On the class number of $\mathbb{Q}(\sqrt{-p})$ 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 $\mathbb{Q}(\sqrt{-p})$ satisfies

\begin{equation}
 h(-p) = 0 \pmod{4},
\end{equation}

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

\begin{equation}
 h(p) = 1 \pmod{2},
\end{equation}

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

\begin{equation}
 \varepsilon_p = T + U\sqrt{p},
\end{equation}

where $T$ and $U$ are positive integers such that

\begin{equation}
 T = 0 \pmod{4}, \quad U = 1 \pmod{4}.
\end{equation}

Recently Lehmer ([8], p. 48), Cohn and Cooke ([3], p. 368) and Kaplan ([9], p. 240) have proved that

\begin{equation}
 h(-p) \equiv T \pmod{8}.
\end{equation}

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

We prove

**Theorem.** If $p \equiv 1 \pmod{8}$ is a prime, then

\begin{equation}
 \begin{cases}
 h(-p) \equiv T + (p-1) \pmod{16}, & \text{if } h(-p) = 0 \pmod{8}, \\
 h(-p) \equiv T + (p-1) + 4(h(p)-1) \pmod{16}, & \text{if } h(-p) = 4 \pmod{8}.
\end{cases}
\end{equation}

* Research supported under Natural Sciences and Engineering Research Council of Canada Grant No. A-7233.
We set \( q = \exp(2\pi i/p) \). The cyclotomic polynomial \( F(z) \) of index \( p \) in the complex variable \( z \) is given by

\[
F(z) = \frac{z^p - 1}{z - 1} = \prod_{j=1}^{p-1} (z - q^j) = z^{p-1} + \cdots + z + 1.
\]

(1.7)

We have

\[
F(z) = F_+(z) F_-(z),
\]

(1.8)

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

\[
F_+(z) = \prod_{j=1}^{\frac{p-1}{2}} (z - q^j), \quad F_-(z) = \prod_{j=1}^{\frac{p-1}{2}} (z - q^{p-j}).
\]

(1.9)

The method used to prove the theorem is completely elementary. We sketch the ideas involved. In \( \S\S 2-4 \) Dirichlet’s class number formulae for \( h(p) \) and \( h(-p) \) are used to evaluate \( F_+(1) \) (Lemma 1), \( F_-(1) \) (Lemma 2) and \( F_+(i) \) (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 \( Z(z) = \frac{1}{V_p} (F_-(z) - F_+(z)) \). In \( \S 5 \) these congruences and equations are combined to give further congruences (Lemma 4) which are required in \( \S 6 \).

In \( \S 6 \) 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 \( \S 7 \) using Dirichlet’s class number formula for \( h(-2p) \) and \( h(-p) \) and an identity of Liouville, \( h(-p) \) is expressed in terms of \( Y(\pm \omega) \), \( Y'(\pm \omega) \), \( Z(\pm \omega) \), 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 \( p \equiv 1 \pmod{2} \) is prime, then

\[
F_+(1) = \mp \sqrt{p(T + UVp)^{h(p)}} \quad \text{and} \quad F_-(1) = \sqrt{p(T + UVp)^{h(p)}}.
\]

Proof. By Dirichlet’s class number formula for \( h(p) \) (see for example [11], p. 237), we have

\[
e_p^{h(p)} = \prod_{j=1}^{p-1} \sin \frac{\pi j}{p} / \prod_{j=1}^{p-1} \sin \frac{\pi j}{p}.
\]

(2.1)

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

\[
2^{p-1} \prod_{j=1}^{p-1} \sin \frac{\pi j}{p} = \prod_{j=1}^{p-1} 2 \sin \frac{\pi j}{p} = p.
\]

(2.2)

Multiplying (2.1) and (2.2) together we obtain

\[
p_e^{h(p)} = 2^{p-1} \prod_{j=1}^{p-1} \sin \frac{\pi j}{p} = \prod_{j=1}^{p-1} 2 \sin \frac{\pi j}{p}.
\]

(2.3)

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 \((\bmod p)\). Since \( e_p > 1 \) and each \( \sin(\pi j/p) > 0 \) \((j = 1, \ldots, p-1)\) we have

\[
e_p^{h(p)} = 2^{p-1} \prod_{j=1}^{p-1} \sin \frac{\pi j}{p} = \prod_{j=1}^{p-1} 2 \sin \frac{\pi j}{p}.
\]

(2.4)

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

\[
2 \sin \frac{\pi j}{p} = e_p^{-1/4}(1 - e^{i\pi j/p}),
\]

so, as

\[
\sum_{j=1}^{p-1} j = p(p-1)/4,
\]

(2.4) gives \( F_-(1) = \sqrt{p} e_p^{h(p)} = \sqrt{p(T + UVp)^{h(p)}} \).

Finally, as \( h(p) = 1 \pmod{2} \) and the norm of \( e_p \) is \(-1\), we have

\[
F_+(1) = \frac{F(1)}{F_-(1)} = \frac{p}{\sqrt{p(T + UVp)^{h(p)}}} = -V_p(T - UVp)^{h(p)}.
\]

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

\[
F_+(z) = \frac{1}{V_p} (Y(z) - Z(z)V_p), \quad F_-(z) = \frac{1}{V_p} (Y(z) + Z(z)V_p),
\]

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

\[
Y(z) = F_-(z) + F_+(z), \quad Z(z) = \frac{1}{V_p} (F_-(z) - F_+(z)).
\]

(2.6)
It is easily verified from (1.9) that for \( x \neq 0 \)

\[
g^{(p-1)/2} F_x \left( \frac{1}{x} \right) = F_x (x),
\]

so that by (2.6) we have

\[
g^{(p-1)/2} Y \left( \frac{1}{x} \right) = Y(x), \quad g^{(p-1)/2} Z \left( \frac{1}{x} \right) = Z(x).
\]

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

\[
Y(x) = \sum_{n=0}^{2l} a_n (x^n + x^{d^n-n}),
\]

\[
Z(x) = \sum_{n=0}^{2l} b_n (x^n + x^{d^n-n}),
\]  

(2.7)

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

\[
a_0 = 2, \quad a_1 = 1, \quad a_n = \frac{1}{2} (p+3), \ldots,
\]

\[
b_0 = 0, \quad b_1 = 1, \quad b_2 = 1, \ldots
\]

Appealing to Lemma 1 we obtain

**Corollary 1.** If \( p = 2l+1 \) is a prime, then

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

and

\[
\sum_{n=0}^{2l} a_n = 9 - 4l \pmod{16}, \quad \sum_{n=0}^{2l} b_n = h(p) T \pmod{16},
\]

\[
\text{if} \quad h(-p) = 4 \pmod{8}.
\]

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

\[
(2.8) \quad U = 4l+1 \pmod{16}.
\]

Hence, working modulo 16, we have

\[
\sum_{n=0}^{2l} a_n = \frac{1}{2} Y(1) \quad \text{(by (2.7))}
\]

\[
= \frac{1}{2} (F_-(1) + F_+(1)) \quad \text{(by (2.6))}
\]

\[
= \frac{V}{2} \left\{ (T + U\sqrt{p})^{h(p)} - (T - U\sqrt{p})^{h(p)} \right\} \quad \text{(by Lemma 1)}
\]

\[
= U^{h(p)} (2l+1)^{h(p)+1} \quad \text{(as \( h(p) \equiv 1 \pmod{2} \), \( T = 0 \pmod{4} \))}
\]

\[
= (4l+1)^{h(p)} (8l+1)^{(h(p)+1)/2} \quad \text{(by (2.8))}
\]

\[
= (4l+1)^{h(p)} (8l+1)^{h(p)}.
\]

\[
= (4l+1)(8l+1)
\]

\[
= 1 - 4l,
\]

and

\[
\sum_{n=0}^{2l} b_n = \frac{1}{2} Z(1) \quad \text{(by (2.7))}
\]

\[
= \frac{1}{2V} (F_-(1) - F_+(1)) \quad \text{(by (2.6))}
\]

\[
= \frac{1}{2} \left\{ (T + U\sqrt{p})^{h(p)} + (T - U\sqrt{p})^{h(p)} \right\} \quad \text{(by Lemma 1)}
\]

\[
= h(p) T U^{h(p)-1} (p^{1/2})^{h(p)-1} \quad \text{(as \( T = 0 \pmod{4} \))}
\]

\[
= h(p) T (4l+1)^{h(p)-1} (8l+1)^{(h(p)-1)/2} \quad \text{(by (2.8))}
\]

\[
= h(p) T (8l+1)^{h(p)-1} \quad \text{(as \( h(p) = 1 \pmod{2} \))}
\]

\[
= h(p) T \quad \text{(as \( h(p) = 1 \pmod{2} \))}
\]

\[
= T \quad \text{(as \( T = 0 \pmod{8} \)).}
\]

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

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

**Lemma 2.** If \( p = 1 \pmod{8} \) is prime, then

\[
F_+(1) = F_-(1) = 1.
\]

**Proof.** From (1.9) we have

\[
F_+(1) F_-(1) = \prod_{j=1}^{p-1} (1 - g^{pj}) = \prod_{j=1}^{p-1} (1 - g^{2j}).
\]

As \( j \) runs through the quadratic non-residues modulo \( p \), so does \( 2j \). Hence
we have
\[ \prod_{i=1}^{p-1} (1-\zeta^i) = \prod_{j=1}^{p-1} (1-\zeta^j) = F_-(1), \]
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 \( p = 81 + 1 \) is prime, then

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

**Proof.** We have
\[ \sum_{n=0}^{2} (-1)^n a_n = \frac{1}{2} \mathcal{X}(-1) \quad \text{(by (3.7))} \]
\[ = \frac{1}{2} (F_-(1) + F_+(1)) \quad \text{(by (2.6))} \]
\[ = 1 \quad \text{(by Lemma 2),} \]
and
\[ \sum_{n=0}^{2} (-1)^n b_n = \frac{1}{2} \mathcal{Z}(-1) \quad \text{(by (2.7))} \]
\[ = \frac{1}{2p} (F_-(1) - F_+(1)) \quad \text{(by (2.6))} \]
\[ = 0 \quad \text{(by Lemma 2).} \]

4. Evaluation of \( \mathcal{F}_-(i) \) and \( \mathcal{F}_+(i) \). Using Dirichlet's class number formula for \( h(-p) \), we prove

**Lemma 3.** If \( p = 1 \) (mod 8) is prime, then

\[ \mathcal{F}_+(i) = \mathcal{F}_-(i) = (-1)^{h(-p)/4}. \]

**Proof.** As \( p = 1 \) (mod 8), we have
\[ (4.1) \quad \mathcal{F}_-(i) = \prod_{j=1}^{p-1} (1-i\zeta^j) = \prod_{j=1}^{p-1} (1-i\zeta^j), \]
so that
\[ \mathcal{F}_-(i) = \prod_{j=1}^{p-1} (1-i\zeta^j) = \prod_{j=1}^{p-1} (1-i\zeta^{-j}), \]
that is
\[ (4.2) \quad \mathcal{F}_-(i) = \prod_{j=1}^{p-1} (1-i\zeta^j), \]
since, as \( j \) runs through the quadratic non-residues modulo \( p \) so does \(-j\). Hence, multiplying (4.1) and (4.2) together, we obtain
\[ |\mathcal{F}_+(i)|^2 = \mathcal{F}_-(i)\mathcal{F}_+(i) = \prod_{j=1}^{p-1} (1+i\zeta^j) = \prod_{j=1}^{p-1} (1+i\zeta^j), \]
since as \( j \) runs through the quadratic non-residues modulo \( p \) so does \( 2j \). Thus, appealing to Lemma 2, we obtain
\[ |\mathcal{F}_+(i)|^2 = \prod_{j=1}^{p-1} (1-i\zeta^j) = F_-(1) = 1, \]
that is
\[ (4.3) \quad |\mathcal{F}_+(i)| = 1. \]
An easy calculation shows that for \( j = 1, 2, \ldots, p-1 \) we have
\[ (4.4) \quad 1+i\zeta^j = 2\cos \left( \frac{\pi}{4} + \frac{\pi j}{p} \right) \exp \left( \frac{\pi i}{4} + \frac{\pi j}{p} \right), \]
so that
\[ (4.5) \quad \mathcal{F}_+(i) = 2^{p-1} \prod_{j=1}^{p-1} \cos \left( \frac{\pi}{4} + \frac{\pi j}{p} \right) \exp \left( \frac{\pi i}{4} (p-1) \right). \]
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
\[ (4.6) \quad \arg (\mathcal{F}_+(i)) = \begin{cases} 0, & \text{if } M_p = 0 \text{ (mod 2), } \quad p = 1 \text{ (mod 16),} \\ \pi, & \text{if } M_p = 0 \text{ (mod 2), } \quad p = 9 \text{ (mod 16),} \\ \pi, & \text{if } M_p = 1 \text{ (mod 2), } \quad p = 1 \text{ (mod 16).} \end{cases} \]
Now a formula of Dirichlet ([4], p. 152) asserts that
\[ h(-p) = 2 \sum_{\nu < d < p/d} \left( \frac{\nu}{p} \right), \]
so that we have
\[ M_p = \frac{1}{d} (p-1) + \frac{h(-p)}{d}. \]
(4.7)

Putting (4.6) and (4.7) together we obtain
\[ \arg \{ F_-(i) \} = \begin{cases} 0, & \text{if } h(-p) \equiv 0 \pmod{8}, \\ \pi, & \text{if } h(-p) \equiv 4 \pmod{8}, \end{cases} \]
that is
\[ e^{i \arg \{ F_-(i) \}} = (-1)^{h(-p)/4}, \]
and hence
\[ F_-(i) = |F_-(i)| e^{i \arg \{ F_-(i) \}} = (-1)^{h(-p)/4} F_-(i), \]
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
\[ \sum_{n=0}^{l} (-1)^n a_{2n} = (-1)^{h(-p)/4}, \quad \sum_{n=0}^{l} (-1)^n b_{2n} = 0. \]

**Proof.** We have
\[ \sum_{n=0}^{l} (-1)^n a_{2n} = \frac{1}{2} Y(i) \quad \text{(by (2.7))} \]
\[ = \frac{1}{2} (F_-(i) + F_+(i)) \quad \text{(by (2.6))} \]
\[ = (-1)^{h(-p)/4} \quad \text{(by Lemma 3)}, \]
and
\[ \sum_{n=0}^{l} (-1)^n b_{2n} = \frac{1}{2} Z(i) \quad \text{(by (2.7))} \]
\[ = \frac{1}{2 \sqrt{p}} (F_-(i) - F_+(i)) \quad \text{(by (2.6))} \]
\[ = 0 \quad \text{(by Lemma 3)}. \]

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
\[ \sum_{n=0}^{l-1} a_{2n+1} = \begin{cases} -2l+1 \pmod{8}, & \text{if } h(-p) \equiv 0 \pmod{8}, \\ -2l+5 \pmod{8}, & \text{if } h(-p) \equiv 4 \pmod{8}, \end{cases} \]
\[ \sum_{n=0}^{l-1} a_{2n+2} = \begin{cases} -2l \pmod{8}, & \text{if } h(-p) \equiv 0 \pmod{8}, \\ -2l+4 \pmod{8}, & \text{if } h(-p) \equiv 4 \pmod{8}, \end{cases} \]
\[ \sum_{n=0}^{l-1} b_{2n+1} = \begin{cases} -l+1 \pmod{4}, & \text{if } h(-p) \equiv 0 \pmod{8}, \\ -l+2 \pmod{4}, & \text{if } h(-p) \equiv 4 \pmod{8}, \end{cases} \]
\[ \sum_{n=0}^{l-1} a_{4n} = \begin{cases} -l \pmod{4}, & \text{if } h(-p) \equiv 0 \pmod{8}, \\ -l+3 \pmod{4}, & \text{if } h(-p) \equiv 4 \pmod{8}, \end{cases} \]

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

\[ A_1 = \sum_{m=0}^{k} a_{2m} (-1)^m, \]
\[ B_1 = \frac{1}{2} \sum_{m=0}^{k-1} (a_{2m+1} - a_{2m+3}) (-1)^m, \]
\[ C_1 = \sum_{m=0}^{k} b_{2m} (-1)^m, \]
\[ D_1 = \frac{1}{2} \sum_{m=0}^{k-1} (b_{2m+1} - b_{2m+3}) (-1)^m, \]

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

\[ A_2 = \sum_{m=0}^{k} a_{2m+1} (-1)^m, \]
\[ B_2 = \frac{1}{2} \left\{ \sum_{m=0}^{k} a_{2m+3} (-1)^m + \sum_{m=0}^{k-1} a_{2m+1} (-1)^m \right\}, \]
\[ C_2 = \sum_{m=0}^{k} b_{2m+2} (-1)^m, \]
\[ D_2 = \frac{1}{2} \left\{ \sum_{m=0}^{k} b_{2m+3} (-1)^m + \sum_{m=0}^{k-1} b_{2m+1} (-1)^m \right\}. \]
$A_1$, $A_2$, $C_1$ and $C_2$ are clearly integers. $B_1$, $B_2$, $D_1$, $D_2$ are integers by Lemma 4.

Setting $\omega = \exp(2\pi i/8) = (1+i)/\sqrt{2}$ (so that $\omega^2 = i$, $\omega^3 = -1$, $\omega^4 = 1$, $\omega + \omega^3 = i\sqrt{2}$, $\omega - \omega^3 = -\sqrt{2}$), a straightforward calculation shows that, for $p = 1 \pmod{16}$, we have
\begin{equation}
2A_1 + 2B_1\sqrt{2} = Y(\omega), \quad 2C_1 + 2D_1\sqrt{2} = Z(\omega),
\end{equation}
and, for $p = 9 \pmod{16}$, we have
\begin{equation}
A_4 + 2B_4\sqrt{2} = Y(\omega), \quad C_4 + 2D_4\sqrt{2} = Z(\omega).
\end{equation}

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

**Lemma 5.** Let $p = 1 \pmod{8}$ be a prime. Then, for $p = 1 \pmod{16}$, we have
\begin{align*}
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) = 0 \pmod{8}, \\
B_1 &= D_1 = 0, \quad 2B_1^2 - pC_1^2 = 1, \quad Y(\omega) = 2B_1\sqrt{2}, \quad Z(\omega) = 2C_1,
\end{align*}
and for $p = 9 \pmod{16}$, we have
\begin{align*}
B_9 &= C_9 = 0, \quad A_9^2 - 2pD_9^2 = -1, \quad Y(\omega) = 2A_9i, \quad Z(\omega) = 2D_9i\sqrt{2}, \\
& \quad \text{if} \quad h(-p) = 0 \pmod{8}, \\
B_9 &= D_9 = 0, \quad 2B_9^2 - pC_9^2 = -1, \quad Y(\omega) = 2B_9i\sqrt{2}, \quad Z(\omega) = 2C_9i,
\end{align*}
and for $p = 9 \pmod{8}$, we have
\begin{align*}
B_9 &= C_9 = 0, \quad A_9^2 - 2pD_9^2 = 1, \quad Y(\omega) = 2A_9i, \quad Z(\omega) = 2D_9i\sqrt{2}, \\
& \quad \text{if} \quad h(-p) = 0 \pmod{8}, \\
B_9 &= D_9 = 0, \quad 2B_9^2 - pC_9^2 = -1, \quad Y(\omega) = 2B_9i\sqrt{2}, \quad Z(\omega) = 2C_9i,
\end{align*}

Proof. From (1.7), (1.8) and (2.5) we have
\begin{equation}
Y(s)^2 - pZ(s)^2 = 4F_+(s)F_-(s) = 4 \frac{s^2-1}{(s-1)}.
\end{equation}

Taking $s = \omega$ in (6.11) we obtain
\begin{equation}
Y(\omega)^2 - pZ(\omega)^2 = 4.
\end{equation}

Using (6.9), (6.10) in (6.12) we obtain, for $p = 16k+1$,
\begin{equation}
[A_4^2 + 2B_4^2 - pC_4^2 - 2pD_4^2 = 1, \\
A_4B_4 - pC_4D_4 = 0,
\end{equation}
and, for $p = 16k+9$,
\begin{equation}
[A_4^2 + 2B_4^2 - pC_4^2 - 2pD_4^2 = -1, \\
A_4B_4 - pC_4D_4 = 0.
\end{equation}

Now, from (1.9), we have
\begin{equation}
F_-(\omega)F_-(\omega) = F_-(i).
\end{equation}

Hence, by (2.5), (6.9), (6.10) and Lemma 3, we have, for $p = 16k+1$,
\begin{equation}
\begin{cases}
A_4^2 - 2B_4^2 + pC_4^2 - 2pD_4^2 = (-1)^{A_4\omega^4}, \\
A_4B_4 - 2B_4D_4 = 0,
\end{cases}
\end{equation}
and, for $p = 16k+9$,
\begin{equation}
\begin{cases}
A_4^2 - 2B_4^2 + pC_4^2 - 2pD_4^2 = (-1)^{A_4\omega^4}, \\
A_4B_4 - 2B_4D_4 = 0,
\end{cases}
\end{equation}

The result now follows from (6.11) and (6.15), if $p = 1 \pmod{16}$, and from (6.14) and (6.16), if $p = 9 \pmod{16}$. This completes the proof of Lemma 5.

Next, for $p = 16k+1$, we define
\begin{equation}
E_1 = \frac{1}{2} \sum_{m=0}^{k-1} (a_{4m+1}(4m+1) + a_{4m+3}(4m+3)-8k)(-1)^m,
\end{equation}
\begin{equation}
E_3 = \frac{1}{2} \sum_{m=0}^{k-1} a_{4m+1}(2m-2k+1)(-1)^m,
\end{equation}
\begin{equation}
G_1 = \frac{1}{2} \sum_{m=0}^{k-1} (a_{4m+1}(4m-8k+1) + a_{4m+3}(4m+3))(1)^m,
\end{equation}
\begin{equation}
H_1 = \frac{1}{2} \sum_{m=0}^{k-1} a_{4m+1}(-1)^{m+1}.
\end{equation}

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 (6.4), (6.3), (6.20), (6.24) and Lemma 5, we have
\begin{equation}
H_1 = -kA_1, \quad P_1 = -kC_1.
\end{equation}

Moreover, from (6.2), (6.4), (6.17), (6.19), (6.21), (6.23) and Lemma 5 we have
\begin{equation}
\begin{cases}
E_1 - G_1 = 4k \sum_{m=0}^{k-1} (a_{4m+1} - a_{4m+3})(-1)^m = 8kB_1, \\
L_1 - N_1 = 4k \sum_{m=0}^{k-1} (b_{4m+1} - b_{4m+3})(-1)^m = 8kD_1,
\end{cases}
\end{equation}
so that 
\[
E_1 = G_1, \quad P_1 = 0, \quad \text{if} \quad h(-p) = 0 \pmod{8}, \\
H_1 = 0, \quad L_1 = N_1, \quad \text{if} \quad h(-p) = 4 \pmod{8}.
\]

Also, working modulo \(4\), we have, from (6.18) and Lemma 4,
\[
F_1 = \sum_{m=0}^{k-1} a_{3m+2}(2m+1)(-1)^m - 2k \sum_{m=0}^{k-1} a_{4m+2}(-1)^m \\
\quad \quad = \sum_{m=0}^{k-1} a_{3m+2} + 2k \sum_{m=0}^{k-1} a_{4m+2},
\]
that is
\[
(6.27a) \quad F_1 = \begin{cases} 
2k \pmod{4}, & \text{if} \quad h(-p) = 0 \pmod{8}, \\
3 \pmod{4}, & \text{if} \quad h(-p) = 4 \pmod{8}.
\end{cases}
\]

Similarly we have
\[
(6.27b) \quad M_1 = \begin{cases} 
T/4 \pmod{4}, & \text{if} \quad h(-p) = 0 \pmod{8}, \\
(2k+1)h(p)T/4 \pmod{4}, & \text{if} \quad h(-p) = 4 \pmod{8}.
\end{cases}
\]

Next we note that
\[
B_1 + E_1 = \sum_{m=0}^{k-1} a_{4m+1}(2m+1)(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(2m+1 - 4k)(-1)^m \\
\quad \quad = \sum_{m=0}^{k-1} a_{4m+1} + \sum_{m=0}^{k-1} a_{4m+3}(mod 4),
\]
that is, by Lemma 4,
\[
B_1 + E_1 \equiv 0 \pmod{4},
\]
and so, in particular, we have by Lemma 5
\[
E_1 \equiv 0 \pmod{4}, \quad \text{if} \quad h(-p) = 0 \pmod{8}.
\]

Similarly we obtain
\[
D_1 + L_1 \equiv T/2 \pmod{4},
\]
so
\[
L_1 \equiv T/2 \equiv 2 \pmod{4}, \quad \text{if} \quad h(-p) = 4 \pmod{8}.
\]

Finally an easy calculation shows that
\[
(6.28) \quad 2E_1 + 4F_1 \omega + 2G_1 \omega^3 + 8H_1 \omega^5 = Y' (\omega), \\
2L_1 + 4M_1 \omega + 2N_1 \omega^3 + 8P_1 \omega^5 = Z' (\omega).
\]

For \( p = 16k+9 \), we define
\[
(6.29) \quad E_9 = \frac{1}{2} \left\{ \sum_{m=0}^{k} a_{4m+1}(4m+1)(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(8k+1 - 4m)(-1)^m \right\},
\]
\[
(6.30) \quad E_9 = (2k+1) \sum_{m=0}^{k} a_{4m+3}(-1)^m,
\]
\[
(6.31) \quad G_9 = \frac{1}{2} \left\{ \sum_{m=0}^{k} a_{4m+1}(8k+3 - 4m)(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(4m+3)(-1)^m \right\},
\]
\[
(6.32) \quad H_9 = \sum_{m=0}^{k} a_{4m}(2k - 2m+1)(-1)^m.
\]

The numbers obtained by replacing each \( a_m \) in (6.29)–(6.32) are denoted by \( E_9, M_9, N_9, P_9 \) respectively (eqns. (6.33)–(6.36)). Clearly \( F_9, G_9, L_9 \) and \( N_9 \) are integers by Lemma 4. By (6.5), (6.7), (6.30), (6.34) and Lemma 5, we have
\[
(6.37) \quad F_9 = (2k+1)A_9, \quad M_9 = (2k+1)C_9.
\]

Moreover, from (6.5), (6.7), (6.29), (6.31), (6.33), (6.35) and Lemma 5, we have
\[
(6.38) \quad \left\{ \begin{array}{ll}
E_9 + G_9 = (4k+2) \left\{ \sum_{m=0}^{k} a_{4m+1}(-1)^m + \sum_{m=0}^{k-1} a_{4m+3}(-1)^m \right\} = (8k+4)E_9, \\
L_9 + N_9 = (4k+2) \left\{ \sum_{m=0}^{k} b_{4m+1}(-1)^m + \sum_{m=0}^{k-1} b_{4m+3}(-1)^m \right\} = (8k+4)D_9,
\end{array} \right.
\]
so that
\[
\left\{ \begin{array}{ll}
E_9 = -G_9, \quad M_9 = 0, & \text{if} \quad h(-p) = 0 \pmod{8}, \\
F_9 = 0, \quad L_9 = -N_9, & \text{if} \quad h(-p) = 4 \pmod{8}.
\end{array} \right.
\]

Also, working modulo \(4\), we have, as before,
\[
(6.39a) \quad H_9 = \begin{cases} 
2k \pmod{4}, & \text{if} \quad h(-p) = 0 \pmod{8}, \\
1 \pmod{4}, & \text{if} \quad h(-p) = 4 \pmod{8}.
\end{cases}
\]
\[
(6.39b) \quad P_9 = \begin{cases} 
T/4 \pmod{4}, & \text{if} \quad h(-p) = 0 \pmod{8}, \\
(2k+1)h(p)T/4 \pmod{4}, & \text{if} \quad h(-p) = 4 \pmod{8}.
\end{cases}
\]

and
\[
\left\{ \begin{array}{ll}
B_9 + E_9 \equiv 2 \pmod{4}, \\
D_9 + L_9 \equiv T/2 \pmod{4}.
\end{array} \right.
\]
so that by Lemma 5 we have

\[ E_i = 2 \pmod{4}, \quad \text{if} \quad h(-p) = 0 \pmod{8}, \]
\[ L_0 = T/2 = 2 \pmod{4}, \quad \text{if} \quad h(-p) = 4 \pmod{8}. \]

Finally an easy calculation shows that

\[
\begin{align*}
2E_3 + 4E_2 \omega + 2G_2 \omega^3 + 4H_2 \omega^3 &= Y'(\omega), \\
2E_2 + 4E_1 \omega + 2N_2 \omega^2 + 4P_2 \omega^3 &= Z'(\omega).
\end{align*}
\]

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

\[
Y(\omega)Y'(\omega) - pZ(\omega)Z'(\omega) = -8I(1 + \omega + \omega^2 + \omega^3).
\]

Using (6.35), (6.26), (6.28), (6.37), (6.38), (6.40) and appealing to Lemma 5, (6.41) gives

**Lemmas 6.** Let \( p = 8l+1 \) be a prime. Then

\[
\begin{align*}
A_1 E_3 - 2pD_1 M_1 &= -4k, \quad \text{if} \quad p = 1 \pmod{16}, h(-p) = 0 \pmod{8}, \\
A_1 E_1 - pD_1 N_1 &= 2k(A_1^2 - 2), \\
2B_3 E_1 - pC_1 L_1 &= -4k, \quad \text{if} \quad p = 1 \pmod{16}, h(-p) = 4 \pmod{8}, \\
B_1 E_1 - pC_1 M_1 &= 2k pC_1^2, \\
A_1 E_2 + 2pD_2 P_2 &= -4k - 2, \quad \text{if} \quad p = 9 \pmod{16}, h(-p) = 0 \pmod{8}, \\
A_1 H_1 + pD_2 L_2 &= (2k + 1)(A_1^2 + 2), \\
-2B_2 H_2 + pC_2 N_2 &= -4k - 2, \quad \text{if} \quad p = 9 \pmod{16}, \\
B_2 E_2 + pC_2 P_2 &= (2k + 1)(pC_2^2 - 2), \quad h(-p) = 4 \pmod{8}.
\end{align*}
\]

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

\[
S_j = \sum_{p=2 \text{ if } 9 \text{ if } p = 1 \pmod{16}, h(-p) = 0 \pmod{8},}
\]

so

\[
\sum_{j=0}^{7} S_j = \sum_{j=0}^{8} \left( \frac{j}{p} \right) = 0.
\]

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

\[
S_j = \sum_{t=1}^{l} \left( \frac{j+1}{p} \right) = \sum_{t=1}^{l} \left( \frac{8j + 8t}{p} \right) = \sum_{t=1}^{l} \left( \frac{j(p-1) + 8t}{p} \right).
\]

that is

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

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

\[
(7.4) \quad S_j = S_{l-j} \quad (j = 0, 1, \ldots, 7).
\]

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

\[
(7.5) \quad h(-p) = 2(S_0 + S_1), \quad h(-2p) = 2(S_0 - S_3), \quad S_3 = S_3.
\]

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

\[
(7.6) \quad \begin{cases} 
S_0 = S_1 & = \frac{1}{2}(h(-p) + h(-2p)), \\
S_1 = S_3 & = S_3 = \frac{1}{2}(h(-p) - h(-2p)), \\
S_3 = S_3 & = \frac{1}{2}(-3h(-p) + h(-2p)).
\end{cases}
\]

Next, for any complex number \( \omega \), we define

\[
K(\omega) = \sum_{s=0}^{n-1} \left( \frac{s}{p} \right) \omega^{p-1-s}.
\]

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

\[
(7.8) \quad K(\omega) = \sum_{j=0}^{7} \omega^j S_j.
\]

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

\[
(7.9) \quad \begin{cases} 
K(\omega) = h(-p)(\omega - \omega^3) + \frac{h(-2p)}{2}(1 + \omega - \omega^3 - \omega^5), \\
K(-\omega) = h(-p)(-\omega - \omega^3) + \frac{h(-2p)}{2}(1 + \omega + \omega^3 + \omega^5),
\end{cases}
\]

from which we obtain

\[
(7.10) \quad 4h(-p) = K(\omega)(1 + \omega + \omega^3 - \omega^5) + K(-\omega)(1 - \omega + \omega^3 + \omega^5).
\]

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

\[
(7.11) \quad \frac{2}{1 - z} K(z) = Y(z)Z'(z) - Y'(z)Z(x).
\]
Taking $z = \pm \omega$ in (7.11) we obtain

$$2K(\omega) = (1 - \omega)\{Y(\omega)Z'(\omega) - Y'(\omega)Z(\omega)\},$$

$$2K(-\omega) = (1 + \omega)\{Y(-\omega)Z'(\omega) - Y'(\omega)Z(-\omega)\}.$$ 

Substituting (7.13) into (7.10) we obtain

$$4h(-p) = \omega^2\{Y'(\omega)Z(\omega) - Y(\omega)Z'(\omega) + Y(-\omega)Z'(\omega) - Y'(\omega)Z(-\omega)\}. $$

Now suppose that $h(-p) \equiv 0 \pmod 8$. By (6.25), (6.26), (6.28), (6.37), (6.38), (6.40), (7.33) and Lemma 5, we have

$$h(-p) = \begin{cases} 4A_1M_1 - 4D_1E_1, & \text{if } p \equiv 1 \pmod {16}, \\ -4A_1P_2 - 4D_2E_1, & \text{if } p \equiv 9 \pmod {16}. \end{cases} $$

Hence as $E_1 = 0 \pmod 4$, $E_2 = 2 \pmod 4$, $D_2 = 1 \pmod 2$, we have

$$h(-p) = \begin{cases} 4A_1M_1 \pmod {16}, & \text{if } p \equiv 1 \pmod {16}, \\ -4A_1P_2 + 8 \pmod {16}, & \text{if } p \equiv 9 \pmod {16}. \end{cases} $$

Appealing to (6.37)(b) and (6.39)(b), we obtain

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

As $T = 0 \pmod 8$ and $A_1 = A_3 \equiv 1 \pmod 2$, we have

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

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

$$h(-p) = \begin{cases} 4B_2L_2 - 4C_1F_1, & \text{if } p \equiv 1 \pmod {16}, \\ 4B_2L_2 + 4C_1H_1, & \text{if } p \equiv 9 \pmod {16}. \end{cases} $$

Hence, as $B_2 = C_3 = 1 \pmod 2$, $L_2 = 2 \pmod 4$, $F_1 = 3 \pmod 4$, $B_3 = 0 \pmod 2$, $C_3 = 1 \pmod 2$, $L_2 = 2 \pmod 4$, $H_3 = 1 \pmod 4$, we have

$$h(-p) = \begin{cases} 8 + 4C_1 \pmod {16}, & \text{if } p \equiv 1 \pmod {16}, \\ 4C_3 \pmod {16}, & \text{if } p \equiv 9 \pmod {16}. \end{cases} $$

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

$$PC_3M_1 = B_2E_1 - 2kpC_1^2,$$

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

$$C_1 = B_1E_1 - 2kM_1 \pmod 4$$

$$\equiv -B_1^2M_1 - 2kM_1 \pmod 4$$

$$\equiv -(1 + 2k)M_1 \pmod 4$$

so that

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

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

$$PC_3P_3 = (2k + 1)(pC_3^2 - 2) - B_2E_1.$$ 

Multiplying by $P_3 = 1 \pmod 2$, we get

$$C_3 = -(2k + 1)P_3 - B_2E_1P_3 \pmod 4$$

$$\equiv -(2k + 1)P_3 - B_2(2 - B_3)P_3 \pmod 4$$

$$\equiv -(2k + 1)P_3 \pmod 4$$

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

so that

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

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

On the distribution modulo 1 of the sequence $am^3 + bn^2 + cn$

by

R. C. Baker (London)

1. Introduction. Let $||$ denote distance to the nearest integer. Let $\varepsilon > 0$, and let $a, b, c$ denote arbitrary real numbers. Recently W. M. Schmidt showed [6] that for $N > c_0(\varepsilon)$ there is a natural number $n \leq N$ having

$$||an^3 + bn^2 + cn|| < N^{-1/2+\varepsilon}.$$ 

This generalizes the well known theorem of Heilbronn [3] and sharpens a result of Davenport [2].

Schmidt's method enabled him to prove that for $N > c_0(\varepsilon)$ there is a natural number $n \leq N$ having

$$||an^3 + bn^2 + cn|| < N^{-1/4+\varepsilon}.$$ 

For $\gamma = 0$, the exponent $-1/6 + \varepsilon$ could be replaced by $-1/4 + \varepsilon$ [6]. Both results sharpen those of Davenport [2].

In the present paper we shall show that for $N > c_0(\varepsilon)$ there is a natural number $n \leq N$ having

$$||an^3 + bn^2 + cn|| < N^{-1/4+\varepsilon}.$$ 

It is no more difficult to prove a more general theorem. We denote by $k$ an integer greater than 1 and write $K = 2^{k-1}$.

Theorem 1. Suppose $k \geq 3$ and $N > c_0(k, \varepsilon)$. Then there is a natural number $n \leq N$ with

$$||am^k + bn^{k-1} + cn|| < N^{-1/k+\varepsilon},$$

We also strengthen Schmidt's theorem [6] for an arbitrary polynomial of degree $k \geq 3$ with constant term zero, but only when $k$ is odd.

Theorem 2. Let $k$ be an odd integer, $k \geq 3$, and write $K_1 = \frac{4}{3}(2^{k-1} - 1)$. Let $N > c_0(k, \varepsilon)$. Given a polynomial $F(n)$ of degree $k$ with constant term zero, there is a natural number $n \leq N$ with

$$||F(n)|| < N^{-1/k+\varepsilon}.$$ 

We shall use ideas normally associated with "major arcs" in the circle method [1]. Schmidt's method, on the other hand, is a very original development of "minor arc" ideas.