Nonvanishing of Fourier coefficients
of newforms in progressions

by

Emre Alkan and Alexandru Zaharescu (Urbana, IL)

1. Introduction. Let $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ be a newform of integer weight $k \geq 2$ without complex multiplication. The arithmetic properties of the Fourier coefficients $a_f(n)$ have been investigated for a long time. The reader is referred to a recent monograph of Ono [8] for an extensive survey on the latest developments on this subject from various perspectives. It is well known that these Fourier coefficients form a multiplicative arithmetic function. This fact is essential for detecting nonzero Fourier coefficients. A famous conjecture of Lehmer predicts that $\tau(n) \neq 0$ for any $n \geq 1$ where

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

is the unique normalized cusp form of weight 12 on $\mathrm{SL}_2(\mathbb{Z})$. Here the Fourier coefficient $\tau(n)$ is Ramanujan's tau function. Ramanujan first realized and studied many of the fascinating arithmetical properties of this multiplicative function (see the survey of Berndt and Ono [4]). In relation to Lehmer's Conjecture, Serre [9] initiated the general study of estimating the size of possible gaps in the Fourier expansion of modular forms via the gap function

(1) $$i_f(n) = \max\{i : a_f(n+j) = 0 \text{ for all } 0 \leq j \leq i\}.$$

In this direction Balog and Ono [3] recently obtained striking nonvanishing results about the Fourier coefficients of cusp forms without complex multiplication regarding their short interval distribution (see also [1]). In the case of the gap function the first author proved that $i_f(n) \ll_{f,\phi} \phi(n)$ for almost all n where ϕ is essentially any function monotonically tending to infinity. This shows that the gap function is very small most of the time. Concerning bounded values of $i_f(n)$, it was shown in [2] that for every $\varepsilon > 0$ there is

---

$M = M(f, \varepsilon)$ such that

$$\#\{n \leq x : i_f(n) \leq M\} \geq (1 - \varepsilon)x.$$

Hence even the bounded gaps occur a lot. The average value of $i_f(n)$ was further studied in [2]. In particular, it was shown that for almost all elliptic curves over $\mathbb{Q}$ without complex multiplication and for any $\varepsilon > 0$,

$$\frac{1}{x} \sum_{n \leq x} i_{f_E}(n) \ll_E e^{\frac{8 \log x}{\log \log x}} \ll_\varepsilon x^\varepsilon$$

where $f_E(z) = \sum_{n=1}^{\infty} a_E(n)q^n$ is the weight 2 newform associated to $E/\mathbb{Q}$.

In this paper we study the nonvanishing of Fourier coefficients of newforms without complex multiplication in arithmetic progressions. In our approach we will not fix an arithmetic progression, but aim at a result that holds uniformly for all arithmetic progressions with moduli as large as x^η for some fixed $\eta > 0$. Our main result is as follows:

THEOREM 1. *For any $\sigma > 9/20$ there exists $\eta > 0$ (effectively computable) depending only on σ such that for any newform $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ without complex multiplication, any large x, any $y \geq x^\sigma$, and any relatively prime integers b, a satisfying $1 \leq b < a \leq x^\eta$, we have*

$$\#\{x - y < n \leq x : a_f(n) \neq 0 \text{ and } n \equiv b \,(\mathrm{mod}\,a)\} \gg_{\sigma,f} \frac{y}{a}.$$

Note that this result applies in particular to Ramanujan's tau function mentioned above. For a newform associated to an elliptic curve $E/\mathbb{Q}$ without complex multiplication we can improve the exponent $9/20$ from Theorem 1.

THEOREM 2. *For any $\sigma > 9/22$ there exists $\theta > 0$ (effectively computable) depending only on σ such that for any newform $f_E(z) = \sum_{n=1}^{\infty} a_E(n)q^n$ associated with an elliptic curve $E/\mathbb{Q}$ without complex multiplication, any large x, any $y \geq x^\sigma$, and any relatively prime integers b, a satisfying $1 \leq b < a \leq x^\theta$, we have*

$$\#\{x - y < n \leq x : a_E(n) \neq 0 \text{ and } n \equiv b \,(\mathrm{mod}\,a)\} \gg_{\sigma,E} \frac{y}{a}.$$

If we consider the problem for almost all n, then a similar conclusion as in Theorem 1 holds for very short intervals.

THEOREM 3. *Let $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ be a newform without complex multiplication and let $\phi(n)$ and $\psi(n)$ be functions monotonically tending to infinity such that $\phi(2n) \ll \phi(n)$ and $\psi(n) = o(\phi(n))$ for large n. Then there exists a constant $c_{f,\phi,\psi} > 0$ such that*

$$\min_{\substack{1 \leq b < a \leq \psi(n) \\ \gcd(a,b)=1}} \frac{a}{\phi(n)} \#\{n - \phi(n) < m \leq n : a_f(m) \neq 0 \text{ and } m \equiv b \,(\mathrm{mod}\,a)\} \geq c_{f,\phi,\psi}$$

for almost all positive integers n.

2. Proof of Theorem 1. It would be enough to prove the statement for $9/20 < \sigma \leq 1/2$, then clearly the statement of the theorem holds for any $\sigma > 9/20$. Hence we may assume in what follows that $9/20 < \sigma \leq 1/2$. For a newform $f(z) = \sum_{n=1}^{\infty} a_f(n) q^n \in S_k(\Gamma_0(N), \chi)$, let us define

$$(2) \qquad B = \{p \text{ prime} : a_f(p) = 0\}$$

and

$$(3) \qquad B(x) = \#\{p \leq x \text{ prime} : p \in B\}.$$

Recall that $f(z)$ is a newform without complex multiplication. We will need the following theorem of Serre [9]:

THEOREM (Serre). *In the above notation,*

$$B(x) \ll_{f,\varepsilon} \frac{x}{(\log x)^{3/2 - \varepsilon}}$$

for any $\varepsilon > 0$.

The theorem follows from a study of the p-adic Galois representations associated to modular forms by Deligne. The form of the estimate follows by a careful application of the Chebotarev Density Theorem.

It follows that $\sum_{p \in B} 1/p$ is finite. Using the multiplicativity of $a_f(n)$, if n is square-free, then we have that

$$a_f(n) = \prod_{p \mid n} a_f(p)$$

so that $a_f(n) \neq 0$ when n is square-free and B-free. Let A be the set of primes in B together with squares of primes not in B. Let b_s denote the elements of A in increasing order. Our goal is to find $\eta > 0$ such that

$$\sum_{\substack{x - y < n \leq x \\ n \equiv b \,(\mathrm{mod}\, a) \\ n \text{ is } A\text{-free}}} 1 \gg_{\sigma,f} \frac{y}{a}$$

where $y = x^\sigma$ for $9/20 < \sigma \leq 1/2$ and b, a are relatively prime integers satisfying $1 \leq b < a \leq x^\eta$. Let us define

$$(4) \qquad P_1 = P_1(x, \delta_1, \mu) = \{x^{\delta_1} \leq p \leq x^{\delta_1 + \mu} : p \text{ prime}\},$$
$$(5) \qquad P_2 = P_2(x, \delta_2, \mu) = \{x^{\delta_2} \leq u \leq x^{\delta_2 + \mu} : u \text{ prime}\}$$

where $\delta_2 + \mu < \delta_1 < \delta_1 + \mu < \sigma$ and $\mu > 0$ is as small as we please. For $n \leq x$, we use the sieving weight

$$(6) \qquad w(n) = \sum_{p \in P_1} \sum_{u \in P_2} \sum_{n \equiv 0 \,(\mathrm{mod}\, pu)} 1.$$

It is easy to see that $w(n) \leq C(\delta_1, \delta_2)$ independently of x. Hence it suffices to show that

$$\sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ n \text{ is } A\text{-free}}} w(n) \gg_{\sigma,f} \frac{y}{a}.$$

Consider

$$(7) \qquad \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ n \text{ is } A\text{-free}}} w(n)$$

$$\geq \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ n\not\equiv 0 \,(\mathrm{mod}\,b_s) \text{ for all } s\leq m}} w(n) - \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ b_m<b_s\leq y/a \\ n\equiv 0 \,(\mathrm{mod}\,b_s) \text{ for some } s>m}} w(n) - \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ y/a<b_s\leq x \\ n\equiv 0 \,(\mathrm{mod}\,b_s) \text{ for some } s>m}} w(n).$$

The parameter m in (7) will be suitably chosen later. Let us denote the right side of (7) by $M_0 - E_1 - E_2$. Using the definition of $w(n)$ and the Inclusion-Exclusion Principle, the main term becomes

$$(8) \quad M_0 = \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ n\not\equiv 0 \,(\mathrm{mod}\,b_s) \text{ for all } s\leq m \\ n\equiv 0 \,(\mathrm{mod}\,pu),\, p\in P_1,\, u\in P_2}} 1 = \sum_{\omega}(-1)^{|\omega|} \sum_{p\in P_1} \sum_{u\in P_2} \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ n\equiv 0 \,(\mathrm{mod}\,d_\omega) \\ n\equiv 0 \,(\mathrm{mod}\,pu)}} 1$$

where ω runs through all subsets of $\{s : 1 \leq s \leq m\}$ and $d_\omega = \prod_{s\in\omega} b_s$ (empty products are taken to be 1). Note that once m is fixed and x is large enough then we have $\gcd(d_\omega, pu) = 1$. Hence

$$(9) \qquad \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ n\equiv 0 \,(\mathrm{mod}\,d_\omega) \\ n\equiv 0 \,(\mathrm{mod}\,pu)}} 1 = \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ n\equiv 0 \,(\mathrm{mod}\,pud_\omega)}} 1.$$

Moreover, if $\eta > 0$ is small enough, then $\gcd(a, pu) = 1$ since $a \leq x^\eta$. Also if $\gcd(a, d_\omega) > 1$ then using $n \equiv 0 \,(\mathrm{mod}\,pud_\omega)$ and $n \equiv b \,(\mathrm{mod}\,a)$ we get $\gcd(a, b) > 1$ contrary to our assumption. It follows that $\gcd(a, pud_\omega) = 1$ and by the Chinese Remainder Theorem the conditions $n \equiv b \,(\mathrm{mod}\,a)$ and $n \equiv 0 \,(\mathrm{mod}\,pud_\omega)$ are equivalent to $n \equiv c \,(\mathrm{mod}\,apud_\omega)$ for a suitable c. Using this on the right side of (9) we get

$$(10) \qquad \sum_{\substack{x-y<n\leq x \\ n\equiv b \,(\mathrm{mod}\,a) \\ n\equiv 0 \,(\mathrm{mod}\,pud_\omega)}} 1 = \sum_{\substack{x-y<n\leq x \\ n\equiv c \,(\mathrm{mod}\,apud_\omega)}} 1 = \frac{y}{apud_\omega} + r_{pud_\omega,a,b}(x,y)$$

where $r_{pud_\omega,a,b}(x,y)$ is a remainder term and $|r_{pud_\omega,a,b}(x,y)| \leq 1$. Combining

(8), (9) and (10) we obtain

$$(11) \qquad M_0 = \frac{y}{a} \prod_{s \leq m} \left(1 - \frac{1}{b_s}\right) \sum_{p \in P_1} \frac{1}{p} \sum_{u \in P_2} \frac{1}{u} + R_{a,b}(x, y)$$

where

$$(12) \qquad R_{a,b}(x, y) = \sum_{\omega} (-1)^{|\omega|} \sum_{p \in P_1} \sum_{u \in P_2} r_{pud_\omega, a, b}(x, y).$$

Note that since $\sum_{p \in B} 1/p$ is finite it follows that $\sum_{s=1}^{\infty} 1/b_s$ is finite and we may put

$$(13) \qquad C_A = \prod_{s=1}^{\infty} \left(1 - \frac{1}{b_s}\right) > 0.$$

Using the asymptotic formula for the sum of reciprocals of primes, we deduce for large x that

$$(14) \qquad \sum_{p \in P_1} \frac{1}{p} = \log\left(1 + \frac{\mu}{\delta_1}\right) + O\left(\frac{1}{\log x}\right) \geq C_1$$

and similarly

$$(15) \qquad \sum_{u \in P_2} \frac{1}{q} \geq C_2$$

where $C_1 > 0$ and $C_2 > 0$ are absolute constants. Hence combining (11), (13), (14) and (15) we conclude for large x that

$$(16) \qquad M_0 \geq C_A C_1 C_2 \frac{y}{a} + R_{a,b}(x, y).$$

Next we estimate the sum of remainder terms $R_{a,b}(x, y)$. Since the sum over ω is finite, it is enough to estimate each individual bilinear sum of remainder terms of the form

$$(17) \qquad \sum_{p \in P_1} \sum_{u \in P_2} r_{pud_\omega, a, b}(x, y) = \sum_{p \in P_1} \sum_{u \in P_2} r_{pu, a, b}\left(\frac{x}{d_\omega}, \frac{y}{d_\omega}\right).$$

The modern version of the linear sieve due to Iwaniec [7] requires nontrivial estimates for such bilinear forms of remainder terms. Here we will adapt the approach of Fouvry and Iwaniec [6] to obtain nontrivial upper bounds for the double sum in (17). Note that the sums we are working with are supported only on an arithmetic progression and therefore the remainder terms are coming only from integers $n \equiv b \pmod{a}$. To this end we let χ_{P_1} and χ_{P_2} be the characteristic functions of P_1 and P_2 respectively. Our goal is to transform the problem of estimating (17) to estimating certain exponential sums. Let $g(z)$ be a C^∞ function supported in a short interval of the form $[x - y - yx^{-\lambda}, x + yx^{-\lambda}]$ for some $\lambda > 0$ such that $g(z) = 1$ for

all $x - y \le z \le x$, $g(z)$ is increasing in $[x - y - yx^{-\lambda}, x - y]$ and decreasing in $[x, x + yx^{-\lambda}]$. Furthermore

$$(18) \qquad\qquad |g^{(j)}(z)| \ll (yx^{-\lambda})^{-j}$$

for any $j \ge 0$ where the implied constant in (18) depends only on j (i.e. $g(z)$ is a very smooth compactly supported approximation to the characteristic function of the interval $[x - y, x]$). We will approximate a sum involving $\chi_{P_1} \cdot \chi_{P_2}$ with the help of $g(z)$. If either $x \le n \le x + yx^{-\lambda}$ or $x - y - yx^{-\lambda} \le n \le x - y$, then there are only finitely many pairs (p, u) with $p \in P_1$ and $u \in P_2$ (depending on δ_1 and δ_2 and independent of x) such that $n = lpu$ for some $l \in \mathbb{Z}$. It follows that

$$(19) \qquad S = \sum_{l \in \mathbb{Z}} \sum_{p \le M = x^{\delta_1 + \mu}} \sum_{u \le N = x^{\delta_2 + \mu}} \sum_{\substack{x - y < lpu \le x \\ lpu \equiv b \,(\mathrm{mod}\, a)}} \chi_{P_1}(p)\chi_{P_2}(u)$$

$$= \sum_{l \in \mathbb{Z}} \sum_{\substack{p \le M,\, u \le N \\ lpu \equiv b \,(\mathrm{mod}\, a)}} \chi_{P_1}(p)\chi_{P_2}(u)g(lpu) + O(yx^{-\lambda})$$

since $0 \le g(lpu) \le 1$ and the number of (p, u) such that $x \le n = lpu \le x + yx^{-\lambda}$ or $x - y - yx^{-\lambda} \le n = lpu \le x - y$ is $O(yx^{-\lambda})$. Let $1 \le p^* < a$ and $1 \le u^* < a$ be the inverses of p and u modulo a. Then $l \equiv bp^*u^* \,(\mathrm{mod}\, a)$ and we may put $l = a\nu + bp^*u^*$ for $\nu \in \mathbb{Z}$. We can rewrite (19) as

$$(20) \qquad S = \sum_{p \le M} \sum_{u \le N} \sum_{\nu \in \mathbb{Z}} \chi_{P_1}(p)\chi_{P_2}(u)g(apu\nu + bpp^*uu^*) + O(yx^{-\lambda}).$$

Let

$$(21) \qquad\qquad g^*(z) = \int\limits_{-\infty}^{\infty} g(t)e^{-2\pi izt}\, dt$$

be the Fourier transform of g and define $G(t) = g(aput + bpp^*uu^*)$ for $t \in \mathbb{R}$. Then we can compute the Fourier transform of G as

$$(22) \qquad G^*(z) = \int\limits_{-\infty}^{\infty} G(t)e^{-2\pi izt}\, dt = \int\limits_{-\infty}^{\infty} g(aput + bpp^*uu^*)e^{-2\pi izt}\, dt$$

and making the change of variable $h = aput + bpp^*uu^*$ we get from (22) that

$$(23) \qquad G^*(z) = \frac{e^{2\pi i \frac{b}{a}p^*u^*z}}{apu} \int\limits_{-\infty}^{\infty} g(h)e^{-2\pi i \frac{z}{apu}h}\, dh$$

$$= \frac{e\left(\frac{b}{a}p^*u^*z\right)}{apu} g^*\left(\frac{z}{apu}\right)$$

where we used the notation $e(z) = e^{2\pi i z}$. By the Poisson Summation Formula applied to G we have

$$(24) \qquad \sum_{\nu \in \mathbb{Z}} G(\nu) = \sum_{\nu \in \mathbb{Z}} G^*(\nu).$$

Hence, combining (20), (23) and (24), we obtain

$$(25) \quad S = \sum_{p \leq M} \sum_{u \leq N} \chi_{P_1}(p)\chi_{P_2}(u) \sum_{\nu \in \mathbb{Z}} G^*(\nu) + O(yx^{-\lambda})$$

$$= \frac{1}{a} \sum_{p \leq M} \sum_{u \leq N} \frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu} \sum_{\nu \in \mathbb{Z}} e\left(\frac{b}{a}p^*u^*\nu\right)g^*\left(\frac{\nu}{apu}\right) + O(yx^{-\lambda}).$$

Note that

$$g^*(0) = \int\limits_{-\infty}^{\infty} g(t)\, dt = y + O(yx^{-\lambda}).$$

The main contribution to S comes from the term $\nu = 0$ in (25) which is

$$(26) \qquad \frac{g^*(0)}{a} \sum_{p \leq M} \sum_{u \leq N} \frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu}$$

$$= \frac{y}{a} \sum_{p \leq M} \sum_{u \leq N} \frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu} + O\left(\frac{y}{a}x^{-\lambda}\sum_{p \leq M}\sum_{u \leq N}\frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu}\right).$$

Using (14) and (15), it is easy to see that

$$\sum_{p \leq M}\sum_{u \leq N}\frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu} = \sum_{p \in P_1}\frac{1}{p}\sum_{u \in P_2}\frac{1}{u} = O(1).$$

Hence from (26) we get

$$(27) \qquad \frac{g^*(0)}{a}\sum_{p \leq M}\sum_{u \leq N}\frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu}$$

$$= \frac{y}{a}\sum_{p \leq M}\sum_{u \leq N}\frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu} + O\left(\frac{y}{a}x^{-\lambda}\right).$$

The sum of all terms with $|\nu| \geq 1$ in (25) will form an upper bound for the sum of all remainder terms so that we have

$$(28) \quad \left|\sum_{p \in P_1}\sum_{u \in P_2} r_{pu,a,b}(x,y)\right|$$

$$\leq \left|\frac{1}{a}\sum_{p \leq M}\sum_{u \leq N}\frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu}\sum_{|\nu| \geq 1}e\left(\frac{b}{a}p^*u^*\nu\right)g^*\left(\frac{\nu}{apu}\right)\right| + O(yx^{-\lambda}).$$

Next we estimate the tail of the sum over ν appearing in (28). Applying integration by parts repeatedly and using the fact that g has compact support

we find that

$$(29) \qquad g^*(z) = \int\limits_{-\infty}^{\infty} g(t)e^{-2\pi izt}\,dt = \int\limits_{-\infty}^{\infty} \frac{e^{-2\pi izt}}{(2\pi iz)^j}\,g^{(j)}(t)\,dt$$

for any $j \geq 1$. Using (18) and the fact that $g^{(j)}(z) = 0$ for $x - y \leq z \leq x$, we obtain the estimate

$$(30) \qquad |g^*(z)| \ll_j \frac{1}{(yx^{-\lambda})^{j-1}|z|^j}.$$

Replacing z by ν/pu in (30) we have

$$(31) \qquad \left|g^*\left(\frac{\nu}{pu}\right)\right| \ll_j \frac{(pu)^j}{(yx^{-\lambda})^{j-1}|\nu|^j}.$$

Let us assume that

$$(32) \qquad |\nu| > H' = \frac{MN}{y}\,x^{2\lambda}.$$

Note that the inequality

$$\frac{(pu)^j}{(yx^{-\lambda})^{j-1}|\nu|^j} \ll_j \frac{1}{|\nu|^2}$$

holds when

$$(33) \qquad \frac{(pu)^j}{(yx^{-\lambda})^{j-1}} \ll_j |\nu|^{j-2}.$$

Using (32) and the fact that $p \leq M$ and $u \leq N$, we see that (33) holds when

$$(MN)^2 \ll_j yx^{(j-3)\lambda}$$

which is clearly true when j is large enough. Combining (31) and (33) we conclude that

$$(34) \qquad \left|g^*\left(\frac{\nu}{apu}\right)\right| \ll \frac{1}{\nu^2}$$

when

$$(35) \qquad |\nu| > H = \frac{aMN}{y}\,x^{2\lambda}.$$

It follows that

$$(36) \qquad \left|\frac{1}{a}\sum_{p \leq M}\sum_{u \leq N}\frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu}\sum_{|\nu| > H} e\left(\frac{b}{a}p^*u^*\nu\right)g^*\left(\frac{\nu}{apu}\right)\right|$$

$$\ll \frac{1}{aH} = O(yx^{-2\lambda}).$$

Combining (28) and (36) we obtain

$$(37) \qquad \left|\sum_{p \in P_1}\sum_{u \in P_2} r_{pu,a,b}(x,y)\right|$$

$$\leq \left|\frac{1}{a}\sum_{p \leq M}\sum_{u \leq N}\frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu}\sum_{|\nu| \leq H} e\left(\frac{b}{a}p^*u^*\nu\right)g^*\left(\frac{\nu}{apu}\right)\right| + O(yx^{-\lambda}).$$

Using the definition of g^*, we may rewrite the right side of (37) to obtain

$$(38) \quad \left| \sum_{p \in P_1} \sum_{u \in P_2} r_{pu,a,b}(x,y) \right|$$

$$\leq \frac{1}{a} \int_{x-y-yx^{-\lambda}}^{x+yx^{-\lambda}} \left| \sum_{|\nu| \leq H} \sum_{p \leq M} \sum_{u \leq N} \frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu} e\left(\frac{b}{a} p^* u^* \nu \right) e\left(-\frac{\nu t}{apu} \right) g(t) \right| dt$$
$$+ O(yx^{-\lambda}).$$

Note that $g(t) = 1$ for $x - y \leq t \leq x$ and $|g(t)| \leq 1$ when $x \leq t \leq x + yx^{-\lambda}$ or $x - y - yx^{-\lambda} \leq t \leq x - y$, moreover the integrand in (38) is $O(1)$ in these intervals. Hence we finally get from (38) that

$$(39) \quad \left| \sum_{p \in P_1} \sum_{u \in P_2} r_{pu,a,b}(x,y) \right|$$

$$\leq \frac{1}{a} \int_{x-y}^{x} \left| \sum_{|\nu| \leq H} \sum_{p \leq M} \sum_{u \leq N} \frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu} e\left(\frac{b}{a} p^* u^* \nu \right) e\left(-\frac{\nu t}{apu} \right) \right| dt$$
$$+ O(yx^{-\lambda}).$$

It now suffices to obtain nontrivial upper bounds for an exponential sum of the type

$$(40) \quad \sum_{1 \leq \nu \leq H} \sum_{1 \leq p \leq M} \sum_{1 \leq u \leq N} \frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu} e\left(\frac{b}{a} p^* u^* \nu \right) e\left(\frac{\nu t}{apu} \right).$$

Decomposing $[1, H]$, $[1, M]$ and $[1, N]$ into dyadic intervals will bring in only a factor which is $O((\log x)^3)$ to our estimates, so that we consider

$$\sum_{H/2 \leq \nu \leq H} \sum_{M/2 \leq p \leq M} \sum_{N/2 \leq u \leq N} \frac{\chi_{P_1}(p)\chi_{P_2}(u)}{pu} e\left(\frac{b}{a} p^* u^* \nu \right) e\left(\frac{\nu t}{apu} \right).$$

Clearly this further reduces to estimating

$$(41) \quad G(H, M, N, t)$$
$$= \sum_{H/2 \leq \nu \leq H} \sum_{M/2 \leq p \leq M} \sum_{N/2 \leq u \leq N} \chi_{P_1}(p)\chi_{P_2}(u) e\left(\frac{b}{a} p^* u^* \nu \right) e\left(\frac{\nu t}{apu} \right).$$

We recall the following result of Fouvry and Iwaniec [6, Theorem 6], which provides strong upper bounds for exponential sums with monomials:

Let $\alpha \neq 0, 1$ and $H, M, N, X \geq 1$. Let $\chi(\nu)$ be an additive character and ϕ_p, ψ_u be complex numbers with $|\phi_p| \leq 1$ and $|\psi_u| \leq 1$. Then

$$\left| \sum_{H/2 \leq \nu \leq H} \sum_{M/2 \leq p \leq M} \sum_{N/2 \leq u \leq N} \phi_p \psi_u \chi(\nu) e\left(X \frac{\nu u^{-1} p^\alpha}{HN^{-1}M^\alpha} \right) \right|$$

$$\ll (HMN)^{1/2} (\log(2HMNX))^4 \times$$

$$\times [X^{1/8}(H+N)^{1/2}(X^{1/8}H^{-1/6}M^{1/12}N^{1/6}$$
$$+ X^{1/8}H^{-1/8}N^{3/8} + N^{1/2} + N^{1/4}M^{1/8})$$
$$+ M^{1/2} + X^{-1/4}M^{1/2}N].$$

We cannot directly apply this theorem to our situation since our additive character $\chi(\nu) = e\left(\frac{b}{a}p^*u^*\nu\right)$ depends on the inverses of p and u modulo a. Therefore, we consider instead the following exponential sum

$$E_{s_1,s_2}(H,M,N,t)$$
$$= \sum_{\substack{H/2\leq\nu\leq H}} \sum_{\substack{M/2\leq p\leq M \\ p^*\equiv s_1\,(\mathrm{mod}\,a)}} \sum_{\substack{N/2\leq u\leq N \\ u^*\equiv s_2\,(\mathrm{mod}\,a)}} \chi_{P_1}(p)\chi_{P_2}(u)e\left(\frac{b}{a}s_1s_2\nu\right)e\left(\frac{\nu t}{apu}\right)$$

where $1 \leq s_1 < a$ and $1 \leq s_2 < a$ are fixed and relatively prime to a. We can apply the above theorem to $E_{s_1,s_2}(H,M,N,t)$ with $\phi_p = \chi^*_{P_1}(p)$, $\psi_u = \chi^*_{P_2}(u)$ where $\chi^*_{P_1}$ is the characteristic function of the primes in $p \in P_1$ that are in the progression $p \equiv s_1^*\,(\mathrm{mod}\,a)$ and $\chi^*_{P_2}$ is defined similarly. We also take $\alpha = -1$ and

$$X = \frac{tH}{aMN} = \frac{t}{y}x^{2\lambda}.$$

Note that $X \geq 1$ since $x - y \leq t \leq x$. We have $\frac{aMN}{y}x^{2\lambda} = H < N$ since using $M = x^{\delta_1+\mu}$ this reduces to $ax^{\delta_1+2\lambda+\mu} < x^\sigma = y$ and clearly we can find $\eta > 0$ small enough such that $a \leq x^\eta$ and $\delta_1 + 2\lambda + \mu + \eta < \sigma$. Hence

(42) $\qquad |E_{s_1,s_2}(H,M,N,t)| \ll MNa^{1/2}y^{-1/2}x^\lambda(\log x)^4 S$

where

(43) $\quad S = N^{1/2}(yM)^{-1/12}x^{1/4+\lambda/6}a^{-1/6} + N^{3/4}(yM)^{-1/8}x^{1/4+\lambda/4}a^{-1/8}$
$\qquad\qquad + Nx^{1/8+\lambda/4}y^{-1/8} + N^{3/4}M^{1/8}x^{1/8+\lambda/4}y^{-1/8}$
$\qquad\qquad + M^{1/2} + M^{1/2}Nx^{-1/4-\lambda/2}y^{1/4}.$

Next we estimate each summand in S. Let $\varepsilon' > 0$ denote an arbitrarily small number. We impose the following conditions on M and N:

(44) $\qquad\qquad\qquad M < yx^{-\varepsilon'},$

(45) $\qquad\qquad\qquad N^6 < My^7x^{-3-\varepsilon'},$

(46) $\qquad\qquad\qquad M^2N^4 < yx^{1-\varepsilon'}.$

Since $y \leq x^{1/2}$, it follows from (44)–(46) that

(47) $\qquad\qquad\qquad N^6 < My^5x^{-2-\varepsilon'},$

(48) $\qquad\qquad\qquad N^8 < y^5x^{-1-\varepsilon'},$

(49) $\qquad\qquad\qquad MN^6 < y^5x^{-1-\varepsilon'}.$

Using (45) we get

(50) $$N^{1/2}(yM)^{-1/12}x^{1/4+\lambda/6}a^{-1/6} < y^{1/2}x^{\lambda/6-\varepsilon'/12}.$$

By (47) it follows that

(51) $$N^{3/4}(yM)^{-1/8}x^{1/4+\lambda/4}a^{-1/8} < y^{1/2}x^{\lambda/4-\varepsilon'/8}.$$

From (48) we obtain

(52) $$Nx^{1/8+\lambda/4}y^{-1/8} < y^{1/2}x^{\lambda/4-\varepsilon'/8}.$$

Using (49) we see that

(53) $$N^{3/4}M^{1/8}x^{1/8+\lambda/4}y^{-1/8} < y^{1/2}x^{\lambda/4-\varepsilon'/8}.$$

Obviously (44) implies that

(54) $$M^{1/2} < y^{1/2}x^{-\varepsilon'/2},$$

and finally using (46) we obtain

(55) $$M^{1/2}Nx^{-1/4-\lambda/2}y^{1/4} < y^{1/2}x^{-\lambda/2-\varepsilon'/4}.$$

Clearly we can choose $\varepsilon' > 0$ such that

(56) $$\max\left(\frac{7\lambda}{6} - \frac{\varepsilon'}{12}, \frac{5\lambda}{4} - \frac{\varepsilon'}{8}\right) = -\gamma < 0.$$

Hence

(57) $$|E_{s_1,s_2}(H,M,N,t)| \ll MNa^{1/2}x^{-\gamma}(\log x)^4.$$

Since the number of pairs of reduced residue classes (s_1,s_2) modulo a is $\varphi(a)^2$ (φ is Euler's function) we find that

(58) $$|G(H,M,N,t)| \ll MN\varphi(a)^2a^{1/2}(\log x)^4x^{-\gamma} \ll MNa^{5/2}(\log x)^4x^{-\gamma}.$$

From (39) we finally obtain that

(59) $$\left|\sum_{p\in P_1}\sum_{u\in P_2} r_{pu,a,b}(x,y)\right| \leq Ca^{3/2}(\log x)^7x^{-\gamma}y + O(yx^{-\lambda})$$

where $C > 0$ is an absolute constant. Since $a \leq x^{\eta}$, choosing $\eta > 0$ small enough and replacing x by x/d_ω and y by y/d_ω we get from (16) that

(60) $$M_0 \geq C_A C_1 C_2 \frac{y}{a} + o(y/a).$$

Next we estimate E_1. The number of $x - y < n \leq x$ satisfying $n \equiv b$ (mod a) and $n \equiv 0$ (mod b_s) is

$$\leq \left[\frac{y}{ab_s}\right] + 1 \leq \frac{2y}{ab_s}$$

since $b_s \leq y/a$. It follows that

$$
(61) \qquad E_1 = \sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ b_m<b_s\leq y/a \\ n\equiv 0\,(\mathrm{mod}\,b_s)\,\text{for some }s>m}} w(n) \leq 2C(\delta_1,\delta_2)\frac{y}{a}\sum_{s=m+1}^{\infty}\frac{1}{b_s}.
$$

We may fix the value of m such that

$$
(62) \qquad C_A C_1 C_2 - 2C(\delta_1,\delta_2)\sum_{s=m+1}^{\infty}\frac{1}{b_s} = C_0 > 0.
$$

Hence we have

$$
(63) \qquad M_0 - E_1 \geq C_0\frac{y}{a} + o\left(\frac{y}{a}\right).
$$

To complete the proof we show that $E_2 = o(y/a)$. By the definition of $w(n)$ we get

$$
(64) \quad E_2 = \sum_{y/a<v^2\leq x}\sum_{p\in P_1}\sum_{u\in P_2}\sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\equiv 0\,(\mathrm{mod}\,v^2) \\ n\equiv 0\,(\mathrm{mod}\,pu)}}1 + \sum_{y/a<r\leq x}\sum_{p\in P_1}\sum_{u\in P_2}\sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\equiv 0\,(\mathrm{mod}\,r) \\ n\equiv 0\,(\mathrm{mod}\,pu)}}1
$$

where r denotes a prime in B and v denotes a prime not in B. Note that there is at most one $x-y<n\leq x$ satisfying either $n\equiv 0\,(\mathrm{mod}\,v^2)$ and $n\equiv b\,(\mathrm{mod}\,a)$ or $n\equiv 0\,(\mathrm{mod}\,r)$ and $n\equiv b\,(\mathrm{mod}\,a)$, since these congruences can be combined to $n\equiv c\,(\mathrm{mod}\,av^2)$ and $n\equiv c'\,(\mathrm{mod}\,ar)$ for suitable c and c' when $a\leq x^{\eta}$ and $\eta>0$ is small enough. But av^2 and ar are both $>y$. Moreover for any such n there are at most finitely many (independent of x) pairs (p,u) with $p\in P_1$ and $u\in P_2$ satisfying $n\equiv 0\,(\mathrm{mod}\,pu)$. Hence

$$
(65) \qquad V = \sum_{p\in P_1}\sum_{u\in P_2}\sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\equiv 0\,(\mathrm{mod}\,v^2) \\ n\equiv 0\,(\mathrm{mod}\,pu)}}1 = O(1),
$$

$$
(66) \qquad R = \sum_{p\in P_1}\sum_{u\in P_2}\sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\equiv 0\,(\mathrm{mod}\,r) \\ n\equiv 0\,(\mathrm{mod}\,pu)}}1 = O(1),
$$

where the implied constants are independent of v,r and x. It follows from (64)–(66) that

$$
(67) \qquad E_2 \ll \sum_{\substack{V>0 \\ y/a<v^2\leq x}}1 + \sum_{\substack{R>0 \\ y/a<r\leq x}}1.
$$

Let us assume that

(68) $$\delta_1 + \delta_2 + \sigma > 1.$$

If $y^2/a^2 < v^2 \leq x$ and $V > 0$, then v is not in P_1 or P_2 (since $a \leq x^\eta$ and $\eta > 0$ is small enough) so that $n \equiv 0 \pmod{puv^2}$ for some n with $x - y < n \leq x$. But $puv^2 \geq x^{\delta_1 + \delta_2 + 2\sigma - 2\eta} > x$ by (68) when η is small enough. Hence

(69) $$\sum_{\substack{V>0 \\ y/a < v^2 \leq x}} 1 \leq \sum_{y < v^2 \leq y^2/a^2} 1 = O\left(\frac{y/a}{\log(y/a)}\right) = o\left(\frac{y}{a}\right).$$

If $y/a < r \leq x$ and $R > 0$ then $n \equiv 0 \pmod{pur}$ for some $x - y < n \leq x$. But $pur \geq x^{\delta_1 + \delta_2 + \sigma - \eta} > x$ by (68) when η is small enough. Hence the sum over r in (67) is empty. This shows that $E_2 = o(y/a)$. Combining this with (63) we have

$$M_0 - E_1 - E_2 \geq C_0\, \frac{y}{a} + o\left(\frac{y}{a}\right).$$

The conditions (44), (45) and (46) are equivalent to $\delta_1 < \sigma$, $6\delta_2 < \delta_1 + 7\sigma - 3$ and $2\delta_1 + 4\delta_2 < 1 + \sigma$. Combining the first two conditions we get $\delta_2 < (8\sigma - 3)/6$. Hence from (68) we obtain $1 < \delta_1 + \delta_2 + \sigma < 2\sigma + (8\sigma - 3)/6$ which is equivalent to $\sigma > 9/20$. Moreover $2\delta_1 + 4\delta_2 < 2\sigma + (16\sigma - 6)/3 \leq 1 + \sigma$ gives $\sigma \leq 9/19$. Hence all of our conditions are compatible for $9/20 < \sigma \leq 9/19$. This completes the proof of Theorem 1. ∎

3. Proof of Theorem 2. The proof is similar to the proof of Theorem 1 so we will only mention the changes that need to be made. Let

$$f_E(z) = \sum_{n=1}^{\infty} a_E(n)q^n$$

be the weight two newform associated to $E/\mathbb{Q}$ without complex multiplication. We define

(70) $$B_E = \{p \text{ prime} : a_E(p) = 0\}.$$

Recall that a prime p not dividing the conductor N_E of $E/\mathbb{Q}$ is a supersingular prime if and only if $a_E(p) = 0$. Elkies [5] proved the striking unconditional estimate

(71) $$\#\{p \leq x : a_E(p) = 0\} \ll_E x^{3/4}.$$

As in the proof of Theorem 1, $a_E(n) \neq 0$ when n is square-free and B_E-free. Let A_E be the set of primes in B_E together with squares of primes not

in B_E. It suffices to show that

$$\sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\ \text{is}\ A_E\text{-free}}} w(n) \gg_{\sigma,E} \frac{y}{a}$$

where $w(n)$ is defined as in (6), $y = x^\sigma$ for $9/22 < \sigma \leq 1/2$ and b,a are relatively prime integers satisfying $1 \leq b < a \leq x^\theta$. Let $b_{s,E}$ denote the elements of A_E in increasing order. Consider

$$(72) \qquad \sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\ \text{is}\ A_E\text{-free}}} w(n)$$

$$\geq \sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\not\equiv 0\,(\mathrm{mod}\,b_{s,E})\ \text{for all}\ s\leq m}} w(n) - \sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ b_{m,E}<b_{s,E}\leq y/a \\ n\equiv 0\,(\mathrm{mod}\,b_{s,E})\ \text{for some}\ s>m}} w(n)$$

$$- \sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ y/a<b_{s,E}\leq x \\ n\equiv 0\,(\mathrm{mod}\,b_{s,E})\ \text{for some}\ s>m}} w(n).$$

Let us denote the right side of (72) by $M_0 - E_1 - E_2$. Note that M_0 and E_1 can be estimated as in the proof of Theorem 1. Using the definition of $w(n)$, E_2 becomes

$$(73) \quad E_2 = \sum_{y/a<v^2\leq x}\sum_{p\in P_1}\sum_{u\in P_2}\sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\equiv 0\,(\mathrm{mod}\,v^2) \\ n\equiv 0\,(\mathrm{mod}\,pu)}} 1 + \sum_{y/a<r\leq x}\sum_{p\in P_1}\sum_{u\in P_2}\sum_{\substack{x-y<n\leq x \\ n\equiv b\,(\mathrm{mod}\,a) \\ n\equiv 0\,(\mathrm{mod}\,r) \\ n\equiv 0\,(\mathrm{mod}\,pu)}} 1$$

where r denotes a prime in B_E and v denotes a prime not in B_E. Similarly we obtain

$$(74) \qquad E_2 \ll \sum_{\substack{V>0 \\ y/a<v^2\leq x}} 1 + \sum_{\substack{R>0 \\ y/a<r\leq x}} 1$$

where V and R are defined as in (65) and (66). Let us assume that

$$(75) \qquad \delta_1 + \delta_2 + \frac{4\sigma}{3} > 1.$$

Note that if for small $\varepsilon' > 0$, $x^{4\sigma/3-\varepsilon'} < r \leq x$ and $R > 0$, then $x-y < n \leq x$ and $n \equiv 0 \,(\mathrm{mod}\,pur)$ gives us a contradiction since
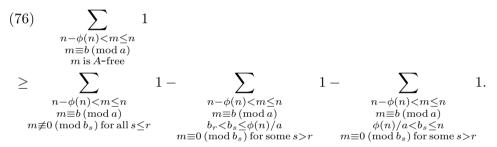
$$pur \geq x^{\delta_1+\delta_2+4\sigma/3-\varepsilon'} > x.$$

Hence using (71) we obtain

$$\sum_{\substack{R>0 \\ y/a<r\leq x}} 1 \leq \sum_{y/a<r\leq x^{4\sigma/3-\varepsilon'}} 1 \ll x^{\sigma-3\varepsilon'/4} = o\left(\frac{y}{a}\right)$$

when $\theta > 0$ is small enough. The sum on v can be estimated as before. Consequently $E_2 = o(y/a)$. The conditions (44), (45), (46) and (75) are compatible for $9/22 < \sigma \leq 9/19$. This completes the proof of Theorem 2. ∎

4. Proof of Theorem 3. Let B be defined as in (2) and let A be the set of primes in B together with squares of primes not in B. Let b_s denote the elements of A in increasing order. As before $a_f(n) \neq 0$ when n is A-free. We consider

$$(76) \qquad \sum_{\substack{n-\phi(n)<m\leq n \\ m\equiv b\,(\mathrm{mod}\,a) \\ m \text{ is } A\text{-free}}} 1$$

$$\geq \sum_{\substack{n-\phi(n)<m\leq n \\ m\equiv b\,(\mathrm{mod}\,a) \\ m\not\equiv 0\,(\mathrm{mod}\,b_s) \text{ for all } s\leq r}} 1 \;-\; \sum_{\substack{n-\phi(n)<m\leq n \\ m\equiv b\,(\mathrm{mod}\,a) \\ b_r<b_s\leq\phi(n)/a \\ m\equiv 0\,(\mathrm{mod}\,b_s) \text{ for some } s>r}} 1 \;-\; \sum_{\substack{n-\phi(n)<m\leq n \\ m\equiv b\,(\mathrm{mod}\,a) \\ \phi(n)/a<b_s\leq n \\ m\equiv 0\,(\mathrm{mod}\,b_s) \text{ for some } s>r}} 1.$$

We denote the right side of (76) by $M_0 - E_1 - E_2$. Using the Inclusion-Exclusion Principle we have

$$(77) \qquad M_0 = \sum_{\omega}(-1)^{|\omega|} \sum_{\substack{n-\phi(n)<m\leq n \\ m\equiv b\,(\mathrm{mod}\,a) \\ m\equiv 0\,(\mathrm{mod}\,d_\omega)}} 1$$

where ω runs over all subsets of $\{s : 1 \leq s \leq r\}$ and $d_\omega = \prod_{s\in\omega} b_s$. Since the congruences $m \equiv b\,(\mathrm{mod}\,a)$ and $m \equiv 0\,(\mathrm{mod}\,d_\omega)$ are equivalent to $m \equiv c\,(\mathrm{mod}\,ad_\omega)$ for some c we obtain

$$(78) \qquad \sum_{\substack{n-\phi(n)<m\leq n \\ m\equiv b\,(\mathrm{mod}\,a) \\ m\equiv 0\,(\mathrm{mod}\,d_\omega)}} 1 = \frac{\phi(n)}{ad_\omega} + r_{d_\omega,a,b}(n,\phi(n))$$

where $r_{d_\omega,a,b}(n,\phi(n))$ is a remainder term with absolute value ≤ 1. Combining (77) and (78) we get

$$(79) \qquad M_0 = \frac{\phi(n)}{a}\prod_{s\leq r}\left(1-\frac{1}{b_s}\right) + R_{a,b}(n,\phi(n))$$

where $R_{a,b}(n, \phi(n))$ is the sum of 2^r remainder terms so that $|R_{a,b}(n, \phi(n))| \leq 2^r$. As before we may put

$$C_A = \prod_{s=1}^{\infty} \left(1 - \frac{1}{b_s}\right) > 0$$

so that from (79) we obtain

$$(80) \qquad M_0 \geq C_A \frac{\phi(n)}{a} + R_{a,b}(n, \phi(n)).$$

The number of $n - \phi(n) < m \leq n$ satisfying $m \equiv b \pmod{a}$ and $m \equiv 0 \pmod{b_s}$ is

$$\leq \left[\frac{\phi(n)}{ab_s}\right] + 1 \leq \frac{2\phi(n)}{ab_s}$$

when $b_s \leq \phi(n)/a$ so that

$$(81) \qquad E_1 \leq \frac{2\phi(n)}{a} \sum_{s=r+1}^{\infty} \frac{1}{b_s}.$$

We may now fix r such that

$$C_A - 2 \sum_{s=r+1}^{\infty} \frac{1}{b_s} = C > 0.$$

Combining (80) and (81) we get

$$(82) \qquad M_0 - E_1 \geq C \frac{\phi(n)}{a} + R_{a,b}(n, \phi(n)).$$

Moreover since r is fixed and $a \leq \psi(n) = o(\phi(n))$ we have

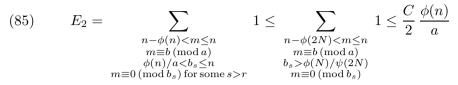$$|R_{a,b}(n, \phi(n))| \leq 2^r = o\left(\frac{\phi(n)}{a}\right).$$

Next we estimate E_2 on the average. Let N be a large integer and consider for $a \leq \psi(2N)$

$$(83) \qquad \sum_{N \leq n \leq 2N} \sum_{\substack{n - \phi(2N) < m \leq n \\ m \equiv b \,(\mathrm{mod}\, a) \\ \phi(N)/\psi(2N) < b_s \leq n \\ m \equiv 0 \,(\mathrm{mod}\, b_s) \text{ for some } s > r}} 1.$$

Changing the order of summation we see that (83) is

$$(84) \qquad \leq \sum_{\substack{N - \phi(2N) < m \leq 2N \\ m \equiv b \,(\mathrm{mod}\, a) \\ b_s > \phi(N)/\psi(2N) \\ m \equiv 0 \,(\mathrm{mod}\, b_s)}} \sum_{m \leq n < m + \phi(2N)} 1 \ll \phi(2N) \frac{N}{a} \sum_{b_s > \phi(N)/\psi(2N)} \frac{1}{b_s}.$$

Using $\phi(2N) \ll \phi(n)$ when $N \leq n \leq 2N$ and the monotonicity of $\phi(n)$, we get from (84) that

$$
(85) \qquad E_2 = \sum_{\substack{n-\phi(n)<m\leq n \\ m\equiv b\,(\mathrm{mod}\,a) \\ \phi(n)/a<b_s\leq n \\ m\equiv 0\,(\mathrm{mod}\,b_s)\,\text{for some}\,s>r}} 1 \leq \sum_{\substack{n-\phi(2N)<m\leq n \\ m\equiv b\,(\mathrm{mod}\,a) \\ b_s>\phi(N)/\psi(2N) \\ m\equiv 0\,(\mathrm{mod}\,b_s)}} 1 \leq \frac{C}{2}\,\frac{\phi(n)}{a}
$$

except for a subset of $[N, 2N]$ of cardinality

$$
O\!\left(N \sum_{b_s>\phi(N)/\psi(2N)} \frac{1}{b_s} \right).
$$

Using a dyadic partition of $[1, N]$ we get that the total number of exceptions $\leq N$ is

$$
(86) \qquad \ll \sum_{j\geq 1} \sum_{b_s>\phi(N/2^j)/\psi(N/2^{j-1})} \frac{N}{2^j b_s}.
$$

Let $\phi(N)/\psi(2N) = f(N)$ and note that $f(N)$ tends to infinity as N tends to infinity. Hence we may rewrite the right side of (86) as

$$
(87) \qquad \sum_{j<\frac12\log_2 N}\;\sum_{b_s>f(N/2^j)} \frac{N}{2^j b_s} + \sum_{j\geq\frac12\log_2 N}\;\sum_{b_s>f(N/2^j)} \frac{N}{2^j b_s}.
$$

If $j < \frac12 \log_2 N$, then $f(N/2^j) \geq f(\sqrt{N})$ and $\sum_{b_s>f(\sqrt{N})} 1/b_s$ tends to zero as N tends to infinity. Moreover the sum on $j \geq \frac12 \log_2 N$ is majorized by the tail of a geometric series. It follows from (87) that the total number of exceptions to (85) that are $\leq N$ is $o(N)$. Hence

$$
M_0 - E_1 - E_2 \geq \frac{C}{2}\,\frac{\phi(n)}{a} + o\!\left(\frac{\phi(n)}{a}\right)
$$

for almost all n. This completes the proof of Theorem 3. ∎

References

[1] E. Alkan, *Nonvanishing of Fourier coefficients of modular forms*, Proc. Amer. Math. Soc. 131 (2003), 1673–1680.

[2] —, *On the sizes of gaps in the Fourier expansion of modular forms*, Canad. J. Math., to appear.

[3] A. Balog and K. Ono, *The Chebotarev Density Theorem in short intervals and some questions of Serre*, J. Number Theory 91 (2001), 356–371.

[4] B. Berndt and K. Ono, *Ramanujan's unpublished manuscript on the partition and tau functions with proofs and commentary*, Sém. Lothar. Combin. 42 (1999).

[5] N. Elkies, *Distribution of supersingular primes*, Astérisque 198–200 (1992), 127–132.

[6] E. Fouvry and H. Iwaniec, *Exponential sums with monomials*, J. Number Theory 33 (1989), 311–333.

[7]   H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith. 37 (1980), 307–320.

[8]   K. Ono, *The Web of modularity*: *Arithmetic of the Coefficients of Modular Forms and q-series*, CBMS Reg. Conf. Ser. Math. 102, Amer. Math. Soc., Providence, RI, 2004, viii+216 pp.

[9]   J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401.

Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana, IL 61801, U.S.A.
E-mail: alkan@math.uiuc.edu
          zaharesc@math.uiuc.edu