On Linear Congruence Relations between Class Numbers of Quadratic Fields

TSUYOSHI UEHARA

Department of Information Science, Saga University, Saga 840, Japan

Communicated by Hans Zassenhaus

Received August 26, 1988; revised May 13, 1989

This paper presents a general congruence modulo a certain power of 2 relating the class numbers and units of the quadratic fields whose discriminants are divisors of \(8m\), where \(m > 1\) is a given square-free rational integer. An application of this congruence gives some relations between the class numbers and units of the quadratic fields \(\mathbb{Q}(m^{1/2})\) and \(\mathbb{Q}((-m)^{1/2})\).

1. INTRODUCTION

Throughout this paper we denote by \(m > 2\) an odd, square-free, rational integer having \(r\) prime divisors. Hardy and Williams [2] obtained a linear congruence modulo \(2^{r+2}\) relating the class numbers of imaginary quadratic fields \(\mathbb{Q}(n^{1/2})\) with \(n \mid 2m\), which is a unified congruence for the congruences proved by Kenku [8] and by Pizer [12] when \(r = 2\). Recently, applying his theoretical aspect for \(p\)-adic \(L\)-functions, Gras [1] deduced a general congruence relation modulo \(2^{r+1} (0 < l < 5)\) between the class numbers and units of real and imaginary quadratic fields \(\mathbb{Q}(n^{1/2})\) with \(n \mid 2m\). In this paper, through elementary transformation of Dirichlet's class number formula in an extension of the 2-adic number field, we prove a more general congruence relation that is described later in this section, and indicate how it includes the earlier results. Using the general congruence relation, we also obtain some congruences for the class numbers and units of \(\mathbb{Q}((fm)^{1/2})\) and \(\mathbb{Q}((-fm)^{1/2})\), where \(f = 1, 2\). It is shown that our congruences cover those of Hikita [4], Kaplan [5], Kaplan and Williams [6, 7], Kudo [9], Lang [10], Lang and Schertz [11], and Williams [13].

We shall now state our main result. For a square-free rational integer \(n \neq 1\), let \(h(n)\) be the class number of the quadratic field \(\mathbb{Q}(n^{1/2})\) when...
$n \neq -1, -3$, and put $h(-1) = \frac{1}{2}, h(-3) = \frac{1}{3}$. Denote by $\chi_n$ the Kronecker symbol corresponding to $n$. We define $H(n)$ by

$$H(n) = \begin{cases} (2 - \chi_n(2)) h(n) \frac{\log \varepsilon(n)}{D(n)^{1/2}} & \text{if } n > 0, \\ (1 - \chi_n(2)) h(n) & \text{if } n < 0, \end{cases} \quad (1.1)$$

where $D(n)$ and $\varepsilon(n)$ denote the discriminant and the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{n})$, and $\log$ means the 2-adic logarithm. It is convenient to put $H(1) = 0$. We take two multiplicative arithmetic functions $\psi, \theta$ such that $\psi(d) \equiv \theta(d) \equiv 1 \pmod{2}$ for every $d \mid m$, and let

$$\Phi_\psi(d) = \prod_{p \mid m} (1 - \theta(p))$$

for every $d \mid m$. Put $E = \{1, -1, 2, -2\}$. We introduce the sums $H^\pm_m(m, \psi, \theta)$ ($e \in E$) expressible as

$$H^+_m(m, \psi, \theta) = \sum_{0 < d \mid m} \sum_{d \equiv 1 \pmod{4}} \psi(d) H(ed) \prod_{p \mid m/d} (1 - \chi_{ed}(p) \theta(p)) + I(e) \quad \text{if } e > 0,$$

$$= \sum_{0 < d \mid m} \sum_{d \equiv -1 \pmod{4}} \psi(d) H(-ed) \prod_{p \mid m/d} (1 - \chi_{-ed}(p) \theta(p)) \quad \text{if } e < 0,$$

and

$$H^-_m(m, \psi, \theta) = \sum_{0 < d \mid m} \sum_{d \equiv 1 \pmod{4}} \psi(d) H(ed) \prod_{p \mid m/d} (1 - \chi_{ed}(p) \theta(p) p) + I(e) \quad \text{if } e > 0,$$

$$= \sum_{0 < d \mid m} \sum_{d \equiv -1 \pmod{4}} \psi(d) H(-ed) \prod_{p \mid m/d} (1 - \chi_{-ed}(p) \theta(p) p) \quad \text{if } e < 0,$$

where $I(e) = -\Phi_\psi(m) H(e)$ if $e \neq 1$ and

$$I(1) = \frac{1}{2} \sum_{p \mid m} \theta(p) \Phi_\psi(m/p) \log p.$$

We shall establish that

$$\sum_{e \in E} (x_e H^+(m, \psi, \theta) + y_e H^-(m, \psi, \theta)) \equiv 0 \pmod{2^r + 1} \quad (1.2)$$
for given 2-adic integers \( x_e, y_e \), where \( 0 \leq l \leq 5 \), is a rational integer determined dependently only upon \( x_e, y_e \). In particular, \( (1, 2) \) is valid modulo \( 2^{n+5} \) if \( x_e = y_e = |e|/\pi \). For example, in the case that \( m = p \equiv 1 \pmod{8} \) is a prime and \( \psi(p) = \theta(p) = 1 \), \( (1, 2) \) gives the congruence

\[
H(p) + H(2p) - H(-p) - H(-2p) \equiv \{3(p - 1) - \log p\}/2 \pmod{64}.
\]

In the following, for a positive integer \( s \in \mathbb{Z} \), we adopt the notations

\[
\prod_{p \mid s} \left( \sum_{p \mid s'} \right), \quad \sum_{a = 1}^{s'}
\]

to mean a product (a sum) taken over the primes \( p \) dividing \( s \), a sum taken over the integers \( a \in \mathbb{Z} \) such that \( 1 \leq a \leq s \) and \( (a, s) = 1 \), respectively.

2. Class Number Formulas

In this section we are concerned with classical formulas for class numbers of quadratic fields.

For any rational integer \( n > 0 \), \( \zeta_n \in \mathbb{C} \) denotes a primitive \( n \)th root of unity. Let \( \chi \) be a primitive Dirichlet character modulo \( n \) with values in \( \mathbb{C} \). The Gauss sum \( S(\chi, \zeta_n) \) is defined by

\[
S(\chi, \zeta_n) = \sum_{a = 1}^{n} \chi(a) \zeta_n^a.
\]

It is known that

\[
S(\chi, \zeta_n^n) = \chi^{-1}(b) S(\chi, \zeta_n)
\]

for every \( b \in \mathbb{Z} \), and

\[
S(\chi, \zeta_{n_1} \zeta_{n_2}) = S(\chi_{n_1}, \zeta_{n_1}) S(\chi_{n_2}, \zeta_{n_2})
\]

if \( n = n_1 n_2 \), \( (n_1, n_2) = 1 \), and \( \chi = \chi_1 \chi_2 \), with \( \chi_i \) a Dirichlet character modulo \( n_i \) \( (i = 1, 2) \).

**Lemma 1.** If \( n > 1 \) then one has

\[
\sum_{a = 1}^{n} \chi(a) a = S(\chi, \zeta_n) \sum_{a = 1}^{n-1} \frac{\chi^{-1}(a)}{1 - \zeta_n^a}.
\]
Proof. By easy calculation we see

\[
\sum_{a=1}^{n} \chi(a) a = -\sum_{a=1}^{n} \chi(a) \sum_{b=1}^{n-1} \frac{1 - \zeta_{n}^{a b}}{1 - \zeta_{n}^{b}} - \sum_{b=1}^{n} \frac{S(\chi, \zeta_{n}^{b})}{1 - \zeta_{n}^{b}}.
\]

Thus the lemma follows from (2.1).

For a given rational integer \(n\) such that \(n \neq t^2\) for any \(t \in \mathbb{Z}\), we denote by \(\chi_n\) the Kronecker symbol corresponding to the quadratic field \(\mathbb{Q}(n^{1/2})\), and define \(h(n)\) by

\[
h(n) = \frac{2h'(n)}{w(n)},
\]

where \(h'(n)\) is the class number of \(\mathbb{Q}(n^{1/2})\) and \(w(n)\) denotes the number of roots of unity in this field.

Let \(D\) be the discriminant of a quadratic field \(\mathbb{Q}(D^{1/2})\), and put \(d = |D|\). The Kronecker symbol \(\chi_D\) is a primitive Dirichlet character modulo \(d\), and \(\chi_D\) is even or odd according as \(D > 0\) or \(D < 0\). We recall that for any prime \(p\) not dividing \(D\)

\[
\chi_D(p) = \left(\frac{2}{d}\right) \quad \text{if} \quad p = 2,
\]

\[
= \left(\frac{D}{p}\right) \quad \text{if} \quad p \neq 2,
\]

where \(\left(\frac{\cdot}{\cdot}\right)\) means the Legendre–Jacobi symbol. One knows that

\[
S(\chi_D, \xi_d) = D^{1/2}
\]

(2.3)

with \(\xi_d = \cos (2\pi/d) + i \sin (2\pi/d)\).

If \(D > 0\), we denote by \(\varepsilon(D) > 1\) the fundamental unit of \(\mathbb{Q}(D^{1/2})\). Let us now recall the following class number formulas due to Dirichlet:

\[
\varepsilon(D)^{-2h(D)} = \prod_{a=1}^{D-1} (1 - \xi_d^{2h(a)}) \quad \text{if} \quad D > 0.
\]

(2.4)

\[
h(D) = -\frac{1}{d} \sum_{a=1}^{d} \chi_D(a) a \quad \text{if} \quad D < 0.
\]

(2.5)

From now on the algebraic closure \(\overline{\mathbb{Q}} \subset \mathbb{C}\) of \(\mathbb{Q}\) is assumed to be contained in an algebraic closure \(\mathbb{Q}_2\) of the 2-adic number field \(\mathbb{Q}_2\). By
TSUYOSHI UEHARA

\[ \log = \log_2 \] we denote the 2-adic logarithm. In the case \( D > 0 \), (2.1), (2.3), and (2.4) imply

\[
\frac{S(\chi_D, \zeta_D)}{D} \sum_{a=1}^{D-1} \chi_D(a) \log(1 - \zeta_a^D) = -2h(D) \frac{\log \varepsilon(D)}{D^{1/2}}.
\] (2.6)

It is convenient to put

\[
L^+(\eta) = \log(1 - \eta), \quad L^-(\eta) = \frac{1}{1 - \eta}
\]

for any \( \eta \in \mathbb{Q}_2, \eta \neq 1 \). We further define \( h(D) \) as follows:

\[
h(D) = \begin{cases} 
2h(D) \frac{\log \varepsilon(D)}{D^{1/2}} & \text{if } D > 0, \\
= h(D) & \text{if } D < 0.
\end{cases}
\]

**Lemma 2.** With the notation and assumptions as above,

\[
-\frac{S(\chi_D, \zeta_D)}{d} \sum_{a=1}^{D-1} \chi_D(a) L^\pm(\zeta_a^D) = h(D) \quad \text{if } \pm D > 0,
\]

\[
= 0 \quad \text{if } \pm D < 0.
\]

**Proof.** The formulas for \( h(D) \) follow immediately from Lemma 1, (2.5), and (2.6). The others are obvious because

\[
L^+(\eta) - L^-(\eta^{-1}) = \log(-\eta) = 0, \quad L^-(\eta) + L^-(\eta^{-1}) = 1
\]

for any root \( \eta \neq 1 \) of unity.

In the following we denote \( r(n) \) the number of prime divisors of a positive rational integer \( n \). Then the Moebius function \( \mu \) is expressible as

\[
\mu(n) = (-1)^{r(n)}
\]

when \( n \) is square-free.

**Lemma 3.** Let \( \chi \) be a Dirichlet character modulo \( n > 1 \) and let \( s > 0 \) be a square-free rational integer with \( (s, n) = 1 \). Suppose \( \zeta_{ns}^\prime = \zeta_{n}^\prime \zeta_{s}^\prime \). Then

\[
\sum_{a=1}^{ns} \chi(a) L^\pm(\zeta_{ns}^a) = \prod_{p|s} (\chi^\pm(p) - 1) \sum_{b=1}^{n} \chi(b) L^\pm(\zeta_{n}^b),
\]

where \( \chi^+(p) = \chi^{-1}(p), \chi^-(p) = \chi^{-1}(p)p \) for every prime \( p | s \).
Proof. We prove the lemma by induction on \( r(s) \). Let \( q \) be a prime dividing \( s \). We put \( t = s/q \), \( \eta_n = \zeta_n^q \), \( \eta_t = \zeta_t^q \) and \( \eta_{nt} = \zeta_{ns}^q = \eta_n \eta_t \). It is easily seen that

\[
\sum_{c=0}^{q-1} L^+(\zeta_c^q) = L^+(\zeta^q), \quad \sum_{c=0}^{q-1} L^-(\zeta_c^q) = qL^-(\zeta^q)
\]

for any \( \zeta \in \mathbb{Q}_2 \), \( \zeta^q \neq 1 \). Using these formulas we compute

\[
\sum_{a=1}^{n_t} \chi(a) L^\pm(\zeta_n^a) = \sum_{a=1}^{n_t} \chi(a) \left( \sum_{c=0}^{q-1} L^\pm(\zeta_{ns}^c) \right) - \sum_{a=1}^{n_t} \chi(aq) L^\pm(\zeta_{ns}^aq)
\]

\[
= \chi(q)(\chi^+(q) - 1) \sum_{a=1}^{n_t} \chi(a) L^\pm(\eta_n^a).
\]

It follows from the inductive hypothesis that

\[
\sum_{a=1}^{n_t} \chi(a) L^\pm(\eta_n^a) = \prod_{p \mid n} (\chi^+(p) - 1) \sum_{b=1}^{n} \chi(b) L^\pm(\eta_n^b)
\]

\[
= \chi^{-1}(q) \prod_{p \mid n} (\chi^+(p) - 1) \sum_{b=1}^{n} \chi(b) L^\pm(\zeta_n^b).
\]

This completes the proof.

3. Linear Congruence Relations

It is the purpose of this section to prove our main result, namely a linear congruence relation between the numbers \( H(n) \) with \( n \mid 2m \). In what follows we suppose that \( \zeta_s = \zeta_t \), for any positive divisors \( s, t \) of \( 8m \) with \( (s, t) = 1 \).

Let \( E = \{1, -1, 2, -2\} \). For any \( e \in E \) and any \( \zeta \in \mathbb{Q}_2 \) (except \( \zeta = \pm 1 \) if \( e = 1 \)) we define \( K^\pm_e(\zeta) \) as

\[
K^\pm_e(\zeta) = \frac{-1}{2} (L^\pm(\zeta) - L^\pm(-\zeta)) \quad \text{if } e = 1,
\]

\[
= -\frac{S(\zeta_e, \zeta_{4f})}{4f} \sum_{a=1}^{4f} \chi_e(a) L^\pm(\zeta_{4f}^a \zeta) \quad \text{if } e \neq 1,
\]

where \( f = |e| \). It is not difficult to see that

\[
K^+_1(\zeta) = \frac{2L^+(\zeta)}{L^+(\zeta^2)} / 2, \quad K^-_1(\zeta) = \frac{L^-(\zeta)}{L^-(\zeta^2)}.
\]
For any divisor \( n \neq 1 \) of \( 2m \), we introduce the number \( H(n) \) defined as in (1.1); namely
\[
H(n) = (1 - \chi_n(2) 2^{-1}) h(D(n)) \quad \text{if } n > 0,
\]
\[
= (1 - \chi_n(2)) h(n) \quad \text{if } n < 0,
\]
where \( D(n) \) is the discriminant of \( \mathbb{Q}(n^{1/2}) \).

**Lemma 4.** For any \( e \in E \) and any divisors \( c, d > 0 \) of \( m \) with \( d \mid c \), let
\[
R^\pm_e (c, d) = \frac{S(\chi_D, \zeta_\pm^d)}{d} \sum_{b=1}^{c'} \chi_D(b) K^\pm_e (\zeta^b_c),
\]
where \( D = (-1)^{(d-1)/2} d \) and \( \chi_i \) is considered to be the trivial character. Then
\[
R^\pm_e (c, d) = H(eD) \prod_{p \mid c/d} (\chi_{eD}(p) - 1) \quad \text{if } \pm eD > 0 \text{ and } eD \neq 1,
\]
\[
= 0 \quad \text{if } \pm eD < 0,
\]
where \( \chi_{eD}(p) = \chi_{eD}(p) \), \( \chi_{cD}(p) = \chi_{eD}(p) p \) for every prime \( p \mid c/d \). Moreover
\[
R^+_1 (c, 1) = -(\log c)/2 \text{ if } r(c) = 1 \text{ and } R^+_1 (c, 1) = 0 \text{ if } r(c) > 1.
\]

**Proof.** If \( d \neq 1 \) then by Lemma 3 one has
\[
R^\pm_1 (c, d) = \frac{S(\chi_D, \zeta^d)}{d} \sum_{b=1}^{c'} \chi_D(b) K^\pm_1 (\zeta^b_c) \prod_{p \mid c/d} (\chi_{eD}(p) - 1).
\]
Hence, when \( e = 1 \) and \( d \neq 1 \), the assertion is a consequence of Lemma 2. It is easy to see that
\[
R^+_1 (c, 1) = \sum_{b=1}^{c'} K^+_1 (\zeta^b_c) = \frac{-1}{2} \sum_{b=1}^{c'} \log(1 - \zeta^b_c) = -(\log c)/2 \quad \text{if } r(c) = 1,
\]
\[
= 0 \quad \text{if } r(c) > 1,
\]
\[
R^-_1 (c, 1) = \sum_{b=1}^{c'} K^-_1 (\zeta^b_c) = - \sum_{b=1}^{c'} \left( \frac{1}{1 - \zeta^b_c} - \frac{1}{1 - \zeta^{2b}_c} \right) = 0.
\]
In the case \( e \neq 1 \), applying (2.2) and Lemma 3 we compute
\[
R^\pm_e (c, d) = - \frac{S(\chi_e, \zeta_4^d)}{4fd} \sum_{a=1}^{d/4} \chi_e(a) L^\pm (\zeta_4^a, \zeta_4^b)
\]
\[
= - \frac{S(\chi_{eD}, \zeta_4^d)}{4fd} \sum_{a=1}^{d/4} \chi_{eD}(a) L^\pm (\zeta_4^a)
\]
\[
= - \frac{S(\chi_{eD}, \zeta_4^d)}{4fd} \sum_{a=1}^{d/4} \chi_{eD}(a) L^\pm (\zeta_4^d) \prod_{p \mid c/d} (\chi_{eD}(p) - 1).
\]
In this case the assertion is also seen from Lemma 2.
Let $\psi$, $\theta$ be multiplicative arithmetic functions with values in $\mathbb{Q}_2$ such that $\psi(d) \equiv \theta(d) \equiv 1 \pmod{2}$ for every divisor $d$ of $m$. We denote by $\theta^{-1}$ an arithmetic function satisfying $\theta^{-1}(d) = \theta(d)^{-1}$ for every divisor $d$ of $m$. We show a formula about the function $\Phi_\theta$ defined by

$$
\Phi_\theta(d) = \prod_{p | d} (1 - \theta(p)).
$$

If $\chi$ is a multiplicative arithmetic function, then

$$
\sum_{0 < t | s} \theta(t) \Phi_\theta(s/t) \prod_{p | t} (1 - \chi(p))
= \theta(s) \prod_{p | s} \left( \theta^{-1}(p) - 1 \right) \prod_{p | t} (1 - \chi(p))
= \prod_{p | s} \left\{ (\theta^{-1}(p) - 1) + (1 - \chi(p)) \right\}
= \prod_{p | s} (1 - \chi(p) \theta(p))
$$

for any divisor $s > 0$ of $m$. For any divisor $c > 0$ of $m$ and any $b \in \mathbb{Z}$, we introduce the product $F_{c, \psi}(b)$ defined by

$$
F_{c, \psi}(b) = \prod_{p | c} \left( \frac{S(\chi_p, \zeta_p)}{p} \psi(p) \chi_p(b) - 1 \right)
$$

where $P = (-1)^{(p-1)/2} p$. For each $e \in E$ let

$$
H^\pm_e(c, \psi) = \sum_{b = 1}^c F_{c, \psi}(b) K^\pm_e(\zeta^b_c)
$$

with $1 < c | m$. We define the sums $H^\pm_e(m, \psi, \theta)$ $(e \in E)$ by

$$
H^\pm_e(m, \psi, \theta) = \sum_{1 < c | m} \theta(c) \Phi_\theta(m/c) H^\pm_e(c, \psi_\theta^{-1}).
$$

We shall prove that the above sums are expressible as in Section 1.

**Lemma 5.** Let the notation and assumptions be as above. Then

$$
H^+_1(m, \psi, \theta) = \sum_{1 < d | m \atop d \equiv 1 \pmod{4}} \psi(d) H(d) \prod_{p | m/d} \left( 1 - \left( \frac{d}{p} \right) \theta(p) \right)
+ \frac{1}{2} \sum_{p | m} \theta(p) \Phi_\theta(m/p) \log p,
$$

641/34/3-9
\[ H^+_1(m, \psi, \theta) = \sum_{1 < d | m, d \equiv -1 \pmod{4}} \psi(d) H(d) \prod_{p | m/d} \left( 1 - \left( \frac{d}{p} \right) \theta(p) \right) \]

\[ H^+_2(m, \psi, \theta) = \sum_{0 < d | m, d \equiv 1 \pmod{4}} \psi(d) H(2d) \prod_{p | m/d} \left( 1 - \left( \frac{2d}{p} \right) \theta(p) \right) - H(2) \Phi_\theta(m). \]

\[ H^-_2(m, \psi, \theta) = \sum_{1 < d | m, d \equiv -1 \pmod{4}} \psi(d) H(2d) \prod_{p | m/d} \left( 1 - \left( \frac{2d}{p} \right) \theta(p) \right), \]

\[ H^-_1(m, \psi, \theta) = \sum_{1 < d | m, d \equiv -1 \pmod{4}} \psi(d) H(-d) \prod_{p | m/d} \left( 1 - \left( \frac{-d}{p} \right) \theta(p) \right) - \frac{1}{2} \Phi_\theta(m). \]

\[ H^-_2(m, \psi, \theta) = \sum_{0 < d | m, d \equiv 1 \pmod{4}} \psi(d) H(-2d) \prod_{p | m/d} \left( 1 - \left( \frac{-2d}{p} \right) \theta(p) \right) - \Phi_\theta(m). \]

**Proof.** The formula (2.2) implies

\[ H^\pm_e(c, \psi) = \sum_{b=1}^c \sum_{0 < d | c} \frac{S(\chi_D, \xi_d)}{d} \mu(c/d) \psi(d) \chi_D(b) K^\pm_e(\xi_d) \]

\[ = \sum_{0 < d | c} \mu(c/d) \psi(d) R^\pm_e(c, d). \]

Here \( \chi_D \) and \( R^\pm_e(c, d) \) are defined as in Lemma 4. Note that \( \pm eD > 0 \) if and only if \( d \equiv \pm f/e \pmod{4} \) with \( f = |e| \). By Lemma 4 one sees that

\[ H^+_1(c, \psi) = \sum_{1 < d | c, d \equiv -1 \pmod{4}} \psi(d) H(\pm d) \prod_{p | c/d} \left( 1 - \chi_{\pm d}(p) \right) + J^\pm(c), \]

where \( J^+(c) = \frac{1}{2} \log c \) if \( r(c) = 1 \), \( J^+(c) = 0 \) otherwise and \( J^-(c) = 0 \), and that

\[ H^\pm_e(c, \psi) = \sum_{0 < d | c, d \equiv \pm e \pmod{4}} \psi(d) H(\pm fd) \prod_{p | c/d} \left( 1 - \chi_{\pm fd}(p) \right) \]
for any $e \neq 1$ with $\sigma = f/e$. Therefore

$$H^\pm_1(m, \psi, \theta) = \sum_{d \mid m, d = \pm 1 \mod 4} \psi(d) \theta^{-1}(d) H(\pm d) \sum_{c \mid d} \theta(c) \Phi_\sigma(m/c) \prod_{p \mid c} (1 - \chi_{\pm f}(p)) + \sum_{p \mid m} \theta(p) \Phi_\sigma(m/p) J^\pm(p),$$

where the sum involving $c$ is taken over the divisors $c$ of $m$ which are divisible by $d$. Similarly we get

$$H^\pm_\sigma(m, \psi, \theta) + \Phi_\sigma(m) K^\pm_\sigma(1) = \sum_{0 < d \mid m} \psi(d) \theta^{-1}(d) H(\pm fd) \times \sum_{c \mid d} \theta(c) \Phi_\sigma(m/c) \prod_{p \mid c} (1 - \chi_{\pm fd}(p))$$

for any $e \neq 1$. Herein $K^\pm_\sigma(1) = H(\pm f)$ if $\pm \sigma = 1$ and $K^\pm_\sigma(1) = 0$ if $\pm \sigma = -1$. Putting $s = m/d$ and $t = c/d$ we apply (3.1) to the right-hand sides of the above formulas to obtain that

$$\theta^{-1}(d) \sum_{c \mid d} \theta(c) \Phi_\sigma(m/c) \prod_{p \mid c} (1 - \chi_{\pm fd}(p)) = \prod_{p \mid m/d} (1 - \chi_{\pm fd}(p)) \theta(p).$$

This proves the lemma.

The following lemma is fundamental for the proof of our main theorem.

**Lemma 6.** Let $\zeta \neq 1$ be an $m$th root of unity, and put

$$w_x = \frac{\zeta^x}{1 + \zeta^{2x}}$$

with $x = \pm 1$. Then

$$K^+_x(\zeta) = \sum_{k=0}^{\infty} \frac{(4x)^k w_x^{2k+1}}{2k+1}, \quad K^-_x(\zeta) = w_{-x},$$

$$K^+_x(\zeta) = \sum_{k=0}^{\infty} \frac{(2x)^k w_x^{2k+1}}{2k+1}, \quad K^-_x(\zeta) = \sum_{k=0}^{\infty} (-2x)^k w_{-x}^{2k+1}.$$
Proof. We first note that $w_\alpha$ are integers in $\mathbb{Q}_2$. Put $\beta = 1$ or $\beta = i = (-1)^{1/2}$ according as $\alpha = 1$ or $\alpha = -1$. We compute

$$K_\alpha^+(\xi) = -\frac{\beta}{2} (L^+(\beta \xi) - L^+(-\beta \xi))$$

$$= -\frac{\beta}{4} \{ \log(1 - 2\beta \xi + \alpha \xi^2) - \log(1 + 2\beta \xi + \alpha \xi^2) \}$$

$$= -\frac{\beta}{4} \log \left( \frac{1 - 2\alpha \beta w_\alpha}{1 + 2\alpha \beta w_\alpha} \right) = \sum_{k=0}^{\infty} \frac{(4\alpha)^k w_\alpha^{2k+1}}{2k+1},$$

$$K_\alpha^-(\xi) = -\frac{\beta}{2} (L^-(-\beta \xi) - L^-(-\beta \xi)) = w_{-\alpha}.$$

We next let $\eta = \cos(\pi/4) + i \sin(\pi/4) = (1 + i)/2^{1/2}$. Then $\eta^3 = -\eta^{-1}$, $\eta^5 = -\eta$, $\eta^7 = \eta^{-1}$ and $\eta + \alpha \eta^{-1} = (2\alpha)^{1/2}$. Hence we have

$$K_{2\alpha}^+(\xi) = -\frac{(8\alpha)^{1/2}}{8} \{ L^+(\eta \xi) + \alpha L^+(\eta^{-1} \xi) - L^+(-\eta \xi) - \alpha L^+(-\eta^{-1} \xi) \}$$

$$= -\frac{(2\alpha)^{1/2}}{4} \{ \log(1 - (2\alpha)^{1/2} \xi + \alpha \xi^2) - \log(1 + (2\alpha)^{1/2} \xi + \alpha \xi^2) \}$$

$$= -\frac{(2\alpha)^{1/2}}{4} \log \left( \frac{1 - (2\alpha)^{1/2} \alpha w_{\alpha}}{1 + (2\alpha)^{1/2} \alpha w_{\alpha}} \right) = \sum_{k=0}^{\infty} \frac{(2\alpha)^k w_{\alpha}^{2k+1}}{2k+1},$$

$$K_{2\alpha}^-(\xi) = -\frac{(8\alpha)^{1/2}}{8} \{ L^-(\eta \xi) - L^-(-\eta \xi) + \alpha(L^-(\eta^{-1} \xi) - L^-(-\eta^{-1} \xi)) \}$$

$$= -\frac{(2\alpha)^{1/2}}{4} \left( \frac{2\eta \xi}{1 - i\xi^2} + \alpha \frac{2\eta^{-1} \xi}{1 + i\xi^2} \right)$$

$$= -\frac{\alpha \xi(1 - \alpha \xi^2)}{1 + \xi^4} = \frac{w_{-\alpha}}{1 + 2\alpha w_{-\alpha}} = \sum_{k=0}^{\infty} (-2\alpha)^k w_{-\alpha}^{2k+1}.$$

Thus the lemma has been proved.

We intend to find congruence relations between $K_\epsilon^+(\xi)$ ($\epsilon \in E$), where $\xi \neq 1$, $\xi^m = 1$. Put $w_\alpha = w_\alpha(\xi) = \alpha \xi/(1 + \alpha \xi^2)$ with $\alpha = \pm 1$ as in Lemma 6. Since $w_i^i \pm w_{-i}^{-i} \equiv 0$ (mod 2) for every $i \geq 0$, one can define 2-adic integers

$$v_{2k+1} = v_{2k+1}(\xi) = ((-1)^k w_{-i}^{2k+1} - w_{i}^{2k+1})/2.$$
Let \( x_e, y_e (e \in E) \) be 2-adic integers. By Lemma 6 we obtain
\[
\sum_{e \in E} (x_e K_e^+ (\xi) + y_e K_e^- (\xi))
= (x_1 + x_2 + y_{-1} + y_{-2}) w_1 + (x_{-1} + x_{-2} + y_1 + y_2) w_{-1}
+ \sum_{k=1}^{\infty} \frac{2^k}{2k + 1} \{2^k x_1 + x_2 + (2k + 1) y_{-2}\} w_{1}^{2k+1}
+ \sum_{k=1}^{\infty} \frac{(-2)^k}{2k + 1} \{2^k x_{-1} + x_{-2} + (2k + 1) y_2\} w_{1}^{2k+1}
= z_0 w_1 + z_1 v_1 + \sum_{k=1}^{\infty} \frac{1}{2k + 1} (z_{2k} w_1^{2k+1} + z_{2k+1} v_{2k+1}),
\]
where
\[
z_0 = \sum_{e \in E} (x_e + y_e), \quad z_1 = 2(x_{-1} + x_{-2} + y_1 + y_2),
z_{2k} = 2^k \{2^k (x_1 + x_{-1}) + (x_2 + x_{-2}) + (2k + 1)(y_2 + y_{-2})\},
z_{2k+1} = 2^{k+1} \{2^k x_{-1} + x_{-2} + (2k + 1) y_2\}.
\]
Suppose \( x_e, y_e (e \in E) \) are not all zero, and denote by \( 2^t \) the highest power of 2 dividing \( z_i \) for every \( i \geq 0 \). From the above calculation we see that
\[
\sum_{e \in E} (x_e K_e^+ (\xi) + y_e K_e^- (\xi)) \equiv 0 \pmod{2^t}.
\]
We now assume \( \tau \geq 6 \). Since
\[
8z_1 - 2z_5 + z_7 \equiv 32y_{-2} \pmod{64},
8(2z_6 - z_7) - 2(2z_4 - z_5) + 2z_6 - z_7 \equiv 32x_2 \pmod{64},
\]
we get \( x_2 \equiv x_{-2} \equiv 0 \pmod{2} \). Next \( z_7 \equiv 2z_6 - z_7 \equiv 0 \pmod{64} \) implies that \( y_2 \equiv y_{-2} \equiv 0 \pmod{2} \) and \( x_{-2} - y_2 \equiv x_2 - y_{-2} \equiv 0 \pmod{4} \). Hence \( z_3 \equiv 8x_{-1} \equiv 0 \pmod{16}, 2z_2 - z_3 \equiv 8x_1 \equiv 0 \pmod{16}, and so \( x_1 \equiv x_{-1} \equiv 0 \pmod{2} \). Observing that \( z_1 \equiv 0 \pmod{4} \) and \( z_0 \equiv 0 \pmod{2} \), we finally see that \( x_e, y_e \) are all even. On the other hand, if \( x_1 = x_{-2} = y_1 = y_{-2} = 1 \) and \( x_{-1} = x_{-2} = y_1 = y_{-2} = -1 \), one has \( \tau \geq 5 \).

Taking the above argument into consideration we state the following

**Lemma 7.** Let \( \xi \) be as in Lemma 6. For any 2-adic integers \( x_e, y_e (e \in E) \) it holds that
\[
\sum_{e \in E} (x_e K_e^+ (\xi) + y_e K_e^- (\xi)) \equiv 0 \pmod{2^t},
\]
where \( 2^t \) is the greatest common divisor of \( z_i (0 \leq i \leq 6) \) and 32.
Proof. Clearly \( z_7 \equiv z_8 \equiv 0 \pmod{16} \) and \( z_j \equiv 0 \pmod{32} \) for all \( j \geq 9 \). If \( z_5 \equiv z_6 \equiv 0 \pmod{32} \), then it is easily seen that \( z_7 \equiv z_8 \equiv 0 \pmod{32} \). Thus \( l \leq 7 \) and the lemma follows from (3.4).

We are now ready to state our main theorem.

THEOREM 1. Let \( m \) be an odd, square-free, rational integer having \( r \) prime divisors, and let \( \psi, \theta \) be multiplicative arithmetic functions such that \( \psi(d) \equiv \theta(d) \equiv 1 \pmod{2} \) for any divisor \( d \mid m \). Then

\[
\sum_{e \in E} (x_e H_e^+(m, \psi, \theta) + y_e H_e^-(m, \psi, \theta)) \equiv 0 \pmod{2^r+1} \quad (3.5)
\]

for any 2-adic integers \( x_e, y_e \ (e \in E) \), where \( 2^l \) is the greatest common divisor of the eight integers \( s_i \ (0 \leq i \leq 7) \) defined by

\[
\begin{align*}
    s_0 &= x_1 + x_{-1} + x_2 + x_{-2} + y_1 + y_{-1} + y_2 + y_{-2}, \\
    s_1 &= 2(x_{-1} + x_{-2} + y_1 + y_2), \\
    s_2 &= 4(x_1 + x_{-1}) + 2(x_2 + x_{-2}) + 6(y_2 + y_{-2}), \\
    s_3 &= 8x_{-1} + 4x_{-2} + 12y_2, \\
    s_4 &= 16(x_1 + x_{-1}) + 4(x_2 + x_{-2}) - 12(y_2 + y_{-2}), \\
    s_5 &= 8(x_{-2} + y_2), \\
    s_6 &= 8(x_2 + x_{-2} - y_2 - y_{-2}), \\
    s_7 &= 32.
\end{align*}
\]

Proof. For any prime \( p \) dividing \( m \) and for any \( b \in \mathbb{Z} \) not divisible by \( p \), it holds that

\[
\frac{1}{p} S(\chi_p, \zeta_p) \chi_p(b) \psi(p) - 1 \equiv 1 + \zeta_p + \cdots + \zeta_p^{p-1} \equiv 0 \pmod{2} \quad (\text{mod 2})
\]

with \( P = (-1)^{(p-1)/2} p \). This shows that \( F_{c,\psi}(b) \equiv 0 \pmod{2^{r(c)}} \) if \( (b, c) = 1 \). On the other hand \( \Phi_{\theta}(m/c) \equiv 0 \pmod{2^{r-c-1}} \). Hence by the definitions (3.2), (3.3) we can write

\[
H_e^\pm(m, \psi, \theta) = 2^r \sum_{a=1}^{m-1} u(\zeta_m^a) K_e^\pm(\zeta_m^a)
\]

with

\[
u(\zeta_m^a) = \frac{1}{2^r} \theta(c) \Phi_{\theta}(m/c) F_{c,\psi \theta^{-1}}(b),
\]

where \( b = a/(a, m) \) and \( c = m/(a, m) \). It is easy to check that \( s_i \equiv z_i \pmod{32} \) for every \( i, 0 \leq i \leq 6 \). Hence the theorem is deduced from Lemma 7.
We next give a supplement of Theorem 1. Let \( \psi, \theta \) be as above. If a divisor \( d \) of \( m \) satisfies \( d \equiv 3 \pmod{8} \), then the class number \( h(-d) \) does not appear in the congruence (3.5) in Theorem 1 because \( H(-d) = (1 - \chi_{-d}(2)) h(-d) = 0 \). So we define

\[
\tilde{H}_1^-(m, \psi, \theta) = \sum_{1 < c | m} \theta(c) \Phi_\theta(m/c) \tilde{H}_1^-(c, \psi \theta^{-1})
\]

with

\[
\tilde{H}_1^-(c, \psi \theta^{-1}) = - \sum_{b = 1}^{c} F_{c, \psi \theta^{-1}}(b) L^-(\zeta_c^b).
\]

**Lemma 8.** With the notation as above

\[
\tilde{H}_1^-(m, \psi, \theta) = \sum_{d \equiv -1 (\text{mod } 4)} \psi(d) h(-d) \prod_{p | m/d} \left( 1 - \left( \frac{-d}{p} \right) \theta(p) p \right) + \frac{1}{2} \left\{ \Phi_\theta(m) - \prod_{p | m} (1 - \theta(p) p) \right\}.
\]

**Proof.** It follows from Lemmas 3, 4 that

\[
\tilde{H}_1^-(c, \psi \theta^{-1}) = - \sum_{1 < d | c} \mu(c/d) \psi \theta^{-1}(d) \frac{S(\chi_D, \zeta_d)}{d}
\]

\[
\times \sum_{b = 1}^{c} \chi_D(b) L^-(\zeta_c^b) - \mu(c) \sum_{b = 1}^{c} L^-(\zeta_c^b)
\]

\[
= \sum_{1 < d | c} \psi \theta^{-1}(d) h(-d)
\]

\[
\times \prod_{p | c/d} (1 - \chi_{-d}(p) p) - \frac{1}{2} \mu(c) \varphi(c)
\]

for any divisor \( c > 1 \) of \( m \), where \( D = (-1)^{(d-1)/2} d \) and \( \varphi \) means the Euler function. Hence

\[
\tilde{H}_1^-(m, \psi, \theta) = \sum_{1 < d | m} \psi(d) \theta^{-1}(d) h(-d)
\]

\[
\times \sum_{d | c | m} \theta(c) \Phi_\theta(m/c) \prod_{p | c/d} (1 - \chi_{-d}(p) p)
\]

\[
- \frac{1}{2} \left\{ \sum_{0 < c | m} \theta(c) \Phi_\theta(m/c) \prod_{p | c} (1 - p) - \Phi_\theta(m) \right\}.
\]

Applying (3.1) to the above we obtain the lemma.
Since $\Phi_\psi(m/c) F_{e, \psi \theta^{-1}}(b) \equiv 0 \pmod{2'}$ for any $b \in \mathbb{Z}$, $(b, c) = 1$, the following assertion is seen immediately from the definition (3.6).

**Theorem 2.** Let $m, \psi, \theta$ be as in Theorem 1. Then

$$
\tilde{H}_t^- (m, \psi, \theta) \equiv 0 \pmod{2'}.
$$

(3.7)

We remark that the congruence (3.7) is equivalent to Gras's [1, Théorème (1.3), $(c_0)$] in the case that $\psi = \mu$ and $\theta(p) = p^{-1}$ for every prime $p | m$.

In the rest of this section we shall show that our general congruence (3.5) in Theorem 1 includes those of Gras [1] and Hardy and Williams [2]. We know $\varepsilon(2) = 1 + \omega$ with $\omega = 2^{1/2}$. Let $a, b$ be the rational integers such that

$$
a + 8b\omega = (17 + 12\omega)^2 = (1 + \omega)^8.
$$

It is easy to see $a \equiv 17^2 \equiv 1 \pmod{32}$ and $b \equiv 19 \pmod{32}$. Hence

$$
H(2) = \frac{\omega}{4} \log \left( \frac{1 + \omega}{1 - \omega} \right) = \frac{\omega}{32} \log \left( \frac{1 + 8b\omega/a}{1 - 8b\omega/a} \right) \equiv \frac{b}{a} \equiv 19 \pmod{32}.
$$

Let $\lambda$ be an arithmetic function such that $\lambda(p) = p^{-1}$ for any prime $p | m$. The sums $A, \bar{A}, B, \bar{B}, X, \bar{X}, Y, \bar{Y}$ in [1] are expressible as

$$
A = H_+^- (m, \mu, \lambda) + \Phi_+ (m)/2, \quad \bar{A} = H_+^- (m, \mu, \lambda),
$$
$$
B = H_-^- (m, \mu, \lambda) + \Phi_- (m), \quad \bar{B} = H_-^- (m, \mu, \lambda),
$$
$$
X = H_+^+ (m, \mu, \lambda) - \Phi_+ (m) \sigma(m)/2, \quad \bar{X} = H_+^+ (m, \mu, \lambda),
$$
$$
Y = H_-^+ (m, \mu, \lambda) + \Phi_- (m) H(2), \quad \bar{Y} = H_-^+ (m, \mu, \lambda),
$$

where

$$
\sigma(m) = \sum_{\substack{p | m}} \frac{\log p}{p - 1}.
$$

Let $a, \bar{a}, b, \bar{b}, x, \bar{x}, y, \bar{y}$ be 2-adic integers such that $a + \bar{a} + b + \bar{b} + x + \bar{x} + y + \bar{y} = 0$. It was proved by Gras [1] that

$$
aA + \bar{a}A + bB + \bar{b}B + xX + \bar{x}X + yY + \bar{y}Y \equiv \Phi_+ (m) \left\{ 31 \left( -a + \frac{2b}{3} + 2y \right) - (16 + \sigma(m)) x \right\} \pmod{2^{r + 1 + r}}, \quad (3.8)
$$

(3.8)
where \( 2^r \) is the greatest common divisor of the following seven integers:

\[
\begin{align*}
t_1 &= \bar{a} + \bar{b} + \bar{x} + \bar{y}, \\
t_2 &= b + \bar{b} + 2(x + \bar{x}) - (y + \bar{y}), \\
t_3 &= 2(b + \bar{y}) - 4(x - y), \\
t_4 &= 4(x + \bar{x} + y + \bar{y}), \\
t_5 &= 8(x + y), \\
t_6 &= 8(x + \bar{x}), \\
t_7 &= 16.
\end{align*}
\]

We claim that (3.8) can be reproved from (3.5). In fact, in the case that \( \psi = \mu \) and \( \theta = \lambda \), putting \( y_{-1} = a, y_1 = \bar{a}, y_2 = b, x_1 = x, x_2 = \bar{x}, x_3 = y \) and \( x_{-2} = \bar{y} \), we can rewrite (3.5) as

\[
aA + a\bar{A} + bB + \bar{b}B + xX + \bar{x}\bar{X} + yY + \bar{y}\bar{Y} \\
\equiv \frac{\Phi_\lambda(m)}{2} (a + 2b - \sigma(m) x + 38y) \pmod{2^r + 1}.
\]

Note that \( s_0 = 0 \) in this case. We first conclude that \( l = l' + 1 \) because

\[
\begin{align*}
s_3 &\equiv 2(3t_3 - t_4 + t_5 + t_6) \pmod{32}, \\
s_4 &\equiv 2(10t_2 + 3t_4 - 3t_6) \pmod{32}, \\
s_5 &\equiv 2(2t_3 + t_5) \pmod{32}, \\
s_6 &\equiv 2(-4t_2 + t_6) \pmod{32}, \\
t_2 &\equiv -3s_2 + s_4 \pmod{32}, \\
t_3 &\equiv 2s_2 + s_3 + s_4 - s_5 \pmod{32}, \\
t_4 &\equiv -2s_2 + s_4 + s_6 \pmod{32}, \\
t_5 &\equiv 4s_2 + 2s_3 + 2s_4 + s_5 \pmod{32}, \\
t_6 &\equiv 4s_2 + 4s_4 + s_6 \pmod{32}.
\end{align*}
\]

Observing that \( \Phi_\lambda(m) \equiv 0 \pmod{2^r} \), we compute

\[
\frac{\Phi_\lambda(m)}{2} \left\{ (a + 2b - \sigma(m) x + 38y) - 31 \left( -a + \frac{2b}{3} + 2y \right) + (16 + \sigma(m)) x \right\} \\
\equiv 4\Phi_\lambda(m)(4a + 3b + 2x + 5y) \pmod{2^{r+5}} \\
\equiv \Phi_\lambda(m)(16s_0 - 8s_1 - 2s_2 + s_3 + 2s_4 - s_5) \pmod{2^{r+5}} \\
\equiv 0 \pmod{2^{r+1}}.
\]

This proves the claim.
To describe a result in [2] we need the products $c_i(m, d)$ ($1 \leq i \leq 4$, $0 < d|m$) expressible as

$$c_1(m, d) = \prod_{p | m/d} \left( \left( \frac{d}{p} \right) - \left( \frac{-1}{p} \right) \right)$$

$$= (-1)^r \left( \frac{-1}{m} \right) \mu \chi_2(d) \prod_{p | m/d} \left( 1 - \left( \frac{-d}{p} \right) \right),$$

$$c_2(m, d) = \prod_{p | m/d} \left( \left( \frac{d}{p} \right) - \left( \frac{-2}{p} \right) \right)$$

$$= (-1)^r \left( \frac{-2}{m} \right) \mu \chi_2(d) \prod_{p | m/d} \left( 1 - \left( \frac{-2d}{p} \right) \right),$$

$$c_3(m, d) = \left( 5 - \left( \frac{2}{d} \right) \right) \prod_{p | m/d} \left( \left( \frac{-d}{p} \right) - \left( \frac{2}{p} \right) \right)$$

$$= (-1)^r \left\{ 4\mu(d) - \left( 1 - \left( \frac{2}{d} \right) \right) \mu \chi_2(d) \right\} \prod_{p | m/d} \left( 1 - \left( \frac{-d}{p} \right) \right),$$

$$c_4(m, d) = - \prod_{p | m/d} \left( \left( \frac{-d}{p} \right) - \left( \frac{2}{p} \right) \right)$$

$$= (-1)^{r+1} \left( \frac{2}{m} \right) \mu \chi_2(d) \prod_{p | m/d} \left( 1 - \left( \frac{-2d}{p} \right) \right).$$

Hardy and Williams [2] obtained

$$\sum_{\substack{0 < d|m \\text{d} \equiv 1 \pmod{4}}} \{ c_1(m, d) h(-d) + c_2(m, d) h(-2d) \}$$

$$+ \sum_{\substack{0 < d|m \\text{d} \equiv -1 \pmod{4}}} \{ c_3(m, d) h(-d) + c_4(m, d) h(-2d) \}$$

$$+ (-1)^r \varphi(m)/2 \equiv 0 \pmod{2^{r+2}}. \quad (3.9)$$

We remark that the terms $c_5(m), c_6(m)$ in [2] do not appear in (3.9) because we adopt the notation $h(-1) = \frac{1}{2}$, $h(-3) = \frac{1}{4}$. We put $y'_1 = -1$, $y_{-1}' = (-1/m)$, $y_2' = -(2/m)$, and $y_{-2}' = (-2/m)$. With our notation the congruence (3.9) can be rewritten as

$$4\tilde{H}_1^-(m, \mu, \lambda) + \sum_{\epsilon \in \mathcal{E}} y'_\epsilon H_\epsilon^-(m, \mu \chi_2, \lambda) \equiv 0 \pmod{2^{r+2}} \quad (3.10)$$
because \( \chi_{-2}(d) = \chi_2(d) \) for \( d \equiv 1 \pmod{4} \), and

\[
2\Phi_\chi(m) - \frac{1}{2} y'_\chi \Phi_\chi(m) - y'_{-\chi} \Phi_\chi(m) \\
\equiv \left\{ 4 - \left( \frac{-1}{m} \right) - 2 \left( \frac{-2}{m} \right) \right\} \Phi_\chi(m)/2 \equiv \varphi(m)/2 \pmod{2^{r+2}}.
\]

Since \( l = 2 \) in Theorem 1 when \( x_e = 0, y_e = y'_e \) \((e \in E)\), (3.10) is also derived from Theorems 1, 2.

4. CONGRUENCES FOR TWO CLASS NUMBERS

In this section, applying Theorem 1 we obtain some congruence relations between the class numbers and units of the quadratic fields \( \mathbb{Q}(\sqrt{fm})^{1/2} \) and \( \mathbb{Q}(\sqrt{-fm})^{1/2} \) with \( f = 1, 2 \).

As in the previous section we take two multiplicative arithmetic functions \( \psi, \theta \) satisfying \( \psi(d) = \theta(d) = 1 \pmod{2} \) for any \( d \mid m \). In the following we let \( f = 1, 2 \).

Letting \( x_f = x_{-f} = -1, y_f = y_{-f} = 1 \), and the other coefficients be all zero in Theorem 1, we derive

\[
H_f^-(m, \psi, \theta) + H_{-f}(m, \psi, \theta) - H_f^+(m, \psi, \theta) - H_{-f}^+(m, \psi, \theta) \equiv 0 \\
\pmod{2^{r+3}}.
\]

(4.1)

When \( x_f = x_{-f} = y_f = y_{-f} = 1 \) and the other coefficients are all zero, Theorem 1 ensures the congruence

\[
H_f^-(m, \psi, \theta) + H_{-f}(m, \psi, \theta) + H_f^+(m, \psi, \theta) + H_{-f}^+(m, \psi, \theta) \equiv 0 \\
\pmod{2^{r+2}}.
\]

(4.2)

Theorem 1 also yields that

\[
H_f^\pm(m, \psi, \theta) + H_{-f}^\pm(m, \psi, \theta) \equiv 0 \pmod{2^{r-1}}.
\]

(4.3)

Using (4.3) in the case that \( \theta(d) = 1 \) for every \( d \mid m \), one can show by induction on \( r \) that

\[
H(-fm) \equiv H(fm) \equiv 0 \pmod{2^{r+3}},
\]

(4.4)

where \( \delta = 1 \) or 0 according as every prime \( p \mid m \) satisfies \( p \equiv \pm 1 \pmod{8} \) or not, because \( 1 - (-f/p) p \equiv 0 \pmod{8} \), \( \log p \equiv 0 \pmod{8} \), and \( 1 - (2/p) = 0 \) for any prime \( p \equiv \pm 1 \pmod{8} \).
We apply (4.1) and (4.2) to the case \( r = 1 \). Let \( p \) be an odd prime and \( \psi(p) = \theta(p) = 1 \). Appealing Lemma 5 we have

\[
H_1^- (p) + H_{-1}^-(p) = H(-p) + H(-1) \left( 1 - \left( -\frac{1}{p} \right) p \right),
\]

\[
H_2^- (p) + H_{-2}^-(p) = H(-2p) + H(-2) \left( 1 - \left( -\frac{2}{p} \right) p \right),
\]

\[
H_1^+ (p) + H_{-1}^+ (p) = H(p) + \frac{\log p}{2},
\]

\[
H_2^+ (p) + H_{-2}^+ (p) = H(2p) + H(2) \left( 1 - \left( \frac{2}{p} \right) \right)
\]

with \( H_r^+ (p) = H_r^+ (p, \psi, \theta) \ (e \in E) \). We recall \( H(2) \equiv 19 \ (\text{mod } 32) \) and compute

\[
\log p - \log \left\{ 1 + \left( \left( -\frac{1}{p} \right) p - 1 \right) \right\}
\]

\[
\equiv \left( \left( -\frac{1}{p} \right) p - 1 \right) - \frac{1}{2} \left( \left( -\frac{1}{p} \right) p - 1 \right)^2 \quad (\text{mod } 32)
\]

\[
\equiv -\frac{1}{2} \left( p - \left( -\frac{1}{p} \right) \right) \left( p - 3 \left( -\frac{1}{p} \right) \right) \quad (\text{mod } 32).
\]

Therefore (4.1) and (4.2) lead to the following result.

**Theorem 3.** Let \( p \) be an odd prime. Then

(i) \( H(-p) - H(p) \equiv \frac{1}{4} \left( p - \left( \frac{-1}{p} \right) \right) \left( p - 5 \left( \frac{-1}{p} \right) \right) \) \ (mod 16),

(ii) \( H(-p) + H(p) \equiv \frac{1}{4} \left( p - \left( \frac{-1}{p} \right) \right)^2 \) \ (mod 8),

(iii) \( H(-2p) - H(2p) \equiv \left( \frac{2}{p} \right) \left( \left( \frac{-1}{p} \right) p - 3 \right) + 2 \) \ (mod 16),

(iv) \( H(-2p) + H(2p) \equiv \left( \frac{2}{p} \right) \left( \left( \frac{-1}{p} \right) p + 3 \right) + 4 \) \ (mod 8).

From now on, for simplicity we suppose \( \psi(d) = \theta(d) = 1 \) for every \( d | m \).
From the definition (3.3) it is seen that for any \( e \in E \)

\[
H^\pm_e(m, \psi, \theta) = H^\pm_e(m, \psi).
\]

The assertion for \( f = 2 \) in the following lemma is equivalent to Hikita's result [4, Lemmas 5, 6].

**Lemma 9.** Let \( \omega \) be a multiplicative arithmetic function such that \( \omega(d) \equiv 1 \pmod{2} \) for any divisor \( d \) of \( m \), and assume that every prime \( p \) dividing \( m \) satisfies \( p \equiv 1 \pmod{4} \).

(i) For any divisor \( c > 1 \) of \( m \),

\[
H_f^+(c, \psi) + H_f^+(c, \psi\omega) \\
\equiv \sum_{p | c} (1 - \omega(p))\{H_f^+(c/p, \psi) + H_f^+(c/p, \psi\chi_p)\} \quad \text{(mod } 2^{r(c)+2}\text{) if } r(c) > 1,
\]

\[
= (1 - \omega(c))(1 - \chi_c(2)) \quad \text{(mod } 8\text{) if } r(c) = 1.
\]

(ii) When \( r > 1 \), \( H_f^+(m, \psi) + H_f^+(m, \psi\chi_2) \equiv 0 \pmod{2^{r+2}} \).

**Proof.** By simple computation we get

\[
F_{c,\psi}(b) + F_{c,\psi\omega}(b) \\
\equiv \prod_{p | c} (S_p\chi_p(b)\psi(p) - 1) \\
\quad + \prod_{p | c} \{(S_p\chi_p(b)\psi(p) - 1) + (1 - \omega(p))\} \quad \text{(mod } 2^{r(c)+1}\text{)}
\]

\[
\equiv \sum_{1 < s | c} \sum_{b = 1}^{c'} F_{c/s,\psi}(b) \prod_{p | s} (1 - \omega(p)) \quad \text{(mod } 2^{r(c)+1}\text{)}
\]

for any \( b \in \mathbb{Z}, \ (b, c) = 1 \), where \( S_p = S(\chi_p, \zeta_p)/p \). By Lemma 7 we have \( K_f^+(\zeta_c^b) + K_{-f}(\zeta_c^b) \equiv 0 \pmod{2} \). Hence

\[
H_f^+(c, \psi) + H_{-f}^+(c, \psi) + H_f^+(c, \psi\omega) + H_{-f}^+(c, \psi\omega) \\
= \sum_{b = 1}^{c'} (F_{c,\psi}(b) + F_{c,\psi\omega}(b))(K_f^+(\zeta_c^b) + K_{-f}(\zeta_c^b))
\]

\[
\equiv \sum_{1 < s | c} \sum_{b = 1}^{c'} F_{c/s,\psi}(b)(K_f^+(\zeta_s^b) + K_{-f}(\zeta_s^b)) \prod_{p | s} (1 - \omega(p)) \quad \text{(mod } 2^{r(c)+2}\text{)}.
\]
Since $p \equiv 1 \pmod{4}$ for any prime $p|m$, it follows from Lemma 5 that $H^+_f(c, \psi) = H^+_f(c, \psi \omega) = 0$. As was seen in the proof of Lemma 5,

$$
\sum_{b=1}^{c} F_{c/p, \psi}(b)(K^+_f(\zeta_c^b) + K^-_f(\zeta_c^b)) = \mu(s) \sum_{1 < d \mid c/s} \psi(d) H(d) \prod_{p \mid c/d} (1 - \chi_d(p)) + J(c) \quad \text{when } f = 1,
$$

$$
= \mu(s) \sum_{0 < d \mid c/s} \psi(d) H(2d) \prod_{p \mid c/d} (1 - \chi_{2d}(p)) \quad \text{when } f = 2,
$$

where $J(c) = (\log c)/2$ or $J(c) = 0$ according as $r(c) = 1$ or $r(c) > 1$.

Applying this formula, by (4.4) we obtain

$$
\sum_{b=1}^{c} F_{c/p, \psi}(b)(K^+_f(\zeta_c^b) + K^-_f(\zeta_c^b)) \equiv 0 \pmod{2^{(c)}}.
$$

This implies that

$$
H^+_f(c, \psi) + H^+_f(c, \psi \omega) \equiv \sum_{p \mid c} (1 - \omega(p)) \sum_{b=1}^{c} F_{c/p, \psi}(b)(K^+_f(\zeta_c^b) + K^-_f(\zeta_c^b)) \pmod{2^{(c) + 2}}.
$$

When $r(c) > 1$, we compute

$$
\sum_{b=1}^{c} F_{c/p, \psi}(b)(K^+_f(\zeta_c^b) + K^-_f(\zeta_c^b)) \equiv \sum_{b=1}^{c/p} \left\{ \pm (K^+_f(\zeta_c^b) + K^-_f(\zeta_c^b)) - (K^+_f(\zeta_c^b) + K^-_f(\zeta_c^b)) \right\} \pmod{2^{(c) + 1}}.
$$

$$
\equiv H^+_f(c/p, \psi \chi_p) + H^+_f(c/p, \psi \chi_p) \pmod{2^{(c) + 1}}.
$$
To obtain the last congruence we have recalled (4.3) and the fact that $H_\pm^+(c/p, \psi) = H_\pm^+(c/p, \psi\chi_p) = 0$. In the case $r(c) = 1$, one has

$$H_\mp^+(c, \psi) + H_\mp^+(c, \psi\omega) \equiv (1 - \omega(c)) \sum_{b=1}^r (K_\mp^+(\zeta_b^h) + K_\mp^+(\zeta_b^{-h}))$$

$$\equiv (1 - \omega(c)) J_r(c) \pmod{8},$$

where $J_1(c) = (\log c)/2$ and $J_2(c) = 1 - \chi_2(c)$. It is obvious that $J_r(c) \equiv 1 - \chi_r(2) \pmod{4}$. Hence (i) has been proved.

We next see from (i) that

$$H_\mp^+(m, \psi) + H_\mp^+(m, \psi\chi_2) \equiv \sum_{(p_1, \ldots, p_r)} \Omega(p_1, \ldots, p_r) \pmod{2^{r+2}}$$

with

$$\Omega(p_1, \ldots, p_r) = (1 - \chi_2(p_1))(1 - \chi_2(2)) \prod_{i=1}^{r-1} (1 - \chi_2(p_{i+1})), $$

where the sum is taken over all $r$-tuples $(p_1, \ldots, p_r)$ of distinct prime divisors of $m = p_1 \cdots p_r$. By the quadratic reciprocity law we get $\Omega(p_1, \ldots, p_r) = \Omega(p_r, \ldots, p_1)$. This shows that

$$H_\mp^+(m, \psi) + H_\mp^+(m, \psi\chi_2) \equiv 2 \sum_{(p_1, \ldots, p_r)} \Omega(p_1, \ldots, p_r) \equiv 0 \pmod{2^{r+2}}.$$

Thus the proof is complete.

Let $\lambda$ be a multiplicative arithmetic function such that $\lambda(d) = d^{-1}$ for any $d|m$. Clearly $\lambda(1) = 1$ and $\lambda(2) = 0$ according as $d \equiv \pm 1 \pmod{8}$ or not. Observing (4.4) we therefore obtain

$$H_\mp^+(m, \psi\lambda^{-1}\chi_{-1}) \equiv H_\mp^+(m, \psi) \pmod{2^{r+2}},$$

for any $e \in E$. We put

$$\Phi(d) = \Phi_\lambda(d).$$

Then

$$\Phi(d) \equiv 0 \pmod{2^{2r(d) + \gamma}} \pmod{2^{r+3}}$$

if $d|m$, where $\gamma$ denotes the number of prime divisors $q$ of $d$ satisfying $q \equiv \pm 1 \pmod{8}$. By (4.3), $H_\mp^+(c, \psi) + H_\mp^+(c, \psi\omega) \equiv 0 \pmod{2^{r(c) + 1}}$ for any $c|m$. Hence we see from (3.3) that

$$H_\mp^+(m, \psi, \lambda\chi_{-1}) + H_\mp^-(m, \psi, \lambda\chi_{-1})$$

$$\equiv H_\mp^-(m, \psi\lambda^{-1}\chi_{-1}) + H_\mp^-(m, \psi\lambda^{-1}\chi_{-1})$$

$$\equiv H_\mp^-(m, \psi) + H_\mp^-(m, \psi) \pmod{2^{r+2}}.$$
Theorem 4. Let $m > 2$ be an odd, square-free, rational integer having $r$ prime divisors and let $f = 1, 2$.

(i) We have

$$H(-fm) \equiv \pm(fm) \pmod{2^{r+1} + \delta},$$

where $\delta = 1$ or $0$ according as any prime $p$ dividing $m$ satisfies $p \equiv \pm 1 \pmod{8}$ or not.

(ii) If there is a prime divisor $q \equiv 5 \pmod{8}$ of $m$ and if $p \equiv 1 \pmod{8}$ for any prime $p$ dividing $m/q$, then

$$H(-m) \equiv H(m) \pmod{2^{r+2}}.$$

(iii) If $p \equiv 1 \pmod{4}$ for any prime $p$ dividing $m$, then

$$H(-2m) \equiv -\left(\frac{2}{m}\right)H(2m) \pmod{2^{r+2}}.$$

(iv) If $p \equiv \pm 1 \pmod{16}$ for any prime $p$ dividing $m$, then

$$H(-fm) \equiv H(fm) \pmod{2^{r+3}}.$$

Proof. We prove all the assertions in the theorem by induction on $r$. Let $p$ be an odd prime. It follows from Theorem 3 that

$$H(-fp) \equiv H(fp) \pmod{8},$$

$$H(-fp) + H(fp) \equiv 0 \pmod{8} \quad \text{if} \quad p \equiv \pm 1 \pmod{8},$$

$$\equiv 4 \pmod{8} \quad \text{if} \quad p \equiv \pm 3 \pmod{8},$$

$$H(-fp) \equiv H(fp) \pmod{16} \quad \text{if} \quad p \equiv \pm 1 \pmod{16}.$$

Hence the assertions are true in the case $r = 1$. Suppose $r \geq 2$ in the following. Combining (4.1) and (4.2) with (4.6) we have

$$H_f(m, \psi, \lambda \chi_{-1}) + H_{-f}(m, \psi, \lambda \chi_{-1}) \pm (H_f^+(m, \psi) + H_{-f}^-(m, \psi)) \equiv 0 \pmod{2^{r+2}}.$$

On the other hand Lemma 5 enables us to describe

$$H_f(m, \psi, \lambda \chi_{-1}) + H_{-f}(m, \psi, \lambda \chi_{-1}) \pm (H_f^+(m, \psi) + H_{-f}^-(m, \psi))$$

$$= -\frac{1}{2} \Phi(m) + \sum_{1 < d | m} (H(-d) \pm H(d)) \prod_{p | m/d} \left(1 - \left(\frac{d}{p}\right)\right) \quad \text{if} \quad f = 1,$$

$$= -\Phi(m) + \sum_{0 < d | m} (H(-2d) \pm H(2d)) \prod_{p | m/d} \left(1 - \left(\frac{2d}{p}\right)\right) \quad \text{if} \quad f = 2.$$
It is seen from (4.5) that $\Phi(m) \equiv 0 \pmod{2^{r+2}}$ and $\Phi(m)/2 \equiv 0 \pmod{2^{r+2}}$ if $p \equiv \pm 1 \pmod{8}$ for any prime $p \mid m$. Further $H(-2) \pm H(2) \equiv 0 \pmod{2}$ and $1 - (2/p) = 0$ for any prime $p \equiv \pm 1 \pmod{8}$. Hence by the inductive hypothesis we derive (i).

We next assume that every prime divisor $p$ of $m$ satisfies $p \equiv 1 \pmod{4}$. Applying (4.1), (4.6), and Lemma 9 we get

$$H_f(m, \psi, \lambda_{-1}) + H_f^+(m, \psi_{-1}) \equiv 0 \pmod{2^{r+2}}.$$
with $T$, $U$, $t$, $u \in \mathbb{Z}$, where $g = 3$ if $m \equiv 5 \pmod{8}$ and $t_0 \equiv u_0 \equiv 1 \pmod{2}$, and $g = 1$ otherwise. It is easy to check that

$$
T = t_0/2, \quad U = u_0/2 \quad \text{if } g = 1,
$$

$$
T = t_0(t_0^2 - 3N(e(m))) / 2, \quad U = u_0(t_0^2 - N(e(m))) / 2 \quad \text{if } g = 3.
$$

By Gauss' genus theory one knows that

$$
h(fm) \equiv 0 \pmod{2^r-2} \quad \text{if } f = 1, m \equiv 1 \pmod{4}, \text{ and } r \geq 2,
$$

$$
\equiv 0 \pmod{2^r-1} \quad \text{otherwise.} \quad (4.8)
$$

When $p \equiv 1 \pmod{4}$ for any prime $p$ dividing $m$, we can write $fm = a^2 + b^2$ with $a, b \in \mathbb{Z}, (a, b) = 1$. Since $a^2 - fm = -b^2$, there is an ideal $A$ of $K$ such that $A^2 = (a + (fm)^{1/2})$. If $N(e(fm)) = 1$ then the order of the narrow ideal class represented by $A$ is 4 because $N(a + (fm)^{1/2}) = -b^2$ is negative. Hence, in this case, it is seen by Gauss' genus theory (cf. [3, Chap. 26.8]) that

$$
h(m) \equiv 0 \pmod{2^{r-1}}, \quad h(2m) \equiv 0 \pmod{2^r}. \quad (4.9)
$$

It is known that (4.9) is always true when $N(e(fm)) = -1$.

We first suppose $m \equiv 1 \pmod{4}$. If $N(\eta(m)) = T^2 - U^2m = 1$ then $T$ is odd and $U \equiv 0 \pmod{4}$ and

$$
\log \eta(m) = \frac{1}{2} \log (T^2 + U^2m + 2TUm^{1/2})
$$

$$
= \frac{1}{2} \log (1 + 2U(Um + Tm^{1/2}))
$$

$$
\equiv U(Um + Tm^{1/2}) - U^2(Um + Tm^{1/2})^2 \pmod{32}
$$

$$
\equiv TU^{1/2} \pmod{32}.
$$

In the case $N(\eta(m)) = -1$, using $T \equiv U + 1 \equiv 0 \pmod{2}$ we compute

$$
\log \eta(m) = \frac{1}{2} \log (1 + 2T(T + Um^{1/2}))
$$

$$
\equiv T(T + Um^{1/2}) - T^2(T + Um^{1/2})^2 \pmod{16}
$$

$$
\equiv TU^{1/2} \pmod{16}.
$$

Therefore by (4.8) and (4.9) we have

$$
H(m) = \left(2 - \left(\frac{2}{m}\right)\right)h(m) \frac{\log \epsilon(m)}{m^{1/2}}
$$

$$
\equiv \left(2 - \left(\frac{2}{m}\right)\right)gTU^{1/2}h(m) \pmod{2^{r-3}}.
$$
This presents the congruence \( H(m) \equiv \pm TUh(m) \pmod{2^{r+2}} \) because 
\( TUh(m) \equiv 0 \pmod{2^r} \).

We next suppose \( m \equiv -1 \pmod{4} \). One knows \( N(\varepsilon(m)) = 1 \). If 
\( T \equiv 1 \pmod{2} \), then \( U \equiv 0 \pmod{4} \) and, as in the previous case, 
\( \log \varepsilon(m) \equiv TUm^{1/2} \pmod{32} \). When \( T \equiv U + 1 \equiv 0 \pmod{2} \), we get 
\[
\log \varepsilon(m) = \frac{1}{2} \log(-\varepsilon(m)^2) 
= \frac{1}{2} \log(1 - 2T(T + Um^{1/2})) \equiv - TUm^{1/2} \quad \pmod{16}.
\]
The above computation and (4.8) imply that 
\[
H(m) = h(m) \frac{\log \varepsilon(m)}{m^{1/2}} \equiv (-1)^U TUh(m) \quad \pmod{2^{r+3}}.
\]

Regarding the unit \( \varepsilon(2m) = t + u(2m)^{1/2} \) it is seen that \( t \) is odd and \( u \) is even 
or odd according as \( N(\varepsilon(2m)) = 1 \) or \(-1\). Put \( M = 2mu + t(2m)^{1/2} \). If \n\( N(\varepsilon(2m)) = 1 \) then 
\[
\log \varepsilon(2m) = \frac{1}{2} \log(1 + 2uM) \equiv uM - u^2M^2 
\equiv tu(2m)^{1/2} \quad \pmod{16(2m)^{1/2}}.
\]
In the case \( N(\varepsilon(2m)) = -1 \), observing \( m \equiv 1 \pmod{4} \) we compute 
\[
\log \varepsilon(2m) = \frac{1}{2} \log(1 - 2uM) \equiv -(uM + u^2M^2 + 2u^4M^4) \pmod{8(2m)^{1/2}}
\equiv -(tu + 4mtu^3)(2m)^{1/2} 
\equiv 2mu^2(1 + 2mu^2 + t^2 + 4mu^2t^4) \pmod{8(2m)^{1/2}}
\equiv -(tu + 4)(2m)^{1/2} \quad \pmod{8(2m)^{1/2}}.
\]
Thus from (4.8) and (4.9) we obtain 
\[
H(2m) = h(2m) \frac{\log \varepsilon(2m)}{(2m)^{1/2}} 
\equiv tuh(2m) \quad \pmod{2^{r+3}} \quad \text{if} \quad N(\varepsilon(2m)) = 1,
\equiv -(tu + 4) h(2m) \quad \pmod{2^{r+3}} \quad \text{if} \quad N(\varepsilon(2m)) = -1.
\]
Remark that if \( N(\varepsilon(2m)) = -1 \) then \( H(2m) \equiv -tuh(2m) \pmod{2^{r+2}} \) by (4.9). In the case that \( p \equiv \pm 1 \pmod{8} \) for any prime \( p \mid m \), we see from (4.4) that 
\( H(2m) \equiv 0 \pmod{2^{r+1}} \). Therefore, in this case, if \( N(\varepsilon(2m)) = -1 \) then 
\( h(2m) \equiv 0 \pmod{2^{r+1}} \) and hence \( H(2m) \equiv -tuh(2m) \pmod{2^{r+3}} \).
For any prime \( p \equiv 1 \pmod{4} \) we know that \( N(\varepsilon(p)) = -1 \) and that \( N(\varepsilon(2p)) = -1 \) if \( p \equiv 5 \pmod{8} \).

Applying the above computation and discussion to Theorems 3, 4 we deduce the following results.

**Corollary 1.** Let \( T, U, t, u, g \) be as in (4.7) and let \( m = p \) be a prime. Put \( \varepsilon = \varepsilon(2p) \).

(i) If \( p \equiv 1 \pmod{8} \) then
\[
\begin{align*}
&h(-p) \equiv TUh(p) + (p - 1) \pmod{16}, \\
&h(-2p) \equiv N(\varepsilon) tuh(2p) + (p - 1) \pmod{16}.
\end{align*}
\]

(ii) If \( p \equiv 3 \pmod{8} \) then
\[
\begin{align*}
&2h(-p) \equiv (-1)^U TUh(p) + (p + 5) \pmod{16}, \\
&h(-2p) \equiv tuh(2p) + (p + 5) \pmod{16}.
\end{align*}
\]

(iii) If \( p \equiv 5 \pmod{8} \) then
\[
\begin{align*}
&h(-p) \equiv 3g TUh(p) + (p - 5) \pmod{16}, \\
&h(-2p) \equiv -(tu + 4) h(2p) + (p - 5) \pmod{16}.
\end{align*}
\]

(iv) If \( p \equiv 7 \pmod{8} \) then
\[
\begin{align*}
&TUh(p) \equiv p + 1 \pmod{16}, \\
&h(-2p) \equiv tuh(2p) + (p + 1) \pmod{16}.
\end{align*}
\]

**Corollary 2.** Let \( T, U, t, u, g \) be as in (4.7), and put \( \varepsilon = \varepsilon(2m) \).

(i) We have
\[
\begin{align*}
&h(-m) \equiv \pm TUh(m) \pmod{2^{r+1} + \delta} \quad \text{if } m \equiv 1 \pmod{4}, \\
&(1 - \left(\frac{2}{m}\right)) h(-m) \equiv \pm TUh(m) \pmod{2^{r+1} + \delta} \quad \text{if } m \equiv -1 \pmod{4}, \\
&h(-2m) \equiv \pm tuh(2m) \pmod{2^{r+1} + \delta},
\end{align*}
\]

where \( \delta = 1 \) or 0 according as every prime \( p \) dividing \( m \) satisfies \( p \equiv \pm 1 \pmod{8} \) or not.

(ii) If there is a prime divisor \( q \equiv 5 \pmod{8} \) of \( m \) and if \( p \equiv 1 \pmod{8} \) for any prime \( p \) dividing \( m/q \), then
\[
\begin{align*}
h(-m) &\equiv -g TUh(m) \pmod{2^{r+2}}.
\end{align*}
\]
(iii) If $p \equiv 1 \pmod{4}$ for any prime $p$ dividing $m$ then
\[ h(-2m) \equiv -\left( \frac{2}{m} \right) N(\epsilon) tuh(2m) \pmod{2^{r+2}}. \]

(iv) If $p \equiv \pm 1 \pmod{16}$ for any prime $p$ dividing $m$, then
\[ \left( 1 + \left( \frac{-1}{m} \right) \right) h(-m)/2 \equiv TUh(m) \pmod{2^{r+3}}, \]
\[ h(-2m) \equiv N(\epsilon) tuh(2m) \pmod{2^{r+3}}. \]

In the rest of this section we relate our congruences in Corollaries 1, 2 to known ones. We first assume that $p \equiv 1 \pmod{8}$ is a prime. Williams [13] proved that
\[ h(-p) \equiv T + (p - 1) \pmod{16} \]

\[ \equiv T + (p - 1) + 4(h(p) - 1) \pmod{16} \]

(4.10)

Kaplan and Williams obtained (cf. [5, 6]) that
\[ h(-2p) + \frac{S}{2} h^+(2p) + (p - 1) \equiv 0 \pmod{16}, \]
(4.11)

where $S = u$ if $N(\epsilon(2p)) = 1$, $S = 2tu$ if $N(\epsilon(2p)) = -1$, and $h^+(2p)$ is the class number of $\mathbb{Q}(\sqrt{2p})$ in the narrow sense. We can reprove (4.10), (4.11) from Corollary 1 (i). In fact, since $N(\epsilon(p)) = T^2 - U^2 p = -1$, it holds that $T \equiv 0 \pmod{4}$ and $U \equiv 1 \pmod{4}$. Hence
\[ h(-p) \equiv TUh(p) + (p - 1) \equiv T + (p - 1) + T(h(p) - 1) \pmod{16}, \]
from which (4.10) is derived. In order to show (4.11) it suffices to verify $Sh^+(2p)/2 \equiv -N(\epsilon(2p)) tuh(2p) \pmod{16}$. By (4.9) we have $h(2p) \equiv 0 \pmod{2}$. In the case $N(\epsilon(2p)) = 1$, one knows $h(2p) = h^+(2p)/2$ and $t + 1 = u \equiv 0 \pmod{2}$. Suppose $u \equiv 2 \pmod{4}$. Then $t^2 - 1 = 2pu^2$ implies that
\[ t = \frac{1}{2} \left( (t - 1) + (t + 1) \right) \}
\[ = \frac{1}{2} \{ 4p^2 w^2 + 2p^1 - \delta (u/2w)^2 \} \equiv -1 \pmod{4} \]
with $w \in \mathbb{Z}$, $w | u/2$ and $\delta = 0, 1$. Thus it holds that either $t \equiv -1 \pmod{4}$ or $u \equiv 0 \pmod{4}$. This gives $uh^+(2p)/2 \equiv -tuh(2p) \pmod{16}$. When $N(\epsilon(2p)) = -1$, one has $Sh^+(2p)/2 = tuh(2p)$ because $h^+(2p) = h(2p)$.

For a prime $p \equiv 5 \pmod{8}$ it was proved (cf. [5, 7]) that
\[ h(-p) \equiv 3Th(p)/g \pmod{16}, \]
(4.12)
\[ h(-2p) \equiv 2(u - 1) + 3th(2p) + (p - 5) \pmod{16}. \]
(4.13)
We assert that our results give another proofs of (4.12), (4.13). From $N(\epsilon(2p)) = -1$ we see that $T \equiv 2 \pmod{4}$, $U \equiv 1 \pmod{2}$, and

$$p - 5 \equiv (1 - U^2) p \equiv 1 - U^2 \pmod{16}.$$  

Every prime dividing $U$ is congruent to 1 modulo 4 because $pU^2 = T^2 + 1$. Hence $U \equiv 1 \pmod{4}$. Observing $h(p) \equiv 1 \pmod{2}$ we compute

$$3gTUh(p) + (p - 5)$$

$$= 3gTh(p) + T(1 - U) + (1 - U^2) \equiv 3Th(p)/g \pmod{16}.$$  

Thus Corollary 1 (iii) proves (4.12). Since $N(\epsilon(2p)) = -1$, we know $t \equiv u \equiv 1 \pmod{2}$. Moreover $2pu^2 = t^2 + 1$ implies $u \equiv 1 \pmod{4}$. By (4.3) we also see that

$$H_2^+(p, \psi, \theta) + H_2^+(p, \psi, \theta) \equiv -tu(h(2p) + \left(1 - \left(\frac{2}{p}\right)\right)) \equiv 0 \pmod{4},$$

which leads to $h(2p) \equiv 2 \pmod{4}$. Hence

$$-(tu + 4)h(2p) \equiv \{3t + (u - 1) - (t + 1)(u + 3)\} h(2p)$$

$$\equiv 2(u - 1) + 3th(2p) \pmod{16}$$

and (4.13) is deduced from Corollary 1 (iii).

To describe a result of Lang and Schertz [11] we need a few more definitions. We put $e_2 = 1$ if $N(\epsilon(2m)) = 1$ and $e_2 = 2$ if $N(\epsilon(2m)) = -1$, and write $\epsilon(2m)^{e_2} = (u_2 + 2v_2(8m)^{1/2})/2$ with $u_2, v_2$ in $\mathbb{Z}$. In the case $m \equiv 1 \pmod{4}$ we define $e_4 = g$ if $N(\epsilon(m)) = 1$ and $e_4 = 2g$ if $N(\epsilon(m)) = -1$, and write $\epsilon(m)^{e_4} = (u_4 + 4v_4m^{1/2})/2$ with $u_4, v_4$ in $\mathbb{Z}$. For each $k = 2, 4$ we define the rational integer $\rho(u_k, v_k)$ by

$$\rho(u_k, v_k) = 2 \left\{ \left(\frac{u_k/2}{v_k}\right) - 1 \right\} + v_k(u_k - 3)$$

if $v_k \equiv 1 \pmod{2}$,

$$= 2 \left\{ \left(\frac{v_k}{u_k/2}\right) - 1 \right\}$$

$$+ \frac{1}{2} u_kv_k \left(\frac{k^2D(fm)}{4} - 1\right) + \frac{3}{2} (u_k - 2)$$

if $v_k \equiv 0 \pmod{2}$,

where $f = 2$ if $k = 2$ and $f = 1$ if $k = 4$, and $D(fm)$ means the discriminant of $\mathbb{Q}((fm)^{1/2})$. It was proved [11, Satz (3.4)] that

$$3h(-2m) \equiv h(2m)(2/e_2) \rho(u_2, v_2) \pmod{2^{e_2 + 1}},$$

(4.14)
and if \( m \equiv 1 \pmod{4} \) then
\[
3h(-m) \equiv h(m) \frac{2(2 - (2/m))}{e_4} \rho(u_4, v_4) \pmod{2^{\tau(r)}}, \tag{4.15}
\]
where \( \tau(r) = \max(3, r + 1) \) or \( \tau(r) = r \) according as any prime \( p \) dividing \( m \) is congruent to 1 modulo 4 or not. We claim that (4.14) is equivalent to our congruence \( h(-2m) \equiv tuh(2m) \pmod{2^{r+1}} \) in Corollary 2 (i). It suffices to verify (2/e_4) \( \rho(u_2, v_2) \equiv - tu \pmod{4} \) because \( h(-2m) \equiv h(2m) \equiv 0 \pmod{2^{r-1}} \). In the case \( N(\varepsilon(2m)) = 1 \), since \( t + 1 \equiv u \equiv 0 \pmod{2} \), \( u_2 - 2t \), and \( v_2 = u/2 \), it is seen that \( 2\rho(u_2, v_2) \equiv - tu \pmod{4} \). When \( N(\varepsilon(2m)) = -1 \), one has \( t \equiv u \equiv 1 \pmod{2} \), \( u_2 = 2(t^2 + 2u^2m) \), and \( v_2 = tu \). Hence \( \rho(u_2, v_2) = tu(u_2 - 3) \equiv tu \pmod{4} \). This proves our claim. Next let \( m \equiv 1 \pmod{4} \). We first exclude the case \( r = 1 \). If \( N(\varepsilon(m)) = 1 \) then \( U \equiv 0 \pmod{4} \), \( u_4 = 2T \), and \( v_4 = U/2 \). If \( N(\varepsilon(m)) = -1 \) then \( T \equiv 0 \pmod{2} \), \( u_4 = 2(T^2 + U^2m) \), and \( v_4 = TU \). In any case we compute (2/e_4) \( \rho(u_4, v_4) \equiv -TU \pmod{4} \). Thus, recalling that \( h(-m) \equiv 0 \pmod{2^{r-1}} \), \( h(m) \equiv 0 \pmod{2^{r-1}} \) when any prime dividing \( m \) is congruent to 1 modulo 4, we rewrite (4.15) as \( h(-m) \equiv TUh(m) \pmod{2^{r(r)}} \), which is contained in Corollary 2 (i). When \( m = p \equiv 1 \pmod{4} \) is a prime, it follows that \( N(\eta(p)) = T^2 - U^2p = -1 \). Therefore \( T \equiv 0 \pmod{2} \), \( U = 1 \pmod{4} \), and
\[
\left( \frac{u_4^2}{v_4} \right) = \left( \frac{T^2 + U^2m}{TU} \right) = \left( \frac{2T^2 + 1}{T} \right) \left( \frac{2U^2m - 1}{U} \right) = 1.
\]
This implies (2/e_4) \( \rho(u_4, v_4) \equiv TU\{2(T^2 + U^2m) - 3\}/g \equiv - gTU \pmod{8} \). Hence, in this case, (4.15) can be expressible as \( h(-p) \equiv -gTUh(p) \pmod{8} \), which is again deduced from Corollary 1 (i, iii) because \( T \equiv 0 \pmod{4} \) if \( p \equiv 1 \pmod{8} \). We note that Lang and Schertz also obtained a congruence between \( h(-m) \) and \( h(m) \) when \( m \equiv -1 \pmod{4} \) (cf. [11, Satz (3.4)]). However it seems to be impossible to derive this congruence from our results.

We now assume that \( p \equiv 1 \pmod{8} \) for any prime \( p \) dividing \( m \). It is seen that \( U \equiv 0 \pmod{4} \) if \( N(\varepsilon(m)) = 1 \) and \( T \equiv 0 \pmod{4} \) if \( N(\varepsilon(m)) = -1 \). By (4.9) and (i) in Corollary 2 we see
\[
h(-4m) \equiv Uh(m) \pmod{2^{r+2}} \quad \text{if} \quad N(\varepsilon(m)) = 1,
\]
\[
\equiv Th(m) \pmod{2^{r+2}} \quad \text{if} \quad N(\varepsilon(m)) = -1. \tag{4.16}
\]
On the other hand it was proved by Lang [10] that
\[
h(-4m) \equiv v(m)h(m) \pmod{2^{r+2}}, \tag{4.17}
\]
where \( v(m) = U + 2(T - 1) \) or \( T \) according as \( N(\varepsilon(m)) = 1 \) or 1.
Suppose \( N(\varepsilon(m)) = 1 \) and write \( U = 2^iV \) with \( i \geq 2 \), \( (2, V) = 1 \). Since \( (T + 1, T - 1) = 2 \) and \( T^2 - 1 = 2^iV^2m \), one has \( T + 1 = 2^iV^2m_1 \) and \( T - 1 = 2^iV_2m_2 \), where \( j, k, V_1, V_2, m_1, m_2 \in \mathbb{Z}, j + k = 2i \). \( V_1, V_2 = V \) and \( m_1m_2 = m \). Clearly either \( j = 1 \) or \( k = 1 \). Moreover from our assumption we see \( m_1 = m_2 \equiv 1 \pmod{8} \). This implies \( T \equiv 2 \pm 1 \pmod{8} \). Observing \( T^2 \equiv T^2 - U^2m \equiv 1 \pmod{16} \) we get \( T \equiv 1 \pmod{8} \). Consequently our congruence (4.16) coincides with (4.17).

We finally treat the congruence in Corollary 2 (iii). In the case \( N(\varepsilon) = 1 \), since \( u \equiv 0 \pmod{2} \) and \( h(2m) \equiv 0 \pmod{2^i} \), it holds that \( tuh(2m) \equiv -tuh(2m) \pmod{2^i+2} \). Hence the right-hand side of the congruence in Corollary 2 (iii) can be rewritten as \( (2/m) tuh(2m) \), and the assertion (iii) is therefore equivalent to Hikita's result \([4]\).

REFERENCES

5. P. Kaplan, Nouvelle démonstration d'une congruence modulo 16 entre les nombres de classes d'idéaux de \( \mathbb{Q}(\sqrt{-2p}) \) et \( \mathbb{Q}(\sqrt{2p}) \) pour \( p \) premier \( \equiv 1 \pmod{4} \), *Proc. Japan Acad. Ser. A. Math. Sci.* **57** (1981), 507–509.
6. P. Kaplan and K. S. Williams, On the class numbers of \( \mathbb{Q}(\sqrt{\pm 2p}) \) modulo 16, for \( p \equiv 1 \pmod{8} \) a prime, *Acta Arith.* **40** (1981/1982), 289–296.
7. P. Kaplan and K. S. Williams, 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, *Acta Arith.* **40** (1981/1982), 375–397.
13. K. S. Williams, On the class number of \( \mathbb{Q}(\sqrt{-p}) \) modulo 16, for \( p \equiv 1 \pmod{8} \) a prime, *Acta Arith.* **39** (1981), 381–398.