2-adic and 3-adic part of class numbers and properties of central values of $L$-functions

by

Matija Kazalicki (Madison, WI)

1. Introduction and statement of results. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, and let $\text{Cl}(\mathbb{Q}(\sqrt{-d}))$ denote its ideal class group. Starting with Gauss, who developed genus theory, many people have investigated the structure of the 2-Sylow subgroup of $\text{Cl}(\mathbb{Q}(\sqrt{-d}))$. In the case when $d = p$ is prime, Barrucand and Cohn [1] in 1969 discovered the beautiful fact that the class number $h(-p) := h(\mathbb{Q}(\sqrt{-p}))$ is divisible by 8 if and only if $p = x^2 + 32y^2$, where $x$ and $y$ are integers. In the early 1980s, Williams [22] showed that if $\epsilon = T + U\sqrt{p}$ is a fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{p})$, then

$$h(-p) \equiv T + (p - 1) \pmod{16},$$

where $8 \mid h(-p)$. Yamamoto [23] and Stevenhagen [18] proved this and similar results by studying small degree extensions of $\mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(\sqrt{-p})$.

Let $d$ be prime or the product of two primes. We study the connection between the 2-part and 3-part of the class numbers $h(-d)$ and $h(-3d)$ and ray class groups of $\mathbb{Q}(\sqrt{d})$ unramified outside 2 and 3. More precisely, if $p_1$ and $p_2$ are primes above 2 and 3 in $\mathbb{Q}(\sqrt{d})$ (we assume that 2 and 3 split), we investigate the ray class groups $G_{m,n}$ of $\mathbb{Q}(\sqrt{d})$ of modulus

$$m = p_1^m p_2^n,$$

where $m, n > C_d$ for some constant $C_d$. If $r_k(\mathbb{Q}(\sqrt{d}))$ denotes the $k$-rank of any such $G_{m,n}$, we obtain the following “reflection” theorems.

2010 Mathematics Subject Classification: Primary 11F30, 11F33, 11F67; Secondary 11F11, 11F37, 11R37.

Key words and phrases: congruences between modular forms, delta function, ray class groups, special values of $L$-functions.

DOI: 10.4064/aa147-1-3 [51] © Instytut Matematyczny PAN, 2011
Theorem 1.1. Suppose that $p$ is prime.

(1) If $p \equiv 1 \pmod{16}$, then
$$4 \parallel h(-p) \iff r_4(\mathbb{Q}(\sqrt{p})) = 1,$$
$$8 \parallel h(-p) \iff r_4(\mathbb{Q}(\sqrt{p})) = 2 \text{ and } r_8(\mathbb{Q}(\sqrt{p})) = 1,$$
$$16 \mid h(-p) \iff r_8(\mathbb{Q}(\sqrt{p})) = 2.$$

(2) If $p \equiv 9 \pmod{16}$, then
$$4 \parallel h(-p) \iff r_4(\mathbb{Q}(\sqrt{p})) = 1,$$
$$8 \parallel h(-p) \iff r_4(\mathbb{Q}(\sqrt{p})) = 2 \text{ and } r_8(\mathbb{Q}(\sqrt{p})) = 1,$$
$$16 \mid h(-p) \iff r_4(\mathbb{Q}(\sqrt{p})) = 2.$$

Remark. Since $h(-p)$ is odd for $p \equiv 3, 7 \pmod{8}$ and $h(-p) \equiv 2 \pmod{4}$ for $p \equiv 5 \pmod{8}$, the only interesting case is $p \equiv 1 \pmod{8}$.

Theorem 1.2. If $p$ and $q$ are primes for which $p, q \equiv 3, 5 \pmod{8}$ and $pq \equiv 1 \pmod{8}$, then
$$4 \parallel h(-pq) \iff r_4(\mathbb{Q}(\sqrt{pq})) = 1,$$
$$8 \parallel h(-pq) \iff r_8(\mathbb{Q}(\sqrt{pq})) = 2,$$
$$16 \mid h(-pq) \iff r_4(\mathbb{Q}(\sqrt{pq})) = 2 \text{ and } r_8(\mathbb{Q}(\sqrt{pq})) = 1.$$

Theorem 1.3. If $p \equiv 1 \pmod{8}$ is prime, then $3 \nmid h(-3p)$ if and only if $r_3(\mathbb{Q}(\sqrt{p})) = 1$.

As a consequence of these theorems, we recover (1.1) and we obtain the following result relating the divisibility of class numbers to congruence properties of fundamental units.

For primes $p$ and $q$, we denote by $(\frac{p}{q})$ and $(\frac{p}{q})_4$ the quadratic and quartic residue symbol.

Theorem 1.4. If $p$ and $q$ are primes for which $p, q \equiv 5 \pmod{8}$, then
$$16 \mid h(-pq) \iff \begin{cases} T \equiv 9 \pmod{16} & \text{if } (\frac{p}{q}) = 1 \text{ and } (\frac{p}{q})_4(\frac{q}{p})_4 = -1, \\ T \equiv 4 \pmod{8} & \text{if } (\frac{p}{q}) = -1, \end{cases}$$
where $T + U \sqrt{pq}$ is a fundamental unit of $\mathbb{Q}(\sqrt{pq})$. When $\text{Norm}(\epsilon) = -1$, we choose the fundamental unit such that $T \equiv 1 \pmod{4}$.

Remark. If $p, q \equiv 3 \pmod{8}$ then $4 \nmid h(-pq)$. Therefore, we do not consider this case.

Using class field theory and facts about fundamental units, we show for the quadratic fields in Theorems 1.1–1.3 that the structure of the ray class groups $G_{m,n}$ is constrained by the 2- and 3-adic valuation of the regulator of $\mathbb{Q}(\sqrt{d})$. On the other hand, the regulator is connected via the $p$-adic class number formula to the value at 1 of the 2- and 3-adic $L$-functions of
the character that corresponds to $\mathbb{Q}(\sqrt{d})$. The following result relating class numbers to $p$-adic $L$-function implies Theorems 1.1–1.3.

**Theorem 1.5.** Let $p$ and $q$ be primes.

(a) If $p \equiv 1 \pmod{16}$, then $16 \mid \left( \frac{1}{3} L_2(1, \chi_p) + 3h(-p) \right)$.

(b) If $p \equiv 9 \pmod{16}$, then $8 \parallel \left( \frac{1}{3} L_2(1, \chi_p) + 3h(-p) \right)$.

(c) If $pq \equiv 1 \pmod{8}$ and $p, q \equiv 3, 5 \pmod{8}$, then $8 \parallel \left( \frac{1}{3} L_2(1, \chi_{pq}) + 3h(-pq) \right)$.

(d) If $p \equiv 1 \pmod{8}$, then $3 \mid (L_3(1, \chi_p) + 2h(-3p))$.

**Remark.** Shanks, Sime and Washington, in their paper on zeros of 2-adic $L$-functions [15], obtained results that are similar to parts (b) and (c) of Theorem 1.5. In those two cases the 2-adic $L$-function has only one zero. The $L$-function from part (a) has more than two zeros.

We prove Theorems 1.1–1.5 by studying congruences between certain half-integral weight modular forms, the Cohen–Eisenstein series and the cube of the Jacobi theta function.

We also consider $L$-functions associated to Ramanujan’s Delta-function,

$$\Delta(z) = \sum_{n=0}^{\infty} \tau(n) z^n := q \prod_{n=1}^{\infty} (1 - q^n)^{24},$$

the unique weight 12 normalized cusp form for the full modular group. Also, denote by $\sigma_k(n) = \sum_{d|n} d^k$ the sum of $k$th powers of divisors of $n$. Ramanujan observed that modulo the powers of certain small primes, there are congruences relating $\tau(n)$ and $\sigma_k(n)$. For example, for the powers of two the following congruences are due to Kolberg [10]:

$$\tau(n) \equiv \sigma_{11}(n) \pmod{2^{11}} \quad \text{if } n \equiv 1 \pmod{8},$$

$$\tau(n) \equiv 1217\sigma_{11}(n) \pmod{2^{13}} \quad \text{if } n \equiv 3 \pmod{8},$$

$$\tau(n) \equiv 1537\sigma_{11}(n) \pmod{2^{12}} \quad \text{if } n \equiv 5 \pmod{8},$$

$$\tau(n) \equiv 705\sigma_{11}(n) \pmod{2^{14}} \quad \text{if } n \equiv 7 \pmod{8}.$$ 

By the work of Eichler, Shimura, Deligne and Serre, for every prime $l$ there is a 2-dimensional $l$-adic Galois representation $\rho_l : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}_l)$ with the property that $\text{Tr}(\rho_l(\text{Frob}_p)) = \tau(p)$ for every prime $p \neq l$ (\text{Frob}_p \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) is a Frobenius element for the prime $p$). Swinnerton–Dyer [19] showed that the image of these representations is “small” for primes $l = 2, 3, 5, 7$ and 691. Moreover, he showed that Kolberg’s congruences determine the structure of $\rho_2$. More precisely, up to conjugation by an element of $\text{GL}_2(\mathbb{Q}_2)$, the image of $\rho_2$ consists of matrices of the form

$$\sigma = \begin{pmatrix} 1 + 2^7A & 2^4B \\ 2^5C & 1 + 2D \end{pmatrix},$$
where $A, B, C, D \in \mathbb{Z}_2$. Since the representation $\rho_2$ is reducible modulo $2^5$, inspired by the Bloch–Kato conjecture, one expects to find some congruences modulo the powers of two between the algebraic part of the central value of the $L$-function associated to the Delta function and its quadratic twists, and a value of the corresponding Dirichlet $L$-function.

For a positive fundamental discriminant $d$, we denote by $\Delta_d$ the twist of $\Delta(z)$ by the quadratic character $(d \cdot \chi_d)$. Square roots of the algebraic parts $\sqrt{L_{\text{alg}}(\Delta_d, 6)}$ will be defined later in this section. We prove the following theorem.

**Theorem 1.6.** If $d$ is a positive fundamental discriminant, then:

\[
\sqrt{L_{\text{alg}}(\Delta_d, 6)} \equiv 49 \cdot 4L_2(11, \chi_d) \pmod{2^9} \quad \text{for } d \equiv 1 \pmod{16},
\]
\[
\sqrt{L_{\text{alg}}(\Delta_d, 6)} \equiv 71 \cdot 4L_2(11, \chi_d) \pmod{2^9} \quad \text{for } d \equiv 5 \pmod{16},
\]
\[
\sqrt{L_{\text{alg}}(\Delta_d, 6)} \equiv 369 \cdot 4L_2(11, \chi_d) \pmod{2^9} \quad \text{for } d \equiv 9 \pmod{16},
\]
\[
\sqrt{L_{\text{alg}}(\Delta_d, 6)} \equiv 7 \cdot 4L_2(11, \chi_d) \pmod{2^9} \quad \text{for } d \equiv 13 \pmod{16},
\]
\[
\sqrt{L_{\text{alg}}(\Delta_d, 6)} \equiv d \cdot 12L_3(15, \chi_d) \pmod{3^4} \quad \text{for all } d.
\]

**Remark.** The question of how congruences modulo a power of a prime between the coefficients of Hecke eigenforms give rise to congruences between the algebraic parts of the critical values of the associated $L$-functions was initially studied by Mazur [12], [13]. Using modular symbols to study algebraic parts of $L$-values, Vatsal [20] proved a general result for congruences between Eisenstein series and cuspidal newforms of weight 2. Vatsal remarks that his result could be generalized to higher weights $k$, but only if $p > k$. Here, we consider small primes $p \in \{2, 3\}$.

Another approach to these questions, introduced by Maeda in [11], is to use the Kohnen–Waldspurger theorem to translate congruences between $L$-values to congruences between half-integral weight modular forms that correspond to integral weight modular forms via Shimura correspondence. More precisely, one can show [14, p. 154] that the Kohnen newform in $S_{6+1/2}^{\text{new}}(T_0(4))$ associated to $\Delta(z)$ is

\[
g(z) = \sum_{n=1}^{\infty} b(n)q^n = \frac{E_4(4z)\Theta(\theta_0(z))}{2} - \frac{\Theta(E_4(4z))\theta_0(z)}{16},
\]

where for integer $k$, $E_{2k}(z)$ is the normalized Eisenstein series of weight $2k$ on $\text{SL}_2(\mathbb{Z})$, and $\Theta$ is Ramanujan’s Theta-operator defined by

\[
\Theta \left( \sum_{n=0}^{\infty} a(n)q^n \right) = \sum_{n=0}^{\infty} na(n)q^n.
\]

Now the Kohnen–Waldspurger theorem for positive fundamental discrimi-
nants $d$ implies that

$$L(\Delta_d, 6) = \frac{\langle \Delta, \Delta \rangle \pi^6}{120d^{11/2} \langle g, g \rangle} \cdot b(d)^2$$

(\text{where $\langle \cdot, \cdot \rangle$ is the standard Petersson inner product). We define the algebraic part of $L(\Delta_d, 6)$ to be $L^{\text{alg}}(\Delta_d, 6) := b(d)^2$, and we define the square root of the algebraic part to be $\sqrt{L^{\text{alg}}(\Delta_d, 6)} := b(d)$. Koblitz [8] showed that the Shimura lifting on cusp forms, as modified by Kohnen, extends to Eisenstein series. The weight $6 + 1/2$ modular form that corresponds to $E_{12}(z)$ is the Cohen–Eisenstein series $H_{6+1/2}(z) \in M_{6+1/2}(\Gamma_0(4))$. In general, for $r \geq 1$ we have Cohen–Eisenstein series of weight $r + 1/2$:

$$H_{r+1/2}(z) = \sum_{N \geq 0} H(r, N) q^N \in M_{r+1/2}(\Gamma_0(4))$$

(cf. [3]), where $H(r, N)$ is an explicit arithmetic function. For example, if $D = (-1)^r N$ is a discriminant of a quadratic field, then $H(r, N) = L(1 - r, \chi_D)$.

Koblitz proved that the congruence $\Delta(z) \equiv E_{12}(z) \pmod{691}$ descends to the congruence $g(z) \equiv -252H_{6+1/2}(z) \pmod{691}$, and Datskovsky and Guerzhoy [4] generalized this to other weights. We have an analogous theorem for moduli which are powers of 2. The difference is that we prove congruences modulo a theta series of weight $1/2$. More precisely we write

$$f(z) \equiv' g(z) \pmod{N} \iff f(z) - g(z) \equiv h(z) \pmod{N}$$

for some $p$-adic modular form $h(z)$ whose non-zero coefficients are supported on squares.

For a modular form $f(z) = \sum a(n) q^n$, we denote by

$$f(z)^+ = \sum_{n \equiv 1 \pmod{8}} a(n) q^n \quad \text{and} \quad f(z)^- = \sum_{n \equiv 5 \pmod{8}} a(n) q^n$$

the modular forms obtained by “twisting”.

**Theorem 1.7.** With $g(z)$ as in (1.2), we have

$$g(z)^+ \equiv' 49 \cdot 4H_{6+1/2}(z)^+ \pmod{2^9}, \quad g(z)^- \equiv' 39 \cdot 4H_{6+1/2}(z)^- \pmod{2^9}.$$  

When we compare $H_{6+1/2}(z)$ and $\theta_0(z)^3$ modulo powers of two and three, we get the following corollary.

**Corollary 1.8.** Let $d$ be a positive fundamental discriminant.

(a) If $d \equiv 1 \pmod{8}$, then $2^5 \mid \sqrt{L^{\text{alg}}(\Delta_d, 6)} + 12h(-d)$.

(b) If $d \equiv 1 \pmod{8}$, then $3^3 \mid \sqrt{L^{\text{alg}}(\Delta_d, 6)} - 120d \cdot H(-3d)$.

Here, $H(-N)$ denotes the Hurwitz class number.

Kohnen first proved in [9] results similar to part (b), and he used them together with the result of Davenport and Heilbronn on the 3-part of the
class group to obtain non-vanishing of a positive proportion of central $L$-
values $L(\Delta_d, 6)$.

2. Preliminaries for the proofs of the theorems

2.1. Ray class groups and class field theory. In this subsection we
use class field theory to show that the structure of the 2- and 3-parts of
ray class groups from the introduction are determined by 2-adic and 3-adic
properties of fundamental units.

Let $E$ be the unit group of the real quadratic field $K = \mathbb{Q}(\sqrt{d})$. For
a prime $p$ of $K$, denote by $U_p$ the group of units of the completion $K_p$.
Fix a rational prime $P$ that splits in $K$. Denote by $p_1$ and $p_2$ primes of
$K$ above $P$. For integers $m, n \geq 0$ let $F_{m,n}$ be the ray class field of
$K$ of modulus $m = p_1^m p_2^n$. Let

$$U_{m,n} = (1 + p_1^m)(1 + p_2^n), \quad U = \prod_{p|P} U_p, \quad U' = \prod_{p|P} U_p, \quad U'' = \prod_{p \nmid P} U_p$$

be subgroups of $I_K$, the group of ideles of $K$ (we put 1 at all other places).
As usual, we embed $K$ diagonally in $I_K$. The image of $E$ in $U' = U_{p_1} U_{p_2}$
under this map is denoted by $\bar{E}$. Let $H$ be the Hilbert class field of $K$.

We will determine the structure of $G_{m,n}$ by studying $\text{Gal}(F_{m,n}/H)$ and
$\text{Cl}(K)$ separately. It is easy to describe the structure of $\text{Gal}(F_{m,n}/H)$ using
the idelic formalism (see [21, pp. 269, 396]).

**Theorem 2.1.** Using the notation above we have

$$\text{Gal}(F_{m,n}/H) \cong \left( \prod_{p|P} U_p \right) / \bar{E} U_{m,n}.$$

**Proof.** By class field theory, $K^\times U$ and $K^\times U'' U_{m,n}$ are open subgroups
of finite index of $I_K$ that correspond to the fields $H$ and $F_{m,n}$. Hence, we have

$$\text{Gal}(F_{m,n}/H) \cong K^\times U / K^\times U'' U_{m,n} \cong (K^\times U'' U_{m,n}) U' / K^\times U'' U_{m,n}
\cong U' / (U' \cap K^\times U'' U_{m,n}).$$

Next we show that $U' \cap K^\times U'' U_{m,n} = \bar{E} U_{m,n}$. One inclusion is easy; if $\epsilon \in E$
then we have $\bar{\epsilon} \in U'$ and $\bar{\epsilon} = \epsilon(\frac{k}{\ell}) \in K^\times U''$. For the other direction, let
$x \in K^\times, u'' \in U''$ and $u \in U_{m,n}$. Suppose that $x u'' u \in U'$. First, observe
that $x$ is a unit since it is a local unit for every finite place. Next, note that
$x u'' \in \bar{E}$. Hence, we have $x u'' u \in \bar{E} U_{m,n}$. ■

The following two lemmas imply that for the real quadratic fields of
interest, the Hilbert class field is disjoint from the cyclotomic extension.

For prime $p$, we define the first step of cyclotomic $\mathbb{Z}_p$-extension of number
fields $L/K$ to be the intermediate field $F$, such that $\text{Gal}(F/K) \cong \mathbb{Z}/p\mathbb{Z}$.
Lemma 2.2. If $d \equiv 1 \pmod{4}$ is a positive fundamental discriminant, then the first step in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Q}(\sqrt{2}, \sqrt{d})$, and the extension $\mathbb{Q}(\sqrt{2}, \sqrt{d})/\mathbb{Q}(\sqrt{d})$ is ramified over primes above 2.

Proof. The first statement is well known (e.g. see [21, p. 319]). For the second statement, note that 2 ramifies in the extension $\mathbb{Q}(\sqrt{2}, \sqrt{d})/\mathbb{Q}$ since it ramifies in $\mathbb{Q}(\sqrt{2})$, but that it does not ramify in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Hence, primes above 2 must ramify in $\mathbb{Q}(\sqrt{2}, \sqrt{d})/\mathbb{Q}(\sqrt{d})$. $lacksquare$

Lemma 2.3. If $d$ is a positive fundamental discriminant such that $3 \nmid d$, then the first step in the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{d})$ is ramified over primes above 3.

Proof. Let $\mathbb{Q}(\zeta)$ be the first step in the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}$. Then $\mathbb{Q}(\zeta)/\mathbb{Q}$ is ramified above 3. Since 3 does not ramify in $\mathbb{Q}(\sqrt{d})$, it ramifies in $\mathbb{Q}(\sqrt{d}, \zeta)/\mathbb{Q}(\sqrt{d})$, which is the first step in the cyclotomic $\mathbb{Z}_3$ tower over $\mathbb{Q}(\sqrt{d})$. $lacksquare$

Now consider $P = 2$ and $P = 3$ in detail.

Ray class groups unramified outside 2. In this case $U_p \cong \mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2$, and we have the following well known result.

For prime $p$, we define $v_p$ to be the $p$-adic valuation on $\mathbb{Z}_p$, normalized such that $v_p(p) = 1$.

Lemma 2.4. The 2-adic logarithm induces an isomorphism

$$\frac{1 + 2\mathbb{Z}_2}{1 + 2^k\mathbb{Z}_2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}.$$ 

Under this map an element $\epsilon$ with $2 \leq v_2(\epsilon - 1) = t \leq k$ is mapped to the element of $\mathbb{Z}/2^{k-t}\mathbb{Z}$ of order $2^{k-t}$.

Remark. More precisely, the 2-adic logarithm induces an isomorphism

$$\Phi : \frac{1 + 4\mathbb{Z}_2}{1 + 2^k\mathbb{Z}_2} \cong 4\mathbb{Z}_2/2^k\mathbb{Z}_2 = \mathbb{Z}/2^{k-2}\mathbb{Z}.$$ 

The isomorphism from Lemma 2.4 maps $x \in (1 + 2\mathbb{Z}_2) - (1 + 4\mathbb{Z}_2)$ to $(1, \Phi(-x))$, and it maps $x \in 1 + 4\mathbb{Z}_2$ to $(0, \Phi(x))$.

We will need the following proposition from group theory.

Proposition 2.5. Let $G = G_0 \times G_1 \times G_2$ be a direct product of cyclic groups of order 2, $2^{k_1}$ and $2^{k_2}$, and let $1 \in G_0$, $\epsilon_1 \in G_1$ and $\epsilon_2 \in G_2$ be elements of order 2, $2^{k_1}$ and $2^{k_2}$. Denote by $H$ the subgroup of $G$ generated by $(1, \epsilon_1, \epsilon_2)$. Then

$$G/H \cong \mathbb{Z}/2^{\min(k_1-l_1,k_2-l_2)+1}\mathbb{Z} \times \mathbb{Z}/2^{k_1+k_2-\min(k_1-l_1,k_2-l_2)-\max(l_1,l_2)}\mathbb{Z}.$$ 

Proof. We may assume that $\min(k_1-l_1, k_2-l_2) = k_1 - l_1$. Let $g_1 \in G_1$ and $g_2 \in G_2$ be generators such that $\epsilon_1 = g_1^{2^{k_1-l_1}}$ and $\epsilon_2 = g_2^{2^{k_2-l_2}}$. It is
easy to check that the element \( \epsilon = (1, g_1, g_2^{2^{k_2-l_2-l_1}}) \in G \) generates the subgroup of \( G/H \) isomorphic to \( \mathbb{Z}/2^{\min(k_1-l_1,k_2-l_2)+1} \mathbb{Z} \). The \( G_1 \) component of \( \epsilon^r \) is not a power of \( \epsilon_1 \) for \( 0 < r < 2^{k_1-l_1} \), so it is not in \( H \). Also, the \( G_0 \) component of \( \epsilon \) is 1, so \( \epsilon \) is not a square in \( G/H \). Now the claim follows since \( H \) contains an element of order 2, which implies that \( G/H \) is a product of two cyclic groups. ■

Now we work out in detail the special cases of Theorem 2.1 for \( K = \mathbb{Q}(\sqrt{d}) \) where \( d \equiv 1 \pmod{8} \) is prime, or a product of two primes \( q, r \equiv 3, 5 \pmod{8} \).

**Theorem 2.6.** Let \( \epsilon = \alpha + U\sqrt{d} \ (T, U \in \mathbb{Z}) \) be a fundamental unit of \( K \), and let \( k = v_2(\text{Norm}(\epsilon - 1)) - 2 \).

(a) If \( d \equiv 1 \pmod{8} \) is prime, or a product of two primes \( p, q \equiv 5 \pmod{8} \), if \( \text{Norm}(\epsilon) = -1 \), and if \( m, n \geq 2 \) are integers, then

\[
\text{Gal}(F_{m,n}/H) \cong \mathbb{Z}/2^k \mathbb{Z} \times \mathbb{Z}/2^{\min(m,n)-2}\mathbb{Z}.
\]

In particular,

\[
r_{2^{k+v_2(\text{Cl}(\mathbb{Q}(\sqrt{d})))}}(\mathbb{Q}(\sqrt{d})) = 2.
\]

(b) If \( d = pq \) is a product of two primes with \( p, q \equiv 3 \pmod{8} \), or \( p, q \equiv 5 \pmod{8} \), and if \( \text{Norm}(\epsilon) = 1 \), then

\[
\text{Gal}(F_{m,n}/H) \cong \mathbb{Z}/2^k \mathbb{Z} \times \mathbb{Z}/2^{\min(m,n)-2}\mathbb{Z}.
\]

In particular,

\[
r_{2^{1+v_2(\text{Cl}(\mathbb{Q}(\sqrt{d})))}}(\mathbb{Q}(\sqrt{d})) = 2.
\]

**Remark.** It is easy to show that if \( \text{Norm}(\epsilon) = -1 \), then \( v_2(\text{Norm}(\epsilon - 1)) = v_2(\log_2 \epsilon) + 1 \). From the proof of part (b), we will see that for suitable \( \epsilon \), \( v_2(\log_2 \epsilon) = 2 \), and \( v_2(\text{Norm}(\epsilon - 1)) = 4 \). We need these facts to relate the structure of ray class groups to the regulator in the class number formula (see Section 3.2).

**Proof of Theorem 2.6** (a) Using Theorem 2.1 and Lemma 2.4, it follows that

\[
\text{Gal}(F_{m,n}/H) \cong \frac{\mathbb{Z}/2^k \mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z} \times \mathbb{Z}/2^m \mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}}{\langle -1, \tilde{\epsilon} \rangle}.
\]

Here \( \langle -1, \tilde{\epsilon} \rangle \) is the group generated by the image of \( -1 \) and \( \epsilon \) under diagonal embedding of \( E \) into \( U_{p_1}U_{p_2} \) composed with the isomorphism from Lemma 2.4. (See the Remark after Lemma 2.4) Next, we calculate \( \tilde{\epsilon} \). Let \( \epsilon_1 \in \mathbb{Z}_2 \) and \( \epsilon_2 \in \mathbb{Z}_2 \) be embeddings of \( \epsilon \) in \( U_{p_1} \) and \( U_{p_2} \). Since \( 2 \parallel \epsilon - \tilde{\epsilon} = 2U_{\sqrt{p}} \), we can assume \( v_2(\epsilon_1 - 1) = 1 \). Then \( v_2(\epsilon_2 - 1) = k + 1 \). Since the norm of \( \epsilon \) is \( -1 \), a short calculation shows that \( \epsilon_1 = 1 + 2 + 2^2 + \cdots + 2^k + 2^{k+2}r \), for some \( r \in \mathbb{Z}_2 \), and hence \( v_2(-\epsilon_1 - 1) = k + 1 \). Therefore, \( \tilde{\epsilon} = (1, \epsilon_1, 0, \epsilon_2) \).
where $e_1 \in \mathbb{Z}/2^{m-2}\mathbb{Z}$ and $e_2 \in \mathbb{Z}/2^{n-2}\mathbb{Z}$ are of order $2^{m-k-1}$ and $2^{n-k-1}$. Proposition 2.5 together with the fact that $-1 = (1,0,1,0)$ implies that

$$\text{Gal}(F_{m,n}/H) \cong \mathbb{Z}/2^{\min(m-2-(m-k-1),n-2-(n-k-1))} \times \mathbb{Z}/2^{\min(m,n)-2}\mathbb{Z}.$$ 

For the second statement, assume that $d = pq$ (if $d = p$ there is nothing to prove because $h(p)$ is odd). First, we recall that, if the extension $L = K(\sqrt{\eta})/K$ is unramified outside 2, then $(\eta) = I^2 \cdot J$, where $I$ and $J$ are ideals of $O_K$, and $J$ is a product of primes above 2. Since $p, q \equiv 5 \pmod{8}$, the primes above 2 are not principal ($x^2 - pqy^2 = \pm 2$ does not have solution mod $p$), and since they have an even order in the class group, $L$ can be either $K(\sqrt{2})$, $K(\sqrt{\epsilon})$, or $K(\sqrt{2\epsilon})$. Hence, we see that $r_2(\text{Gal}(F_{m,n}/K)) = 2$, and we can write $F_{m,n}/K$ as a product of two cyclic fields, one of them containing $H$. There is a totally real $\mathbb{Z}_2$-extension $K_2$ of $K$ (the cyclotomic extension) that is unramified outside 2. It is disjoint from $H$ by Lemma 2.2 and obviously $\text{Gal}((F_{m,n} \cap K_2) \cdot H/H) \cong \mathbb{Z}/2^{\min(m,n)-2}\mathbb{Z}$. It follows that

$$\text{Gal}(F_{m,n}/H) \cong \mathbb{Z}/2^{k+v_2(\text{Cl}(\mathbb{Q}(\sqrt{d})))} \times \mathbb{Z}/2^{\min(m,n)-2}\mathbb{Z}$$

and that $r_{2^{k+v_2(\text{Cl}(\mathbb{Q}(\sqrt{d})))}}(\mathbb{Q}(\sqrt{d})) = 2$.

(b) We argue as in (a). The difference is that now the norm of $\epsilon$ is 1. A calculation shows that we can choose $\epsilon$ such that $\epsilon_1, \epsilon_2 \equiv 5 \pmod{8}$. Now, let $\tilde{\epsilon} = (0, \epsilon_1, 0, \epsilon_2)$, where $\epsilon_1$ and $\epsilon_2$ are generators of $\mathbb{Z}/2^{m-2}\mathbb{Z}$ and $\mathbb{Z}/2^{n-2}\mathbb{Z}$. From Proposition 2.5 the first claim follows. An argument similar to the one in (a) implies the second statement.

Ray class groups unramified outside 3

Lemma 2.7. The 3-adic logarithm induces an isomorphism

$$\mathbb{Z}_3^\times \cong \frac{1 + 3\mathbb{Z}_3}{1 + 3^k\mathbb{Z}_2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^{k-1}\mathbb{Z}.$$ 

Under this map an element $\epsilon \in 1 + 3\mathbb{Z}_3$ with $v_3(\epsilon - 1) = t \leq k$ is mapped to the element of $\mathbb{Z}/3^{k-1}\mathbb{Z}$ of order $3^{k-t}$.

Theorem 2.8. If $p \equiv 1 \pmod{4}$ is prime, and if $\epsilon$ is a fundamental unit of $\mathbb{Q}(\sqrt{p})$, then

$$r_3(\mathbb{Q}(\sqrt{p})) = 1 \iff 3 \nmid h(p) \text{ and } v_3(\text{Norm}(\epsilon - 1)) = 1.$$ 

Proof. Let $m, n > 0$ be integers. We have $r_3(\mathbb{Q}(\sqrt{p})) = 1$ if and only if $3 \nmid h(p)$ and the 3-part of $\text{Gal}(F_{m,n}/H)$ is cyclic since $H$ is disjoint from the $\mathbb{Z}_3$-cyclotomic extension of $K$ by Lemma 2.3. From Theorem 2.1 and Lemma 2.7, it follows that

$$\text{Gal}(F_{m,n}/H) \cong \frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^{m-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^{n-1}\mathbb{Z}}{\langle -1, \tilde{\epsilon} \rangle}.$$
Here \((-1, \bar{\epsilon})\) is the group generated by the image of \(-1\) and \(\epsilon\) under the diagonal embedding of \(E\) into \(U_{p_1}U_{p_2}\) composed with the isomorphism from Lemma 2.7. Let \(\epsilon_1 \in \mathbb{Z}_3\) and \(\epsilon_2 \in \mathbb{Z}_3\) be embeddings of \(\epsilon\) in \(U_{p_1}\) and \(U_{p_2}\). We may choose \(\epsilon\) such that \(\epsilon_1 \equiv 1 \pmod{3}\), and \(\epsilon_2 \equiv 2 \pmod{3}\) since the norm of \(\epsilon\) is \(-1\). One may check that \((\epsilon_1 - 1)/( - \epsilon_2 - 1)\) is a unit. It follows that if \(\bar{\epsilon} = (0, e_1, 1, e_2)\), then \(e_1\) is a generator of \(\mathbb{Z}/3^{m-1}\mathbb{Z}\) if and only if \(e_2\) is a generator of \(\mathbb{Z}/3^{n-1}\mathbb{Z}\), which by Lemma 2.7 is equivalent to \(3 \parallel \epsilon_1 - 1\), or \(v_3(\text{Norm}(\epsilon - 1)) = 1\).

Remark. Hoelscher in [7] obtained interesting results about ray class groups of quadratic and cyclotomic fields unramified outside one prime.

2.2. \(L\)-values and class numbers as the coefficients of modular forms. We use modular forms to study congruences between \(L\)-values and class numbers. In this subsection we introduce modular forms whose Fourier coefficients are essentially the \(L\)-values that interest us. The main reference for this subsection is [14].

Modular forms and the Shimura correspondence ([14, pp. 52, 154]). For a positive integer \(k\), and a positive and squarefree integer \(N\), we will denote by \(M_{k+1/2}(\Gamma_0(4N))\) the space of half-integral weight modular forms of weight \(k + 1/2\) and level \(4N\), and by \(M_{k+1/2}^+(\Gamma_0(4N))\) the Kohnen plus-space. It is the subspace of \(M_{k+1/2}(\Gamma_0(4N))\) consisting of modular forms whose \(n\)th Fourier coefficient vanishes whenever \((-1)^kn \equiv 2, 3 \pmod{4}\). The significance of these subspaces is that the restriction of the Shimura correspondence to the new part of \(M_{k+1/2}^+(\Gamma_0(4N))\) defines an isomorphism of Hecke modules to the new part of \(M_{2k}(\Gamma_0(2N))\), a space of integral weight modular forms. When \(k = 6\), the map defined by the formula ([9, Theorem 1])

\[
\sum_{n \geq 0} b(n)q^n \rightarrow \frac{b(0)}{2}\zeta(-5) + \sum_{n \geq 1} \left( \sum_{d | n} d^5 b\left(\frac{n^2}{d^2}\right) \right) q^n
\]

is an isomorphism between \(M_{6+1/2}^+(\Gamma_0(4))\) and \(M_{12}(\Gamma_0(1))\). The modular form from (1.2),

\[g(z) = \sum_{n=1}^{\infty} b(n)q^n = \frac{E_4(4z)\Theta(\theta_0(z))}{2} - \frac{\Theta(E_4(4z))\theta_0(z)}{16},\]

corresponds under the above map to \(\Delta(z)\), and the Cohen–Eisenstein series \(H_{6+1/2}(z)\) corresponds to the Eisenstein series \(E_{12}(z)\).

The theta function ([14, pp. 12, 134]). A prototypical example of a half-integral weight modular form is the theta function.
**Definition 2.9.** The theta function \( \theta_0(z) \) is given by the Fourier series

\[
\theta_0(z) = 1 + 2 \sum_{n=1}^{\infty} q^{n^2} \in M_{1/2}(\Gamma_0(4)).
\]

We will be interested in

\[
\theta_0(z)^3 = \sum_{n=0}^{\infty} r(n)q^n = 1 + 6q + 12q^2 + 8q^3 + \cdots.
\]

A classical result of Gauss states that

\[
r(n) = \begin{cases} 
12H(-4n) & \text{if } n \equiv 1, 2 \pmod{4}, \\
24H(-n) & \text{if } n \equiv 3 \pmod{8}, \\
r(n/4) & \text{if } n \equiv 0 \pmod{4}, \\
0 & \text{if } n \equiv 7 \pmod{8}.
\end{cases}
\]

Here \( H(-n) \) is a Hurwitz class number. It is related to the class number \( h(-n) \) by the following formula:

\[
H(-n) = \frac{h(-D)}{w(-D)} \sum_{d|n} \mu(d) \left( \frac{-D}{d} \right) \sigma_1(f/d),
\]

where \( -N = -Df^2 \) \((-D\) is a negative fundamental discriminant\), \( w(-D) \) is half the number of units in \( \mathbb{Q}(\sqrt{-D}) \), and \( \mu(d) \) is the Möbius function.

**Cohen–Eisenstein series** ([14, p. 14]). To study special values of Dirichlet \( L \)-functions at negative integers we define Cohen–Eisenstein series.

**Definition 2.10.** If \( r \geq 2 \) is an integer, then the weight \( r + 1/2 \) Cohen–Eisenstein series is defined by

\[
H_r(z) = \sum_{N=0}^{\infty} H(r, N)q^N.
\]

Here \( H(r, N) \) is defined by

\[
H(r, N) = L(1 - r, \chi_D) \sum_{d|n} \mu(d) \chi_D(d)d^{r-1}\sigma_2r-1(n/d),
\]

where \( \chi_D(d) = \left( \frac{D}{d} \right) \). In particular, \( H(r, N) = L(1 - r, \chi_D) \) if \( D = (-1)^r N \) is a fundamental discriminant.

Cohen proved the following important result ([3]).

**Theorem 2.11.** If \( r \geq 2 \) is an integer, then \( H_r(z) \in M_{r+1/2}(\Gamma_0(4)) \).

**Sturm’s theorem** ([17, p. 171]). Sturm’s theorem states that in order to prove congruences between modular forms it is enough to check congruences between a finite number of their Fourier coefficients.
Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma)$, be a modular form of weight $k \in \mathbb{Z}$ for a congruence group $\Gamma \subset \text{SL}_2(\mathbb{Z})$ with $a(n) \in \mathcal{O}_K$, and let $m \subset \mathcal{O}_K$ be an ideal. Define
\[
\text{ord}_m(f) = \min\{n : a(n) \notin m\}.
\]

**Theorem 2.12 (Sturm).** If
\[
\text{ord}_m(f) > \frac{k}{12}[\text{SL}_2(\mathbb{Z}) : \Gamma],
\]
then $\text{ord}_m(f) = \infty$.

We will apply this result to half-integral weight modular forms. We call the quantity in the theorem the *Sturm bound* for $M_k(\Gamma)$.

**Proposition 2.13.** Let $k$ be an integer and $f(z) \in M_{k+1/2}(M,N)$. If
\[
\text{ord}_m(f) > \frac{2k+1}{24} M\phi(N) \prod_{p|\Delta} \left(1 + \frac{1}{p}\right),
\]
then $\text{ord}_m(f) = \infty$.

For the proof, we will need the following elementary lemma.

**Lemma 2.14.**
\[
[\text{SL}_2(\mathbb{Z}) : \Gamma_0(M) \cap \Gamma_1(N)] = \phi(N)M \prod_{p|\Delta} \left(1 + \frac{1}{p}\right).
\]

**Proof.** It is easy to see that the map $\Gamma_0(M) \to (\mathbb{Z}/N\mathbb{Z})^\times$ given by $(a\ b\ c\ d) \mapsto d \pmod{N}$ is surjective with kernel $\Gamma_0(M) \cap \Gamma_1(N)$. Since $[\text{SL}_2(\mathbb{Z}) : \Gamma_0(M)] = M \prod_{p|\Delta} (1 + 1/p)$, the claim follows.

**Proof of Proposition 2.13.** If $f(z) \in M_{k+1/2}(M,N)$, then $f(z)^2 \in M_{2k+1}(M,N)$. By Lemma 2.14, the Sturm bound is
\[
\frac{2k+1}{12} M \prod_{p|\Delta} \left(1 + \frac{1}{p}\right).
\]
The result follows.

### 2.3. Weight 1 Eisenstein series.

Let $p$ be prime, and let $n \geq 2$ be a positive integer. In this subsection, we construct a weight one Eisenstein series $W_n \equiv 1 \pmod{p^n}$. 
DEFINITION 2.15. For primitive Dirichlet characters \(\psi\) and \(\phi\) such that \((\psi\phi)(-1) = -1\), we define an Eisenstein series

\[
E_{1}^{\psi,\phi}(z) = \delta(\phi)L(0, \psi) + \delta(\psi)L(0, \phi) + 2\sum_{n=1}^{\infty} \sigma_{0}^{\psi,\phi}(n)q^{n}.
\]

Here \(\delta(\psi) = 1\) if \(\psi = 1\), and 0 otherwise, and the generalized divisor sum is

\[
\sigma_{0}^{\psi,\phi}(n) = \sum_{m|n} \psi\left(\frac{n}{m}\right)\phi(m).
\]

Also, for a positive integer \(t\), we define

\[
E_{1}^{\psi,\phi,t}(z) = E_{1}^{\psi,\phi}(tz).
\]

The following well known result gives a basis for the Eisenstein subspace of weight 1 (for the proof see [5, p. 141]).

THEOREM 2.16. Let \(N\) be a positive integer. Let \(A_{N}\) be a set of pairs \((\{\psi, \phi\}, t)\) where \(\psi\) and \(\phi\) are primitive Dirichlet characters of modulus \(u\) and \(v\), such that \((\psi\phi)(-1) = -1\), and \(t\) is a positive integer such that \(tuv|N\). Then the set

\[
\{E_{1}^{\psi,\phi,t}(z) : (\{\psi, \phi\}, t) \in A_{N}\}
\]

represents a basis of the Eisenstein subspace of \(M_{1}(\Gamma_{1}(N))\).

Recall that the group of Dirichlet characters of modulus \(2^{n}\) is isomorphic to \(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}\). Also, if \(\psi\) is an odd Dirichlet character of conductor \(f\), we have

\[
L(0, \psi) = -B_{1,\psi} = -\frac{1}{f} \sum_{i=0}^{f-1} \psi(i)i,
\]

where \(B_{1,\psi}\) is a generalized Bernoulli number.

THEOREM 2.17. Let \(n \geq 2\) be a positive integer, and let \(\psi\) and \(\phi\) be the generators of the group of Dirichlet characters of modulus \(2^{n}\) of order 2 and \(2^{n-2}\). Then the Eisenstein series

\[
W_{n} = \sum_{i=0}^{\infty} a_{i}q^{i} = -2 \sum_{i=0}^{2^{n-2}-1} (-1)^{i}E_{1}^{1,\psi\phi^{i}}(z) \in M_{1}(\Gamma_{1}(2^{n}))
\]

satisfies \(W_{n} \equiv 1 \pmod{2^{n}}\).

Proof. First we will check that \(a_{0} = 1\). We have

\[
a_{0} = -2 \sum_{i=0}^{2^{n-2}-1} (-1)^{i}L(0, \psi\phi^{i}) = 2 \sum_{i=0}^{2^{n-2}-1} (-1)^{i}B_{1,\psi\phi^{i}}
\]

\[
= 2 \sum_{i=0}^{2^{n-2}-1} \frac{1}{2^{n}} \sum_{c=0}^{2^{n-1}} (-1)^{i}(\psi\phi^{i})(c)c = \frac{2}{2^{n}} \sum_{c=0}^{2^{n-1}} \psi(c)c \sum_{i=0}^{2^{n-2}-1} (-1)^{i}\phi^{i}(c).
\]
For a positive integer $m$, define the polynomial

$$P_m(x) = (1 - x)(1 + x^2) \cdots (1 + x^{2^{m-1}}) = \sum_{i=0}^{2^m-1} (-1)^i x^i.$$  

Since the order of $\psi$ is $2^{n-2}$, we have $P_{n-2}(\psi(c)) = 2^{n-2}$ if $\psi(c) = -1$, and $P_{n-2}(\psi(c)) = 0$ otherwise. If $0 \leq c \leq 2^n - 1$ then $\psi(c) = -1$ implies that $c = 2^n - 1$ or $c = 2^n + 1$. In the first case, we have $\phi(c) = -1$, and in the second, we have $\phi(c) = 1$. Therefore

$$a_0 = \frac{2}{2^n} \sum_{c=2^{n-2} - 1}^{2^n-1} 2^{n-2} c\psi(c) = 1.$$  

To complete the proof, for a positive integer $j$, consider

$$a_j = -4 \sum_{i=0}^{2^{n-2} - 1} \sum_{m | j} (-1)^i \psi(m) \phi^i(m) = -4 \sum_{m | j} \psi(m) P_{n-2}(\phi(m)).$$

As before, $2^{n-2} | P_{n-2}(\phi(m))$, so the theorem follows.

Now consider prime $p > 2$. In this case the group of Dirichlet characters is cyclic.

**Theorem 2.18.** Let $n$ be a positive integer, let $p > 2$ be prime, let $\phi$ be a generator of the group of Dirichlet characters of modulus $p^n$, and let $u = -2/((p-1)(2 - p^n))$. Then the Eisenstein series

$$W_n' = \sum_{i=0}^{\infty} a_i q^i = up \sum_{i=0}^{(p-1)p^{n-1}/2 - 1} E_1^1,\phi^{2i+1}(z) \in M_1(\Gamma_1(p^n))$$

satisfies $W_n' \equiv 1 \pmod{p^n}$.

**Proof.** First we calculate $a_0$. We have

$$a_0 = up \sum_{i=0}^{(p-1)p^{n-1}/2 - 1} L(0, \phi^{2i+1}) = -up \sum_{i=0}^{(p-1)p^{n-1}/2 - 1} B_{1, \phi^{2i+1}}$$

$$= -up \sum_{i=0}^{(p-1)p^{n-1}/2 - 1} \frac{1}{p^n} \sum_{c=0}^{p^n-1} (\phi^{2i+1})(c) c = \frac{-up}{p^n} \sum_{c=0}^{p^n-1} c \sum_{i=0}^{(p-1)p^{n-1}/2 - 1} \phi^{2i+1}(c).$$

For a positive integer $m$, define the polynomial

$$P_m(x) = \sum_{i=0}^{(p-1)p^{n-1}/2 - 1} x^{2i+1}.$$  

The following identity is easy to check: $P_{m+1}(x)x^{p-1} = P_m(x^p)$.

Let $\zeta$ be a $(p-1)p^{n-1}$th root of unity. It follows from the previous identity, by an inductive argument, that if $\zeta \notin \{-1, 1\}$, then $P_n(\zeta) = 0$. 
Now we have
\[ a_0 = \frac{-up}{p^n} \sum_{c=0}^{p^n-1} cP_n(\phi(c)) = \frac{-up}{p^n}(P_n(1) + (p^n - 1)P_n(\phi(p^n - 1))) \]
\[ = \frac{-up}{p^n} \frac{(p - 1)p^{n-1}}{2}(1 - p^n + 1) = 1. \]

For a positive integer \( j \), we have
\[ (p-1)p^{n-1}/2-1 \]
\[ a_j = up \sum_{i=0}^{j} \sum_{m|j} \phi^{2i+1}(m) = up \sum_{m|j} P_n(\phi(m)). \]

Now, since \( p^{n-1} | P_n(\phi(m)) \), the theorem follows. \( \blacksquare \)

3. Proofs of the theorems

3.1. Congruences between class numbers and special values of Dirichlet \( L \)-functions. We require the notions of \( \overline{U} \)- and \( \overline{V} \)-operators and of a twist. We briefly recall these ideas.

**Definition 3.1.** If \( d \) is a positive integer, the \( \overline{U} \)- and \( \overline{V} \)-operators are given by
\[
\left( \sum_{n \geq n_0} c(n)q^n \right) | U(d) = \sum_{n \geq n_0} c(dn)q^n, \quad \left( \sum_{n \geq n_0} c(n)q^n \right) | V(d) = \sum_{n \geq n_0} c(n)q^{dn}.
\]

**Proposition 3.2.**
(a) If \( f(z) \in M_{r+1/2}(\Gamma_1(4N)) \) and if \( d \mid N \), then we have \( f(z) | U(d) \in M_{r+1/2}(\Gamma_1(4N)). \)
(b) If \( f(z) \in M_{r+1/2}(\Gamma_1(4N)) \), then \( f(z) | V(d) \in M_{r+1/2}(\Gamma_1(4Nd)) \).

**Definition 3.3.** Suppose that \( \psi \) is a Dirichlet character, and
\[ g(z) = \sum_{n=0}^{\infty} c(n)q^n \in M_{r+1/2}(\Gamma_0(4N), \chi). \]

Then the \( \psi \)-twist of \( g(z) \) is given by \( g_{\psi}(z) = \sum_{n=0}^{\infty} \psi(n)c(n)q^n \).

**Proposition 3.4.** If \( \psi \) is Dirichlet character of conductor \( m \), and if \( g(z) \) is as in the previous definition, then \( g_{\psi}(z) \in M_{r+1/2}(\Gamma_0(4Nm^2), \chi\psi^2) \).

For a power series \( f(z) = \sum c(n)q^n \), and positive integers \( a < b \) with \( \gcd(a, b) = 1 \), denote by \( f(z)_{a,b} \) the power series \( \sum_{n=a \mod b} c(n)q^n \).

**Remark.** The previous proposition implies that if \( f(z) \) is a modular form of level \( 4N \), then \( f(z)^+ = f(z)_{1,8} \) and \( f(z)^- = f(z)_{5,8} \) defined in the introduction are modular forms of level \( 256N \). In general, \( f(z)_{a,b} \) is a modular form of level \( 4Nb^2 \). In fact, it follows from Proposition 3.4 that if \( f(z) \in M_{k+1/2}(M, 2^N) \), then \( f(z)_{a,2^b} \in M_{k+1/2}(M \cdot 2^{2b}, \max(2^N, 2^{b-1})) \).
Moreover, if \( N \) is a positive integer, then \( \Theta(f(z)) \) is modular form modulo \( N \). More precisely, we find that
\[
\Theta(f(z)) \equiv \sum_{0 \leq a < N} a f(z)_{a,N} \pmod{N}.
\]

The following propositions imply Theorem 1.5

**Proposition 3.5.** The following congruences hold:

(a) We have \( 2\theta_0(z)^{3+} \equiv 59\theta_0(z)^+ + 64F_1(z) - 8H_{4+1/2}(z)^+ \pmod{128} \), where \( F_1(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_1(\Gamma_1(128)) \) is an Eisenstein series. Moreover, for prime numbers \( p \) and \( q \),
\[
\begin{align*}
a(p) &\equiv 0 \pmod{2} \quad \text{if } p \equiv 1 \pmod{16}, \\
a(p) &\equiv 1 \pmod{2} \quad \text{if } p \equiv 9 \pmod{16}, \\
a(pq) &\equiv 1 \pmod{2} \quad \text{if } p, q \equiv 3, 5 \pmod{8} \text{ and } pq \equiv 1 \pmod{8}.
\end{align*}
\]

(b) We have
\[
9(H_{3+1/2}(z)|U(3))^+ \equiv 6(\theta_0(z)^3|U(3))^+ + 2\theta_0(z)^+ + 9(\theta_0(z)|V(9))^+ \pmod{27}.
\]

**Proof.** (a) By applying Proposition 2.13 to the form
\[
2\theta_0(z)^{3+}W_6(z) - 59\theta_0(z)^+W_5(z)^4 - 64F_1(z)\theta_0(z) + 8H_{4+1/2}(z)^+ \in M_{4+1/2}(256, 128),
\]
we get Sturm’s bound 9216.

The Eisenstein subspace of \( M_1(\Gamma_1(128)) \) has dimension 80, and
\[
F_1(z) = q + q^{25} + q^{33} + q^{41} + q^{57} + q^{65} + q^{73} + 26q^{76} + 5q^{81} - 40q^{82} + 52q^{83} - 58q^{84} - 20q^{85} + 104q^{86} + 8q^{87} - 9q^{89} - 72q^{90} - 48q^{91} + 12q^{92} - 26q^{93} - 28q^{94} - 32q^{95} + 2q^{97} + 78q^{98} - 10q^{99} + O(q^{100}).
\]

Since \( F_1(z) \) is an Eisenstein series of weight 1 and level 128, it follows from Theorem 2.16 that if \( p \equiv p' \pmod{128} \) and \( q \equiv q' \pmod{128} \) are primes, then
\[
a(p) \equiv a(p') \pmod{2}, \quad a(pq) \equiv a(p'q') \pmod{2}.
\]

So to prove the second statement, one finds a prime in each relevant residue class modulo 128, and then checks the statement for these primes using a computer. To check the first two congruences, we produce Table 1. We omit the details for the congruences \( a(pq) \pmod{2} \).

(b) Proposition 2.13 implies that Sturm’s bound for the modular form
\[
9(H_{3+1/2}(z)|U(3))^+ - 6(\theta_0(z)^3|U(3))^+W_2'(z)^2 - 2\theta_0(z)^+W_2'(z)^3 - 9(\theta_0(z)|V(9))^+W_1'(z)^3 \in M_{3+1/2}(2^8 \cdot 9, 4 \cdot 9)
\]
is 16128. ■
To relate $L_p(1, \chi)$ and $L_p(1-n, \chi)$, we need the following result of Shiratani [16].

**Proposition 3.6 (Shiratani).** For a prime $p$, $p$-adic integers $s, s'$, and a Dirichlet character $\chi$ of the first kind, we have

$$L_p(s, \chi) \equiv L_p(s', \chi) \pmod{p^{v_2(s-s')-1}q^2},$$

where $q = 4$ if $p = 2$ and $q = p$ otherwise.

Proposition 3.6 implies the following corollary:

**Corollary 3.7.** If $d \neq 8$ is a positive integer (we exclude the field $\mathbb{Q}(\sqrt{2})$), then:

(a) $L_2(1, \chi_d) \equiv L_2(1 - 2^2, \chi_d) \pmod{32}$.

(b) $L_2(11, \chi_d) \equiv L_2(11 - 2^6, \chi_d) \pmod{2^9}$.

(c) $L_3(1, \chi_d) \equiv L_3(1 - 3, \chi_d) \pmod{9}$.

(d) $L_3(15, \chi_d) \equiv L_3(15 - 3^3, \chi_d) \pmod{3^4}$.

**Proposition 3.8.** Let $g(z)$ be as in (1.2).

(a) We have

$$g(z)^+ \equiv 49 \cdot 4H_{6+1/2}(z)^+ + 200 \sum_{d \equiv 1 \pmod{2}} \frac{q^{d^2}}{d^2} \pmod{2^9},$$

$$g(z)^- \equiv 39 \cdot 4H_{6+1/2}(z)^- \pmod{2^9}.$$  

(b) We have

$$g(z)^+ \equiv 369 \cdot 4H_{54+1/2}(z)^+ + 64 \cdot 27 \cdot 4H_{54+1/2}(z)_{1,16} + 4 \cdot 27 \sum_{d \equiv 1 \pmod{2}} d^4q^{d^2} + 4 \cdot 72 \sum_{d \equiv \pm 1 \pmod{8}} d^4q^{d^2} \pmod{2^{11}},$$

$$g(z)^- \equiv 7 \cdot 4H_{54+1/2}(z)^- + 64 \cdot 4H_{54+1/2}(z)_{5,16} \pmod{2^{10}}.$$

<table>
<thead>
<tr>
<th>mod 128</th>
<th>p</th>
<th>a(p)</th>
<th>mod 128</th>
<th>p</th>
<th>a(p)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>257</td>
<td>275436</td>
<td>65</td>
<td>193</td>
<td>103678</td>
</tr>
<tr>
<td>9</td>
<td>137</td>
<td>30489</td>
<td>73</td>
<td>73</td>
<td>3449</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
<td>22</td>
<td>81</td>
<td>337</td>
<td>729396</td>
</tr>
<tr>
<td>25</td>
<td>281</td>
<td>377907</td>
<td>89</td>
<td>89</td>
<td>6757</td>
</tr>
<tr>
<td>33</td>
<td>673</td>
<td>8209442</td>
<td>97</td>
<td>97</td>
<td>9326</td>
</tr>
<tr>
<td>41</td>
<td>41</td>
<td>451</td>
<td>105</td>
<td>233</td>
<td>195569</td>
</tr>
<tr>
<td>49</td>
<td>433</td>
<td>1752562</td>
<td>113</td>
<td>113</td>
<td>15540</td>
</tr>
<tr>
<td>57</td>
<td>313</td>
<td>562819</td>
<td>128</td>
<td>761</td>
<td>12342375</td>
</tr>
</tbody>
</table>
(c) We have
\[ g(z) ≡ 4 \cdot 3\Theta(H_{13+1/2}(z) \mid U(3)) + 9 \cdot 5 \sum_{d \geq 1} d^4 q^d \pmod{3^4}. \]

(d) We have
\[ g(z)^+ ≡ 5\Theta(\theta_0(z)^3 \mid U(3))^+ + \frac{15}{2} \sum_{d \equiv \pm 1 \pmod{6}} d^2 q^d \pmod{3^3}. \]

**Proof.** First note that
\[ 200 \sum_{d^2 \equiv 1 \pmod{8}} \frac{q^d}{d^2} \equiv 200 \sum_{i \equiv 1 \pmod{8}} \frac{1}{i} \theta_0(z)_{i,25} \pmod{2^9}, \]
\[ 4 \cdot 27 \sum_{d^2 \equiv 1 \pmod{8}} d^4 q^d \equiv 4 \cdot 27 \sum_{i \equiv 1 \pmod{8}} i^2 \theta_0(z)_{i,27} \pmod{2^{11}}, \]
\[ 4 \cdot 72 \sum_{d^2 \equiv 1 \pmod{16}} d^4 q^d \equiv 4 \cdot 72 \sum_{i \equiv 1 \pmod{16}} i^2 \theta_0(z)_{i,24} \pmod{2^{11}}. \]

For part (a), we apply Proposition 2.13 to the forms
\[ g(z)^+ - 49 \cdot 4H_{6+1/2}(z)^+ - 200W_4(z)^6 \sum_{i \equiv 1 \pmod{8}} \frac{1}{i} \theta_0(z)_{i,25} \in M_{6+1/2}(2^{12}, 2^4), \]
\[ g(z)^- - 39 \cdot 4H_{6+1/2}(z)^- \in M_{6+1/2}(2^8, 2^3). \]

The Sturm bounds are 26624 and 832.

For (b), we find that
\[ g(z)^+ \cdot W_7(z)^{16 \cdot 3} - 369 \cdot 4H_{54+1/2}(z)^+ - 64 \cdot 27 \cdot 4H_{54+1/2}(z)_{1,16} \]
\[ - 4 \cdot 27W_7(z)^{2 \cdot 27} \sum_{i \equiv 1 \pmod{8}} i^2 \theta_0(z)_{i,27} \]
\[ - 4 \cdot 72W_4(z)^{2 \cdot 27} \sum_{i \equiv 1 \pmod{16}} i^2 \theta_0(z)_{i,24} \in M_{54+1/2}(2^{16}, 2^7) \]

and
\[ g(z)^- \cdot W_6(z)^{16 \cdot 3} - 7 \cdot 4H_{54+1/2}(z)^- - 64 \cdot 4H_{54+1/2}(z)_{5,16} \in M_{54+1/2}(2^{10}, 2^6). \]

In this case, the Sturm bounds are 28573696 and 223232.

To prove the rest of the proposition, note that
\[ 4 \cdot 3\Theta(H_{13+1/2}(z) \mid U(3)) ≡ 4 \cdot 3 \sum_{0 < i < 81} i(H_{13+1/2}(z) \mid U(3))_{i,81} \pmod{3^4}, \]
Now a calculation as in (a) and (b) shows that we can “lift” forms from part (c) to the space \( M_{13+1/2}(4 \cdot 3^9, 4 \cdot 3^4) \) whose Sturm bound is 19131876. Similarly, we can lift forms from part (d) to the space \( M_{6+1/2}(2^8 \cdot 3^7, 2^2 \cdot 3^3) \) with Sturm bound 21835008.

### 3.2. Proofs of Theorems 1.1–1.5

**Proof of Theorem 1.5.**

If \( d \equiv 1 \pmod{8} \) is a positive fundamental discriminant, then Proposition 3.5 implies that \( 3h(-d) \equiv L(-3, \chi_d) \pmod{16} \), \( 16h(-3d) \equiv L(-2, \chi_{3d}) \pmod{3} \). Moreover, if \( d \equiv 9 \pmod{16} \) is prime, or \( d = pq \) where \( p \) and \( q \) are as in the statement of the theorem, then \( 16 \mid L(-3, \chi_d) - 3h(-d) \). To prove parts (a)–(c) of the theorem we prove the congruence \( L(-3, \chi_d) \equiv \frac{1}{3}L_2(1, \chi_d) \pmod{32} \).

To relate the Dirichlet \( L \)-function to the 2-adic \( L \)-function we need the following formula [21, p. 57]:

\[
L_2(1 - 2^n, \chi_d) = (1 - \chi_d(2)2^{2^n-1})L(1 - 2^n, \chi_d).
\]

Corollary 3.7(a) implies that

\[
L_2(1, \chi_d) \equiv L(1 - 2^2, \chi_d) \equiv (1 + \chi_d(2)2^3)L(1 - 2^2, \chi_d) \equiv 9L(-3, \chi_d) \pmod{32}
\]

since \( \chi_d(2) = 1 \) for \( d \equiv 1 \pmod{8} \). For the 3-adic \( L \)-function we have the following identity (again [21, p. 57]):

\[
L_3(1 - 3^n, \chi_d) = (1 - \chi_{3d}(3)3^{3n-1})L(1 - 3^n, \chi_{3d}).
\]

From this formula it follows that \( L_3(1 - 3, \chi_d) \equiv L(1 - 3, \chi_{3d}) \pmod{9} \). On the other hand, Corollary 3.7(c) implies that \( L_3(1, \chi_d) \equiv L(1 - 3, \chi_d) \pmod{3} \). Hence, we conclude that \( h(-3d) \equiv L_3(1, \chi_d) \pmod{3} \).

For the rest of this subsection we need the \( p \)-adic class number formula [21, p. 71]. Let \( d \equiv 1 \pmod{4} \) be a positive integer, and let \( \epsilon \) be a fundamental unit of \( \mathbb{Q}(\sqrt{d}) \). Then (up to sign)

\[
\frac{2h(d) \log_p \epsilon}{\sqrt{d}} = \left(1 - \frac{\chi_d(p)}{p}\right)^{-1}L_p(1, \chi_d).
\]
Proof of Theorem 1.1. Assume that $4 \parallel h(-p)$. Then Theorem 1.5(a) implies that $4 \parallel L_2(1, \chi_p)$. On the other hand, it follows from the 2-adic class number formula that $4 \parallel h(p) \log_2 \epsilon$. Now in the notation of Theorem 2.6 (see the Remark following the theorem), we have

$$k = v_2(\log_2 \epsilon) - 1 = 1 - v_2(h(p)).$$

Hence $r_4(\mathbb{Q}(\sqrt{p})) = 1$. Since all implications in this argument are equivalences, the claim follows. Similar arguments can be used in the other cases of the theorem. ■

Proof of Theorem 1.2. The argument is the same as for the previous theorem. In the case when $\text{Norm}(\epsilon) = 1$, we use the Remark after Theorem 2.6. ■

Proof of Theorem 1.3. Let $\epsilon$ be a fundamental unit of $\mathbb{Q}(\sqrt{p})$. We fix an embedding of $\mathbb{Q}(\sqrt{p})$ in $\mathbb{Q}_2$. Assume that $3 \nmid h(-3p)$. By Theorem 1.5(d) this is equivalent to $3 \nmid L_3(1, \chi_p)$, and by the 3-adic class number formula, it is equivalent to $3 \parallel h(p) \log_3 \epsilon$. Scholz’s result [21, p. 191] implies that $3 \nmid h(p)$. Hence, $v_3(\log_3 \epsilon) = v_3(\text{Norm}(\epsilon - 1)) = 1$ where the first equality follows from the fact that $\text{Norm}(\epsilon) = -1$ and that $v_3(\log_3 \epsilon) = v_3(\epsilon - 1)$ if $\epsilon \equiv 1 \pmod{3}$. Now Theorem 2.8 implies that $r_3(\mathbb{Q}(\sqrt{p})) = 1$.

If $r_3(\mathbb{Q}(\sqrt{p})) = 1$, then Theorem 2.8 implies $3 \nmid h(p)$ and $v_3(\text{Norm}(\epsilon - 1)) = v_3(\log_3 \epsilon) = 1$. Hence, $3 \parallel h(p) \log_3 \epsilon$, which we showed is equivalent to $3 \nmid h(-3p)$. ■

Proof of Theorem 1.4. Since $X^2 - pqY^2 = \pm 4$ has no solution mod 8 unless $X$ and $Y$ are both even, we see that $U$ and $T$ are integers. We will show that $v_2(\log_2(\epsilon)) \geq 2$. First, consider the case when $\text{Norm}(\epsilon) = -1$. If we reduce the equation $T^2 - pqU^2 = -1$ modulo 8, we immediately see that $4 \mid T$. Hence $\text{Norm}(\epsilon - 1) = -2T$. We conclude that $4 \mid \log_2(\epsilon)$. If $\text{Norm}(\epsilon) = 1$, we reduce $T^2 - pqU^2 = 1$ modulo 8 to get $T \equiv 1 \pmod{2}$. By plugging in $T = 5 + 8T'$ to the previous equation, we get

$$pqU^2 = 8(8T'^2 + 10T' + 3).$$

Hence $8 \parallel pqU^2$, which implies that $T \equiv 1 \pmod{8}$ and $v_2(\log_2(\epsilon)) \geq 2$. Note that we showed in 2.6 that $v_2(\log_2(\epsilon)) = 2$.

Theorems 1.2 and 2.6 imply that $16 \mid h(-pq)$ if and only if $v_2(h(pq) \log_2(\epsilon)) = 3$. Since $2 \mid h(pq)$ by genus theory, it follows that $16 \mid h(-pq)$ is equivalent to $2 \parallel h(pq)$ and $4 \parallel \log_2(\epsilon)$. Then Theorem 2 of [2] implies that $2 \parallel h(pq)$ happens if either $(\frac{p}{q}) = 1$ and $(\frac{p}{q}) \cdot (\frac{q}{p}) \cdot (\frac{q}{p}) = -1$, or $(\frac{p}{q}) = -1$. Finally, the result of Dirichlet [6] implies that in the first case the norm of a fundamental unit is 1, while in the second case it is $-1$. Now $\log_2(\epsilon) = 2$ implies in the first case that $T \equiv 9 \pmod{16}$ and in the second case that $T \equiv 4 \pmod{8}$. ■

Remark. The same argument reproduces the result (1.1) of Williams.
3.3. Proofs of 1.6, 1.8

Proof of Theorem 1.6. Part (b) of Proposition 3.8 implies that
\[ g(z)_{1,16} \equiv 49 \cdot 4H_{54+1/2}(z)_{1,16} \pmod{2^{11}}, \]
\[ g(z)_{5,16} \equiv 71 \cdot 4H_{54+1/2}(z)_{5,16} \pmod{2^{10}}, \]
\[ g(z)_{9,16} \equiv 369 \cdot 4H_{54+1/2}(z)_{9,16} \pmod{2^{11}}, \]
\[ g(z)_{13,16} \equiv 7 \cdot 4H_{54+1/2}(z)_{13,16} \pmod{2^{10}}, \]
\[ 3g(z) \equiv 2^{2} \cdot 3 \cdot 2 \Theta(H_{13+1/2}(z) | U(3)) \pmod{3^5}. \]

Using formulas (3.1) and (3.2), we get
\[ L_{2}(11 - 2^6, \chi_d) \equiv L(11 - 2^6, \chi_d) \pmod{2^{11}}, \]
\[ L_{3}(15 - 3^3, \chi_d) \equiv L(15 - 3^3, \chi_{3d}) \pmod{3^4}. \]

Now by recalling the interpretation of the coefficients of \( g(z) \) and \( H_{r+1/2}(z) \),
the statements follow from Corollary 3.7, parts (b) and (d).

Proof of Theorem 1.7. This follows from Proposition 3.8.

Proof of Corollary 1.8. Propositions 3.8, 3.5, and 3.6 imply that
\[ 2^9 | c(d) - 49 \cdot 4L(1 - 6, \chi_d), \quad 2^5 | 12h(-d) + 4L(1 - 4, \chi_d), \]
\[ L_{2}(1 - 6, \chi_d) \equiv L_{2}(1 - 4, \chi_d) \pmod{2^{4}}. \]

Part (a) of the corollary now follows from formula (3.1). The formula is true if we replace \( 2^n \) by any even integer. Part (b) of the corollary follows directly from part (d) of Proposition 3.8.

Acknowledgments. I would like to thank Ken Ono for suggesting this project to me, and for his comments on drafts of the paper. Also, I would like to thank Tonghai Yang for his comments and suggestions. Finally, I would like to thank the referee for his numerous helpful comments that greatly improved the exposition of this paper.

References


[22] 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.


Matija Kazalicki
Department of Mathematics
University of Wisconsin
480 Lincoln Drive
Madison, WI 53706, U.S.A.
E-mail: kazalick@math.wisc.edu

Received on 21.10.2009
and in revised form on 26.4.2010  (6180)