ACTA ARITHMETICA
147.1 (2011)

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 $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ denote its ideal class group. Starting with Gauss, who developed genus theory, many people have investigated the structure of the 2-Sylow subgroup of $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$. 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

$$h(-p) \equiv T + (p-1) \pmod{16}, \tag{1.1}$$

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 $\mathfrak{p}_1$ and $\mathfrak{p}_2$ 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

$$\mathfrak{m} = \mathfrak{p}_1^m \mathfrak{p}_2^n,$$

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

THEOREM 1.1. *Suppose that p is prime.*

(1) *If* $p \equiv 1 \pmod{16}$, *then*

$$\begin{aligned} 4 \,\|\, h(-p) &\Leftrightarrow r_4(\mathbb{Q}(\sqrt{p})) = 1, \\ 8 \,\|\, h(-p) &\Leftrightarrow r_4(\mathbb{Q}(\sqrt{p})) = 2 \textit{ and } r_8(\mathbb{Q}(\sqrt{p})) = 1, \\ 16 \mid h(-p) &\Leftrightarrow r_8(\mathbb{Q}(\sqrt{p})) = 2. \end{aligned}$$

(2) *If* $p \equiv 9 \pmod{16}$, *then*

$$\begin{aligned} 4 \,\|\, h(-p) &\Leftrightarrow r_4(\mathbb{Q}(\sqrt{p})) = 1, \\ 8 \,\|\, h(-p) &\Leftrightarrow r_8(\mathbb{Q}(\sqrt{p})) = 2, \\ 16 \mid h(-p) &\Leftrightarrow r_4(\mathbb{Q}(\sqrt{p})) = 2 \textit{ and } r_8(\mathbb{Q}(\sqrt{p})) = 1. \end{aligned}$$

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*

$$\begin{aligned} 4 \,\|\, h(-pq) &\Leftrightarrow r_4(\mathbb{Q}(\sqrt{pq})) = 1, \\ 8 \,\|\, h(-pq) &\Leftrightarrow r_8(\mathbb{Q}(\sqrt{pq})) = 2, \\ 16 \mid h(-pq) &\Leftrightarrow r_4(\mathbb{Q}(\sqrt{pq})) = 2 \textit{ and } r_8(\mathbb{Q}(\sqrt{pq})) = 1. \end{aligned}$$

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 $\left(\frac{p}{q}\right)$ and $\left(\frac{p}{q}\right)_4$ the quadratic and quartic residue symbol.

THEOREM 1.4. *If p and q are primes for which* $p, q \equiv 5 \pmod 8$, *then*

$$16 \mid h(-pq) \Leftrightarrow \begin{cases} T \equiv 9 \pmod{16} & \textit{if } \left(\frac{p}{q}\right) = 1 \textit{ and } \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = -1, \\ T \equiv 4 \pmod 8 & \textit{if } \left(\frac{p}{q}\right) = -1, \end{cases}$$

where $T + U\sqrt{pq}$ is a fundamental unit of $\mathbb{Q}(\sqrt{pq})$. When $\mathrm{Norm}(\epsilon) = -1$, *we choose the fundamental unit such that* $T \equiv 1 \pmod 4$.

REMARK. If $p, q \equiv 3 \pmod 8$ then $4 \,\|\, h(-pq)$. 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* $16 \mid \big(\frac{1}{9}L_2(1,\chi_p) + 3h(-p)\big)$.
(b) *If* $p \equiv 9 \pmod{16}$, *then* $8 \parallel \big(\frac{1}{9}L_2(1,\chi_p) + 3h(-p)\big)$.
(c) *If* $pq \equiv 1 \pmod 8$ *and* $p, q \equiv 3, 5 \pmod 8$, *then* $8 \parallel \big(\frac{1}{9}L_2(1,\chi_{pq}) + 3h(-pq)\big)$.
(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 $\sigma_k(n) = \sum_{d \mid n} d^k$ the sum of kth 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]:

$$\begin{aligned}
\tau(n) &\equiv \sigma_{11}(n) \pmod{2^{11}} && \text{if } n \equiv 1 \pmod 8,\\
\tau(n) &\equiv 1217\sigma_{11}(n) \pmod{2^{13}} && \text{if } n \equiv 3 \pmod 8,\\
\tau(n) &\equiv 1537\sigma_{11}(n) \pmod{2^{12}} && \text{if } n \equiv 5 \pmod 8,\\
\tau(n) &\equiv 705\sigma_{11}(n) \pmod{2^{14}} && \text{if } n \equiv 7 \pmod 8.
\end{aligned}$$

By the work of Eichler, Shimura, Deligne and Serre, for every prime l there is a 2-dimensional l-adic Galois representation $\rho_l : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_l)$ with the property that $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = \tau(p)$ for every prime $p \neq l$ ($\mathrm{Frob}_p \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 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 ρ_2. More precisely, up to conjugation by an element of $\mathrm{GL}_2(\mathbb{Q}_2)$, the image of ρ_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 ρ_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 Δ_d the twist of $\Delta(z)$ by the quadratic character $\left(\frac{d}{\cdot}\right)$. Square roots of the algebraic parts $\sqrt{L^{\mathrm{alg}}(\Delta_d, 6)}$ will be defined later in this section. We prove the following theorem.

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

$$\begin{aligned}
\sqrt{L^{\mathrm{alg}}(\Delta_d, 6)} &\equiv 49 \cdot 4L_2(11, \chi_d) \pmod{2^9} && \text{for } d \equiv 1 \pmod{16},\\
\sqrt{L^{\mathrm{alg}}(\Delta_d, 6)} &\equiv 71 \cdot 4L_2(11, \chi_d) \pmod{2^9} && \text{for } d \equiv 5 \pmod{16},\\
\sqrt{L^{\mathrm{alg}}(\Delta_d, 6)} &\equiv 369 \cdot 4L_2(11, \chi_d) \pmod{2^9} && \text{for } d \equiv 9 \pmod{16},\\
\sqrt{L^{\mathrm{alg}}(\Delta_d, 6)} &\equiv 7 \cdot 4L_2(11, \chi_d) \pmod{2^9} && \text{for } d \equiv 13 \pmod{16},\\
\sqrt{L^{\mathrm{alg}}(\Delta_d, 6)} &\equiv d \cdot 12L_3(15, \chi_d) \pmod{3^4} && \text{for all } d.
\end{aligned}$$

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 $S^{\mathrm{new}}_{6+1/2}(\Gamma_0(4))$ associated to $\Delta(z)$ is

$$g(z) = \sum_{n=1}^{\infty} b(n)q^n = \frac{E_4(4z)\Theta(\theta_0(z))}{2} - \frac{\Theta(E_4(4z))\theta_0(z)}{16}, \tag{1.2}$$

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

$$\Theta\Big(\sum_{n=0}^{\infty} a(n)q^n\Big) = \sum_{n=0}^{\infty} na(n)q^n.$$

Now the Kohnen–Waldspurger theorem for positive fundamental discriminants d implies that

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

(where $\langle\cdot,\cdot\rangle$ is the standard Petersson inner product). We define the algebraic part of $L(\Delta_d,6)$ to be $L^{\mathrm{alg}}(\Delta_d,6):=b(d)^2$, and we define the square root of the algebraic part to be $\sqrt{L^{\mathrm{alg}}(\Delta_d,6)}:=b(d)$. 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 $D=(-1)^rN$ 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

$$f(z)\equiv' g(z)\pmod N\ \Leftrightarrow\ f(z)-g(z)\equiv h(z)\pmod N$$

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

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

the modular forms obtained by "twisting".

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

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

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 $2^5\mid\sqrt{L^{\mathrm{alg}}(\Delta_d,6)}+12h(-d)$.*
(b) *If $d\equiv 1\pmod 8$, then $3^3\mid\sqrt{L^{\mathrm{alg}}(\Delta_d,6)}-120d\cdot H(-3d)$.*

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 $\mathfrak{p}$ of K, denote by $U_\mathfrak{p}$ the group of units of the completion $K_\mathfrak{p}$. Fix a rational prime P that splits in K. Denote by $\mathfrak{p}_1$ and $\mathfrak{p}_2$ primes of K above P. For integers $m, n \geq 0$ let $F_{m,n}$ be the ray class field of K of modulus $\mathfrak{m} = \mathfrak{p}_1^m \mathfrak{p}_2^n$. Let

$$U_{m,n} = (1+\mathfrak{p}_1^m)(1+\mathfrak{p}_2^n), \quad U = \prod U_\mathfrak{p}, \quad U' = \prod_{\mathfrak{p}|P} U_\mathfrak{p}, \quad U'' = \prod_{\mathfrak{p}\nmid P} U_\mathfrak{p}$$

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 $U' = U_{\mathfrak{p}_1}U_{\mathfrak{p}_2}$ 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 $\mathrm{Gal}(F_{m,n}/H)$ and $\mathrm{Cl}(K)$ separately. It is easy to describe the structure of $\mathrm{Gal}(F_{m,n}/H)$ using the idelic formalism (see [21, pp. 269, 396]).

THEOREM 2.1. *Using the notation above we have*

$$\mathrm{Gal}(F_{m,n}/H) \cong \Big(\prod_{\mathfrak{p}|p} U_\mathfrak{p}\Big)/\bar{E}U_{m,n}.$$

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

$$\begin{aligned}\mathrm{Gal}(F_{m,n}/H) &\cong K^\times U/K^\times U''U_{m,n} \cong (K^\times U''U_{m,n})U'/K^\times U''U_{m,n}\\ &\cong U'/(U' \cap K^\times U''U_{m,n}).\end{aligned}$$

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 $\bar{\epsilon} = \epsilon\big(\frac{\bar{\epsilon}}{\epsilon}\big) \in K^\times U''$. For the other direction, let $x \in K^\times$, $u'' \in U''$ and $u \in U_{m,n}$. Suppose that $xu''u \in U'$. First, observe that x is a unit since it is a local unit for every finite place. Next, note that $xu'' \in \bar{E}$. Hence, we have $xu''u \in \bar{E}U_{m,n}$. ∎

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 $\mathrm{Gal}(F/K) \cong \mathbb{Z}/p\mathbb{Z}$.

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 $\mathbb{Q}(\sqrt{2}, \sqrt{d})/\mathbb{Q}(\sqrt{d})$. ∎

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 $\mathbb{Q}(\sqrt{d})$. ∎

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

Ray class groups unramified outside 2. In this case $U_{\mathfrak{p}} \cong \mathbb{Z}_2^{\times} = 1 + 2\mathbb{Z}_2$, 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 ϵ *with* $2 \le v_2(\epsilon - 1) = t \le k$ *is mapped to the element of* $\mathbb{Z}/2^{k-2}\mathbb{Z}$ *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^{l_1} *and* 2^{l_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 $\epsilon = (1, g_1, g_2^{2^{k_2-l_2-(k_1-l_1)}}) \in G$ 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 ϵ^r is not a power of ϵ_1 for $0 < r < 2^{k_1-l_1}$, so it is not in H. Also, the G_0 component of ϵ is 1, so ϵ 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* $\epsilon = T + U\sqrt{d}$ $(T, U \in \mathbb{Z})$ *be a fundamental unit of* K, *and let* $k = v_2(\mathrm{Norm}(\epsilon - 1)) - 2$.

(a) *If* $d \equiv 1 \pmod 8$ *is prime, or a product of two primes* $p, q \equiv 5 \pmod 8$, *if* $\mathrm{Norm}(\epsilon) = -1$, *and if* $m, n \geq 2$ *are integers, then*
$$\mathrm{Gal}(F_{m,n}/H) \cong \mathbb{Z}/2^k\mathbb{Z} \times \mathbb{Z}/2^{\min(m,n)-2}\mathbb{Z}.$$
In particular,
$$r_{2^{k+v_2(\mathrm{Cl}(\mathbb{Q}(\sqrt{d})))}}(\mathbb{Q}(\sqrt{d})) = 2.$$

(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* $\mathrm{Norm}(\epsilon) = 1$, *then*
$$\mathrm{Gal}(F_{m,n}/H) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\min(m,n)-2}\mathbb{Z}.$$
In particular,
$$r_{2^{1+v_2(\mathrm{Cl}(\mathbb{Q}(\sqrt{d})))}}(\mathbb{Q}(\sqrt{d})) = 2.$$

REMARK. It is easy to show that if $\mathrm{Norm}(\epsilon) = -1$, then $v_2(\mathrm{Norm}(\epsilon - 1)) = v_2(\log_2 \epsilon) + 1$. From the proof of part (b), we will see that for suitable ϵ, $v_2(\log_2 \epsilon) = 2$, and $v_2(\mathrm{Norm}(\epsilon - 1)) = 4$. 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
$$\mathrm{Gal}(F_{m,n}/H) \cong \frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}}{\langle -1, \tilde{\epsilon} \rangle}.$$
Here $\langle -1, \tilde{\epsilon} \rangle$ is the group generated by the image of -1 and ϵ under diagonal embedding of E into $U_{\mathfrak{p}_1} U_{\mathfrak{p}_2}$ 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 ϵ in $U_{\mathfrak{p}_1}$ and $U_{\mathfrak{p}_2}$. Since $2 \parallel \epsilon - \bar{\epsilon} = 2U\sqrt{p}$, we can assume $v_2(\epsilon_1 - 1) = 1$. Then $v_2(\epsilon_2 - 1) = k + 1$. Since the norm of ϵ 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, $\tilde{\epsilon} = (1, e_1, 0, e_2)$

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

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

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 $r_2(\mathrm{Gal}(F_{m,n}/K)) = 2$, 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 $\mathrm{Gal}((F_{m,n} \cap K_2) \cdot H/H) \cong \mathbb{Z}/2^{\min(m,n)-2}\mathbb{Z}$. It follows that

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

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

(b) We argue as in (a). The difference is that now the norm of ϵ is 1. A calculation shows that we can choose ϵ such that $\epsilon_1, \epsilon_2 \equiv 5 \pmod 8$. Now, let $\tilde{\epsilon} = (0, e_1, 0, e_2)$, where e_1 and e_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*

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

Under this map an element $\epsilon \in 1+3\mathbb{Z}_3$ with $v_3(\epsilon - 1) = t \le k$ 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 ϵ is a fundamental unit of $\mathbb{Q}(\sqrt{p})$, then*

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

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 $\mathrm{Gal}(F_{m,n}/H)$ 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

$$\mathrm{Gal}(F_{m,n}/H) \cong \frac{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^{m-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^{n-1}\mathbb{Z}}{\langle -1, \tilde{\epsilon}\rangle}.$$

Here $\langle -1, \tilde{\epsilon}\rangle$ is the group generated by the image of -1 and ϵ under the diagonal embedding of E into $U_{\mathfrak{p}_1}U_{\mathfrak{p}_2}$ 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 ϵ in $U_{\mathfrak{p}_1}$ and $U_{\mathfrak{p}_2}$. We may choose ϵ such that $\epsilon_1 \equiv 1 \pmod 3$, and $\epsilon_2 \equiv 2 \pmod 3$ since the norm of ϵ is -1. One may check that $(\epsilon_1 - 1)/(-\epsilon_2 - 1)$ is a unit. It follows that if $\tilde{\epsilon} = (0, e_1, 1, e_2)$, 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 $v_3(\mathrm{Norm}(\epsilon - 1)) = 1$. ∎

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 nth Fourier coefficient vanishes whenever $(-1)^k n \equiv 2, 3 \pmod 4$. The significance of these subspaces is that the restriction of 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])

$$\sum_{n\ge 0} b(n)q^n \to \frac{b(0)}{2}\zeta(-5) + \sum_{n\ge 1}\Big(\sum_{d\mid n} d^5 b\Big(\frac{n^2}{d^2}\Big)\Big)q^n$$

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:

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

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 $\Gamma<\mathrm{SL}_2(\mathbb{Z})$ with $a(n)\in\mathcal{O}_K$, and let $\mathfrak{m}\subset\mathcal{O}_K$ be an ideal. Define

$$\mathrm{ord}_{\mathfrak{m}}(f)=\min\{n:a(n)\notin\mathfrak{m}\}.$$

THEOREM 2.12 (Sturm). *If*

$$\mathrm{ord}_{\mathfrak{m}}(f)>\frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}):\Gamma],$$

then $\mathrm{ord}_{\mathfrak{m}}(f)=\infty$.

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

Let N, M and $2k$ be integers. Assume $4\mid N$ and $N\mid M$. We define

$$M_k(M,N)=\bigoplus_{\chi}M_k(\Gamma_0(M),\chi),$$

where the sum is over all Dirichlet characters of conductor dividing N.

PROPOSITION 2.13. *Let k be an integer and $f(z)\in M_{k+1/2}(M,N)$. If*

$$\mathrm{ord}_{\mathfrak{m}}(f)>\frac{2k+1}{24}M\phi(N)\prod_{p\mid M}\left(1+\frac{1}{p}\right),$$

then $\mathrm{ord}_{\mathfrak{m}}(f)=\infty$.

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

LEMMA 2.14.

$$[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(M)\cap\Gamma_1(N)]=\phi(N)M\prod_{p\mid M}\left(1+\frac{1}{p}\right).$$

Proof. It is easy to see that the map $\Gamma_0(M)\to(\mathbb{Z}/N\mathbb{Z})^\times$ given by $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\mapsto d\pmod N$ is surjective with kernel $\Gamma_0(M)\cap\Gamma_1(N)$. Since $[\mathrm{SL}_2(\mathbb{Z}):\Gamma_0(M)]=M\prod_{p\mid M}(1+1/p)$, 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

$$\frac{2k+1}{12}M\prod_{p\mid M}\left(1+\frac{1}{p}\right).$$

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 ψ and ϕ 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 $\psi = \mathbf{1}$, 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 ψ and ϕ are primitive Dirichlet characters of modulus u and v, such that $(\psi\phi)(-1) = -1$, and t is a positive integer such that $tuv \mid N$. 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 ψ 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 ψ and ϕ be the generators of the group of Dirichet characters of modulus 2^n of order 2 and 2^{n-2}. Then the Eisenstein series*

$$W_n = \sum_{i=0}^{\infty} a_i q^i = -2\sum_{i=0}^{2^{n-2}} (-1)^i E_1^{\mathbf{1},\psi\phi^i}(z) \in M_1(\Gamma_1(2^n))$$

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 ψ 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 $0 \le c \le 2^n - 1$ then $\psi(c) = -1$ implies that $c = 2^{n-2} - 1$ or $c = 2^{n-2} + 1$. In the first case, we have $\phi(c) = -1$, and in the second, we have $\phi(c) = 1$. Therefore

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

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

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

As before, $2^{n-2} \mid P_{n-2}(\phi(m))$, 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 ϕ 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*

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

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

Proof. First we calculate a_0. We have

$$\begin{aligned} a_0 &= up \sum_{i=0}^{(p-1)p^{n-1}/2-1} L(0,\phi^{2i+1}) = -up \sum_{i=0}^{(p-1)p^{n-1}/2-1} B_{1,\phi^{2i+1}} \\ &= -up \sum_{i=0}^{(p-1)p^{n-1}/2-1} \frac{1}{p^n} \sum_{c=0}^{p^n-1} (\phi^{2i+1})(c)c = \frac{-up}{p^n} \sum_{c=0}^{p^n-1} c \sum_{i=0}^{(p-1)p^{n-1}/2-1} \phi^{2i+1}(c). \end{aligned}$$

For a positive integer m, define the polynomial

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

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

Let ζ 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

$$\begin{aligned} a_0 &= \frac{-up}{p^n}\sum_{c=0}^{p^n-1} cP_n(\phi(c)) = \frac{-up}{p^n}(P_n(1)+(p^n-1)P_n(\phi(p^n-1))) \\ &= \frac{-up}{p^n}\,\frac{(p-1)p^{n-1}}{2}(1-p^n+1) = 1. \end{aligned}$$

For a positive integer j, we have

$$a_j = up\sum_{i=0}^{(p-1)p^{n-1}/2-1}\sum_{m\mid j}\phi^{2i+1}(m) = up\sum_{m\mid j}P_n(\phi(m)).$$

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

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

$$\Big(\sum_{n\ge n_0} c(n)q^n\Big)\,|\,U(d) = \sum_{n\ge n_0} c(dn)q^n, \qquad \Big(\sum_{n\ge n_0} c(n)q^n\Big)\,|\,V(d) = \sum_{n\ge n_0} c(n)q^{dn}.$$

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

PROPOSITION 3.4. *If ψ 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 $\sum_{n\equiv a\,(\mathrm{mod}\,b)} c(n)q^n$.

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

$$\Theta(f(z)) \equiv \sum_{0\le a<N} af(z)_{a,N} \pmod{N}.$$

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,

$$\begin{aligned} a(p) &\equiv 0 \pmod{2} && \text{if } p \equiv 1 \pmod{16},\\ a(p) &\equiv 1 \pmod{2} && \text{if } p \equiv 9 \pmod{16},\\ a(pq) &\equiv 1 \pmod{2} && \text{if } p,q \equiv 3,5 \pmod{8} \text{ and } pq \equiv 1 \pmod{8}.\end{aligned}$$

(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

$$\begin{aligned} F_1(z) = q &+ q^{25} + q^{33} + q^{41} + q^{57} + q^{65} + q^{73} + 26q^{76} + 5q^{81} - 40q^{82} + 52q^{83}\\ &- 58q^{84} - 20q^{85} + 104q^{86} + 8q^{87} - 9q^{89} - 72q^{90} - 48q^{91} + 12q^{92}\\ &- 26q^{93} - 28q^{94} - 32q^{95} + 2q^{97} + 78q^{98} - 10q^{99} + O(q^{100}).\end{aligned}$$

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

$$a(p) \equiv a(p') \pmod{2}, \qquad a(pq) \equiv a(p'q') \pmod{2}.$$

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 $a(pq)$ mod 2.

(b) Proposition 2.13 implies that Sturm's bound for the modular form

$$\begin{aligned} 9(H_{3+1/2}(z)\,|\,U(3))^+ - 6(\theta_0(z)^3\,|\,U(3))^+W_2'(z)^2 - 2\theta_0(z)^+W_2'(z)^3&\\ - 9(\theta_0(z)\,|\,V(9))^+W_1'(z)^3 \in M_{3+1/2}(2^8\cdot 9, 4\cdot 9)&\end{aligned}$$

is 16128. ∎

Table 1

mod 128	p	$a(p)$	mod 128	p	$a(p)$
1	257	275436	65	193	103678
9	137	30489	73	73	3449
17	17	22	81	337	729396
25	281	377907	89	89	6757
33	673	8209442	97	97	9326
41	41	451	105	233	195569
49	433	1752562	113	113	15540
57	313	562819	128	761	12342375

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 χ 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*

$$g(z)^+ \equiv 49 \cdot 4H_{6+1/2}(z)^+ + 200 \sum_{d\equiv 1 \,(\mathrm{mod}\, 2)} \frac{q^{d^2}}{d^2} \pmod{2^9},$$
$$g(z)^- \equiv 39 \cdot 4H_{6+1/2}(z)^- \pmod{2^9}.$$

(b) *We have*

$$\begin{aligned} g(z)^+ \equiv{}& 369 \cdot 4H_{54+1/2}(z)^+ + 64 \cdot 27 \cdot 4H_{54+1/2}(z)_{1,16} \\ &+ 4 \cdot 27 \sum_{d\equiv 1 \,(\mathrm{mod}\, 2)} d^4 q^{d^2} + 4 \cdot 72 \sum_{d\equiv \pm 1 \,(\mathrm{mod}\, 8)} d^4 q^{d^2} \pmod{2^{11}}, \end{aligned}$$
$$g(z)^- \equiv 7 \cdot 4H_{54+1/2}(z)^- + 64 \cdot 4H_{54+1/2}(z)_{5,16} \pmod{2^{10}}.$$

(c) *We have*

$$g(z) \equiv 4 \cdot 3\Theta(H_{13+1/2}(z) \,|\, U(3)) + 9 \cdot 5 \sum_{d \ge 1} d^4 q^{d^2} \pmod{3^4}.$$

(d) *We have*

$$g(z)^+ \equiv 5\Theta(\theta_0(z)^3 \,|\, U(3))^+ + \frac{15}{2} \sum_{d \equiv \pm 1 \,(\mathrm{mod}\, 6)} d^2 q^{d^2} \pmod{3^3}.$$

Proof. First note that

$$200 \sum_{d^2 \equiv 1 \,(\mathrm{mod}\, 8)} \frac{q^{d^2}}{d^2} \equiv 200 \sum_{\substack{i \equiv 1 \,(\mathrm{mod}\, 8) \\ 0<i<2^5}} \frac{1}{i} \theta_0(z)_{i,2^5} \pmod{2^9},$$

$$4 \cdot 27 \sum_{d^2 \equiv 1 \,(\mathrm{mod}\, 8)} d^4 q^{d^2} \equiv 4 \cdot 27 \sum_{\substack{i \equiv 1 \,(\mathrm{mod}\, 8) \\ 0<i<2^7}} i^2 \theta_0(z)_{i,2^7} \pmod{2^{11}},$$

$$4 \cdot 72 \sum_{d^2 \equiv 1 \,(\mathrm{mod}\, 16)} d^4 q^{d^2} \equiv 4 \cdot 72 \sum_{\substack{i \equiv 1 \,(\mathrm{mod}\, 16) \\ 0<i<2^4}} i^2 \theta_0(z)_{i,2^4} \pmod{2^{11}}.$$

For part (a), we apply Proposition 2.13 to the forms

$$g(z)^+ - 49 \cdot 4H_{6+1/2}(z)^+ - 200W_4(z)^6 \sum_{\substack{i \equiv 1 \,(\mathrm{mod}\, 8) \\ 0<i<2^5}} \frac{1}{i} \theta_0(z)_{i,2^5} \in M_{6+1/2}(2^{12}, 2^4),$$

$$g(z)^- - 39 \cdot 4H_{6+1/2}(z)^- \in M_{6+1/2}(2^8, 2^3).$$

The Sturm bounds are 26624 and 832.

For (b), we find that

$$\begin{aligned} g(z)^+ \cdot W_7(z)^{16\cdot 3} &- 369 \cdot 4H_{54+1/2}(z)^+ - 64 \cdot 27 \cdot 4H_{54+1/2}(z)_{1,16} \\ &- 4 \cdot 27 W_7(z)^{2\cdot 27} \sum_{\substack{i \equiv 1 \,(\mathrm{mod}\, 8) \\ 0<i<2^7}} i^2 \theta_0(z)_{i,2^7} \\ &- 4 \cdot 72 W_4(z)^{2\cdot 27} \sum_{\substack{i \equiv 1 \,(\mathrm{mod}\, 16) \\ 0<i<2^4}} i^2 \theta_0(z)_{i,2^4} \in M_{54+1/2}(2^{16}, 2^7) \end{aligned}$$

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

$$4 \cdot 3\Theta(H_{13+1/2}(z) \,|\, U(3)) \equiv 4 \cdot 3 \sum_{0<i<81} i(H_{13+1/2}(z) \,|\, U(3))_{i,81} \pmod{3^4},$$

$$9\cdot 5\sum_{d\ge 1} d^4 q^{d^2} \equiv 9\cdot 5 \sum_{0\le i<9} i^2\cdot \frac{1}{2}\theta_0(z)_{i,9} \pmod{3^4},$$
$$5\Theta(\theta_0(z)^3\,|\,U(3))^+ \equiv 5\sum_{0\le i<27} i(\theta_0(z)^3\,|\,U(3))^+_{i,27} \pmod{3^3},$$
$$\frac{15}{2}\sum_{d^2\equiv 1 \,(\mathrm{mod}\, 3\cdot 8)} d^2 q^{d^2} \equiv \frac{15}{2}\sum_{\substack{i\equiv 1\,(\mathrm{mod}\,24)\\ 0\le i<9}} i\theta_0(z)_{i,9} \pmod{3^3}.$$

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 $16 \parallel L(-3,\chi_d)-3h(-d)$. To prove parts (a)–(c) of the theorem we prove the congruence $L(-3,\chi_d)\equiv \frac{1}{9}L_2(1,\chi_d) \pmod{32}$.

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

$$L_2(1-2^n,\chi_d) = (1-\chi_d(2)2^{2^n-1})L(1-2^n,\chi_d). \tag{3.1}$$

Corollary 3.7(a) implies that

$$\begin{aligned} L_2(1,\chi_d) &\equiv L(1-2^2,\chi_d) \equiv (1+\chi_d(2)2^3)L(1-2^2,\chi_d)\\ &\equiv 9L(-3,\chi_d) \pmod{32}\end{aligned}$$

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])

$$L_3(1-3^n,\chi_d) = (1-\chi_{3d}(3)3^{3^n-1})L(1-3^n,\chi_{3d}). \tag{3.2}$$

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 $L_3(1,\chi_d)\equiv L(1-3,\chi_d) \pmod 9$. 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 ϵ 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 $4 \,\|\, h(-p)$. Then Theorem 1.5(a) implies that $4 \,\|\, L_2(1, \chi_p)$. On the other hand, it follows from the 2-adic class number formula that $4 \,\|\, h(p) \log_2 \epsilon$. 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 $\mathrm{Norm}(\epsilon) = 1$, we use the Remark after Theorem 2.6. ∎

Proof of Theorem 1.3. Let ϵ 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 $3 \,\|\, h(p) \log_3 \epsilon$. Scholtz's result [21, p. 191] implies that $3 \nmid h(p)$. Hence, $v_3(\log_3 \epsilon) = v_3(\mathrm{Norm}(\epsilon - 1)) = 1$ where the first equality follows from the fact that $\mathrm{Norm}(\epsilon) = -1$ 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 $v_3(\mathrm{Norm}(\epsilon - 1)) = v_3(\log_3 \epsilon) = 1$. Hence, $3 \,\|\, h(p) \log_3 \epsilon$, 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 $\mathrm{Norm}(\epsilon) = -1$. If we reduce the equation $T^2 - pqU^2 = -1$ modulo 8, we immediately see that $4 \mid T$. Hence $\mathrm{Norm}(\epsilon - 1) = -2T$. We conclude that $4 \mid \log_2(\epsilon)$. If $\mathrm{Norm}(\epsilon) = 1$, we reduce $T^2 - pqU^2 = 1$ modulo 8 to get $T \equiv 1 \pmod 4$. By plugging in $T = 5 + 8T'$ to the previous equation, we get

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

Hence $8 \,\|\, pqU^2$, 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 $16 | h(-pq)$ 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 $2 \,\|\, h(pq)$ and $4 \,\|\, \log_2(\epsilon)$. Then Theorem 2 of [2] implies that $2 \,\|\, h(pq)$ happens if either $\left(\frac{p}{q}\right) = 1$ and $\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = -1$, or $\left(\frac{p}{q}\right) = -1$. 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

$$\begin{aligned} g(z)_{1,16} &\equiv' 49 \cdot 4H_{54+1/2}(z)_{1,16} \pmod{2^{11}}, \\ g(z)_{5,16} &\equiv' 71 \cdot 4H_{54+1/2}(z)_{5,16} \pmod{2^{10}}, \\ g(z)_{9,16} &\equiv' 369 \cdot 4H_{54+1/2}(z)_{9,16} \pmod{2^{11}}, \\ g(z)_{13,16} &\equiv' 7 \cdot 4H_{54+1/2}(z)_{13,16} \pmod{2^{10}}, \\ 3g(z) &\equiv' 2^2 \cdot 3^2 \Theta(H_{13+1/2}(z) \,|\, U(3)) \pmod{3^5}. \end{aligned}$$

Using formulas (3.1) and (3.2), we get

$$\begin{aligned} L_2(11-2^6, \chi_d) &\equiv L(11-2^6, \chi_d) \pmod{2^{11}}, \\ L_3(15-3^3, \chi_d) &\equiv L(15-3^3, \chi_{3d}) \pmod{3^4}. \end{aligned}$$

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

$$2^9 \mid c(d) - 49 \cdot 4L(1-6, \chi_d), \qquad 2^5 \mid 12h(-d) + 4L(1-4, \chi_d),$$
$$L_2(1-6, \chi_d) \equiv L_2(1-4, \chi_d) \pmod{2^4}.$$

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

[1] P. Barrucand and H. Cohn, *Note on primes of type $x^2 + 32y^2$, class number, and residuacity*, J. Reine Angew. Math. 238 (1969), 67–70.

[2] E. Brown, *Class numbers of real quadratic number fields*, Trans. Amer. Math. Soc. 190 (1974), 99–107.

[3] H. Cohen, *Sums involving the values at negative integers of L-functions of quadratic characters*, Math. Ann. 217 (1975), 271–285.

[4] B. Datskovsky and P. Guerzhoy, *On Ramanujan congruences for modular forms of integral and half-integral weights*, Proc. Amer. Math. Soc. 124 (1996), 2283–2291.

[5] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, 2005.

[6] P. G. L. Dirichlet, *Einige neue Sätze über unbestimmte Gleichungen*, Abh. K. Preuss. Akad. Wiss. 1834, 649–664.

[7] J. L. Hoelscher, *Ray class groups of quadratic and cyclotomic fields*, Int. J. Number Theory 6 (2010), 1169–1182.

[8] N. Koblitz, *p-adic congruences and modular forms of half integer weight*, Math. Ann. 274 (1986), 199–220.

[9] W. Kohnen, *Modular forms of half-integral weight on* $\Gamma_0(4)$, ibid. 248 (1980), 249–266.

[10] O. Kolberg, *Congruences for Ramanujan's function* $\tau(n)$, Arbok Univ. Bergen Mat.-Natur. Ser. 1962, no. 11.

[11] Y. Maeda, *A congruence between modular forms of half-integral weight*, Hokkaido Math. J. 12 (1983), 64–73.

[12] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[13] —, *On the arithmetic of special values of L functions*, Invent. Math. 55 (1979), 207–240.

[14] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-Series*, CBMS Reg. Conf. Ser. Math. 102, Amer. Math. Soc., 2003.

[15] D. C. Shanks, P. J. Sime and L. C. Washington, *Zeros of 2-adic L-functions and congruences for class numbers and fundamental units*, Math. Comp. 68 (1999), 1243–1255.

[16] K. Shiratani, *On certain values of p-adic L-functions*, Mem. Fac. Sci. Kyushu Univ. Ser. A 28 (1974), 59–82.

[17] W. Stein, *Modular Forms, a Computational Approach*, Grad. Stud. Math. 79, Amer. Math. Soc., 2007.

[18] P. Stevenhagen, *Divisibility by 2-powers of certain quadratic class numbers*, J. Number Theory 43 (1993), 1–19.

[19] H. P. F. Swinnerton-Dyer, *On l-adic representations and congruences for coefficients of modular forms*, in: Modular Functions of One Variable, III (Antwerp, 1972), Lecture Notes in Math. 350, Springer, 1973, 1–55.

[20] V. Vatsal, *Canonical periods and congruence formulae*, Duke Math. J. 98 (1999), 397–419.

[21] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

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

[23] Y. Yamamoto, *Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic*, Osaka J. Math. 21 (1984), 1–22.

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)