Congruences modulo 16 for the class numbers of the quadratic fields $\mathbb{Q}(\sqrt{\pm p})$ and $\mathbb{Q}(\sqrt{\pm 2p})$ for $p$ a prime congruent to 5 modulo 8

by

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

I. $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$

1. Introduction. Throughout this paper $p$ denotes a prime congruent to 5 modulo 8. We set $p = 8l + 5$. The fundamental unit $(>1)$ of the ring $A$ of integers of the real quadratic field $\mathbb{Q}(\sqrt{p})$ is denoted by $\varepsilon_p$. We have

$$\varepsilon_p = \frac{1}{2}(t + u\sqrt{p}),$$

where $t$ and $u$ are positive integers satisfying $t = u \pmod{2}$. The norm of $\varepsilon_p$ is $-1$ so

$$t^2 - pu^2 = -4.$$  

We let $\eta_p$ be the fundamental unit of the subring $B$ of $A$ of integers of the form $x + y\sqrt{p}$ ($x, y \in \mathbb{Z}$), that is, $\eta_p$ is the smallest power of $\varepsilon_p$ in $B$. It is a result going back to at least Dirichlet ([1], p. 249) that

$$\eta_p = \begin{cases}  
\varepsilon_p, & \text{if } t = u = 0 \pmod{2}, \\
\varepsilon_p^3, & \text{if } t = u = 1 \pmod{2},
\end{cases}$$

and that the ideal class number of $A$, written $h(p)$, is related to the ideal class number of $B$, written $k = k(p)$, by

$$k = \begin{cases}  
3h(p), & \text{if } \eta_p = \varepsilon_p, \\
h(p), & \text{if } \eta_p = \varepsilon_p^3.
\end{cases}$$

*Research supported by the Natural Sciences and Engineering Research Council of Canada, Grant No. A-7233, and by the University of Nancy.
It follows immediately from (1.3) and (1.4) that
\[(1.5)\]
\[c^k_p = \eta_p^k.\]

It is well known that \(h(p)\) (and thus \(k\)) is odd.

As \(\eta_p \in B\) we have
\[(1.6)\]
\[\eta_p = T + UV\sqrt{p},\]
where \(T + UV\sqrt{p}\) is the least positive integral solution of
\[(1.7)\]
\[T^2 - pU^2 = -1,\]
and \(T, U\) are related to \(t, u\) by
\[(1.8)\]
\[
\begin{align*}
T &= t/2, & U &= u/2, & \text{if } t = u = 0 \pmod{2}, \\
T &= t(t^2 + 3)/2, & U &= u(t^2 + 1)/2, & \text{if } t = u = 1 \pmod{2}.
\end{align*}
\]

Taking (1.7) modulo 8 we see that
\[(1.9)\]
\[T = 2 \pmod{4},\]
and that \(U\) is odd. Clearly all prime factors of \(U\) are congruent to 1 modulo 4, so that \(U = 1 \pmod{4}\). Then, taking (1.7) modulo 32, we obtain
\[(1.10)\]
\[U = 4l + 1 \pmod{16}.\]

Now we let \(h = h(-p)\) denote the class number of the imaginary quadratic field \(\mathcal{O} = \mathbb{Q}(\sqrt{-p})\). It is well-known that \(h = 2 \pmod{4}\), as \(p = 5 \pmod{8}\).

It is the purpose of this paper to relate the class number \(h\) modulo 16 to the class number \(k\) and the integer \(T\). We prove

**Theorem 1.** If \(p\) is a prime congruent to 5 modulo 8, then:
\[(1.11)\]
\[h = Tk \pmod{16}.\]

The congruence
\[(1.12)\]
\[h = Tk \pmod{8}\]
has already been established by one of us [11] in notation involving \(h\), \(h(p)\) and \(t\). The congruence (1.12) will be reproved in this paper in a different way and use of it will be made in proving (1.11). The proof of (1.11) follows the ideas of [9] but with considerable difference in details. The congruence (1.11) can be expressed in the equivalent form
\[hk = T \pmod{16},\]
and this is analogous to the congruence obtained in [9] for primes \(p = 1 \pmod{8}\), which can be formulated
\[hk = T + p - 1 \pmod{16},\]
since the class numbers of the rings \(A\) and \(B\) coincide when \(p = 1 \pmod{8}\).
Before starting the proof, we mention that in the second part of this paper we will prove an analogous formula modulo 16 for the class numbers \( h' \) and \( k' \) of \( Q(\sqrt{-2p}) \) and \( Q(\sqrt{2p}) \). (See Theorem 2, Section 9.)

To prove Theorem 1 we will make use of Dirichlet’s class number formulas for \( h(p) \), \( h(-p) \), and \( h(-2p) \). For \( h(p) \) we use:

\[
(1.13) \quad \sqrt{p} \cdot \xi_p^{h(p)} = \prod (1 - q^j),
\]

where \( q = \exp(2\pi i/p) \). (A \( \pm \) sign under a product (or a sum) symbol will always indicate that the product (or the sum) is taken over those integers \( j \) satisfying \( 1 \leq j \leq p - 1 \) and \( (j,p) = \pm 1 \).) Formula (1.13) is proved in [10], Lemma 1, the square of (1.13) appears in Dirichlet [2], p. 494. From (1.5) and (1.13) we obtain

\[
(1.14) \quad p^{3/2} \eta_p^k = \prod (1 - q^j)^3.
\]

For \( h(-p) \) and \( h(-2p) \) we will use the following formulas ([1], p. 276; [2], p. 493):

\[
(1.15) \quad h = h(-p) = 2(S_0 + S_1),
\]

\[
(1.16) \quad h' = h(-2p) = 2(S_0 - S_3),
\]

where

\[
(1.17) \quad S_j = \sum_{\gcd(i,j) \leq p} \left( \frac{i}{p} \right), \quad j = 0, 1, \ldots, 7.
\]

2. The polynomials \( G_+(z) \) and \( G_-(z) \). Formula (1.14) suggests introducing the polynomials

\[
(2.1) \quad G_+(z) = \prod (z - q^j)^3, \quad G_-(z) = \prod (z - q^j)^3.
\]

With this notation (1.14) can be rewritten

\[
(2.2) \quad G_-(1) = p^{3/2} \eta_p^k.
\]

Setting

\[
(2.3) \quad G(z) = \prod_{j=1}^{p-1} (z - q^j)^3 = G_+(z)G_-(z),
\]

and noting that

\[
(2.4) \quad G(1) = p^3 = G_+(1)G_-(1),
\]

we have (as \( k \) is odd)

\[
(2.5) \quad G_+(1) = -p^{3/2} \eta_p^k,
\]

where \( \eta_p = T - UV \sqrt{p} = -\eta_p^{-1} \).
Next, as in the proof of Lemma 2 of [9], we obtain
\[ G_\pm(1)G_\pm(-1) = G_\mp(1), \]
from which we deduce, by appealing to (2.2) and (2.5)
\[ G_+(1) = \eta_p^{2k}, \quad G_-(1) = \eta_p^{2k}. \]

Further, following the proof of Lemma 3 in [9] we obtain, using here (1.15):
\[ G_+(i) = -\varepsilon i\eta_p^k, \quad G_-(i) = -\varepsilon i\eta_p^k, \]
where
\[ \varepsilon = (-1)^{(k-2)/4}. \]
We note that
\[ h = 2\varepsilon \pmod{8}, \quad \varepsilon h = 2 \pmod{8}. \]

We also note that, if \( \omega = \exp(2\pi i/8) = (1+i)/\sqrt{2} \) (so that \( \omega^2 = i, \omega^3 = -1, \omega + \omega^3 = i\sqrt{2}, \omega - \omega^3 = \sqrt{2} \)), then:
\[ G_\pm(\omega)G_\pm(\omega) = G_\mp(i) \]
follows easily from the definition (2.1), as \( p = 5 \pmod{8} \). Finally we observe that
\[ \frac{1}{2}(\eta_p^k + \eta_p'^k) = \frac{1}{2}(T + UVp)^k + \frac{1}{2}(T - UVp)^k \]
and
\[ \frac{1}{2\sqrt{p}}(\eta_p^k - \eta_p'^k) = \frac{1}{2\sqrt{p}}(T + UVp)^k - \frac{1}{2\sqrt{p}}(T - UVp)^k \]
are rational integers. Moreover, as \( k \) is odd and \( T = 2 \pmod{4} \) we have:
\[ \frac{1}{2}(\eta_p^k + \eta_p'^k) = \sum_{s=0}^{(k-1)/2} \binom{k}{2s+1} T^{2s+1} (pU^2)^{(k-1)/2-s} \]
\[ = kT(pU^2)^{(k-1)/2} + \frac{k}{3} T^3 (pU^2)^{(k-3)/2} \pmod{16} \]
\[ = kT5^{(k-1)/2} + 4 \binom{k}{3} T \pmod{16} \]
\[ = kT[2k - 1 + 2k(k - 1)] \pmod{16}, \]
that is
\[ \frac{1}{2}(\eta_p^k + \eta_p'^k) = kT \pmod{16}. \]
Similarly we obtain

\[(2.12) \quad \frac{1}{2\sqrt{p}}(\eta_{p}^k - \eta_{p}'^k) = U = 4l + 1 \pmod{16}.\]

### 3. The polynomials \(Y(z)\) and \(Z(z)\)

The polynomials \(\prod_{\gamma \neq \infty} (z - \gamma')\) are each of degree \(\frac{1}{2}(p - 1) = 4l + 2\) and their coefficients belong to the ring of integers of \(O(\sqrt{p})\). It follows that \(G_{+}(z)\) and \(G_{-}(z)\) are polynomials of degree \(12l + 6\) which can be expressed in the form

\[(3.1) \quad G_{+}(z) = \frac{1}{2}(Y(z) - Z(z)\sqrt{p}), \quad G_{-}(z) = \frac{1}{2}(Y(z) + Z(z)\sqrt{p}),\]

where \(Y(z)\) and \(Z(z)\) are polynomials of degree at most \(12l + 6\) with ational integral coefficients. From (3.1) we have

\[(3.2) \quad Y(z) = G_{-}(z) + G_{+}(z), \quad Z(z) = \frac{1}{\sqrt{p}}(G_{-}(z) - G_{+}(z)).\]

It is easily deduced from (2.1) that for \(z \neq 0\)

\[s^{3l+6}G_{\pm}(1/z) = G_{\pm}(z),\]

so that by (3.2)

\[s^{3l+6}Y(1/z) = Y(z), \quad s^{3l+6}Z(1/z) = Z(z).\]

Hence the coefficient of \(s^n\) \((n = 0, 1, 2, \ldots, 6l + 2)\) in \(Y(z)\) (resp. \(Z(z)\)) is the same as that of \(s^{3l+6-n}\). Using (2.2), (2.5) and (3.2) with \(z = 1\), we see that \(Y(1)\) and \(Z(1)\) are both even. Hence the middle coefficients of \(s^{6l+3}\) of \(Y(z)\) and \(Z(z)\) are both even. Thus we can set

\[(3.3) \quad Y(z) = \sum_{n=0}^{6l+3} a_n(z^n + s^{3l+6-n}),\]

\[Z(z) = \sum_{n=0}^{6l+3} b_n(z^n + s^{3l+6-n}),\]

where the \(a_n\) and \(b_n\) are integers.

We now state three relations between the polynomials \(Y(z)\), \(Z(z)\) and their derivatives (equations (3.4), (3.5), (3.10) below), which we will make use of later. The first two of these are trivial, the third is an extension of a result of Liouville [8].

From (3.1) and (2.5) we have (cf. [4], p. 427)

\[(3.4) \quad Y^2(z) - pZ^2(z) = 4G(z),\]

and by differentiating (3.4) we obtain

\[(3.5) \quad Y(z)Y'(z) - pZ(z)Z'(z) = 2G'(z).\]
Taking $z = \omega$ in (3.4) and (3.5) we obtain
\begin{equation}
Y^2(\omega) - pZ^2(\omega) = -20\omega - 28i - 20\omega i,
\end{equation}
\begin{equation}
Y(\omega) Y'(\omega) - pZ(\omega) Z'(\omega)
= (51 - 9p) + 21(1 - p)\omega - 21(1 + p)\omega^3 - (51 + 9p)\omega^3.
\end{equation}

Next we introduce the polynomial
\begin{equation}
K(z) = \sum_{s=1}^{p-1} \left( \frac{s}{p} \right) z^{p-1}.
\end{equation}

Using the Gauss sum
\begin{equation}
\sum_+ g^j - \sum_- g^j = \sqrt{p},
\end{equation}
we easily deduce the following partial fraction decomposition:
\begin{equation}
\frac{K(z)}{z^p - 1} \sqrt{p} = \sum_+ \frac{1}{z - g^j} - \sum_- \frac{1}{z - g^j}.
\end{equation}

Since by (2.1), (3.2) and (3.9)
\begin{equation}
Y'Z - YZ' = \frac{2}{\sqrt{p}} (G'_+ G_- G'_+ G_-) = \frac{6G}{\sqrt{p}} \left( \sum_+ \frac{1}{z - g^j} - \sum_- \frac{1}{z - g^j} \right)
\end{equation}
we obtain
\begin{equation}
Y'Z - YZ' = 6 \left( \frac{z^p - 1}{z - 1} \right)^2 K(z).
\end{equation}

In order to apply (3.10) with $z = \omega$ we must first evaluate $K(\omega)$. This is done as in the first part of § 7 of [9]. We have
\begin{equation}
K(\omega) = \sum_{s=1}^{p-1} \left( \frac{s}{p} \right) \omega^{p-1-s} = - \sum_{s=1}^{p-1} \left( \frac{s}{p} \right) \omega^{-s}.
\end{equation}

For $j = 0, 1, 2, \ldots, 7$ we set $s = 8r - j$.

As $1 \leq 8r - j < 8l + 5$, we have
\begin{align*}
r & = 1, \ldots, l, \quad \text{for} \quad j = 0, 1, 2, 3, \\
r & = 1, \ldots, l+1, \quad \text{for} \quad j = 4, 5, 6, 7.
\end{align*}

Then, as $-\left( \frac{8r - j}{p} \right) = \left( \frac{2r + (2l+1)j}{p} \right)$, we find that
\begin{equation}
K(\omega) = - \sum_{j=0}^{7} \omega^j T_j
\end{equation}
where

\[
T_j = \begin{cases} 
\sum_{r=1}^{l} \left( \frac{2r + (2l+1)j}{p} \right), & j = 0, 1, 2, 3, \\
\sum_{r=1}^{l+1} \left( \frac{2r + (2l+1)j}{p} \right), & j = 4, 5, 6, 7.
\end{cases}
\]

Noting that, with definition (1.16), \( S_j = S_{7-j} \), we find that

\[
T_j = \begin{cases} 
-S_0, & j = 0, 3, \\
-S_1, & j = 5, 6, \\
-S_2, & j = 1, 2, \\
-S_3, & j = 4, 7,
\end{cases}
\]

so that

\[(3.11) \quad K(\omega) = (1 + \omega^2)(S_0 - S_3) + (\omega + \omega^2)(S_2 - S_1).\]

Now it has been proved by Gauss and Dedekind (\([3]\), p. 301 = \([4]\), p. 694), as well as by Dirichlet (\([2]\), p. 493), (cf. also \([5]\)) that:

\[(3.12) \quad 4S_0 = -h + h'; \quad 4S_1 = 3h - h'; \quad 4S_3 = -h - h'.\]

As \( S_0 = l \pmod{2} \) and \( S_1 = S_3 = l+1 \pmod{2} \), each of these relations proves the well-known result:

\[(3.13) \quad h' \equiv h + 4l \pmod{8}.\]

Using \((3.12)\) in \((3.11)\) we have (as \( S_0 + S_1 + S_2 + S_3 = 0 \)):

\[(3.14) \quad 4h = K(\omega)(1 - \omega + \omega^3 + \omega^5) + K(-\omega)(1 + \omega + \omega^3 - \omega^5),\]

\[(3.15) \quad 2h' = K(\omega)(1 - \omega) + K(-\omega)(1 + \omega).\]

Taking \( z = \pm \omega \) in \((3.14)\) and \((3.15)\) we find:

\[(3.16) \quad 12h = (5(1 + \omega^2) - 7\omega)(Y'(\omega)Z(\omega) - Y(\omega)Z'(\omega)) + (5(1 + \omega^2) + 7\omega)(Y'(-\omega)Z(-\omega) - Y(-\omega)Z'(-\omega)),\]

\[(3.17) \quad 12h' = (7(1 + \omega^2) - 10\omega)(Y'(\omega)Z(\omega) - Y(\omega)Z'(\omega)) + (7(1 + \omega^2) + 10\omega)(Y'(-\omega)Z(-\omega) - Y(-\omega)Z'(-\omega)).\]

Both expressions \((3.16)\) and \((3.17)\) have the form:

\[H = (a(1 + \omega^2) - \beta\omega)(Y'(\omega)Z(\omega) - Y(\omega)Z'(\omega)) + (\gamma)(\delta),\]

where \((\gamma)\) is the same expression with \(- \omega\) instead of \(\omega\).
In Sections 7 and 8 we will find (see (7.30) and (8.29))
\[ Y'(\omega)Z(\omega) - Y(\omega)Z'(\omega) = a(1 - \omega^2) + b\omega^3 \]
with the expressions for \( a \) and \( b \) depending on the parity of \( l \). Then, clearly:
\[ (3.18) \quad H = 4aa + 2b\beta. \]

4. Congruences for the coefficients of \( Y(z) \) and \( Z(z) \). We begin by introducing the following notation. Whenever we write \( \sum a_{n+f} \) it will be understood that \( e \) and \( f \) are fixed rational integers such that \( 0 \leq f < e \) and that the variable of summation \( n \) varies so that \( 0 \leq en+f \leq 6l+3. \)

From (3.3), (3.2), (2.2), (2.5), (2.12), we have
\[ \sum a_n = \frac{1}{2} Y(1) = \frac{1}{2}(G_-(1) + G_+(1)) = \frac{1}{2}p^{32}(\eta_p^k - \eta_p'^k) = p^2(4l+1) \mod 16 \]
that is
\[ (4.1) \quad \sum a_n = 4l + 9 \mod 16. \]
Similarly we obtain
\[ (4.2) \quad \sum b_n = 5Tk \mod 16. \]
Similarly, making use of \( Y(-1), Z(-1), Y(i) \) and \( Z(i) \), we obtain
\[ (4.3) \quad \sum a_n(-1)^n = 9 \mod 16, \]
\[ (4.4) \quad \sum b_n(-1)^n = -2Tk \mod 16, \]
\[ (4.5) \quad \sum a_{2n+1}(-1)^n = -\varepsilon Tk \mod 16, \]
\[ (4.6) \quad \sum b_{2n+1}(-1)^n = -\varepsilon(4l+1) \mod 16. \]
Adding and subtracting these congruences appropriately, we get
\[ (4.7) \quad \sum a_{2n} = 2l+1 \mod 8, \]
\[ (4.8) \quad \sum b_{2n} = \frac{3Tk}{2} \mod 8, \]
\[ (4.9) \quad \sum a_{2n+1} = 2l \mod 8, \]
\[ (4.10) \quad \sum b_{2n+1} = \frac{Tk}{2} \mod 8, \]
\[ (4.11) \quad \sum a_{4n+1} = l - \frac{\varepsilon Tk}{2} \mod 4, \]
\[ \sum_{\beta_{4n+1}} = \begin{cases} \frac{2 - (2e + Tk)}{4} \pmod{4}, & \text{if } l \text{ odd}, \\ \frac{-(2e + Tk)}{4} \pmod{4}, & \text{if } l \text{ even}, \end{cases} \]

\[ \sum a_{4n+3} = l + \frac{eTk}{2} \pmod{4}, \]

\[ \sum_{\beta_{4n+3}} = \begin{cases} \frac{2 + (2e - Tk)}{4} \pmod{4}, & \text{if } l \text{ odd}, \\ \frac{(2e - Tk)}{4} \pmod{4}, & \text{if } l \text{ even}. \end{cases} \]

5. Evaluation of \( Y(\omega) \) and \( Z(\omega) \). Taking \( z = \omega \) in (3.3) we obtain

\[ Y(\omega) = L + 2M\omega + (-1)^{l-1}L\omega + 2N\omega i, \]

\[ Z(\omega) = L' + 2M'\omega + (-1)^{l-1}L'i + 2N'\omega i, \]

where

\[ L = \sum a_{4m} (-1)^m + (-1)^{l-1} \sum a_{4m+2} (-1)^m, \]

\[ M = \frac{1}{2} \left[ 1 + (-1)^{l-1} \sum a_{4m+1} (-1)^m \right], \]

\[ N = \frac{1}{2} \left[ 1 + (-1)^l \sum a_{4m+3} (-1)^m \right]. \]

\( L', M', N' \) are defined as in (5.3), (5.4), (5.5) by replacing \( a_n \) by \( b_n \) (equations (5.3)', (5.4)', (5.5)'). Clearly

\[ M = M' = 0, \quad \text{if } l \text{ even}, \]

\[ N = N' = 0, \quad \text{if } l \text{ odd}, \]

suggesting that we treat the two cases \( l \text{ odd and } l \text{ even separately.} \)

Case (i): \( l \text{ odd}. \) From (5.1), (5.2) and (5.6) we have

\[ Y(\omega) = L + 2M\omega + L\omega, \quad Z(\omega) = L' + 2M'\omega + L'i. \]

Appealing to (3.6) we obtain

\[ L^2 + 2M^2 - pL'^2 - 2pM'^2 = -14, \]

\[ LM - pL'M' = -5. \]

Further using (2.7), (2.10), (2.11), (2.12), (3.1) and (5.7), we get

\[ L^2 - 2M^2 + pL'^2 - 2pM'^2 = -2eTk \pmod{32}, \]

\[ LL' - 2MM' = e(4l+1) \pmod{16}. \]
Finally we have
\[ L = \sum a_{4m}(-1)^m + \sum a_{4m+2}(-1)^n \quad \text{(by (5.3))} \]
\[ = \sum a_{4m} + \sum a_{4m+2} \pmod{2} = \sum a_{2m} \pmod{2}, \]
\[ = 1 \pmod{2} \quad \text{(by (4.7))}. \]

Similarly we obtain \( L' = 1 \pmod{2} \) and \( M = 0 \pmod{2} \). Then, appealing to (5.8), we get \( M' = 1 \pmod{2} \). Summarizing we have
\[ (5.12) \quad L = L' = M' = 1 \pmod{2}, \quad M = 0 \pmod{2}. \]

Case (ii): \( l \) even. From (5.1), (5.2) and (5.6) we have
\[ (5.13) \quad Y(\omega) = L - Li + 2Ni, \quad Z(\omega) = L' - L'i + 2N'i. \]

Appealing to (3.6) we obtain
\[ (5.14) \quad L^2 + 2N^2 - pL'^2 - 2pN'^2 = 14, \]
\[ (5.15) \quad LN - pL'N' = -5. \]

Further using (2.7), (2.10), (2.11), (2.12), (3.1) and (5.13),
\[ (5.16) \quad L^2 - 2N^2 + pL'^2 - 2pN'^2 = 2\varepsilon Tk \pmod{32}, \]
\[ (5.17) \quad LL' - 2NN' = -\varepsilon(4l+1) \pmod{16}. \]

As in the case when \( l \) is odd, we obtain
\[ (5.18) \quad L = L' = N = 1 \pmod{2}, \quad N' = 0 \pmod{2}. \]

It is convenient to note here that
\[ (5.19) \quad L^2 = 3 - \varepsilon Tk \pmod{16}, \quad \text{if} \quad l \text{ is odd,} \]
and
\[ (5.20) \quad L'^2 = -1 - 3\varepsilon Tk \pmod{16}, \quad \text{if} \quad l \text{ is even,} \]
follow from (5.8), (5.10), (5.12) and (5.14), (5.16), (5.18) respectively.

6. Proof of \( h = Tk \pmod{8} \). We consider the two cases.

Case (i): \( l \) odd. From (4.12), (5.4)' and (5.12), we have
\[ 1 = M' = \sum b_{4m+1} = -\frac{1}{2}(2\varepsilon + Tk) \pmod{2}, \]
so, as \( 2\varepsilon = h \pmod{8} \), we have
\[ Tk = -2\varepsilon - 4 = 2\varepsilon = h \pmod{8}. \]

Case (ii): \( l \) even. From (4.14), (5.5)' and (5.18), we have
\[ 0 = N' = \sum b_{4m+3} = \frac{1}{4}(2\varepsilon - Tk) \pmod{2}, \]
We close this section by noting that the congruence \( h \equiv T_k \) (mod 8) enables us to obtain from (4.11), (4.12), (4.13), (4.14):

\[
\sum a_{4n+1} \equiv l-1 \pmod{4},
\]

\[
\sum b_{4n+1} \equiv 1 \pmod{2},
\]

\[
\sum a_{4n+3} \equiv l+1 \pmod{4},
\]

\[
\sum b_{4n+3} \equiv 0 \pmod{2}.
\]

7. Proof of \( h \equiv T_k \) (mod 16). Case (i): \( l \) odd. Differentiating (3.3) with respect to \( \varepsilon \) and setting \( \varepsilon = \omega \) we obtain

\[
Y'(\omega) = 2P + 2Q\omega + 8R\varepsilon + 4S\varepsilon^2,
\]

\[
Z'(\omega) = 2P' + 2Q'\omega + 8R'\varepsilon + 4S'\varepsilon^2,
\]

where \( P, Q, \ldots, S' \) are integers given by the following formulae:

\[
P = (6l+3) \sum a_{4n+1} (-1)^m,
\]

\[
Q = \sum ((6l+3-2m)a_{4m} + (2m+1)a_{4m+2}) (-1)^m,
\]

\[
R = \sum \left(m - \frac{3l}{2}\right) a_{4m+1} (-1)^m,
\]

\[
S = \sum (-ma_{4m} -(3l-m+1)a_{4m+2}) (-1)^m,
\]

and \( P', Q', R', S' \) are given by the corresponding formulae (eqns. (7.7)–(7.10)) where each \( a_n \) above is replaced by \( b_n \). We note that (6.3) and (6.4) guarantee that \( R \) and \( R' \) are integers.

From (5.4) and (5.4)' we see that

\[
P = (6l+3)M, \quad P' = (6l+3)M',
\]

and, from (5.3) and (5.3)', that

\[
Q = 2S + (6l+3)L, \quad Q' = 2S' + (6l+3)L'.
\]

These two equations show that, of the quantities \( P, Q, R, S, P', Q', R' \) and \( S' \), we need only consider \( R, R', S \) and \( S' \). It will suffice to deter-
mine them modulo 2. From (7.9), as \((2m+1)(-1)^m = 1 \pmod{4}\) and as \(3l+1\) is even, we have

\[
2R' = \sum (2m+1)(-1)^m b_{4m+3} - (3l+1) \sum b_{4m+3} (-1)^m
\]

\[
= \sum b_{4m+3} - (3l+1) \sum b_{4m+3} = l \sum b_{4m+3} = l \left(2 + \frac{(2e-Tk)}{4}\right) \pmod{4},
\]

by (4.14), that is:

\[
R' = 1 + \frac{1}{l}(2e-Tk) \pmod{2}.
\]  

(7.13)

Similarly we obtain

\[
R = \frac{1}{l}(l+1) \pmod{2},
\]

(7.14)

\[
S = \frac{1}{l}(L+1) \pmod{2},
\]

(7.15)

\[
S' = \frac{1}{l}(L'-1) + \left(2 + \frac{Tk}{4}\right) \pmod{2}.
\]

(7.16)

We will now show that

\[
S = S' \pmod{2}.
\]  

(7.17)

From (5.11) and (5.12) we have

\[
L+L'-1 = LL' = \varepsilon \pmod{4}.
\]

Hence, from (7.15), (7.16) and the result \(Tk = 2\varepsilon \pmod{8}\), we have

\[
S + S' = \frac{1}{l}(L+L') + \frac{(2+Tk)}{4} = \frac{1}{l}(1+\varepsilon) + \frac{1}{l}(2+2\varepsilon) = 0 \pmod{2}.
\]

Next we replace \(Y(\omega), Y'(\omega), Z(\omega), Z'(\omega)\) in (3.7) by the formulae given in (5.7), (7.1), (7.2) obtaining (in view of (5.8) and (5.9)):

\[
2LR + 2MS - p(2L'R' + 2M'S') = 3l - 9,
\]  

(7.18)

\[
8MR + 4LS - p(8M'R' + 4L'S')
\]

\[
= -(6l+3)(L'-pL') - 48 - 36l.
\]

We have used (7.11) and (7.12) to eliminate \(P, P', Q, Q'\).

The next step is to use (5.9) and (5.11) to obtain \(L'\) and \(M\) in terms of \(L\) and \(M'\) modulo 8. We get:

\[
L' = 3\varepsilon L + 2M' \pmod{8},
\]

(7.20)

\[
M = -3L - \varepsilon M' \pmod{8}.
\]  

(7.21)

Using (7.13), (7.14), (7.15), (7.17) and (5.12) in (7.18), we obtain

\[
4L = 4 + Tk - 2\varepsilon \pmod{16}.
\]  

(7.22)
Next using (5.19) and (7.20) we obtain

\[(7.23) \quad L^2 - pL'^2 = 8 + 4eLM' = 4eL + 4eM' + 8 - 4e \pmod{16} \]

Writing (7.19) modulo 16 we obtain by using (5.12), (7.13) and (7.23)

\[(7.24) \quad 4(LS - L'S') = 4L + 4M' + 6e - 4l - Tk \pmod{16}.\]

As \(4(L + L')(S - S') = 0 \pmod{16}\) by (5.12) and (7.17), (7.24) gives

\[(7.25) \quad 4(L'S - LS') = -4L - 4M' - 6e + 4l + Tk \pmod{16}.\]

We need also the following which follow easily using (5.12), (7.13), (7.14), (7.15) and (7.17):

\[(7.26) \quad 8(LE' - L'E) = 4l + 4 + 2e - Tk \pmod{16},\]

\[(7.27) \quad 8(MR' - MR') = 4l + 4 \pmod{16},\]

\[(7.28) \quad 8(MS' - MS') = 4L + 4 \pmod{16},\]

and using (7.20) and (7.21) we have

\[(7.29) \quad L'M - LM' = -2L - 2M' - 3e + 2 \pmod{8}.\]

Using the expressions for \(Y(\omega), Z(\omega), Y'(\omega), Z'(\omega)\) given in (5.7), (7.1) and (7.2), we obtain

\[Y'(\omega)Z(\omega) - Y(\omega)Z'(\omega) = a - ao^2 + bo^2,\]

where

\[(7.30) \quad a = 8(LE' - L'E) + 8(MS' - MS') + 2(6l + 3)(L'M - LM'),\]

\[b = 8(L'S - LS') + 16(MR' - MR').\]

Then using (3.16), (3.17) and (3.18) we obtain:

\[(7.31) \quad 3h = 10(6l + 3)(L'M - LM') + 40(MS' - MS') +
\quad + 40(LE' - L'E) + 28(L'S - LS') + 56(MR' - MR'),\]

\[(7.32) \quad 3h' = 56(LE' - L'E) + 56(MS' - MS') + 14(6l + 3)(L'M - LM') +
\quad + 40(L'S - LS') + 80(MR' - MR').\]

Using (7.22), (7.25), (7.26), (7.27), (7.28) and (7.29) in (7.31), we obtain

\[3h = 8 - Tk \pmod{16}\]

which for \(l\) odd, is equivalent to our main result (see (1.11))

\[h \equiv Tk \pmod{16}.\]
Using now (1.11), (7.22), (7.25), (7.26), (7.27), (7.28) and (7.29) in (7.32), we have:

\[(7.33) \quad h' = h + 4M' \pmod{16}.
\]

We will use (7.33) in Sections 9 to 12. We note that it is consistent with (3.13), as \(M'\) is odd.

**8. Proof of** \(h = Tk \pmod{16}\). **Case (ii):** \(l\) even. Differentiating (3.3) with respect to \(z\) and setting \(z = \omega\) we obtain

\[
(8.1) \quad Y'(\omega) = 4P + 2Q\omega + 2R\omega^2 + 4S\omega^3,
\]

\[
(8.2) \quad Z'(\omega) = 4P' + 2Q'\omega + 2R'\omega^2 + 4S'\omega^3,
\]

where \(P, Q, \ldots, S'\) are integers given by the following formulae:

\[
(8.3) \quad P = \sum (2m - 3l - 1)a_{4m+1}\zeta(-1)^m,
\]

\[
(8.4) \quad Q = \sum ((2m - 3 - 6l)a_{4m} + (2m + 1)a_{4m+2})(-1)^m,
\]

\[
(8.5) \quad R = (6l + 3) \sum a_{4m+3}\zeta(-1)^m,
\]

\[
(8.6) \quad S = \sum (-ma_{4m} + (3l + 1 - m)a_{4m+2})(-1)^m,
\]

and \(P', Q', R', S'\) are given by the corresponding formulae (equations (8.7)–(8.10)) obtained from the above by replacing each \(a_n\) by \(b_n\). From (5.5) we see that

\[
(8.11) \quad R = (6l + 3)N, \quad R' = (6l + 3)N',
\]

and

\[
(8.12) \quad Q = -2S - (6l + 3)L, \quad Q' = -2S' - (6l + 3)L'.
\]

These show that, of the quantities \(P, Q, R, S, P', Q', R'\) and \(S'\), we need only consider \(P, P', S\) and \(S'\). It suffices to determine \(P\) and \(P'\) modulo 4 and \(S\) and \(S'\) modulo 2.

From (8.7), as \((2m - 1)(-1)^m = -1 \pmod{4}\) and \(l\) is even, we have, using (4.12)

\[
P' = \sum (2m - 1)(-1)^mb_{4m+1} - 3l \sum b_{4m+1}\zeta(-1)^m
\]

\[= -\sum b_{4m+1} - 3l \sum b_{4m+1}(\zeta^{-1})^m \pmod{4}
\]

\[= -(1 + 3l) \sum b_{4m+1}(\zeta^{-1})^m \pmod{4}
\]

\[= (1 - l) \frac{(2e + Tk)}{4} \pmod{4},
\]
that is

\[(8.13) \quad P' = \frac{2\varepsilon + Tk}{4} - 1 \pmod{4}.\]

Similarly, using (6.1) for $P$; using (4.7), (8.4) and (8.12) for $S$; and using (1.12), (4.8), (8.8) and (8.12) for $S'$; we obtain

\[(8.14) \quad P \equiv 1 \pmod{4},\]
\[(8.15) \quad S = \frac{1}{2}(L-1) \pmod{2},\]
\[(8.16) \quad S' = \frac{1}{2}(L' + 1) + \frac{(h-2)}{4} \pmod{2}.\]

We now use (5.17) to show that

\[(8.17) \quad S = S' \pmod{2}.\]

From (5.17) and (5.18) we have

\[L + L' - 1 = LL' = -\varepsilon \pmod{4}.\]

Hence from (8.15) and (8.16)

\[S + S' = \frac{(L + L')}{2} + \frac{(h-2)}{4} = \left(\frac{1 - \varepsilon}{2}\right) + \left(\frac{\varepsilon - 1}{2}\right) = 0 \pmod{2}.\]

Next we put the expressions for $Y(\omega), Z(\omega), Y'(\omega), Z'(\omega)$ given in (5.13), (8.1) and (8.2) into (3.7) obtaining (in view of (5.14) and (5.15))

\[(8.18) \quad LP + 2NS - p(L'P' + 2N'S') = 24 + 27l,\]
\[(8.19) \quad 2NP + 2LS - p(2N'P' + 2L'S') = (6l + 3)(N^2 - pN'^2) - 45 - 60l.\]

(We have used (8.11) and (8.12) to eliminate $Q, Q', R, R'$.)

The next step is to use (5.15) and (5.17) to obtain $L'$ and $N$ in terms of $L$ and $N'$ modulo 8. We get:

\[(8.20) \quad L' = -\varepsilon L + 2N' \pmod{8},\]
\[(8.21) \quad N = 3L + 3\varepsilon N' \pmod{8}.\]

Using (1.12), (5.18), (8.13), (8.14), (8.15), and (8.20) in (8.18) taken modulo 4, we obtain

\[(8.22) \quad 4L = -6\varepsilon - Tk + 4 \pmod{16}.\]

Next from (5.18) we have:

\[(8.23) \quad N^2 - pN'^2 = 1 - 5N'^2 = 1 + 2N' \pmod{8},\]
so that (8.19) gives:

\[ LS - L'S' = L + N' + l - 1 \pmod{4}, \]

which, combined with \((L + L')(S - S') = 0 \pmod{4}\), gives

\[ L'S - LS' = -L + N' - l + 1 \pmod{4}. \]

We note also the following:

\[
\begin{align*}
4(L'P - LP') &\equiv 4l - 6\varepsilon L - LTk \pmod{16}, \\
4(N'P - NP') &\equiv 4l - 6\varepsilon L - 3LTk \pmod{16}, \\
4(LP - LP') - 4(NP - NP') &\equiv 4L + 4\varepsilon - 4 \pmod{16},
\end{align*}
\]

\[ 8(N'S - NS') \equiv 4L - 4 \pmod{16}, \]

\[ LN' - L'N \equiv 3\varepsilon - 2N' \pmod{8}. \]

Using the expressions for \(Y(\omega), Z(\omega), Y'(\omega), Z'(\omega)\) given in (5.13), (8.1), (8.2) we obtain (eliminating \(Q, Q', R, R'\) with the help of (8.11), (8.12))

\[ Y'(\omega)Z(\omega) - Y(\omega)Z'(\omega) = a - a\omega^2 + b\omega^3, \]

where

\[
\begin{align*}
a &= 4(L'P - LP') - 2(6l + 3)(L'N - LN') + 8(N'S - NS'), \\
b &= 8(N'P - NP') + 8(L'S - LS').
\end{align*}
\]

Then, using (3.16), (3.17) and (3.18) we obtain:

\[ 3h = 20(L'P - LP') + 28(N'P - NP') + 28(L'S - LS') + 40(N'S - NS') + 30(2l + 1)(LN' - L'N), \]

and

\[ 3h' = 28(L'P - LP') + 56(N'S - NS') - 14(6l + 3)(L'N - LN') + 40(N'P - NP') + 40(L'S - LS'). \]

Using (8.22), (8.25), (8.26), (8.27) and (8.28) in (8.30), we obtain

\[ 3h \equiv Tk + 4\varepsilon \pmod{16}, \]

which, for \(l\) even, is equivalent to our main result (see (1.11))

\[ h \equiv Tk \pmod{16}. \]

Now, using (1.11) in (8.31) together with (8.22), (8.25), (8.26), (8.27) and (8.28), we obtain

\[ 4N' \equiv h' - h + \varepsilon h - 2 \pmod{16}. \]
We note that (8.32) is consistent with (3.13), as $\varepsilon h = 2 \pmod{8}$ and as $N'$ is even. Use will be made of (8.32) in Sections 9 to 12.

II. $Q(\sqrt{2p})$ and $Q(\sqrt{-2p})$

9. Introduction to the second part. In this part (Sections 9, 10, 11, 12) we consider the ideal class numbers $h' = h(-2p)$ and $k' = h(2p)$ of the quadratic fields $Q(\sqrt{-2p})$ and $Q(\sqrt{2p})$ respectively. It is well known that $h' = h' = 2 \pmod{4}$ and we have already mentioned that $h' = h + 4t \pmod{8}$ (see (3.13)).

The fundamental unit of $Q(\sqrt{2p})$ is:

$$\varepsilon_{2p} = V + W\sqrt{2p},$$

where $V$, $W$ are the smallest positive rational integers such that

$$V^2 - 2pW^2 = -1.$$  

The positive integers $V$, $W$ are both odd and:

$$V = \pm 3 \pmod{8}; \quad W = 1 \pmod{4}.$$  

The aim of the second part is to prove the following

**Theorem 2.** Let $p = 8l + 5$ be a prime. Then

$$h' = 2(W - 1) + 3k' V + 8l \pmod{16}.$$  

Modulo 8 this result reduces to:

$$h' = k' + 2V + 2 \pmod{8},$$

which has already been proved by one of us [10]. We reprove (9.5) and use it in the proof of (9.4).

To prove (9.4) we will evaluate $\prod (\omega - \zeta^j)$ as:

$$\prod (\omega - \zeta^j) = (-1)^j \eta_p^{-k/4} \varepsilon_{2p}^{(h-k)/4} \omega (1 + \sqrt{2})^{1/2}.$$  

The proof of (9.6) is similar to the proof given in [6], Lemma, to evaluate $F_p(\omega)$ when $p = 1 \pmod{8}$, and will be given in the next section.

We will need the sixth power of (9.6) which will be written as:

$$\frac{1}{2} \left\{ Y(\omega) + Z(\omega) \sqrt{2p} \right\}^2 = (-1)^{j+1} 2i \eta_p^{-k} \varepsilon_{2p}^{2g+1} (7 + 5\sqrt{2}) = (-1)^j A$$

where we define the rational integer $g$ by

$$3k' = 2g + 1.$$
We note that \( k' = 2 \) or \( 6 \) (mod 8) according as \( g \equiv 1 \) or \( 0 \) (mod 2) so that:

\[
\varepsilon' = (-1)^{(k'-2)4} = -(1)^g = -1 + 2g^2 \, (\text{mod } 8);
\]

(9.9)

\[
2\varepsilon' = k' \, (\text{mod } 8).
\]

Rational integers \( T_1, U_1, V_1, W_1 \) are defined by:

\[
T_1 + U_1 \sqrt{p} = -\eta_p^{-k}; \quad V_1 + W_1 \sqrt{p} = \eta_p^{2g+1}.
\]

Then we have:

\[
\mathcal{A} = 2(T_1 + U_1 \sqrt{p})(V_1 + W_1 (\omega - \omega^2) \sqrt{p})[5(\omega + \omega^2) + 7\omega^g],
\]

that is

(9.11)

\[
\mathcal{A} = (10T_1 V_1 + 14p U_1 W_1)(\omega + \omega^2) + (14T_1 V_1 + 20p U_1 W_1)i +
+(10U_1 V_1 + 14T_1 W_1)(\omega + \omega^2) \sqrt{p} + (14 U_1 V_1 + 20 T_1 W_1)4 \sqrt{p}.
\]

Applying the binomial theorem in (9.10) written in the form:

\[
T_1 + U_1 \sqrt{p} = (T - U \sqrt{p})^k; \quad V_1 + W_1 \sqrt{p} = (V + W \sqrt{p})^{2g+1},
\]

we find the following congruences:

(9.13)

\[
T_1 \equiv h \, (\text{mod } 16); \quad U_1 \equiv -(4l + 1) \, (\text{mod } 16),
\]

(9.14)

\[
V_1 \equiv V(1 - 2g^2) \, (\text{mod } 8); \quad W_1 \equiv 1 \, (\text{mod } 4),
\]

(9.15)

\[
W_1 \equiv W(1 + 2g + 2g^2) \equiv W + 2g(g + 1) \, (\text{mod } 8).
\]

Using (9.13), (9.14), (9.15) we obtain congruences modulo 16 or 8 for the coefficients of \( i, \omega + \omega^2, i\sqrt{p}, (\omega + \omega^2)\sqrt{p} \) in \( \mathcal{A} / 2 \mathcal{A} / 2 \):
(10.2) \[ 3k(p) \log \varepsilon_p = k \log \eta_p = \frac{3\sqrt{p}}{2} \sum_{n=1}^{\infty} \frac{1}{n} \left( \frac{p}{n} \right), \]

(10.3) \[ k' = k(-2p) = \frac{2}{\pi} \sqrt{2p} \sum_{n=1}^{\infty} \frac{1}{n} \left( \frac{-8p}{n} \right), \]

(10.4) \[ k' \log \varepsilon_p = \sqrt{2p} \sum_{n=1}^{\infty} \left( \frac{8p}{n} \right) \frac{1}{n}. \]

One finds easily:

(10.5) \[ \prod (\omega - \varepsilon^j) = (-1)^i \prod (1 + \omega^3 \varepsilon^j). \]

We set:

(10.6) \[ x_j = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} \omega^{3n} \varepsilon^{nj}}{n}, \]

so that \( \exp(x_j) = 1 + \omega^3 \varepsilon^j \) and:

(10.7) \[ (-1)^{i-1} \exp(-\omega) = \exp\left( \sum x_j \right). \]

We calculate \( \sum x_j \):

\[ \sum x_j = \sum \sum_{n=1}^{\infty} \frac{(-1)^{n-1} \omega^{3n} \varepsilon^{nj}}{n} = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} \omega^{3n}}{n} \sum \varepsilon^{nj} \]

\[ = \frac{1}{2} \sum_{n=1}^{\infty} \frac{(-1)^{n} \omega^{3n}}{n} + \frac{\sqrt{p}}{2} \sum_{n=1}^{\infty} \frac{(-1)^{n} \omega^{3n}}{n} \left( \frac{n}{p} \right) - \frac{1}{2} \sum_{n=1}^{\infty} \frac{(-1)^{n} \omega^{3np}}{n}, \]

that is

(10.8) \[ \sum x_j = -\frac{1}{2} \log \frac{1 + \omega^3}{1 - \omega^3} + \frac{\sqrt{p}}{2} \sum_{u=0}^{3} \omega^u T_u, \]

where

\[ T_u = \sum_{k=1}^{\infty} \frac{(-1)^k}{4k-u} \left( \frac{4k-u}{p} \right) \quad (u = 1, 2, 3, 4), \]

and where we have used the formula valid for all \( n \):

\[ \sum \varepsilon^{nj} = \frac{1}{2} \left( 1 - \left( \frac{n}{p} \right)^2 \right) \left( p - \frac{1}{2} \frac{n}{p} \right) \sqrt{p} - \frac{1}{2}. \]
Using (10.1)–(10.4) one finds easily, as in [6], Proof of Lemma:

\[ T_0 = -\frac{k}{3\sqrt{p}} \log \eta_p; \quad T_2 = \frac{\pi h}{4\sqrt{p}}; \]
\[ T_1 = -\frac{\pi h'}{4\sqrt{2p}} + \frac{k' \log \varepsilon_{2p}}{2\sqrt{2p}}; \quad T_3 = -\frac{\pi h'}{4\sqrt{2p}} - \frac{k' \log \varepsilon_{2p}}{2\sqrt{2p}}. \]

Using these values in (10.8), we obtain:

\[ \sum x_j = -\frac{k \log \eta_p}{6} + k' \log \varepsilon_{2p} + \frac{\pi i}{4} (h - h') - \frac{1}{2} \log \frac{1 + \omega^3}{1 - \omega^3}, \]

which is (9.6).

11. Case 1: \( \lambda \) odd. Using the values of \( Y(\omega) \) and \( Z(\omega) \) as given in (5.7) one finds:

\[ \frac{1}{2}[Y(\omega) + Z(\omega)\sqrt{p}] = -D = (L^2 + pL'^2 + 2M^2 + 2pM'^2)\log \omega + 2(LM + pL'M')(\omega + \omega^3) + 2k\sqrt{p} [(L'L' + 2MM')\log \omega + (L'M' + LM')(\omega + \omega^3)]. \]

Comparing (11.1) and (9.11) we get:

\[ L^2 + pL'^2 + 2M^2 + 2pM'^2 = -14T_1V_1 - 20pU_1W_1, \]
\[ LM + pL'M' = -5T_1V_1 - 7pU_1W_1, \]
\[ LL' + 2MM' = -7U_1V_1 - 10T_1W_1, \]
\[ LM' + L'M = -5U_1V_1 - 7T_1W_1. \]

Using (5.10), (5.12), (7.20), (7.21) we evaluate the left-hand sides as follows:

\[ L^2 + pL'^2 + 2M^2 + 2pM'^2 = -2\varepsilon Tk + 4M^2 + 4pM'^2 \pmod{32}, \]
\[ = -h^2 + 4 \equiv 0 \pmod{16}, \]
\[ LM + pL'M' = -1 - 2\varepsilon LM' \pmod{8}, \]
\[ LL' + 2MM' = \varepsilon + 4 \pmod{8}, \]
\[ LM' + L'M = -3\varepsilon \pmod{8}. \]

From (11.6), (11.2), (9.16) we obtain

\[ hV(1 - 2\varepsilon^3) \equiv 6 \pmod{8}. \]
Introducing $k'$ by equations (9.9), (11.10) becomes \( \frac{h}{2} \frac{k'}{2} \equiv V \pmod{4} \)
that is:

\[(11.11) \quad h = k'V \pmod{8}.
\]

Remembering that $h' = h + 4 \pmod{8}$, and linearizing we obtain:

\[(11.12) \quad h' = k' + 2V + 2 \pmod{8}.
\]

Now we use (5.12) and (5.19) to solve (5.9) and (5.11) modulo 16, obtaining $L'$ and $M$ as linear functions of $L$ and $M'$:

\[(11.13) \quad L' = (5h + \varepsilon)L + 10M' + 8 + 8l' \pmod{16},
\]
\[(11.14) \quad M = -(\varepsilon h + 1)L + (9h - 3\varepsilon)M' + 8 + 8l' \pmod{16},
\]
where the integer $l'$ is defined by

\[(11.15) \quad 4l + 1 = 8l' + 5.
\]

Thus, using (7.22) and (7.33), we find

\[(11.16) \quad LL' + 2MM' = -2h + 3\varepsilon + h' + 8l' \pmod{16},
\]
\[(11.17) \quad L'M + LM' = 3h + 7\varepsilon + 8 + 8l' \pmod{16}.
\]

Now, using (9.13), (9.14), (9.15) and (11.15), we make more precise (9.18) and (9.19) as:

\[(11.18) \quad 7U_1V_1 + 10T_1W_1 = -3V_1 + 2h + 8l' \pmod{16},
\]
\[(11.19) \quad 5U_1V_1 + 7T_1W_1 = 7V_1 + 2hg(g + 1) + 8l - hW \pmod{16}.
\]

Comparing (11.16) with (11.18) and (11.17) with (11.19) we get:

\[(11.20) \quad \varepsilon = V_1 - 3h' \pmod{16},
\]
\[(11.21) \quad \varepsilon = -V_1 + 3h + 8 - hW + 2gh(g + 1) \pmod{16}.
\]

The comparison of (11.20) and (11.21) gives, remembering that $h + h' = 0 \pmod{8}$,

\[(11.22) \quad h + h' = 2V + hW + 2gh + 8 \pmod{16}.
\]

Noting that $hW = (h - 2)(W - 1) + 2(W - 1) + h$, we find

\[(11.23) \quad h' = 2V + 2(W - 1) + 2gh + 8 \pmod{16}.
\]
Now, we note that \( h' = -h \pmod{8} \), \( 2g = \frac{1}{4}(3k' - 2) \) so that finally:
\[
(11.24) \quad h' = 3k'V + 2(W-1) + 8 \pmod{16},
\]
completing the proof of Theorem 2 when \( l \) is odd.

**12. Case 2: \( l \) even.** Using the values of \( Y(\omega) \) and \( Z(\omega) \) given in (5.13), we find
\[
(12.1) \quad \frac{1}{2} \left[ Y(\omega) + Z(\omega) \sqrt{p} \right]^2
= -(L^2 + pL'^2 + 2N^2 + pN'^2)i + 2(LN + pL'N')(\omega + \omega^3) + \\
+ 2\sqrt{p} \left[ -(LL' + 2NN')i + (LN' + L'N)(\omega + \omega^3) \right].
\]
Comparing the coefficients of \( i, \omega + \omega^3, i\sqrt{p} \) and \( (\omega + \omega^3)\sqrt{p} \) in (9.11) and (12.1) we obtain:
\[
(12.2) \quad L^2 + pL'^2 + 2N^2 + 2pN'^2 = -14T_1V_1 - 20pU_1W_1,
(12.3) \quad LN + pL'N' = 5T_1V_1 + 7pU_1W_1,
(12.4) \quad LL' + 2NN' = -7U_1V_1 - 10T_1W_1,
(12.5) \quad LN' + L'N = 5U_1V_1 + 7T_1W_1.
\]
Using (5.15), (5.16), (5.17), (5.18), (8.20), (8.21) one finds:
\[
(12.6) \quad L^2 + pL'^2 + 2N^2 + 2pN'^2 = 2sT_k + 4N^2 + 4N'^2 \pmod{32}
\quad = 2\epsilon h + 4 \pmod{16},
(12.7) \quad LN + pL'N' = 3 + 2N' \pmod{8},
(12.8) \quad LL' + 2NN' = -\epsilon \pmod{8},
(12.9) \quad LN' + L'N = -3\epsilon \pmod{8}.
\]
We first use (12.2), (12.6) and (9.16) to get:
\[
(12.10) \quad hV(1 - 2g^2) = 2 \pmod{8}.
\]
As in the case \( l \) odd, this can be written, using (9.9):
\[
(12.11) \quad h' = h = -k'V \pmod{8},
\]
or equivalently:
\[
(12.12) \quad h' = k' + 2V + 2 \pmod{8}.
\]
Now we use (12.3), (12.7), (12.10) and (9.17) to get
\[
3 + 2N' = 2 - 3W + 2g(g+1) \pmod{8}.
\]
Using (8.32) for \( 4N' \), we have:
\[
h' \equiv h - \epsilon h - 6W + 4g(g+1) \pmod{16}.
\]
Now we use (12.8), (12.4) and (9.18) to obtain
\[
\epsilon = V(1 - 2g^2) + 4 \pmod{8}.
\]
Eliminating $\varepsilon$ we find, as $h' \equiv h \pmod{8}$:

\[(12.13) \quad h'V(1 - 2g^2) = 2W + 4g(g+1) \pmod{16}.\]

Noting that $1 - 2g^2 = \pm 1 \pmod{8}$, we find:

\[(12.14) \quad h'V = 2W(1 - 2g^2) + 4g(g+1) \equiv 2W + 4g \pmod{16},\]

that is:

\[(12.15) \quad h'V = 2(W - 1) + 3k' \pmod{16}.

Multiplying by $V$ we get the result of Theorem 2 for $l$ even:

\[(12.16) \quad h' = 3k'V + 2(W - 1) \pmod{16}.\]

References


[10] — The class number of $Q(\sqrt{-2p})$ modulo 8, for $p \equiv 5 \pmod{8}$ a prime, Rocky Mountain J. Math. 11(1981), pp. 19-26.


10, Allée Jacques Offenbach
54420 — Saintruppes les Nancy
France

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
Ottawa, Ontario, Canada

K1S 5B5

Received on 18.12.1979

(1189)