JOURNAL OF NUMBER THEORY 15, 182–198 (1982)

Congruences Modulo 8 for the Class Numbers of $Q(\sqrt{\pm p})$, $p \equiv 3 \pmod 4$ a Prime

KENNETH S. WILLIAMS*

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada

Communicated by H. Zassenhaus

Received December 15, 1980; revised May 7, 1981

A congruence modulo 8 is proved relating the class numbers of the quadratic fields $Q(\sqrt{p})$ and $Q(\sqrt{-p})$, where p is a prime congruent to 3 modulo 4.

1. INTRODUCTION

Throughout this paper p denotes a prime (greater than 3) which is congruent to 3 modulo 4. The class number of the quadratic field $Q(\sqrt{p})$ (resp. $Q(\sqrt{-p})$) is denoted by $h(p)$ (resp. $h(-p)$). It is well known that (see, for example, [2, p. 413; 3, p. 100])

$$h(p) \equiv h(-p) \equiv 1 \pmod 2. \tag{1.1}$$

In [7] the author determined a congruence (see (4.1) below) relating $h(p)$ and $h(-p)$ modulo 4. It is the purpose of this paper to determine congruences relating these class numbers modulo 8. (The analogous problem for primes $p \equiv 1 \pmod 4$ has been treated by the author elsewhere [5, 7–11].)

2. THE FUNDAMENTAL UNIT ε_p

The fundamental unit ε_p (> 1) of the real quadratic field $Q(\sqrt{p})$ is of the form (see, for example, [4, Sect. 7])

$$\varepsilon_p = T + U\sqrt{p} = \tfrac{1}{2}(R + S\sqrt{p})^2, \tag{2.1}$$

* Research supported by the Natural Sciences and Engineering Research Council of Canada under Grant A-7233.

0022-314X/82/050182–17$02.00/0

where T and U are positive coprime integers which satisfy

$$T \equiv 0 \pmod{2}, \quad U \equiv 1 \pmod{2}, \quad N(\varepsilon_p) = T^2 - pU^2 = +1, \tag{2.2}$$

and where R and S are positive coprime integers satisfying

$$\begin{aligned} R \equiv S \equiv 1 \pmod{2}, \quad R^2 - pS^2 &= -2, \qquad \text{if} \quad p \equiv 3 \pmod{8}, \\ &= +2, \qquad \text{if} \quad p \equiv 7 \pmod{8}. \end{aligned} \tag{2.3}$$

Clearly T, U, R and S are related by

$$T = \tfrac{1}{2}(R^2 + pS^2), \qquad U = RS. \tag{2.4}$$

The integers R and S play a central role in everything that follows.

3. Congruences for R and S modulo 8

From (2.3) we have

$$\left(\frac{-2}{S}\right) = \left(\frac{R^2 - pS^2}{S}\right) = \left(\frac{R^2}{S}\right) = +1, \qquad \text{if} \quad p \equiv 3 \pmod{8},$$

$$\left(\frac{+2}{S}\right) = \left(\frac{R^2 - pS^2}{S}\right) = \left(\frac{R^2}{S}\right) = +1, \qquad \text{if} \quad p \equiv 7 \pmod{8},$$

so that

$$\begin{cases} S \equiv 1, 3 \pmod{8}, & \text{if} \quad p \equiv 3 \pmod{8}, \\ S \equiv 1, 7 \pmod{8}, & \text{if} \quad p \equiv 7 \pmod{8}. \end{cases} \tag{3.1}$$

Then, from (2.3) and (3.1), we obtain

LEMMA 1. (a) *If* $p \equiv 3 \pmod{16}$ *then*

$$(R, S) \equiv (1, 1), (3, 3), (5, 3) \quad \text{or} \quad (7, 1) \pmod{8}.$$

(b) *If* $p \equiv 7 \pmod{16}$ *then*

$$(R, S) \equiv (3, 1), (3, 7), (5, 1) \quad \text{or} \quad (5, 7) \pmod{8}.$$

(c) *If* $p \equiv 11 \pmod{16}$ *then*

$$(R, S) \equiv (1, 3), (3, 1), (5, 1) \quad \text{or} \quad (7, 3) \pmod{8}.$$

(d) *If* $p \equiv 15 \pmod{16}$ *then*

$$(R, S) \equiv (1, 1), (1, 7), (7, 1) \quad or \quad (7, 7) \pmod 8.$$

4. Congruences Relating $h(p)$ and $h(-p)$ (mod 4)

In [7] the author showed that

$$h(-p) \equiv h(p) + U + 1 \pmod 4. \tag{4.1}$$

Appealing to (1.1), (2.3), (2.4) and (4.1) we obtain

LEMMA 2. (a) *If* $R \equiv S \pmod 4$

$$h(-p) + h(p) \equiv 0 \pmod 4.$$

(b) *If* $R \equiv -S \pmod 4$

$$h(-p) - h(p) \equiv 0 \pmod 4.$$

5. Congruences Relating $h(p)$ and $h(-p)$ (mod 8)—Statement of Main Theorem

It is the purpose of this paper to prove, by extending the ideas used in [7], a more precise form of Lemma 2. We prove

THEOREM. (a) *If* $R \equiv S \pmod 4$

$$h(-p) + h(p) \equiv R + S + 2(-1)^{(p-3)/4} \pmod 8.$$

(b) *If* $R \equiv -S \pmod 4$

$$h(-p) - h(p) \equiv R - S - 2 \pmod 8.$$

The proof of this theorem is completed in Section 12, after a number of lemmas are proved in Sections 6–11. It uses the ideas of [7] but is much more complicated in its details.

6. The polynomials $F_+(z)$ and $F_-(z)$

We set $\rho = \exp(2\pi i/p)$ and, for z a complex variable, we define (as in [7])

$$F_+(z) = \prod_{\substack{j=1 \\ (\frac{j}{p})=+1}}^{p-1} (z-\rho^j), \qquad F_-(z) = \prod_{\substack{j=1 \\ (\frac{j}{p})=-1}}^{p-1} (z-\rho^j), \tag{6.1}$$

so that

$$F(z) = F_+(z)\,F_-(z) = \prod_{j=1}^{p-1} (z-\rho^j) = \frac{z^p-1}{z-1} = z^{p-1} + z^{p-2} + \cdots + 1. \tag{6.2}$$

It is easily checked that

$$F(1) = p, \qquad F(-1) = 1, \qquad F(\pm i) = \pm i, \tag{6.3}$$

and

$$\begin{gathered} F'(1) = \tfrac{1}{2}p(p-1), \qquad F'(-1) = -\tfrac{1}{2}(p-1), \\ F'(\pm i) = \tfrac{1}{2}(p-1) \pm \tfrac{1}{2}(p+1)\,i. \end{gathered} \tag{6.4}$$

7. Evaluation of $F_\pm(-1)$ and $F_\pm(\pm i)$

Throughout the rest of the paper the convention $\sqrt{-p} = i\sqrt{p}$ is used. We prove

LEMMA. 3.

$$F_+(1) = (-1^{1/2(h(-p)+1)}\sqrt{-p},$$

$$F_-(1) = (-1)^{1/2(h(-p)-1)}\sqrt{-p},$$

$$F_+(-1) = F_-(-1) = (-1)^{1/4(p-3)},$$

$$F_+(i) = \begin{Bmatrix} \omega^3(-1)^{1/2(h(-p)+1)}\,\varepsilon_p^{-h(p)/2}, \\ \quad \text{if} \quad p \equiv 3 \pmod 8 \\ \omega^5\varepsilon_p^{-h(p)/2} \quad \text{if} \quad p \equiv 7 \pmod 8 \end{Bmatrix},$$

$$F_-(i) = \begin{Bmatrix} \omega^7(-1)^{1/2(h(-p)+1)}\,\varepsilon_p^{h(p)/2}, \\ \quad \text{if} \quad p \equiv 3 \pmod 8 \\ \omega^5\varepsilon_p^{h(p)/2}, \quad \text{if} \quad p \equiv 7 \pmod 8 \end{Bmatrix},$$

$$F_+(-i) = \begin{cases} \omega(-1)^{1/2(h(-p)+1)}\,\varepsilon_p^{h(p)/2}, & \\ \quad \text{if} \quad p \equiv 3 \pmod 8 & \\ \omega^3 \varepsilon_p^{h(p)/2}, \quad \text{if} \quad p \equiv 7 \pmod 8 & \end{cases},$$

$$F_-(-i) = \begin{cases} \omega^5(-1)^{1/2(h(-p)+1)}\,\varepsilon_p^{-h(p)/2}, & \\ \quad \text{if} \quad p \equiv 3 \pmod 8 & \\ \omega^3 \varepsilon_p^{-h(p)/2}, \quad \text{if} \quad p \equiv 7 \pmod 8 & \end{cases},$$

where $\omega = (1+i)/\sqrt{2}$ *is an eighth root of unity.*

Proof. We just give the details of the evaluation of $F_-(i)$ as the other cases are similar. From (6.1) we have (where the dash indicates that j is restricted to satisfy $(\frac{j}{p}) = -1$)

$$F_-(i) = \prod_{j=1}^{p-1}{}' (i - \rho^j) = i^{1/2(p-1)} \prod_{j=1}^{p-1}{}' (1 + i\rho^j).$$

As $i\rho^j$ $(1 \leqslant j \leqslant p-1)$ is a root of unity (not equal to 1), we have

$$\gamma_j = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}\, i^n \rho^{jn}}{n} = \log(1 + i\rho^j) \qquad (j = 1, 2, \ldots, p-1)$$

and so

$$\exp(\gamma_j) = 1 + i\rho^j.$$

Thus we have

$$\prod_{j=1}^{p-1}{}' (1 + i\rho^j) = \prod_{j=1}^{p-1}{}' \exp(\gamma_j) = \exp\left(\sum_{j=1}^{p-1}{}' \gamma_j\right).$$

Now

$$\begin{aligned} \sum_{j=1}^{p-1}{}' \gamma_j &= \sum_{j=1}^{p-1}{}' \sum_{n=1}^{\infty} \frac{(-1)^{n-1}\, i^n \rho^{jn}}{n} \\ &= \sum_{n=1}^{\infty} \frac{(-1)^{n-1}\, i^n}{n} \sum_{j=1}^{p-1}{}' \rho^{jn} \\ &= \frac{1}{2} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}\, i^n}{n} \left\{ p - 1 - \left(\frac{n}{p}\right)\sqrt{-p} - \left(\frac{n}{p}\right)^2 p \right\}, \end{aligned}$$

where we have again used the evaluation of the Gauss sum in the form which includes $n \equiv 0 \pmod p$. After a little simplification we obtain

$$\sum_{j=1}^{p-1}{}' \gamma_j = \frac{1}{2} \sum_{n=1}^{\infty} \frac{(-i)^n - i^n}{n} + \frac{1}{2}\sqrt{-p} \sum_{n=1}^{\infty} \frac{(-i)^n}{n} \left(\frac{n}{p}\right).$$

Now

$$\sum_{n=1}^{\infty} \frac{(-i)^n - i^n}{n} = -2i \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} = -\frac{\pi i}{2}$$

and

$$\sum_{n=1}^{\infty} \frac{(-i)^n}{n} \left(\frac{n}{p}\right) = \frac{1}{2} \left(\frac{2}{p}\right) \sum_{n=1}^{\infty} \frac{(-1)^n}{n} \left(\frac{n}{p}\right) - i \sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} \left(\frac{2n+1}{p}\right).$$

From Dirichlet's class number formulae for $Q(\sqrt{-p})$ and $Q(\sqrt{p})$ (see, for example, [1, p. 343]), we deduce easily that

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

and

$$\sum_{n=0}^{\infty} \left(\frac{2n+1}{p}\right) \frac{(-1)^n}{2n+1} = \frac{h(p)}{\sqrt{p}} \log \varepsilon_p,$$

so that

$$\sum_{n=1}^{\infty} \frac{(-i)^n}{n} \left(\frac{n}{p}\right) = \frac{\pi h(-p)}{2\sqrt{p}} \left(1 - \left(\frac{2}{p}\right)\right) - \frac{ih(p)}{\sqrt{p}} \log \varepsilon_p.$$

Hence

$$\sum_{j=1}^{p-1}{}' \gamma_j = -\frac{\pi i}{4} + \frac{\pi i h(-p)}{4} \left(1 - \left(\frac{2}{p}\right)\right) + \frac{h(p)}{2} \log \varepsilon_p$$

and so

$$\prod_{j=1}^{p-1}{}' (1 + i\rho^j) = \omega^{-1} i^{1/2(1-(2/p))h(-p)} \varepsilon_p^{h(p)/2}$$

giving

$$\begin{aligned} F_-(i) &= \omega^{-1} i^{(p-1)/2 + 1/2(1-(2/p))h(-p)} \varepsilon_p^{h(p)/2} \\ &= \omega^7 (-1)^{1/2(h(-p)+1)} \varepsilon_p^{h(p)/2}, \qquad \text{if } p \equiv 3 \pmod 8, \\ &= \omega^5 \varepsilon_p^{h(p)/2}, \qquad \text{if } p \equiv 7 \pmod 8). \end{aligned}$$

The value of $F_+(i)$ now follows from (6.2) and (6.3). For the values of $F_\pm(-i)$ we have only to note that

$$F_\pm(-i) = \prod_{\substack{j=1 \\ \left(\frac{j}{p}\right)=\pm 1}}^{p-1} (-i-\rho^j) = \prod_{\substack{j=1 \\ \left(\frac{j}{p}\right)=\mp 1}}^{p-1} (-i-\rho^{-j}) = \overline{F_\mp(i)}.$$

8. The Polynomials $Y(z)$ and $Z(z)$

$F_\pm(z)$ are polynomials in z of degree $\frac{1}{2}(p-1)$ with coefficients in the ring of integers of $Q(\sqrt{-p})$ (see [3]). Hence we can write

$$F_+(z) = \tfrac{1}{2}(Y(z) - Z(z)\sqrt{-p}), \qquad F_-(z) = \tfrac{1}{2}(Y(z) + Z(z)\sqrt{-p}), \quad (8.1)$$

where $Y(z)$ and $Z(z)$ are polynomials with rational integer coefficients. Clearly we have

$$Y(z) = F_-(z) + F_+(z), \qquad Z(z) = \frac{F_-(z) - F_+(z)}{\sqrt{-p}}. \quad (8.2)$$

Taking $z = 1, -1, i$ in (8.2) and appealing to Lemma 3 we obtain

$$Y(1) = 0, \qquad Z(1) = 2(-1)^{1/2(h(-p)-1)} \quad (8.3)$$

$$Y(-1) = 2(-1)^{1/4(p-3)}, \qquad Z(-1) = 0, \quad (8.4)$$

$$\left.\begin{aligned} Y(i) &= \omega^3(-1)^{1/2(h(-p)-1)}(\varepsilon_p^{h(p)/2} - \varepsilon_p^{-h(p)/2}), && \text{if } p \equiv 3 \pmod 8,\\ &= \omega^5(\varepsilon_p^{h(p)/2} + \varepsilon_p^{-h(p)/2}), && \text{if } p \equiv 7 \pmod 8,\\ Z(i) &= \omega^3(-1)^{1/2(h(-p)-1)}(\varepsilon_p^{h(p)/2} + \varepsilon_p^{-h(p)/2})/\sqrt{-p}, && \text{if } p \equiv 3 \pmod 8,\\ &= \omega^5(\varepsilon_p^{h(p)/2} - \varepsilon_p^{-h(p)/2})/\sqrt{-p}, && \text{if } p \equiv 7 \pmod 8. \end{aligned}\right\} \quad (8.5)$$

Since (using (2.1) and 2.3))

$$\varepsilon_p^{h(p)/2} = (T + U\sqrt{p})^{(h(p)-1)/2} \frac{(R + S\sqrt{p})}{\sqrt{2}}$$

and

$$\varepsilon_p^{-h(p)/2} = (T - U\sqrt{p})^{(h(p)-1)/2} \frac{(R - S\sqrt{p})}{\sqrt{2}} (-1)^{(p+1)/4},$$

we see from (8.5) that

$$\begin{aligned} Y(i) &= A_3(1-i), && \text{if} \quad p \equiv 3 \pmod 8, \\ &= A_7(1+i), && \text{if} \quad p \equiv 7 \pmod 8, \\ Z(i) &= -B_3(1+i), && \text{if} \quad p \equiv 3 \pmod 8, \\ &= B_7(1-i), && \text{if} \quad p \equiv 7 \pmod 8, \end{aligned} \tag{8.6}$$

for rational integers A_3, B_3, A_7, B_7 (see [3, Eq. (10)]). From (6.2) and (8.1) we have [3, Eq. (6)])

$$Y(z)^2 + pZ(z)^2 = 4F(z). \tag{8.7}$$

Taking $z = i$ in (8.7), and using (6.3) and (8.6), we obtain (see [3, Eq. (12)])

$$\begin{cases} A_3^2 - pB_3^2 = -2, & \text{if} \quad p \equiv 3 \pmod 8, \\ A_7^2 - pB_7^2 = +2, & \text{if} \quad p \equiv 7 \pmod 8). \end{cases} \tag{8.8}$$

Clearly (8.8) shows that A_3, B_3, A_7, B_7 are all odd.

9. The Polynomials $Y'(z)$ and $Z'(z)$

Differentiating (8.7) with respect to z, we obtain

$$Y(z)\,Y'(z) + pZ(z)\,Z'(z) = 2F'(z) \tag{9.1}$$

(see [3, Eq. (9)]). In [7, Eq. (14)] the following identity of Liouville was noted

$$Z(z)\,Y'(z) - Y(z)\,Z'(z) = 2G(z), \tag{9.2}$$

where

$$G(z) = \frac{1}{z-1} \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) z^{p-1-j}. \tag{9.3}$$

Solving (9.1) and (9.2) simultaneously for $Y'(z)$ and $Z'(z)$, we obtain (making use of (8.7))

$$\begin{cases} Y'(z) = \dfrac{F'(z)\,Y(z) + pG(z)\,Z(z)}{2F(z)}, \\[2ex] Z'(z) = \dfrac{-G(z)\,Y(z) + F'(z)\,Z(z)}{2F(z)}. \end{cases} \tag{9.4}$$

Since

$$G(1) = ph(-p), \qquad \left(\text{recalling } \sum_{j=1}^{p-1} j\left(\frac{j}{p}\right) = -ph(-p)\right), \tag{9.5}$$

$$G(-1) = \left\{1 - 2\left(\frac{2}{p}\right)\right\} h(-p), \quad \left(\text{using } \sum_{j=1}^{1/2(p-1)} \left(\frac{j}{p}\right) = \left(2 - \left(\frac{2}{p}\right)\right) h(-p)\right), \tag{9.6}$$

$$G(i) = \left\{2 - \left(\frac{2}{p}\right)\right\} h(-p), \qquad (\text{see [7, Eq. (17)]}) \tag{9.7}$$

we have

$$Y'(1) = (-1)^{1/2(h(-p)-1)}\, ph(-p), \qquad Z'(1) = (-1)^{1/2(h(-p)-1)}\, \frac{p-1}{2}, \tag{9.8}$$

$$Y'(-1) = \left(\frac{2}{p}\right)\frac{p-1}{2}, \qquad Z'(-1) = \left\{\left(\frac{2}{p}\right) - 2\right\} h(-p), \tag{9.9}$$

$$\begin{aligned}
Y'(i) &= \frac{1}{2}(A_3 - 3ph(-p)\,B_3) + \frac{i}{2}(-pA_3 + 3ph(-p)\,B_3), && \text{if } p \equiv 3 \pmod 8,\\
&= \frac{1}{2}(pA_7 - ph(-p)\,B_7 + \frac{i}{2}(A_7 - ph(-p)\,B_7), && \text{if } p \equiv 7 \pmod 8,\\
Z'(i) &= \frac{1}{2}(3h(-p)\,A_3 - pB_3) + \frac{i}{2}(3h(-p)\,A_3 - B_3), && \text{if } p \equiv 3 \pmod 8,\\
&= \frac{1}{2}(-h(-p)\,A_7 + B_7) + \frac{i}{2}(h(-p)\,A_7 - pB_7), && \text{if } p \equiv 7 \pmod 8.
\end{aligned} \tag{9.10}$$

10. $h(-p)$ Determined Modulo 8

In [7, Eq. (20)] we showed that

$$\begin{aligned}
h(-p) &\equiv -A_3B_3 \pmod 4, \qquad \text{if } p \equiv 3 \pmod 8,\\
&\equiv -A_7B_7 \pmod 4, \qquad \text{if } p \equiv 7 \pmod 8.
\end{aligned} \tag{10.1}$$

Our next task in this paper is to extend (10.1) to a congruence modulo 8. We prove

LEMMA 4.

$$h(-p) \equiv A_3 B_3 + 2B_3 \pmod 8, \quad \text{if } p \equiv 3 \pmod 8,$$
$$\equiv A_7 B_7 + 2B_7 \pmod 8, \quad \text{if } p \equiv 7 \pmod 8.$$

Proof. It is known that $Y(z)$ and $Z(z)$ have the form (see [7, Eq. (7)])

$$Y(z) = \sum_{n=0}^{(p-3)/4} a_n (z^{(p-1)/2-n} - z^n), \quad Z(z) = \sum_{n=0}^{(p-3)/4} b_n (z^{(p-1)/2-n} + z^n), \tag{10.2}$$

where the a_n and b_n are integers. (This is a consequence of the easily proved result $z^{(p-1)/2} F_\pm(\frac{1}{z}) = -F_\mp(z)$ $(z \neq 0)$.) Differentiating (10.2) with respect to z we obtain (see [7, Eq. (8)])

$$\begin{cases} Y'(z) = \displaystyle\sum_{n=0}^{(p-3)/4} a_n \left(\left(\frac{p-1}{2} - n \right) z^{(p-3)/2-n} - nz^{n-1} \right), \\ Z'(z) = \displaystyle\sum_{n=0}^{(p-3)/2} b_n \left(\left(\frac{p-1}{2} - n \right) z^{(p-3)/2-n} + nz^{n-1} \right). \end{cases} \tag{10.3}$$

We now consider two cases according as $p \equiv 3$ or $7 \pmod 8$, just providing the details when $p \equiv 3 \pmod 8$. With $p = 8l + 3$, taking $z = i$ in (10.3) we obtain

$$\begin{aligned} Y'(i) = {} & \\ & \left\{ \sum_{0 \leqslant m \leqslant l/2} a_{4m}(4l - 4m + 1) - \sum_{0 \leqslant m \leqslant (l-1)/2} a_{4m+1}(4m + 1) \right. \\ & \left. + \sum_{0 \leqslant m \leqslant (l-1)/2} a_{4m+2}(4m - 4l + 1) + \sum_{0 \leqslant m < l/2 - 1} a_{4m+3}(4m + 3) \right\} \\ & + i \left\{ \sum_{0 \leqslant m \leqslant l/2} a_{4m} 4m - \sum_{0 \leqslant m \leqslant (l-1)/2} a_{4m+1} 4(l - m) - \sum_{0 \leqslant m \leqslant (l-1)/2} a_{4m+2}(4m + 2) \right. \\ & \left. + \sum_{0 \leqslant m \leqslant l/2 - 1} a_{4m+3}(4l - 4m - 2) \right\}. \end{aligned}$$

Hence from (9.10) we have

$$\begin{aligned} \tfrac{1}{2}(A_3 - 3ph(-p)\, B_3) = {} & \sum_{0 \leqslant m \leqslant l/2} a_{4m} - \sum_{0 \leqslant m \leqslant (l-1)/2} a_{4m+1} + \sum_{0 \leqslant m \leqslant (l-1)/2} a_{4m+2} \\ & - \sum_{0 \leqslant m \leqslant l/2 - 1} a_{4m+3} \pmod 4 \end{aligned}$$

$$\equiv \sum_{0\leqslant m\leqslant l} a_{2m} - \sum_{0\leqslant m\leqslant l-1} a_{2m+1} \pmod 4$$
$$= -\tfrac{1}{2}Y(-1) \qquad \text{(by (10.2))}$$
$$= -1 \qquad \text{(by (8.4))}$$

so

$$A_3 - 3ph(-p)\,B_3 \equiv -2 \pmod 8,$$

and thus

$$h(-p) \equiv A_3B_3 + 2B_3 \pmod 8.$$

Similarly, with $p = 8l + 7$, we obtain

$$h(-p) \equiv A_7B_7 + 2B_7 \pmod 8.$$

11. Consideration of $(R + S\sqrt{p})^{h(p)}$

From (8.1) and (8.6) we have

$$F_-(i) = \frac{1}{2}\,(Y(i) + Z(i)\sqrt{-p})$$

$$= \begin{cases} \dfrac{1}{2}\,(A_3(1-i) - B_3(1+i)\,i\sqrt{p}), & \text{if } p \equiv 3 \pmod 8, \\[2ex] \dfrac{1}{2}\,(A_7(1+i) + B_7(1-i)\,i\sqrt{p}), & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

$$= \begin{cases} \dfrac{1-i}{2}\,(A_3 + B_3\sqrt{p}), & \text{if } p \equiv 3 \pmod 8, \\[2ex] \dfrac{1+i}{2}\,(A_7 + B_7\sqrt{p}), & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

$$= \begin{cases} \dfrac{\omega^7}{\sqrt{2}}\,(A_3 + B_3\sqrt{p}), & \text{if } p \equiv 3 \pmod 8, \\[2ex] \dfrac{\omega}{\sqrt{2}}\,(A_7 + B_7\sqrt{p}), & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

On the other hand, from Lemma 3, we have

$$F_-(i) = \begin{cases} \omega^7(-1)^{1/2(h(-p)+1}\,\varepsilon_p^{h(p)/2}, & \text{if } p \equiv 3 \pmod 8, \\ \omega^5\varepsilon_p^{h(p)/2}, & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

$$= \begin{cases} \dfrac{\omega^7}{2^{h(p)/2}} (-1)^{1/2(h(-p)+1)} (R + S\sqrt{p})^{h(p)}, & \text{if } p \equiv 3 \pmod 8, \\ \dfrac{\omega^5}{2^{h(p)/2}} (R + S\sqrt{p})^{h(p)}, & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Equating these two expressions for $F_-(i)$ we obtain

LEMMA 5.

$$\begin{aligned} &(R + S\sqrt{p})^{h(p)} \\ &\quad = (-1)^{(h(-p)+1)/2}\, 2^{(h(p)-1)/2}(A_3 + B_3\sqrt{p}), \qquad \text{if } p \equiv 3 \pmod 8, \\ &\quad = -2^{(h(p)-1)/2}(A_7 + B_7\sqrt{p}), \qquad \text{if } p \equiv 7 \pmod 8. \end{aligned}$$

We next expand $(R + S\sqrt{p})^{h(p)}$ in such a way that, using Lemma 5, we can obtain A_3, B_3, A_7, B_7 as polynomials in R and S with integral coefficients. This is done by using the following well-known identity (see, for example, [6])

$$\alpha^{2m+1} + \beta^{2m+1} = \sum_{j=0}^{m} (-1)^j \frac{2m+1}{2m+1-j} \binom{2m+1-j}{j} (\alpha+\beta)^{2m+1-2j} (\alpha\beta)^j. \tag{11.1}$$

Taking $\alpha = R + S\sqrt{p}$ and $\beta = \pm(R - S\sqrt{p})$ in (11.1) and adding, we obtain (as $R^2 - pS^2 = (-1)^{(p+1)/4}\, 2$)

$$\begin{aligned} &(R + S\sqrt{p})^{2m+1} \\ &\quad = \sum_{j=0}^{m} (-1)^{((p-3)/4)j} \frac{2m+1}{2m+1-j} \binom{2m+1-j}{j} 2^{2m-j} R^{2(m-j)+1} \\ &\qquad + \sqrt{p} \sum_{j=0}^{m} (-1)^{((p+1)/4)j} \frac{2m+1}{2m+1-j} \binom{2m+1-j}{j} \\ &\qquad \times 2^{2m-j} p^{m-j} S^{2(m-j)+1}. \end{aligned}$$

Changing the summation variable from j to $k = m - j$, and noting that

$$\frac{2m+1}{2m+1-j} \binom{2m+1-j}{j} = \frac{2m+1}{m+k+1} \binom{m+k+1}{m-k} = \frac{2m+1}{2k+1} \binom{m+k}{m-k},$$

we obtain

$$(R+S\sqrt{p})^{2m+1} = \sum_{k=0}^{m} (-1)^{((p-3)/4)(m-k)} \frac{2m+1}{2k+1}\binom{m+k}{m-k} 2^{m+k}R^{2k+1}$$
$$+\sqrt{p}\sum_{k=0}^{m} (-1)^{((p+1)/4)(m-k)} \frac{2m+1}{2k+1}\binom{m+k}{m-k}$$
$$\times 2^{m+k}p^kS^{2k+1}.$$

Taking $m=\frac{1}{2}(h(p)-1)$ in this identity and applying Lemma 5 we obtain

LEMMA 6. (i) $p\equiv 3 \pmod 8$

$$A_3 = (-1)^{(h(-p)+1)/2}h(p) \sum_{k=0}^{(h(p)-1)/2} \frac{2^k}{2k+1}\binom{(h(p)+2k-1)/2}{(h(p)-2k-1)/2} R^{2k+1},$$

$$B_3 = (-1)^{(h(-p)+h(p))/2}h(p) \sum_{k=0}^{(h(p)-1)/2} \frac{(-1)^k 2^k}{2k+1}$$
$$\times \binom{(h(p)+2k-1)/2}{(h(p)-2k-1)/2} p^kS^{2k+1}.$$

(ii) *If* $p\equiv 7 \pmod 8$

$$A_7 = (-1)^{(h(p)+1)/2}\, h(p) \sum_{k=0}^{(h(p)-1)/2} \frac{(-1)^k 2^k}{2k+1}\binom{(h(p)+2k-1)/2}{(h(p)-2k-1)/2} R^{2k+1},$$

$$B_7 = -h(p) \sum_{k=0}^{(h(p)-1)/2} \frac{2^k}{2k+1}\binom{(h(p)+2k-1)/2}{(h(p)-2k-1)/2} p^kS^{2k+1}.$$

Reducing the expressions in Lemma 6 modulo 8, we obtain (using 4.2)).

LEMMA 7. (i) *If* $p\equiv 3 \pmod 8$ *then*

$$(A_3,B_3) \equiv (7(-1)^{(R+S)/2}R,\ 7(-1)^{(R+S)/2}S) \pmod 8, \quad \text{if } h(p)\equiv 1 \pmod 8,$$
$$\equiv (5(-1)^{(R+S)/2}R,\ 3(-1)^{(R+S)/2}S) \pmod 8, \quad \text{if } h(p)\equiv 3 \pmod 8,$$
$$\equiv (5(-1)^{(R+S)/2}R,\ 5(-1)^{(R+S)/2}S) \pmod 8, \quad \text{if } h(p)\equiv 5 \pmod 8,$$
$$\equiv (7(-1)^{(R+S)/2}R,\ (-1)^{(R+S)/2}S) \pmod 8, \quad \text{if } h(p)\equiv 7 \pmod 8.$$

(ii) *If* $p \equiv 7 \pmod 8$ *then*

$$\begin{aligned}(A_7, B_7) &\equiv (7R, 7S) \pmod 8, && \text{if } h(p) \equiv 1 \pmod 8,\\ &\equiv (R, 7S) \pmod 8, && \text{if } h(p) \equiv 3 \pmod 8,\\ &\equiv (R, S) \pmod 8, && \text{if } h(p) \equiv 5 \pmod 8,\\ &\equiv (7R, S) \pmod 8, && \text{if } h(p) \equiv 7 \pmod 8.\end{aligned}$$

The next lemma tells us the congruence classes of (A_3, B_3) and (A_7, B_7) modulo 8.

LEMMA 8. (a) *If* $p \equiv 3 \pmod{16}$ *then*

$$(A_3, B_3) = (1, 1),\ (1, 7),\ (3, 3) \text{ or } (3, 5) \pmod 8.$$

(b) *If* $p \equiv 7 \pmod{16}$ *then*

$$(A_7, B_7) \equiv (3, 1),\ (3, 7),\ (5, 1) \text{ or } (5, 7) \pmod 8.$$

(c) *If* $p \equiv 11 \pmod{16}$ *then*

$$(A_3, B_3) \equiv (5, 1),\ (5, 7),\ (7, 3) \text{ or } (7, 5) \pmod 8.$$

(d) *If* $p \equiv 15 \pmod{16}$ *then*

$$(A_7, B_7) \equiv (1, 1),\ (1, 7),\ (7, 1) \text{ or } (7, 7) \pmod 8.$$

Proof. We just provide the details for $p \equiv 3 \pmod{16}$. By Lemma 1 we have

$$(-1)^{(R+S)/2} R \equiv 5 \text{ or } 7 \pmod 8,$$

and by Lemma 7 we have

$$A_3 \equiv 5(-1)^{(R+S)/2} R \text{ or } 7(-1)^{(R+S)/2} R \pmod 8,$$

so

$$A_3 \equiv 1 \text{ or } 3 \pmod 8.$$

If $A_3 \equiv 1 \pmod 8$, $B_3^2 \equiv 11pB_3^2 \equiv 11(A_3^2 + 2) \equiv 1 \pmod{16}$,

$$B_3 \equiv 1, 7 \pmod 8.$$

If $A_3 \equiv 3 \pmod 8$, $B_3^2 \equiv 11pB_3^2 \equiv 11(A_3^2 + 2) \equiv 9 \pmod{16}$,

$$B_3 \equiv 3, 5 \pmod 8.$$

Putting together Lemmas 4 and 8 we obtain

LEMMA 9. (a) *If* $p \equiv 3 \pmod{16}$ *then*

$$\begin{aligned} h(-p) &\equiv 1 \pmod 8, && \textit{if} \quad (A_3, B_3) \equiv (3, 5) \pmod 8,\\ &\equiv 3 \pmod 8, && \textit{if} \quad (A_3, B_3) \equiv (1, 1) \pmod 8,\\ &\equiv 5 \pmod 8, && \textit{if} \quad (A_3, B_3) \equiv (1, 7) \pmod 8,\\ &\equiv 7 \pmod 8, && \textit{if} \quad (A_3, B_3) \equiv (3, 3) \pmod 8. \end{aligned}$$

(b) *If* $p \equiv 7 \pmod{16}$ *then*

$$\begin{aligned} h(-p) &\equiv 1 \pmod 8, && \textit{if} \quad (A_7, B_7) \equiv (5, 7) \pmod 8,\\ &\equiv 3 \pmod 8, && \textit{if} \quad (A_7, B_7) \equiv (3, 7) \pmod 8,\\ &\equiv 5 \pmod 8, && \textit{if} \quad (A_7, B_7) \equiv (3, 1) \pmod 8,\\ &\equiv 7 \pmod 8, && \textit{if} \quad (A_7, B_7) \equiv (5, 1) \pmod 8. \end{aligned}$$

(c) *If* $p \equiv 11 \pmod{16}$ *then*

$$\begin{aligned} h(-p) &\equiv 1 \pmod 8, && \textit{if} \quad (A_3, B_3) \equiv (5, 7) \pmod 8,\\ &\equiv 3 \pmod 8, && \textit{if} \quad (A_3, B_3) \equiv (7, 3) \pmod 8),\\ &\equiv 5 \pmod 8, && \textit{if} \quad (A_3, B_3) \equiv (7, 5) \pmod 8,\\ &\equiv 7 \pmod 8, && \textit{if} \quad (A_3, B_3) \equiv (5, 1) \pmod 8. \end{aligned}$$

(d) *If* $p \equiv 15 \pmod{16}$ *then*

$$\begin{aligned} h(-p) &\equiv 1 \pmod 8, && \textit{if} \quad (A_7, B_7) \equiv (7, 1) \pmod 8,\\ &\equiv 3 \pmod 8, && \textit{if} \quad (A_7, B_7) \equiv (1, 1) \pmod 8,\\ &\equiv 5 \pmod 8, && \textit{if} \quad (A_7, B_7) \equiv (1, 7) \pmod 8,\\ &\equiv 7 \pmod 8, && \textit{if} \quad (A_7, B_7) \equiv (7, 7) \pmod 8. \end{aligned}$$

12. PROOF OF THEOREM

The theorem now follows easily from Lemmas 1, 7 and 9. We just give the details when $p \equiv 3 \pmod{16}$, as the other cases can be treated similarly (see Table).

We remark that tables of $h(p)$, $h(-p)$ and ε_p show that every one of the 64 possible cases of $(h(p), R, S) \pmod 8$ actually occurs.

Next we give a single numerical example to illustrate the theorem. We take $p = 9539 \equiv 3 \pmod{16}$. In this case

$$\varepsilon_p = \tfrac{1}{2}(293 + 3\sqrt{9539})^2,$$

TABLE I

$h(p)$ (mod 8)	R(mod 8) (from Lemma 1)	S(mod 8)	A_3(mod 8) (from Lemma 7)	B_3(mod 8)	$h(-p)$(mod 8) (from Lemma 9)	$h(-p) + (-1)^{(R-S)/2} h(p)$ (mod 8)
1	1	1	1	1	3	4
1	3	3	3	3	7	0
1	5	3	3	5	1	0
1	7	1	1	7	5	4
3	1	1	3	5	1	4
3	3	3	1	7	5	0
3	5	3	1	1	3	0
3	7	1	3	3	7	4
5	1	1	3	3	7	4
5	3	3	1	1	3	0
5	5	3	1	7	5	0
5	7	1	3	5	1	4
7	1	1	1	7	5	4
7	3	3	3	5	1	0
7	5	3	3	3	7	0
7	7	1	1	1	3	4

so $R = 293 \equiv 5 \pmod 8$, $S \equiv 3 \pmod 8$. Thus by the theorem $h(-p) - h(p) \equiv 0 \pmod 8$. Indeed $h(-p) = 55$, $h(p) = 7$.

Finally we remark that as (appealing to (2.3) and (2.4))

$$\left(\frac{T}{U}\right) = \left(\frac{-1}{S}\right), \qquad \text{if} \quad p \equiv 3 \pmod 8,$$
$$= \left(\frac{-1}{R}\right), \qquad \text{if} \quad p \equiv 7 \pmod 8,$$

the theorem can also be formulated in the form

THEOREM′.

$$h(-p) \equiv h(p)\left(2 + pU - 2\left(\frac{T}{U}\right)\right) \pmod 8.$$

ACKNOWLEDGMENTS

The author acknowledges a remark of Pierre Kaplan (University of Nancy) which simplified his original proof of Lemma 3. He would also like to thank Mr. Lee-Jeff Bell who did some computing for him in connection with this paper.

References

1. Z. I. Borevich and I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.
2. E. Brown, The power of 2 dividing the class number of a binary quadratic discriminant, *J. Number Theory* **5** (1973), 413–419.
3. E. Brown, Class numbers of real quadratic number fields, *Trans. Amer. Math. Soc.* **190** (1974), 99–107.
4. E. L. Ince, Cycles of reduced ideals in quadratic fields, *in* "Mathematical Tables Volume IV," British Association for the Advancement of Science, London, 1934.
5. Pierre Kaplan and Kenneth S. Williams, Congruence modulo 16 for the class numbers of the quadratic fields $Q(\sqrt{\pm p})$ and $Q(\sqrt{\pm 2p})$ for p a prime congruent to 5 modulo 8, to appear.
6. Kenneth S. Williams, A generalisation of Cardan's solution of the cubic, *Math. Gaz.* **46** (1962), 221–223.
7. K. S. Williams, The class number of $Q(\sqrt{-p})$ modulo 4, for $p \equiv 3 \pmod 4$ a prime, *Pacific J. Math.* **83** (1979), 565–570.
8. K. S. Williams, On the class number of $Q(\sqrt{-p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime, *Acta Arith.*, in press.
9. K. S. Williams, The class number of $Q(\sqrt{-2p})$ modulo 8, for $p \equiv 5 \pmod 8$ a prime, *Rocky Mountain J. Math.* **11** (1981), 19–26.
10. K. S. Williams, On the class number of $Q(\sqrt{\pm 2p})$ modulo 16, for $p \equiv 1 \pmod 8$ a prime, *Acta Arith.*, in press.
11. K. S. Williams, The class number of $Q(\sqrt{p})$ modulo 4, for $p \equiv 5 \pmod 8$ a prime, *Pacific J. Math*, in press.