ACTA ARITHMETICA
XL (1982)

On the class numbers of $Q(\sqrt{\pm 2p})$ 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 $Q(\sqrt{-2p})$ and the ideal class number $h(2p)$ in the narrow sense of $Q(\sqrt{2p})$. It is well known that $h(-2p) \equiv h(2p) \equiv 0 \pmod 4$. Let $\eta_{2p} = R+S\sqrt{2p} > 1$ be the fundamental unit of norm $+1$ of the real quadratic field $Q(\sqrt{2p})$, so that

$$R^2-2pS^2 = 1. \tag{1.1}$$

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

THEOREM.

$$h(-2p)+\frac{S}{2}\cdot h(2p)+p-1 \equiv 0 \pmod{16}. \tag{1.2}$$

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]):

$$h(-2p) \equiv h(-p)+4l \pmod 8, \tag{1.3}$$

$$h(2p) \equiv 0 \pmod 8 \Leftrightarrow h(-p) \equiv 0 \pmod 8 \text{ and } p \equiv 1 \pmod{16}, \tag{1.4}$$

* Research supported by grant no. A-7233 of the Natural Sciences and Engineering Research Council Canada.

(1.5) $$h(-p) \equiv 0 \pmod 8,\ p \equiv 9 \pmod{16} \Rightarrow E_p = -1,$$

(1.6) $$h(-p) \equiv 4 \pmod 8,\ p \equiv 1 \pmod{16} \Rightarrow E_p = +2,$$

(1.7) $$h(-p) \equiv 4 \pmod 8,\ p \equiv 9 \pmod{16} \Rightarrow E_p = -2.$$

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 $h(-p)+h(-2p) = 4S_0$, and $S_0 \equiv l \pmod 2$. 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:

$$\begin{cases} R+1 = 2pW^2, \\ R-1 = V^2; \end{cases} \quad \begin{cases} R+1 = V^2, \\ R-1 = 2pW^2; \end{cases} \quad \begin{cases} R+1 = p(2W)^2, \\ R-1 = 2V^2; \end{cases} \quad \begin{cases} R+1 = 2W^2, \\ R-1 = p(2V)^2, \end{cases}$$

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:

(1.9) $$-2 = V^2-2pW^2,\ R = 1+V^2,\ S = VW,\ V \equiv S \equiv 0 \pmod 4,$$

(1.10) $$2 = V^2-2pW^2,\ R = V^2-1,\ S = VW,\ V \equiv S \equiv 2 \pmod 4,$$

(1.11) $$-1 = V^2-2pW^2, \quad R = 1+2V^2, \quad S = 2VW,$$
$$W \equiv 1 \pmod 4, \quad S \equiv 2 \pmod 4.$$

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

(1.12) $$S \equiv 0 \pmod 4 \Leftrightarrow E_p = -2.$$

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

(2.1) $$h(-p) = \frac{2}{\pi}\sqrt{p}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{-4p}{n}\right),$$

(2.2) $$h(-2p) = \frac{2}{\pi}\sqrt{2p}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{-8p}{n}\right),$$

(2.3) $$h(2p)\log \eta_{2p} = 2\sqrt{2p}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{8p}{n}\right).$$

One finds easily from the definition of $F_-(z)$ given in [4], (1.9), that

$$F_-(\omega) = (-1)^{(p-1)/8} \prod_{j=1}^{p-1}{}^{-} (1+\omega^3 \varrho^j),$$

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

$$(2.4) \qquad (-1)^{(p-1)/8} F_-(\omega) = e^{S_1},$$

where

$$(2.5) \qquad S_1 = \sum_{j=1}^{p-1}{}^{-} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}\omega^{3n}\varrho^{nj}}{n} = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}\omega^{3n}}{n} \sum_{j=1}^{p-1}{}^{-} \varrho^{nj}.$$

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

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

we obtain

$$(2.6) \qquad S_1 = \frac{1}{2} p^{1/2} \sum_{n=1}^{\infty} \frac{(-1)^n \omega^{3n}}{n} \left(\frac{n}{p}\right).$$

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

$$(2.7) \qquad 2p^{-1/2} S_1 = T_0 + T_1\omega + T_2\omega^2 + T_3\omega^3,$$

where

$$(2.8) \qquad T_j = \sum_{k=1}^{\infty} \frac{(-1)^k}{4k-j}\left(\frac{4k-j}{p}\right) \qquad (j = 0, 1, 2, 3).$$

Now

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

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

so

$$(2.9) \qquad T_0 = 0,$$

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

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

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

$$(2.11) \qquad T_1 = \frac{-\pi h(-2p)}{4\sqrt{2p}} + \frac{h(2p)\log \eta_{2p}}{4\sqrt{2p}},$$

$$(2.12) \qquad T_3 = \frac{-\pi h(-2p)}{4\sqrt{2p}} - \frac{h(2p)\log \eta_{2p}}{4\sqrt{2p}}.$$

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

$$(2.13) \qquad F_-(\omega) = \eta_{2p}^{h(2p)/8} i^{-(h(-p)+h(-2p))/4}(-1)^{(p-1)/8},$$

$$(2.14) \qquad F_-^2(\omega) = \eta_{2p}^{h(2p)/4}(-1)^{(h(-p)+h(-2p))/4}.$$

Making use of (1.3) we obtain

$$(2.15) \qquad F_-^2(\omega) = (-1)^{(p-1)/8}\eta_{2p}^{h(2p)/4}.$$

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),

$$(3.1) \quad 4h(-2p)$$
$$= (1-\omega^2)[Y(\omega)Z'(\omega)-Y'(\omega)Z(\omega)+Y(-\omega)Z'(-\omega)-Y'(-\omega)Z(-\omega)].$$

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

$$(3.2) \quad \begin{cases} Y(\omega) = 2A, & Y'(\omega) = 2E+4F\omega+2E\omega^2-4lA\omega^3, \\ Z(\omega) = 2D\sqrt{2}, & Z'(\omega) = 2L+4M\omega+2(L-4lD)\omega^2, \end{cases}$$

and

$$(3.3) \qquad A^2-2pD^2 = 1, \quad D+L \equiv 0 \pmod 4.$$

From (2.5) of [4], (3.2) and (3.3) we deduce

$$(3.4)\qquad F_-(\omega) = \tfrac{1}{2}[Y(\omega)+Z(\omega)\sqrt{p}] = A+D\sqrt{2p},$$

$$(3.5)\qquad A \equiv 1 \pmod 2, \quad D \equiv L \equiv 0 \pmod 2.$$

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

$$(3.6)\qquad h(-2p) = 4AL-8DF-8lAD \equiv 4AL \equiv 4AD \pmod{16}.$$

By (3.4) and (2.13) we have

$$(3.7)\qquad F_-(\omega) = A+D\sqrt{2p} = (-1)^{(h(-p)+h(-2p)+p-1)/8}\eta_{2p}^{h(2p)/8}.$$

Now (3.3) shows that $A+D\sqrt{2p}$ is a unit of norm $+1$ of $Q(\sqrt{2p})$; but η_{2p} is the fundamental unit of norm $+1$ of $Q(\sqrt{2p})$, 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

$$(3.8)\qquad (A+D\sqrt{2p})^2 = (R+S\sqrt{2p})^{h(2p)/4}.$$

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

$$(3.9)\qquad 2AD = \frac{h(2p)}{4}R^{h(2p)/4-1}S \equiv \frac{h(2p)}{4}S \pmod 8,$$

where we have used $h(2p)/4 \equiv S \equiv R-1 \equiv 0 \pmod 2$.

Then, from (3.6), we obtain

$$(3.10)\qquad h(-2p) \equiv h(2p)\frac{S}{2} \pmod{16}.$$

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:

$$(3.11)\qquad h(-2p) \equiv 0 \pmod{16} \Leftrightarrow h(2p) \equiv 0 \pmod{16} \text{ or } E_p = -2;$$

$$(3.12)\qquad \begin{cases} \text{if } E_p = -2, & h(-2p) \equiv 0 \pmod{16}, \\ \text{if } E_p = -1, 2, & h(-2p) \equiv h(2p) \pmod{16}. \end{cases}$$

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

$$(3.13)\qquad \begin{cases} Y(\omega) = 2B\sqrt{2}, & Y'(\omega) = 2E+4F\omega+2(E-4lB)\omega^2, \\ Z(\omega) = 2C, & Z'(\omega) = 2L+4M\omega+2L\omega^2-4lC\omega^3, \end{cases}$$

and

$$(3.14)\qquad 2B^2-pC^2=1,\quad B+E\equiv 0\ (\mathrm{mod}\ 4),\quad M\equiv 1\ (\mathrm{mod}\ 2).$$

From (3.14) we have $(2B)^2-2pC^2=2$, so that $E_p=2$, and also

$$(3.15)\qquad B\equiv C\equiv 1\ (\mathrm{mod}\ 2).$$

From (3.13) we have

$$(3.16)\qquad F_-(\omega)=B\sqrt{2}+C\sqrt{p}.$$

Using (3.13) in (3.1), and then applying (3.14) and (3.15), we find

$$(3.17)\qquad h(-2p)=-4CE+8BM+8lBC\equiv 4BC+8\ (\mathrm{mod}\ 16).$$

From (2.14) and (3.16) we have

$$(B\sqrt{2}+C\sqrt{p})^2=(R+S\sqrt{2p})^{h(2p)/4}.$$

As S is even, we obtain by considering the coefficients of 1 and $\sqrt{2p}$

$$(3.18)\qquad 2B^2+C^2\equiv R^{h(2p)/4}\ (\mathrm{mod}\ 8),$$

$$(3.19)\qquad 2BC\equiv\frac{h(2p)}{4}R^{h(2p)/4-1}S\ (\mathrm{mod}\ 8).$$

From (3.15) and (3.18) we deduce that $R^{h(2p)/4}\equiv 3\ (\mathrm{mod}\ 4)$, so tha $h(2p)\equiv 4\ (\mathrm{mod}\ 8)$, proving (1.4) in this case.

Then, in (3.19), we have $R^{h(2p)/4-1}\equiv 1\ (\mathrm{mod}\ 8)$, and so by (3.17) we obtain

$$(3.20)\qquad h(-2p)\equiv h(2p)\frac{S}{2}+8\ (\mathrm{mod}\ 16),$$

which completes the proof of the theorem in this case.

Case (iii). $p\equiv 9\ (\mathrm{mod}\ 16)$, $h(-p)\equiv 0\ (\mathrm{mod}\ 8)$. (Here $h(-2p)\equiv 4\ (\mathrm{mod}\ 8)$ by (1.3).) From § 6 of [4], letting $p\equiv 16k+9$, we have

$$(3.21)\qquad \begin{cases} Y(\omega)=2Ai, & Y'(\omega)=2E(1-\omega^2)+4(2k+1)A\omega+4H\omega^3,\\ Z(\omega)=2Di\sqrt{2}, & Z'(\omega)=2L(1-\omega^2)+8(2k+1)D\omega^2+4P\omega^3,\end{cases}$$

and

$$(3.22)\qquad A^2-2pD^2=-1,\quad D+L\equiv 0\ (\mathrm{mod}\ 4),\quad H\equiv 0\ (\mathrm{mod}\ 2).$$

From (3.22) we see that $E_p=-1$ and $A\equiv D\equiv 1\ (\mathrm{mod}\ 2)$. Then, as before, (3.1) gives

$$(3.23)\qquad h(-2p)=4AL+8DH-(16k+8)AD\equiv -4AD+8 \equiv 4AD\ (\mathrm{mod}\ 16).$$

By (2.15) we have

$$(3.24)\qquad (F_{-}(\omega))^2 = -(A+D\sqrt{2p})^2 = -(R+S\sqrt{2p})^{h(2p)/4},$$

which gives the two congruences

$$A^2+2pD^2 \equiv R^{h(2p)/4} \pmod 8,$$

and

$$2AD \equiv \frac{h(2p)}{4} R^{h(2p)/4-1} S \pmod 8.$$

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

$$(3.25)\qquad h(-2p) \equiv h(2p)\frac{S}{2} \pmod{16},$$

which completes the proof of the theorem in this case.

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

$$(3.26)\qquad \begin{cases} Y(\omega) = 2Bi\sqrt{2}, & Y'(\omega) = 2E(1-\omega^2)+8(2k+1)B\omega^2+4H\omega^3, \\ Z(\omega) = 2Ci, & Z'(\omega) = 2L(1-\omega^2)+4(2k+1)C\omega+4P\omega^3, \end{cases}$$

and

$$(3.27)\qquad 2B^2-pC^2 = -1; \quad B+E \equiv 2 \pmod 4.$$

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

$$(3.28)\qquad B \equiv C-1 \equiv 0 \pmod 2.$$

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

$$(3.29)\qquad h(-2p) = -4CE-8BP+(16k+8)BC \equiv 4BC+8 \pmod{16}.$$

From (2.13) we obtain

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

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

$$2BC \equiv \frac{h(2p)}{4} R^{h(2p)/4-1} S \pmod 8.$$

Then, as $S \equiv 0 \pmod 4$ by (1.12), we obtain

$$h(-2p) \equiv h(2p)\frac{S}{2} + 8 \pmod{16},$$

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

[1] Pierre Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan 25 (1973), pp. 596–608.

[2] Edmund Landau, *Elementary number theory*, Chelsea Publishing Company, New York 1958.

[3] Bernard Oriat, *Sur la divisibilité par 8 et 16 des nombres de classes d'idéaux des corps quadratiques $Q(\sqrt{2p})$ at $Q(\sqrt{-2p})$*, J. Math. Soc. Japan 30 (1978), pp. 279–285.

[4] Kenneth S. Williams, *On the class number of $Q(\sqrt{-p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime*, Acta Arith. 39 (1981), pp. 381–398.

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 (1151)