ACTA ARITHMETICA
XL (1982)

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

by

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

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

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 $Q(\sqrt{p})$ is denoted by ε_p. We have

$$\varepsilon_p = \tfrac{1}{2}(t+u\sqrt{p}), \tag{1.1}$$

where t and u are positive integers satisfying $t \equiv u \pmod 2$. The norm of ε_p is -1 so

$$t^2-pu^2 = -4. \tag{1.2}$$

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

$$\eta_p = \begin{cases} \varepsilon_p, & \text{if} \quad t \equiv u \equiv 0 \pmod 2, \\ \varepsilon_p^3, & \text{if} \quad t \equiv u \equiv 1 \pmod 2, \end{cases} \tag{1.3}$$

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

$$k = \begin{cases} 3h(p), & \text{if} \quad \eta_p = \varepsilon_p, \\ h(p), & \text{if} \quad \eta_p = \varepsilon_p^3. \end{cases} \tag{1.4}$$

---

*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) $$\varepsilon_p^{3h(p)} = \eta_p^k.$$

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

As $\eta_p \in B$ we have

(1.6) $$\eta_p = T + U\sqrt{p},$$

where $T+U\sqrt{p}$ 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) $$\begin{aligned} &T = t/2, && U = u/2, && \text{if} \quad t \equiv u \equiv 0 \pmod 2, \\ &T = t(t^2+3)/2, && U = u(t^2+1)/2, && \text{if} \quad t \equiv u \equiv 1 \pmod 2). \end{aligned}$$

Taking (1.7) modulo 8 we see that

(1.9) $$T \equiv 2 \pmod 4,$$

and that U is odd. Clearly all prime factors of U are congruent to 1 modulo 4, so that $U \equiv 1 \pmod 4$. Then, taking (1.7) modulo 32, we obtain

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

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

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) $$h \equiv Tk \pmod{16}.$$

The congruence

(1.12) $$h \equiv Tk \pmod 8$$

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

$$hk \equiv T \pmod{16},$$

and this is analogous to the congruence obtained in [9] for primes $p \equiv 1 \pmod 8$, which can be formulated

$$hk \equiv T+p-1 \pmod{16},$$

since the class numbers of the rings A and B coincide when $p \equiv 1 \pmod 8$.

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:

$$\sqrt{p}\,\varepsilon_p^{h(p)} = \prod_{-}(1-\varrho^j), \tag{1.13}$$

where $\varrho = \exp(2\pi i/p)$. (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 $1 \leqslant j \leqslant p-1$ 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

$$p^{3/2}\eta_p^k = \prod_{-}(1-\varrho^j)^3. \tag{1.14}$$

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

$$h = h(-p) = 2(S_0+S_1), \tag{1.15}$$

$$h' = h(-2p) = 2(S_0-S_3), \tag{1.16}$$

where

$$S_j = \sum_{jp/8<s<(j+1)p/8}\left(\frac{s}{p}\right), \quad j = 0, 1, \ldots, 7. \tag{1.17}$$

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

$$G_+(z) = \prod_{+}(z-\varrho^j)^3, \quad G_-(z) = \prod_{-}(z-\varrho^j)^3. \tag{2.1}$$

With this notation (1.14) can be rewritten

$$G_-(1) = p^{3/2}\eta_p^k. \tag{2.2}$$

Setting

$$G(z) = \prod_{j=}^{p-1}(z-\varrho^j)^3 = G_+(z)G_-(z), \tag{2.3}$$

and noting that

$$G(1) = p^3 = G_+(1)G_-(1), \tag{2.4}$$

we have (as k is odd)

$$G_+(1) = -p^{3/2}\eta_p'^k, \tag{2.5}$$

where $\eta_p' = T-U\sqrt{p} = -\eta_p^{-1}$.

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)

(2.6) $$G_{+}(-1) = \eta_p^{2k}, \quad G_{-}(-1) = \eta_p'^{2k}.$$

Further, following the proof of Lemma 3 in [9] we obtain, using here (1.15):

(2.7) $$G_{+}(i) = -\varepsilon i \eta_p'^{k}, \quad G_{-}(i) = -\varepsilon i \eta_p^{k},$$

where

(2.8) $$\varepsilon = (-1)^{(h-2)/4}.$$

We note that

(2.9) $$h \equiv 2\varepsilon \pmod 8, \quad \varepsilon h \equiv 2 \pmod 8.$$

We also note that, if $\omega = \exp(2\pi i/8) = (1+i)/\sqrt{2}$ (so that $\omega^2 = i$, $\omega_4 = -1$, $\omega + \omega^3 = i\sqrt{2}$, $\omega - \omega^3 = \sqrt{2}$), then:

(2.10) $$G_{\pm}(\omega)G_{\pm}(-\omega) = G_{\mp}(i)$$

follows easily from the definition (2.1), as $p \equiv 5 \pmod 8$. Finally we observe that

$$\tfrac{1}{2}(\eta_p^k + \eta_p'^k) = \tfrac{1}{2}(T+U\sqrt{p})^k + \tfrac{1}{2}(T-U\sqrt{p})^k$$

and

$$\frac{1}{2\sqrt{p}}(\eta_p^k - \eta_p'^k) = \frac{1}{2\sqrt{p}}(T+U\sqrt{p})^k - \frac{1}{2\sqrt{p}}(T-U\sqrt{p})^k$$

are rational integers. Moreover, as k is odd and $T \equiv 2 \pmod 4$ we have:

$$\begin{aligned}\tfrac{1}{2}(\eta_p^k + \eta_p'^k) &= \sum_{s=0}^{(k-1)/2} \binom{k}{2s+1} T^{2s+1}(pU^2)^{(k-1)/2-s} \\ &\equiv kT(pU^2)^{(k-1)/2} + \binom{k}{3} T^3 (pU^2)^{(k-3)/2} \pmod{16} \\ &\equiv kT5^{(k-1)/2} + 4\binom{k}{2} T \pmod{16} \\ &\equiv kT\big(2k-1+2k(k-1)\big) \pmod{16},\end{aligned}$$

that is

(2.11) $$\tfrac{1}{2}(\eta_p^k + \eta_p'^k) \equiv kT \pmod{16}.$$

Similarly we obtain

(2.12) $$\frac{1}{2\sqrt{p}}(\eta_p^k - \eta_p'^k) \equiv U \equiv 4l+1 \pmod{16}.$$

3. The polynomials $Y(z)$ **and** $Z(z)$. The polynomials $\prod_{\pm}(z-\varrho^j)$ are each of degree $\frac{1}{2}(p-1) = 4l+2$ and their coefficients belong to the ring of integers of $Q(\sqrt{p})$. It follows that $G_+(z)$ and $G_-(z)$ are polynomials of degree $12l+6$ which can be expressed in the form

(3.1) $$G_+(z) = \tfrac{1}{2}\big(Y(z) - Z(z)\sqrt{p}\big), \quad G_-(z) = \tfrac{1}{2}\big(Y(z)+Z(z)\sqrt{p}\big),$$

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) $$Y(z) = G_-(z) + G_+(z), \quad Z(z) = \frac{1}{\sqrt{p}}\big(G_-(z) - G_+(z)\big).$$

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

$$z^{12l+6}G_{\pm}(1/z) = G_{\pm}(z),$$

so that by (3.2)

$$z^{12l+6}\,Y(1/z) = Y(z), \quad z^{12l+6}Z(1/z) = Z(z).$$

Hence the coefficient of z^n $(n = 0, 1, 2, \ldots, 6l+2)$ in $Y(z)$ (resp. $Z(z)$) is the same as that of $z^{12l+6-n}$. 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 rthe coefficients of z^{6l+3}) of $Y(z)$ and $Z(z)$ are both even. Thus we can set

(3.3) $$Y(z) = \sum_{n=0}^{6l+3} a_n(z^n + z^{12l+6-n}), \qquad Z(z) = \sum_{n=0}^{6l+3} b_n(z^n + z^{12l+6-n}),$$

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) $$Y^2(z) - pZ^2(z) = 4G(z),$$

and by differentiating (3.4) we obtain

(3.5) $$Y(z)\,Y'(z) - pZ(z)Z'(z) = 2G'(z).$$

Taking $z = \omega$ in (3.4) and (3.5) we obtain

(3.6) $$Y^2(\omega) - pZ^2(\omega) = -20\omega - 28i - 20\omega i,$$

(3.7) $$Y(\omega)Y'(\omega) - pZ(\omega)Z'(\omega)$$
$$= (51-9p) + 21(1-p)\omega - 21(1+p)\omega^2 - (51+9p)\omega^3.$$

Next we introduce the polynomial

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

Using the Gauss sum

$$\sum_{+} \varrho^j - \sum_{-} \varrho^j = \sqrt{p},$$

we easily deduce the following partial fraction decomposition:

(3.9) $$\frac{K(z)}{z^p - 1}\sqrt{p} = \sum_{+} \frac{1}{z-\varrho^j} - \sum_{-} \frac{1}{z-\varrho^j}.$$

Since by (2.1), (3.2) and (3.9)

$$Y'Z - YZ' = \frac{2}{\sqrt{p}}(G'_+ G_- - G_+ G'_-) = \frac{6G}{\sqrt{p}}\left(\sum_{+} \frac{1}{z-\varrho^j} - \sum_{-} \frac{1}{z-\varrho^j}\right)$$

we obtain

(3.10) $$Y'Z - YZ' = 6\frac{(z^p-1)^2}{(z-1)^3} K(z).$$

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

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

For $j = 0, 1, 2, \ldots, 7$ we set $s = 8r - j$.
As $1 \leqslant 8r - j < 8l + 5$, we have

$$r = 1, \ldots, l, \quad \text{for} \quad j = 0, 1, 2, 3,$$
$$r = 1, \ldots, l+1, \quad \text{for} \quad j = 4, 5, 6, 7.$$

Then, as $\left(\frac{8r-j}{p}\right) = \left(\frac{2r+(2l+1)j}{p}\right)$, we find that

$$K(\omega) = -\sum_{j=0}^{7} \omega^j T_j$$

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) $$K(\omega) = (1+\omega^3)(S_0-S_3)+(\omega+\omega^2)(S_2-S_1).$$

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) $$4S_0 = -h+h'; \quad 4S_1 = 3h-h'; \quad 4S_3 = -h-h'.$$

As $S_0 \equiv l \pmod 2$ and $S_1 \equiv S_3 \equiv l+1 \pmod 2$, each of these relations proves the well-known result:

(3.13) $$h' \equiv h+4l \pmod 8.$$

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

$$2K(\omega) = -2h(\omega+\omega^2)+h'(1+\omega+\omega^2+\omega^3)$$

from which we deduce, after changing ω into $-\omega$:

(3.14) $$4h = K(\omega)(1-\omega+\omega^2+\omega^3)+K(-\omega)(1+\omega+\omega^2-\omega^3),$$

(3.15) $$2h' = K(\omega)(1-\omega)+K(-\omega)(1+\omega).$$

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

(3.16) $$12h = \big(5(1+\omega^2)-7\omega\big)\big(Y'(\omega)Z(\omega)-Y(\omega)Z'(\omega)\big)+ \\ +\big(5(1+\omega^2)+7\omega\big)\big(Y'(-\omega)Z(-\omega)-Y(-\omega)Z'(-\omega)\big),$$

(3.17) $$12h' = \big(7(1+\omega^2)-10\omega\big)\big(Y'(\omega)Z(\omega)-Y(\omega)Z'(\omega)\big)+ \\ +\big(7(1+\omega^2)+10\omega\big)\big(Y'(-\omega)Z(-\omega)-Y(-\omega)Z'(-\omega)\big).$$

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

$$H = \big(a(1+\omega^2)-\beta\omega\big)\big(Y'(\omega)Z(\omega)-Y(\omega)Z'(\omega)\big)+(\ )^-(\ )^-,$$

where $(\ )^-$ is the same expression with $-\omega$ instead of ω.

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:

$$H = 4a\alpha+2b\beta. \tag{3.18}$$

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

From (3.3), (3.2), (2.2), (2.5), (2.12), we have

$$\sum a_n = \tfrac{1}{2}Y(1) = \tfrac{1}{2}\big(G_-(1)+G_+(1)\big) = \tfrac{1}{2}p^{3/2}(\eta_p^k-\eta_p'^k) \equiv p^2(4l+1) \pmod{16}$$

that is

$$\sum a_n \equiv 4l+9 \pmod{16}. \tag{4.1}$$

Similarly we obtain

$$\sum b_n \equiv 5Tk \pmod{16}. \tag{4.2}$$

Similarly, making use of $Y(-1)$, $Z(-1)$, $Y(i)$ and $Z(i)$, we obtain

$$\sum a_n(-1)^n \equiv 9 \pmod{16}, \tag{4.3}$$

$$\sum b_n(-1)^n \equiv -2Tk \pmod{16}, \tag{4.4}$$

$$\sum a_{2n+1}(-1)^n \equiv -\varepsilon Tk \pmod{16}, \tag{4.5}$$

$$\sum b_{2n+1}(-1)^n \equiv -\varepsilon(4l+1) \pmod{16}. \tag{4.6}$$

Adding and subtracting these congruences appropriately, we get

$$\sum a_{2n} \equiv 2l+1 \pmod 8, \tag{4.7}$$

$$\sum b_{2n} \equiv \frac{3Tk}{2} \pmod 8, \tag{4.8}$$

$$\sum a_{2n+1} \equiv 2l \pmod 8, \tag{4.9}$$

$$\sum b_{2n+1} \equiv -\frac{Tk}{2} \pmod 8, \tag{4.10}$$

$$\sum a_{4n+1} \equiv l-\frac{\varepsilon Tk}{2} \pmod 4, \tag{4.11}$$

(4.12)
$$\sum b_{4n+1} \equiv \begin{cases} 2-\dfrac{(2\varepsilon+Tk)}{4} \pmod 4, & \text{if} \quad l \text{ odd}, \\ -\dfrac{(2\varepsilon+Tk)}{4} \pmod 4, & \text{if} \quad l \text{ even}, \end{cases}$$

(4.13)
$$\sum a_{4n+3} \equiv l+\frac{\varepsilon Tk}{2} \pmod 4,$$

(4.14)
$$\sum b_{4n+3} \equiv \begin{cases} 2+\dfrac{(2\varepsilon-Tk)}{4} \pmod 4, & \text{if} \quad l \text{ odd}, \\ \dfrac{(2\varepsilon-Tk)}{4} \pmod 4, & \text{if} \quad l \text{ even}. \end{cases}$$

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

(5.1)
$$Y(\omega) = L+2M\omega+(-1)^{l-1}Li+2N\omega i,$$

(5.2)
$$Z(\omega) = L'+2M'\omega+(-1)^{l-1}L'i+2N'\omega i,$$

where

(5.3)
$$L = \sum a_{4m}(-1)^m+(-1)^{l-1}\sum a_{4m+2}(-1)^m,$$

(5.4)
$$M = \tfrac{1}{2}(1+(-1)^{l-1})\sum a_{4m+1}(-1)^m,$$

(5.5)
$$N = \tfrac{1}{2}(1+(-1)^{l})\sum a_{4m+3}(-1)^m.$$

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

(5.6)
$$M = M' = 0, \quad \text{if} \quad l \text{ even}, \qquad N = N' = 0, \quad \text{if} \quad l \text{ odd},$$

suggesting that we treat the two cases l odd and l even separately.

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

(5.7)
$$Y(\omega) = L+2M\omega+Li, \qquad Z(\omega) = L'+2M'\omega+L'i.$$

Appealing to (3.6) we obtain

(5.8)
$$L^2+2M^2-pL'^2-2pM'^2 = -14,$$

(5.9)
$$LM-pL'M' = -5.$$

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

(5.10)
$$L^2-2M^2+pL'^2-2pM'^2 \equiv -2\varepsilon Tk \pmod{32},$$

(5.11)
$$LL'-2MM' \equiv \varepsilon(4l+1) \pmod{16}.$$

Finally we have

$$L = \sum a_{4m}(-1)^m + \sum a_{4m+2}(-1)^m \quad (\text{by } (5.3))$$
$$\equiv \sum a_{4m} + \sum a_{4m+2} \ (\text{mod } 2) \equiv \sum a_{2m} \ (\text{mod } 2),$$
$$\equiv 1 \ (\text{mod } 2) \quad (\text{by } (4.7)).$$

Similarly we obtain $L' \equiv 1 \pmod 2$ and $M \equiv 0 \pmod 2$. Then, appealing to (5.8), we get $M' \equiv 1 \pmod 2$. Summarizing we have

(5.12) $$L \equiv L' \equiv M' \equiv 1 \ (\text{mod } 2), \qquad M \equiv 0 \ (\text{mod } 2).$$

Case (ii): l even. From (5.1), (5.2) and (5.6) we have

(5.13) $$Y(\omega) = L - Li + 2N\omega i, \qquad Z(\omega) = L' - L'i + 2N'\omega i.$$

Appealing to (3.6) we obtain

(5.14) $$L^2 + 2N^2 - pL'^2 - 2pN'^2 = 14,$$

(5.15) $$LN - pL'N' = -5.$$

Further using (2.7), (2.10), (2.11), (2.12), (3.1) and (5.13),

(5.16) $$L^2 - 2N^2 + pL'^2 - 2pN'^2 \equiv 2\varepsilon Tk \ (\text{mod } 32),$$

(5.17) $$LL' - 2NN' \equiv -\varepsilon(4l+1) \ (\text{mod } 16).$$

As in the case when l is odd, we obtain

(5.18) $$L \equiv L' \equiv N \equiv 1 \ (\text{mod } 2), \qquad N' \equiv 0 \ (\text{mod } 2).$$

It is convenient to note here that

(5.19) $$L^2 \equiv 3 - \varepsilon Tk \ (\text{mod } 16), \quad \text{if} \quad l \text{ is odd},$$

and

(5.20) $$L'^2 \equiv -1 - 3\varepsilon Tk \ (\text{mod } 16), \quad \text{if} \quad l \text{ is even},$$

follow from (5.8), (5.10), (5.12) and (5.14), (5.16), (5.18) respectively.

6. Proof of $h \equiv Tk \pmod 8$. We consider the two cases.

Case (i): l odd. From (4.12), (5.4)′ and (5.12), we have

$$1 \equiv M' \equiv \sum b_{4m+1} \equiv -\tfrac{1}{4}(2\varepsilon + Tk) \ (\text{mod } 2),$$

so, as $2\varepsilon \equiv h \pmod 8$, we have

$$Tk \equiv -2\varepsilon - 4 \equiv 2\varepsilon \equiv h \ (\text{mod } 8).$$

Case (ii): l even. From (4.14), (5.5)′ and (5.18), we have

$$0 \equiv N' \equiv \sum b_{4m+3} \equiv \tfrac{1}{4}(2\varepsilon - Tk) \ (\text{mod } 2),$$

so

$$Tk \equiv 2\varepsilon \equiv h \pmod{8}.$$

We close this section by noting that the congruence $h \equiv Tk \pmod{8}$ enables us to obtain from (4.11), (4.12), (4.13), (4.14):

$$\sum a_{4n+1} \equiv l-1 \pmod{4}, \tag{6.1}$$

$$\sum b_{4n+1} \equiv 1 \pmod{2}, \tag{6.2}$$

$$\sum a_{4n+3} \equiv l+1 \pmod{4}, \tag{6.3}$$

$$\sum b_{4n+3} \equiv 0 \pmod{2}. \tag{6.4}$$

7. Proof of $h \equiv Tk \pmod{16}$. Case (i) : l **odd.** Differentiating (3.3) with respect to z and setting $z = \omega$ we obtain

$$Y'(\omega) = 2P+2Q\omega+8Ri+4S\omega i, \tag{7.1}$$

$$Z'(\omega) = 2P'+2Q'\omega+8R'i+4S'\omega i, \tag{7.2}$$

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

$$P = (6l+3)\sum a_{4m+1}(-1)^m, \tag{7.3}$$

$$Q = \sum\big((6l+3-2m)a_{4m}+(2m+1)a_{4m+2}\big)(-1)^m, \tag{7.4}$$

$$R = \sum\left(m-\frac{3l}{2}\right)a_{4m+3}(-1)^m, \tag{7.5}$$

$$S = \sum\big(-ma_{4m}-(3l-m+1)a_{4m+2}\big)(-1)^m, \tag{7.6}$$

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

$$P = (6l+3)M, \quad P' = (6l+3)M', \tag{7.11}$$

and, from (5.3) and (5.3)′, that

$$Q = 2S+(6l+3)L, \quad Q' = 2S'+(6l+3)L'. \tag{7.12}$$

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 determine them modulo 2. From (7.9), as $(2m+1)(-1)^m \equiv 1 \pmod 4$ and as $3l+1$ is even, we have

$$2R' = \sum (2m+1)(-1)^m b_{4m+3} - (3l+1)\sum b_{4m+3}(-1)^m$$
$$\equiv \sum b_{4m+3} - (3l+1)\sum b_{4m+3} \equiv l\sum b_{4m+3} \equiv l\left(2+\frac{(2\varepsilon - Tk)}{4}\right) \pmod 4,$$

by (4.14), that is:

(7.13) $$R' \equiv 1+\tfrac{1}{8}(2\varepsilon - Tk) \pmod 2.$$

Similarly we obtain

(7.14) $$R \equiv \tfrac{1}{2}(l+1) \pmod 2,$$

(7.15) $$S \equiv \tfrac{1}{2}(L+1) \pmod 2,$$

(7.16) $$S' \equiv \tfrac{1}{2}(L'-1)+\left(\frac{2+Tk}{4}\right) \pmod 2.$$

We will now show that

(7.17) $$S \equiv S' \pmod 2.$$

From (5.11) and (5.12) we have

$$L+L'-1 \equiv LL' \equiv \varepsilon \pmod 4.$$

Hence, from (7.15), (7.16) and the result $Tk \equiv 2\varepsilon \pmod 8$, we have

$$S+S' \equiv \tfrac{1}{2}(L+L')+\frac{(2+Tk)}{4} \equiv \tfrac{1}{2}(1+\varepsilon)+\tfrac{1}{4}(2+2\varepsilon) \equiv 0 \pmod 2.$$

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)):

(7.18) $$2LR+2MS-p(2L'R'+2M'S') = 3l-9,$$

(7.19) $$8MR+4LS-p(8M'R'+4L'S') = -(6l+3)(L^2-pL'^2)-48-36l.$$

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:

(7.20) $$L' \equiv 3\varepsilon L+2M' \pmod 8,$$

(7.21) $$M \equiv -3L-\varepsilon M' \pmod 8.$$

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

(7.22) $$4L \equiv 4+Tk-2\varepsilon \pmod{16}.$$

Next using (5.19) and (7.20) we obtain

$$(7.23)\qquad L^2-pL'^2 \equiv 8+4\varepsilon LM' \equiv 4\varepsilon L+4\varepsilon M'+8-4\varepsilon \pmod{16}.$$

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

$$(7.24)\qquad 4(LS-L'S') \equiv 4L+4M'+6\varepsilon-4l-Tk \pmod{16}.$$

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

$$(7.25)\qquad 4(L'S-LS') \equiv -4L-4M'-6\varepsilon+4l+Tk \pmod{16}.$$

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

$$(7.26)\qquad 8(LR'-L'R) \equiv 4l-4+2\varepsilon-Tk \pmod{16},$$

$$(7.27)\qquad 8(M'R-MR') \equiv 4l+4 \pmod{16},$$

$$(7.28)\qquad 8(MS'-M'S) \equiv 4L+4 \pmod{16},$$

and using (7.20) and (7.21) we have

$$(7.29)\qquad L'M-LM' \equiv -2L-2M'-3\varepsilon+2 \pmod{8}.$$

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

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

where

$$(7.30)\qquad \begin{aligned} a &= 8(LR'-L'R)+8(MS'-M'S)+2(6l+3)(L'M-LM'),\\ b &= 8(L'S-LS')+16(M'R-MR'). \end{aligned}$$

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

$$(7.31)\qquad \begin{aligned} 3h = {}& 10(6l+3)(L'M-LM')+40(MS'-M'S)+\\ &+40(LR'-L'R)+28(L'S-LS')+56(M'R-MR'), \end{aligned}$$

$$(7.32)\qquad \begin{aligned} 3h' = {}& 56(LR'-L'R)+56(MS'-M'S)+14(6l+3)(L'M-LM')+\\ &+40(L'S-LS')+80(M'R-MR'). \end{aligned}$$

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

$$3h \equiv 8-Tk \pmod{16}$$

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:

$$h' \equiv h + 4M' \pmod{16}. \tag{7.33}$$

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

$$Y'(\omega) = 4P + 2Q\omega + 2R\omega^2 + 4S\omega^3, \tag{8.1}$$

$$Z'(\omega) = 4P' + 2Q'\omega + 2R'\omega^2 + 4S'\omega^3, \tag{8.2}$$

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

$$P = \sum (2m - 3l - 1) a_{4m+1} (-1)^m, \tag{8.3}$$

$$Q = \sum \left((2m - 3 - 6l) a_{4m} + (2m+1) a_{4m+2}\right) (-1)^m, \tag{8.4}$$

$$R = (6l + 3) \sum a_{4m+3} (-1)^m, \tag{8.5}$$

$$S = \sum \left(-m a_{4m} + (3l + 1 - m) a_{4m+2}\right) (-1)^m, \tag{8.6}$$

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

$$R = (6l+3)N, \quad R' = (6l+3)N', \tag{8.11}$$

and

$$Q = -2S - (6l+3)L, \quad Q' = -2S' - (6l+3)L'. \tag{8.12}$$

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 $(2m-1)(-1)^m \equiv -1 \pmod 4$ and l is even, we have, using (4.12)

$$\begin{aligned} P' &= \sum (2m-1)(-1)^m b_{4m+1} - 3l \sum b_{4m+1} (-1)^m \\ &\equiv -\sum b_{4m+1} - 3l \sum b_{4m+1} \pmod 4 \\ &\equiv -(1+3l) \sum b_{4m+1} \pmod 4 \\ &\equiv (1-l) \frac{(2\varepsilon + Tk)}{4} \pmod 4, \end{aligned}$$

that is

(8.13) $$P' \equiv \frac{2\varepsilon+Tk}{4} - l \pmod 4.$$

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) $$P \equiv 1 \pmod 4,$$

(8.15) $$S \equiv \tfrac{1}{2}(L-1) \pmod 2,$$

(8.16) $$S' \equiv \tfrac{1}{2}(L'+1) + \frac{(h-2)}{4} \pmod 2.$$

We now use (5.17) to show that

(8.17) $$S \equiv S' \pmod 2.$$

From (5.17) and (5.18) we have

$$L+L'-1 \equiv LL' \equiv -\varepsilon \pmod 4.$$

Hence from (8.15) and (8.16)

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

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) $$LP+2NS-p(L'P'+2N'S') = 24+27l,$$

(8.19) $$2NP+2LS-p(2N'P'+2L'S') = (6l+3)(N^2-pN'^2)-45-60l.$$

(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) $$L' \equiv -\varepsilon L + 2N' \pmod 8,$$

(8.21) $$N \equiv 3L + 3\varepsilon N' \pmod 8.$$

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

(8.22) $$4L \equiv -6\varepsilon - Tk + 4 \pmod{16}.$$

Next from (5.18) we have:

(8.23) $$N^2 - pN'^2 \equiv 1-5N'^2 \equiv 1+2N' \pmod 8,$$

so that (8.19) gives:

$$LS - L'S' \equiv L + N' + l - 1 \pmod 4, \tag{8.24}$$

which, combined with $(L+L')(S-S') \equiv 0 \pmod 4$, gives

$$L'S - LS' \equiv -L + N' - l + 1 \pmod 4. \tag{8.25}$$

We note also the following:

$$\begin{cases} 4(L'P - LP') \equiv 4l - 6\varepsilon L - LTk \pmod{16}, \\ 4(N'P - NP') \equiv 4l - 6\varepsilon L - 3LTk \pmod{16}, \\ 4(L'P - LP') - 4(N'P - NP') \equiv 4L + 4\varepsilon - 4 \pmod{16}, \end{cases} \tag{8.26}$$

$$8(N'S - NS') \equiv 4L - 4 \pmod{16}, \tag{8.27}$$

$$LN' - L'N \equiv 3\varepsilon - 2N' \pmod 8. \tag{8.28}$$

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

$$\begin{aligned} a &= 4(L'P - LP') - 2(6l+3)(L'N - LN') + 8(N'S - NS'), \\ b &= 8(N'P - NP') + 8(L'S - LS'). \end{aligned} \tag{8.29}$$

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

$$\begin{aligned} 3h = {} & 20(L'P - LP') + 28(N'P - NP') + 28(L'S - LS') + \\ & + 40(N'S - NS') + 30(2l+1)(LN' - L'N), \end{aligned} \tag{8.30}$$

and

$$\begin{aligned} 3h' = {} & 28(L'P - LP') + 56(N'S - NS') - 14(6l+3)(L'N - LN') + \\ & + 40(N'P - NP') + 40(L'S - LS'). \end{aligned} \tag{8.31}$$

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

$$4N' \equiv h' - h + \varepsilon h - 2 \pmod{16}. \tag{8.32}$$

We note that (8.32) is consistent with (3.13), as $\varepsilon h \equiv 2 \pmod 8$ 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 $h' \equiv k' \equiv 2 \pmod 4$ and we have already mentioned that $h' \equiv h+4l \pmod 8$ (see (3.13)).

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

$$\varepsilon_{2p} = V + W\sqrt{2p}, \tag{9.1}$$

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

$$V^2 - 2pW^2 = -1. \tag{9.2}$$

The positive integers V, W are both odd and:

$$V \equiv \pm 3 \pmod 8; \qquad W \equiv 1 \pmod 4). \tag{9.3}$$

The aim of the second part is to prove the following

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

$$h' \equiv 2(W-1) + 3k'V + 8l \pmod{16}. \tag{9.4}$$

Modulo 8 this result reduces to:

$$h' \equiv k' + 2V + 2 \pmod 8, \tag{9.5}$$

which has already be 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 $\prod_{-}(\omega - \varrho^j)$ as:

$$\prod_{-} (\omega - \varrho^j) = (-1)^l \eta_p^{-k/6} \varepsilon_{2p}^{k'/4} i^{(h-h')/4} \omega (1+\sqrt{2})^{1/2}. \tag{9.6}$$

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

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

$$\tfrac{1}{2}[Y(\omega) + Z(\omega)\sqrt{p}]^2 = (-1)^{l+1} 2i\eta_p^{-k} \varepsilon_{2p}^{2g+1}(7+5\sqrt{2}) = (-1)^l \mathscr{A} \tag{9.7}$$

where we define the rational integer g by

$$3k'/2 = 2g+1. \tag{9.8}$$

We note that $k' \equiv 2$ or $6 \pmod 8$ according as $g \equiv 1$ or $0 \pmod 2$ so that:

(9.9)
$$\varepsilon' = (-1)^{(k'-2)/4} \equiv -(-1)^g \equiv -1+2g^2 \pmod 8;$$
$$2\varepsilon' \equiv k' \pmod 8.$$

Rational integers T_1, U_1, V_1, W_1 are defined by:

(9.10)
$$T_1 + U_1\sqrt{p} = -\eta_p^{-k}; \qquad V_1 + W_1\sqrt{2p} = \varepsilon_{2p}^{2g+1}.$$

Then we have:

$$\mathscr{A} = 2(T_1 + U_1\sqrt{p})(V_1 + W_1(\omega - \omega^3)\sqrt{p})[5(\omega+\omega^3) + 7\omega^2],$$

that is

(9.11)
$$\mathscr{A} = (10T_1V_1 + 14pU_1W_1)(\omega+\omega^3) + (14T_1V_1 + 20pU_1W_1)i + \\ + (10U_1V_1 + 14T_1W_1)(\omega+\omega^3)\sqrt{p} + (14U_1V_1 + 20T_1W_1)i\sqrt{p}.$$

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

(9.12)
$$T_1 + U_1\sqrt{p} = (T - U\sqrt{p})^k; \qquad V_1 + W_1\sqrt{2p} = (V + W\sqrt{2p})^{2g+1},$$

we find the following congruences:

(9.13)
$$T_1 \equiv h \pmod{16}; \qquad U_1 \equiv -(4l+1) \pmod{16},$$

(9.14)
$$V_1 \equiv V(1-2g^2) \pmod 8; \qquad W_1 \equiv 1 \pmod 4,$$

(9.15)
$$W_1 \equiv W(1+2g+2g^2) \equiv W + 2g(g+1) \pmod 8.$$

Using (9.13), (9.14), (9.15) we obtain congruences modulo 16 or 8 for the coefficients of i, $\omega+\omega^3$, $i\sqrt{p}$, $(\omega+\omega^3)\sqrt{p}$ in $\frac{1}{2}\mathscr{A}$:

(9.16)
$$7T_1V_1 + 10pU_1W_1 \equiv 7hV(1-2g^2) - 2W(1+2g+2g^2) + \\ + 8l \pmod{16} \equiv 3hV(1-2g^2) - 2 \pmod 8,$$

(9.17)
$$5T_1V_1 + 7pU_1W_1 \equiv 5hV(1-2g^2) + 5W(1+2g+2g^2) + \\ + 4l \pmod 8,$$

(9.18)
$$7U_1V_1 + 10T_1W_1 \equiv V(1-2g^2) + 2h + 4l \pmod 8,$$

(9.19)
$$5U_1V_1 + 7T_1W_1 \equiv 3V(1-2g^2) - h + 4l \pmod 8.$$

10. Calculation of $\prod\limits_{-} (\omega - \varrho^j)$. In this section we make use of the following class number formulae of Dirichlet, namely:

(10.1)
$$h = h(-p) = \frac{2}{\pi}\sqrt{p}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{-4p}{n}\right),$$

$$3h(p)\log\varepsilon_p = k\log\eta_p = \frac{3\sqrt{p}}{2}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{p}{n}\right), \tag{10.2}$$

$$h' = h(-2p) = \frac{2}{\pi}\sqrt{2p}\sum_{n=1}^{\infty}\frac{1}{n}\left(\frac{-8p}{n}\right), \tag{10.3}$$

$$k'\log\varepsilon_{2p} = \sqrt{2p}\sum_{n=1}^{\infty}\left(\frac{8p}{n}\right)\frac{1}{n}. \tag{10.4}$$

One finds easily:

$$\prod_{-}(\omega-\varrho^j) = (-1)^l i\prod_{-}(1+\omega^3\varrho^j). \tag{10.5}$$

We set:

$$x_j = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}\omega^{3n}\varrho^{nj}}{n}, \tag{10.6}$$

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

$$(-1)^{l-1}iF_{-}(\omega) = \exp\left(\sum_{-}x_j\right). \tag{10.7}$$

We calculate $\sum_{-}x_j$:

$$\sum_{-}x_j = \sum_{-}\sum_{n=1}^{\infty}\frac{(-1)^{n-1}\omega^{3n}\varrho^{nj}}{n} = \sum_{n=1}^{\infty}\frac{(-1)^{n-1}\omega^{3n}}{n}\sum_{-}\varrho^{nj}$$

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

that is

$$\sum_{-}x_j = -\frac{1}{2}\log\frac{1+\omega^3}{1-\omega^3} + \frac{\sqrt{p}}{2}\sum_{u=0}^{3}\omega^u T_u, \tag{10.8}$$

where

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

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

$$\sum_{-}\varrho^{nj} = \frac{1}{2}\left(1-\left(\frac{n}{p}\right)^2\right)p - \frac{1}{2}\left(\frac{n}{p}\right)\sqrt{p} - \frac{1}{2}.$$

Using (10.1)–(10.4) one finds easily, as in [6], Proof of Lemma:

$$T_0 = -\frac{k}{3\sqrt{p}}\log\eta_p; \qquad T_2 = \frac{\pi h}{4\sqrt{p}};$$

$$T_1 = \frac{-\pi h'}{4\sqrt{2p}} + \frac{k'\log\varepsilon_{2p}}{2\sqrt{2p}}; \qquad T_3 = \frac{-\pi h'}{4\sqrt{2p}} - \frac{k'\log\varepsilon_{2p}}{2\sqrt{2p}}.$$

Using these values in (10.8), we obtain:

$$\sum_{-} x_j = -\frac{k\log\eta_p}{6} + \frac{k'\log\varepsilon_{2p}}{4} + \frac{\pi i}{8}(h-h') - \frac{1}{2}\log\frac{1+\omega^3}{1-\omega^3},$$

which is (9.6).

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

(11.1) $\frac{1}{2}[Y(\omega)+Z(\omega)\sqrt{p}]^2$

$$= -\mathcal{A} = (L^2+pL'^2+2M^2+2pM'^2)i+2(LM+pL'M')(\omega+\omega^3)+$$
$$+2\sqrt{p}[(LL'+2MM')i+(L'M+LM')(\omega+\omega^3)].$$

Comparing (11.1) and (9.11) we get:

(11.2) $$L^2+pL'^2+2M^2+2pM'^2 = -14T_1V_1-20pU_1W_1,$$

(11.3) $$LM+pL'M' = -5T_1V_1-7pU_1W_1,$$

(11.4) $$LL'+2MM' = -7U_1V_1-10T_1W_1,$$

(11.5) $$LM'+L'M = -5U_1V_1-7T_1W_1.$$

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

(11.6) $$L^2+pL'^2+2M^2+2pM'^2 \equiv -2\varepsilon Tk+4M^2+4pM'^2 \pmod{32}$$
$$\equiv -h^2+4 \equiv 0 \pmod{16},$$

(11.7) $$LM+pL'M' \equiv -1-2\varepsilon LM' \pmod 8,$$

(11.8) $$LL'+2MM' \equiv \varepsilon+4 \pmod 8,$$

(11.9) $$LM'+L'M \equiv -3\varepsilon \pmod 8.$$

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

(11.10) $$hV(1-2g^2) \equiv 6 \pmod 8.$$

Introducing k' by equations (9.9), (11.10) becomes $\frac{h}{2}\frac{k'}{2}V \equiv 1 \pmod 4$ that is:

(11.11) $$h \equiv k'V \pmod 8.$$

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

(11.12) $$h' \equiv k'+2V+2 \pmod 8.$$

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) $$\begin{aligned} L' &\equiv (5h+\varepsilon)L+10M'+8+8l' \pmod{16}, \\ M &\equiv -(\varepsilon h+1)L+(9h-3\varepsilon)M'+8+8l' \pmod{16}, \end{aligned}$$

where the integer l' is defined by

(11.14) $$l = 2l'+1,$$

so that

(11.15) $$4l+1 = 8l'+5.$$

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

(11.16) $$LL'+2MM' \equiv -2h+3\varepsilon+h'+8l' \pmod{16},$$

(11.17) $$L'M+LM' \equiv 3h+7\varepsilon+8+8l' \pmod{16}.$$

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

(11.18) $$7U_1V_1+10T_1W_1 \equiv -3V_1+2h+8l' \pmod{16},$$

(11.19) $$5U_1V_1+7T_1W_1 \equiv 7V_1+2hg(g+1)+8l'-hW \pmod{16}.$$

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

(11.20) $$\varepsilon \equiv V_1-3h' \pmod{16},$$

(11.21) $$\varepsilon \equiv -V_1+3h+8-hW+2gh(g+1) \pmod{16}.$$

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

(11.22) $$h+h' \equiv 2V+hW+2gh+8 \pmod{16}.$$

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

(11.23) $$h' \equiv 2V+2(W-1)+2gh+8 \pmod{16}.$$

Now, we note that $h' \equiv -h \pmod 8$, $2g = \frac{1}{2}(3k'-2)$ so that finally:

(11.24) $$h' \equiv 3k'V + 2(W-1) + 8 \pmod{16},$$

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) $$\tfrac{1}{2}[Y(\omega)+Z(\omega)\sqrt{p}]^2 = -(L^2+pL'^2+2N^2+pN'^2)i+2(LN+pL'N')(\omega+\omega^3)+ +2\sqrt{p}[-(LL'+2NN')i+(LN'+L'N)(\omega+\omega^3)].$$

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) $$L^2+pL'^2+2N^2+2pN'^2 = -14T_1V_1-20pU_1W_1,$$

(12.3) $$LN+pL'N' = 5T_1V_1+7pU_1W_1,$$

(12.4) $$LL'+2NN' = -7U_1V_1-10T_1W_1,$$

(12.5) $$LN'+L'N = 5U_1V_1+7T_1W_1.$$

Using (5.15), (5.16), (5.17), (5.18), (8.20), (8.21) one finds:

(12.6) $$L^2+pL'^2+2N^2+2pN'^2 \equiv 2\varepsilon Tk+4N^2+4N'^2 \pmod{32} \equiv 2\varepsilon h+4 \pmod{16},$$

(12.7) $$LN+pL'N' \equiv 3+2N' \pmod 8,$$

(12.8) $$LL'+2NN' \equiv -\varepsilon \pmod 8,$$

(12.9) $$L'N+LN' \equiv -3\varepsilon \pmod 8.$$

We first use (12.2), (12.6) and (9.16) to get:

(12.10) $$hV(1-2g^2) \equiv 2 \pmod 8.$$

As in the case l odd, this can be written, using (9.9):

(12.11) $$h' \equiv h \equiv -k'V \pmod 8,$$

or equivalently:

(12.12) $$h' \equiv k'+2V+2 \pmod 8.$$

Now we use (12.3), (12.7), (12.10) and (9.17) to get

$$3+2N' \equiv 2-3W+2g(g+1) \pmod 8.$$

Using (8.32) for $4N'$, we have:

$$h' \equiv h-\varepsilon h-6W+4g(g+1) \pmod{16}.$$

Now we use (12.8), (12.4) and (9.18) to obtain

$$\varepsilon \equiv V(1-2g^2)+4 \pmod 8.$$

Eliminating ε we find, as $h' \equiv h \pmod 8$:

(12.13) $$h' V(1-2g^2) \equiv 2W + 4g(g+1) \pmod{16}.$$

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

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

that is:

(12.15) $$h'V \equiv 2(W-1) + 3k' \pmod{16}.$$

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

(12.16) $$h' \equiv 3k'V + 2(W-1) \pmod{16}.$$

References

[1] P. G. L. Dirichlet and R. Dedekind, *Vorlesungen über Zahlentheorie,* Chelsea Publishing Company, Bronx, New York 1968.

[2] P. G. L. Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*; *Werke I*, pp. 411–496, Chelsea Publishing Company, Bronx, New York 1969.

[3] C. F. Gauss, *Werke II,* Königlichen Gesellschaft der Wissenschaften, Göttingen 1876.

[4] — *Untersuchungen über höhere Arithmetik,* Chelsea Publishing Company, Bronx, New York 1965.

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

[6] P. Kaplan and K. S. Williams, *On the class numbers of* $Q(\sqrt{\pm 2p})$ *modulo* 16, *for* $p \equiv 1 \pmod 8$ *a prime,* Acta Arith. 40(1982), pp. 289–296.

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

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

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

[10] — *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.

[11] — *The class number of* $Q(\sqrt{p})$ *modulo* 4, *for* $p \equiv 5 \pmod 8$ *a prime,* Pacific J. Math. 92(1981), pp. 241–248.

10, Allée Jacques Offenbach
54420 — Saulxures les Nancy
France

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

Received on 18.12.1979 (1189)