Mathematical Research Letters **7**, 205–212 (2000)

ON "GOOD" HALF-INTEGRAL WEIGHT MODULAR FORMS

Jorge Jimenez Urroz and Ken Ono

1. Introduction and statement of results

If k is a positive integer, 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 (see [Ri]). For a non-negative integer k and any positive integer $N \equiv 0 \pmod 4$, 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 $\Gamma_1(N)$. Similarly, if $k \in \frac{1}{2}\mathbb{N}$, then let $M_k(N,\chi)$ (resp. $S_k(N,\chi)$) denote the space of modular (resp. cusp) forms with respect to $\Gamma_0(N)$ and Nebentypus character χ. Throughout this note we shall refer to classical facts which may be found in [Ko, Mi, S-S, Sh].

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

$$\theta_{a,i,r,t}(z) := \sum_{n \equiv r \pmod t} n^i q^{an^2} \tag{1}$$

(Note: $q := e^{2\pi i z}$ throughout). Each $\theta_{a,i,r,t}(z)$ is a holomorphic modular form of weight $i + \frac{1}{2}$. If $\Theta(N)$ is the set of modular forms generated by such functions of level dividing N, then the Serre-Stark Theorem [S-S] implies

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

If $g(z) \in M_{k+\frac{1}{2}}(N_1)$ and $h(z) \in \Theta(N_2)$, then let $g_h(n)$ denote the Fourier coefficient of q^n of the modular form

$$g(z) \cdot h(z) = \sum_{n=0}^{\infty} g_h(n) q^n.$$

Received February 2, 1999.

1991 *Mathematics Subject Classification.* Primary 11F37, 11F11.

Key words and phrases. The "Good" conjecture.

The first author is partially supported by PB90-0179 and the second author is supported by grants from the National Science Foundation and the National Security Agency. In addition, the second author thanks the Alfred P. Sloan Foundation and the David and Lucile Packard Foundation for their generous support.

Moreover, let $G_h(z)$ denote the modular form

$$G_h(z) := \sum_{\gcd(n, N_1 N_2)=1} g_h(n) q^n. \tag{3}$$

It follows from [Lemma 4, S-S] that $G_h(z)$ is a modular form on $\Gamma_1(N_1^2 N_2^2)$ of integral weight $k+1$ or $k+2$.

Definition. *A modular form $g(z) \in M_{k+\frac{1}{2}}(N_1)$ is* **good** *if there is an integer N_2 and a function $h(z) \in \Theta(N_2)$ for which*

(i) *$G_h(z)$ is a nonzero cusp form.*
(ii) *$G_h(z) \notin S_{k+1}^{cm}(N_1^2 N_2^2) \cup S_{k+2}^{cm}(N_1^2 N_2^2)$.*

There have been a number of recent papers on the non-vanishing of Fourier coefficients of half-integral weight modular forms modulo primes ℓ (see [B2, J, O-S1]), and in this direction the first author and C. Skinner were able to prove the following theorem for "good" forms.

Theorem. [p. 454, O-S1] *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 are infinitely many square-free integers m for which $|c(m)|_\ell = 1$.*

Here $| \bullet |_\ell$ denotes an extension of the usual ℓ-adic valuation to an algebraic closure of $\mathbb{Q}$.

In [O-S1], the first author and Skinner made the following natural conjecture:

The "Good" Conjecture. [p. 468, O-S1] *Every form in $M_{k+\frac{1}{2}}(N) \setminus \Theta(N)$ is good.*

In this note we prove:

Theorem 1. *The "Good" Conjecture is true.*

In a recent preprint, W. McGraw [M] obtains another proof of Theorem 1.

To prove the conjecture, we employ a well known result of M.-F. Vignéras, the Fundamental Lemma from [pp. 653–654, O-S2], and Brun's sieve.

2. Proof of Theorem 1

Here we begin by recalling a well-known result due to M.-F. Vignéras [V] (see [B1] for a new elementary proof).

Theorem 2. [Th. 3, V] *Suppose that $f(z) = \sum_{n=0}^{\infty} a(n) q^n$ is in $M_{k+\frac{1}{2}}(N)$. If there are finitely many square-free integers $d_1, d_2, \ldots, d_j$ such that $a(n) = 0$ for every n not of the form $d_i m^2$ with $1 \le i \le j$ and $m \in \mathbb{Z}^+$, then $f(z) \in \Theta(N)$.*

We begin by combining Theorem 2 and [Fund. Lemma, pp. 653–654, O-S2] to obtain a lower bound for the number of non-zero coefficients of any modular form $f(z) \in M_{k+\frac{1}{2}}(N, \chi) \backslash \Theta(N)$.

Theorem 3. *Suppose that* $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ *is a modular form in* $M_{k+\frac{1}{2}}(N,\chi)\backslash\Theta(N)$. *If* $f(z)$ *is an eigenform of the Hecke operators* $T(p^2)$ *for every prime* $p \nmid N$, *then*

$$\#\{n \leq X \ : \ a(n) \neq 0\} \gg_f \frac{X}{\log X}.$$

Proof. By [Lemma 8, S-S], we may assume that all of the Fourier coefficients $a(n)$ and the eigenvalues of the Hecke operators $T(p^2)$, for primes $p \nmid N$, are algebraic integers in a fixed number field K. Let v be a place in K over 2.

By Theorem 2 there are infinitely many square-free positive integers $d_1 < d_2 < \dots$ for which there are positive integers n with $a(d_i n^2) \neq 0$. Let s_0 be the smallest integer for which there is a square-free integer $d > 1$, with $d \nmid N$, and a positive integer n for which $\mathrm{ord}_v(a(dn^2)) = s_0$. Moreover, let d_0 be such a d and let n_0 be a positive integer for which $\mathrm{ord}_v(a(d_0 n_0^2)) = s_0$. Since $d_0 \nmid N$, there are square-free integers $D_0 > 1$ and D_1 for which $d_0 = D_0 D_1$ and $D_1 \mid N$ and $\gcd(D_0, N) = 1$. Similarly, let m_0 and m_1 denote the unique positive integers for which $n_0 = m_0 m_1$, $\gcd(m_0, N) = 1$, and every prime $p \mid m_1$ also divides N.

Now recall the action of the Hecke operators. If p is prime, then

$$f(z) \mid T(p^2) := \sum_{n=0}^{\infty} \left(a(p^2 n) + \chi(p) \left(\frac{(-1)^k n}{p} \right) p^{k-1} a(n) + \chi(p^2) p^{2k-1} a(n/p^2) \right) q^n. \tag{4}$$

Suppose that d is a positive integer and $p \nmid N$ is a prime for which $p^2 \nmid d$. Since $f(z)$ is an eigenform, it is easy to see that $a(d) \mid a(dp^{2i})$. As a consequence, it turns out that $a(D_0 D_1 m_1^2) \neq 0$ and $\mathrm{ord}_v(a(D_0 D_1 m_1^2)) = s_0$.

If $p \mid N$ is prime, then by [Lemma 1, S-S] it is known that

$$f(z) \mid U(p) = \sum_{n=0}^{\infty} a(pn) q^n, \tag{5}$$

is a cusp form in $M_{k+\frac{1}{2}}(N, \chi \cdot (\frac{4p}{\bullet}))$. Therefore, if j is any positive integer for which every prime $p \mid j$ also divides N, then

$$f(z) \mid U(j) = \sum_{n=0}^{\infty} a(jn) q^n \in M_{k+\frac{1}{2}}(N, \chi \cdot \left(\frac{4j}{\bullet}\right)).$$

Now define $f_0(z) \in M_{k+\frac{1}{2}}(N, \chi \cdot (\frac{4D_1}{\bullet}))$ by

$$f_0(z) = \sum_{n=0}^{\infty} b(n) q^n := f(z) \mid U(D_1 m_1^2) = \sum_{n=0}^{\infty} a(D_1 m_1^2 n) q^n.$$

By construction, we have that $b(D_0) = a(D_0 D_1 m_1^2) \neq 0$ and $\mathrm{ord}_v(b(D_0)) = s_0$.

Also by construction, if there is an integer $s < s_0$ and an integer n for which $\mathrm{ord}_v(b(n)) = s$, then $\gcd(n, N) \neq 1$. This follows from the minimality of s_0. If this is the case, then define $f_1(z) \in M_{k+\frac{1}{2}}(N^2, \chi \cdot \left(\frac{4D_1}{\bullet}\right))$ (see [Lemma 4, S-S]) by

$$f_1(z) = \sum_{n=1}^{\infty} c(n) q^n := \sum_{\gcd(n,N)=1} b(n) q^n. \tag{6}$$

If there is no such s, then let $f_1(z) = \sum_{n=0}^{\infty} c(n) q^n := f_0(z)$.

In either case, $f_1(z) = \sum_{n=0}^{\infty} c(n) q^n$ is in $M_{k+\frac{1}{2}}(N^2, \chi \cdot \left(\frac{4D_1}{\bullet}\right))$ and has the property that s_0 is indeed the smallest integer for which there is an n with $\mathrm{ord}_v(c(n)) = s_0$. Moreover, the square-free integer D_0 which is coprime to N^2 is such an n. By the Fundamental Lemma [pp. 653–654, O-S2], if $f_1(z)$ is a cusp form, then

$$\#\{n \leq X \ : \ \gcd(n, N^2) = 1 \text{ and } a(D_1 m_1^2 n) = c(n) \neq 0\} \gg_{f_1} \frac{X}{\log X}.$$

Although the Fundamental Lemma is stated for eigenforms which are cusp forms, it is easy to modify the argument to apply to forms $f_1(z)$ which are not cuspidal. Following the proof of the Fundamental Lemma, consider the integer weight form

$$F(z) := f_1(z) \cdot \left(1 + 2\sum_{n=1}^{\infty} q^{n^2}\right),$$

and decompose it into a cusp form $C(z)$ and a linear combination of Eisenstein series $E(z)$. By construction, the coefficient of q^{D_0} in $F(z)$ has minimal 2-adic valuation s_0, and is determined by a linear combination of generalized divisor functions related to the Eisenstein series in $E(z)$ (see [Mi]) and the collection of 2-adic Galois representations associated to the newforms constituting $C(z)$. By Dirichlet's Theorem on primes in arithmetic progressions, the Chebotarev Density theorem, and the multiplicativity of the coefficients of newforms, it follows that a 'positive proportion' of the square-free integers D with the same number of prime factors as D_0 have the property that the coefficient of q^D in $F(z)$ have minimal 2-adic valuation s_0. As in the proof of the Fundamental Lemma, this implies that

$$\#\{1 \leq n \leq X \ : \ c(n) \neq 0\} \gg \frac{X}{\log X} (\log \log X)^{r-1}$$

where D_0 has exactly r prime factors. □

As a corollary, we obtain the following result (see [O] for a similar result).

Corollary 4. *If $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ is a modular form in $M_{k+\frac{1}{2}}(N,\chi)\backslash\Theta(N)$, then*

$$\#\{n \leq X \ : \ a(n) \neq 0\} \gg_f \frac{X}{\log X}.$$

Proof. If $w = \sum_{n=0}^{\infty} a_w(n)q^n$ is a formal power series in q, then define

$$M_w(X) := \#\{0 \leq n \leq X \ : \ a_w(n) \neq 0\}.$$

Now suppose that $M_f(X) = o(X/\log X)$. In view of (4), it is easy to see that if $p \nmid N$ is prime, then

$$M_{f|T(p^2)}(X) \leq M_f(p^2X) + 2M_f(X). \tag{7}$$

By (7), if $p \nmid N$ is prime, then $M_{f|T(p^2)}(X) = o(X/\log X)$.

If w_1 and w_2 are formal power series, then it is obvious that

$$M_{w_1+w_2}(X) \leq M_{w_1}(X) + M_{w_2}(X).$$

Therefore, if $\mathbb{T}$ is the Hecke algebra generated by the Hecke operators $T(p^2)$ and $\mathbb{X} = \mathbb{T}f$, then for every $u(z) \in \mathbb{X}$ we have that $M_u(X) = o(X/\log X)$.

Since $\mathbb{T}$ is commutative, every simple submodule of $\mathbb{X}$ is generated by an eigenform. If $u(z)$ is such an eigenform, then Theorem 3 contradicts the conclusion that $M_u(X) = o(X/\log X)$. Therefore, it must be that $M_f(X) \gg_f X/\log X$. □

Now we employ Brun's sieve to obtain an important technical result regarding the prime divisors of a shifted set of integers. As usual, $p^a||n$ means that a is the exact power of p dividing n.

Lemma 5. *Let ℓ be a fixed prime, and let $1 \leq r < t$ be integers for which $\gcd(r,t) = 1$. If A is a set of non-negative integers for which*

$$\#\{n \leq X \ : \ n \in A\} \gg \frac{X}{\log X},$$

then there is a positive integer E and at least one integer $n \in A$ with $n < \ell^E$ such that $p||(n + \ell^E)$ for some prime $p \equiv r \pmod{t}$.

Proof. If $\phi(\bullet)$ denotes the usual Euler phi-function, then define the polynomial $F(n)$ by

$$F(n) = (n+\ell)(n+\ell^2)\cdots(n+\ell^{\phi(t)+1}). \tag{8}$$

Let $\mathcal{A}_X$ denote the set of integers

$$\mathcal{A}_X := \{F(n) \ : \ n \leq X\}, \tag{9}$$

and let P_X denote the set

$$P_X := \{p \equiv r \pmod{t} \text{ prime } : \log^2 X < p < X\}. \tag{10}$$

It is easy to see that if X is sufficiently large, then every prime $p \in P_X$ has the property that the multiplicative order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^\times$ is larger than $\phi(t)+1$. Therefore, if n is an integer and $p \in P_X$ is any prime for which $F(n) \equiv 0 \pmod{p}$, then there is exactly one integer $1 \leq i \leq \phi(t)+1$ for which

$$n + \ell^i \equiv 0 \pmod{p}. \tag{11}$$

Moreover, it is obvious that if $p \in P_X$, then there are $\phi(t)+1$ distinct residue classes $n \pmod{p}$ for which $F(n) \equiv 0 \pmod{p}$.

Now we consider the function $\mathcal{S}(\mathcal{A}_X, P_X, X)$ which is defined by

$$\mathcal{S}(\mathcal{A}_X, P_X, X) := \#\{1 \leq n \leq X \ : \ \gcd(F(n), p) = 1 \text{ for every } p \in P_X\}. \tag{12}$$

By a straightforward application of Brun's sieve method [Theorem 2.2, H-R] we find that

$$\mathcal{S}(\mathcal{A}_X, P_X; X) \ll X \prod_{p \in P_X} \left(1 - \frac{\phi(t)+1}{p}\right). \tag{13}$$

Using the well known fact [p. 605, R] that

$$\prod_{\substack{p \leq X \\ p \equiv r \pmod{t}}} \left(1 - \frac{1}{p}\right) \ll \frac{1}{(\log X)^{1/\phi(t)}},$$

it is easy to deduce

$$\mathcal{S}(\mathcal{A}_X, P_X; X) \ll \frac{X}{(\log X)^{1+1/2\phi(t)}}. \tag{14}$$

Therefore, if X is sufficiently large, then there are integers $n \in A$ with $n \leq X$ for which there is at least one prime $p \in P_X$ with $F(n) \equiv 0 \pmod{p}$. In particular, in view of (14) we find that

$$\#\{n \leq X \ : \ n \in A \text{ and } F(n) \equiv 0 \pmod{p} \text{ for some prime } p \in P_X\} \gg \frac{X}{\log X}. \tag{15}$$

However, the number of positive integers $n \leq X$ which are divisible by p^2 for some prime $p \in P_X$ is

$$\ll X \sum_{\log^2 X < p < X} \frac{1}{p^2} < \frac{X}{\log^2 X} \sum_{p < X} \frac{1}{p} \ll \frac{X}{(\log X)^{1+1/2}},$$

since $\sum_{p\le X} 1/p \ll \log\log X$. Therefore, by (11) and (15) we find that the number of integers $n \le X$ and $n \in A$ for which there is at least one prime $p \in P_X$ and an integer $1 \le e \le \phi(t)+1$ such that $p||n+\ell^e$ is $\gg X/\log X$.

To conclude the proof, we note that if $p||(n+\ell^e)$, then $p||(n+\ell^{E(j)})$ where $E(j) := e + p(p-1)(p(p-1)+1)^j$ and $j \ge 0$. To see this, note that $n+\ell^{E(j)} = n+\ell^e+(\ell^{E(j)}-\ell^e)$, $\ell^{p-1} \equiv 1 \pmod p$ and $\ell^{p(p-1)} \equiv 1 \pmod{p^2}$. Therefore if j is sufficiently large, then $n < \ell^E$. □

Proof of Theorem 1. Here we recall the essential facts regarding modular forms with complex multiplication (see [Ri]). If $\phi(z) = \sum_{n=1}^{\infty} a_\phi(n)q^n \in S_k(N,\chi)$ is a newform with complex multiplication by the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, where d is the discriminant of K, then $d \mid N$, and if p is a prime for which $\left(\frac{d}{p}\right) = -1$, then $a_\phi(p) = 0$.

Now suppose that $F(z) = \sum_{n=1}^{\infty} a_F(n)q^n$ is an integer weight cusp form in $S_w(N,\psi)$. There are finitely many fundamental discriminants of imaginary quadratic fields, say $d_1, d_2, \dots, d_j$ for which $d_i \mid N$. Therefore, it is easy to construct an arithmetic progression $r \pmod t$ with $\gcd(r,t)=1$ such that every prime $p \equiv r \pmod t$ has the property that $\left(\frac{d_i}{p}\right) = -1$ for each $1 \le i \le j$. Therefore, by the multiplicativity of the Fourier coefficients of newforms, $F(z)$ cannot be a linear combination of forms with complex multiplication if there is a positive integer n and a prime $p \equiv r \pmod t$ for which $p||n$ and $a_F(n) \neq 0$.

Now we prove Theorem 1 by considering two different cases.

Case I. Suppose that $g(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_{k+\frac{1}{2}}(N,\chi)\backslash\Theta(N)$. By Corollary 4, we know that

$$\#\{n \le X \;:\; a(n) \neq 0\} \gg_g \frac{X}{\log X}.$$

Now let $\ell \mid 576N$ be prime, and let $r \mod t$ with $\gcd(r,t)=1$ be an arithmetic progression such that $\left(\frac{d_i}{p}\right) = -1$ for every prime $p \equiv r \pmod t$ and every fundamental discriminant of an imaginary quadratic field $d_i \mid 576N$. By Lemma 5, there exists an integer $n < \ell^E$ for which $a(n) \neq 0$, a prime $p \equiv r \pmod t$, and a positive integer E such that $p||n+\ell^E$.

Now consider the cusp form $g(z)\cdot\eta(24\ell^E z)$, where $\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ denotes Dedekind's eta-function. It is well known that

$$\eta(24z) = q + \cdots \in S_{1/2}(576, \chi_{12}),$$

where χ_{12} is the non-trivial quadratic character with conductor 12. Obviously, $\eta(24\ell^E z) \in \Theta(576\ell^E)$, and so $g(z)\eta(24\ell^E z) \in S_{k+1}(576N\ell^E)$. The coefficient of $q^{n+\ell^E}$ of this form is $a(n) \neq 0$. Since every fundamental discriminant of an imaginary quadratic field $d \mid 576N\ell^E$ already divides $576N$, we find that $g(z)\eta(24\ell^E z)$ cannot be a linear combination of forms with complex multiplication (i.e., $g(z)$ is good).

Case II. Suppose that $g(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_{k+\frac{1}{2}}(N)\backslash\Theta(N)$. It is well known that if $w \in \frac{1}{2}\mathbb{Z}$, then

$$M_w(N) = \oplus_\chi M_w(N, \chi), \tag{16}$$

where the direct sum is over Dirichlet characters $\chi \mod N$. Therefore, we may decompose $g(z)$ as

$$g(z) = \sum_{\chi} \alpha_\chi g_\chi(z).$$

If χ is a character for which $\alpha_\chi g_\chi(z) \neq 0$, then by Case I there is a weight 1/2 cusp form $\theta(z) \in S_{1/2}(N_2, \Psi)$ for which $g_\chi(z)\theta(z)$ is a weight $k+1$ cusp form which is not a linear combination of forms with complex multplication.

If χ_1 and χ_2 are distinct characters mod N, then $g_{\chi_1}(z)\theta(z)$ and $g_{\chi_2}(z)\theta(z)$ will lie in different spaces of weight $k+1$ cusp forms with Nebentypus. Therefore, it follows immediately that $g(z)\theta(z)$ is good. □

References

[B1] J. Bruinier, *On a theorem of Vignéras*, Abh. Math. Sem. Univ. Hamburg **68** (1998), 163–168.

[B2] ———, *Nonvanishing modulo ℓ of Fourier coefficients of half-integral weight modular forms*, Duke Math. J. **98** (1999), 595–611.

[H-R] H. Halberstam and H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs, No. 4, Academic Press, London, 1974.

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

[Ko] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, 97, Springer-Verlag, New York, 1984.

[M] W.J. McGraw, *On a theorem of Ono and Skinner*, preprint.

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

[O] K. Ono, *On Gordon's ϵ-conjecture*, C. R. Math. Acad. Sci. Soc. R. Can. **20** (1998), 103–107.

[O-S1] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo ℓ*, Ann, of Math. (2) **147** (1998), 453–470.

[O-S2] ———, *Nonvanishing of quadratic twists of modular L-functions*, Invent. Math. **134** (1998), 651–660.

[R] D. Redmond, *Number Theory*, Marcel Dekker, New York, 1996.

[Ri] K. Ribet, *Galois representations attached to eigenforms with Nebentypus*, Lect. Notes. in Math., vol. 601, Springer, Berlin,, 1976, pp. 17–51.

[S-S] J.-P. Serre and H. Stark, *Modular forms of weight $\frac{1}{2}$*, Lect. Notes in Math., vol. 627, Springer, Berlin, 1977, pp. 27–67.

[Sh] G. Shimura, *On modular forms of half-integral weight*, Ann. Math. (2) **97** (1973), 440–481.

[V] M.-F. Vignéras, *Facteurs gamma et équations fonctionnelles*, Lect. Notes in Math., vol. 627, Springer, Berlin, 1977, pp. 79–103.

Dept. Matemáticas, Facultad de Ciencias, Universidad Autónoma de Madrid, 28049, Madrid, ESPAÑA.

E-mail address: jorge.jimenez@uam.es

Dept. of Math., Penn State University, University Park, Pennsylvania 16802.

E-mail address: ono@math.psu.edu