New York Journal of Mathematics

New York J. Math. **20** (2014) 1–11.

Divisors of Fourier coefficients of modular forms

Sanoli Gun and M. Ram Murty

Abstract. Let $d(n)$ denote the number of divisors of n. In this paper, we study the average value of $d(a(p))$, where p is a prime and $a(p)$ is the p-th Fourier coefficient of a normalized Hecke eigenform of weight $k \geq 2$ for $\Gamma_0(N)$ having rational integer Fourier coefficients.

Contents

1. Introduction

Throughout the paper, let p, ℓ be primes, $\mathcal{H} = \{z \in \mathcal{C} \mid \Im(z) > 0\}$ be the upper half plane. Also let $N \geq 1$ be a natural number and $k \geq 2$ be an even integer. Let $\pi(x)$ denote the usual prime counting function up to x. Let f be a normalized Hecke eigen cusp form of weight k for $\Gamma_0(N)$ with Nebentypus χ. Suppose that the Fourier expansion of f at $i\infty$ is

$$f(z) = \sum_{n \geq 1} a(n) q^n,$$

where $q = e^{2\pi i z}$. In this paper, we assume that $a(n)$ are rational integers. The second author and Kumar Murty [12] considered the average value of $\nu(a(n))$, where $\nu(n)$ is the number of distinct prime divisors of n. In this paper, we investigate the sum $\sum_{p \leq x} d(a(p))$, where $d(n) = \sum_{\delta | n} 1$. An essential ingredient in our work is a technique that can be traced back

Received November 27, 2013.

2010 *Mathematics Subject Classification.* 11F30, 11N37.

Key words and phrases. Divisor function, Fourier coefficients of modular forms, generalized Riemann hypothesis, Chebotarev density theorem.

Research of the first author was partially supported by IMSc Number Theory grant. Research of the second author was partially supported by an NSERC Discovery grant.

ISSN 1076-9803/2014

to van der Corput [22] who majorized the divisor function by short sums. This technique was later refined by many authors. We use a refinement due to Friedlander and Iwaniec [7]. Our result can be thought of as a modular analogue of a result of Erdös [6] who considered the asymptotics of $\sum_{n\le x} d(F(n))$, where $F(x)$ is an irreducible polynomial with integral coefficients. Finding average value of divisors of arithmetic functions has a long history. Some of the relevant papers in this direction are [6], [7] and [10].

2. Preliminaries and statement of the result

For an integer $\delta \ge 1$ and $x \in \mathbb{R}$, set

$$\pi^*(x,\delta) = \#\{p \le x \mid a(p) \equiv 0 \pmod{\delta}\},$$
$$\pi(x,\delta) = \#\{p \le x \mid a(p) \ne 0,\ a(p) \equiv 0 \pmod{\delta}\}.$$

As before, let $f(z) = \sum_{n\ge1} a(n)q^n$ be a normalized Hecke eigenform of weight k for $\Gamma_0(N)$ with Nebentypus χ and rational integer Fourier coefficients. For a prime ℓ, let $\mathbb{Z}_\ell$ denote the ring of ℓ-adic integers and $\mathrm{G} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By the work of Deligne [3] and as the Fourier coefficients of f are integers, there is a continuous representation

$$\rho_\delta : \mathrm{G} \to \mathrm{GL}_2\left(\prod_{\ell|\delta} \mathbb{Z}_\ell\right)$$

(where the product is over distinct prime divisors) for any positive integer $\delta > 1$. This representation is unramified outside the primes dividing δN and for $p \nmid N\delta$,

$$\mathrm{tr}\ \rho_\delta(\sigma_p) = a(p), \qquad \det\ \rho_\delta(\sigma_p) = \chi(p)p^{k-1},$$

where σ_p is a Frobenius element of p in G and $\mathbb{Z}$ is embedded diagonally in $\prod_{\ell|\delta}\mathbb{Z}_\ell$. Denote by $\tilde{\rho}_\delta$ the reduction modulo δ of ρ_δ:

$$\tilde{\rho}_\delta : \mathrm{G} \xrightarrow{\rho_\delta} \mathrm{GL}_2\left(\prod_{\ell|\delta} \mathbb{Z}_\ell\right) \twoheadrightarrow \mathrm{GL}_2(\mathbb{Z}/\delta).$$

Let H_δ be the kernel of $\tilde{\rho}_\delta$, K_δ the sub field of $\overline{\mathbb{Q}}$ fixed by H_δ and $\mathrm{G}_\delta = \mathrm{Gal}(\mathrm{K}_\delta/\mathbb{Q})$. Let C_δ be the subset of $\tilde{\rho}_\delta(G)$ consisting of elements of trace zero and let $h(\delta) = |\mathrm{C}_\delta|/|\mathrm{G}_\delta|$.

The condition $a(p) \equiv 0 \,(\mathrm{mod}\ \delta)$, where $(p,\delta\mathrm{N}) = 1$ means that for any Frobenius element σ_p of p, $\tilde{\rho}_\delta(\sigma_p) \in \mathrm{C}_\delta$. Hence by the Chebotarev density theorem applied to $\mathrm{K}_\delta/\mathbb{Q}$, we have

$$\pi^*(x,\delta) \sim \frac{|\mathrm{C}_\delta|}{|\mathrm{G}_\delta|}\pi(x) = h(\delta)\pi(x).$$

As C_δ contains the image of complex conjugation, it is nonempty. Note that $K_{\ell_1^{n_1}} \cap K_{\ell_2^{n_2}} = \mathbb{Q}$ for distinct primes ℓ_1, ℓ_2 and natural numbers n_1, n_2. This implies that $h(\delta) = \prod_{\ell^n || \delta} h(\ell^n)$, where $\ell^n || \delta$ means that $\ell^n | \delta$ and $\ell^{n+1} \nmid \delta$.

Now suppose that the Generalized Riemann Hypothesis (GRH), i.e., the Riemann Hypothesis for all Artin L-series is true. Then by the works of Lagarias and Odlyzko [9], one can show that

$$\pi^*(x, \delta) = h(\delta)\pi(x) + O\left(\delta^3 x^{1/2} \log(\delta \mathrm{N} x)\right).$$

An improved error term is available provided one also assumes the Artin holomorphy conjecture as proved by M. R. Murty, V. K. Murty and N. Saradha [13]. Moreover, if we define

$$\mathrm{Z}(x) = \{p \leq x \mid a(p) = 0\}$$

then as mentioned in [12] one can show the following lemma from the works of Ribet [16] and Serre [20];

Lemma 1. *Suppose that f does not have complex multiplication. Then $\mathrm{Z}(x) \ll x/(\log x)^{3/2-\epsilon}$ for all $\epsilon > 0$. Further, suppose that GRH is true. Then $\mathrm{Z}(x) \ll x^{3/4}$.*

If f has complex multiplication, then $\mathrm{Z}(x) \sim \frac{1}{2}\pi(x)$. Now suppose that GRH is true. Then as noted by the second author and Kumar Murty [12], one has:

Lemma 2. *Suppose that f does not have complex multiplication and GRH is true. Then for $x \geq 2$,*

$$\pi(x, \delta) = h(\delta)\pi(x) + O\left(\delta^3 x^{1/2} \log(\delta \mathrm{N} x)\right) + O(x^{3/4}).$$

Also it follows from the works of Carayol [2], Momose [11], Ribet [15, 17], Serre [19] and Swinnerton-Dyer [21] that for ℓ sufficiently large,

$$\mathrm{T}_\ell := \ \mathrm{Im}\ \rho_\ell = \left\{\gamma \in \mathrm{GL}_2(\mathbb{F}_\ell) \mid \det \gamma \in (\mathbb{F}_\ell^\times)^{k-1}\right\}.$$

In this paper, we prove:

Theorem 3. *Assume that GRH is true. Also, assume that f is a normalized Hecke eigen cusp form of weight k for $\Gamma_0(N)$ with rational integer Fourier coefficients $\{a(n)\}$. Moreover, suppose that f does not have complex multiplication. We have*

$$x \ll \sum_{\substack{p \leq x \\ a(p) \neq 0}} d(a(p)) \ll x(\log x)^A, \tag{1}$$

where A is an absolute constant which depends on f.

Remark 4. It is worth noting that above theorem is true unconditionally when f is a normalized Hecke eigen cusp form of $k = 2$. Indeed, the estimate in Lemma 2 is unconditional if one is considering the case $k = 2$. For in this case, the modular form corresponds to an elliptic curve by a celebrated theorem of Wiles [23] and subsequent work of Breuil, Conrad, Diamond and Taylor [1]. With this theorem in hand, the primes enumerated by $\mathrm{Z}(x)$ are precisely the supersingular primes. Indeed, based on a suggestion of the second author, Elkies (see p. 25 of [4] and [5]) has shown unconditionally that the number of supersingular primes is $O(x^{3/4})$. Thus, for $k = 2$, we can dispense with the GRH in Lemma 2.

In order to prove the theorem, the following lemmas play an important role. The first one was proved by Friedlander and Iwaniec [7] and for the proof of the second lemma we use Rankin's trick. But as Rankin [14] points out, it should really be called Ingham's trick since Ingham told Rankin about it.

Lemma 5. *Let $m, r \geq 2$ and $n \geq 1$. Then*

$$d_r(n) \leq \sum_{\substack{\delta | n \\ \delta \leq n^{1/m}}} (2d(\delta))^{(r-1)\frac{m \log m}{\log 2}},$$

where

$$d_r(n) = \sum_{\substack{n_1 \cdots n_r = n \\ n_1, \cdots, n_r \geq 1}} 1.$$

Proof. See [7].

Lemma 6. *Suppose $b(n) \geq 0$ for $n \geq 1$ and*

$$D(s) := \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$$

converges for $s \in \mathbb{C}$ with $\Re(s) > t \geq 0$. Then

$$\sum_{n \leq x} b(n) \leq x^u \ D(u)$$

for any $u, x \in \mathbb{R}$ with $u > t$ and $x \geq 1$.

Proof. Note that for any real number $u > t$, we have

$$\sum_{n \leq x} b(n) \ \leq \ \sum_{n=1}^{\infty} b(n) \left(\frac{x}{n}\right)^u \ \leq \ x^u D(u). \qquad \square$$

In most applications, we choose $u = t + (1/\log x)$.

3. A group theoretic estimate

For an odd prime ℓ, let $\mathrm{B}_\ell := \mathrm{GL}_2(\mathbb{F}_\ell)$ and

$$\mathrm{A}_\ell := \{\gamma \in \mathrm{B}_\ell \mid \mathrm{tr}\ \gamma = 0\}.$$

The conjugacy classes of B_ℓ are one of the following four types:

$$\alpha_a := \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \qquad \alpha_b := \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix},$$
$$\alpha_{a,\delta} := \begin{pmatrix} a & 0 \\ 0 & \delta \end{pmatrix},\ a \neq \delta, \qquad \beta_{a,b} := \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix},\ b \neq 0,$$

where $a, b, \delta \in \mathbb{F}_\ell^\times$ and $\{1, \sqrt{\epsilon}\}$ is a basis for $\mathbb{F}_\ell^2$ over $\mathbb{F}_\ell$. The number of elements in these classes are $1, \ell^2-1, \ell^2+\ell$ and $\ell^2-\ell$ respectively (see Fulton and Harris [8], page 68 for details). Hence the elements of A_ℓ come from the conjugacy classes $\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ and $\begin{pmatrix} 0 & \epsilon b \\ b & 0 \end{pmatrix}$, where $a, b \in \mathbb{F}_\ell^\times$. Further, the elements $\begin{pmatrix} a & 0 \\ 0 & -a \end{pmatrix}$ and $\begin{pmatrix} -a & 0 \\ 0 & a \end{pmatrix}$ belong to the same class and the elements $\begin{pmatrix} 0 & \epsilon b \\ b & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & -\epsilon b \\ b & 0 \end{pmatrix}$ belong to the same class. Therefore

$$|\mathrm{A}_\ell| = [(\ell^2+\ell)(\ell-1) + (\ell^2-\ell)(\ell-1)]/2 = \ell^2(\ell-1).$$

Also $|\mathrm{B}_\ell| = |\{\gamma \in \mathrm{A}_\ell \mid \ \det\gamma \in \mathbb{F}_\ell^\times\}| = (\ell^2-1)(\ell^2-\ell)$. Further, we calculate the cardinality of the sets $\mathrm{B}_{\ell^n} := \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ and

$$\mathrm{A}_{\ell^n} := \{\gamma \in \mathrm{B}_{\ell^n} \mid \mathrm{tr}\ \gamma = 0\}$$

for all $n \geq 1$. Note that any $\begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \mathrm{B}_\ell$ lifts to

$$\begin{pmatrix} a+\beta_1\ell & b+\beta_2\ell \\ c+\beta_3\ell & \delta+\beta_4\ell \end{pmatrix} \in \mathrm{B}_{\ell^n},$$

where $1 \leq \beta_1, \beta_2, \beta_3, \beta_4 \leq \ell^{n-1}$, $\beta_i \in \mathbb{Z}$ for all $1 \leq i \leq 4$. Also any $\begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in \mathrm{A}_\ell$ lifts to

$$\begin{pmatrix} a+\beta_1\ell & b+\beta_2\ell \\ c+\beta_3\ell & -a-\beta_1\ell \end{pmatrix} \in \mathrm{A}_{\ell^n}$$

for any choice of $\beta_1, \beta_2, \beta_3 \in \mathbb{Z}$ with $1 \leq \beta_1, \beta_2, \beta_3 \leq \ell^{n-1}$. Since the maps $\mathrm{B}_{\ell^n} \to \mathrm{B}_\ell$ and $\mathrm{A}_{\ell^n} \to \mathrm{A}_\ell$ are surjective, it is easy to see from the above observations that $|\mathrm{B}_{\ell^n}| = \ell^{4(n-1)}|\mathrm{B}_\ell|$ and $|\mathrm{A}_{\ell^n}| = \ell^{3(n-1)}|\mathrm{A}_\ell|$.

Next for an even integer $k > 2$, we calculate the cardinality of the sets

$$C_\ell := \left\{\gamma \in \mathrm{B}_\ell \mid \det\gamma \in (\mathbb{F}_\ell^\times)^{k-1}\right\},$$
$$D_\ell := \{\gamma \in C_\ell \mid \mathrm{tr}\ \gamma = 0\}.$$

Writing $\gcd(\ell-1, k-1) := d$, one has

$$\begin{aligned} C_\ell &= \left\{\gamma \in \mathrm{B}_\ell \mid \det\gamma \in (\mathbb{F}_\ell^\times)^d\right\} \\ &= \left\{\gamma \in \mathrm{B}_\ell \mid (\det\gamma)^{(\ell-1)/d} \equiv 1 \pmod{\ell}\right\}. \end{aligned}$$

Consider the surjective group homomorphism

$$\phi : GL_2(\mathbb{F}_\ell) \to (\mathbb{F}_\ell^\times)^{(\ell-1)/d}$$

which sends $\gamma \mapsto (\det \gamma)^{(\ell-1)/d}$. From the previous discussions, it is clear that $\ker \phi = C_\ell$. Hence

$$|C_\ell| = \frac{|B_\ell|}{|(\mathbb{F}_\ell^\times)^{\frac{\ell-1}{d}}|}.$$

But

$$|(\mathbb{F}_\ell^\times)^{\frac{\ell-1}{d}}| = \frac{|\mathbb{F}_\ell^\times|}{\left|\left\{x \in \mathbb{F}_\ell^\times \mid x^{(\ell-1)/d} \equiv 1 \pmod{\ell}\right\}\right|} = \frac{\ell-1}{(\ell-1)/d} = d.$$

Therefore

$$|C_\ell| = \frac{(\ell^2-1)(\ell^2-\ell)}{d}.$$

The elements of D_ℓ come from the conjugacy classes $\alpha_{a,-a}$ with $-a^2 \in (\mathbb{F}_\ell^\times)^{k-1}$ and $\beta_{0,a}$ with $-\epsilon a^2 \in (\mathbb{F}_\ell^\times)^{k-1}$. Let g be the primitive root of $\mathbb{F}_\ell^\times$. We would like to find the cardinality of the sets

$$\{a \mid -a^2 \equiv w^{k-1} \pmod{\ell} \text{ for some } w \in \mathbb{F}_\ell^\times\} \tag{2}$$

and

$$\{a \mid -\epsilon a^2 \equiv w^{k-1} \pmod{\ell} \text{ for some } w \in \mathbb{F}_\ell^\times\}. \tag{3}$$

Write $a = g^r, -1 = g^{\frac{\ell-1}{2}}$ and $w = g^s$, where $0 \le r, s \le \ell - 1$. Then the cardinality of (2) is equal to the number of solutions r for which

$$\frac{\ell-1}{2} + 2r \equiv s(k-1) \pmod{\ell-1}, \tag{4}$$

where $0 \le s \le \ell - 1$. This congruence has a solution $\{r_0, s_0\}$ if and only if $2r_0 \equiv -\frac{\ell-1}{2} \pmod{d}$. Since $(2, d) = 1$, the last congruence has a unique solution in r_0. Hence the number of r's which are solutions of (4) is $\frac{\ell-1}{d}$. Note that if a is in the set (2), then so is $-a$ and that $\alpha_{a,-a} = \alpha_{-a,a}$. Hence

$$|\{a \mid -a^2 \equiv w^{k-1} \pmod{\ell} \text{ for some } w \in \mathbb{F}_\ell^\times\}| = \frac{\ell-1}{2d}.$$

Again writing $a = g^r, -\epsilon = g^{t_0}$ and $w = g^s$, where $0 \le r, s \le \ell - 1$ and solving the congruence

$$t_0 + 2r \equiv s(k-1) \pmod{\ell-1}$$

we show that the cardinality of the set (3) is $\frac{\ell-1}{2d}$. Hence

$$|D_\ell| = \frac{\ell-1}{2d}(\ell^2+\ell) + \frac{\ell-1}{2d}(\ell^2-\ell) = \frac{\ell^2(\ell-1)}{d}.$$

Finally, we calculate for $n \ge 1$, the cardinality of the sets

$$C_{\ell^n} := \{\gamma \in B_{\ell^n} \mid \gamma \pmod{\ell} \in C_\ell\}$$

and

$$D_{\ell^n} = \{\gamma \in C_{\ell^n} \mid \operatorname{tr} \gamma = 0\}.$$

Clearly, $|C_{\ell^n}| = \ell^{4(n-1)}|\mathrm{C}_\ell|$ and $|D_{\ell^n}| = \ell^{3(n-1)}|\mathrm{D}_\ell|$.

4. Proof of the theorem

Proof. Suppose that f is a normalized Hecke eigenform of weight k for $\Gamma_0(\mathrm{N})$ and δ is a large positive integer with the property that if $p|\delta$, then $p \gg 1$. It follows from the previous two sections that for such δ, we have

$$h(\delta) = \prod_{\ell^n || \delta} h(\ell^n) = \prod_{\ell^n || \delta} \frac{\ell^{3(n-1)}\ell}{\ell^{4(n-1)}(\ell^2-1)} = \prod_{\ell^n || \delta} \frac{\ell}{\ell^{n-1}(\ell^2-1)}. \tag{5}$$

Clearly when $\delta = \ell$ a prime, $h(\ell) \asymp \frac{1}{\ell}$ for sufficiently large ℓ. For a lower bound, note that

$$\begin{aligned}\sum_{\substack{p \le x \\ a(p) \neq 0}} d(a(p)) = \sum_{\substack{p \le x \\ a(p) \neq 0}} \sum_{\delta | a(p)} 1 &\ge \sum_{\substack{p \le x \\ a(p) \neq 0}} \sum_{\substack{\delta < x^{1/12} \\ a(p) \equiv 0 \, (\mathrm{mod}\ \delta)}} 1 \\ &\ge \sum_{\delta < x^{1/12}}{}^{*} \pi(x, \delta),\end{aligned}$$

where $\sum^*$ varies over all those natural numbers δ whose prime divisors are sufficiently large. Hence by Lemma 2, we have

$$\begin{aligned}\sum_{\substack{p \le x \\ a(p) \neq 0}} d(a(p)) &\ge \pi(x) \sum_{\delta < x^{1/12}}{}^{*} h(\delta) + O\left(x^{1/2} \sum_{\delta < x^{1/12}}{}^{*} \delta^3 \log \delta\right) + O(x^{5/6}) \\ &= \pi(x) \sum_{\substack{\delta < x^{1/12} \\ \ell | \delta \iff \ell \gg 1}} h(\delta) + O(x^{5/6} \log x) \gg x.\end{aligned}$$

For an upper bound, we can use Lemma 5 to get

$$\sum_{\substack{p \le x \\ a(p) \neq 0}} d(a(p)) \ll \sum_{\substack{p \le x \\ a(p) \neq 0}} \sum_{\substack{\delta | a(p) \\ \delta \le |a(p)|^{1/m}}} d(\delta)^{\frac{m \log m}{\log 2}}.$$

We choose m so that $m > 7k$. Write $c = \frac{m \log m}{\log 2}$. As $|a(p)| < 2p^{k/2}$, we have

$$\begin{aligned}\sum_{\substack{p \le x \\ a(p) \neq 0}} d(a(p)) &\ll \sum_{\substack{p \le x \\ a(p) \neq 0}} \sum_{\substack{\delta | a(p) \\ \delta < x^{1/12}}} d(\delta)^c \\ &= \sum_{\delta < x^{1/12}} d(\delta)^c \, \pi(x, \delta) \\ &= \sum_{\delta < x^{1/12}} d(\delta)^c \left\{ h(\delta)\pi(x) + O\left(\delta^3 x^{1/2} \log(\delta \mathrm{N} x)\right) + O(x^{3/4}) \right\}\end{aligned}$$

by using Lemma 2. Note that when δ has small prime divisors, the value of $h(\delta)$ is less than the value of the right hand side of (5). Hence for an upper bound we can use the right hand side of (5) for all values of δ.

Consider the Dirichlet series

$$\mathrm{F}(s) := \sum_{n\geq 1} \frac{d(n)^c h(n)}{n^s} = \zeta(s+1)^{2^c} g(s),$$

where $g(s)$ is analytic for $\Re(s) \geq 0$. Thus by Lemma 6, we have

$$\sum_{n\leq z} d(n)^c h(n) \leq z^u F(u),$$

for any real number $u > 0$. We choose $u = 1/\log z$ so that

$$\sum_{n\leq z} d(n)^c h(n) \ll F\left(\frac{1}{\log z}\right).$$

Since

$$|\zeta(s)| \leq \frac{1}{s-1} + L,$$

where L is an absolute constant, we see easily

$$\sum_{n\leq z} d(n)^c h(n) \ll (\log z)^{2^c}.$$

Again consider the Dirichlet series

$$\mathrm{G}(s) := \sum_{n\geq 1} \frac{d(n)^c}{n^s} = \zeta(s)^{2^c} g_1(s),$$

where $g_1(s)$ is analytic for $\Re(s) \geq 1$. Thus by Lemma 6, we have

$$\sum_{n\leq z} d(n)^c \leq z^u G(u),$$

for any real number $u > 1$. We choose $u = 1/\log z + 1$ so that

$$\sum_{n\leq z} d(n)^c \ll zG\left(\frac{1}{\log z} + 1\right)$$

and hence

$$\sum_{n\leq z} d(n)^c \ll z(\log z)^{2^c}.$$

This implies that

$$\sum_{\substack{p\leq x \\ a(p)\neq 0}} d(a(p)) \ll x(\log x)^{2^c-1} + O\left(x^{5/6}(\log x)^{2^c+1}\right) \ll x(\log x)^{2^c-1}.$$

This completes the proof of the theorem. $\square$

5. Concluding remarks

We hasten to remark that the full strength of the GRH is not essential if one only wants an estimate of the form $x(\log x)^A$ for some A. Indeed, if one assumes a quasi-GRH (that is, the assumption for any given $\epsilon > 0$, the Artin L-series have no zero in the region $\Re(s) > 1-\epsilon$), then one can deduce a result of the form

$$\sum_{\substack{p\le x,\\ a(p)\neq 0}} d(a(p)) \ll x(\log x)^A,$$

for some A depending on ϵ. This is not difficult to see. Indeed, a version of Lemma 1 with an estimate of the form $x^{1-\epsilon}$ can easily be deduced under such a hypothesis. In addition, one can choose m appropriately in Lemma 5 so as to ensure that the subsequent sums in the proof of the main theorem can be reasonably estimated. It is also evident that the lower bound can be deduced from a version of the Chebotarev density theorem derived from a quasi-GRH. We leave the details to the reader. All of this analysis suggests the following question. Is it reasonable to expect that there exist constants B and v such that we have an asymptotic formula of the type

$$\sum_{p\le x} d(a(p)) \ \sim\ Bx(\log x)^v$$

as $x \to \infty$? Perhaps $v = 0$.

Acknowledgments. The authors thank Kumar Murty and the referee for making some valuable suggestions on an earlier draft of this paper.

References

[1] Breuil, Christophe; Conrad, Brian; Diamond, Fred; Taylor, Richard. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *J. Amer. Math.* **14** (2001), no. 4, 843–939. MR1839918 (2002d:11058), Zbl 0982.11033, doi: 10.1090/S0894-0347-01-00370-8.

[2] Carayol, Henri. Sur les représentations l-adiques attachées aux formes modulaires de Hilbert. *C. R. Acad. Sci. Paris Sér. I Math.* **296** (1983), no. 15, 629–632. MR0705677 (85e:11039), Zbl 0537.10018, doi: 10.1215/S0012-7094-89-05937-1.

[3] Deligne, Pierre. Formes modulaires et représentations l-adiques. *Séminaire Bourbaki. 1968/69: Exposés 347–363*, Exp. No. 355, 139–172. Lecture Notes in Math., 175, *Springer, Berlin*, 1971. MR3077124, Zbl 0206.49901, doi: 10.1007/BFb0058810.

[4] Elkies, N. Supersingular primes of a given elliptic curve over a number field. Ph.D. Thesis. Harvard University, 1987.

[5] Elkies, Noam D. Distribution of supersingular primes. Journées Arithmétiques, 1989 (Luminy, 1989). *Astérisque* **198–200** (1991), 127–132. MR1144318 (93b:11070), Zbl 0754.14019.

[6] Erdös, P. On the sum $\sum_{k=1}^{x} d(f(k))$. *J. London Math. Soc.* **27** (1952), 7–15. MR0044565 (13,438f), Zbl 0046.04103.

[7] Friedlander, J. B.; Iwaniec, H. Divisor weighted sums. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov.* **322** (2005), Trudy po Teorii Chisel, 212-219, 255; translation in *J. Math. Sci. (N. Y.)* **137** (2006), no. 2, 4739–4743. MR2138460 (2006b:11116), Zbl 1088.11069, doi: 10.1007/s10958-006-0269-5.

[8] Fulton, William; Harris, Joe. Representation theory. A first course. Graduate Texts in Mathematics, 129. Readings in Mathematics. *Springer-Verlag, New York*, 1991. xvi+551 pp. ISBN: 0-387-97527-6; 0-387-97495-4. MR1153249 (93a:20069), Zbl 0744.22001.

[9] Lagarias, J. C.; Odlyzko, A. M. Effective versions of the Chebotarev density theorem. *Algebraic number fields: L-functions and Galois properties*, 409–464. *Academic Press, London*, 1977. MR0447191 (56:5506), Zbl 0362.12011.

[10] Luca, Florian; Pomerance, Carl. On the average number of divisors of the Euler function. *Publ. Math. Debrecen* **70** (2007), no. 1–2, 125–148. MR2288471 (2007k:11159), Zbl 1127.11065.

[11] Momose, Fumiyuki. On the ℓ-adic representations attached to modular forms. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **28** (1981), no. 1, 89–109. MR0617867 (84a:10025), Zbl 0482.10023.

[12] Murty, M. Ram; Murty, V. Kumar. Prime divisors of Fourier coefficients of modular forms. *Duke Math. J.* **51** (1984), no. 1, 57–76. MR0744288 (85j:11050), Zbl 0537.10026, doi: 10.1215/S0012-7094-84-05104-4.

[13] Murty, M. Ram; Murty, V. Kumar; Saradha, N. Modular forms and the Chebotarev density theorem. *Amer. J. Math.* **110** (1988), no. 2, 253–281. MR0935007 (89d:11036), Zbl 0644.10018, http://www.jstor.org/stable/2374502.

[14] Rankin, Robert A. G. H. Hardy as I knew him. *Number theory for the millennium, III (Urbana, IL, 2000)*, 191–203. *A K Peters, Natick, MA*, 2002. MR1956275 (2004a:01033), Zbl 1042.01013.

[15] Ribet, Kenneth A. On l-adic representations attached to modular forms. *Invent. Math.* **28** (1975), 245–275. MR0419358 (54:7379), Zbl 0302.10027.

[16] Ribet, Kenneth A. Galois representations attached to eigenforms with Nebentypus. *Modular functions of one variable, V*, 17–51. Lecture Notes in Mathermatics, 601, *Springer, Berlin*, 1977. MR0453647 (56:11907), Zbl 0363.10015, doi: 10.1007/BFb0063943.

[17] Ribet, Kenneth A. On l-adic representations attached to modular forms II. *Glasgow Math. J.* **27** (1985), 185–194. MR0819838 (88a:11041), Zbl 0596.10027, doi: 10.1017/S0017089500006170.

[18] Serre, Jean–Pierre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* **15** (1972), no. 4, 259–331. MR0387283 (52:8126), Zbl 0235.14012.

[19] Serre, Jean–Pierre Divisibilité de certaines fonctions arithmétiques. *Enseignement Math.* (2) **22** (1976), no. 3-4, 227–260. MR0434996 (55:7958), Zbl 0355.10021.

[20] Serre, Jean–Pierre Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sc. Publ. Math.* **54** (1981), 323–401. MR0644559 (83k:12011), Zbl 0496.12011, doi: 10.1007/BF02698692.

[21] Swinnerton–Dyer, H.P.F. On l-adic representations and congruences for coefficients of modular forms. *Modular functions of one variable, III*, 1-55. Lecture Notes in Mathematics, 350, *Springer, Berlin*, 1973. MR0406931 (53:10717a), Zbl 0267.10032, doi: 10.1007/978-3-540-37802-0_1.

[22] van der Corput, J.G. Une inégalité relative au nombre des diviseurs. *Nederl. Akad. Wetensch. Proc.* **42** (1939), 547–553. MR0000249 (1,41b), Zbl 0022.00804.

[23] Wiles, Andrew. Modular elliptic curves and Fermat's last theorem. *Ann. of Math.* (2) **141** (1995), 443–551. MR1333035 (96d:11071), Zbl 0823.11029, doi: 10.2307/2118559.

(Sanoli Gun) Institute for Mathematical Sciences, CIT Campus, Taramani, Chennai, 600 113, India
sanoli@imsc.res.in

(M. Ram Murty) Department of Mathematics, Queen's University, Kingston, Ontario, K7L 3N6, Canada.
murty@mast.queensu.ca

This paper is available via http://nyjm.albany.edu/j/2014/20-1.html.