

NONVANISHING OF FOURIER COEFFICIENTS OF MODULAR FORMS

EMRE ALKAN

(Communicated by David E. Rohrlich)

ABSTRACT. Let $f = \sum_{n=1}^{\infty} a_f(n)q^n$ be a cusp form with integer weight $k \geq 2$ that is not a linear combination of forms with complex multiplication. For $n \geq 1$, let

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

Improving on work of Balog, Ono, and Serre we show that $i_f(n) \ll_{f,\phi} \phi(n)$ for almost all n , where $\phi(x)$ is any good function (e.g. such as $\log \log(x)$) monotonically tending to infinity with x . Using a result of Fouvry and Iwaniec, if f is a weight 2 cusp form for an elliptic curve without complex multiplication, then we show for all n that $i_f(n) \ll_{f,\varepsilon} n^{\frac{69}{169} + \varepsilon}$. We also obtain conditional results depending on the Generalized Riemann Hypothesis and the Lang-Trotter Conjecture.

1. INTRODUCTION AND STATEMENT OF RESULTS

Estimating the size of possible gaps in the Fourier expansion of modular forms of various types has been an interesting subject for a long time. Perhaps the most famous open problem in the subject is a conjecture of Lehmer which says that $\tau(n) \neq 0$ for every positive integer n , where $\tau(n)$ is the Ramanujan function defined by ($q = e^{2\pi iz}$)

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

In recent years, there has been substantial progress on these questions. To investigate these gaps, Serre introduced the quantity

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

and he proved [S] that

$$i_f(n) \ll n$$

whenever $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ is a cusp form with integer weight $k \geq 2$, which is not a linear combination of forms with complex multiplication. In the same paper he asks for improvements of this estimate. In recent work, Balog and Ono [B-O] improved Serre's estimate with the following result.

Received by the editors January 9, 2002.

2000 *Mathematics Subject Classification*. Primary 11F30.

©2002 American Mathematical Society

Theorem. Suppose that $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ is a nonzero modular form with integer weight $k \geq 2$ that is not a linear combination of forms with complex multiplication. For every $\varepsilon > 0$ and $x^{\frac{17}{41}+\varepsilon} \leq y$ we have

$$\#\{x < n < x + y : a_f(n) \neq 0\} \gg_{f,\varepsilon} y.$$

In particular, we have $i_f(n) \ll_{f,\varepsilon} n^{\frac{17}{41}+\varepsilon}$.

Here we will pursue these questions and obtain the following results. Before stating our results, we require a simple definition. We shall call a function $\phi(x)$ good if

$$\phi(2x) \ll \phi(x)$$

for all large x . Observe that functions like $\log(x)$, $\log \log(x)$ and $x^{1/100}$ are all good functions.

Theorem 1. Let $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_k(\Gamma_0(N), \chi)$ be a nonzero cusp form with integer weight $k \geq 2$ that is not a linear combination of forms with complex multiplication. If $\phi(x)$ is a good function which tends monotonically to infinity with x , then for almost all n we have

$$\#\{n < m < n + \phi(n) : a_f(m) \neq 0\} \gg_{f,\phi} \phi(n).$$

In particular, we have $i_f(n) \ll_{f,\phi} \phi(n)$ for almost all n .

Thanks to a celebrated theorem of Elkies and the modularity of elliptic curves over \mathbb{Q} , we obtain the following result which holds for all n .

Theorem 2. Let E/\mathbb{Q} be an elliptic curve without complex multiplication, and let

$$L(E, s) = \sum_{n=1}^{\infty} a_E(n)n^{-s}$$

be its Hasse-Weil L -function. If $F_E(z) = \sum_{n=1}^{\infty} a_E(n)q^n$ is the associated weight 2 newform, then for any $\varepsilon > 0$ and $x^{\frac{69}{169}+\varepsilon} \leq y$ we have

$$\#\{x < n < x + y : a_E(n) \neq 0\} \gg_{E,\varepsilon} y.$$

In particular, we have $i_{F_E}(n) \ll_{E,\varepsilon} n^{\frac{69}{169}+\varepsilon}$ for every $\varepsilon > 0$.

We also have the following conditional results.

Theorem 3. Assuming the hypotheses of Theorem 1 and the Generalized Riemann Hypothesis for Dedekind Zeta functions, for every $\varepsilon > 0$ we have

$$\#\{x < n < x + y : a_f(n) \neq 0\} \gg_{f,\varepsilon} y,$$

where $x^{\frac{69}{169}+\varepsilon} \leq y$. In particular $i_f(n) \ll_{f,\varepsilon} n^{\frac{69}{169}+\varepsilon}$.

Let $B = \{p \text{ prime} : a_f(p) = 0\}$, where $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n$ is a nonzero cusp form on $\Gamma_0(N)$ with integer weight $k \geq 2$ and without complex multiplication. Then the Lang-Trotter conjecture (LT) says that

$$\#\{p < x : p \in B\} \ll_f \frac{x^{\frac{1}{2}}}{\log x}.$$

Theorem 4. Assuming LT, and the hypotheses of Theorem 1, if $\varepsilon > 0$, then

$$\#\{x < n < x + y : a_f(n) \neq 0\} \gg_{f,\varepsilon} y$$

where $x^{\frac{1}{3}+\varepsilon} \leq y$. In particular, we have $i_f(n) \ll_{f,\varepsilon} n^{\frac{1}{3}+\varepsilon}$.

2. RESULTS IN MULTIPLICATIVE NUMBER THEORY

By a B -free integer we mean an integer not divisible by any integer in the set B . We have the following result about B -free and square-free integers.

Theorem 2.1. *Let S be a set of primes for which $\sum_{p \in S} \frac{1}{p}$ converges, and let $\phi(x)$ be a good function monotonically tending to infinity with x . Then the number of S -free square-free integers in the interval $(n, n + \phi(n))$ is $\gg \phi(n)$ for almost all positive integers n .*

Proof. For simplicity, we will let $y = \phi(n)$ and let A be the set of primes in S together with squares of primes not in S . Clearly,

$$(2) \quad \sum_{\substack{n < m < n+y \\ m \text{ is } A\text{-free}}} 1 \geq \sum_{\substack{n < m < n+y \\ m \not\equiv 0 \pmod{b_s} \text{ for all } s \leq k}} 1 - \sum_{\substack{n < m < n+y \\ b_k < b_s \leq y \\ m \equiv 0 \pmod{b_s} \text{ for some } s > k}} 1 - \sum_{\substack{n < m < n+y \\ y < b_s < n+y \\ m \equiv 0 \pmod{b_s} \text{ for some } s > k}} 1,$$

where b_1, b_2, \dots are the elements of A in increasing order. Now,

$$\sum_{\substack{n < m < n+y \\ m \not\equiv 0 \pmod{b_s} \text{ for all } s \leq k}} 1 = y \prod_{s=1}^k \left(1 - \frac{1}{b_s}\right) + O(2^k),$$

where $B = \prod_{s=1}^{\infty} \left(1 - \frac{1}{b_s}\right) > 0$. Also

$$\sum_{\substack{n < m < n+y \\ b_k < b_s \leq y \\ m \equiv 0 \pmod{b_s} \text{ for some } s > k}} 1 \leq 2y \cdot \sum_{s=k+1}^{\infty} \frac{1}{b_s},$$

so that if k is large enough, then we have $B - 2 \cdot \sum_{s=k+1}^{\infty} \frac{1}{b_s} = C > 0$. Note that once k is fixed then clearly $O(2^k) = o(y)$, and the inequality in (2) becomes

$$(3) \quad \sum_{\substack{n < m < n+y \\ m \text{ is } A\text{-free}}} 1 \geq Cy + o(y) - \sum_{\substack{n < m < n+y \\ y < b_s < n+y \\ m \equiv 0 \pmod{b_s} \text{ for some } s > k}} 1.$$

Next assume $N < n < 2N$ and consider

$$\sum_{N < n < 2N} \sum_{\substack{n < m < n+\phi(2N) \\ \phi(N) < b_s < n+\phi(2N) \\ m \equiv 0 \pmod{b_s} \text{ for some } s > k}} 1.$$

By changing the order of summation, this double sum is easily seen to be $\ll \phi(2N)N \cdot \sum_{b_s > \phi(N)} \frac{1}{b_s}$, and so using monotonicity of ϕ and the fact that $\phi(2N) \ll \phi(n) = y$ for $N < n < 2N$, we get

$$(4) \quad \sum_{\substack{n < m < n+y \\ y < b_s < n+y \\ m \equiv 0 \pmod{b_s} \text{ for some } s > k}} 1 \leq \sum_{\substack{n < m < n+\phi(2N) \\ \phi(N) < b_s < n+\phi(2N) \\ m \equiv 0 \pmod{b_s} \text{ for some } s > k}} 1 \leq \frac{C}{2}y,$$

except for a subset of $(N, 2N)$ of cardinality $O(N \cdot \sum_{b_s > \phi(N)} \frac{1}{b_s})$. Taking $\frac{N}{2}, \frac{N}{2^2}, \frac{N}{2^3}, \dots$ successively, we get that the cardinality of exceptions in $(1, N)$ is

$$\ll \sum_{j \geq 1} \sum_{b_s > \phi(\frac{N}{2^j})} \frac{N}{2^j} \frac{1}{b_s}.$$

To see that this sum is $o(N)$ consider

$$\sum_{j \geq 1} \sum_{b_s > \phi(\frac{N}{2^j})} \frac{1}{2^j} \frac{1}{b_s} = \sum_{j < \frac{1}{2} \cdot \log_2(N)} \sum_{b_s > \phi(\frac{N}{2^j})} \frac{1}{2^j} \frac{1}{b_s} + \sum_{j \geq \frac{1}{2} \cdot \log_2(N)} \sum_{b_s > \phi(\frac{N}{2^j})} \frac{1}{2^j} \frac{1}{b_s}.$$

In the first double sum we just observe that $\phi(\frac{N}{2^j}) \geq \phi(N^{\frac{1}{2}})$ when $j < \frac{1}{2} \cdot \log_2(N)$ and $\sum_{b_s > \phi(N^{\frac{1}{2}})} \frac{1}{b_s}$ tends to zero with N . The second double sum is majorized by a tail of a geometric series, hence both double sums are $o(1)$. Therefore (3) and (4) imply the theorem. \square

Theorem 2.1 will be used to prove Theorem 1. The remaining results in this paper will follow from the next two theorems.

Theorem 2.2. *Let B be a subset of primes, and let $B(x)$ be the number of primes in B less than x . If $B(x) \ll x^\rho$ for some $\frac{1}{2} \leq \rho < 1$, then the number of B -free square-free integers in $(x, x + y)$ is $\gg y$, where $y = x^\varepsilon$ with $\varepsilon > \max(\frac{7}{19}, \frac{23\rho}{35\rho+16})$.*

Proof. Again let A be the set consisting of primes in B together with squares of primes not in B , and let b_1, b_2, \dots be elements of A in increasing order. Consider

$$P_1 := P_1(x, \delta_1, \mu) := \{x^{\delta_1} < p < x^{\delta_1 + \mu} : p \text{ is prime}\},$$

$$P_2 := P_2(x, \delta_2, \mu) := \{x^{\delta_2} < q < x^{\delta_2 + \mu} : q \text{ is prime}\},$$

and assume that $\delta_1 + \mu < \delta_2 < \delta_2 + \mu < \varepsilon$ and μ is as small as we want. For $n \leq x$ let

$$w(n) = \sum_{p \in P_1} \sum_{q \in P_2} \sum_{n \equiv 0 \pmod{pq}} 1.$$

Clearly $w(n) \leq C(\delta_1, \delta_2)$, a constant independent of x . Moreover, we have

$$(5) \quad \sum_{\substack{x < n < x+y \\ n \text{ is } A\text{-free}}} w(n) \geq \sum_{\substack{x < n < x+y \\ n \not\equiv 0 \pmod{b_s} \text{ for all } s \leq k}} w(n) - \sum_{\substack{x < n < x+y \\ b_k < b_s \leq y \\ n \equiv 0 \pmod{b_s} \text{ for some } s > k}} w(n) - \sum_{\substack{x < n < x+y \\ y < b_s < x+y \\ n \equiv 0 \pmod{b_s} \text{ for some } s > k}} w(n).$$

Next we estimate these sums:

$$(6) \quad \sum_{\substack{x < n < x+y \\ n \not\equiv 0 \pmod{b_s} \text{ for all } s \leq k}} w(n) = \sum_{\substack{x < n < x+y \\ n \not\equiv 0 \pmod{b_s} \text{ for all } s \leq k \\ n \equiv 0 \pmod{pq} \text{ } p \in P_1, q \in P_2}} 1$$

$$= \sum_{\omega} (-1)^{|\omega|} \sum_{p \in P_1, q \in P_2} \sum_{\substack{x < n < x+y \\ n \equiv 0 \pmod{pq} \\ n \equiv 0 \pmod{d_\omega}}} 1,$$

where ω runs through all subsets of $1, 2, \dots, k$ and $d_\omega = \prod_{s \in \omega} b_s$ ($d_\omega = 1$ if ω is empty). Note that once k is fixed and x is large enough then we have $\gcd(d_\omega, pq) = 1$ for all subsets ω . We define the remainder terms $r_d(x, y)$ as

$$r_d(x, y) + \frac{y}{d} = \# \text{ of multiples of } d \text{ in } (x, x + y),$$

so that

$$\sum_{\substack{x < n < x+y \\ n \equiv 0 \pmod{pqd_\omega}}} 1 = r_{pqd_\omega}(x, y) + \frac{y}{pqd_\omega}.$$

We now have, by (6),

$$\begin{aligned} \sum_{\substack{x < n < x+y \\ n \not\equiv 0 \pmod{b_s} \text{ for all } s \leq k}} w(n) &= y \sum_{x^{\delta_1} < p < x^{\delta_1 + \mu}} \frac{1}{p} \sum_{x^{\delta_2} < q < x^{\delta_2 + \mu}} \frac{1}{q} \cdot \prod_{s \leq k} \left(1 - \frac{1}{b_s}\right) \\ (7) \qquad &+ \sum_{\omega} (-1)^{|\omega|} \sum_{p \in P_1, q \in P_2} r_{pqd_\omega}(x, y) \\ &\geq Cy \sum_{x^{\delta_1} < p < x^{\delta_1 + \mu}} \frac{1}{p} \sum_{x^{\delta_2} < q < x^{\delta_2 + \mu}} \frac{1}{q} + R, \end{aligned}$$

where

$$R = \sum_{\omega} (-1)^{|\omega|} \sum_{p \in P_1, q \in P_2} r_{pq} \left(\frac{x}{d_\omega}, \frac{y}{d_\omega} \right)$$

and $C = \prod_{s=1}^{\infty} (1 - \frac{1}{b_s}) > 0$. Note that

$$\sum_{x^{\delta_1} < p < x^{\delta_1 + \mu}} \frac{1}{p} = \log \left(1 + \frac{\mu}{\delta_1} \right) + O \left(\frac{1}{\log x} \right) \geq C_1$$

and similarly

$$\sum_{x^{\delta_2} < q < x^{\delta_2 + \mu}} \frac{1}{q} \geq C_2$$

when x is large enough and C_1, C_2 are constants independent of x . To estimate R we recall the following result from [F-I]:

Theorem. *Let $x^{\frac{7}{19}} < y < x^{\frac{11}{23}}$. If $\theta > 0$, then*

$$R(M, N) = \sum_{1 \leq m < M} \sum_{1 \leq n < N} a_m c_n r_{mn}(x, y) \ll yx^{-\theta},$$

provided $M < yx^{-\eta}$ and $N < y^{\frac{19}{16}} x^{-\frac{7}{16} - \eta}$, where $\eta = K\theta$, $K > 0$ is independent of θ , and all a_m, c_n are complex numbers with modulus at most 1.

We apply the theorem with $a_m = 1$ if $m \in P_1$ and 0 otherwise, similarly $c_n = 1$ if $n \in P_2$ and 0 otherwise. We choose δ_1, δ_2 such that $\delta_2 + \mu < \varepsilon - \eta$ and $\delta_1 + \mu < \frac{19\varepsilon - 7}{16} - \eta$. As $\theta > 0$ can be arbitrarily small, $\eta > 0$ is also arbitrarily small. Also recall that by assumption $\mu > 0$ is arbitrarily small. Hence these inequalities are clearly equivalent to $\delta_2 < \varepsilon$ and $\delta_1 < \frac{19\varepsilon - 7}{16}$. Replacing x and y by $\frac{x}{d_\omega}$ and $\frac{y}{d_\omega}$ respectively in the above theorem gives

$$\sum_{p \in P_1, q \in P_2} r_{pq} \left(\frac{x}{d_\omega}, \frac{y}{d_\omega} \right) = o(y).$$

Hence $R = o(y)$, and so (7) implies that

$$(8) \quad \sum_{\substack{x < n < x+y \\ n \not\equiv 0 \pmod{b_s} \text{ for all } s \leq k}} w(n) \geq CC_1C_2y + o(y).$$

We also have

$$\sum_{\substack{x < n < x+y \\ b_k < b_s \leq y \\ n \equiv 0 \pmod{b_s} \text{ for some } s > k}} w(n) \leq 2C(\delta_1, \delta_2)y \cdot \sum_{s=k+1}^{\infty} \frac{1}{b_s}$$

and

$$\begin{aligned} \sum_{\substack{x < n < x+y \\ y < b_s < x+y \\ n \equiv 0 \pmod{b_s} \text{ for some } s > k}} w(n) &= \sum_{y < v^2 < x+y} \sum_{p \in P_1} \sum_{q \in P_2} \sum_{\substack{x < n < x+y \\ n \equiv 0 \pmod{v^2} \\ n \equiv 0 \pmod{pq}}} 1 \\ &+ \sum_{y < r < x+y} \sum_{p \in P_1} \sum_{q \in P_2} \sum_{\substack{x < n < x+y \\ n \equiv 0 \pmod{r} \\ n \equiv 0 \pmod{pq}}} 1, \end{aligned}$$

where in the above summations v denotes a prime not in B and r denotes a prime in B . Note that there is at most one n with $x < n < x + y$ such that $n \equiv 0 \pmod{v^2}$ or $n \equiv 0 \pmod{r}$. Moreover for such n , there are at most finitely many (independent of x) pairs (p, q) , $p \in P_1, q \in P_2$, satisfying $n \equiv 0 \pmod{pq}$. Hence

$$V := \sum_{p \in P_1} \sum_{q \in P_2} \sum_{\substack{x < n < x+y \\ n \equiv 0 \pmod{v^2} \\ n \equiv 0 \pmod{pq}}} 1 = O(1)$$

and

$$R := \sum_{p \in P_1} \sum_{q \in P_2} \sum_{\substack{x < n < x+y \\ n \equiv 0 \pmod{r} \\ n \equiv 0 \pmod{pq}}} 1 = O(1),$$

where the implied constants are independent of v, r and x . It follows that

$$\sum_{\substack{x < n < x+y \\ y < b_s < x+y \\ n \equiv 0 \pmod{b_s} \text{ for some } s > k}} w(n)$$

\ll the number of v^2 such that $y < v^2 < x + y$ and $V > 0$ + the number of r such that $y < r < x + y$ and $R > 0$. Let us now assume that $\delta_1 + \delta_2 + \frac{\varepsilon}{\rho} > 1$. Note that this also implies $\delta_1 + \delta_2 + 2\varepsilon > 1$. If $y^2 \leq v^2 < x + y$ and $V > 0$, then v is not in P_1 or P_2 and $n \equiv 0 \pmod{pqv^2}$ for some n with $x < n < x + y$, but $pqv^2 \geq x + y$ when x is large enough, and this is a contradiction. Hence the number of v^2 such that $y < v^2 < x + y$ and $V > 0$ is \leq the number of v^2 such that $y < v^2 < y^2$, which is $o(y)$. Similarly if $\frac{x^\rho}{\log(x)} \leq r < x + y$ and $R > 0$, then we get a contradiction and the number of r such that $y < r < x + y$ and $R > 0$ is \leq the number of r such that

$y < r < \frac{x^\varepsilon}{\log(x)}$, which is again $o(y)$. Finally (5) and (8) imply that

$$\sum_{\substack{x < n < x+y \\ n \text{ is } A\text{-free}}} 1 \gg \sum_{\substack{x < n < x+y \\ n \text{ is } A\text{-free}}} w(n) \geq CC_1C_2 \cdot y - 2C(\delta_1, \delta_2) \cdot y \sum_{s=k+1}^\infty \frac{1}{b_s} + o(y),$$

and when x is large enough we get

$$\sum_{\substack{x < n < x+y \\ n \text{ is } A\text{-free}}} 1 \gg y = x^\varepsilon.$$

The compatibility of the conditions we have imposed gives the condition on ε as stated. This completes the proof of Theorem 2.2. \square

Theorem 2.3. *Let B be a subset of primes such that $B(x) \ll x^{\frac{1}{2}}$, and let $\varepsilon > \frac{1}{3}$. Then the number of B -free square-free integers in $(x, x + y)$ is $\gg y$, where $y = x^\varepsilon$.*

Proof. The proof is very similar to the proof of Theorem 2.2 so we will mention only the slight changes that have to be made. Let

$$P = P(x, \delta, \mu) =: \{x^\delta < p < x^{\delta+\mu} : p \text{ is prime}\}.$$

For $n \leq x$ consider

$$w(n) = \sum_{p \in P} \sum_{n \equiv 0 \pmod{p}} 1.$$

We assume $\delta + \mu < \varepsilon$ and as before $w(n)$ is bounded independently of x and

$$\begin{aligned} \sum_{\substack{x < n < x+y \\ n \text{ is } A\text{-free}}} w(n) &\geq \sum_{\substack{x < n < x+y \\ n \not\equiv 0 \pmod{b_s} \text{ for some } s \leq k}} w(n) - \sum_{\substack{x < n < x+y \\ b_k < b_s \leq y \\ n \equiv 0 \pmod{b_s} \text{ for some } s > k}} w(n) \\ &\quad - \sum_{\substack{x < n < x+y \\ y < b_s < x+y \\ n \equiv 0 \pmod{b_s} \text{ for some } s > k}} w(n). \end{aligned}$$

We have

$$\sum_{\substack{x < n < x+y \\ n \not\equiv 0 \pmod{b_s} \text{ for all } s \leq k}} w(n) \geq Cy \cdot \sum_{x^\delta < p < x^{\delta+\mu}} \frac{1}{p} + R,$$

where

$$R = \sum_{\omega} (-1)^{|\omega|} \sum_{p \in P} r_p \left(\frac{x}{d_\omega}, \frac{y}{d_\omega} \right) = O \left(\frac{x^{\delta+\mu}}{\log(x)} \right) = o(y).$$

The other summations can be estimated as before with the only change in the last summation where we can impose $2\varepsilon + \delta > 1$ this time because of our assumption $B(x) \ll x^{\frac{1}{2}}$. This gives $\varepsilon > \frac{1}{3}$ and Theorem 2.3 follows. \square

3. PROOFS OF THEOREMS 1, 2, 3, 4

Without loss of generality we may prove Theorems 1, 3 and 4 for newforms

$$f(z) = \sum_{n=1}^\infty a_f(n)q^n.$$

The general case for forms of weight $k \geq 2$ without CM follows from the newform case by applying the argument appearing at the beginning of the proof of [B-O, Th. 1].

Proof of Theorem 1. Serre has proved [S] unconditionally for every $\varepsilon > 0$ that

$$\#\{p < x : \text{prime and } a_f(p) = 0\} \ll_{f,\varepsilon} \frac{x}{\log(x)^{\frac{3}{2}-\varepsilon}}.$$

Now let S be the set of primes p for which either p divides N or $a_f(p) = 0$.

If n is square-free, then

$$a_f(n) = \prod_{p|n} a_f(p),$$

by multiplicativity of the Fourier coefficients of a newform. Hence $a_f(n)$ is nonzero when n is S -free and square-free. Clearly, $\sum_{p \in S} \frac{1}{p}$ is finite, and so Theorem 2.1 implies that the number of S -free square-free integers in $(n, n + \phi(n))$ is $\gg \phi(n)$ for almost all n . This completes the proof of Theorem 1. \square

Proof of Theorem 2. If E/\mathbb{Q} is an elliptic curve without complex multiplication and $\pi_0(x)$ is the number of supersingular primes for E/\mathbb{Q} up to x , then Elkies [E] proved that $\pi_0(x) \ll x^{\frac{3}{4}}$. To complete the proof it is enough to take $\rho = \frac{3}{4}$ in Theorem 2.2. Also note that p is a supersingular prime for E/\mathbb{Q} if and only if the number of \mathbb{F}_p points $p + 1 - a_E(p)$ on E/\mathbb{Q} modulo p is exactly $p + 1$ (i.e. $a_E(p) = 0$). \square

Proof of Theorem 3. Under GRH for Dedekind Zeta functions, Serre has proved [S] that

$$\#\{p < x : \text{prime and } a_f(p) = 0\} \ll_f x^{\frac{3}{4}}.$$

Let S be defined as in the proof of Theorem 1. Hence we can take $\rho = \frac{3}{4}$ in Theorem 2.2 to complete the proof of Theorem 3 similarly. \square

Proof of Theorem 4. Let S be as above. By LT we have

$$\#\{p < x : \text{prime and } a_f(p) = 0\} \ll \frac{x^{\frac{1}{2}}}{\log(x)} \ll x^{\frac{1}{2}}.$$

Theorem 2.3 completes the proof. \square

ACKNOWLEDGEMENT

The author thanks A. Balog, K. Ono and D. Rohrlich for helpful comments.

REFERENCES

- [B-O] A. Balog and K. Ono, *The Chebotarev density theorem in short intervals and some questions of Serre*, J. Number Theory **91** (2001), 356–371.
- [F-I] E. Fouvry and H. Iwaniec, *Exponential sums with monomials*, J. Number Theory **33** (1989), 311–33. MR **91b**:11097
- [E] N. Elkies, *Distribution of supersingular primes*, Astérisque (1992), 127–132. MR **93b**:11070
- [S] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. MR **83k**:12011

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN 53706
E-mail address: `alkan@math.wisc.edu`