ACTA ARITHMETICA
XXXIX (1981)

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

by

KENNETH S. WILLIAMS* (Ottawa, Ontario)

1. Introduction. Throughout this paper p denotes a prime congruent to 1 modulo 8, and we set $p = 8l+1$. For such primes, the class number $h(-p)$ of the imaginary quadratic field $Q(\sqrt{-p})$ satisfies

(1.1) $$h(-p) \equiv 0 \pmod 4,$$

see for example [1], p. 413, and the class number $h(p)$ of the real quadratic field $Q(\sqrt{p})$ satisfies

(1.2) $$h(p) \equiv 1 \pmod 2,$$

see for example [2], p. 100. The fundamental unit ε_p (>1) of the real quadratic field $Q(\sqrt{p})$ has norm -1 and can be written in the form

(1.3) $$\varepsilon_p = T+U\sqrt{p},$$

where T and U are positive integers such that

(1.4) $$T \equiv 0 \pmod 4, \qquad U \equiv 1 \pmod 4.$$

Recently Lehmer ([8], p. 48), Cohn and Cooke ([3], p. 368) and Kaplan ([6], p. 240) have proved that

(1.5) $$h(-p) \equiv T \pmod 8.$$

It is our purpose to determine $h(-p)$ modulo 16.

We prove

THEOREM. *If $p \equiv 1 \pmod 8$ is a prime, then*

(1.6)
$$\begin{cases} h(-p) \equiv T+(p-1) \pmod{16}, & \textit{if} \quad h(-p) \equiv 0 \pmod 8, \\ h(-p) \equiv T+(p-1)+4\big(h(p)-1\big) \pmod{16}, & \textit{if} \quad h(-p) \equiv 4 \pmod 8. \end{cases}$$

* Research supported under Natural Sciences and Engineering Research Council of Canada Grant No. A-7233.

We set $\varrho = \exp(2\pi i/p)$. The cyclotomic polynomial $F(z)$ of index p in the complex variable z is given by

$$(1.7)\qquad F(z) = \frac{z^p-1}{z-1} = \prod_{j=1}^{p-1}(z-\varrho^j) = z^{p-1}+\ldots+z+1.$$

We have

$$(1.8)\qquad F(z) = F_+(z)F_-(z),$$

where $F_+(z)$ and $F_-(z)$ are polynomials of degree $\frac{1}{2}(p-1)$ given by

$$(1.9)\qquad F_+(z) = \prod_{\substack{j=1\\ \left(\frac{j}{p}\right)=+1}}^{p-1}(z-\varrho^j),\qquad F_-(z) = \prod_{\substack{j=1\\ \left(\frac{j}{p}\right)=-1}}^{p-1}(z-\varrho^j).$$

The method used to prove the theorem is completely elementary. We sketch the ideas involved. In §§ 2–4 Dirichlet's class number formulae for $h(p)$ and $h(-p)$ are used to evaluate $F_\pm(1)$ (Lemma 1), $F_\pm(-1)$ (Lemma 2) and $F_\pm(i)$ (Lemma 3). From these evaluations certain linear congruences and equations are obtained (Corollaries 1, 2, 3) for the coefficients a_n and b_n of the polynomials $Y(z) = F_-(z)+F_+(z)$ and $Z(z) = \frac{1}{\sqrt{p}}\big(F_-(z)-F_+(z)\big)$. In § 5 these congruences and equations are combined to give further congruences (Lemma 4) which are required in § 6. In § 6 the quantities $Y(\omega)$, $Z(\omega)$, $Y'(\omega)$, $Z'(\omega)$ ($\omega = 1+i/\sqrt{2}$), are given in terms of the a_n and b_n, and certain equations derived (Lemmas 5 and 6). Finally in § 7 using Dirichlet's class number formulae for $h(-p)$ and $h(-2p)$ and an identity of Liouville, $h(-p)$ is expressed in terms of $Y(\pm\omega)$, $Z(\pm\omega)$, $Y'(\pm\omega)$, $Z'(\pm\omega)$, and the theorem follows by appealing to Lemmas 5 and 6.

2. Evaluation of $F_+(1)$ and $F_-(1)$. Using Dirichlet's class number formula for $h(p)$, we prove

LEMMA 1. *If $p \equiv 1 \pmod 8$ is prime, then*

$$F_+(1) = -\sqrt{p}(T-U\sqrt{p})^{h(p)},\qquad F_-(1) = \sqrt{p}(T+U\sqrt{p})^{h(p)}.$$

Proof. By Dirichlet's class number formula for $h(p)$ (see for example [7], p. 227), we have

$$(2.1)\qquad \varepsilon_p^{2h(p)} = \prod_{\substack{j=1\\ \left(\frac{j}{p}\right)=-1}}^{p-1}\sin\frac{\pi j}{p}\Big/\prod_{\substack{j=1\\ \left(\frac{j}{p}\right)=+1}}^{p-1}\sin\frac{\pi j}{p}.$$

It is well-known (see for example [11], p. 173) that

$$(2.2)\qquad 2^{p-1}\prod_{\substack{j=1\\ \left(\frac{j}{p}\right)=-1}}^{p-1}\sin\frac{\pi}{p}\prod_{\substack{j=1\\ \left(\frac{j}{p}\right)=+1}}^{1}\sin\frac{\pi j}{p}=\prod_{j=1}^{p-1}2\sin\frac{\pi j}{p}=p.$$

Multiplying (2.1) and (2.2) together we obtain

$$(2.3)\qquad p\varepsilon_p^{2h(p)}=2^{p-1}\Big\{\prod_{j=1}^{p-1}{}'\sin\frac{\pi j}{p}\Big\},$$

where, here and throughout the rest of the paper, we use a prime (′) to indicate that the product or summation variable is restricted to quadratic non-residues (mod p). Since $\varepsilon_p>1$ and each $\sin(\pi j/p)>0$ $(j=1,\ldots$ $\ldots,p-1)$ we have

$$(2.4)\qquad \sqrt{p}\varepsilon_p^{h(p)}=2^{(p-1)/2}\prod_{j=1}^{p-1}{}'\sin\frac{\pi j}{p}=\prod_{j=1}^{p-1}{}'2\sin\frac{\pi j}{p}.$$

Now, for $j=1,\ldots,p-1$, we have

$$2\sin\frac{\pi j}{p}=i\varrho^{-j/2}(1-\varrho^j),$$

so, as

$$\sum_{j=1}^{p-1}{}'j=p(p-1)/4,$$

(2.4) gives $F_-(1)=\sqrt{p}\,\varepsilon_p^{h(p)}=\sqrt{p}(T+U\sqrt{p})^{h(p)}$ as required.

Finally, as $h(p)\equiv 1\pmod 2$ and the norm of ε_p is -1, we have

$$F_+(1)=\frac{F(1)}{F_-(1)}=\frac{p}{\sqrt{p}(T+U\sqrt{p})^{h(p)}}=-\sqrt{p}(T-U\sqrt{p})^{h(p)}.$$

This completes the proof of Lemma 1.

It is clear from (1.9) that $F_+(z)$ and $F_-(z)$ are polynomials in z of degree $\frac{1}{2}(p-1)$ with coefficients in the ring of integers of $Q(\sqrt{p})$ (see for example [10], p. 215). Hence we can write

$$(2.5)\qquad F_+(z)=\tfrac{1}{2}\big(Y(z)-Z(z)\sqrt{p}\big),\qquad F_-(z)=\tfrac{1}{2}\big(Y(z)+Z(z)\sqrt{p}\big),$$

where $Y(z)$ and $Z(z)$ are polynomials of degree at most $\frac{1}{2}(p-1)$ with rational integral coefficients. From (2.5) we have

$$(2.6)\qquad Y(z)=F_-(z)+F_+(z),\qquad Z(z)=\frac{1}{\sqrt{p}}\big(F_-(z)-F_+(z)\big).$$

It is easily verified from (1.9) that for $z \neq 0$

$$z^{(p-1)/2} F_{\pm}\left(\frac{1}{z}\right) = F_{\pm}(z),$$

so that by (2.6) we have

$$z^{(p-1)/2} Y\left(\frac{1}{z}\right) = Y(z), \quad z^{(p-1)/2} Z\left(\frac{1}{z}\right) = Z(z).$$

Hence the coefficient of z^n ($n = 0, 1, 2, \ldots, (p-5)/4$) in $Y(z)$ (resp. $Z(z)$) is the same as that of $z^{(p-1)/2-n}$ in $Y(z)$ (resp. $Z(z)$). Moreover, by (2.6) and Lemma 1, $Y(1)$ and $Z(1)$ are both even, so the middle coefficients of $Y(z)$ and $Z(z)$ are both even. Hence we can set

$$(2.7) \qquad \begin{aligned} Y(z) &= \sum_{n=0}^{2l} a_n (z^n + z^{4l-n}), \\ Z(z) &= \sum_{n=0}^{2l} b_n (z^n + z^{4l-n}), \end{aligned}$$

where the a_n and b_n are integers. It is known (see for example [12], pp. 210–212) that

$$a_0 = 2, \; a_1 = 1, \; a_2 = \tfrac{1}{4}(p+3), \ldots,$$

$$b_0 = 0, \; b_1 = 1, \; b_2 = 1, \ldots$$

Appealing to Lemma 1 we obtain

Corollary 1. *If $p = 8l+1$ is a prime, then*

$$\sum_{n=0}^{2l} a_n \equiv 1-4l \pmod{16}, \quad \sum_{n=0}^{2l} b_n \equiv T \pmod{16}, \quad \text{if} \quad h(-p) \equiv 0 \pmod 8,$$

and

$$\sum_{n=0}^{2l} a_n \equiv 9-4l \pmod{16}, \quad \sum_{n=0}^{2l} b_n \equiv h(p) T \pmod{16},$$
$$\text{if} \quad h(-p) \equiv 4 \pmod 8.$$

Proof. If $h(-p) \equiv 0 \pmod 8$, by (1.5) we have $T \equiv 0 \pmod 8$. Then, as $T^2 - pU^2 = -1$ and $U \equiv 1 \pmod 4$, we have

$$(2.8) \qquad U \equiv 4l+1 \pmod{16}.$$

Hence, working modulo 16, we have

$$
\begin{aligned}
\sum_{n=0}^{2l} a_n &= \tfrac{1}{2}Y(1) && \text{(by (2.7))}\\
&= \tfrac{1}{2}\big(F_-(1)+F_+(1)\big) && \text{(by (2.6))}\\
&= \frac{\sqrt{p}}{2}\{(T+U\sqrt{p})^{h(p)}-(T-U\sqrt{p})^{h(p)}\} && \text{(by Lemma 1)}\\
&\equiv U^{h(p)}p^{(h(p)+1)/2} && \text{(as } h(p)\equiv 1 \pmod 2,\ T\equiv 0 \pmod 4)\\
&\equiv (4l+1)^{h(p)}(8l+1)^{(h(p)+1)/2} && \text{(by (2.8))}\\
&\equiv (4l+1)(8l+1)^{h(p)}\\
&\equiv (4l+1)(8l+1)\\
&\equiv 1-4l,
\end{aligned}
$$

and

$$
\begin{aligned}
\sum_{n=0}^{2l} b_n &= \tfrac{1}{2}Z(1) && \text{(by (2.7))}\\
&= \frac{1}{2\sqrt{p}}\big(F_-(1)-F_+(1)\big) && \text{(by (2.6))}\\
&= \tfrac{1}{2}\big((T+U\sqrt{p})^{h(p)}+(T-U\sqrt{p})^{h(p)}\big) && \text{(by Lemma 1)}\\
&\equiv h(p)TU^{h(p)-1}p^{(h(p)-1)/2} && \text{(as } T\equiv 0 \pmod 4)\\
&\equiv h(p)T(4l+1)^{h(p)-1}(8l+1)^{(h(p)-1)/2} && \text{(by (2.8))}\\
&\equiv h(p)T(8l+1)^{h(p)-1} && \text{(as } h(p)\equiv 1 \pmod 2)\\
&\equiv h(p)T && \text{(as } h(p)\equiv 1 \pmod 2)\\
&\equiv T && \text{(as } T\equiv 0 \pmod 8).
\end{aligned}
$$

The case $h(-p)\equiv 4 \pmod 8$ can be treated similarly. In this case we have $T\equiv 4 \pmod 8$ and $U\equiv 4l+9 \pmod{16}$.

3. Evaluation of $F_+(-1)$ and $F_-(-1)$. A simple argument proves

LEMMA 2. *If $p\equiv 1 \pmod 8$ is prime, then*

$$F_+(-1) = F_-(-1) = 1.$$

Proof. From (1.9) we have

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

As j runs through the quadratic non-residues modulo p, so does $2j$. Hence we have

$$\prod_{j=1}^{p-1}{}' (1-\varrho^{2j}) = \prod_{j=1}^{p-1}{}' (1-\varrho^{j}) = F_-(1),$$

giving

$$F_-(-1) = 1,$$

as $F_-(1) \neq 0$. Finally we have

$$F_+(-1) = \frac{F(-1)}{F_-(-1)} = 1.$$

This completes the proof of Lemma 2.

Appealing to Lemma 2 we obtain

COROLLARY 2. *If* $p = 8l+1$ *is prime, then*

$$\sum_{n=0}^{2l} (-1)^n a_n = 1, \quad \sum_{n=0}^{2l} (-1)^n b_n = 0.$$

Proof. We have

$$\begin{aligned}\sum_{n=0}^{2l} (-1)^n a_n &= \tfrac{1}{2} Y(-1) && \text{(by (2.7))}\\ &= \tfrac{1}{2}\big(F_-(-1)+F_+(-1)\big) && \text{(by (2.6))}\\ &= 1 && \text{(by Lemma 2)},\end{aligned}$$

and

$$\begin{aligned}\sum_{n=0}^{2l} (-1)^n b_n &= \tfrac{1}{2} Z(-1) && \text{(by (2.7))}\\ &= \frac{1}{2\sqrt{p}}\big(F_-(-1)-F_+(-1)\big) && \text{(by (2.6))}\\ &= 0 && \text{(by Lemma 2)}.\end{aligned}$$

4. Evaluation of $F_+(i)$ and $F_-(i)$. Using Dirichlet's class number formula for $h(-p)$, we prove

LEMMA 3. *If* $p \equiv 1 \pmod 8$ *is prime, then*

$$F_+(i) = F_-(i) = (-1)^{h(-p)/4}.$$

Proof. As $p \equiv 1 \pmod 8$, we have

$$F_-(i) = \prod_{j=1}^{p-1}{}' (i-\varrho^{j}) = \prod_{j=1}^{p-1}{}' (1+i\varrho^{j}), \tag{4.1}$$

so that

$$\overline{F_-(i)} = \prod_{j=1}^{p-1}{}'(1-i\bar{\varrho}^j) = \prod_{j=1}^{p-1}{}'(1-i\varrho^{-j}),$$

that is

$$\overline{F_-(i)} = \prod_{j=1}^{p-1}{}'(1-i\varrho^j), \tag{4.2}$$

since, as j runs through the quadratic non-residues modulo p so does $-j$. Hence, multiplying (4.1) and (4.2) together, we obtain

$$|F_-(i)|^2 = F_-(i)\overline{F_-(i)} = \prod_{j=1}^{p-1}{}'(1+\varrho^{2j}) = \prod_{j=1}^{p-1}{}'(1+\varrho^j),$$

since as j runs through the quadratic non-residues modulo p so does $2j$. Thus, appealing to Lemma 2, we obtain

$$|F_-(i)|^2 = \prod_{j=1}^{p-1}{}'(-1-\varrho^j) = F_-(-1) = 1,$$

that is

$$|F_-(i)| = 1. \tag{4.3}$$

An easy calculation shows that for $j = 1, 2, \ldots, p-1$ we have

$$1+i\varrho^j = 2\cos\left(\frac{\pi}{4}+\frac{\pi j}{p}\right)\exp\left\{\left(\frac{\pi}{4}+\frac{\pi j}{p}\right)i\right\}, \tag{4.4}$$

so that

$$F_-(i) = 2^{(p-1)/2}\prod_{j=1}^{p-1}{}'\cos\left(\frac{\pi}{4}+\frac{\pi j}{p}\right)\exp\left\{\tfrac{3}{8}(p-1)\pi i\right\}. \tag{4.5}$$

Let M_p denote the number of integers j satisfying

$$\frac{p}{4} < j < p, \quad \left(\frac{j}{p}\right) = -1.$$

As $\cos(\pi/4+\pi j/p) > 0$, for $0 < j < p/4$, and $\cos(\pi/4+\pi j/p) < 0$, for $p/4 < j < p$, we have

$$\arg(F_-(i)) = \begin{cases} 0, & \text{if } M_p \equiv 0 \pmod 2,\ p \equiv 1 \pmod{16}, \text{ or} \\ & \phantom{\text{if }} M_p \equiv 1 \pmod 2,\ p \equiv 9 \pmod{16}, \\ \pi, & \text{if } M_p \equiv 0 \pmod 2,\ p \equiv 9 \pmod{16}, \text{ or} \\ & \phantom{\text{if }} M_p \equiv 1 \pmod 2,\ p \equiv 1 \pmod{16}. \end{cases} \tag{4.6}$$

Now a formula of Dirichlet ([4], p. 152) asserts that

$$h(-p) = 2 \sum_{0<j<p/4} \left(\frac{j}{p}\right),$$

so that we have

$$M_p = \tfrac{3}{8}(p-1) + \frac{h(-p)}{4}. \tag{4.7}$$

Putting (4.6) and (4.7) together we obtain

$$\arg(F_-(i)) = \begin{cases} 0, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ \pi, & \text{if} \quad h(-p) \equiv 4 \pmod 8, \end{cases} \tag{4.8}$$

that is

$$e^{i\arg(F_-(i))} = (-1)^{h(-p)/4},$$

and hence

$$F_-(i) = |F_-(i)|\, e^{i\arg(F_-(i))} = (-1)^{h(-p)/4},$$

and

$$F_+(i) = \frac{F(i)}{F_-(i)} = (-1)^{h(-p)/4}.$$

This completes the proof of Lemma 3.

From Lemma 3 we obtain

COROLLARY 3. *If $p = 8l+1$ is a prime, then*

$$\sum_{n=0}^{l} (-1)^n a_{2n} = (-1)^{h(-p)/4}, \qquad \sum_{n=0}^{l} (-1)^n b_{2n} = 0.$$

Proof. We have

$$\begin{aligned} \sum_{n=0}^{l} (-1)^n a_{2n} &= \tfrac{1}{2} Y(i) && \text{(by (2.7))} \\ &= \tfrac{1}{2}\big(F_-(i) + F_+(i)\big) && \text{(by (2.6))} \\ &= (-1)^{h(-p)/4} && \text{(by Lemma 3),} \end{aligned}$$

and

$$\begin{aligned} \sum_{n=0}^{l} (-1)^n b_{2n} &= \tfrac{1}{2} Z(i) && \text{(by (2.7))} \\ &= \frac{1}{2\sqrt{p}}\big(F_-(i) - F_+(i)\big) && \text{(by (2.6))} \\ &= 0 && \text{(by Lemma 3).} \end{aligned}$$

5. An important lemma. By adding and subtracting the results of Corollaries 1, 2 and 3 as appropriate, we obtain a number of congruences which we put together as Lemma 4. This lemma is essential to what follows in § 6.

LEMMA 4. *If $p = 8l+1$ is a prime, then*

$$\sum_{n=0}^{l} a_{2n} \equiv \begin{cases} -2l+1 \pmod 8, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ -2l+5 \pmod 8, & \text{if} \quad h(-p) \equiv 4 \pmod 8, \end{cases}$$

$$\sum_{n=0}^{l-1} a_{2n+1} \equiv \begin{cases} -2l \pmod 8, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ -2l+4 \pmod 8, & \text{if} \quad h(-p) \equiv 4 \pmod 8, \end{cases}$$

$$\sum_{n=0}^{[l/2]} a_{4n} \equiv \begin{cases} -l+1 \pmod 4, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ -l+2 \pmod 4, & \text{if} \quad h(-p) \equiv 4 \pmod 8, \end{cases}$$

$$\sum_{n=0}^{[l-1/2]} a_{4n+2} \equiv \begin{cases} -l \pmod 4, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ -l+3 \pmod 4, & \text{if} \quad h(-p) \equiv 4 \pmod 8, \end{cases}$$

$$\sum_{n=0}^{l} b_{2n} \equiv \sum_{n=0}^{l-1} b_{2n+1} \equiv \begin{cases} T/2 \pmod 8, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ h(p)T/2 \pmod 8, & \text{if} \quad h(-p) \equiv 4 \pmod 8, \end{cases}$$

$$\sum_{n=0}^{[l/2]} b_{4n} \equiv \sum_{n=0}^{[l-1/2]} b_{4n+2} \equiv \begin{cases} T/4 \pmod 4, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ h(p)T/4 \pmod 4, & \text{if} \quad h(-p) \equiv 4 \pmod 8. \end{cases}$$

6. Evaluation of $Y(\omega)$, $Z(\omega)$, $Y'(\omega)$, $Z'(\omega)$. If $p = 16k+1$, so that $l = 2k$, we define

(6.1) $$A_1 = \sum_{m=0}^{k} a_{4m}(-1)^m,$$

(6.2) $$B_1 = \tfrac{1}{2} \sum_{m=0}^{k-1} (a_{4m+1} - a_{4m+3})(-1)^m,$$

(6.3) $$C_1 = \sum_{m=0}^{k} b_{4m}(-1)^m,$$

(6.4) $$D_1 = \tfrac{1}{2} \sum_{m=0}^{k-1} (b_{4m+1} - b_{4m+3})(-1)^m,$$

and, if $p = 16k+9$, so that $l = 2k+1$, we define

(6.5) $$A_9 = \sum_{m=0}^{k} a_{4m+2}(-1)^m,$$

(6.6) $$B_9 = \tfrac{1}{2} \Big\{ \sum_{m=0}^{k} a_{4m+1}(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(-1)^m \Big\},$$

(6.7) $$C_9 = \sum_{m=0}^{k} b_{4m+2}(-1)^m,$$

(6.8) $$D_9 = \tfrac{1}{2} \Big\{ \sum_{m=0}^{k} b_{4m+1}(-1)^m + \sum_{m=0}^{k-1} b_{4m+3}(-1)^m \Big\}.$$

A_1, A_9, C_1 and C_9 are clearly integers. B_1, B_9, D_1, D_9 are integers by Lemma 4.

Setting $\omega = \exp(2\pi i/8) = (1+i)/\sqrt{2}$ (so that $\omega^2 = i$, $\omega^4 = -1$, $\omega^8 = 1$, $\omega+\omega^3 = i\sqrt{2}$, $\omega-\omega^3 = \sqrt{2}$), a straightforward calculation shows that, for $p \equiv 1 \pmod{16}$, we have

$$2A_1+2B_1\sqrt{2} = Y(\omega), \quad 2C_1+2D_1\sqrt{2} = Z(\omega), \tag{6.9}$$

and, for $p \equiv 9 \pmod{16}$, we have

$$2A_9 i+2B_9 i\sqrt{2} = Y(\omega), \quad 2C_9 i+2D_9 i\sqrt{2} = Z(\omega). \tag{6.10}$$

Our next lemma makes (6.9) and (6.10) more precise.

LEMMA 5. *Let $p \equiv 1 \pmod 8$ be a prime. Then, for $p \equiv 1 \pmod{16}$, we have*

$$B_1 = C_1 = 0, \quad A_1^2-2pD_1^2 = 1, \quad Y(\omega) = 2A_1, \quad Z(\omega) = 2D_1\sqrt{2}, \quad \text{if} \quad h(-p) \equiv 0 \pmod 8,$$

$$A_1 = D_1 = 0, \quad 2B_1^2-pC_1^2 = 1, \quad Y(\omega) = 2B_1\sqrt{2}, \quad Z(\omega) = 2C_1, \quad \text{if} \quad h(-p) \equiv 4 \pmod 8,$$

and for $p \equiv 9 \pmod{16}$, we have

$$B_9 = C_9 = 0, \quad A_9^2-2pD_9^2 = -1, \quad Y(\omega) = 2A_9 i, \quad Z(\omega) = 2D_9 i\sqrt{2}, \quad \text{if} \quad h(-p) \equiv 0 \pmod 8,$$

$$A_9 = D_9 = 0, \quad 2B_9^2-pC_9^2 = -1, \quad Y(\omega) = 2B_9 i\sqrt{2}, \quad Z(\omega) = 2C_9 i, \quad \text{if} \quad h(-p) \equiv 4 \pmod 8.$$

Proof. From (1.7), (1.8) and (2.5) we have

$$Y(z)^2-pZ(z)^2 = 4F_+(z)F_-(z) = 4\frac{(z^p-1)}{(z-1)}. \tag{6.11}$$

Taking $z = \omega$ in (6.11) we obtain

$$Y(\omega)^2-pZ(\omega)^2 = 4. \tag{6.12}$$

Using (6.9), (6.10) in (6.12) we obtain, for $p = 16k+1$,

$$\begin{cases} A_1^2+2B_1^2-pC_1^2-2pD_1^2 = 1, \\ A_1B_1-pC_1D_1 = 0, \end{cases} \tag{6.13}$$

and, for $p = 16k+9$,

$$\begin{cases} A_9^2+2B_9^2-pC_9^2-2pD_9^2 = -1, \\ A_9B_9-pC_9D_9 = 0. \end{cases} \tag{6.14}$$

Now, from (1.9), we have

$$F_{-}(\omega)F_{-}(-\omega) = F_{-}(i).$$

Hence, by (2.5), (6.9), (6.10) and Lemma 3, we have, for $p = 16k+1$,

$$(6.15)\qquad \begin{cases} A_1^2-2B_1^2+pC_1^2-2pD_1^2 = (-1)^{h(-p)/4}, \\ A_1C_1-2B_1D_1 = 0, \end{cases}$$

and, for $p = 16k+9$,

$$(6.16)\qquad \begin{cases} A_9^2-2B_9^2+pC_9^2-2pD_9^2 = -(-1)^{h(-p)/4}, \\ A_9C_9-2B_9D_9 = 0. \end{cases}$$

The result now follows from (6.13) and (6.15), if $p \equiv 1 \pmod{16}$, and from (6.14) and (6.16), if $p \equiv 9 \pmod{16}$. This completes the proof of Lemma 5.

Next, for $p = 16k+1$, we define

$$(6.17)\qquad E_1 = \tfrac{1}{2}\sum_{m=0}^{k-1}\big(a_{4m+1}(4m+1)+a_{4m+3}(4m+3-8k)\big)(-1)^m,$$

$$(6.18)\qquad F_1 = \sum_{m=0}^{k-1} a_{4m+2}(2m-2k+1)(-1)^m,$$

$$(6.19)\qquad G_1 = \tfrac{1}{2}\sum_{m=0}^{k-1}\big(a_{4m+1}(4m-8k+1)+a_{4m+3}(4m+3)\big)(-1)^m,$$

$$(6.20)\qquad H_1 = k\sum_{m=0}^{k} a_{4m}(-1)^{m+1}.$$

The numbers obtained by replacing each a_n by b_n in (6.17)–(6.20) are denoted by L_1, M_1, N_1, P_1 respectively (eqns. (6.21)–(6.24)). Clearly F_1, H_1, M_1 and P_1 are integers. E_1, G_1, L_1 and N_1 are integers by Lemma 4. By (6.1), (6.3), (6.20), (6.24) and Lemma 5, we have

$$(6.25)\qquad H_1 = -kA_1, \quad P_1 = -kC_1.$$

Moreover, from (6.2), (6.4), (6.17), (6.19), (6.21), (6.23) and Lemma 5 we have

$$(6.26)\qquad \begin{cases} E_1-G_1 = 4k\sum\limits_{m=0}^{k-1}(a_{4m+1}-a_{4m+3})(-1)^m = 8kB_1, \\ L_1-N_1 = 4k\sum\limits_{m=0}^{k-1}(b_{4m+1}-b_{4m+3})(-1)^m = 8kD_1, \end{cases}$$

so that

$$\begin{cases} E_1 = G_1,\ P_1 = 0, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ H_1 = 0,\ L_1 = N_1, & \text{if} \quad h(-p) \equiv 4 \pmod 8). \end{cases}$$

Also, working modulo 4, we have, from (6.18) and Lemma 4,

$$F_1 = \sum_{m=0}^{k-1} a_{4m+2}(2m+1)(-1)^m - 2k \sum_{m=0}^{k-1} a_{4m+2}(-1)^m$$
$$\equiv \sum_{m=0}^{k-1} a_{4m+2} + 2k \sum_{m=0}^{k-1} a_{4m+2},$$

that is

(6.27)(a) $$F_1 \equiv \begin{cases} 2k \pmod 4, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ 3 \pmod 4, & \text{if} \quad h(-p) \equiv 4 \pmod 8). \end{cases}$$

Similarly we have

(6.27)(b) $$M_1 \equiv \begin{cases} T/4 \pmod 4, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ (2k+1)h(p)T/4 \pmod 4, & \text{if} \quad h(-p) \equiv 4 \pmod 8). \end{cases}$$

Next we note that

$$B_1 + E_1 = \sum_{m=0}^{k-1} a_{4m+1}(2m+1)(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(2m+1-4k)(-1)^m$$
$$\equiv \sum_{m=0}^{k-1} a_{4m+1} + \sum_{m=0}^{k-1} a_{4m+3} \pmod 4$$
$$\equiv \sum_{m=0}^{2k-1} a_{2m+1} \pmod 4,$$

that is, by Lemma 4,

$$B_1 + E_1 \equiv 0 \pmod 4,$$

and so, in particular, we have by Lemma 5

$$E_1 \equiv 0 \pmod 4, \quad \text{if} \quad h(-p) \equiv 0 \pmod 8).$$

Similarly we obtain

$$D_1 + L_1 \equiv T/2 \pmod 4,$$

so

$$L_1 \equiv T/2 \equiv 2 \pmod 4, \quad \text{if} \quad h(-p) \equiv 4 \pmod 8).$$

Finally an easy calculation shows that

(6.28) $$\begin{cases} 2E_1 + 4F_1\omega + 2G_1\omega^2 + 8H_1\omega^3 = Y'(\omega), \\ 2L_1 + 4M_1\omega + 2N_1\omega^2 + 8P_1\omega^3 = Z'(\omega). \end{cases}$$

For $p = 16k+9$, we define

(6.29) $$E_9 = \tfrac{1}{2}\left\{\sum_{m=0}^{k} a_{4m+1}(4m+1)(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(8k+1-4m)(-1)^m\right\},$$

(6.30) $$F_9 = (2k+1)\sum_{m=0}^{k} a_{4m+2}(-1)^m,$$

(6.31) $$G_9 = \tfrac{1}{2}\left\{\sum_{m=0}^{k} a_{4m+1}(8k+3-4m)(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(4m+3)(-1)^m\right\},$$

(6.32) $$H_9 = \sum_{m=0}^{k} a_{4m}(2k-2m+1)(-1)^m.$$

The numbers obtained by replacing each a_n by b_n in (6.29)–(6.32) are denoted by L_9, M_9, N_9, P_9 respectively (eqns. (6.33)–(6.36)). Clearly F_9, H_9, M_9 and P_9 are integers. E_9, G_9, L_9 and N_9 are integers by Lemma 4. By (6.5), (6.7), (6.30), (6.34) and Lemma 5, we have

(6.37) $$F_9 = (2k+1)A_9, \qquad M_9 = (2k+1)C_9.$$

Moreover, from (6.5), (6.7), (6.29), (6.31), (6.33), (6.35) and Lemma 5, we have

(6.38)
$$\begin{cases} E_9+G_9 = (4k+2)\left\{\sum_{m=0}^{k} a_{4m+1}(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(-1)^m\right\} = (8k+4)B_9, \\ L_9+N_9 = (4k+2)\left\{\sum_{m=0}^{k} b_{4m+1}(-1)^m + \sum_{m=0}^{k-1} b_{4m+3}(-1)^m\right\} = (8k+4)D_9, \end{cases}$$

so that

$$\begin{cases} E_9 = -G_9, \quad M_9 = 0, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ F_9 = 0, \quad L_9 = -N_9, & \text{if} \quad h(-p) \equiv 4 \pmod 8. \end{cases}$$

Also, working modulo 4, we have, as before,

(6.39)(a) $$H_9 \equiv \begin{cases} 2k \pmod 4, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ 1 \pmod 4, & \text{if} \quad h(-p) \equiv 4 \pmod 8, \end{cases}$$

(6.39)(b) $$P_9 \equiv \begin{cases} T/4 \pmod 4, & \text{if} \quad h(-p) \equiv 0 \pmod 8, \\ (2k+1)h(p)T/4 \pmod 4, & \text{if} \quad h(-p) \equiv 4 \pmod 8, \end{cases}$$

and

$$B_9+E_9 \equiv 2 \pmod 4,$$

$$D_9+L_9 \equiv T/2 \pmod 4,$$

so that by Lemma 5 we have

$$E_9 \equiv 2 \pmod 4, \quad \text{if} \quad h(-p) \equiv 0 \pmod 8,$$
$$L_9 = T/2 \equiv 2 \pmod 4, \quad \text{if} \quad h(-p) \equiv 4 \pmod 8.$$

Finally an easy calculation shows that

$$\text{(6.40)} \qquad \begin{cases} 2E_9+4F_9\omega+2G_9\omega^2+4H_9\omega^3 = Y'(\omega), \\ 2L_9+4M_9\omega+2N_9\omega^2+4P_9\omega^3 = Z'(\omega). \end{cases}$$

Differentiating (6.11) and setting $z = \omega$, we obtain

$$\text{(6.41)} \qquad Y(\omega)Y'(\omega)-pZ(\omega)Z'(\omega) = -8l(1+\omega+\omega^2+\omega^3).$$

Using (6.25), (6.26), (6.28), (6.37), (6.38), (6.40) and appealing to Lemma 5, (6.41) gives

LEMMA 6. *Let $p = 8l+1$ be a prime. Then*

$$\begin{cases} A_1E_1-2pD_1M_1 = -4k, & \text{if} \quad p \equiv 1 \pmod{16},\ h(-p) \equiv 0 \pmod 8, \\ A_1F_1-pD_1N_1 = 2k(A_1^2-2), \end{cases}$$

$$\begin{cases} 2B_1F_1-pC_1L_1 = -4k, & \text{if} \quad p \equiv 1 \pmod{16},\ h(-p) \equiv 4 \pmod 8, \\ B_1E_1-pC_1M_1 = 2kpC_1^2, \end{cases}$$

$$\begin{cases} A_9E_9+2pD_9P_9 = -4k-2, & \text{if} \ p \equiv 9 \pmod{16},\ h(-p) \equiv 0 \pmod 8, \\ A_9H_9+pD_9L_9 = (2k+1)(A_9^2+2), \end{cases}$$

$$\begin{cases} -2B_9H_9+pC_9N_9 = -4k-2, & \text{if} \quad p \equiv 9 \pmod{16}, \\ B_9E_9+pC_9P_9 = (2k+1)(pC_9^2-2), & \qquad h(-p) \equiv 4 \pmod 8. \end{cases}$$

7. Proof of theorem. For $p = 8l+1$ a prime, we define for $j = 0, 1, \ldots, 7$

$$\text{(7.1)} \qquad S_j = \sum_{jp/8<s<(j+1)p/8} \left(\frac{s}{p}\right) = \sum_{s=jl+1}^{(j+1)l} \left(\frac{s}{p}\right),$$

so

$$\text{(7.2)} \qquad \sum_{j=0}^{7} S_j = \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) = 0.$$

Setting $s = jl+t$ $(t = 1, \ldots, l)$ in (7.1) we have, as $(2/p) = 1$,

$$S_j = \sum_{t=1}^{l} \left(\frac{jl+t}{p}\right) = \sum_{t=1}^{l} \left(\frac{8jl+8t}{p}\right) = \sum_{t=1}^{l} \left(\frac{j(p-1)+8t}{p}\right),$$

that is

$$S_j = \sum_{t=1}^{l} \left(\frac{8t-j}{p}\right). \tag{7.3}$$

Mapping $t \to l+1-t$ in the right-hand side of (7.3), we obtain (as $(-1/p) = +1$)

$$S_j = S_{7-j} \quad (j = 0, 1, \ldots, 7). \tag{7.4}$$

From [4], p. 152, and [5], p. 120, we have

$$h(-p) = 2(S_0 + S_1), \quad h(-2p) = 2(S_0 - S_3), \quad S_1 = S_3. \tag{7.5}$$

Putting (7.2), (7.4) and (7.5) together, we obtain

$$\begin{cases} S_0 = S_7 = \frac{1}{4}\big(h(-p) + h(-2p)\big), \\ S_1 = S_3 = S_4 = S_6 = \frac{1}{4}\big(h(-p) - h(-2p)\big), \\ S_2 = S_5 = \frac{1}{4}\big(-3h(-p) + h(-2p)\big). \end{cases} \tag{7.6}$$

Next, for any complex number z, we define

$$K(z) = \sum_{s=1}^{p-1} \left(\frac{s}{p}\right) z^{p-1-s}. \tag{7.7}$$

Taking $z = \omega_r$ $(r = 0, 1, \ldots, 7)$ in (7.7), and using (7.3), we obtain

$$K(\omega^r) = \sum_{j=0}^{7} \omega^{rj} S_j. \tag{7.8}$$

Choosing $r = 1, 5$ in (7.8), and appealing to (7.6), we get

$$\begin{cases} K(\omega) = h(-p)(\omega - \omega^2) + \dfrac{h(-2p)}{2}(1 - \omega + \omega^2 - \omega^3), \\ K(-\omega) = h(-p)(-\omega - \omega^2) + \dfrac{h(-2p)}{2}(1 + \omega + \omega^2 + \omega^3), \end{cases} \tag{7.9}$$

from which we obtain

$$4h(-p) = K(\omega)(1 + \omega + \omega^2 - \omega^3) + K(-\omega)(1 - \omega + \omega^2 + \omega^3). \tag{7.10}$$

Now Liouville ([9], p. 415) has shown that

$$\frac{2}{1-z} K(z) = Y(z)Z'(z) - Y'(z)Z(z). \tag{7.11}$$

Taking $z = \pm\omega$ in (7.11) we obtain

$$(7.12)\quad \begin{cases} 2K(\omega) = (1-\omega)\{Y(\omega)Z'(\omega) - Y'(\omega)Z(\omega)\}, \\ 2K(-\omega) = (1+\omega)\{Y(-\omega)Z'(-\omega) - Y'(-\omega)Z(-\omega)\}. \end{cases}$$

Substituting (7.12) into (7.10) we obtain

$$(7.13)\quad 4h(-p) = \omega^3\{Y'(\omega)Z(\omega) - Y(\omega)Z'(\omega) + Y(-\omega)Z'(-\omega) - Y'(-\omega)Z(-\omega)\}.$$

Now suppose that $h(-p) \equiv 0 \pmod 8$. By (6.25), (6.26), (6.28), (6.37), (6.38), (6.40), (7.13) and Lemma 5, we have

$$h(-p) = \begin{cases} 4A_1M_1 - 4D_1E_1, & \text{if} \quad p \equiv 1 \pmod{16}, \\ -4A_9P_9 - 4D_9E_9, & \text{if} \quad p \equiv 9 \pmod{16}. \end{cases}$$

Hence, as $E_1 \equiv 0 \pmod 4$, $E_9 \equiv 2 \pmod 4$, $D_9 \equiv 1 \pmod 2$, we have

$$h(-p) \equiv \begin{cases} 4A_1M_1 \pmod{16}, & \text{if} \quad p \equiv 1 \pmod{16}, \\ -4A_9P_9 + 8 \pmod{16}, & \text{if} \quad p \equiv 9 \pmod{16}. \end{cases}$$

Appealing to (6.27)(b) and (6.39)(b), we obtain

$$h(-p) \equiv \begin{cases} A_1T \pmod{16}, & \text{if} \quad p \equiv 1 \pmod{16}, \\ -A_9T + 8 \pmod{16}, & \text{if} \quad p \equiv 9 \pmod{16}. \end{cases}$$

As $T \equiv 0 \pmod 8$ and $A_1 \equiv A_9 \equiv 1 \pmod 2$, we have

$$h(-p) \equiv \begin{cases} T \pmod{16}, & \text{if} \quad p \equiv 1 \pmod{16}, \\ T + 8 \pmod{16}, & \text{if} \quad p \equiv 9 \pmod{16}, \end{cases}$$

that is

$$h(-p) \equiv T + p - 1 \pmod{16},$$

as required.

Finally we suppose that $h(-p) \equiv 4 \pmod 8$. As above we have

$$h(-p) = \begin{cases} 4B_1L_1 - 4C_1F_1, & \text{if} \quad p \equiv 1 \pmod{16}, \\ 4B_9L_9 + 4C_9H_9, & \text{if} \quad p \equiv 9 \pmod{16}. \end{cases}$$

Hence, as $B_1 \equiv C_1 \equiv 1 \pmod 2$, $L_1 \equiv 2 \pmod 4$, $F_1 \equiv 3 \pmod 4$, $B_9 \equiv 0 \pmod 2$, $C_9 \equiv 1 \pmod 2$, $L_9 \equiv 2 \pmod 4$, $H_9 \equiv 1 \pmod 4$, we have

$$h(-p) \equiv \begin{cases} 8 + 4C_1 \pmod{16}, & \text{if} \quad p \equiv 1 \pmod{16}, \\ 4C_9 \pmod{16}, & \text{if} \quad p \equiv 9 \pmod{16}. \end{cases}$$

Now if $p \equiv 1 \pmod{16}$ we have from Lemma 6

$$pC_1M_1 = B_1E_1 - 2kpC_1^2.$$

Multiplying by $M_1 \equiv 1 \pmod 2$, we get

$$\begin{aligned} C_1 &\equiv B_1E_1M_1 - 2kM_1 \pmod 4 \\ &\equiv -B_1^2M_1 - 2kM_1 \pmod 4 \\ &\equiv -(1+2k)M_1 \pmod 4 \\ &\equiv -h(p)T/4 \pmod 4, \end{aligned}$$

so that

$$h(-p) \equiv 8 - h(p)T \equiv T + (p-1) + 4\big(h(p)-1\big) \pmod{16}.$$

On the other hand if $p \equiv 9 \pmod{16}$ we have from Lemma 6

$$pC_9P_9 = (2k+1)(pC_9^2-2) - B_9E_9.$$

Multiplying by $P_9 \equiv 1 \pmod 2$, we get

$$\begin{aligned} C_9 &\equiv -(2k+1)P_9 - B_9E_9P_9 \pmod 4 \\ &\equiv -(2k+1)P_9 - B_9(2-B_9)P_9 \pmod 4 \\ &\equiv -(2k+1)P_9 \pmod 4 \\ &\equiv -h(p)T/4 \pmod 4, \end{aligned}$$

so that

$$h(-p) \equiv 8 - h(p)T \equiv T + (p-1) + 4\big(h(p)-1\big) \pmod{16},$$

as required.

This completes the proof of the theorem.

The author would like to acknowledge the help of Mr. Lee–Jeff Bell who did some numerical calculations in connection with the preparation of this paper. The author would also like to thank an unknown referee who pointed out that the author's original proof of Lemma 3 was incomplete.

The ideas of this paper have been extended to determine $h(-2p) \pmod{16}$, where $p \equiv 1 \pmod 8$ is prime.

References

[1] Ezra Brown, *The power of 2 dividing the class-number of a binary quadratic discriminant*, J. Number Theory 5 (1973), pp. 413–419.

[2] — *Class numbers of real quadratic number fields*, Trans. Amer. Math. Soc. 190 (1974), pp. 99–107.

[3] Harvey Cohn and George Cooke, *Parametric form of an eight class field*, Acta Arith. 30 (1976), pp. 367–377.

[4] P. G. L. Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. 21 (1840), pp. 134–155.

[5] Wells Johnson and Kevin J. Mitchell, *Symmetries for sums of the Legendre symbol*, Pacific J. Math. 69 (1977), pp. 117–124.

[6] Pierre Kaplan, *Unités de norme* -1 *de* $Q(\sqrt{p})$ *et corps de classes de degré* 8 *de* $Q(\sqrt{-p})$ *où* p *est un nombre premier congru à* 1 *modulo* 8, Acta Arith. 32 (1977), pp. 239–243.

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

[8] Emma Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. 250 (1971), pp. 42–48.

[9] J. Liouville, *Un point de la théorie des équations binômes*, J. Math. Pures Appl. 2 (1857), pp. 413–423.

[10] G. B. Mathews, *Theory of numbers*, Chelsea Publishing Company, New York, N. Y., 1961.

[11] Trygve Nagell, *Introduction to number theory*, Almqvist & Wiksell, Stockholm 1951.

[12] G. K. C. von Staudt, *Ueber die Functionen* Y *und* Z, *welche der* $\frac{4(x^p-1)}{x-1} = Y^2 \mp pZ^2$ *Genüge leisten, wo* p *eine Primzahl der Form* $4k \pm 1$ *ist*, J. Reine Angew. Math. 67 (1867), pp. 205–217.

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

Received on 27.12.1978
and in revised form on 20.3.1979 (1123)