ACTA ARITHMETICA
LXI.2 (1992)

Modular forms and class number congruences

by

Antone Costa* (Washington, D.C.)

1. Introduction. Let D be a squarefree integer, and let $h(D)$, $C(D)$ be the class number and classgroup of $\mathbb{Q}(\sqrt{D})$, respectively. The theory of genera, due to Gauss, readily determines the 2-rank of $C(D)$, and in a series of articles from the 1930's, Rédei [17] develops the machinery necessary to compute both the 4- and 8-ranks. For example, if $p \equiv 1 \bmod 4$ is a prime integer, then 2-$C(-p)$, the 2-Sylow subgroup of $C(-p)$ has both 2-rank and 4-rank one, and, in fact, we have

$$(a) \quad h(-p) \equiv 0 \bmod 8 \quad \text{iff } (1-i \,|\, p) = 1\,, \text{ i.e. iff } 1-\sqrt{-1} \text{ is a square mod } p.$$

In 1969, Barrucand and Cohn [2] reinterpreted this result, using the arithmetic of $\mathbb{Q}(\sqrt{2}, i)$ to show

$$(a') \qquad h(-p) \equiv 0 \bmod 8 \quad \text{iff } p = x^2 + 32y^2, \text{ for } x, y \in \mathbb{Z}\,.$$

In 1976, Pizer [16] used quaternion algebras to obtain, in various cases, information on the sums of certain class numbers. In particular, he showed

$$(b) \qquad h(-p) + h(-2p) \equiv \frac{p-1}{2} \bmod 8\,.$$

More recently, Williams [24] in 1981 was able to relate $h(-p)$ to the fundamental unit ε_p of $\mathbb{Q}(\sqrt{p})$. Specifically, given $p \equiv 1 \bmod 8$ and $\varepsilon_p = T + U\sqrt{p} > 1$ with $T \equiv 0 \bmod 4$, $U \equiv 1 \bmod 4$, he improved the result of Lehmer [14], Cohn and Cook [3], and Kaplan [12]: $h(-p) \equiv T \bmod 8$, to a more refined

$$(c) \qquad \begin{aligned} &h(-p) \equiv T + (p-1) \bmod 16 && \text{if } h(-p) \equiv 0 \bmod 8\,, \\ &h(-p) \equiv T + (p-1) + 4(h(p)-1) \bmod 16 && \text{if } h(-p) \equiv 4 \bmod 8 \end{aligned}$$

essentially by manipulating the analytic class number formula.

In the literature of the past few years, a number of authors, perhaps most notably Gras [9] and Pioui [15], but also Desnoux [8], Hardy and Williams [10], Hikita [11], Stevenhagen [21] and Uehara [22] (among others) have

* Partially supported by NSA/MSP grant #MDS90-H-1019.

shown through a variety of means that (a)–(c) are in fact part of a rather broad family of results which can in many ways be expanded and refined. For example, with a fairly simple computation one can show that the results of [9] and [15] (themselves obtained through p-adic measure theory) imply the following

PROPOSITION (see Proposition 3.1 and Corollaries 3.1 and 3.2). *Let* $P = p_1 \dots p_k$ *with* $p_i \equiv 1 \bmod 8$, k *odd or* $k = 2$, *with* $(p_i \mid p_j) = -1\ \forall i \neq j$. *Then*

(A) $h(-P) \equiv 0 \bmod 2^{k+2}$ *iff* $(1 - i \,|\, P) = 1$.
(B) $h(-P) + h(-2P) \equiv 2^{k-2}(P-1) \bmod 2^{k+2}$.
(C) *Let* $\varepsilon_P > 1$ *be the fundamental unit of* $\mathbb{Q}(\sqrt{P})$. *Then*

$$\frac{h(P)\log_2(\varepsilon_P)}{\sqrt{P}} \equiv 2^{k-1}(P-1) + h(-P) \bmod 2^{k+3}\,.$$

(We note that (A) and (B) can be found in [13], (B) for the cases $k = 1, 2$ in [16]. That (C) in the case $k = 1$ is precisely Williams' result (c) can be seen by taking the 2-adic power series expansion for $\log_2(x)$ [23].)

In this article we establish a uniform procedure for obtaining congruences such as (A)–(C) by studying the cuspidal behavior of certain 2-adic modular forms. Through it one can derive a family of results, similar in form and refinement to those found in [9] and [15]. This is essentially the content of [6], and is outlined in Sections 2 and 3. While it should be noted that the method developed does suppress some fairly heavy machinery (for instance Rappoport's q-expansion principle), it does, however, succeed in reducing our problem to some fairly simple computations. Finally, we note that the arguments used are structured so that they may be lifted from $\mathbb{Q}$ to a totally real number field K, to consider the relative class numbers of certain CM extensions through Hilbert modular forms. As such, results analogous to (A)–(C) are often attainable. This is done for a specific example in Section 4.

2. We now recall several modular forms and their behavior at a certain class of unramified cusps. Rappoport's q-expansion principle, as mentioned before, will be crucial to our arguments, and as such will be stated in the form that will be needed.

We begin with a result of Deligne and Ribet [7], again weakened slightly to fit our situation. Let K be a totally real number field of degree r over $\mathbb{Q}$. By $\mathcal{O}_K$, $\mathcal{O}_K^*$, and $\widehat{K}^*$ we shall mean, respectively, the integers, units and ideles of K. Then

THEOREM 2.1. *Let* $k \geq 1$ *be an integer, and let* ε *be an idele class character of parity* k *and conductor* f, f *nontrivial if* $k = 2$ *and* $K = \mathbb{Q}$.

Then there exists a modular form $E^K_{k,1,\varepsilon} \in M_k(\Gamma_{00}(f), \mathbb{C})$ *(the space of weight* k*, level* f *Hilbert forms with coefficients in the complex numbers) whose q-expansion at the cusp determined by* $\tau \in \widehat{K}^*$ *with* $\tau_\omega = 1$ *at all infinite places* ω *and* $i(\tau)$ *(ideal content) trivial, is given by the formula*

$$\varepsilon(\tau)\Big[2^{-r}L(1-k,\varepsilon) + \sum_{\mu \gg 0}\Big(\sum_{\mathcal{A}\,|\,(\mu)} \varepsilon(\mathcal{A})\mathcal{N}_{K/\mathbb{Q}}(\mathcal{A})^{k-1}\Big)q^\mu\Big] + C$$

where C *is a constant depending on* ε *and* τ*, and by* $\varepsilon(\mathcal{A})$ *and* $L(1-k,\varepsilon)$*, we mean their values when* ε *is viewed as a ray class character and* $L(s,\varepsilon)$ *is the usual Dedekind L-function.*

We add that in the cases we shall be considering, the contribution of C will be identically 0.

THEOREM 2.2. *Let* $\mu, \nu \gg 0$ *be elements of* K*, and let* $L = K(\sqrt{-\mu\nu}) > K$*. Moreover, let* ε *be the idele class character associated with* L/K*,* $\varepsilon : \widehat{K}^* \to \{1, -1\}$*. Then, for suitable* $N > 1$*, a weight one modular form on* $\Gamma_{00}(N)$ *exists whose q-expansion at the cusp described in Theorem* 2.1 *is given by the series*

$$\varepsilon(\tau) \sum_{x,y \in \mathcal{O}_K} q^{\mu x^2 + \nu y^2}\,.$$

Two other types of modular forms will also be considered. The first of these is the generalized Eisenstein series, which is formed as follows. Let χ_1 and χ_2 be ideal class characters with parity $k \geq 1$ and relatively prime conductors N_1 and N_2. Then we have a weight k, level N_1N_2, character $\chi_1\chi_2$ modular form with q-expansion

$$E^K_{k,\chi_1,\chi_2} = B + \sum_{\mu \gg 0}\Big(\sum_{\mathcal{A}\,|\,(\mu)} \chi_1(\mu/\mathcal{A})\chi_2(\mathcal{A})\mathcal{N}_{K/\mathbb{Q}}(\mathcal{A})^{k-1}\Big)q^\mu\,.$$

If $K = \mathbb{Q}$, then $B = -L(0,\chi_1)L(1-k,\chi_2)$. For $K \neq \mathbb{Q}$, the situation is a bit more complicated, but we have already considered the case where χ_1 is the trivial character in Theorem 2.1, and by following Shimura's construction in [20, p. 654] we find that if χ_1 and χ_2 have nontrivial conductors, then $B = 0$ (i.e. we have a semicusp form).

The second type of form we consider is purely cuspidal and is discussed by Serre in [19] and by Rogawski and Tunnell in [18]. Here we assume that K is again totally real, and, moreover, has narrow class number one. We let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K. Then, if ϱ is a 2-dimensional, irreducible, continuous and odd representation, $\varrho : G_K \to \mathrm{GL}_2(\mathbb{C})$, the transform, under certain conditions, of $L(s,\varrho)$ is a weight one cusp form of a certain prescribed type. More specifically, if a weakened form of the Artin conjecture is true, and ϱ is such a representation with

$L(s,\varrho)=\sum_{\beta\in I_K}a_\beta\mathcal{N}_{K/\mathbb{Q}}(\beta^{-s})$, then $f(z)=\sum_{\mu\gg 0}a_{(\mu)}q^\mu$ is a weight one cusp form of some determinable level and character.

For example, suppose $K=\mathbb{Q}$, $F/\mathbb{Q}$ is quadratic with discriminant d_F, σ a coset representative of $G_\mathbb{Q}/G_F$, $\{\chi,\chi_\sigma\}$ one-dimensional characters on G_F with $\chi_\sigma(\gamma)=\chi(\sigma\gamma\sigma^{-1})$ $\forall\gamma\in G_F$ and $\varrho=\mathrm{Ind}_{F/\mathbb{Q}}(\chi)$. Then we have the following [19]

THEOREM 2.3. *Under the above conditions*

(1) *ϱ is irreducible iff $\chi\neq\chi_\sigma$,*
(2) *the conductor of ϱ is $|d_F|\mathcal{N}_{F/\mathbb{Q}}(f_\chi)$, where f_χ is the conductor of χ,*
(3) *the representation of $G_\mathbb{Q}$ is odd iff either*
   (a) *F is imaginary, or*
   (b) *F is real and χ has mixed signature.*

Thus if $p\equiv 1 \bmod 8$ is a prime integer, $(p)=p'p''$ in $I_{\mathbb{Q}(i)}$, we have a modular form $F_{\chi_{p'}}=\sum_{n\geq 1}a'_nq^n\in S_1(\Gamma_0(4p),\psi_4\chi_p)$, where by ψ_4, χ_p we mean the characters corresponding to $\mathbb{Q}(i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ respectively, and by $\chi_{p'}$ we mean the unique quadratic ray class character on $I_{\mathbb{Q}(i)}$ of conductor p'.

Finally, we consider p-adic forms F_k, $k\geq 0$, on $\Gamma_{00}(N)$ of respective weights $k=0,1,2,\ldots$ ($k=0$ meaning that the form is just a constant), all but finitely many of them being 0. In addition we assume that there exists a cusp $\alpha\in\widehat{K}^*$ such that the coefficients of $F_{k,\alpha}$, the q-expansion of F_k at α, are rational for all k. Then, if α_p is the p-component of $\alpha\in\widehat{K}^*$, $\alpha_p\in K\otimes\mathbb{Q}_p$, $\mathcal{N}\alpha_p\in\mathbb{Q}_p$ and $\mathcal{O}_{K,p}$ is the localization of $\mathcal{O}_K$ at p, and if we set

$$S(\alpha)=\sum_{k\geq 0}\mathcal{N}\alpha_p^{-k}F_{k,\alpha}\,,$$

then we have the following version of Rappoport's q-expansion principle [7].

THEOREM 2.4. *If $S(\alpha)$ has coefficients in $\mathcal{O}_{K,p}$ for one α, then $S(\alpha)$ has coefficients in $\mathcal{O}_{K,p}$ for all $\alpha\in\widehat{K}^*$, where p is any finite prime of K.*

COROLLARY 2.1. *If $S(\alpha)=\sum_{k\geq 0}\mathcal{N}\alpha_p^{-k}F_{k,\alpha}$, $T(\alpha)=\sum_{k\geq 0}\mathcal{N}\alpha_p^{-k}G_{k,p}$ with F_k, G_k being weight k forms on $\Gamma_{00}(N)$, again with all but finitely many of them being 0, then if $S(\alpha)\equiv T(\alpha) \bmod p^n$ holds for some $\alpha\in\widehat{K}^*$, it holds for all $\alpha\in\widehat{K}^*$.*

3. In this section K will always be assumed to be $\mathbb{Q}$, and the following additional notation will be considered in effect.

1. If n is a positive integer congruent to 1 (resp. 3) mod 4, then χ_n (resp. ψ_n) is the unique even (resp. odd) quadratic Dirichlet, ideal, or idele class character associated to $\mathbb{Q}(\sqrt{n})$ (resp. $\mathbb{Q}(\sqrt{-n})$).

2. ψ_4 is the character associated to $\mathbb{Q}(i)$; ψ_8 to $\mathbb{Q}(\sqrt{-2})$; χ_8 to $\mathbb{Q}(\sqrt{2})$.
3. $\tau \in \widehat{K}^*$ is such that $i(\tau) = 1$ and $\tau_\omega = 1$ at all infinite places ω.

We begin by considering the classical result: $h(-r) \equiv 1 \bmod 2$, for r a prime, $r \equiv 3 \bmod 4$, recovering it by manipulating the coefficients of an Eisenstein series. We let

$$\sum_{n\geq 1} a_n q^n = E_{1,1,\psi_r} - \tfrac{1}{2}L(0,\psi_r) = \sum_{n\geq 1}\Big(\sum_{d\,|\,n}\psi_r(d)\Big)q^n\,.$$

Now if $n = r^\alpha n'$, $(r,n') = 1$, then we have

$$a_n = \sum_{d\,|\,n'}\psi_r(d) = \psi_r(\sqrt{n'}) + \sum_{\substack{d\,|\,n'\\ d<\sqrt{n'}}}(\psi_r(d) + \psi_r(n'/d))$$

where $\psi_r(\sqrt{n'}) = 0$ if $\sqrt{n'}$ is not an integer. Therefore $a_n \equiv 0 \bmod 2$ if n' is not a square, and $a_n \equiv 1 \bmod 2$ if it a square. In other words,

$$\begin{aligned}\sum_{n\geq 1} a_n q^n &\equiv \sum_{n\geq 1} q^{n^2} + \sum_{m\geq 1} q^{rm^2} \bmod 2\\ &\equiv \tfrac{1}{2}\Big(\sum_{n\in\mathbb{Z}} q^{n^2} - 1 + \sum_{m\in\mathbb{Z}} q^{rm^2} - 1\Big) \bmod 2\,.\end{aligned}$$

But since $(\sum_{n\in\mathbb{Z}} q^{n^2} - 1)(\sum_{m\in\mathbb{Z}} q^{rm^2} - 1) \equiv 0 \bmod 4$, we have

$$\sum_{n\geq 1} a_n q^n \equiv \tfrac{1}{2}\Big(\sum_{n,m\in\mathbb{Z}} q^{n^2+rm^2} - 1\Big) \bmod 2$$

or

$$E_{1,1,\psi_r} - \tfrac{1}{2}L(0,\psi_r) \equiv \tfrac{1}{2}\sum_{n,m\in\mathbb{Z}} q^{n^2+rm^2} - \tfrac{1}{2} \bmod 2\,.$$

Now this congruence should, by Corollary 2.1, hold for *every* Fourier coefficient, at *any* unramified cusp. In particular, if $\tau \in \widehat{\mathbb{Q}}^*$ and $\tau_\omega = 1$ at all places $\omega \neq r$ with τ_r a nonsquare unit modulo r, we would have

$$E_{1,1,\psi_r}|_\tau - \tfrac{1}{2}L(0,\psi_r)|_\tau \equiv \tfrac{1}{2}\sum_{n,m\in\mathbb{Z}} q^{n^2+rm^2}|_\tau - \tfrac{1}{2}|_\tau \bmod 2\,.$$

Now if we simply consider the constant coefficients, we find from Theorems 2.1 and 2.2 that

$$\tfrac{1}{2}(\psi_r(\tau) - 1)L(0,\psi_r) \equiv \tfrac{1}{2}(\psi_r(\tau) - 1) \bmod 2\,.$$

But here $\psi_r(\tau) = -1$, from which we conclude $h(-r) = L(0,\psi_r) \equiv 1 \bmod 2$. Similarly, for $p \equiv 1 \bmod 4$, a prime, we may determine the parity of $h(-p)$

by considering

$$E_{1,1,\psi_4\chi_p} - \tfrac{1}{2}L(0,\psi_4\chi_p) \equiv \tfrac{1}{2}\Big(\sum_{n,m\in\mathbb{Z}} q^{n^2+pm^2} - 1\Big) + \tfrac{1}{2}\Big(\sum_{n,m\in\mathbb{Z}} q^{2n^2+2pm^2} - 1\Big) \bmod 2\,.$$

Selecting τ with τ_p a nonsquare unit, and $\tau_\omega = 1$ otherwise, we obtain $h(-p) = L(0,\psi_4\chi_p) \equiv 0 \bmod 2$.

To determine $h(-p)$ modulo 4, we consider a_n modulo 4 where

$$\sum_{n\geq 1} a_n q^n = E_{1,1,\psi_4\chi_p} - \tfrac{1}{2}L(0,\psi_4\chi_p) + E_{1,\psi_4,\chi_p}\,.$$

If $n = 2^\alpha p^\beta n'$, we have

$$\begin{aligned} a_n &= \sum_{d\,|\,n'} \psi_4\chi_p(d) + \sum_{d\,|\,n'} \psi_4(p^\beta d)\chi_p(2^\alpha n'/d) \\ &= \sum_{d\,|\,n'} \psi_4\chi_p(d)(1 + \psi_4(p)^\beta\chi_p(2)^\alpha\chi_p(n')) \\ &= \sum_{d\,|\,n'} \psi_4\chi_p(d)(1 + \chi_p(2)^\alpha\chi_p(n'))\,. \end{aligned}$$

As before, if n' is not a square, we have $a_n \equiv 0 \bmod 4$, implying

$$\sum_{n\geq 1} a_n q^n \equiv \begin{cases} \displaystyle\sum_{n,m\in\mathbb{Z}} q^{n^2+pm^2} - 1 \bmod 4 & \text{if } p \equiv 5 \bmod 8, \\ \Big(\displaystyle\sum_{n,m\in\mathbb{Z}} q^{n^2+pm^2} - 1\Big) + \Big(\displaystyle\sum_{n,m\in\mathbb{Z}} q^{2n^2+2pm^2} - 1\Big) \bmod 4 & \\ & \text{if } p \equiv 1 \bmod 8\,. \end{cases}$$

Choosing τ as before, we obtain

$$h(-p) \equiv \begin{cases} 2 \bmod 4 & \text{if } p \equiv 5 \bmod 8, \\ 0 \bmod 4 & \text{if } p \equiv 1 \bmod 8. \end{cases}$$

To determine $h(-p)$ modulo 8, for $p \equiv 1 \bmod 8$, we consider the two-dimensional irreducible representations induced from the quadratic characters modulo p' and p'' on the ideals of $\mathbb{Q}(i)$, where $(p) = p'p''$ in $I_{\mathbb{Q}(i)}$. By Theorem 2.3 we have two cusp forms $F_{\chi_{p'}}$, $F_{\chi_{p''}}$ and if $L(s,\chi_{p'}) = \sum_{n\geq 1} a'_n q^n$ and $F_{\chi_{p''}} = \sum_{n\geq 1} a''_n q^n$, we consider a_n modulo 8, where

$$\sum_{n\geq 1} a_n q^n = E_{1,1,\psi_4\chi_p} - \tfrac{1}{2}L(0,\psi_4\chi_p) + F_{\chi_{p'}} + F_{\chi_{p''}}\,.$$

If $n = 2^\alpha p^\beta n'$, then

$$a_n = \Big(\sum_{d\,|\,n'} \psi_4\chi_p(d)(1 + \chi_p(n'))\Big) + (a'_n + a''_n)\,.$$

Clearly, if $n' = l_1^{2k_1+1} l_2^{2k_2+1} n''$ for distinct odd primes $l_i \neq p$, then both summands are congruent to 0, i.e.

$$\sum_{d \mid n'} \psi_4\chi_p(d)(1+\chi_p(n')) = \sum_{d \mid n''} \psi_4\chi_p(d) \sum_{d \mid l_1^{2k_1+1}} \psi_4\chi_p(d) \sum_{d \mid l_2^{2k_2+1}} \psi_4\chi_p(d)(1+\chi_p(n''))\,,$$

each of the last three factors on the right being even, while similarly

$$a'_n = a'_{2^\alpha p^\beta} a'_{l_1^{2k_1+1}} a'_{l_2^{2k_2+1}} a'_{n''} \equiv 0 \bmod 4$$

by multiplicativity and the fact that $a_{l_i^{2k_i+1}} \equiv 0 \bmod 2$ (i.e. in $I_{\mathbb{Q}(i)}$ there are an even number of ideals having norm $l_i^{2k_i+1}$). Hence $a'_n = \pm a''_n$ and $a'_n + a''_n \equiv 0 \bmod 8$.

Likewise, if $n' = l^{2k+1}(n'')^2$, then $a_n \equiv 0 \bmod 8$ again since

$$(*) \qquad \sum_{d \mid n'} \psi_4\chi_p(d)(1+\chi_p(n'))$$

$$= \sum_{d \mid n''} \psi_4\chi_p(d) \sum_{d \mid l^{2k+1}} (1+\chi_p(l))$$

$$= \sum_{d \mid (n'')^2} \psi_4\chi_p(d)((k+1)(1+\psi_4\chi_p(l)))(1+\chi_p(l))$$

$$\equiv (1+\psi_4(l))(1+\chi_p(l))(k+1) \bmod 8$$

while, since $\chi_{p'}(p'') = \chi_{p''}(p')$ (if $F = \mathbb{Q}(i)$ and $F(\gamma')/F$ is the quadratic extension corresponding to $\chi_{p'}$, then, if γ'' is the conjugate of γ' over $\mathbb{Q}$, $F(\gamma'')/F$ will correspond to $\chi_{p''}$. But clearly, γ' will be a square mod p'' iff γ'' is a square mod p'), and $\chi_{p'}(1+i) = \chi_{p''}(1-i) = \chi_{p''}(1+i)$ (as $p \equiv 1 \bmod 8$, and $1+i$ is a uniformizer for the dyadic prime of F), we have

$$\begin{aligned} a'_n + a''_n &= a'_{2^\alpha p^\beta} a'_{l^{2k+1}} a'_{(n'')^2} + a''_{2^\alpha p^\beta} a''_{l^{2k+1}} a''_{(n'')^2} \\ &= (a'_{2^\alpha p^\beta} a'_{l^{2k+1}} + a''_{2^\alpha p^\beta} a''_{l^{2k+1}}) a'_{(n'')^2} \qquad \text{since } a'_{m^2} = a''_{m^2} \\ &= a'_{2^\alpha p^\beta} a'_{(n'')^2} (a'_{l^{2k+1}} + a''_{l^{2k+1}})\,. \end{aligned}$$

Now if $l \equiv 3 \bmod 4$ (or $\psi_4(l) = -1$), then, as $F_{\chi_{p'}}$ is the transform of the L-function

$$L(s, \mathrm{Ind}_{F/\mathbb{Q}}(\chi_{p'})) = \sum_{\mathcal{A} \in I_F} \chi_{p'}(\mathcal{A}) \mathcal{N}_{F/\mathbb{Q}}(\mathcal{A})^{-s}\,,$$

we have $a'_{l^{2k+1}} = a''_{l^{2k+1}} = 0$. Likewise, if $\chi_p(l) = -1$, we have $a'_{l^{2k+1}} = -a''_{l^{2k+1}}$, since $\chi_{p'}(l'l'') = \chi_{p'}(l) = \chi_p(l) = -1$. If $\chi_p(l) = \psi_4(l) = 1$ then $\chi_{p'}(l') = \chi_{p'}(l'') = \chi_{p''}(l') = \chi_{p''}(l'')$, hence

$$a'_{l^{2k+1}} + a''_{l^{2k+1}} = 2(2k+2)\chi_{p'}(l')$$

since the $2k+2$ ideals, $l'^j l''^{2k+1-j}$, $j=0$ to $2k+1$, each have norm equal to l^{2k+1}, and their images under $\chi_{p'}$ and $\chi_{p''}$ are identically one or negative one. This, combined with $(*)$, gives us $a_n \equiv 0 \bmod 8$.

Finally, if $n' = n''^2 = \prod_{i=1}^{t} l_i^{2k_i}$ and $0 \le s \le t$, with $\chi_p(l_i) = 1$ iff $i > s$, we have

$$\sum_{d \,|\, n'} \psi_4\chi_p(d)(1+\chi_p(n')) = 2\prod_{i=1}^{t}\Big(\sum_{d \,|\, l_i^{2k_i}} \psi_4\chi_p(d)\Big)$$

$$= 2\prod_{i=1}^{t}(k_i + 1 + k_i\psi_4\chi_p(l_i))\,,$$

while, since $a'_{n''^2} = a''_{n''^2}$,

$$a'_n + a''_n = a'_{2^\alpha p^\beta}(a'_{n''^2} + a''_{n''^2}) = 2a'_{2^\alpha p^\beta} a'_{n''^2} = 2a'_{2^\alpha p^\beta}\prod_{i=1}^{t} a'_{l_i^{2k_i}}$$

$$= 2a'_{2^\alpha p^\beta}\prod_{i=1}^{s}\chi_p(l_i)^{k_i}\prod_{j=s+1}^{t}(k_j + 1 + k_j\chi_p(l_j))$$

(since, if $\chi_p(l) = 1$, the ideals of $\mathbb{Q}(i)$ with norm $l_j^{2k_j}$ are simply those of the form $l_j'^{2k_j-h} l_j''^h$, $h = 1, \dots, 2k_j$). Now

$$k_i + 1 - k_i\chi_p(l_i) = k_i(1 - \chi_p(l_i)) + 1 \equiv \chi_p(l_i)^{k_i} \bmod 4\,,$$

hence

$$a_n \equiv 2 + 2a'_{2^\alpha p^\beta} \equiv 2 + 2\chi_{p'}(1+i)^\alpha \chi_{p'}(p'')^\beta\,.$$

But if $p = a^2 + b^2$, a odd and $p' = (a+bi)$, then $\chi_{p'}(p'') = (a - bi \,|\, a+bi) = (2a \,|\, p) = (a \,|\, p) = (p \,|\, a)$ (by reciprocity) $= (a^2 + b^2 \,|\, a) = (b^2 \,|\, a) = 1$. Therefore, we have shown

$$\sum_{n\ge 1} a_n q^n \equiv \begin{cases} 2\Big(\displaystyle\sum_{n,m\in\mathbb{Z}} q^{n^2+pm^2} - 1 + \sum_{n,m\in\mathbb{Z}} q^{2n^2+2pm^2} - 1\Big) \bmod 8 \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } (1-i \,|\, p) = 1, \\ 2\Big(\displaystyle\sum_{n,m\in\mathbb{Z}} q^{n^2+pm^2} - 1\Big) \bmod 8 \qquad \text{if } (1-i \,|\, p) = -1\,. \end{cases}$$

Using the same basic techniques, we find that the following generalization is possible.

PROPOSITION 3.1. *Let $P = p_1 p_2 \dots p_k$ be the product of prime integers with $p_i \equiv 1 \bmod 8$ $\forall i$, with $(p_i \,|\, p_j) = -1$ $\forall i, j$ and $k = 2$ or k odd. Then 2^{k+1} divides both $h(-P)$ and $h(-2P)$, and*

(A) $h(-P) \equiv 0 \bmod 2^{k+2}$ *iff* $(1-i \,|\, P) = 1$.
(B) $h(-2P) \equiv 0 \bmod 2^{k+2}$ *iff* $(\sqrt{-2} \,|\, P) = 1$.

P r o o f. (A) We have already discussed the case $k = 1$ at the beginning of this section. We proceed then to the case $k = 2$.

For $j = 1, 2, \dots, k$ we again let $\chi_{p'_j}$, $\chi_{p''_j}$ be the unique quadratic characters on the ideals of $\mathbb{Q}(i)$, of respective conductors p'_j, p''_j, and consider

$$\begin{aligned}
\sum_{n\geq 1} a_n q^n &= E_{1,1,\psi_4\chi_{p_1p_2}} - L(0, \psi_4\chi_{p_1p_2}) + E_{1,\psi_4,\chi_{p_1p_2}} \\
&\qquad + E_{1,\chi_{p_1},\psi_4\chi_{p_2}} + E_{1,\chi_{p_2},\psi_4\chi_{p_1}}\,, \\
\sum_{n\geq 1} b_n q^n &= F_{\chi_{p'_1p'_2}} + F_{\chi_{p'_1p''_2}} + F_{\chi_{p''_1p'_2}} + F_{\chi_{p''_1p''_2}}\,. \\
\sum_{n\geq 1} c_n q^n &= \sum_{n\geq 1} (a_n + b_n) q^n\,.
\end{aligned}$$

Reducing c_n modulo 16, we find that, if $n = 2^\alpha p_1^{\beta_1} p_2^{\beta_2}$, $c_n \equiv 0 \bmod 16$ if n' is not a square. If n' is a square, then we have

$$\begin{aligned}
c_n \equiv\ & (1 + (-1)^{\beta_1+\beta_2})^2 \\
& + \chi_{p_1p_2}(1+i)^\alpha((\chi_{p'_1} + \chi_{p''_1})(\chi_{p'_2} + \chi_{p''_2}))[p_1^{\beta_1} p_2^{\beta_2}]
\end{aligned}$$

where $\chi_{d'}[d] = \chi_{d'}(d'')$, $d = d'd''$ in $\mathbb{Q}(i)$. (For example, $\chi_{p'_1p''_2}[p_1p_2] = \chi_{p'_1p''_2}(p''_1p'_2)$.) Now if $\beta_1 \not\equiv \beta_2 \bmod 2$, say $\beta_1 \equiv 1 \bmod 2$, then clearly $a_n = 0$. Moreover, we have $c_n \equiv 0 \bmod 16$, since

$$\begin{aligned}
\chi_{p'_1p'_2}(p''_1) &= \chi_{p'_1}(p''_1)\chi_{p'_2}(p''_1) \\
&= \chi_{p''_1}(p'_1)\chi_{p'_2}(p'_1)(-1) \quad \text{since } \chi_{p'_2}(p_1) = -1 \text{ by assumption} \\
&= -\chi_{p''_1p'_2}(p'_1)
\end{aligned}$$

implies that b_n's contribution is cancelled out as well. This is likewise the case for $\beta_1 \equiv 0$, $\beta_2 \equiv 1 \bmod 2$. If both β_1, $\beta_2 \equiv 1 \bmod 2$, then we have

$$\begin{aligned}
\chi_{p'_1p'_2}(p''_1p''_2) &= \chi_{p'_1p''_2}(p''_1p'_2) = \chi_{p''_1p'_2}(p'_1p''_2) = \chi_{p''_1p''_2}(p'_1p'_2) \\
&= \chi_{p'_1}(p''_1)\chi_{p'_1}(p''_2)\chi_{p''_2}(p'_2)\chi_{p''_2}(p'_1) = \chi_{p'_1}(p''_2)\chi_{p''_2}(p'_1) \\
&= (\alpha'_1, \alpha''_2)_{p'_1}(\alpha'_1, \alpha''_2)_{p''_2} \\
&\qquad\qquad ((\gamma,\delta)_\omega \text{ the Hilbert symbol over } F = \mathbb{Q}(i)) \\
&= \prod_{\omega \nmid p'_1p''_2} (\alpha'_1, \alpha''_2)_\omega\,.
\end{aligned}$$

But this is equal to one, since $F(\sqrt{\alpha'_1})/F$, $F(\sqrt{\alpha''_2})/F$ are unramified outside p'_1, p''_2. Hence, in this case, $c_n \equiv 4(1 + \chi_P(1+i)^\alpha) \bmod 16$. Similarly, if $\beta_1 \equiv \beta_2 \equiv 0 \bmod 2$, we find immediately that again

$c_n \equiv 4(1+\chi_P(1+i)^\alpha) \bmod 16$. Putting this all together yields

$$\sum_{n\geq 1} c_n q^n \equiv \begin{cases} 4\Big(\sum\limits_{n,m\in\mathbb{Z}} q^{n^2+Pm^2} - 1\Big) \bmod 16 & \text{if } \chi_P(1+i) = -1\,, \\ 4\Big(\sum\limits_{n,m\in\mathbb{Z}} q^{n^2+Pm^2} - 1 + \sum\limits_{n,m\in\mathbb{Z}} q^{2n^2+2Pm^2} - 1\Big) \bmod 16 & \\ & \text{if } \chi_P(1+i) = 1\,, \end{cases}$$

which gives us our result for $k=2$. For $k>1$, k odd, we make a similar argument, considering c_n modulo 2^{k+2} where

$$\sum_{n\geq 1} a_n q^n = \sum_{\substack{S\subset\{1,\ldots,k\} \\ S\neq\emptyset}} E_{1,\psi_4\chi_{P_{S^c}},\chi_{P_S}} + E_{1,1,\psi_4\chi_P} - \tfrac{1}{2}L(0,\psi_4\chi_P)\,,$$

$$\sum_{n\geq 1} b_n q^n = \sum_{\substack{S\subset\{1,\ldots,k\} \\ S\neq\emptyset}} F_{\chi_{P'_S P''_{S^c}}}\,, \qquad \sum_{n\geq 1} c_n q^n = \sum_{n\geq 1}(a_n+b_n)q^n\,,$$

where for a subset $T\in\{1,\ldots,k\}$, $\chi_{P'_T P''_{T^c}} = \prod_{j\in T}\chi_{p'_j}\prod_{i\notin T}\chi_{p''_i}$ and $\chi_{P_T} = \prod_{j\in T}\chi_{p_j}$. Reducing to the case of $n = 2^\alpha\prod_{i=1}^k p_i^{\beta_i} n'$, with n' a square, we have

$$a_n = \sum_{d\,|\,n'} \psi_4\chi_P(d)(1+(-1)^{\sum_{i=1}^k\beta_i+\beta_1}\chi_{p_1}(n'))\ldots \\ \ldots(1+(-1)^{\sum_{i=1}^k\beta_i+\beta_k}\chi_{p_k}(n'))\,.$$

As in the case $k=2$ we then have, modulo 2^{k+2},

$$c_n = (1+(-1)^{\sum\beta_i+\beta_1})\ldots(1+(-1)^{\sum\beta_i+\beta_k}) \\ + \chi_P(1+i)^\alpha\Big(\prod_{j=1}^k(\chi_{p'_j}+\chi_{p''_j})\Big)[p_1^{\beta_1}\ldots p_k^{\beta_k}]\,.$$

Now if some $\beta_h \not\equiv \beta_j \bmod 2$, then $c_n \equiv 0 \bmod 2^{k+2}$, since a_n's contribution will be zero (i.e. $(\sum\beta_i+\beta_h)+(\sum\beta_i+\beta_j)\not\equiv 0 \bmod 2$, and so the terms cannot both be even), and, we claim, b_n's vanish as well. But this is clear, for if $\beta_1\equiv\ldots\equiv\beta_s\equiv 0 \bmod 2$, and $\beta_{s+1}\equiv\ldots\equiv\beta_k\equiv 1 \bmod 2$ $(1\leq s<k)$, then we have

$$\chi_{p'_1p'_2\ldots p'_k}\Big(\prod_{i=s+1}^k p''_i\Big) = (-1)^{k-s}\chi_{p''_1p'_2\ldots p'_k}\Big(\prod_{i=s+1}^k p''_i\Big) \\ = (-1)^{k-s-1}\chi_{p'_1p''_2\ldots p''_k}\Big(\prod_{i=s+1}^{k-1} p''_i p'_k\Big)$$

since k is odd, and our terms again pair off and cancel. Using the fact that

$\chi_{p_i'}(p_j'') = \chi_{p_j''}(p_i')$ as in the case $k=2$, we are left with

$$\sum_{n\geq 1} c_n q^n \equiv \begin{cases} 2^k\Big(\sum\limits_{n,m\in\mathbb{Z}} q^{n^2+Pm^2} - 1\Big) \bmod 2^{k+2} & \text{if } (1+i\,|\,P) = -1\,, \\ 2^k\Big(\sum\limits_{n,m\in\mathbb{Z}} q^{n^2+Pm^2} - 1 + \sum\limits_{n,m\in\mathbb{Z}} q^{2n^2+2Pm^2} - 1\Big) \bmod 2^{k+2} & \\ & \text{if } (1+i\,|\,P) = 1\,. \end{cases}$$

Hence the result.

To prove (B), we proceed in a nearly identical manner, this time considering c_n modulo 2^{k+2} where

$$\sum_{n\geq 1} a_n q^n = \sum_{\substack{S\subset\{1,\ldots,k\} \\ S\neq\emptyset}} E_{1,\psi_8\chi_{P_{S^c}},\chi_{P_S}} + E_{1,1,\psi_8\chi_P} - \tfrac{1}{2}L(0,\psi_8\chi_P)\,,$$

$$\sum_{n\geq 1} b_n q^n = \sum_{\substack{S\subset\{1,\ldots,k\} \\ S\neq\emptyset}} F_{\chi_{P'_S}\chi_{P''_{S^c}}}\,, \qquad \sum_{n\geq 1} c_n q^n = \sum_{n\geq 1}(a_n+b_n)q^n$$

with $p_j = p_j' p_j''$ in $F = \mathbb{Q}(\sqrt{-2}\,)$, and where $\chi_{p_j'}$, $\chi_{p_j''}$ are, respectively, the unique quadratic ray class characters over F of conductors p_j', p_j''. If $n = 2^\alpha \prod_{j=1}^k p_j^{\beta_j} n'$ we again find that if n' is not a square, then $c_n \equiv 0 \bmod 2^{k+2}$. If n' is a square, then

$$\begin{aligned} c_n \equiv{}& (1+(-1)^{\sum_{i=1}^k \beta_i + \beta_1}) \ldots (1+(-1)^{\sum_{i=1}^k \beta_i + \beta_k}) \\ &+ \chi_P(\sqrt{-2}\,)^\alpha \prod_{j=1}^k (\chi_{p_j'} + \chi_{p_j''})[p_1^{\beta_1}\ldots p_k^{\beta_k}]\,. \end{aligned}$$

Once again, we have $c_n \equiv 0 \bmod 2^{k+2}$ unless $\beta_i \equiv \beta_j \bmod 2$, $\forall i,j$. In this case, we use Hilbert symbols to show that $\chi_{p_i'}(p_j'') = \chi_{p_j''}(p_i')$, yielding

$$c_n \equiv 2^k(1+\chi_P(\sqrt{-2}\,)^\alpha) \prod_{j=1}^k \chi_{p_j'}(p_j'')^{\beta_j}\,.$$

But $\chi_{p_j'}(p_j'') = \chi_{p_j'}(\sqrt{-2}\,)$, since, if $p_j' = a - b\sqrt{-2}$, $p_j'' = a + b\sqrt{-2}$ with $a^2 + 2b^2 = p_j$, $a, b \in \mathbb{Z}$, $b = 2^{c_j} b'$, b' odd, then

$$\begin{aligned} (\sqrt{-2}\,|\,a - b\sqrt{-2})&(a + b\sqrt{-2}\,|\,a - b\sqrt{-2}) \\ &= (a\sqrt{-2} - 2b\,|\,a - b\sqrt{-2}) \\ &= (b\,|\,a - b\sqrt{-2})(ab\sqrt{-2} - 2b^2\,|\,a - b\sqrt{-2}) \\ &= (b'\,|\,p_j)(a^2 - 2b^2\,|\,a - b\sqrt{-2}) \\ &= (p_j\,|\,b')(a^2 - 2b^2\,|\,p_j) = (a^2\,|\,b')(2a^2\,|\,p_j) = 1\,. \end{aligned}$$

Therefore, since k is odd, we have $c_n \equiv 2^k(1+\chi_P(\sqrt{-2})^{\alpha+1})$, implying

$$\sum_{n\ge1} c_n \equiv \begin{cases} 2^k\Big(\sum\limits_{n,m\in\mathbb{Z}} q^{n^2+2Pm^2}-1\Big) \bmod 2^{k+2} & \text{if } (\sqrt{-2}\,|\,P)=-1\,,\\ 2^k\Big(\sum\limits_{n,m\in\mathbb{Z}} q^{n^2+2Pm^2}-1+\sum\limits_{n,m\in\mathbb{Z}} q^{2n^2+Pm^2}-1\Big) \bmod 2^{k+2} & \\ & \text{if } (\sqrt{-2}\,|\,P)=1\,. \end{cases}$$

Choosing an appropriate cusp then gives us our result.

Corollary 3.2. *Let P be as in Proposition* 3.1. *Then*

$$h(-P)+h(-2P) \equiv 2^{k-2}(P-1) \bmod 2^{k+2}\,.$$

Proof. Since $P\equiv 1 \bmod 8$, $(\sqrt{-2}\,|\,P)=(\sqrt{2}\,|\,P)$. Now $(1+i\,|\,\sqrt{2})=e^{\pi i/4}$ is a primitive 8th root of unity, and therefore, $(1+i\,|\,P)=(\sqrt{-2}\,|\,P)$ iff $P\equiv 1 \bmod 16$, that is, iff $2^{k-2}(P-1)\equiv 0 \bmod {}^{k+2}$.

Corollary 3.3. *Let P be as in Proposition* 3.1. *Then*

$$\frac{h(P)\log_2(\varepsilon_P)}{\sqrt{P}} \equiv h(-P)+2^{k-1}(P-1) \bmod 2^{k+3}\,.$$

Proof. Using Amice–Fresnel's [1] residue formula, we have

$$\frac{2h(P)\log_2(\varepsilon_P)}{\sqrt{P}} = \left(1-\frac{\chi_P(2)}{2}\right)^{-1} L_2(1,\chi_P)\,.$$

Since $\chi_P(2)=1$ here, this, by the continuity of 2-adic L-functions [23], implies

$$\frac{h(P)\log_2(\varepsilon_P)}{\sqrt{P}} = L_2(1,\chi_P) \equiv L_2(1-2^{k+3},\chi_P) \bmod 2^{k+3}\,.$$

From Corollary 3.2, $2L(0,\psi_4\chi_P)+2L(0,\psi_8\chi_P)\equiv 2^{k-1}(P-1) \bmod 2^{k+3}$. Thus, we need only show

$$L(1-2^{k+3},\chi_P) \equiv 3L(0,\psi_4\chi_P)+2L(0,\psi_8\chi_P) \bmod 2^{k+3}\,.$$

To this end, we consider d_n modulo 2^{k+3}, where

$$\sum_{n\ge1} a_n q^n = E_{2^{k+3},1,\chi_P} - \tfrac{1}{2}L(1-2^{k+3},\chi_P) + \sum_{\substack{S\subset\{1,\dots,k\}\\ S\ne\emptyset}} E_{2^{k+3},\chi_{P_S},\chi_{P_{S^c}}}\,,$$

$$\sum_{n\ge1} b_n q^n = E_{1,1,\psi_4\chi_P} - \tfrac{1}{2}L(0,\psi_4\chi_P) + \sum_{\substack{S\subset\{1,\dots,k\}\\ S\ne\emptyset}} E_{1,\psi_4\chi_{P_{S^c}},\chi_{P_S}}\,,$$

$$\sum_{n\geq 1} c_n q^n = E_{1,1,\psi_8\chi_P} - \tfrac{1}{2}L(0,\psi_8\chi_P) + \sum_{\substack{S\subset\{1,\dots,k\}\\ S\neq\emptyset}} E_{1,\psi_8\chi_{P_{S^c}},\chi_{P_S}}\,,$$

$$\sum_{n\geq 1} d_n q^n = \sum_{n\geq 1}(a_n - 3b_n - 2c_n)q^n\,.$$

Now if $n = 2^\alpha \prod_{j=1}^k p_j^{\beta_j} n'$, we have

$$\begin{aligned}
a_n &\equiv \sum_{d\,|\,n'} \chi_P(d) d^{2^{k+3}-1}(1 + p_1^{\beta_1}(-1)^{k\beta_1+\Sigma\beta_j}\chi_{p_1}(n'))\dots \\
&\qquad\qquad \dots(1 + p_k^{\beta_k}(-1)^{k\beta_k+\Sigma\beta_j}\chi_{p_k}(n'))\,, \\
b_n &= \sum_{d\,|\,n'} \psi_4\chi_P(d)(1 + (-1)^{k\beta_1+\Sigma\beta_j}\chi_{p_1}(n'))\dots \\
&\qquad\qquad \dots(1 + (-1)^{k\beta_k+\Sigma\beta_j}\chi_{p_k}(n'))\,, \\
c_n &= \sum_{d\,|\,n'} \psi_8\chi_P(d)(1 + (-1)^{k\beta_1+\Sigma\beta_j}\chi_{p_1}(n'))\dots \\
&\qquad\qquad \dots(1 + (-1)^{k\beta_k+\Sigma\beta_j}\chi_{p_k}(n'))\,.
\end{aligned}$$

If n' is not a square, then, since by assumption $p_j \equiv 1 \bmod 8\ \forall j$, we have

$$a_n \equiv \sum_{d\,|\,n'} \chi_P(d)(d - 3\psi_4(d) - 2\psi_8(d)) \prod_{h=1}^k (1 + (-1)^{k\beta_h+\Sigma\beta_j}\chi_{p_h}(n'))\,.$$

We note, however, that for d odd, $d - 3\psi_4(d) - 2\psi_8(d) \equiv 4 \bmod 8$, implying

$$\begin{aligned}
a_n &\equiv 4\sum_{d\,|\,n'} \chi_P(d)(1 + (-1)^{k\beta_1+\Sigma\beta_j}\chi_{p_1}(n'))\dots \\
&\qquad\qquad \dots(1 + (-1)^{k\beta_k+\Sigma\beta_j}\chi_{p_k}(n')) \equiv 0 \bmod 2^{k+3}\,.
\end{aligned}$$

If n' is a square, then, if $S \subset \{1,\dots,k\}$ is the set of indices such that $p_i \equiv 9 \bmod 16$ and $\beta_i \equiv 1 \bmod 2$ iff $i \in S$, then

$$\begin{aligned}
a_n \equiv\ & \sum_{d\,|\,n'} \chi_P(d)(d - 3\psi_4(d) - 2\psi_8(d)) \prod_{h=1}^k (1 + (-1)^{k\beta_h+\Sigma\beta_j}\chi_{p_h}(n')) \\
& + (*)8\sum_{i\in S}\sum_{d\,|\,n'} \chi_P(d) d \prod_{h\neq i}(1 + (-1)^{k\beta_h+\Sigma\beta_j})\,.
\end{aligned}$$

If $k = 2$, then clearly the contribution from $(*)$ will be congruent to 0. Similarly, if k is odd, the contribution from the ith auxiliary term will likewise be congruent to 0 unless the simultaneous system of $k-1$ equations

in $\mathbb{F}_2$ holds for each $i \in S$

$$\begin{aligned}
&0\beta_1 + \beta_2 + \ldots + 0\beta_i + \ldots + \beta_{k-1} + \beta_k \equiv 1\,,\\
&\beta_1 + 0\beta_2 + \ldots + 0\beta_i + \ldots + \beta_{k-1} + \beta_k \equiv 1\,,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\beta_1 + \beta_2 + \ldots + 0\beta_i + \ldots + \beta_{k-1} + 0\beta_k \equiv 1\,.
\end{aligned}$$

But we see immediately that adding equation h to equation j produces $\beta_h \equiv \beta_j$. The fact that k is odd thus implies $\beta_h \equiv 1\ \forall h$. Again using the identity $d - 3\psi_4(d) - 2\psi_8(d) \equiv 4 \bmod 8$ leads us to conclude

$$\sum_{n\geq 1} a_n q^n \equiv 2^{k+1}\Big(\sum_{n,m\in\mathbb{Z}} q^{n^2+2m^2} - 1 + A\sum_{n,m\in\mathbb{Z}} q^{Pn^2+2Pm^2} - 1\Big) \bmod 2^{k+3}$$

where $A = 1 +$ the number of elements in S. Choosing an appropriate cusp gives us our result. A similar proof yields

Corollary 3.4. *Let P be as in Proposition* 3.1. *Then*

$$\frac{h(2P)\log_2(\varepsilon_{2P})}{\sqrt{2P}} \equiv h(-2P) + 2^{k-1}(P-1) \bmod 2^{k+3}\,.$$

4. In this section we will be assuming that $K = \mathbb{Q}(\sqrt{2})$ and our forms will be Hilbert modular forms over that field. Moreover, we will be assuming the Artin conjecture for representations of G_K. For a prime integer $p \equiv 1 \bmod 8$, we let $p' \in K$ be a totally positive representative of a prime ideal of K dividing p, and let $\tau = 2+\sqrt{2}$, $\varepsilon = 1+\sqrt{2}$ be, respectively, a representative for the unique dyadic prime of K, and K's fundamental unit. We note that if ζ_n is a primitive nth root of unity, n a positive integer, then $K(i) = \mathbb{Q}(\zeta_8)$ and $K(\sqrt{\tau}) = K(\zeta_{16} + \overline{\zeta}_{16}) = \mathbb{Q}(\zeta_{16})^+$, the maximum totally real subextension of $\mathbb{Q}(\zeta_{16})$.

If we make the additional assumption that ε is a square modulo p (or, equivalently, by 3.1, $8 \,|\, h(-p)$ since $\frac{1+\sqrt{2}}{1+i} = (\frac{1-i+\sqrt{2}}{2})^2$), the extension $K(\sqrt{p'})/K$ will be ramified only at p', corresponding to the unique quadratic ray class character $\chi_{p'}$ of conductor p'. Likewise, corresponding to the extensions $K(i)/K$ and $K(\sqrt{-\tau})/K$ we have quadratic ray class characters which we shall denote (respectively) by ψ_1 and ψ_2. Finally, for $d \in K$, we let $h(d)$ be the class number of $K(\sqrt{d})$ and show the following analog to (a)–(c) of Section 1.

Proposition 4.1. *Let p, p' be as above. Then*

$$\text{(A) } h(-p') \equiv \begin{cases} 0 \bmod 2\,, & \\ 0 \bmod 4 & \text{iff } p \equiv 1 \bmod 16,\\ 0 \bmod 8 & \text{iff } p \equiv 1 \bmod 16 \text{ and } (1+\zeta_8 \mid p) = 1\,, \end{cases}$$

$$\text{(A}')\ h(-\tau p') \equiv \begin{cases} 0 \bmod 2\,, & \\ 0 \bmod 4 & \textit{iff } p \equiv 1 \bmod 16\,, \\ 0 \bmod 8 & \textit{iff } p \equiv 1 \bmod 16 \textit{ and } (\sqrt{-\tau} \mid p) = 1\,. \end{cases}$$

If $p \equiv 1 \bmod 16$ *then*

$$\text{(B)}\ h(-p') + h(-\tau p') \equiv \tfrac{1}{4}(p-1) \bmod 8,$$

$$\text{(C)}\ \frac{h(p')R_2(K(\sqrt{p'}))}{\sqrt{8p}\log_2(\varepsilon)} \equiv h(-p') \bmod 16,$$

where, for a number field E, $R_2(E)$ *is the* 2*-adic regulator of* E.

P r o o f. (A) Here we proceed as at the beginning of Section 3. To show $h(-p') \equiv 0 \bmod 2$, we consider a_μ modulo 2, where

$$\sum_{\mu \gg 0} a_\mu q^\mu = E^K_{1,1,\psi_1\chi_{p'}} - \tfrac{1}{4}L(0,\psi_1\chi_{p'})\,.$$

If $\mu = \tau^\alpha p'^\beta \mu'$, we once again find that

$$a_\mu = \sum_{\mathcal{A} \mid \mu} \psi_1\chi_{p'}(\mathcal{A}) = \sum_{\mathcal{A} \mid \mu'} \psi_1\chi_{p'}(\mathcal{A}) \equiv \begin{cases} 0 \bmod 2 & \text{if } \mu' \text{ is not a square,} \\ 1 \bmod 2 & \text{if } \mu' \text{ is a square,} \end{cases}$$

leading us to conclude

$$\sum_{\mu \gg 0} a_\mu q^\mu \equiv \tfrac{1}{2}\Big(\sum_{\mu,\nu \in \mathcal{O}_K} q^{\mu^2 + p'\nu^2} - 1 + \sum_{\mu,\nu \in \mathcal{O}_K} q^{\tau\nu^2 + \tau p'\nu^2} - 1 \Big) \bmod 2\,.$$

As before, choosing an appropriate cusp (for example, $\tau_\omega = 1$ at all places ω except p', where it is a nonsquare unit) yields $L(0,\psi_1\chi_{p'}) \equiv 0 \bmod 4$. But $L(0,\psi_1\chi_{p'}) = 2h(-p')$.

To determine the 4-divisibility of $h(-p')$, we consider $a_\mu \bmod 4$ where

$$\sum_{\mu \gg 0} a_\mu q^\mu = E^K_{1,1,\psi_1\chi_{p'}} - \tfrac{1}{4}L(0,\psi_1\chi_{p'}) + E^K_{1,\psi_1,\chi_{p'}}$$

and find, for $\mu = \tau^\alpha p'^\beta \mu'$,

$$a_\mu = \sum_{\mathcal{A} \mid \mu'} \psi_1\chi_{p'}(\mathcal{A})(1 + \psi_1(p')^\beta \chi_{p'}(\tau)^\alpha \chi_{p'}(\mu'))\,.$$

But $\psi_1(p') = 1$, since $p \equiv 1 \bmod 8$, leaving

$$\sum_{\mu \gg 0} a_\mu q^\mu \equiv \begin{cases} \Big(\displaystyle\sum_{\mu,\nu \in \mathcal{O}_K} q^{\mu^2 + p'\nu^2} - 1 + \sum_{\mu,\nu \in \mathcal{O}_K} q^{\tau\mu^2 + \tau p'\nu^2} - 1 \Big) \bmod 4 & \\ & \text{if } \chi_{p'}(\tau) = 1\,, \\ \Big(\displaystyle\sum_{\mu,\nu \in \mathcal{O}_K} q^{\mu^2 + p'\nu^2} - 1 \Big) \bmod 4 & \\ & \text{if } \chi_{p'}(\tau) = -1\,. \end{cases}$$

Now since $K(\sqrt{\tau}) = \mathbb{Q}(\zeta_{16})^+$, it follows that $\chi_{p'}(\tau) = 1$ iff $p \equiv 1 \bmod 16$. Hence the result.

Finally, to determine $h(-p')$ modulo 8, we let $F = K(i)$ and note that the units of $\mathcal{O}_F$ and $\mathcal{O}_K$ are the same up to roots of unity ([5, 13.6] for example). If $p \equiv 1 \bmod 16$ and $\chi_p(\varepsilon) = 1$, then we will have quadratic ray class characters $\chi_{\varrho'}$, $\chi_{\varrho''}$ on the ideals of F of respective prime conductors ϱ', ϱ'', where $p' = \varrho'\varrho''$. We let $F_{\chi_{\varrho'}}$, $F_{\chi_{\varrho''}}$ be the corresponding Hilbert forms, and consider $a_\mu \bmod 8$ where

$$\sum_{\mu \gg 0} a_\mu q^\mu = E^K_{1,1,\psi_1\chi_{p'}} - \tfrac{1}{4}L(0,\psi_1\chi_{p'}) + E^K_{1,\psi_1,\chi_{p'}} + F_{\chi_{\varrho'}} + F_{\chi_{\varrho''}}\,.$$

Our arguments from here on are precisely identical to those used over $\mathbb{Q}$. We need only demonstrate that $\chi_{\varrho'}(\varrho'') = \chi_{\varrho''}(\varrho') = 1$. But this computation is greatly facilitated by the well known fact that $\mathbb{Q}(\zeta_8)$ (as well as $\mathbb{Q}(\zeta_{16})$[23, p. 352]) has class number one. We let $\varrho' = a - bi$, $\varrho'' = a + bi$, where $\tau a, \tau b \in \mathcal{O}_F = \mathbb{Z}(\zeta_8)$, and observe that

$$\begin{aligned}(a+bi \,|\, a-bi) = (2a \,|\, p') &= (\tau a \,|\, p') \quad \text{since } p \equiv 1 \bmod 16\\ &= (\tau a, p')_{p'} = \prod_{\omega \nmid p'} (\tau a, p')_\omega\\ &= \prod_{\omega \nmid \tau p'} (a', p')_\omega \quad \text{where } \tau a = \tau^\alpha a'\\ &= \prod_{\omega \nmid \tau p'} (a', b^2)_\omega = 1\,.\end{aligned}$$

Noting that $1+\zeta_8$ serves as a uniformizer for the unique dyadic prime of F, we find

$$\sum_{\mu \gg 0} a_\mu q^\mu \equiv \begin{cases} 2\Big(\displaystyle\sum_{\mu,\nu \in \mathcal{O}_K} q^{\mu^2+p'\nu^2} - 1 + \sum_{\mu,\nu\in\mathcal{O}_K} q^{\tau\mu^2+\tau p'\nu^2} - 1\Big) \bmod 8 & \\ \qquad\qquad \text{if } \chi_p(1+\zeta_8) = 1\,, & \\ 2\Big(\displaystyle\sum_{\mu,\nu\in\mathcal{O}_K} q^{\mu^2+p'\nu^2} - 1\Big) \bmod 8 \qquad \text{if } \chi_p(1+\zeta_8) = -1\,. & \end{cases}$$

Thus we have shown (A). To show (A′), our argument is essentially the same. In this instance, we replace ψ_1 with ψ_2, observing that $\psi_2(p') = 1$ iff p' splits to $K(\sqrt{\tau}) = \mathbb{Q}(\zeta_{16})^+$, that is, iff $p \equiv 1 \bmod 16$. Moreover, for F we choose $K(\sqrt{-\tau})$, noting that here, $\sqrt{-\tau}$ serves as a uniformizer for the unique dyadic prime of F. Therefore, we need only show that $\chi_{\varrho'}(\varrho'') = \chi_{\varrho'}(\sqrt{-\tau})$, where $\varrho' = a - \sqrt{-\tau}b$, $\varrho'' = a + \sqrt{-\tau}b$, with $a, b \in \mathcal{O}_K$ since a simple check verifies that $\mathcal{O}_F = \mathcal{O}_K[\sqrt{-\tau}\,]$. But this may be accomplished as follows. We consider

$$\begin{aligned}\chi_{\varrho'}(\sqrt{-\tau}\varrho'') &= (a\sqrt{-\tau} - \tau b \,|\, a - \sqrt{-\tau}b) = (b \,|\, p')(ab\sqrt{-\tau} - \tau b^2 \,|\, a - \sqrt{-\tau}b)\\ &= (b, p')_{p'}(2a^2 \,|\, p') = \prod_{\omega \,|\, b} (b, p')_\omega\end{aligned}$$

$$= \prod_{\omega \mid b\tau} (b, p')_\omega \quad \text{since } p \equiv 1 \bmod 16$$
$$= \prod_{\omega \mid b\tau} (b, a^2)_\omega = 1\,.$$

To prove (B), we need only make the brief computation

$$\frac{1+\zeta_8}{\sqrt{\tau}} = \frac{\frac{2+\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i}{\sqrt{2+\sqrt{2}}} = \zeta_{16}\,.$$

Part (C) follows from Colmez's residue formula for p-adic zeta functions [4] once we have shown that $L(1, \chi_{p'}) \equiv L(-31, \chi_{p'}) \equiv L(0, \psi_1\chi_{p'}) \bmod 32$. To this end, we consider c_μ modulo 16 where

$$\sum_{\mu \gg 0} a_\mu q^\mu = E^K_{31,1,\chi_{p'}} - L(-31, \chi_{p'}) + E^K_{31,\chi_{p'},1}\,,$$
$$\sum_{\mu \gg 0} b_\mu q^\mu = E^K_{1,1,\psi_1\chi_{p'}} - L(0, \psi_1\chi_{p'}) + E^K_{1,\chi_{p'},\psi_1}\,,$$
$$\sum_{\mu \gg 0} c_\mu q^\mu = \sum_{\mu \gg 0} (a_\mu - b_\mu) q^\mu\,.$$

As $p \equiv 1 \bmod 16$ by assumption, we have

$$c_\mu \equiv \sum_{\mathcal{A} \mid \mu'} \chi_{p'}(\mathcal{A})(\mathcal{N}\mathcal{A}^{31} - \psi_1(\mathcal{A}))(1 + \chi_{p'}(\mu'))$$
$$\equiv 0 \bmod 16 \quad \text{since } \mathcal{N}(\mathcal{A})^{31} - \psi_1(\mathcal{A}) \equiv 0 \bmod 8\,.$$

Choosing an appropriate cusp gives us our result.

In conclusion, the author wishes to thank Drs. T. Chinburg, P. Conner and J. Hurrelbrink for their advice and support.

References

[1] Y. Amice et J. Fresnel, *Fonctions zêta p-adiques des corps de nombres abéliens réels*, Acta Arith. 20 (1972), 353–384.

[2] 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.

[3] H. Cohn and G. Cooke, *Parametric form of an eight class field*, Acta Arith. 30 (1976), 367–377.

[4] P. Colmez, *Résidu en $s = 1$ des fonctions zêta p-adiques*, Invent. Math. 91 (1988), 371–389.

[5] P. Conner and J. Hurrelbrink, *Class Number Parity*, Ser. Pure Math. 8, World Scientific, 1988.

[6] A. Costa, *Modular forms and class number congruences*, Ph.D. thesis, University of Pennsylvania, 1989.
[7] P. Deligne and K. Ribet, *Values of abelian L-functions at negative integers over totally real fields*, Invent. Math. 59 (1980), 227–286.
[8] P.-J. Desnoux, *Congruences dyadiques entre nombres de classes de corps quadratiques*, Manuscripta Math. 62 (1988), 163–179.
[9] G. Gras, *Relations congruentielles linéaires entre nombres de classes de corps quadratiques*, Acta Arith. 52 (1989), 147–162.
[10] K. Hardy and K. Williams, *Congruences modulo* 16 *for the class numbers of complex quadratic fields*, J. Number Theory 27 (1989), 178–195.
[11] M. Hikita, *On the congruences for the class numbers of the quadratic fields whose discriminants are divisible by* 8, ibid. 23 (1986), 86–101.
[12] P. Kaplan, *Unités de norme* -1 *de* $\boldsymbol{Q}(\sqrt{p})$ *et corps de classes de degré* 8 *de* $\boldsymbol{Q}(\sqrt{-p})$ *où* p *est un nombre premier congru à* 1 *modulo* 8, Acta Arith. 32 (1977), 239–243.
[13] —, *Sur le* 2*-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. 284 (1976), 313–363.
[14] E. Lehmer, *On the quadratic character of some quadratic surds*, ibid. 250 (1971), 42–48.
[15] R. Pioui, *Mesures de Haar p-adiques et interprétation arithmétique de* $\frac{1}{2}L_2(\chi, s) - \frac{1}{2}L_2(\chi, t)$, $s, t \in \mathbb{Q}_2$ (χ *quadratique*), Ph.D. thesis, Université de Franche-Comté, Besançon 1990.
[16] A. Pizer, *On the* 2*-part of the class number of imaginary quadratic number fields*, J. Number Theory 8 (1976), 184–192.
[17] L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper. I*, J. Reine Angew. Math. 180 (1939), 1–43.
[18] J. Rogawski and J. Tunnell, *On Artin L-functions associated to Hilbert modular forms of weight one* , Invent. Math. 74 (1983), 1–42.
[19] J.-P. Serre, *Modular forms of weight one and Galois representations*, in: Algebraic Number Fields, Academic Press, London 1977, 193–268.
[20] G. Shimura, *The special values of the zeta functions associated with Hilbert modular forms*, Duke Math. J. 45 (1978), 637–679.
[21] P. Stevenhagen, *Class groups and governing fields*, Ph.D. thesis, University of California at Berkeley, 1988.
[22] T. Uehara, *On linear congruence relations between class numbers of quadratic fields*, J. Number Theory 34 (1990), 362–392.
[23] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. 83, Springer, 1982.
[24] K. S. Williams, *On the class number of* $Q(\sqrt{-p})$ *modulo* 16, *for* $p \equiv 1 (\mathrm{mod} 8)$ *a prime*, Acta Arith. 39 (1981), 381–398.

DEPARTMENT OF MATHEMATICS
THE AMERICAN UNIVERSITY
4400 MASSACHUSETTS AVE.
WASHINGTON, D.C., 20016
U.S.A.

Received on 19.12.1989
and in revised form on 7.6.1991 (1996)