}\right) + \sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{k}{p}\right) = \sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{2k}{p}\right) = \sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{k}{p}\right),$$

so

$$T_0 = 0,$$
and

\[ T_2 = \frac{1}{2} \sum_{k=1}^{\infty} \frac{(-1)^k}{2k-1} \left( \frac{2k-1}{p} \right) = -\frac{1}{2} \sum_{n=1}^{\infty} \frac{1}{n} \left( \frac{-4p}{p} \right) , \]

so

(2.10) \[ T_2 = -\frac{\pi h(-p)}{4\sqrt{p}} , \]

by (2.1). In a similar manner, using (2.2) and (2.3), we find that

(2.11) \[ T_1 = -\frac{\pi h(-2p)}{4\sqrt{2}p} + \frac{h(2p)\log n_{2p}}{4\sqrt{2}p} , \]

(2.12) \[ T_3 = -\frac{\pi h(-2p)}{4\sqrt{2}p} - \frac{h(2p)\log n_{2p}}{4\sqrt{2}p} . \]

Putting (2.9), (2.10), (2.11), (2.12) into (2.7), we obtain (as \( \omega^2 = i, \omega + \omega^3 = i\sqrt{2}, \omega - \omega^3 = \sqrt{2} \))

(2.13) \[ F_-(\omega) = \eta_{2p}^{\frac{1}{4}} \frac{i}{\sqrt{2}} (-h(-p) + h(-2p))^{1/4} (-1)^{(p-1)/2} , \]

(2.14) \[ F_{-2}(\omega) = \eta_{2p}^{\frac{1}{4}} (-1)^{(1)(h(-p) + h(-2p))} . \]

Making use of (1.3) we obtain

(2.15) \[ F_{-2}(\omega) = (-1)^{(p-1)/2} \eta_{2p}^{\frac{1}{4}} . \]

3. Proof of the theorem. We consider four cases according to the values of \( h(-p) \) modulo 8 and \( p \) modulo 16. As in each case \( p \) is fixed modulo 16, we need not mention the subscripts 1 and 9 used in [4], and we omit them.

From (7.9) of [4] we deduce, proceeding as for (7.13),

(3.1) \[ 4h(-2p) \]

\[ = (1-\omega^2)[Y(\omega)Z'(\omega) - Y'(\omega)Z(\omega) + Y(-\omega)Z'(-\omega) - Y'(-\omega)Z(-\omega)] . \]

Case (i). \( p \equiv 1 \pmod{16} \), \( h(-p) \equiv 0 \pmod{8} \). (Here \( h(-2p) \equiv 0 \pmod{8} \) by (1.3).) From § 6 of [4] we have

(3.2) \[ Y(\omega) = 2A, \quad Y'(\omega) = 2E + 4Fo + 2E\omega^2 - 4LA\omega^3 , \]

\[ Z(\omega) = 2D\sqrt{2} , \quad Z'(\omega) = 2L + 4Mo + 2(L - 4ID)\omega^3 , \]

and

(3.3) \[ A^2 - 2pD^2 = 1 , \quad D + L \equiv 0 \pmod{4} . \]
From (2.5) of [4], (3.2) and (3.3) we deduce

\[ F_-(\omega) = \frac{1}{2} [Y(\omega) + Z(\omega)\sqrt{-2}] = A + D\sqrt{-2}, \]

\[ A = 1 \pmod{2}; \quad D = L = 0 \pmod{2}. \]

Using (3.2) in (3.1), and then applying (3.3) and (3.5), we find

\[ h(-2p) = 4AL - 8DF - 8LAD = 4AL = 4AD \pmod{16}. \]

By (3.4) and (2.13) we have

\[ F_-(\omega) = A + D\sqrt{-2} = (-1)^{(h(-2p) + h(-2p) + p - 3)/8} \eta_{2p}/8. \]

Now (3.3) shows that \( A + D\sqrt{-2} \) is a unit of norm \( +1 \) of \( \mathbb{Q}(\sqrt{-2}) \),
but \( \eta_{2p} \) is the fundamental unit of norm \( +1 \) of \( \mathbb{Q}(\sqrt{-2}) \), so that \( h(2p)/8 \)
must be an integer, proving that \( h(2p) \equiv 0 \pmod{8} \), which is (1.4) in
this case. Now by (3.4) and (2.15) we have

\[ (A + D\sqrt{-2})^2 = (E + S\sqrt{-2})^{h(2p)/4}. \]

As (3.6) suggests, we consider the coefficients of \( \sqrt{-2} \) modulo 8 in
(3.8). We obtain

\[ 2AD = \frac{h(2p)}{4} E^{h(2p)/4} - 1 S = \frac{h(2p)}{4} S \pmod{8}, \]

where we have used \( h(2p)/4 = S = E - 1 = 0 \pmod{2} \).

Then, from (3.6), we obtain

\[ h(-2p) = h(2p) S \frac{S}{2} \pmod{16}. \]

This completes the proof of the theorem in this case.

As \( S \equiv 0 \pmod{4} \) if and only if \( E_p = -2 \) by (1.12), (3.10) can be expressed in the following equivalent ways:

\[ h(-2p) \equiv 0 \pmod{16} \iff h(2p) \equiv 0 \pmod{16} \text{ or } E_p = -2; \]

\[ \begin{align*}
\text{if } E_p = -2, \quad h(-2p) &\equiv 0 \pmod{16}, \\
\text{if } E_p = -1, 2, \quad h(-2p) &\equiv h(2p) \pmod{16}.
\end{align*} \]

Case (ii). \( p \equiv 1 \pmod{16}, \ h(-p) \equiv 4 \pmod{8}. \) (Here \( h(-2p) \equiv 4 \pmod{8} \) by (1.3).) From § 6 of [4] we have

\[ \begin{align*}
Y(\omega) &= 2B\sqrt{2}, \quad Y'(\omega) = 2E + 4F\omega + 2(E - 4B)\omega^3, \\
Z(\omega) &= 2C, \quad Z'(\omega) = 2L + 4M\omega + 2L\omega^3 - 4L\omega^5,
\end{align*} \]
and
\[(3.14) \quad 2B^2 - pC^2 = 1, \quad B + E \equiv 0 \pmod{4}, \quad M \equiv 1 \pmod{2}.\]

From (3.14) we have \((2B)^2 - 2pC^2 = 2\), so that \(E = 2\), and also
\[(3.15) \quad B = C \equiv 1 \pmod{2}.
\]

From (3.13) we have
\[(3.16) \quad \Phi_\omega = B\sqrt{2} + C\sqrt{p}.
\]

Using (3.13) in (3.1), and then applying (3.14) and (3.15), we find
\[(3.17) \quad h(-2p) = -4CE + 8BM + 8BC = 4BC + 8 \pmod{16}.
\]

From (2.14) and (3.16) we have
\[(3.18) \quad (B\sqrt{2} + C\sqrt{p})^2 = (R + S\sqrt{2p})^{4L}\sqrt{p}^{4L}\sqrt{p}^{-1}.
\]

As \(S\) is even, we obtain by considering the coefficients of \(1\) and \(\sqrt{2p}\)
\[(3.19) \quad 2B^2 + C^2 \equiv R^{4L}\sqrt{p}^{4L} \equiv 4 \pmod{8}, \quad 2BC = \frac{h(2p)}{4} \equiv R^{4L}\sqrt{p}^{4L-1} S \pmod{8}.
\]

From (3.15) and (3.18) we deduce that \(R^{4L}\sqrt{p}^{4L} \equiv 3 \pmod{4}\), so that
\(h(2p) = 4 \pmod{8}\), proving (1.4) in this case.

Then, in (3.19), we have \(R^{4L}\sqrt{p}^{4L-1} \equiv 1 \pmod{8}\), and so by (3.17) we obtain
\[(3.20) \quad h(-2p) = h(2p) \frac{S}{2} + 8 \pmod{16},
\]
which completes the proof of the theorem in this case.

Case (iii). \(p = 9 \pmod{16}\), \(h(-p) = 0 \pmod{8}\). (Here \(h(-2p) = 4 \pmod{8}\) by (1.3).) From § 6 of [4], letting \(p = 16k + 9\), we have
\[(3.21) \quad \begin{align*}
Y(\omega) &= 2A\omega, \quad Y'(\omega) = 2E(1 - \omega^2) + 4(2k + 1)A\omega + 4H\omega^2, \\
Z(\omega) &= 2D\sqrt{\omega}, \quad Z'(\omega) = 2L(1 - \omega^2) + 8(2k + 1)D\omega + 4P\omega^2,
\end{align*}
\]
and
\[(3.22) \quad A^2 - 2pD^2 = -1, \quad D + L \equiv 0 \pmod{4}, \quad H \equiv 0 \pmod{2}.
\]

From (3.22) we see that \(E = -1\) and \(A = D \equiv 1 \pmod{2}\). Then, as before, (3.1) gives
\[(3.23) \quad h(-2p) = 4AL + 8DH - (16k + 8)AD = -4AD + 8 = 4AD \pmod{16}.
\]
By (2.15) we have

\[(3.24) \quad (P_{\omega}(w))^2 = -(A + D\sqrt{2p})^2 = -(R + S\sqrt{2p})^{4k(2p)/4}, \]

which gives the two congruences

\[A^2 + 2pD^2 = R^{h(2p)/4} (\text{mod } 8), \]

and

\[2AD = \frac{h(2p)}{4} R^{h(2p)/4 - 1} S (\text{mod } 8). \]

As \(A\) and \(D\) are odd, \(A^2 + 2pD^2 = 3 (\text{mod } 8)\), so that \(h(2p) = 4 (\text{mod } 8)\), proving (1.4) in this case. Then we have, from (3.23),

\[(3.25) \quad h(-2p) = h(2p) \frac{S}{2} (\text{mod } 16), \]

which completes the proof of the theorem in this case.

Case (iv). \(p = 9 (\text{mod } 16)\), \(h(-p) = 4 (\text{mod } 8)\). (Here \(h(-2p) = 0 (\text{mod } 8)\) by (1.3).) From § 6 of [4] we have

\[(3.26) \quad \begin{align*}
Y(w) &= 2B\sqrt{2}, \\
Y'(w) &= 2E(1 - \omega^2) + 8(2k + 1)B\omega^2 + 4H\omega^3, \\
Z(w) &= 2C\sqrt{2}, \\
Z'(w) &= 2L(1 - \omega^2) + 4(2k + 1)C\omega + 4P\omega^3,
\end{align*} \]

and

\[(3.27) \quad 2B^2 - pC^2 = -1; \quad B + E = 2 (\text{mod } 4). \]

From (3.27) we deduce that \(E_p = -2\). Also we have

\[(3.28) \quad B = C - 1 = 0 (\text{mod } 2). \]

Now, by (3.1), (3.26) and (3.27), we have

\[(3.29) \quad h(-2p) = -4CE - 8BP + (16k + 8)BC = 4BC + 8 (\text{mod } 16). \]

From (2.13) we obtain

\[(3.30) \quad B\sqrt{2} + C\sqrt{p} = (-1)^{(h(-p) + h(-2p) - 4)/2} (R + S\sqrt{2p})^{h(2p)/8}, \]

which shows that \(h(2p) = 4 (\text{mod } 8)\). This proves (1.4) in this case. Squaring (3.30) and equating coefficients of \(\sqrt{2p}\), we obtain

\[2BC = \frac{h(2p)}{4} R^{h(2p)/4 - 1} S (\text{mod } 8). \]
Then, as $S = 0 \pmod{4}$ by (1.12), we obtain
\[ h(-2p) = h(2p) \frac{S}{2} + 8 \pmod{16}, \]
which completes the proof of the theorem in this case.

The authors would like to thank Mr. Lee-Jeff Bell, who did some computing for them in connection with preparation of this paper.

References


10 Allée Jacques Offenbach
54420 — Saulxures les Nancy
France

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
Ottawa, Ontario, Canada
K1S 5B6

Received on 27.3.1979
and in revised form on 21.12.1979