FOURIER COEFFICIENTS OF HALF-INTEGRAL WEIGHT MODULAR FORMS MODULO ℓ

Ken Ono and Christopher Skinner

Appearing in the Annals of Mathematics

1. Introduction

S. Chowla conjectured that for a given prime p there are infinitely many imaginary quadratic fields whose class number is not a multiple of p. For $p = 2$ this conjecture is a consequence of Gauss's genus theory, and for $p = 3$ it follows from the work of Davenport and Heilbronn [D-H] (who prove the stronger result that a positive proportion of such fields have class numbers coprime to 3). Via an elementary argument based on the Kronecker relations, Hartung [Ha] established the conjecture for odd primes p. Variants of his argument have been employed in other similar studies [Ho1,Ho2, Ho-On].

Hartung's result can be interpreted as an indivisibility result for coefficients of the weight $\frac{3}{2}$ modular form $\Theta^3(z)$, where $\Theta(z) := 1 + 2q + 2q^4 + 2q^9 + 2q^{16} + \dots$ ($q := e^{2\pi i z}$ throughout) is the classical theta function. For if $\Theta^3(z) = \sum_{n=0}^{\infty} r(n)q^n$, and if $n > 3$ is square-free, then by a well-known theorem of Gauss

$$r(n) = \begin{cases} 12h(-4n) & \text{if } n \equiv 1, 2, 5, 6 \pmod 8, \\ 24h(-n) & \text{if } n \equiv 3 \pmod 8, \end{cases} \tag{1}$$

where $h(D)$ is the class number of $\mathbb{Q}(\sqrt{D})$. The flavor of the Kronecker relations and their role in Hartung's work is captured by the observation that the product $\Theta^3(z) \cdot \Theta(z)$ is the normalized Eisenstein series of weight 2 on $\Gamma_0(4)$. Equating Fourier coefficients yields

$$\sum_{k=-\infty}^{\infty} r(n - k^2) = 8 \sum_{\substack{d \mid n \\ d \not\equiv 0 \pmod 4}} d, \tag{2}$$

1991 *Mathematics Subject Classification.* Primary 11F33; Secondary 11G40.

Key words and phrases. modular forms, critical values of $L-$functions.

The first author was supported by NSF grants DMS-9508976 and DMS-9304580, and the second author was supported by a Sloan Foundation Doctoral Dissertation Fellowship.

which in light of (1) is essentially a recurrence relation for class numbers. Indivisibility results for class numbers can thus be deduced by examining the right hand side of (2). This idea of extracting indivisibility results for the coefficients of a half-integral weight form $g(z)$ from properties of the coefficients of the integral weight form obtained by multiplying $g(z)$ by a theta function inspired (and underlies) the work described in this paper.

In this paper we study the indivisibility of the Fourier coefficients of half-integral weight eigenforms. For each prime ℓ we fix throughout an extension $|\cdot|_\ell$ of the usual ℓ-adic valuation to an algebraic closure of $\mathbb{Q}$. A half-integral weight modular form $g(z)$ is said to be *good* if for some theta function $\theta(z)$ the expansion of the product $G(z) = g(z) \cdot \theta(z)$ into integral weight eigenforms contains a newform without complex multiplication (see also the beginning of §2). Our main result is the following.

Theorem. *Let $g(z) = \sum_{n=0}^{\infty} c(n)q^n \in M_{k+\frac{1}{2}}(N)$ be an eigenform whose coefficients are algebraic integers. If $g(z)$ is good, then for all but finitely many primes ℓ there exist infinitely many square-free integers m for which*

$$|c(m)|_\ell = 1.$$

The idea behind the proof of this theorem is simple. Write $G(z) = \sum \alpha_i f_i(z) + \tilde{f}(z) = \sum_{n=0}^{\infty} b(n)q^n$ with each f_i a non-CM newform, each α_i algebraic, and $\tilde{f}$ a linear combination of CM-forms and oldforms. For large primes ℓ, the mod ℓ Galois representation ρ_i associated to f_i has 'big' image, and the ρ_i's are essentially independent (one has to be careful about twist-equivalent forms). Using this together with the connection between the traces of the ρ_i's and the coefficients of the f_i's and a simple application of the Chebotarev Density Theorem one can show that $|b(n)|_\ell = 1$ for many more n than can be accounted for if $|c(m)|_\ell = 1$ for only finitely many square-free m's. In this argument, the mod ℓ Galois representations take the place of explicit relations of the form (2).

Motivation for studying the indivisibility of Fourier coefficients of half-integral weight eigenforms is provided by the work of Shimura [Sh] and Waldspurger [Wal] relating the coefficients of such cuspforms to the central critical values of the L-functions of quadratic twists of even-weight newforms and by the connections (often conjectural) of such values to the Tate-Shafarevich groups of elliptic curves and the motives attached to newforms. Further motivation is provided by the connections between the coefficients of half-integral weight modular forms, class numbers of imaginary quadratic fields, and generalized Bernoulli numbers.

As a consequence of the aforementioned connections the Theorem has a number of corollaries of arithmetic interest. Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{2k}(N, \chi_0)$ be a newform with trivial Nebentypus χ_0, and let $L(f,s) := \sum_{n=1}^{\infty} a(n)n^{-s}$ be its L-function. Then $\Lambda(f,s) := (2\pi)^{-s}\Gamma(s)N^{s/2}L(f,s)$ satisfies the functional equation

$$\Lambda(f,s) = \epsilon \cdot \Lambda(f, 2k-s),$$

where $\epsilon = \pm 1$ is the sign of the functional equation. We shall be interested in the quadratic twists of this function. If $D \neq 0$, then let χ_D denote the Kronecker character for the field

$\mathbb{Q}(\sqrt{D})$, and if $D = 0$, then let χ_0 denote the trivial character. The D-quadratic twist of f, denoted f_D, is the newform corresponding to the twist of f by the character χ_D. If $D = 0$ or if $(D, N) = 1$, then $f_D(z) := \sum_{n=1}^{\infty} \chi_D(n)a(n)q^n$. Its L-function satisfies the functional equation

$$\Lambda(f_D, s) = \epsilon \cdot \chi_D(-N)\Lambda(f_D, 2k - s).$$

Combining the Theorem with the work of Waldspurger yields the following.

Corollary 1. *Let $f(z) \in S_{2k}(N, \chi_0)$ be a newform, let ϵ be the sign of the functional equation for $L(f, s)$, and let Ω be a period for f. Then for all but finitely many primes ℓ there are infinitely many fundamental discriminants D for which*

$$\epsilon D > 0 \quad \textit{and} \quad \left| \frac{L(f_D, k)D^{k-\frac{1}{2}}}{\Omega} \right|_\ell = 1.$$

There is also a 'local' version of Corollary 1.

Corollary 2. *Let $f(z) \in S_{2k}(N, \chi_0)$ be a newform, let ϵ be the sign of the functional equation for $L(f, s)$, and let Ω be a period for f. Let $\{p_1, p_2, \dots p_s\}$ be a finite set of primes, and $(\epsilon_1, \epsilon_2, \dots \epsilon_s) \in \{\pm 1\}^s$. For all but finitely many primes ℓ there are infinitely many fundamental discriminants D for which $\epsilon D > 0$, $\chi_D(p_i) = \epsilon_i$ for every $1 \le i \le s$, and*

$$\left| \frac{L(f_D, k)D^{k-\frac{1}{2}}}{\Omega} \right|_\ell = 1.$$

For an elliptic curve $E/\mathbb{Q}$ and a fundamental discriminant D let $L(E, s)$ denote the Hasse-Weil L-function for E, and let E_D denote the D-quadratic twist of E. As a special case of Corollary 1 we obtain the following partial resolution of a conjecture of Kolyvagin [Conjecture F, Ko2].

Corollary 3. *Let $E/\mathbb{Q}$ be a modular elliptic curve, and let ϵ be the sign of the functional equation for $L(E, s)$. If* Sha(E, D) *denotes the order of $Ш(E_D)$ as predicted by the Birch and Swinnerton-Dyer Conjecture, then for all but finitely many primes ℓ there are infinitely many fundamental discriminants for which*

$$\epsilon D > 0, \quad L(E_D, 1) \neq 0, \quad \textit{and} \quad \mathrm{Sha}(E, D) \not\equiv 0 \pmod{\ell}.$$

By virtue of a result of Rubin [Ru], restricting attention to elliptic curves having complex multiplication yields the following result about Tate-Shafarevich groups.

Corollary 4. *If $E/\mathbb{Q}$ is an elliptic curve with complex multiplication, then for all but finitely many primes ℓ there are infinitely many fundamental discriminants D for which $L(E_D, 1) \neq 0$ and*

$$|Ш(E_D)| \not\equiv 0 \pmod{\ell}.$$

Combining Corollaries 2 and 3 with work of Kolyvagin [Ko1] yields the following for elliptic curves of analytic rank 1.

Corollary 5. *Let $E/\mathbb{Q}$ be a modular elliptic curve for which $L(E,s)$ has a simple zero at $s=1$. For all primes ℓ outside a finite set which is effectively determinable (see Remark 2)*

$$ord_\ell(|\text{Ш}(E)|) \leq ord_\ell(\text{Sha}(E)),$$

where $\text{Sha}(E)$ *denotes the order of* $\text{Ш}(E)$ *as predicted by the Birch and Swinnerton-Dyer Conjecture.*

Most of the rest of this paper is devoted to proving the Theorem and deducing the corollaries. We conclude with a few remarks on the proofs and three examples of applications of the ideas therein (involving, respectively, CM-curves, Ramanujan's Delta function, and class numbers of fields of the form $\mathbb{Q}(\sqrt{-32n-20})$). Finally, we note that results similar to those in this paper have been obtained independently by Bruinier [B] and Jochnowitz [Jo1, Jo2] via different methods.

2. Results

If k is a positive integer, then let $S_k(N)$ denote the space of cusp forms of weight k on $\Gamma_1(N)$, and let $S_k^{cm}(N)$ denote the subspace of $S_k(N)$ spanned by those forms having complex multiplication (cf. [R2]). If χ is a Dirichlet character modulo N, then let $S_k(N,\chi)$ denote the subspace of $S_k(N)$ consisting of those forms having Nebentypus character χ. By the theory of newforms, every $f(z) \in S_k(N)$ can be uniquely expressed as a linear combination

$$f(z) = \sum_{i=1}^{r} \alpha_i A_i(z) + \sum_{j=1}^{s} \beta_j B_j(\delta_j z),$$

where $A_i(z)$ and $B_j(z)$ are newforms of weight k and level a divisor of N, and where each δ_j is a non-trivial divisor of N. Let

$$f^{\text{new}}(z) := \sum_{i=1}^{r} \alpha_i A_i(z) \quad \text{and} \quad f^{\text{old}}(z) := \sum_{j=1}^{s} \beta_j B_j(\delta_j z)$$

be, respectively, the *new part of* f and the *old part of* f.

For a non-negative integer k, let $M_{k+\frac{1}{2}}(N)$ (resp. $S_{k+\frac{1}{2}}(N)$) denote the space of modular forms (resp. cusp forms) of half-integral weight $k+\frac{1}{2}$ on $\Gamma_1(4N)$. If $i=0$ or 1, $0 \leq r < t$, and $a \geq 1$, then let $\theta_{a,i,r,t}(z)$ denote the Shimura theta function

$$\theta_{a,i,r,t}(z) := \sum_{n \equiv r \pmod{t}} n^i q^{an^2}.$$

If $\Theta(N)$ is the space of such functions of level $4N$, then the Serre-Stark Theorem [S-S] implies

$$\Theta(N) = M_{\frac{1}{2}}(N) \oplus \left\{ \text{subspace of } M_{\frac{3}{2}}(N) \text{ spanned by those } \theta_{a,1,r,t}(z) \text{ on } \ \Gamma_1(4N) \right\}.$$

If $g(z) \in M_{k+\frac{1}{2}}(N)$ and $h(z) \in \Theta(N')$, then $G_h(z) := g(z) \cdot h(z)$ is a modular form on $\Gamma_1(4NN')$ of integral weight $k+1$ or $k+2$.

Definition. *A modular form* $g(z) \in M_{k+\frac{1}{2}}(N)$ *is* **good** *if there exists some* N' *and some* $h(z) \in \Theta(N')$ *for which*

$$(G1) \quad G_h(z) \text{ is a cusp form.}$$
$$(G2) \quad G_h^{\text{new}}(z) \notin S_{k+1}^{cm}(4NN') \cup S_{k+2}^{cm}(4NN').$$

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, and for each rational prime ℓ, let $\overline{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$. Fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_\ell$. This fixes a choice of decomposition group D_ℓ. In particular, if K is any finite extension of $\mathbb{Q}$, and if $\mathcal{O}_K$ is the ring of integers of K, then for each ℓ this fixes a choice of a prime ideal $\mathfrak{p}_{\ell,K}$ of $\mathcal{O}_K$ dividing ℓ. Let $\mathbb{F}_{\ell,K}$ be the residue field of $\mathfrak{p}_{\ell,K}$, and let $|\cdot|_\ell$ be an extension to $\overline{\mathbb{Q}}_\ell$ of the usual ℓ-adic absolute value on $\mathbb{Q}_\ell$.

If $f(z) = \sum_{n=1}^\infty a(n)q^n \in S_k(N,\chi)$ is a newform, then the $a(n)$'s are algebraic integers and generate a finite extension of $\mathbb{Q}$, say K_f. If K is any finite extension of $\mathbb{Q}$ containing K_f, and if ℓ is any prime, then by the work of Eichler, Shimura, Deligne, and Serre (see [D], [D-S]) there is a continuous, semisimple representation

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_{\ell,K})$$

for which

$$(R1) \quad \rho_{f,\ell} \text{ is unramified at all primes } p \nmid N\ell.$$
$$(R2) \quad \text{trace } \rho_{f,\ell}(\text{frob}_p) = a(p) \bmod \mathfrak{p}_{\ell,K} \text{ for all primes } p \nmid N\ell.$$
$$(R3) \quad \det \rho_{f,\ell}(\text{frob}_p) = \chi(p)p^{k-1} \bmod \mathfrak{p}_{\ell,K} \text{ for all primes } p \nmid N\ell.$$
$$(R4) \quad \det \rho_{f,\ell}(c) = -1 \text{ for any complex conjugation } c.$$

Here frob_p denotes any Frobenius element for the prime p. These representations capture many properties of the reductions of the $a(n)$'s modulo $\mathfrak{p}_{\ell,K}$.

Proof of Theorem. Since $g(z)$ is good, there exists a Shimura theta function $h(z) \in \Theta(N')$ for which $G_h(z) = g(z) \cdot h(z)$ satisfies $(G1)$ and $(G2)$. If $G_h(z) = \sum_{n=1}^\infty a(n)q^n$, and if $h(z) = \sum_{n=0}^\infty b(n)q^{an^2}$, then

$$a(n) = \sum_{\substack{x,y \\ x+ay^2=n}} c(x)b(y). \tag{3}$$

Since the $c(x)$'s and $b(y)$'s are algebraic integers, the same is true of the $a(n)$'s.

Let k' be the weight of $G_h(z)$ (so k' is either $k+1$ or $k+2$), and let $\mathcal{N}_0$ be the set of newforms of weight k' and level dividing $4NN'$. The new part of $G_h(z)$ can be uniquely expressed as a linear combination

$$G_h^{\text{new}}(z) = \sum_{f(z) \in \mathcal{N}_0} \alpha_f f(z). \tag{4}$$

Since the Fourier coefficients of $G_h(z)$ are algebraic, the same is true for those of $G_h^{\rm new}(z)$ and $G_h^{\rm old}(z)$, and each α_f. Note that by $(G2)$ some α_f is non-zero.

A critical feature of the proof is the proper 'bookkeeping' of newforms which are related via twisting and Galois conjugation. We now fix our notation. Let X be the set of Dirichlet characters of conductor dividing $8NN'$, and let

$$\mathcal{N} = \{f_\chi(z) \ : f \in \mathcal{N}_0,\ \chi \in X\},$$

where f_χ is the newform corresponding to the twist of f by χ. Each newform in $\mathcal{N}$ has level divisible only by primes dividing $4NN'$ and the conductor of its Nebentypus character is a divisor of $4NN'$. Let K be a finite, Galois extension of $\mathbb{Q}$ containing the Fourier coefficients of each $f \in \mathcal{N}$, the α_f's, the Fourier coefficients of $G_h^{\rm old}(z)$, and the values of the characters in X.

If $f \in \mathcal{N}$, then let $G_f \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the subgroup stabilizing the set

$$\mathcal{N}_f := \{f_\chi(z) \ : \ \chi \in X\}.$$

For each prime ℓ, let $D_{f,\ell} := G_f \cap D_\ell$, and let $\mathbb{F}_{f,\ell} := \mathbb{F}_{\ell,K}^{D_{f,\ell}}$.

Fix a prime ℓ for which:

- $(L1)$ K is unramified at ℓ.
- $(L2)$ $\ell \nmid 4NN'$ and $\ell > 2(k+2)$.
- $(L3)$ If $\alpha_f \neq 0$, then $|\alpha_f|_\ell = 1$.
- $(L4)$ The characters $\chi \in X$, viewed as taking values in $\mathbb{F}_{\ell,K}$, are distinct.
- $(L5)$ The representations $\rho_{f,\ell}$ $(f \in \mathcal{N})$ are pairwise non-isomorphic.
- $(L6)$ If $f \in \mathcal{N}$ does not have complex multiplication, then the image of $\rho_{f,\ell}$ contains a normal subgroup H_f conjugate to $SL_2(\mathbb{F}_{f,\ell})$ and for which $\mathrm{Im}\rho_{f,\ell}/H_f$ is abelian.

It is clear that $(L1) - (L4)$ hold for all sufficiently large primes ℓ. Property $(L5)$ is also true for all large primes. For if not, then $\rho_{f_1,\ell} \cong \rho_{f_2,\ell}$ for some $f_1, f_2 \in \mathcal{N}$ and for infinitely many primes ℓ. It then follows from $(R2)$ that $a_{f_1}(p) = a_{f_2}(p)$ for all primes $p \nmid 4NN'$, contradicting 'multiplicity one' for newforms [Theorem 4.6.19, Mi]. Ribet [R3], following the ideas of Serre [Se], has shown that $(L6)$ holds for all large primes. This property essentially asserts that the image of $\rho_{f.\ell}$ is almost always 'as big as possible.'

For each $f \in \mathcal{N}_0$, let $S_f \subset D_\ell$ be a set of representatives for the classes $D_\ell/D_{f,\ell}$, and put $\mathcal{N}_{f,\ell} = \cup_{\sigma \in S_f} \mathcal{N}_{f^\sigma}$, a disjoint union. Let $\mathcal{N}' = \{f_1(z), f_2(z), ..., f_u(z)\}$ be a subset of $\mathcal{N}_0$ such that $\mathcal{N}$ is a disjoint union of the $\mathcal{N}_{f_i,\ell}$'s. We assume that $f_1(z), ..., f_v(z)$ do not have complex multiplication and that $f_{v+1}(z), ..., f_u(z)$ do. Since $G_h(z)$ satisfies $(G2)$, $f_1(z)$ can be chosen so that the coefficient α_{f_1} of $f_1(z)$ in (4) is non-zero. Write $f_i(z) = \sum_{n=1}^\infty a_i(n)q^n$, write ρ_i for $\rho_{f_i,\ell}$, S_i for S_{f_i}, H_i for H_{f_i}, and $\mathbb{F}_i$ for $\mathbb{F}_{f_i\ell}$. In this way we are able to conveniently keep track of those distinct newforms which are closely related.

Lemma. *With the above notation,*

(*i*) *The image of* $\rho_1 \times \cdots \times \rho_v$ *contains a normal subgroup conjugate to* $SL_2(\mathbb{F}_1) \times \cdots \times SL_2(\mathbb{F}_v)$.

(*ii*) *If* $f_i(z)$ *does not have complex multiplication, then for each positive integer* d *and each* $w \in \mathbb{F}_i$, *a positive density of primes* $p \equiv 1 \pmod{d}$ *satisfies*

$$a_i(p) \equiv w \pmod{\mathfrak{p}_{\ell,K}}.$$

(*iii*) *If* $f_i(z)$ *does not have complex multiplication, then for each pair of coprime positive integers* r, d, *a positive density of primes* $p \equiv r \pmod{d}$ *satisfies*

$$|a_i(p)|_\ell = 1.$$

Proof of Lemma. Part (*i*) is surely well-known, and in any event can be proved by a simple modification of the arguments in [R1], [R3], and [Se]. Without loss of generality, we can assume that $H_i = SL_2(\mathbb{F}_i)$. Let

$$H := \bigcap_{i=1}^{v} \rho_i^{-1}(H_i).$$

The map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/H \hookrightarrow \mathrm{Im}\rho_1/H_1 \times \cdots \times \mathrm{Im}\rho_v/H_v$ is injective, hence by (*L*6) the quotient $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/H$ is abelian. It follows that $\mathrm{Im}\rho_i/\rho_i(H)$ is also abelian. Since $\rho_i(H) \subseteq H_i$ and since $H_i = SL_2(\mathbb{F}_i)$ has no non-trivial abelian quotients, $\rho_i(H) = H_i$. It suffices to show that $(\rho_1 \times \cdots \times \rho_v)(H)$ contains $SL_2(\mathbb{F}_1) \times \cdots \times SL_2(\mathbb{F}_v)$. By [Lemma 3.3, R1], it suffices to show that $(\rho_i \times \rho_j)(H)$ contains $SL_2(\mathbb{F}_i) \times SL_2(\mathbb{F}_j)$ if $i \neq j$. Arguing as in the proofs of [Lemme 8, §6.2, Se] and [Theorem 3.8, R1], one easily sees that if this is not true, then there is a $\sigma \in D_\ell$ such that $\rho_i^\sigma \cong \rho_j \otimes \phi$ for some Dirichlet character ϕ unramified at primes not dividing $4NN'\ell$. Arguing as in the proof of [Theorem 6.1, R1], one sees that since $\ell > 2(k+2)$ (see (*L*2)) ϕ is unramified at ℓ. Ribet's arguments employ various results of Swinnerton-Dyer about level 1 modular forms mod ℓ, which have been generalized to higher level by Katz [Ka] (see also [§4, Gr]). Now, comparing determinants shows that the conductor of ϕ^2 divides $4NN'$, so the conductor of ϕ divides $8NN'$. Therefore, $f^\sigma(z)$ and $f_\phi(z)$ are in $\mathcal{N}$ and $\rho_{f^\sigma,\ell} \cong \rho_{f_\phi,\ell}$, contradicting (*L*5). This proves part (*i*).

Parts (*ii*) and (*iii*) are simple consequences of property (*L*6). Let $\epsilon : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/d)^\times$ be the character defined by $\epsilon(\sigma) = s$ if $\zeta_d^\sigma = \zeta_d^s$. The condition $p \equiv r \pmod{d}$ is equivalent to $\epsilon(\mathrm{frob}_p) = r$. Since $SL_2(\mathbb{F}_i)$ has no non-trivial abelian quotient, the image of $\rho_i \times \epsilon$ contains $SL_2(\mathbb{F}_i) \times 1$. Let $g = \left(\begin{smallmatrix} 0 & 1 \\ -1 & w \end{smallmatrix}\right) \in SL_2(\mathbb{F}_i)$. By the Chebotarev Density Theorem, a positive proportion of primes p satisfy $(\rho_i \times \epsilon)(\mathrm{frob}_p) = (g, 1)$. For such a p,

$$a_i(p) \equiv \mathrm{trace} \begin{pmatrix} 0 & 1 \\ -1 & w \end{pmatrix} \equiv w \pmod{\mathfrak{p}_{\ell,K}} \quad \text{and} \quad p \equiv \epsilon(\mathrm{frob}_p) \equiv 1 \pmod{d}.$$

This proves part (*ii*). Now choose $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\epsilon(\sigma) = r$. Clearly, there exists some $g \in SL_2(\mathbb{F}_i)$ for which trace $(\rho_i(\sigma) \cdot g) \neq 0$. Again by the Chebotarev Density Theorem, a positive proportion of the primes p satisfy $(\rho_i \times \epsilon)(\mathrm{frob}_p) = (\rho_i(\sigma), r)(g, 1) = (\rho_i(\sigma) \cdot g, r)$. This proves part (iii).

Q.E.D. Lemma

Returning to the proof of the theorem, rewrite (4) as

$$G_h^{\mathrm{new}}(z) = \sum_{i=1}^{u} \sum_{\sigma \in S_i} \sum_{\chi \in X} \alpha(\sigma, i, \chi) f_{i,\chi}^{\sigma}(z), \tag{5}$$

where $\alpha(\sigma, i, \chi) = \alpha_{f_{i,\chi}^{\sigma}}$, and define $a(n)^{\mathrm{new}}$ by $G_h^{\mathrm{new}}(z) = \sum_{i=1}^{\infty} a(n)^{\mathrm{new}} q^n$. If n is a positive integer relatively prime to $4NN'$, then by (5)

$$a(n)^{\mathrm{new}} = \sum_{i=1}^{u} \sum_{\sigma \in S_i} \left(\sum_{\chi \in X} \alpha(\sigma, i, \chi) \chi^{\sigma}(n) \right) a_i(n)^{\sigma}. \tag{6}$$

If σ_1 is the element of S_1 for which $f_1^{\sigma_1} = f_1$, then $\alpha(\sigma_1, 1, \chi_0) = \alpha_{f_1} \neq 0$. By $(L3)$, $|\alpha(\sigma_1, 1, \chi_0)|_\ell = 1$, and from $(L4)$, one sees easily that there is an integer r relatively prime to $4NN'$ for which $|\sum_{\chi \in X} \chi^{\sigma_1}(r)|_\ell = 1$. Fix such an r, and put

$$\lambda(\sigma, i) = \sum_{\chi \in X} \alpha(\sigma, i, \chi) \chi^{\sigma}(r), \quad (1 \leq i \leq u;\ \sigma \in S_i).$$

By (6),

$$a(n)^{\mathrm{new}} = \sum_{i=1}^{u} \sum_{\sigma \in S_i} \lambda(\sigma, i) a_i(n)^{\sigma} \quad \text{if} \quad n \equiv r \pmod{8NN'}.$$

Suppose that there are only finitely many square-free integers m for which $|c(m)|_\ell = 1$. Let these be $m_1, ..., m_t$. Let N'' be the product of the odd prime factors of $NN'm_1 \cdots m_t$. Let r_1 and d_1 be relatively prime positive integers such that if p is any prime congruent to r_1 modulo d_1, then p does not split in any imaginary quadratic subfield having discriminant a divisor of $4N''$. Choose a prime p_1 for which $p_1 \nmid 4N''$, $p_1 \equiv r_1 \pmod{d_1}$, and $|a_1(p_1)|_\ell = 1$. This is possible by part (iii) of the Lemma. If $v+1 \leq i \leq u$, then $a_i(p_1) = 0$ since $f_i(z)$ has complex multiplication. Choose a prime p_2 not dividing $4N''$ and for which $|a_1(p_2)|_\ell = 1$ and $|a_i(p_2)|_\ell < 1$ $(i = 2, ..., v)$. This is possible by part (i) of the Lemma. For example, let $g \in \mathrm{Im}(\rho_1 \times \cdots \times \rho_v)$ be conjugate to

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \times \cdots \times \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

By the Chebotarev Density Theorem, a positive proportion of primes $p \nmid 4N''$ satisfy $(\rho_1 \times \cdots \times \rho_v)(\mathrm{frob}_p) = g$. Any such prime clearly has the desired properties. Next, choose a prime p_3 for which $p_3 \equiv r(p_1p_2)^{-1} \pmod{8NN'}$ and $|a_1(p_3)|_\ell = 1$. This is possible by part (*iii*) of the Lemma.

For $w \in \mathcal{O}_K$, write $\overline{w}$ for its image in $\mathbb{F}_{\ell,K}$. Since $|\lambda(\sigma_1, 1)a_1(p_1p_2p_3)^{\sigma_1}|_\ell = 1$, and since $|\lambda(\sigma, 1)a_1(p_1p_2p_3)^{\sigma}|_\ell \leq 1$ for all $\sigma \in S_1$, one sees easily that there is some $w \in \mathcal{O}_K$ for which

$$\overline{w} \in \mathbb{F}_1^\times \quad \text{and} \quad |\sum_{\sigma \in S_1} \lambda(\sigma, 1)a_1(p_1p_2p_3)^{\sigma} w^{\sigma}|_\ell = 1. \tag{7}$$

Now choose a prime p_4 for which $p_4 \equiv 1 \pmod{8NN'}$ and $a_1(p_4) \equiv w \pmod{\mathfrak{p}_{\ell,K}}$. This is possible by part (*ii*) of the Lemma. Let $m = p_1p_2p_3p_4$. By the multiplicitivity of the Fourier coefficients of a newform, it follows from the choices of p_1 and p_2 that

$$|a_i(m)|_\ell < 1, \quad (i = 2, ..., u).$$

Therefore, by (7)

$$|\sum_{i=2}^{u} \sum_{\sigma \in S_i} \lambda(\sigma, i)a_i(m)^{\sigma}|_\ell < 1 \quad \text{and} \quad |\sum_{\sigma \in S_1} \lambda(\sigma, 1)a_1(m)^{\sigma}|_\ell = 1,$$

so

$$|a(m)^{\text{new}}|_\ell = 1.$$

Since m is prime to $4NN'$, the mth coefficient of G^{old} is zero, so it follows that

$$|a(m)|_\ell = |a(m)^{\text{new}}|_\ell = 1. \tag{8}$$

By (3) and the fact that $g(z)$ is an eigenform, m must be of the form

$$m = m_j x^2 + ay^2 \tag{9}$$

for some $j \in \{1, ..., t\}$ and some integers x and y. Since $m_jX^2 + aY^2$ is a positive definite quadratic form with discriminant, say d_j, a divisor of $4N''$, a necessary condition for a solution of (9) is that $\left(\frac{d_j}{p}\right) = 1$ for every prime divisor of p of m. But $m = p_1p_2p_3p_4$ was chosen so that $\left(\frac{d_j}{p_1}\right) = -1$ for each d_j. This contradiction proves the theorem.

Q.E.D. Theorem

We now turn to the proofs of the corollaries. Suppose $f(z) \in S_{2k}(N, \chi_0)$ is a newform and that $\epsilon \in \{\pm 1\}$ is the sign of the functional equation for $L(f, s)$. If D is a fundamental discriminant, then let D_0 be defined by

$$D_0 := \begin{cases} |D| & \text{if } D \text{ is odd,} \\ |D|/4 & \text{if } D \text{ is even.} \end{cases}$$

A non-zero complex number $\Omega \in \mathbb{C}^\times$ is a *period for* $f(z)$ if

$$\frac{L(f_D,k)D_0^{k-\frac{1}{2}}}{\Omega}, \quad \epsilon D > 0, \tag{10}$$

is always an algebraic number (this is a slight abuse of standard terminology). A period Ω is *nice* if the quantity (10) is always an algebraic integer. That nice periods exist is essentially a result of Shimura and follows easily from the theory of modular symbols (cf. [M-T-T] and [Theorem 3.5.4, G-S]). Moreover, any period is a multiple of a nice period by some algebraic number. As a consequence of the Theorem we obtain Corollary 1.

Proof of Corollary 1. Since any period is the multiple of a nice one by an algebraic number, it suffices to prove the corollary for Ω a nice period. There is a twist f_χ, $\chi(-1) = (-1)^k\epsilon$, satisfying Hypotheses H1 and H2 of [pp. 377-378 , Wal]. By [Théorème 1, Wal] there is an integer N' and an eigenform $g(z) = \sum_{n=1}^{\infty} c(n)q^n \in S_{k+\frac{1}{2}}(N')$ such that $N|N'$ and for each fundamental discriminant D for which $\epsilon D > 0$

$$c(D_0)^2 = \begin{cases} \varepsilon_D \frac{L(f_D,k)D_0^{k-\frac{1}{2}}}{\Omega} & \text{if } D_0 \text{ is relatively prime to } 4N', \\ 0, & \text{otherwise,} \end{cases} \tag{11}$$

where ε_D is an algebraic integer with $|\varepsilon_D|_\ell = 1$. If $g(z)$ is good, then the conclusion of the corollary follows from the theorem.

Let p be a prime that does not divide $4N'$ and that does not split in any imaginary quadratic field having discriminant dividing $4N'$. By [Theorem B(i), F-H], there is a fundamental discriminant D' such that $p|D'$, $\epsilon D' > 0$, D' is relatively prime to $4N'$, and $L(f_{D'},k) \neq 0$. It follows from (11) that $c(D') \neq 0$. For sufficiently large integers ν, the D'th Fourier coefficient of the cusp form $G_\nu(z) = g(z) \cdot \theta_{N'^\nu,0,1,1}(z) \in S_{k+1}(4{N'}^{\nu+1})$ is equal to $c(D')$ and therefore is non-zero. Since D' is coprime to $4N'$, the D'th coefficient of $G_\nu^{\text{old}}(z)$ is zero. Therefore $c(D')$ is the D'th coefficient of $G_\nu^{\text{new}}(z)$, and the former being non-zero implies the same for the latter. Furthermore, the choice of p implies that the new part of $G_\nu(z)$ is not contained in $S_{k+1}^{cm}(4{N'}^{\nu+1})$ (as the pth Fourier coefficient of any CM-form of level dividing $4{N'}^{\nu+1}$ is zero). This proves that $g(z)$ is good and completes the proof of the corollary.

Q.E.D.

Proof of Corollary 2. Let $g(z) \in S_{k+\frac{1}{2}}(N')$ be as in the proof of Corollary 1. By taking combinations of quadratic twists of g (and possibly twists of twists) one obtains an eigenform $g^*(z)$ whose coefficients are supported on integers of the form D_0m^2 for those discriminants D for which $\chi_D(p_i) = \epsilon_i$ for each i. A straightforward generalization of the proof of Corollary 1 shows that $g^*(z)$ is good (in particular, it is non-zero).

Q.E.D.

Proof of Corollary 3. Let $E/\mathbb{Q}$ be a modular elliptic curve, let N be the conductor of E, and let ϵ be the sign of the functional equation for $L(E,s)$. For each fundamental discriminant $\epsilon D > 0$, let E_D be the D-quadratic twist of E. Let ω_D be a Neron differential on E_D, and let

$$\Omega_D = \int_{E_D(\mathbb{R})} |\omega_D|.$$

Write Ω_E for Ω_ϵ. Then

$$\Omega_D D_0^{\frac{1}{2}} = \Omega_E. \tag{12}$$

Since E is modular, it follows that

$$\frac{L(E_D,1)}{\Omega_D} \in \mathbb{Q}. \tag{13}$$

However, much more is conjectured to be true. The Birch and Swinnerton-Dyer Conjecture states that if $L(E_D,1) \neq 0$, then

$$\frac{L(E_D,1)}{\Omega_D} = \frac{|\text{Ш}(E_D)|}{|E_D(\mathbb{Q})_{tor}|^2} Tam(E_D), \tag{14}$$

where $Tam(E_D)$ is the Tamagawa factor. Moreover, $Tam(E_D)/Tam(E_\epsilon)$ is an integer divisible only by the primes 2 or 3. By the work of Mazur [Ma] the order of the torsion group $E_D(\mathbb{Q})_{tor}$ is not divisible by any prime $p > 7$. Since E is modular, there is a newform $f(z) \in S_2(N, \chi_0)$ such that $L(E,s) = L(f,s)$. More generally,

$$L(E_D,s) = L(f_D,s). \tag{15}$$

It follows from (12), (13), and (14) that Ω_E is a period for $f(z)$. The conclusion of the corollary follows from Corollary 1.

Q.E.D.

Proof of Corollary 4. Rubin [Ru] has shown that if $E/\mathbb{Q}$ is an elliptic curve having complex multiplication by the CM field K, then the only possible primes $p \nmid |O_K^\times|$ dividing $|\text{Ш}(E_D)|$ are those predicted by the Birch and Swinnerton-Dyer Conjecture. This, together with (12), (13), and (14) implies that

$$\ell > 7, \quad |\text{Ш}(E_D)| \equiv 0 \pmod{\ell} \quad \Rightarrow \quad \ell \text{ divides the numerator of } \frac{L(E_D,1)\sqrt{D_0}}{\Omega_E}.$$

Q.E.D.

Proof of Corollary 5. This is just [Corollary G, Ko2], which is conditional on part (i) of [Conjecure F, Ko2] where the discriminants satisfy the congruence condition $D \equiv \square \pmod{4N}$.

Corollary 2 removes this condition for all but finitely many primes ℓ, and the proof of the Theorem shows how to effectively determine this finite set (see Remark 2).

Q.E.D.

Remark 1. Theorem 1 is a result about the coefficients of an eigenform $g(z)$ of half-integral weight. However, the proof can be applied in a slightly different setting. Let N be an odd square-free integer, and let $f(z) \in S_{2k}(N, \chi_0)$ be a newform. Kohnen and Zagier [K], [K-Z] have constructed an explicit cusp form $g(z) = \sum_{n=1}^{\infty} c(n)q^n \in S_{k+\frac{1}{2}}(N)$ for which $c(n) = 0$ unless $(-1)^k n \equiv 0, 1 \pmod 4$ and for which

$$L(f_D, k) = 2^{-\nu(N)} |D|^{\frac{1}{2}-k} \frac{\pi^k}{(k-1)!} \frac{\langle f, f\rangle}{\langle g, g\rangle} |c(|D|)|^2$$

for any fundamental discriminant D for which $(-1)^k D > 0$ and $\chi_D(\ell) = w_\ell$, the eigenvalue of the Atkin-Lehner involution at ℓ, for each prime ℓ dividing N. The conclusion and proof of the Theorem apply (*mutatis mutandis*).

Remark 2. Let $E/\mathbb{Q}$ be a modular elliptic curve with conductor N for which $L(E, s)$ has a simple zero at $s = 1$. Let $g(z)$ be the relevant half-integral weight eigenform, and let $h(z)$ be a theta function for which $G_h(z) = g(z) \cdot h(z)$ satisfies $(G1)$ and $(G2)$. Let S_1 denote the set of primes ℓ not satisfying $(L1) - (L6)$. If $c(E)$ denotes the Manin constant for E, and D denotes the discriminant of $End(E)$, then define S_2 by

$$S_2 := \{\ell \mid 6D, \ell \mid Tam(E), \ell \mid c(E)\}.$$

If E does not have complex multiplication, then let S_3 denote the finite set of primes ℓ for which the $\ell-$adic representation of the Tate module is not surjective, and if E has complex multiplication then let S_3 be empty. The conclusion of Corollary 5 holds for every prime $\ell \notin S_1 \cup S_2 \cup S_3$.

3. Examples

Example 1. If $N \neq 0$ is an integer, then let $E(N)$ denote the elliptic curve/$\mathbb{Q}$

$$E(N): \quad y^2 = x^3 - N^2 x.$$

Let $g_1(z) := \sum_{n=1}^{\infty} a_1(n)q^n \in S_{\frac{3}{2}}(128, \chi_0)$ and $g_2(z) := \sum_{n=1}^{\infty} a_2(n)q^n \in S_{\frac{3}{2}}(128, \chi_2)$ be the eigenforms defined by

$$g_i(z) := \eta(8z)\eta(16z)\Theta(2^i z).$$

Recall that $\eta(z) := q^{1/24} \prod_{n=1}^{\infty}(1 - q^n)$. If $N \geq 1$ is an odd square-free integer, then Tunnell [T] proved, assuming the Birch and Swinnerton-Dyer Conjecture, that

$$|\text{Ш}(E(iN))| = \left(\frac{a_i(N)}{2^{\nu(N)}}\right)^2 \quad \text{if} \quad a_i(N) \neq 0. \tag{16}$$

If $F(z) := g_1(z)\Theta(4z) = g_2(z)\Theta(2z) = \eta(8z)\eta(16z)\Theta(2z)\Theta(4z)$, then

$$F^*(z) := \sum_{n \not\equiv 7 \pmod 8} A(n)q^n - \sum_{n \equiv 7 \pmod 8} A(n)q^n$$

is in $S_2^{\text{new}}(128, \chi_0)$ and does not have complex multiplication. The new part of $F(z)$ is easily seen to be a linear combination of $F^*(z)$ and its twists by Dirichlet characters modulo 8, so $g_1(z)$ and $g_2(z)$ are both good. By Theorem 1, for all sufficiently large primes ℓ, there are infinitely many odd, square-free integers N and M for which $a_1(N) \not\equiv 0 \pmod \ell$ and $a_2(M) \not\equiv 0 \pmod \ell$. In fact, a quick inspection of the proof of the theorem shows that in this case 'sufficiently large' means that the image of $\rho_{F^*,\ell}$ is conjugate to $GL_2(\mathbb{F}_\ell)$. The eigenform $F^*(z)$ is the newform associated to the elliptic curve $y^2 = x^3 + 2x^2 - x$ which is a quadratic twist of $y^2 = x^3 - 2x^2 - x$. Serre [5.9.1, Se] has shown that the image of the mod ℓ Galois representation of the latter curve is $GL_2(\mathbb{F}_\ell)$ for every odd prime ℓ. The same is therefore true for $\rho_{F^*,\ell}$.

By Rubin's theorem [Ru] and (16), if ℓ is an odd prime, then there are infinitely many odd square-free integers N and M for which $E(N)$ and $E(2M)$ have rank 0 and Ш$(E(N))$ and Ш$(E(2M))$ have no elements of order ℓ. The analogous statement when $\ell = 2$ is well known and follows from 2-descents.

Example 2. Let $\Delta(z) = \eta^{24}(z) = \sum_{n=1}^{\infty} \tau(n)q^n \in S_{12}(1)$ denote Ramanujan's cusp form, and let $g(z) = \sum_{n=1}^{\infty} c(n)q^n \in S_{\frac{13}{2}}(4, \chi_0)$ denote the eigenform defined by

$$g(z) := \frac{\Theta^9(z)\eta^8(4z)}{\eta^4(2z)} - \frac{18\Theta^5(z)\eta^{16}(4z)}{\eta^8(2z)} + \frac{32\Theta(z)\eta^{24}(4z)}{\eta^{12}(2z)}.$$

Kohnen and Zagier proved [K-Z] that if $D > 0$ is a fundamental discriminant, then

$$L(\Delta_D, 6) = \left(\frac{\pi}{D}\right)^6 \frac{\sqrt{D}}{5!} \frac{\langle \Delta(z), \Delta(z) \rangle}{\langle g(z), g(z) \rangle} \cdot c(D)^2. \tag{17}$$

If $F(z) := g(z)\Theta(z) \in S_7(4, \chi_{-1})$, then $F(z) = \dfrac{\mathfrak{B}_1(z) + \mathfrak{B}_2(z)}{2}$, where $\mathfrak{B}_1(z)$ and $\mathfrak{B}_2(z)$ are complex conjugate newforms in $S_7(4, \chi_{-1})$ and where $\mathfrak{B}_1(z)$ is given by

$$\mathfrak{B}_1(z) = \left(1 - \frac{\sqrt{-15}}{15}\right) F(z) + \frac{\sqrt{-15}}{30} F(z) | U_2.$$

The first few terms of the Fourier expansion of $\mathfrak{B}_1(z) = \sum_{n=1}^{\infty} b(n)q^n$ are:

$$\mathfrak{B}_1(z) = q + (2 - 2\sqrt{-15})q^2 + 8\sqrt{-15}q^3 - (56 + 8\sqrt{-15})q^4 + 10q^5 + \ldots$$

Since $\mathfrak{B}_1(z)$ and $\mathfrak{B}_2(z)$ do not have complex multiplication, for all sufficiently large primes ℓ there exist infinitely many fundamental discriminants $D > 0$ for which $c(D) \not\equiv 0 \pmod \ell$

(see Remark 2). As $\mathfrak{B}_2(z)$ is the newform associated to the twist of $\mathfrak{B}_2(z)$ by χ_{-1}, an inspection of the proof of Theorem 1 shows that in this case 'sufficiently large' means $\rho_{\mathfrak{B}_1,\ell}$ is 'big' (i.e. ($L6$) holds). It is straightforward to check that $\rho_{\mathfrak{B}_1,\ell}$ is irreducible if $\ell \neq 2$, 5, or 61. This can be done by writing down all the possibilities for a reducible $\rho_{\mathfrak{B}_1,\ell}$ and then comparing with the Fourier coefficients of $\mathfrak{B}_1(z)$ using ($R2$). As in the proofs of [Lemma 5.7, R1] and [Theorem 2.1, R3], if $\rho_{\mathfrak{B}_1,\ell}$ is not 'big', then either its image is dihedral, or for each prime $p \nmid N\ell$

$$\bar{b}(p)^2/\chi_{-1}(p)p^6 \in \{0,1,2,4\} \quad \text{or} \quad \bar{b}(p)^4 - 3\chi_{-1}(p)\bar{b}(p)^2p^6 + p^{12} = 0,$$

where $\bar{b}(p)$ denotes the image of $b(p)$ in $\mathbb{F}_{\mathfrak{B}_1,\ell}$. A simple check of the Fourier coefficients of $\mathfrak{B}_1$ shows that $\rho_{\mathfrak{B}_1,\ell}$ is 'big' if $\ell \neq 2, 3, 5$ or 61. We leave it to the reader to determine what happens at $\ell = 2$ and 3. For $\ell = 5$ and $\ell = 61$ we find that

$$\mathfrak{B}_1(z) + \mathfrak{B}_2(z) \equiv \begin{cases} E_{\chi_{-1}\omega,\omega^{-1}} + E_{\omega,\chi_{-1}\omega^{-1}} & \pmod 5, \\ E_{\chi_0,\chi_{-1}} + E_{\chi_{-1},\chi_0} & \pmod{61}, \end{cases}$$

where $E_{\phi,\psi}$ is the Eisenstein series whose L-function is $L(\phi,s)L(\psi,s-6)$. These congruences, together with the definition of $F(z)$, yield the following Kronecker-style congruences

$$\sum_{k=-\infty}^{\infty} c(N-k^2) \equiv \begin{cases} \frac{1}{2}N\sum_{d\mid N}\left(\chi_{-1}(d)+\chi_{-1}(N/d)\right)d^4 & \pmod 5, \\ \frac{1}{2}\sum_{d\mid N}\left(\chi_{-1}(d)+\chi_{-1}(N/d)\right)d^6 & \pmod{61}. \end{cases} \tag{18}$$

Example 3. In this example we examine ℓ-indivisibility of class numbers of imaginary quadratic fields. Since obtaining indivisibility results follow easily by Kronecker's class number relations (cf. [Ha]), we select an arithmetic progression of discriminants for which these indivisibility results do not follow so easily. We investigate the ℓ-indivisibility of the class numbers $h(-32n-20)$. Using the following identity of Jacobi

$$\frac{\eta^2(16z)}{\eta(8z)} := \sum_{n=0}^{\infty} q^{(2n+1)^2},$$

it is easy to see that

$$\frac{\eta^4(32z)}{\eta(8z)} = \frac{\eta^2(16z)}{\eta(8z)}\left(\frac{\eta^2(32z)}{\eta(16z)}\right)^2 = \sum_{n\geq 5 \text{ odd}} c(n)q^n = \sum_{x,y,z\geq 1 \text{ odd}} q^{x^2+2y^2+2z^2}.$$

Since the ternary quadratic form $x^2+2y^2+2z^2$ is the only class in its genus, if $8n+5$ is square-free, then $h(-32n-20) = 2c(n)$. Incidentally, if $n \equiv 5 \pmod 8$, then $c(n)$ is the number of 4−core partitions of $\frac{n-5}{8}$ (see [O-S]).

If $F(z) \in S_3(32, \chi_{-1})$ is defined by

$$F(z) := \frac{\eta^4(16z)}{\eta(4z)}\eta^3(4z) = q^3 - 2q^7 - q^{11} + 2q^{15} + \dots,$$

then by Jacobi's triple product identity

$$\eta^3(8z) := \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{(2n+1)^2},$$

we find that

$$F(z) = \sum_{\substack{n\geq 5\\ x\geq 0}}(-1)^x(2x+1)c(n)q^{(n+(2x+1)^2)/2}.$$

Moreover, $F(z) = \dfrac{\mathfrak{B}_2(z) - \mathfrak{B}_1(z)}{8i}$, where $\mathfrak{B}_1(z)$ and $\mathfrak{B}_2(z) \in S_3(32, \chi_{-1})$ are complex conjugate newforms in $S_3(32, \chi_{-1})$ which do not have complex multiplication, and $\mathfrak{B}_1(z)$ is given by

$$\mathfrak{B}_1(z) := F(z)|T_3 - 4iF(z) = q - 4iq^3 + 2q^5 + 8iq^7 - 7q^9 + \cdots$$

Just as in Example 2, $\mathfrak{B}_2(z)$ is also the newform associated to the twist of $\mathfrak{B}_1(z)$ by χ_{-1}. While $\dfrac{\eta^4(32z)}{\eta(8z)}$ is an eigenform, $\dfrac{\eta^4(16z)}{\eta(4z)}$ is not, so we cannot appeal directly to Theorem 1. However the methods used to prove Theorem 1 show that if ℓ is any odd prime for which $\rho_{\mathfrak{B}_1,\ell}$ is 'big' (i.e. for which $(L6)$ holds), then there are infinitely many fundamental discriminants $-32n-20$ for which $h(-32n-20) \not\equiv 0 \pmod{\ell}$. The arguments employed in the previous example show that if $\ell \geq 5$, then $\rho_{\mathfrak{B}_1,\ell}$ is big. Again, we leave the case where $\ell = 3$ to the reader.

4. Concluding remarks

It is unfortunate that the Theorem only pertains to good forms $g(z)$. However, this condition is expected to be very mild. For suppose $g(z) = \sum_{n=1}^{\infty} c(n)q^n \in S_{k+\frac{1}{2}}(N, \chi_d)$ is a 'bad' eigenform lifting to a newform $f(z) \in S_{2k}(N', \chi_0)$ satisfying Hypotheses H1 and H2 of [Wal]. By [Cor. 2, Wal] there is at least one arithmetic progression $r \pmod{t}$ for which every square-free positive integer $n \equiv r \pmod{t}$ has the property that the sign of the functional equation of $L(f_{(-1)^k dn}, s)$ is $+1$ and

$$L(f_{(-1)^k dn}, k) = c(n)^2 \cdot A_n$$

where A_n is an explicit non-zero constant. By hypothesis, for every $\nu \geq 1$ the new part of $g(z)\Theta(N^\nu z)$ is a linear combination of CM-forms. Therefore $c(n) = 0$ for every 'inert' n, a set of positive integers with arithmetic density 1, and so $L(f_{(-1)^k dn}, k) = 0$ for almost every square-free $n \equiv r \pmod{t}$. Since it is widely believed that there is no such newform $f(z)$, we are led to the following conjecture.

Conjecture. *If $g(z) \in M_{k+\frac{1}{2}}(N) \setminus \Theta(N)$, then $g(z)$ is good.*

Acknowledgements

The authors thank B. Duke, V. Kolyvagin, D. Lieman, and K. Soundararajan for helpful comments. The authors also thank the referee for making numerous suggestions that improved the exposition and presentation of the paper.

References

[B] J. H. Bruinier, *Nonvanishing modulo ℓ of Fourier coefficients of half-integral weight modular forms,* (preprint).

[B-D] M. Bertolini and H. Darmon, *Euler systems and Jochnowitz congruences*, in preparation.

[D-H] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II*, Proc. Roy. Soc. Lond. A **322** (1971), 405-420.

[D] P. Deligne, *Formes modulaires et repŕesentations $\ell-$adiques*, Seminaire Bourbaki **355** (1969).

[D-S] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. École Normale Sup. 4^e sér. 7 (1974).

[F-H] S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automophic $L-$functions on $GL(2)$*, Ann. Math. **142** (1995), 385-423.

[G-S] R. Greenberg and G. Stevens, *On the conjecture of Mazur, Tate, and Teitelbaum*, p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecure (B.Mazur and G. Stevens, ed.).

[Gr] B. Gross, *A tameness criterion for galois representations associated to modular forms* (mod p), Duke Math. J. **61** (1990), 445-517.

[Ha] P. Hartung, *Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3*, J. Number Th. **6** (1974), 276-278.

[Ho1] K. Horie, *A note on basic Iwasawa λ-invariants of imaginary quadratic fields*, Invent. Math. **88** (1987), 31-38.

[Ho2] K. Horie, *Trace formulae and imaginary quadratic fields*, Math. Ann. **288** (1990), 605-612.

[Ho-On] K. Horie and Y. Onishi, *The existence of certain infinite families of imaginary quadratic fields*, J. Reine und ange. Math. **390** (1988), 97-133.

[Jo1] N. Jochnowitz, *Congruences between modular forms of half integral weights and implications for class numbers and elliptic curves*, preprint.

[Jo2] N. Jochnowitz, *A p-adic conjecture about derivatives of L-series attached to modular forms*, p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecure (B. Mazur and G. Stevens, ed.).

[Ka] N. Katz, *A result on modular forms in characteristic p*, Springer Lect. Notes in Math. **601** (1976), 53-61.

[K] W. Kohnen, *Fourier coefficients of modular forms of half-integral weight*, Math. Ann. **271** (1985), 237-268.

[K-Z] W. Kohnen and D. Zagier, *Values of $L-$series of modular forms at the center of the critical strip*, Invent. Math. **64** (1981), 173-198.

[Ko1] V. Kolyvagin, *Finiteness of $E(\mathbb{Q})$ and $Ш_{E/\mathbb{Q}}$ for a subclass of Weil curves (Russian)*, Izv. Akad. Nauk. USSR, ser. Matem. **52** (1988), 522-540.

[Ko2] V. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Progress in Math. 87, ed. P. Cartier et. al. (1990), 435-483.

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

[M-T-T] B. Mazur, J. Tate, and J. Teitlebaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **85** (1986), 1-48.

[Mi] T. Miyake, *Modular forms*, Springer Verlag, New York, 1989.

[O-S] K. Ono and L. Sze, $4-$*core partitions and class numbers*, Acta. Arith. **80** (1997), 249-272.

[R1] K. Ribet, *On ℓ-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245-275.

[R2] K. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Springer Lect. Notes. **601** (1976), 17-51.

[R3] K. Ribet, *On $\ell-$adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985), 185-194.

[Ru] K. Rubin, *Tate-Shafarevich groups and $L-$functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-560.

[Se] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[S-S] J.-P. Serre and H. Stark, *Modular forms of weight* $\frac{1}{2}$, Springer Lect. Notes 627 (1977), 27-67.

[Sh] G. Shimura, *On modular forms of half-integral weight*, Ann. Math. **97** (1973), 440-481.

[T] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. **72** (1983), 323-334.

[Wal] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures et Appl. **60** (1981), 375-484.

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540
E-mail address: ono@math.ias.edu

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802
E-mail address: ono@math.psu.edu

Department of Mathematics, Princeton University, Princeton, New Jersey 08540
E-mail address: cmcls@math.princeton.edu