On the Congruences for the Class Numbers of the Quadratic Fields Whose Discriminants Are Divisible by 8

MITSUHIKO HIKITA

Department of Mathematics, Osaka University.
Toyonakku, Osaka 560, Japan

Communicated by H. Zassenhaus

Received August 23, 1983; revised July 10, 1984

We prove a congruence modulo a certain power of 2 for the class numbers of the quadratic fields whose discriminants are divisible by 8 and have no prime factor ( > 0) congruent to 3 modulo 4. Such a congruence enables us to obtain some information about the relations between the structures of the ideal class groups of those fields. Some of these can be rewritten with the use of Legendre symbols.

1. INTRODUCTION AND RESULTS

Let \( m > 0 \) be a squarefree odd rational integer. It is well known from the genus theory of the quadratic fields that if \( m \) has no prime factor \(( > 0)\) congruent to 3 modulo 4, then the 2-ranks of the ideal class groups of the real quadratic field \( \mathbb{Q}(\sqrt{2m}) \) and the imaginary quadratic field \( \mathbb{Q}(\sqrt{-2m}) \) are both equal to \( r \), the number of primes dividing \( m \), so that their class numbers \( h(2m) \) and \( h(-2m) \), respectively, are divisible by \( 2^r \). In this paper, it will be proved that \( h(2m) \) and \( h(-2m) \) are related to each other modulo \( 2^{r+2} \) through the fundamental unit of \( \mathbb{Q}(\sqrt{2m}) \).

For an odd rational integer \( n > 0 \), let \((a/n)\) denote the Legendre-Jacobi symbol, where \((a, n) = 1\).

The main result is the following.

THEOREM. Let \( m > 0 \) be a squarefree odd rational integer, having no prime factor \(( > 0)\) congruent to 3 modulo 4, and

\[ e = T + U \sqrt{2m} > 1 \]

\[ \sqrt{2m} > 1 \]

\[ 86 \]

Copyright © 1986 by Academic Press, Inc.
All rights of reproduction in any form reserved.
with $T$ and $U$ rational integers, be the fundamental units of the real quadratic field $\mathbb{Q}(\sqrt{2m})$. Then we have

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

where $r$ is the number of primes dividing $m$.

From the theorem, we obtain some relations between the structures of the ideal class groups of $\mathbb{Q}(\sqrt{\pm 2m})$. For a rational integer $n \geq 1$, let $r_2(\pm 2m)$ denote the $2^n$-rank of the ideal class group of $\mathbb{Q}(\sqrt{\pm 2m})$, respectively. Then, letting $N$ be the absolute norm, we obtain

**Corollary.**

(i) $r_4(-2m) = 0$, if and only if $r_4(2m) = 0$, $N(\varepsilon) = -1$.

(ii) $r_4(-2m) = 1$, $r_8(-2m) = 0$, if and only if (A) or (B).

(A) $r_4(2m) = 1$, $r_8(2m) = 0$, $N(\varepsilon) = -1$.

(B) $r_4(2m) = 0$, $N(\varepsilon) = +1$, $U \equiv 2 \pmod{4}$.

(iii) $r_4(-2m) \geq 2$ or $r_8(-2m) \geq 1$, if and only if (C) or (D) or (E).

(C) $r_4(2m) \geq 2$ or $r_8(2m) \geq 1$.

(D) $r_4(2m) = 1$, $r_8(2m) = 0$, $N(\varepsilon) = +1$.

(E) $r_4(2m) = 0$, $N(\varepsilon) = +1$, $U \equiv 0 \pmod{4}$.

It is remarked that if $r_4(-2m) = 0$ then, from the theorem, the odd parts of the class numbers $h(\pm 2m)$ are related to each other modulo 4 through $T$ and $U$. In fact, it is seen that $U \equiv 1 \pmod{4}$ in this case, so that $U$ may be omitted.

Let $a$ and $b$ be squarefree positive odd rational integers, such that $(a, b) = 1$. We define $\phi_{2b}^a$ by

$$\phi_{2b}^a = \prod_{p \mid a} \left( \left(1 - \left(\frac{2}{p}\right)\left(\frac{p}{b}\right)\right)/2 \right).$$

Clearly the value of $\phi_{2b}^a$ is 0 or 1. The condition $r_4(-2m) = 0$ can be written as follows.

**Proposition 1.** Putting $n_0 = m$, we have

$$h(-2m)/2^r \equiv \sum_{n_j \mid n_{j-1}} \phi_{2n_j}^{n_j/n_{j-1}} \phi_{2n_{j+1}}^{n_{j+1}/n_j} \cdots \phi_{2n_s}^{n_s/n_{s-1}} \pmod{2},$$

where the summation runs over all finite tuples $(n_0, n_1, \ldots, n_s)$ of rational integers such that $n_j \mid n_{j-1}$ and $0 < n_j < n_{j-1}$ for $j = 1, \ldots, s$. 


Putting together Corollary (i) and Proposition 1, it follows that

**Proposition 2.** Putting \( n_0 = m \), we have \( h(2m)/2' \equiv 1 \pmod{2} \) and \( N(\varepsilon) = -1 \), if and only if

\[
\sum_{n_1 \mid n_2 \mid \ldots \mid n_r} \phi_{n_1/n_2} \phi_{n_2/n_3} \cdots \phi_{n_{r-1}/n_r} \equiv 1 \pmod{2}.
\]

As a simple application of Proposition 2, we obtain

**Proposition 3.** Letting \( m = \prod_{j=1}^{r} p_j \) be the prime decomposition, we have

(i) If \( p_1 \equiv \cdots \equiv p_r \equiv 5 \pmod{8} \) and \( (p_i/p_j) = 1 \) for every \( i < j \), then \( h(2m)/2' \equiv 1 \pmod{2} \) and \( N(\varepsilon) = -1 \).

(ii) If \( p_1 \equiv \cdots \equiv p_r \equiv 5 \pmod{8} \), \( (p_i/p_j) = -1 \) for every \( i < j \), and \( r \equiv 0 \pmod{2} \), then \( h(2m)/2' \equiv 1 \pmod{2} \) and \( N(\varepsilon) = -1 \).

### 2. Preliminary Lemma

Let \( d \mid m \) be a positive rational integer, and \( \varepsilon_{2d} = T_d + U_d \sqrt{2d} > 1 \) be the fundamental unit of \( \mathbb{Q}(\sqrt{2d}) \), where \( T_d \) and \( U_d \) are rational integers. Let \( h^+(-2d) \) denote the narrow class number of \( \mathbb{Q}(\sqrt{-2d}) \), respectively, so that \( h^+(-2d) = h(2d) \) if \( N(\varepsilon_{2d}) = -1 \), and \( h^+(-2d) = 2h(2d) \) if \( N(\varepsilon_{2d}) = +1 \), and always \( h^+(-2d) = h(-2d) \). Let \( r(d) \) denote the number of primes dividing \( d \).

**Lemma 1.** Letting \( d \) divide \( m \) and \( d > 0 \), we have

\[ h(-2d) \equiv T_d U_d h(2d) \pmod{2^{r(d)+1}}. \]

**Proof.** It is known (e.g., [1, Chap. 26.8]) that the 2-Sylow subgroup of the ideal class group of \( \mathbb{Q}(\sqrt{-2d}) \) has rank \( r(d) \), and so does that of the narrow ideal class group. Hence \( h(\pm 2d) \equiv 0 \pmod{2^{r(d)}} \), and if \( N(\varepsilon_{2d}) = +1 \) then \( h^+(-2d) \equiv 0 \pmod{2^{r(d)+1}} \). Now, for a quadratic discriminant \( D \), let \( D = D_1 D_2 \) be a decomposition into two quadratic discriminants \( D_1 \) and \( D_2 \). Then, according to Rédéi–Reichardt [3], the decomposition \( D = D_1 D_2 \) is said to be properly of the second kind, if and only if \( (D_1/p) = 1 \) for every prime \( p \mid D_2 \), and \( (D_2/p) = 1 \) for every prime \( p \mid D_1 \), where \( (D/p) \) denotes the Kronecker symbol. From the result of [3], \( D = D_1 D_2 \) is properly of
the second kind, if and only if there exists a cyclic extension of degree 4 over \( Q(\sqrt{D}) \), being unramified at any finite prime divisor of \( Q(\sqrt{D}) \), and containing the field \( Q(\sqrt{D_1}, \sqrt{D_2}) \). To return to the proof, it is
easy to see that \( 8d = (8d_1) d_2 \) is properly of the second kind, if
and only if \( -8d = (-8d_1) d_2 \) is properly of the second kind. Hence
\( h^+(2d) \equiv 0 \pmod{2^{r(d)+1}} \), if and only if \( h(-2d) \equiv 0 \pmod{2^{r(d)+1}} \). That is,
\( h^+(2d) \equiv h(-2d) \pmod{2^{r(d)+1}} \). Therefore, noting that \( T_d \equiv 1 \pmod{2} \) and
\[
U_d \equiv \begin{cases} 1 \pmod{2} & \text{if } N(e_{2d}) = -1, \\ 0 \pmod{2} & \text{if } N(e_{2d}) = +1, \end{cases}
\]
the lemma is proved.

3. Modification of Dirichlet's Class Number Formula

For an odd prime \( p \), let \( \chi_p \) be the primitive Dirichlet character modulo \( p \) defined by
\[
\chi_p(a) = \begin{cases} \left( \frac{a}{p} \right) & \text{if } p \nmid a, \\ 0 & \text{if } p \mid a. \end{cases}
\]

Let \( \chi_2 \) and \( \chi_{-1} \) be the primitive Dirichlet characters modulo 8 and 4, respectively, defined by
\[
\chi_2(a) = \begin{cases} (-1)^{(a^2 - 1)/8} & \text{if } a \text{ is odd}, \\ 0 & \text{if } a \text{ is even}, \end{cases}
\]
\[
\chi_{-1}(a) = \begin{cases} (-1)^{(a - 1)/2} & \text{if } a \text{ is odd}, \\ 0 & \text{if } a \text{ is even}. \end{cases}
\]

For positive \( d \mid m \), let \( \chi_d \) and \( \chi_{2d} \) be the primitive Dirichlet characters modulo \( d \) and \( 8d \), respectively, defined by
\[
\chi_d(a) = \prod_{p \mid d} \chi_p(a), \quad \chi_{2d}(a) = \chi_2(a) \chi_d(a),
\]
and
\[
\chi_{-2d}(a) = \chi_{-1}(a) \chi_{2d}(a).
\]
From Dirichlet's class number formula for the quadratic fields (e.g., [2. Sects. 51, 52, Theorem 150]), we have

\[ \sum_{a \mod 8d} \chi_{2d}(a) \log(1 - \zeta_{8d}^a) = -2h(2d) \log(\varepsilon_{2d}), \]

and

\[ \sum_{a \mod 8d} \chi_{-2d}(a) \log(1 - \zeta_{8d}^a) = -h(-2d) \pi i, \]

where \( \zeta_n = e^{2\pi i/n} \) (\( n > 0 \)), and \( \log \) denotes the principal branch of the logarithm.

**Lemma 2.** Letting \( d \mid m \) and \( d > 0 \), we have

\[ \sum_{a \mod 8m, \ (a,8m) = 1} \chi_{2d}(a) \log(1 - \zeta_{8m}^a) = -\left( \prod_{p \mid m/d} (1 - \chi_{2d}(p)) \right) 2h(2d) \log(\varepsilon_{2d}), \]

and

\[ \sum_{a \mod 8m, \ (a,8m) = 1} \chi_{-2d}(a) \log(1 - \zeta_{8m}^a) = -\left( \prod_{p \mid m/d} (1 - \chi_{-2d}(p)) \right) h(-2d) \pi i. \]

**Proof.** Let \( p \) be a prime such that \( p \mid m/d \). Put \( m' = m/p \) and \( a = pa' + 8m'x \). If \( a' \) and \( x \) run over complete reduced systems of residues modulo \( 8m' \) and modulo \( p \), respectively, then \( a \) runs over a complete reduced system of residues modulo \( 8m \). Therefore

\[ \sum_{a \mod 8m, \ (a,8m) = 1} \chi_{2d}(a) \log(1 - \zeta_{8m}^a) \]

\[ = - \sum_{a \mod 8m, \ (a,8m) = 1} \chi_{2d}(a) \sum_{n=1}^{\infty} \frac{1}{n} \zeta_{8m}^{an} \]

\[ = - \sum_{a' \mod 8m', \ (a',8m') = 1} \sum_{n=1}^{\infty} \chi_{2d}(pa') \frac{\chi_{8m'}(a')}{n} \sum_{x \mod p, \ (x,p) = 1} \zeta_{p}^{nx}, \]

where, noting

\[ \zeta_{p}^{nx} = \begin{cases} -1 & \text{if } p \mid n, \\ p-1 & \text{if } p \nmid n. \end{cases} \]
CONGRUENCES FOR CLASS NUMBERS

the rearrangement of the formula continues as follows

\[
- \sum_{a' \mod 8m' \atop (a', 8m') = 1} \left( \sum_{n=1}^{\infty} \frac{\chi_{2d}(p^a)}{n^m} \zeta_{8m}^{a'n} (-1) + \sum_{n=1}^{\infty} \frac{\chi_{2d}(p^a)}{pn} \zeta_{8m'}^{a'n} (p) \right) = -(-\chi_{2d}(p) + 1) \sum_{a' \mod 8m' \atop (a', 8m') = 1} \chi_{2d}(a') \zeta_{8m}^{a'} (1 - \zeta_{8m}^{a'})
\]

where every interchange of summation is guaranteed by Abel’s continuity theorem (e.g., [4, Sect. 3.7]). Therefore, by the induction on \( r \) and the class number formula, we get the first formula. The second formula is proved in exactly the same way.

Letting \( m = \prod_{j=1}^{r} p_j \) be the prime decomposition, we see

\[
- \sum_{a \mod 8m \atop (a, 8m) = 1} \chi_{2d}(a) (1 - \chi_{-1}(a)) \left( \prod_{j=1}^{r} (1 + \chi_{p_j}(a)) \right) \log(1 - \zeta_{8m}^{a})
\]

- \[
\sum_{d \mid m \atop (a, 8m) = 1} \chi_{2d}(a) \log(1 - \zeta_{8m}^{a})
\]

- \[
\sum_{a \mod 8m \atop (a, 8m) = 1} \chi_{-2d}(a) \log(1 - \zeta_{8m}^{a})
\]

Here, observing

\[
(1 - \chi_{-1}(a)) \left( \prod_{j=1}^{r} (1 + \chi_{p_j}(a)) \right) = \begin{cases} 
2^{r+1} & \text{if } \chi_{-1}(a) = -1, \text{ and } \chi_{p_j}(a) = 1 \text{ for every } j, \\
0 & \text{otherwise,}
\end{cases}
\]

the left-hand side is equal to

\[
2^{r+1} \left( \sum' \log(1 - \zeta_{8m}^{a}) - \sum' \log(1 - \zeta_{8m}^{a}) \right)
\]

where each summation \( \sum' \pm \) runs over all \( a \mod 8m \) such that \( \chi_{-1}(a) = -1 \), \( \chi_{p_j}(a) = 1 \) for every \( j \), and \( \chi_{2d}(a) = \pm 1 \), respectively. Put \( m_j = m/p_j \) and \( a = mx + \sum_{j=1}^{r} 8m_j x_j \). If \( x \) and \( x_j \) run over complete reduced systems of residues
modulo $8$ and modulo $p_j$, respectively, then $a$ runs over a complete reduced system of residues modulo $8m$. Therefore, as $\chi_{p_j}(a) = \chi_{p_j}(2m_j x_j)$, the left-hand side is further equal to

$$2^r + 1 \sum' \prod' \left( \log(1 + \zeta_{p_1}^{x_1} \cdots \zeta_{p_r}^{x_r}) - \log(1 - \zeta_{p_1}^{x_1} \cdots \zeta_{p_r}^{x_r}) \right),$$

where we put $\zeta = -(2/m)\zeta_{\frac{8}{m}}$, and each summation $\sum'_{x_j}$ runs over all $x_j \mod p_j$ such that $\chi_{p_j}(x_j) = \chi_{p_j}(2m_j)$. On the other hand, applying Lemma 2, and since $\chi_{2d}(p) = \chi_{-2d}(p)$, the right-hand side is equal to

$$\sum_{d | m} \left( \prod_{p | m/d} (1 - \chi_{2d}(p)) \right) (2h(2d) \log(e_{2d}) - h(-2d) \pi i).$$

Thus we conclude that

$$2^r + 1 \sum' \prod' \left( \log(1 + \zeta_{p_1}^{x_1} \cdots \zeta_{p_r}^{x_r}) - \log(1 - \zeta_{p_1}^{x_1} \cdots \zeta_{p_r}^{x_r}) \right) = \sum_{d | m} \left( \prod_{p | m/d} (1 - \chi_{2d}(p)) \right) (2h(2d) \log(e_{2d}) - h(-2d) \pi i). \quad (1)$$

Letting each product $\prod'_{x_j}$ run over the same $x_j$ as in (1), set

$$\Psi_m(X) = \prod' \prod' (1 - X_{p_1}^{x_1} \cdots X_{p_r}^{x_r}).$$

Then we see that $\Psi_m(X)$ is one of the irreducible factors of the $m$th cyclotomic polynomial over the field $K = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})$, and the coefficients of $\Psi_m(X)$ belong to the integral ring $O_K$ of $K$. Let $c$ and $d$ be positive squarefree rational integers such that $(c, d) = 1$. We define $\phi_d$ by

$$\phi_d = \prod_{p | c} \frac{(1 - \chi_d(p))/2}{1},$$

in particular, $\phi_d = 1$, and if $d \equiv 0 \pmod{2}$ then the definition clearly coincides with that introduced in Section 1. Letting $d | m$ and $d > 0$, we put

$$k(\pm 2d) = h(\pm 2d)/2^{r(d)},$$

respectively. Then we see that $k(\pm 2d)$ is a rational integer. With these notations we obtain from (1) the formula

$$\frac{\Psi_m(-\zeta)}{\Psi_m(\zeta)} = \prod_{d | m} (e^{k(2d)/2} - k(-2d)) \phi_d^{\omega(d)} \quad (2).$$
4. CONSIDERATION MODULO $\omega^6$

Put $\omega = 1 - \zeta_8$. As $\zeta_8 = (1 + i)/\sqrt{2}$ and $\epsilon_2 = 1 + \sqrt{2}$, we see $\sqrt{2} = \zeta_8^3 \epsilon_2 \omega^2$. We will investigate the both sides of the formula (2) by the modulus $\omega^6$. Every congruence is considered in the integral ring of the field $K(\zeta_8)$.

Lemma 3. Letting $d|m$ and $d > 0$, we have

$$\epsilon_{2d} \equiv \epsilon_2^T d U_d \pmod{\omega^6}.$$  

Proof. Since

$$U_{2d} \equiv \begin{cases} 1 \pmod{2} & \text{if } N(\epsilon_{2d}) = -1, \\ 0 \pmod{2} & \text{if } N(\epsilon_{2d}) = +1, \end{cases}$$

we have

$$\epsilon_{2d} \equiv \begin{cases} (T_d + \sqrt{2d} \pmod{\omega^6}) & \text{if } N(\epsilon_{2d}) = -1, \\ T_d \pmod{\omega^6} & \text{if } N(\epsilon_{2d}) = +1. \end{cases}$$

First, suppose $N(\epsilon_{2d}) = -1$. Then we have

$$\epsilon_{2d} \pm \epsilon_2 = T_d \pm 1 \pm 2 \sqrt{2} \frac{1 \pm \sqrt{d}}{2},$$

so that

$$\epsilon_{2d} \pm \epsilon_2 \equiv T_d \pm 1 \pmod{\omega^6}.$$  

Hence

$$\epsilon_{2d} \equiv \pm \epsilon_2 \pmod{\omega^6},$$

respectively, if $T_d \equiv \pm 1 \pmod{4}$. Therefore, as $\epsilon_2^2 = 3 + 2 \sqrt{2} \equiv -1 \pmod{\omega^6}$, we get $\epsilon_{2d} \equiv \epsilon_2^d \pmod{\omega^6}$. Moreover, from $T_d^2 - 2dU_d^2 = -1$, we see $T_d^2 \equiv -1 \pmod{p}$ for every prime $p | U_d$, so that $U_d \equiv 1 \pmod{4}$. Hence $\epsilon_{2d} \equiv \epsilon_2^T d U_d \pmod{\omega^6}$. Second, suppose $N(\epsilon_{2d}) = +1$. Then we have

$$\epsilon_{2d} \equiv T_d \equiv (-1)^{(T_d - 1)/2} \equiv \epsilon_2^T d - 1 \pmod{\omega^6}.$$  

Moreover, from $T_d^2 - 2dU_d^2 = 1$, we have $(T_d - 1)(T_d + 1) = 2dU_d^2$, where $(T_d - 1, T_d + 1) = 2$, so that we may set

$$T_d \pm 1 = 2d_1 V_1^2, \quad T_d \mp 1 = d_2 V_2^2,$$
respectively, if $T_d \equiv \pm 1 \pmod{4}$, with rational integers $d_1$, $d_2$, $V_1$, and $V_2$ such that

$$d = d_1 d_2, \quad U_d = V_1 V_2, \quad V_1 \equiv 1 \pmod{2}, \quad V_2 \equiv 0 \pmod{2}.$$ 

Hence

$$d_1 V_1^2 - 2d_2 (V_2/2)^2 = \pm 1,$$

respectively, if $T_d \equiv \pm 1 \pmod{4}$. So

$$V_2 \equiv \begin{cases} 0 \pmod{4} & \text{if } T_d \equiv 1 \pmod{4}, \\ 2 \pmod{4} & \text{if } T_d \equiv -1 \pmod{4}, \end{cases}$$

which proves $U_d \equiv T_d - 1 \pmod{4}$. Hence $e_{2d} \equiv e_{2d}^{U_d T_d} \pmod{\omega^6}$.

Put

$$C_d = (T_d U_d k(2d) - k(-2d))/2,$$

and

$$D_d = -k(-2d).$$

Then, from Lemma 1, $C_d$ and $D_d$ are rational integers. From Lemma 3, we have

$$e_{2d}^{k(2d)} I_{-2d} \equiv e_{2d}^{T_d U_d k(2d) - k(-2d)} \pmod{\omega^6},$$

and

$$\equiv e_{2d}^{T_d U_d k(2d) - k(-2d)} (e_2^{-1} i)^{-k(-2d)} \pmod{\omega^6},$$

Hence, from (2), it follows that

$$\frac{\Psi_m(-\zeta)}{\Psi_m(\zeta)} \equiv (-1) \sum_{d \mid m} \phi_{d}^{\mu_d} C_d (e_2^{-1} i)^{\sum_{d \mid m} \phi_d^{m_d}} \pmod{\omega^6}. \quad (3)$$

**Lemma 4.** We have

$$\frac{\Psi_m(-\zeta)}{\Psi_m(\zeta)} = \begin{cases} (e_2^{-1} i)^{-1} \pmod{\omega^6} & \text{if } m = 1, \\ (-1)^{\phi} \pmod{\omega^6} & \text{if } m = p, \text{a prime}, \\ 1 \pmod{\omega^6} & \text{if } r > 1. \end{cases}$$

**Proof.** As $(1 - \zeta_s)/(1 + \zeta_s) = e_2 t^{-1}$, the lemma is valid for $m = 1$. Hence we assume $m > 1$ in the following. Since $\Psi_m(X)$ is a polynomial with coef-
CONGRUENCES FOR CLASS NUMBERS

Letting $f$ be the degree of $\Psi_m(X)$, we see $X^f\Psi_m(X^{-1}) = \Psi_m(X)$, in particular, $\zeta^f\Psi_m(\zeta^{-1}) = \Psi_m(\zeta)$. Hence, comparing the coefficients of $\zeta^k$, we get $\alpha_0 = \alpha_2$, $\alpha_3 = 0$ if $f \equiv 2 \pmod{8}$, $\alpha_4 = \alpha_0 = 0$ if $f \equiv 4 \pmod{8}$, $\alpha_0 = -\alpha_2$, $\alpha_1 = 0$ if $f \equiv 6 \pmod{8}$, and $\alpha_2 = -\alpha_4$ if $f \equiv 0 \pmod{8}$. Therefore, observing $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$, we may set $\Psi_m(\zeta) = \zeta^{f/2}(x + \sqrt{2} \beta)$ with $\alpha, \beta$ in $O_K$. Applying the conjugation $(-x \rightarrow -x)$, we get $\Psi_m(-\zeta) = (-\zeta)^{f/2}(x - \sqrt{2} \beta)$. Hence $\Psi_m(-\zeta)/\Psi_m(\zeta) = (1 - \sqrt{2} \beta)/(x + \sqrt{2} \beta)$. Therefore, since $x - \sqrt{2} \beta \equiv x + \sqrt{2} \beta \pmod{\omega^6}$, we obtain $\Psi_m(-\zeta)/\Psi_m(\zeta) = (-1)^{\frac{f}{2}} \pmod{\omega^6}$, which proves the lemma.

5. CONSIDERATION WITH $\Phi^d$

Let $\{d_i\}_{i=1}^{L} (L = 2')$ be an ordered set of all positive $d|m$, such that $r(d_i) \geq r(d_{i+1})$ for $i = 1, \ldots, L - 1$ ($d_1 = m$, $d_L = 1$). We fix this set once and for all. Let $\Phi$ be the $L \times L$ matrix whose $(k, l)$ components are defined to be $\Phi_{2d_i, d_k}$ if $d_i | d_k$, and 0 if $d_i \not| d_k$. Then, $\Phi$ is an upper triangular matrix whose diagonal elements are all 1. Let $\delta, \gamma, \Delta$ and $\Gamma$ be $L$-dimensional column vectors defined by

$$\delta = (D_{d_1}, D_{d_2}, \ldots, D_{d_L})^t,$$
$$\gamma = (C_{d_1}, C_{d_2}, \ldots, C_{d_L})^t,$$
$$\Delta = (\Delta_{d_1}, \Delta_{d_2}, \ldots, \Delta_{d_L})^t,$$

and

$$\Gamma = (\Gamma_{d_1}, \Gamma_{d_2}, \ldots, \Gamma_{d_L})^t,$$

where

$$\Delta_{d_l} = \begin{cases} -1 & \text{if } d_l = 1, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\Gamma_{d_l} = \begin{cases} \phi_p^2 & \text{if } d_l = p, \text{ a prime,} \\ 0 & \text{otherwise.} \end{cases}$$

We see $\varepsilon_2^{-1}i - 1 = \varepsilon_2 \omega^3$, $\varepsilon_2^{-1}i + 1 = -\varepsilon_8 \varepsilon_2^{-2} \omega^3$, and $(\varepsilon_2^{-1}i)^2 = \varepsilon_2^{-2}(-1) \equiv (-1)(-1) \equiv 1 \pmod{\omega^6}$. Hence, in the multiplicative group modulo $\omega^6$,
\( e^{-i} \) and \(-1\) have the order 2, and are independent of each other. Therefore, applying Lemma 4 to (3), we obtain
\[
\sum_{d \mid m} \phi_{2d}^{m/d} D_d \equiv A_m \pmod{2} \tag{4}
\]
and
\[
\sum_{d \mid m} \phi_{2d}^{m/d} C_d \equiv \Gamma_m \pmod{2}. \tag{5}
\]
Clearly (4) and (5) are valid for every \( d \), in place of \( m \). Hence
\[
\Phi \delta \equiv A \pmod{2} \tag{6}
\]
and
\[
\Phi \gamma \equiv \Gamma \pmod{2}. \tag{7}
\]

**Lemma 5.** Let \( d \mid m \), \( d > 0 \), and \( q \) be a prime such that \( q \nmid d \). Then we have
\[
\sum_{\substack{n \mid d \\text{and} \ \ 0 < n < d}} D_n \phi_{2n}^{d/n} \phi_{d/n}^{q} \equiv \left\{ \begin{array}{ll}
\phi_p^q \phi_2^q \pmod{2} & \text{if } d = p, \text{a prime}, \\
\sum_{p \mid d} \phi_p^q \sum_{n \mid d/p} D_n \phi_{2n}^{(d/p)/n} \phi_{(d/p)/n}^{p} \pmod{2} & \text{if } r(d) > 1.
\end{array} \right.
\]

**Proof.** If \( d = p \) a prime, then from (6) (or (4), putting \( m = p \)) we have
\( D_p - \Phi_p^q \equiv 0 \pmod{2} \), so that Lemma 5 is valid. Suppose \( r(d) > 1 \). In view of \( \phi_M^{q} \equiv \phi_M^q + \phi_M^q \pmod{2} \) for \( MN \mid d/n \), we see
\[
\phi_{d/n}^{q} \equiv \sum_{p \mid d/n} \phi_p^q \pmod{2}.
\]
Hence
\[
\sum_{\substack{n \mid d \\text{and} \ \ 0 < n < d}} D_n \phi_{2n}^{d/n} \phi_{d/n}^{q} \equiv \sum_{\substack{n \mid d \\text{and} \ \ 0 < n < d}} D_n \phi_{2n}^{d/n} \sum_{p \mid d/n} \phi_p^q \pmod{2} = \sum_{p \mid d, n \mid d/p} \phi_p^q \sum_{n \mid d/p} D_n \phi_{2n}^{d/n}.
\]
Therefore, observing \( \phi_{2n}^{d/n} = \phi_{2n}^{(d/p)/n} \phi_{2n}^p \), it follows that

\[
\sum_{n \mid d} D_n \phi_{2n}^{d/n} \phi_{a/n}^q \equiv \sum_{p \mid d} \phi_p^q \sum_{n \mid d/p} D_n \phi_{2n}^{(d/p)/n} \phi_{2n}^p \pmod{2}. \tag{8}
\]

From (6) (or (4), putting \( m = d/p \)), we have

\[
D_{d/p} \equiv \sum_{n \mid d/p} D_n \phi_{2n}^{(d/p)/n} \pmod{2}.
\]

Hence

\[
\sum_{n \mid d/p} D_n \phi_{2n}^{(d/p)/n} \phi_{2n}^p \equiv \sum_{n \mid d/p} D_n \phi_{2n}^{(d/p)/n} (\phi_{2n}^p + \phi_{2d/p}^p) \pmod{2}. \tag{9}
\]

Here, we see

\[
\phi_{2n}^p + \phi_{2d/p}^p \equiv \phi_{(d/p)/n}^p \pmod{2}. \tag{10}
\]

Putting (8), (9), and (10) together, we obtain Lemma 5.

Let \( \Theta \) be the \( L \times L \) diagonal matrix whose \((l, l)\) components are defined to be \( \phi_{d/l}^2 \).

**Lemma 6.** \( \Phi \Theta \delta = \Gamma \pmod{2} \).

**Proof.** Let \( d \mid m \). Noting \( \phi_1^2 - 0 \), we may assume \( d > 1 \). From (6) (or (4), putting \( m = d \)), we have

\[
D_d \equiv \sum_{n \mid d} D_n \phi_{2n}^{d/n} \pmod{2}.
\]

Hence

\[
\sum_{n \mid d} D_n \phi_{2n}^{d/n} \phi_n^2 \equiv \sum_{n \mid d} D_n \phi_{2n}^{d/n} (\phi_n^2 + \phi_2^2) \pmod{2}
\]

\[
= \sum_{n \mid d} D_n \phi_{2n}^{d/n} \phi_{n/d}^2 \pmod{2}.
\]

Here, we apply Lemma 5 successively \( r(d) \) times (first putting \( q = 2 \)). Then, we obtain
\[
\sum_{n \mid d} D_n \phi_{2n}^d \phi_n^2 \equiv \begin{cases} 
\phi_p^2 \phi_2^p \pmod{2} & \text{if } d = p, \text{ a prime} \\
\left( \sum_{q_1 \mid d/q_2} \phi_{q_1}^2 \right) \left( \sum_{q_2 \mid d/q_1} \phi_{q_2}^2 \right) \cdots \left( \sum_{q_r \mid d/\prod_{i=1}^{r-1} q_i} \phi_{q_r}^2 \right) \times (\phi_{q_r}^{q_r-1} \phi_2^{q_r}) \pmod{2} & \text{if } r(d) > 1,
\end{cases}
\]

where we put \( r' = r(d) \) and \( q_r = d/\prod_{j=1}^{r-1} q_j \). That is,

\[
\sum_{n \mid d} D_n \phi_{2n}^d \phi_n^2 \equiv \sum_{q_1, \ldots, q_r = d/q, \text{ primes}} \phi_{q_1}^2 \phi_{q_2}^2 \cdots \phi_{q_r}^{q_r-1} \phi_2^{q_r} \pmod{2},
\]

where the summation on the right hand side runs over all \( r' \)-tuples \((q_1, \ldots, q_r)\). Therefore, as \( \phi_{q_1}^2 \phi_{q_2}^2 \cdots \phi_{q_r}^{q_r-1} \phi_2^{q_r} = \phi_{q_1}^2 \phi_{q_2}^{q_2-1} \cdots \phi_{q_r}^{q_r-1} \phi_2^{q_r} \), we conclude that

\[
\sum_{n \mid d} D_n \phi_{2n}^d \phi_n^2 \equiv \begin{cases} 
\phi_p^2 \pmod{2} & \text{if } d = p, \text{ a prime,}
\end{cases}
\]

\[
\begin{cases} 
0 \pmod{2} & \text{if } r(d) > 1,
\end{cases}
\]

which proves Lemma 6.

6. Proof of the Theorem

Since \( \det(\Phi) = 1 \), from (8) and Lemma 6, it follows that

\[ \Theta \delta \equiv \gamma \pmod{2}. \]

Hence

\[ \phi_m^2 D_m \equiv C_m \pmod{2}. \]

That is,

\[
- \frac{1 - \chi_m(2)}{2} k(-2m) \equiv \frac{T_m U_m k(2m) - k(-2m)}{2} \pmod{2}.
\]

Hence

\[ k(-2m) \equiv \chi_m(2) T_m U_m k(2m) \pmod{4}, \]

which completes the proof of the theorem.
7. PROOF OF PROPOSITIONS

We prove Proposition 1 and 3 by induction on \( r \). Then Proposition 2 has already been proved in Section 1.

Now, from (4), we have

\[
D_m = \sum_{0 < n < m} \phi_{2n/m} D_n \pmod{2},
\]

which proves Proposition 1 from the induction assumption.

To prove Proposition 3, we first observe that

\[
\phi_{2n_1/n_1}^{m_0/n_1} = \begin{cases} 
1 \quad \text{in case (i)} \\
1 \quad \text{in case (ii), and if } r(n_1) \text{ is even,} \\
0 \quad \text{in case (ii), and if } r(n_1) \text{ is odd.}
\end{cases}
\]

Therefore, from the induction assumption, it follows that

\[
\sum_{n \mid m} \phi_{2n_1/n_1}^{m_0/n_1} \phi_{2n_2/n_2}^{m_1/n_1} \cdots \phi_{2n_s/n_s}^{m_{s-1}/n_s} = \sum_{n \mid m} \phi_{2n_1/n_1}^{m_0/n_1} \sum_{n_2 \mid n_1} \phi_{2n_2/n_2}^{m_1/n_1} \cdots \phi_{2n_s/n_s}^{m_{s-1}/n_s}
\]

\[
\equiv \begin{cases} 
\sum_{n \mid m} 1 \pmod{2} \quad \text{in case (i),} \\
\sum_{n \mid m} 1 \pmod{2} \quad \text{in case (ii).}
\end{cases}
\]

Here we see

\[
\sum_{n \mid m} 1 = 2^r - 1 = 1 \pmod{2},
\]

and

\[
\sum_{n \mid m} 1 \equiv \sum_{n \mid m} (r(n) + 1) \equiv \sum_{n \mid m} r(n) + 1
\]
\[ \equiv \sum_{j=0}^{r} \binom{r}{j} j - r + 1 \pmod{2} \]
\[ = \sum_{j=1}^{r} \binom{r-1}{j-1} r - r + 1 \]
\[ = 2^r \cdot r - r + 1 \]
\[ = 1 \pmod{2}, \]

which proves Proposition 3 from Proposition 2.

8. Note

Finally we give some numerical examples for the fact that the theorem does not hold for the modulus \(2^r + 3\), nor in the case where \(m\) contains a prime factor \((>0)\) congruent to 3 modulo 4. Put \(w = h(-2m) - \left(\frac{2}{m}\right) TUh(2m)\).

(i) A counterexample for the modulus \(2^r + 3\):

\(m = 65, \quad r = 2, \quad h(-2m) = 4 \quad (h(-2m)/2^r \text{ is odd}), \left(\frac{2}{m}\right) = 1, \)
\[ h(2m) = 4, \quad e = 57 + 5 \sqrt{130}, \quad w = -2^4 \cdot 71; \]
\(m = 901, \quad r = 2, \quad h(-2m) = 32 \quad (h(-2m)/2^r \text{ is even}), \left(\frac{2}{m}\right) = -1, \)
\[ h(2m) = 4, \quad e = 849 + 20 \sqrt{1802}, \quad w = 2^4 \times 4247. \]

(ii) A counterexample for a modulus \(m\), having a prime factor \(p \equiv 3 \pmod{4}\)

\(m = 133, \quad 7 | m, \quad r = 2, \quad h(-2m) = 20 \quad (h(-2m)/2^r \text{ is odd}), \left(\frac{2}{m}\right) = -1, \)
\[ h(2m) = 2, \quad e = 685 + 42 \sqrt{266}, \quad w = 2^3 \times 7195. \]
\(m = 209, \quad 11 | m, \quad r = 2, \quad h(-2m) = 8 \quad (h(-2m)/2^r \text{ is even}), \left(\frac{2}{m}\right) = 1, \)
\[ h(2m) = 2, \quad e = 33857 + 1656 \sqrt{418}, \quad w = -2^3 \times 14016797. \]
REFERENCES