Annals of Mathematics, **165** (2007), 593–635

An uncertainty principle for arithmetic sequences

By Andrew Granville and K. Soundararajan*

Abstract

Analytic number theorists usually seek to show that sequences which appear naturally in arithmetic are "well-distributed" in some appropriate sense. In various discrepancy problems, combinatorics researchers have analyzed limitations to equidistribution, as have Fourier analysts when working with the "uncertainty principle". In this article we find that these ideas have a natural setting in the analysis of distributions of sequences in analytic number theory, formulating a general principle, and giving several examples.

1. Introduction

In this paper we investigate the limitations to the equidistribution of interesting "arithmetic sequences" in arithmetic progressions and short intervals. Our discussions are motivated by a general result of K. F. Roth [15] on irregularities of distribution, and a particular result of H. Maier [11] which imposes restrictions on the equidistribution of primes.

If $\mathcal{A}$ is a subset of the integers in $[1, x]$ with $|\mathcal{A}| = \rho x$ then, as Roth proved, there exists $N \le x$ and an arithmetic progression $a \pmod q$ with $q \le \sqrt{x}$ such that

$$\Big| \sum_{\substack{n\in\mathcal{A},\ n\le N\\ n\equiv a \pmod q}} 1 - \frac{1}{q}\sum_{\substack{n\in\mathcal{A}\\ n\le N}} 1 \Big| \gg \sqrt{\rho(1-\rho)}\,x^{\frac{1}{4}}.$$

In other words, keeping away from sets of density 0 or 1, there must be an arithmetic progression in which the number of elements of $\mathcal{A}$ is a little different from the average. Following work of A. Sarkozy and J. Beck, J. Matousek and J. Spencer [12] showed that Roth's theorem is best possible, in that there is a

*Le premier auteur est partiellement soutenu par une bourse du Conseil de recherches en sciences naturelles et en génie du Canada. The second author is partially supported by the National Science Foundation.

set $\mathcal{A}$ containing $\sim x/2$ integers up to x, for which

$$|\#\{n \in \mathcal{A}:\ n \le N,\ n \equiv a \pmod q\} - \#\{n \in \mathcal{A}:\ n \le N\}/q| \ll x^{1/4}$$

for all q and a with $N \le x$.

Roth's result concerns arbitrary sequences of integers, as considered in combinatorial number theory and harmonic analysis. We are more interested here in sets of integers that arise in arithmetic, such as the primes. In [11] H. Maier developed an ingenious method to show that for any $A \ge 1$ there are arbitrarily large x such that the interval $(x, x + (\log x)^A)$ contains significantly more primes than usual (that is, $\ge (1+\delta_A)(\log x)^{A-1}$ primes for some $\delta_A > 0$) and also intervals $(x, x + (\log x)^A)$ containing significantly fewer primes than usual. Adapting his method J. Friedlander and A. Granville [3] showed that there are arithmetic progressions containing significantly more (and others with significantly fewer) primes than usual. A weak form of their result is that, for every $A \ge 1$ there exist large x and an arithmetic progression $a \pmod q$ with $(a, q) = 1$ and $q \le x/(\log x)^A$ such that

$$\left|\pi(x; q, a) - \frac{\pi(x)}{\phi(q)}\right| \gg_A \frac{\pi(x)}{\phi(q)}. \tag{1.1}$$

If we compare this to Roth's bound we note two differences: the discrepancy exhibited is much larger in (1.1) (being within a constant factor of the main term), but the modulus q is much closer to x (but not so close as to be trivial).

Recently A. Balog and T. Wooley [1] proved that the sequence of integers that may be written as the sum of two squares also exhibits "Maier type" irregularities in some intervals $(x, x+(\log x)^A)$ for any fixed, positive A. While previously Maier's results on primes had seemed inextricably linked to the mysteries of the primes, Balog and Wooley's example suggests that such results should be part of a general phenomenon. Indeed, we will provide here a general framework for such results on irregularities of distribution, which will include, among other examples, the sequence of primes and the sequence of sums of two squares. Our results may be viewed as an "uncertainty principle" which establishes that most arithmetic sequences of interest are either not-so-well distributed in longish arithmetic progressions, or are not-so-well distributed in both short intervals and short arithmetic progressions.

1a. *Examples.* We now highlight this phenomenom with several examples: For a given set of integers $\mathcal{A}$, let $\mathcal{A}(N)$ denote the number of elements of $\mathcal{A}$ which are $\le N$, and $\mathcal{A}(N; q, a)$ denote those that are $\le N$ and $\equiv a \pmod q$.

• We saw in Maier's theorem that the primes are not so well-distributed. We might ask whether there are subsets $\mathcal{A}$ of the primes up to x which are well-distributed. Fix $u \ge 1$. We show that for any x there exists $y \in (x/4, x)$ such that either

$$|\mathcal{A}(y)/y - \mathcal{A}(x)/x| \gg_u \mathcal{A}(x)/x \tag{1.2a}$$

(meaning that the subset is poorly distributed in short intervals), or there exists some arithmetic progression $a \pmod{\ell}$ with $(a,\ell)=1$ and $\ell \le x/(\log x)^u$, for which

$$\left|\mathcal{A}(y;\ell,a) - \frac{\mathcal{A}(y)}{\phi(\ell)}\right| \gg_u \frac{\mathcal{A}(x)}{\phi(\ell)}. \tag{1.2b}$$

In other words, we find "Maier type" irregularities in the distribution of *any subset of the primes.* (If we had chosen $\mathcal{A}$ to be the primes $\equiv 5 \pmod 7$ then this is of no interest when we take $a=1, \ell=7$. To avoid this minor technicality we can add "For a given finite set of "bad primes" $\mathcal{S}$, we can choose such an ℓ for which $(\ell,\mathcal{S})=1$". Here and henceforth $(\ell,\mathcal{S})=1$ means that $(\ell,p)=1$ for all $p\in\mathcal{S}$.)

• With probability 1 there are *no* "Maier type" irregularities in the distribution of randomly chosen subsets of the integers. Indeed such irregularities seem to depend on the subset having some arithmetic structure. So instead of taking subsets of all the integers, we need to take subsets of a set which already has some arithmetic structure. For example, define $\mathcal{S}_\varepsilon$ to be the set of integers n having no prime factors in the interval $[(\log n)^{1-\varepsilon}, \log n]$, so that $\mathcal{S}_\varepsilon(N) \sim (1-\varepsilon)N$. Notice that the primes are a subset of $\mathcal{S}_\varepsilon$. Our results imply that any subset $\mathcal{A}$ of $\mathcal{S}_\varepsilon$ is poorly distributed in that for any x there exists $y \in (x/4, x)$ such that either (1.2a) holds, or there exists some arithmetic progression $a \pmod{\ell}$ and $\ell \le x/(\log x)^u$ with $(a,\ell)=1$, for which a suitably modified (1.2b) holds (that is with $\phi(\ell)$ replaced by $\ell\prod_{p|\ell,\ (\log x)^{1-\varepsilon}<p<\log x}(1-1/p)$).

• Let K be an algebraic number field with $[K:\mathbb{Q}]>1$. Let R denote the ring of integers of K and let C be an ideal class from the class group of R. Take $\mathcal{A}$ to be the set of positive integers which are the norm of some (integral) ideal belonging to C. (In Balog and Wooley's example, $\mathcal{A}$ is the set of numbers of the form x^2+y^2, with C the class of principal ideals in $R=\mathbb{Z}[i]$.) From our work it follows that the set $\mathcal{A}$ is poorly distributed in arithmetic progressions; that is, a suitably modified version of (1.2b) holds. Moreover, if we replace R by any order in K then either (1.2a) holds or a suitably modified version of (1.2b) holds (and we expect that, with some effort, one can prove that the suitably modified (1.2b) holds).

• Let $\mathcal{B}$ be a given set of x integers and $\mathcal{P}$ be a given set of primes. Define $\mathcal{S}(\mathcal{B},\mathcal{P},z)$ to be the number of integers in $\mathcal{B}$ which do not have a prime factor $p\in\mathcal{P}$ with $p\le z$. Sieve theory is concerned with estimating $\mathcal{S}(\mathcal{B},\mathcal{P},z)$ under certain natural hypotheses for $\mathcal{B},\mathcal{P}$ and $u := \log x/\log z$. The fundamental lemma of sieve theory (see [7]) implies (for example when $\mathcal{B}$ is the set of integers

in an interval) that

$$\left|\mathcal{S}(\mathcal{B},\mathcal{P},z) - x\prod_{p\in\mathcal{P},p\le z}\left(1-\frac{1}{p}\right)\right| \ll \left(\frac{1+o(1)}{u\log u}\right)^u x\prod_{p\in\mathcal{P},p\le z}\left(1-\frac{1}{p}\right)$$

for $u < z^{1/2+o(1)}$. It is known that this result is essentially "best-possible" in that one can construct examples for which the bound is obtained (both as an upper and lower bound). However these bounds are obtained in quite special examples, and one might suspect that in many cases which one encounters, those bounds might be significantly sharpened. It turns out that these bounds cannot be improved for intervals $\mathcal{B}$, when $\mathcal{P}$ contains at least a positive proportion of the primes:

COROLLARY 1.1. *Suppose that $\mathcal{P}$ is a given set of primes for which $\#\{p\in\mathcal{P}:\ p\le y\}\gg\pi(y)$ for all $y\in(\sqrt{z},z]$. There exist constants $c>0$ such that for any $u\ll\sqrt{z}$ there exist intervals $I_\pm$ of length $\ge z^u$ for which*

$$\mathcal{S}(I_+,\mathcal{P},z)\ge\left\{1+\left(\tfrac{c}{u\log u}\right)^u\right\}|I_+|\prod_{p\in\mathcal{P},p\le z}\left(1-\tfrac{1}{p}\right)$$

and

$$\mathcal{S}(I_-,\mathcal{P},z)\le\left\{1-\left(\tfrac{c}{u\log u}\right)^u\right\}|I_-|\prod_{p\in\mathcal{P},p\le z}\left(1-\tfrac{1}{p}\right).$$

Moreover if $u\le(1-o(1))\log\log z/\log\log\log z$ then our intervals $I_\pm$ have length $\le z^{u+2}$.

• What about sieve questions in which the set of primes does not have positive lower density (in the set of primes)? If $\mathcal{P}$ contains too few primes then we should expect the sieve estimate to be very accurate; so we must insist on some lower bound: for instance that if $q=\prod_{p\in\mathcal{P}}p$ then

$$\sum_{p|q}\frac{\log p}{p}\ge 60\log\log\log q. \tag{1.3}$$

(Note that $\sum_{p|q}(\log p)/p\le(1+o(1))\log\log q$, the bound being attained when q is the product of the primes up to some large y.)

COROLLARY 1.2. *Let q be a large, square-free number, which satisfies* (1.3), *and define $z:=(\prod_{p|q}p^{1/p})^{c_1}$ for a certain constant $c_1>0$. There exists a constant $c_2>0$ such that if $\sqrt{z}\ge u\gg(\log\log q/\log z)^3$ then there exist intervals $I_\pm$ of length at least z^u such that*

$$\sum_{\substack{n\in I_+\\(n,q)=1}}1\ge\{1+1/u^{c_2u}\}\frac{\phi(q)}{q}|I_+|,\quad\text{and}\quad\sum_{\substack{n\in I_-\\(n,q)=1}}1\le\{1-1/u^{c_2u}\}\frac{\phi(q)}{q}|I_-|.$$

• The reduced residues $\pmod q$ are expected to be distributed much like random numbers chosen with probability $\phi(q)/q$. Indeed when $\phi(q)/q\to 0$

this follows from work of C. Hooley [10]; and of H. L. Montgomery and R. C. Vaughan [13] who showed that $\#\{n \in [m, m+h) : (n,q) = 1\}$ has Gaussian distribution with mean and variance equal to $h\phi(q)/q$, as m varies over the integers, provided h is suitably large. This suggests that $\#\{n \in [m, m+h) : (n,q) = 1\}$ should be $\{1 + o(1)\}(h\phi(q)/q)$ provided $h \geq \log^2 q$; however, by Corollary 1.2, this is not true for $h = \log^A q$ for any given $A > 0$, provided that $\sum_{p|q}(\log p)/p \gg \log\log q$ (a condition satisfied by many highly composite q).

In Section 6 we shall give further new examples of sequences to which our results apply.

1b. *General results.* Our main result (Theorem 3.1) is too technical to introduce at this stage. Instead we motivate our setup (postponing complete details to §2) and explain some consequences.

Let $\mathcal{A}$ denote a sequence $a(n)$ of nonnegative real numbers. We are interested in determining whether the $a(n)$ are well-distributed in short intervals and in arithmetic progressions, so let $\mathcal{A}(x) = \sum_{n \leq x} a(n)$ (so if $\mathcal{A}$ is a set of positive integers then $a(n)$ is its indicator function). Thinking of $\mathcal{A}(x)/x$ as the average value of $a(n)$, we may expect that if $\mathcal{A}$ is well-distributed in short intervals then

$$\mathcal{A}(x+y) - \mathcal{A}(x) \approx y\frac{\mathcal{A}(x)}{x}, \tag{1.4}$$

for suitable y.

To understand the distribution of $\mathcal{A}$ in arithmetic progressions, we begin with those n divisible by d. We will suppose that the proportion of $\mathcal{A}$ which is divisible by d is approximately $h(d)/d$ where $h(.)$ is a nonnegative multiplicative function; in other words,

$$\mathcal{A}_d(x) := \sum_{\substack{n \leq x \\ d|n}} a(n) \approx \frac{h(d)}{d}\mathcal{A}(x), \tag{1.5}$$

for each d (or perhaps when $(d, \mathcal{S}) = 1$, where $\mathcal{S}$ is a finite set of 'bad' primes). The reason for taking $h(d)$ to be a multiplicative function is that for most sequences that appear in arithmetic one expects that the criterion of being divisible by an integer d_1 should be "independent" of the criterion of being divisible by an integer d_2 coprime to d_1.

If the asymptotic behavior of $\mathcal{A}(x; q, a)$ for $(q, \mathcal{S}) = 1$ depends only on the g.c.d. of a and q then, by (1.5), we arrive at the prediction that, for $(q, \mathcal{S}) = 1$,

$$\mathcal{A}(x; q, a) \approx \frac{f_q(a)}{q\gamma_q}\mathcal{A}(x), \tag{1.6}$$

where $\gamma_q = \prod_{p|q}((p-1)/(p-h(p)))$ and $f_q(a)$ is a certain nonnegative multiplicative function of a for which $f_q(a) = f_q((a,q))$ (thus $f_q(a)$ is periodic (mod q)). In Section 2 we shall give an explicit description of f_q in terms of h.

In the spirit of Roth's theorem we ask how good is the approximation (1.6)? And, in the spirit of Maier's theorem we ask how good is the approximation (1.4)?

Example 1. We take $a(n) = 1$ for all n. We may take $\mathcal{S} = \emptyset$ and $h(n) = 1$ for all n. Then $f_q(a) = 1$ for all q and all a, and $\gamma_q = 1$. Clearly both (1.6) and (1.4) are good approximations with an error of at most 1.

Example 2. We take $a(n) = 1$ if n is prime and $a(n) = 0$ otherwise. Then we may take $\mathcal{S} = \emptyset$ and $h(n) = 1$ if $n = 1$ and $h(n) = 0$ if $n > 1$. Further $f_q(a) = 1$ if $(a, q) = 1$ and $f_q(a) = 0$ otherwise, and $\gamma_q = \phi(q)/q$. The approximation (1.6) is then the prime number theorem for arithmetic progressions for small $q \le (\log x)^A$. Friedlander and Granville's result (1.1) sets limitations to (1.6), and Maier's result sets limitations to (1.4).

Example 3. Take $a(n) = 1$ if n is the sum of two squares and $a(n) = 0$ otherwise. Here we take $\mathcal{S} = \{2\}$, and for odd prime powers p^k we have $h(p^k) = 1$ if $p^k \equiv 1 \pmod 4$ and $h(p^k) = 1/p$ otherwise. Balog and Wooley's result places restrictions on the validity of (1.4).

COROLLARY 1.3. *Let $\mathcal{A}$, $\mathcal{S}$, h, f_q and γ_q be as above. Let x be sufficiently large and in particular suppose that $\mathcal{S} \subset [1, \log\log x]$. Suppose that $0 \le h(n) \le 1$ for all n. Suppose that*

$$\sum_{p \le \log x} \frac{1 - h(p)}{p} \log p \ge \alpha \log\log x, \tag{1.7}$$

for some $\alpha \ge 60 \log\log\log x / \log\log x$ and set $\eta = \min(\alpha/3, 1/100)$. Then for each $5/\eta^2 \le u \le \eta(\log x)^{\eta/2}$ there exists $y \in (x/4, x)$ and an arithmetic progression $a \pmod \ell$ with $\ell \le x/(\log x)^u$ and $(\ell, \mathcal{S}) = 1$ such that

$$\Big|\mathcal{A}(y; \ell, a) - \frac{f_\ell(a)}{\ell\gamma_\ell} y \frac{\mathcal{A}(x)}{x}\Big| \gg \exp\Big(-\frac{u}{\eta}(1 + 25\eta)\log(2u/\eta^3)\Big) \frac{\mathcal{A}(x)}{\phi(\ell)}.$$

Remarks. Since the corollary appears quite technical, some explanation is in order.

• The condition $0 \le h(n) \le 1$ is not as restrictive as it might appear. We will show in Proposition 2.1 if there are many primes with $h(p) > 1$ then it is quite easy to construct large discrepancies for the sequence $\mathcal{A}$.

• The condition (1.7) ensures that $h(p)$ is not always close to 1; this is essential in order to eliminate the very well behaved Example 1.

• The conclusion of the corollary may be weakly (but perhaps more transparently) written as

$$\Big|\mathcal{A}(y; \ell, a) - \frac{f_\ell(a)}{\ell\gamma_\ell} y \frac{\mathcal{A}(x)}{x}\Big| \gg_{\alpha,u} \frac{\mathcal{A}(x)}{\phi(\ell)}.$$

• The lower bound given is a multiple of $\mathcal{A}(x)/\phi(\ell)$, rather than of the main term $(f_\ell(a)/\ell\gamma_\ell)(y\mathcal{A}(x)/x)$. The main reason for this is that $f_\ell(a)$ may well be 0, in which case such a bound would have no content. In fact, since $(y/x) < 1$ and $\phi(\ell) \le \ell\gamma_\ell$, so the function used is larger and more meaningful than the main term itself.

• It might appear more natural to compare $\mathcal{A}(y;\ell,a)$ with $(f_\ell(a)/\ell\gamma_\ell)\mathcal{A}(y)$. In most examples that we consider the average $\mathcal{A}(x)/x$ "varies slowly" with x, so we expect little difference between $\mathcal{A}(y)$ and $y\mathcal{A}(x)/x$ (we have $\sim 1/\log x$ in Example 2, and $\sim C/\sqrt{\log x}$ in Example 3 above). If there is a substantial difference between $\mathcal{A}(y)$ and $y\mathcal{A}(x)/x$ then this already indicates large scale fluctuations in the distribution of $\mathcal{A}$.

Corollary 1.3 gives a Roth-type result for general arithmetic sequences which do not look like the set of all natural numbers. We will deduce it in Section 2 from the stronger, but more technical, Theorem 2.4 below. Clearly Corollary 1.3 applies to the sequences of primes (with $\alpha = 1 + o(1)$) and sums of two squares (with $\alpha = 1/2 + o(1)$), two results already known. Surprisingly it applies also to any subset of the primes:

Example 4. Let $\mathcal{A}$ be any subset of the primes. Then for any fixed $u \ge 1$ and sufficiently large x there exists $\ell \le x/(\log x)^u$ such that, for some $y \in (x/4, x)$ and some arithmetic progression $a \pmod{\ell}$ with $(a,\ell) = 1$, we have

$$\Big|\mathcal{A}(y;\ell,a) - \frac{1}{\phi(\ell)}\frac{y\mathcal{A}(x)}{x}\Big| \gg_u \frac{\mathcal{A}(x)}{\phi(\ell)}.$$

This implies the first result of Section 1a. A similar result holds for any subset of the numbers that are sums of two squares.

Example 5. Let $\mathcal{A}$ be any subset of those integers $\le x$ having no prime factor in the interval $[(\log x)^{1-\varepsilon}, \log x]$. We can apply Corollary 1.3 since $\alpha \ge \varepsilon + o(1)$, and then easily deduce the second result of Section 1a.

Our next result gives an "uncertainty principle" implying that we either have poor distribution in long arithmetic progressions, or in short intervals.

Corollary 1.4. *Let $\mathcal{A}$, $\mathcal{S}$, h, f_q and γ_q be as above. Suppose that $0 \le h(n) \le 1$ for all n. Suppose that* (1.7) *holds for some $\alpha \ge 60 \log\log\log x/\log\log x$ and set $\eta = \min(\alpha/3, 1/100)$. Then for each $5/\eta^2 \le u \le \eta(\log x)^{\eta/2}$ at least one of the following two assertions holds*:

(i) *There exists an interval $(v, v+y) \subset (x/4, x)$ with $y \ge (\log x)^u$ such that*

$$\Big|\mathcal{A}(v+y) - \mathcal{A}(v) - y\frac{\mathcal{A}(x)}{x}\Big| \gg \exp\Big(-\frac{u}{\eta}(1+25\eta)\log(2u/\eta^3)\Big)y\frac{\mathcal{A}(x)}{x}.$$

(ii) *There exists* $y \in (x/4, x)$ *and an arithmetic progression* $a \pmod q$ *with* $(q, \mathcal{S}) = 1$ *and* $q \le \exp(2(\log x)^{1-\eta})$ *such that*

$$\Big|\mathcal{A}(y; q, a) - \frac{f_q(a)}{q\gamma_q} y \frac{\mathcal{A}(x)}{x}\Big| \gg \exp\Big(-\frac{u}{\eta}(1+25\eta)\log(2u/\eta^3)\Big)\frac{\mathcal{A}(x)}{\phi(q)}.$$

Corollary 1.4 is our general version of Maier's result; it is a weak form of the more technical Theorem 2.5. Again condition (1.7) is invoked to keep away from Example 1. Note that we are only able to conclude a dichotomy: either there is a large interval $(v, v+y) \subset (x/4, x)$ with $y \ge (\log x)^u$ where the density of $\mathcal{A}$ is altered, or there is an arithmetic progression to a very small modulus ($q \le x^\varepsilon$) where the distribution differs from the expected. This is unavoidable in general, and our "uncertainty principle" is aptly named, for we can construct sequences (see §6a, Example 6) which are well distributed in short intervals (and then by Corollary 1.4 such a sequence will exhibit fluctuations in arithmetic progressions). In Maier's original result the sequence was easily proved to be well-distributed in these long arithmetic progressions (and so exhibited fluctuations in short intervals, by Corollary 1.4).

Our proofs develop Maier's "matrix method" of playing off arithmetic progressions against short intervals or other arithmetic progressions (see §2). In the earlier work on primes and sums of two squares, the problem then reduced to showing oscillations in certain sifting functions arising from the theory of the half dimensional (for sums of two squares) and linear (for primes) sieves. In our case the problem boils down to proving oscillations in the mean-value of the more general class of multiplicative functions satisfying $0 \le f(n) \le 1$ for all n (see Theorem 3.1). Along with our general formalism, this forms the main new ingredient of our paper and is partly motivated by our previous work [6] on multiplicative functions and integral equations. In Section 7 we present a simple analogue of such oscillation results for a wide class of integral equations which has the flavor of a classical "uncertainty principle" from Fourier analysis.

This broader framework has allowed us to improve the uniformity of the earlier result for primes, and to obtain perhaps best possible results in this context.

THEOREM 1.5. *Let* x *be large and suppose*

$$\log x \le y \le \exp(\beta\sqrt{\log x}/2\sqrt{\log\log x}),$$

for a certain absolute constant $\beta > 0$. *Define*

$$\Delta(x, y) = (\vartheta(x+y) - \vartheta(x) - y)/y,$$

where $\vartheta(x) = \sum_{p \le x} \log p$. *There exist numbers* $x_\pm$ *in* $(x, 2x)$ *such that*

$$\Delta(x_+, y) \ge y^{-\delta(x,y)} \qquad \textit{and} \qquad \Delta(x_-, y) \le -y^{-\delta(x,y)},$$

where

$$\delta(x,y) = \frac{1}{\log\log x}\Big(\log\Big(\frac{\log y}{\log\log x}\Big) + \log\log\Big(\frac{\log y}{\log\log x}\Big) + O(1)\Big).$$

These bounds are $\gg 1$ if $y = (\log x)^{O(1)}$. If $y = \exp((\log x)^\tau)$ for $0 < \tau < 1/2$ then these bounds are $\gg y^{-\tau(1+o(1))}$. Thus we note that the asymptotic, suggested by probability considerations,

$$\vartheta(x+y) - \vartheta(x) = y + O(y^{\frac{1}{2}+\varepsilon}),$$

fails sometimes for $y \le \exp((\log x)^{\frac{1}{2}-\varepsilon})$. A. Hildebrand and Maier [14] had previously shown such a result for $y \le \exp((\log x)^{\frac{1}{3}-\varepsilon})$ (more precisely they obtained a bound $\gg y^{-(1+o(1))\tau/(1-\tau)}$ in the range $0 < \tau < 1/3$), and were able to obtain our result assuming the validity of the Generalized Riemann Hypothesis. We have also been able to extend the uniformity with which Friedlander and Granville's result (1.1) holds, obtaining results which previously Friedlander, Granville, Hildebrand and Maier [4] established conditionally on the Generalized Riemann Hypothesis. We will describe these in Section 5.

This paper is structured as follows: In Section 2 we describe the framework in more detail, and show how Maier's method reduces our problems to exhibiting oscillations in the mean-values of multiplicative functions. This is investigated in Section 3 which contains the main new technical results of the paper. From these results we quickly obtain in Section 4 our main general results on irregularities of distribution. In Section 5 we study in detail irregularities in the distribution of primes. Our general framework allows us to substitute a zero-density result of P. X. Gallagher where previously the Generalized Riemann Hypothesis was required. In Section 6 we give more examples of sequences covered by our methods. Finally in Section 7 we discuss the analogy between integral equations and mean-values of multiplicative functions, showing that the oscillation theorems of Section 3 may be viewed as an "uncertainty principle" for solutions to integral equations.

2. The framework

Recall from the introduction that $a(n) \ge 0$ and that $\mathcal{A}(x) = \sum_{n\le x} a(n)$. Recall that $\mathcal{S}$ is a finite set of 'bad' primes, and that h denotes a nonnegative multiplicative function that we shall think of as providing an approximation

$$\mathcal{A}_d(x) := \sum_{\substack{n\le x\\ d|n}} a(n) \approx \frac{h(d)}{d}\mathcal{A}(x), \tag{2.1}$$

for each $(d,\mathcal{S}) = 1$. Roughly speaking, we think of $h(d)/d$ as being the "probability" of being divisible by d. The condition that h is multiplicative means

that the "event" of being divisible by d_1 is independent of the "event" of being divisible by d_2, for coprime integers d_1 and d_2. We may assume that $h(p^k) < p^k$ for all prime powers p^k without any significant loss of generality. As we shall see shortly we may also assume that $h(p^k) \le 1$ without losing interesting examples. Let

$$\mathcal{A}(x;q,a) = \sum_{\substack{n\le x\\ n\equiv a \pmod q}} a(n).$$

We hypothesize that, for $(q,\mathcal{S})=1$, the asymptotics of $\mathcal{A}(x;q,a)$ depends only on the greatest common divisor of a and q. Our aim is to investigate the limitations of such a model.

First let us describe what (2.1) and our hypothesis predict for the asymptotics of $\mathcal{A}(x;q,a)$. Writing $(q,a)=m$, since $|\{b \pmod q : (b,q)=m\}| = \varphi(q/m)$, from our hypothesis on $\mathcal{A}(x;q,a)$ depending only on (q,a) we would guess that

$$\begin{aligned}\mathcal{A}(x;q,a) \approx \frac{1}{\varphi(q/m)} \sum_{\substack{n\le x\\ (q,n)=m}} a(n) &= \frac{1}{\varphi(q/m)} \sum_{\substack{n\le x\\ m|n}} a(n) \sum_{\substack{d|\frac{q}{m}\\ d|\frac{n}{m}}} \mu(d)\\ &= \frac{1}{\varphi(q/m)} \sum_{d|\frac{q}{m}} \mu(d)\mathcal{A}_{dm}(x).\end{aligned}$$

Using now (2.1) we would guess that

$$\mathcal{A}(x;q,a) \approx \mathcal{A}(x)\frac{1}{\varphi(q/m)} \sum_{d|\frac{q}{m}} \mu(d)\frac{h(dm)}{dm} =: \frac{f_q(a)}{q\gamma_q}\mathcal{A}(x), \tag{2.2}$$

where

$$\gamma_q = \prod_{p|q}\Big(\frac{1-h(p)/p}{1-1/p}\Big)^{-1} = \prod_p \Big(1-\frac{1}{p}\Big)\Big(1+\frac{f_q(p)}{p}+\frac{f_q(p^2)}{p^2}+\dots\Big), \tag{2.3}$$

and $f_q(a)$ is a suitable multiplicative function with $f_q(a) = f_q((a,q))$ so that it is periodic with period q, which we now define. Evidently $f_q(p^k)=1$ if $p \nmid q$. If p divides q, indeed if p^e is the highest power of p dividing q then

$$f_q(p^k) := \begin{cases} \Big(h(p^k) - \frac{h(p^{k+1})}{p}\Big)\Big(1-\frac{h(p)}{p}\Big)^{-1} & \text{if } k<e\\ h(p^e)\Big(1-\frac{1}{p}\Big)\Big(1-\frac{h(p)}{p}\Big)^{-1} & \text{if } k\ge e.\end{cases}$$

Note that if q is squarefree and $h(p)\le 1$ then $f_q(p^k)\le 1$ for all prime powers p^k.

We are interested in understanding the limitations to the model (2.2). We begin with a simple observation that allows us to restrict attention to the case $0\le h(n)\le 1$ for all n.

PROPOSITION 2.1. *Suppose that $q \le x$ is an integer for which $h(q) > 9$. Then either*

$$\Big|\mathcal{A}(x;q,0) - \frac{f_q(0)}{q\gamma_q}\mathcal{A}(x)\Big| \ge \frac{1}{2}\frac{f_q(0)}{q\gamma_q}\mathcal{A}(x)$$

or, for every prime ℓ in the range $x \ge \ell \ge 3(x+2q)/h(q)$ which does not divide q, there is an arithmetic progression $b \pmod{\ell}$ such that

$$\Big|\mathcal{A}(x;\ell,b) - \frac{f_\ell(b)}{\ell\gamma_\ell}\mathcal{A}(x)\Big| \ge \frac{1}{2}\frac{f_\ell(b)}{\ell\gamma_\ell}\mathcal{A}(x).$$

The first criterion is equivalent to $|\mathcal{A}_q(x) - (h(q)/q)\mathcal{A}(x)| \ge \frac{1}{2}(h(q)/q)\mathcal{A}(x)$, since $f_q(0)/q\gamma_q = f_q(q)/q\gamma_q = h(q)/q$.

Proof. If the first option fails then

$$\sum_{n\le x/q}\mathcal{A}(x;\ell,nq) \ge \sum_{n\le x/q} a(nq) = \mathcal{A}(x;q,0) \ge \frac{1}{2}\frac{f_q(0)}{q\gamma_q}\mathcal{A}(x) = \frac{h(q)}{2q}\mathcal{A}(x).$$

On the other hand, if prime $\ell \nmid q$ then $f_\ell(nq) = 1$ if $\ell \nmid n$, and $f_\ell(nq) = h(\ell)\gamma_\ell$ if $\ell | n$. Therefore for any N,

$$\begin{aligned}\sum_{n\le N}\frac{f_\ell(nq)}{\ell\gamma_\ell} &= \sum_{\substack{n\le N\\ l\nmid n}}\frac{1}{\ell\gamma_\ell} + \sum_{\substack{n\le N\\ l|n}}\frac{h(\ell)}{\ell}\\ &\le \frac{1}{\ell\gamma_\ell}\Big(N - \frac{N}{\ell} + 1\Big) + \frac{h(\ell)}{\ell}\frac{N}{\ell} \le \frac{N+2}{\ell}.\end{aligned}$$

Combining this (taking $N = x/q$) with the previous display yields

$$\sum_{n\le x/q}\mathcal{A}(x;\ell,nq) \ge \frac{h(q)}{2q}\mathcal{A}(x) \ge \frac{3(x+2q)}{2q\ell}\mathcal{A}(x) \ge \frac{3}{2}\sum_{n\le x/q}\frac{f_\ell(nq)}{\ell\gamma_\ell}\mathcal{A}(x),$$

which implies the proposition with $b = nq$ for some $n \le x/q$.

We typically apply this theorem with $h(q) > \log^A x$ for some large A. This is easily organized if, say, $h(p) \ge 1+\eta$ for $\ge \eta z/\log z$ primes $p \in (z/2, z)$ where $z \le \log x$, and by letting q be the product of $[\eta z/\log z]$ of these primes so that $q = e^{\eta z(1+o(1))}$. We can select any ℓ in the range $x \ge \ell \ge x/\exp((\eta^2/2)z/\log z)$.

Proposition 2.1 allows us to handle sequences for which $h(p)$ is significantly larger than 1 for many primes. Therefore we will, from now on, restrict ourselves to the case when $0 \le h(n) \le 1$ for all n. Suppose that $(q,\mathcal{S}) = 1$ and define $\Delta_q = \Delta_q(x)$ by

$$\Delta_q(x) := \max_{x/4\le y\le x}\ \max_{a \pmod q}\Big|\mathcal{A}(y;q,a) - \frac{f_q(a)}{q\gamma_q}\frac{y}{x}\mathcal{A}(x)\Big| \Big/ \frac{\mathcal{A}(x)}{\phi(q)}. \tag{2.4}$$

In view of (2.2) it seems more natural to consider $|\mathcal{A}(y;q,a) - f_q(a)/(q\gamma_q)\mathcal{A}(y)|$ instead of (2.4) above. However (2.4) seems to be the most convenient way to

formulate our results, and should be thought of as incorporating a hypothesis that $\mathcal{A}(y)/y$ is very close to $\mathcal{A}(x)/x$ when $x/4 \le y \le x$. Formally we say that $\mathcal{A}(x)/x$ is slowly varying: a typical case is when $\mathcal{A}(x)/x$ behaves like a power of $\log x$, a feature seen in the motivating examples of $\mathcal{A}$ being the set of primes, or sums of two squares. With these preliminaries in place we can now formulate our main principle.

PROPOSITION 2.2. *Let x be large and let $\mathcal{A}$, $\mathcal{S}$ h, f_q and Δ_q be as above. Let $q \le \sqrt{x} \le \ell \le x/4$ be positive coprime integers with $(q, \mathcal{S}) = (\ell, \mathcal{S}) = 1$. Then*

$$\frac{q}{\phi(q)}\Delta_q(x) + \frac{\ell}{\phi(\ell)}\Delta_\ell(x) + x^{-\frac{1}{8}} \gg \Big|\frac{1}{[x/2\ell]}\sum_{s\le x/(2\ell)}\frac{f_q(s)}{\gamma_q} - 1\Big|.$$

Proof. Let $R := [x/(4q)] \ge \sqrt{x}/5$ and $S := [x/(2\ell)] \le \sqrt{x}/2$. We sum the values of $a(n)$ as n varies over the integers in the following $R \times S$ "Maier matrix."

$$\begin{array}{|cccc|}
\hline
(R+1)q+\ell & (R+1)q+2\ell & \cdots & (R+1)q+S\ell \\
(R+2)q+\ell & (R+2)q+2\ell & \cdots & (R+2)q+S\ell \\
(R+3)q+\ell & \cdot & \cdot & \vdots \\
(R+4)q+\ell & \vdots & \boxed{\begin{array}{l}(r,s)^{\text{th}}\text{ entry}:\\ (R+r)q+s\ell\end{array}} & \vdots \\
\vdots & \vdots & \cdot & \vdots \\
2Rq+\ell & \cdots & \cdots & 2Rq+S\ell \\
\hline
\end{array}$$

We sum the values of $a(n)$ in two ways: first row by row, and second, column by column. Note that the n appearing in our "matrix" all lie between $x/4$ and x.

The rth row contributes $\mathcal{A}((R+r)q+\ell S; \ell, (R+r)q) - \mathcal{A}((R+r)q; \ell, (R+r)q)$. Using (2.4), and noting that $f_\ell((R+r)q) = f_\ell(R+r)$ as $(\ell, q) = 1$, we have

$$\frac{f_\ell(R+r)}{\ell\gamma_\ell}\frac{\ell S}{x}\mathcal{A}(x) + O\Big(\frac{\Delta_\ell}{\phi(\ell)}\mathcal{A}(x)\Big).$$

Summing this over all the rows we see that the sum of a_n with n ranging over the Maier matrix above equals

$$\frac{\ell S}{x}\mathcal{A}(x)\sum_{r=R+1}^{2R}\frac{f_\ell(r)}{\ell\gamma_\ell} + O\Big(\frac{\Delta_\ell}{\phi(\ell)}\mathcal{A}(x)R\Big). \tag{2.5a}$$

The contribution of column s is $\mathcal{A}(2Rq+\ell s;q,\ell s)-\mathcal{A}(Rq+\ell s;q,\ell s)$. By (2.4), and since $f_q(\ell s)=f_q(s)$ as $(\ell,q)=1$, we see that this is

$$\frac{f_q(s)}{q\gamma_q}\frac{Rq}{x}\mathcal{A}(x)+O\Big(\frac{\Delta_q}{\phi(q)}\mathcal{A}(x)\Big).$$

Summing this over all the columns we see that the Maier matrix sum is

$$\frac{Rq}{x}\mathcal{A}(x)\sum_{s=1}^{S}\frac{f_q(s)}{q\gamma_q}+O\Big(\frac{\Delta_q}{\phi(q)}\mathcal{A}(x)S\Big). \tag{2.5b}$$

Comparing (2.5a) and (2.5b) we deduce that

$$\frac{1}{S\gamma_q}\sum_{s=1}^{S}f_q(s)+O\Big(\frac{q\Delta_q}{\phi(q)}\Big)=\frac{1}{R\gamma_\ell}\sum_{r=R+1}^{2R}f_\ell(r)+O\Big(\frac{\ell\Delta_\ell}{\phi(\ell)}\Big). \tag{2.6}$$

Write $f_\ell(r)=\sum_{d|r}g_\ell(d)$ for a multiplicative function g_ℓ. Note that $g_\ell(p^k)=0$ if $p\nmid\ell$. We also check easily that $|g_\ell(p^k)|\le(p+1)/(p-1)$ for primes $p|\ell$, and note that $\gamma_\ell=\sum_{d=1}^{\infty}g_\ell(d)/d$. Thus

$$\begin{aligned}\frac{1}{R\gamma_\ell}\sum_{r=R+1}^{2R}f_\ell(r)&=\frac{1}{R\gamma_\ell}\sum_{d\le 2R}g_\ell(d)\Big(\frac{R}{d}+O(1)\Big)\\&=1+O\Big(\frac{1}{\gamma_\ell}\sum_{d>2R}\frac{|g_\ell(d)|}{d}+\frac{1}{R\gamma_\ell}\sum_{d\le 2R}|g_\ell(d)|\Big).\end{aligned}$$

We see easily that the error terms above are bounded by

$$\ll\frac{1}{R^{\frac13}\gamma_\ell}\sum_{d=1}^{\infty}\frac{|g_\ell(d)|}{d^{\frac23}}\ll\frac{1}{R^{\frac13}}\prod_{p|\ell}\Big(1+O\Big(\frac{1}{p^{\frac23}}\Big)\Big)\ll\frac{1}{R^{\frac14}},$$

since $\ell\le x$, and $R\gg\sqrt{x}$. We conclude that

$$\frac{1}{R\gamma_\ell}\sum_{r=R+1}^{2R}f_\ell(r)=1+O(R^{-\frac14}).$$

Combining this with (2.6) we obtain the proposition. □

In Proposition 2.2 we compared the distribution of $\mathcal{A}$ in two arithmetic progressions. We may also compare the distribution of $\mathcal{A}$ in an arithmetic progression versus the distribution in short intervals. Define $\tilde\Delta(y)=\tilde\Delta(y,x)$ by

$$\tilde\Delta(y,x):=\max_{(v,v+y)\subset(x/4,x)}\Big|\mathcal{A}(v+y)-\mathcal{A}(v)-y\frac{\mathcal{A}(x)}{x}\Big|\Big/\,y\frac{\mathcal{A}(x)}{x}. \tag{2.7}$$

PROPOSITION 2.3. *Let x be large and let $\mathcal{A}$, $\mathcal{S}$, h, f_q, Δ_q and $\tilde{\Delta}$ be as above. Let $q \le \sqrt{x}$ with $(q, \mathcal{S}) = 1$ and let $y \le x/4$ be positive integers. Then*

$$\frac{q}{\phi(q)}\Delta_q(x) + \tilde{\Delta}(x, y) \gg \Big|\frac{1}{\gamma_q y}\sum_{s \le y} f_q(s) - 1\Big|.$$

Proof. The argument is similar to the proof of Proposition 2.2, starting with an $R \times y$ "Maier matrix" (again $R = [x/(4q)]$) whose $(r, s)^{\text{th}}$ entry is $(R + r)q + s$. We omit the details.

We are finally ready to state our main general theorems which will be proved in Section 4.

THEOREM 2.4. *Let x be large, and in particular suppose that $\mathcal{S} \subset [1, \log\log x]$. Let $1/100 > \eta \ge 20 \log\log\log x/\log\log x$ and suppose that $(\log x)^\eta \le z \le (\log x)/3$ is such that*

$$\sum_{z^{1-\eta} \le p \le z} \frac{1 - h(p)}{p} \ge \eta \log((1 - \eta)^{-1}).$$

Then for all $5/\eta^2 \le u \le \sqrt{z}$

$$\max_{\substack{\ell \le x/z^u \\ (\ell, \mathcal{S}) = 1}} \Delta_\ell \gg \exp\left(-u(1 + 25\eta)\log(2u/\eta^2)\right).$$

Note that $\sum_{z^{1-\eta} \le p \le z} 1/p \sim \log((1 - \eta)^{-1})$. There is an analogous result for short intervals.

THEOREM 2.5. *Let x be large, and in particular suppose that $\mathcal{S} \subset [1, \log\log x]$. Let $1/100 \ge \eta \ge 20 \log\log\log x/\log\log x$ and suppose that $(\log x)^\eta \le z \le (\log x)/3$ is such that*

$$\sum_{z^{1-\eta} \le p \le z} \frac{1 - h(p)}{p} \ge \eta \log((1 - \eta)^{-1}).$$

Then for each $5/\eta^2 \le u \le \sqrt{z}$ at least one of the following statements is true:

(i) *For $q \le e^{2z}$ which is composed only of primes in $[z^{1-\eta}, z]$ (and so with $(q, \mathcal{S}) = 1$) and such that $\sum_{p|q}(1 - h(p))/p \ge \eta^2$, there is*

$$\Delta_q \gg \exp(-u(1 + 25\eta)\log(2u/\eta^2)).$$

(ii) *There exists $y \ge z^u$ with $\tilde{\Delta}(y) \gg \exp(-u(1 + 25\eta)\log(2u/\eta^2))$.*

Deduction of Corollary 1.3. We see readily that there exists $(\log x)^\eta \le z \le (\log x)/3$ satisfying the hypothesis of Theorem 2.4. Applying Theorem 2.4 (with u/η there instead of u) we find that there exists $\ell \le x/z^{u/\eta} \le x/(\log x)^u$

with $(\ell, \mathcal{S}) = 1$ and $\Delta_\ell \gg \exp(-(u/\eta)(1+25\eta)\log(2u/\eta^3))$. The corollary follows easily.

Deduction of Corollary 1.4. We may find $(\log x)^\eta \le z \le (\log x)^{1-\eta}$ satisfying the hypothesis of Theorem 2.5. The corollary follows easily by applyication of Theorem 2.5 with u/η there in place of u.

3. Oscillations in mean-values of multiplicative functions

3a. *Large oscillations.* Throughout this section we shall assume that z is large, and that q is an integer all of whose prime factors are $\le z$. Let $f_q(n)$ be a multiplicative function with $f_q(p^k) = 1$ for all $p \nmid q$, and $0 \le f_q(n) \le 1$ for all n. Note that $f_q(n) = f_q((n,q))$ is periodic $\pmod q$. Define

$$F_q(s) = \sum_{n=1}^{\infty} \frac{f_q(n)}{n^s} = \zeta(s) G_q(s),$$

where

$$G_q(s) = \prod_{p|q} \Big(1 - \frac{1}{p^s}\Big)\Big(1 + \frac{f_q(p)}{p^s} + \frac{f_q(p^2)}{p^{2s}} + \dots\Big).$$

To start with, F_q is defined in $\mathrm{Re}(s) > 1$, but note that the above furnishes a meromorphic continuation to $\mathrm{Re}(s) > 0$. Note also that $\gamma_q = G_q(1)$ in the notation of Section 2. Define

$$E(u) := \frac{1}{z^u} \sum_{n \le z^u} (f_q(n) - G_q(1)),$$

and put for all complex numbers ξ

$$H_j(\xi) := \sum_{p|q} \frac{1 - f_q(p)}{p} p^{\xi/\log z} \Big(\frac{\log(z/p)}{\log z}\Big)^j \text{ for each } j \ge 0,$$

and

$$J(\xi) := \sum_{p|q} \frac{1}{p^2} p^{2\xi/\log z}.$$

Let $H(\xi) := H_0(\xi)$.

THEOREM 3.1. *With notation as above, for* $1 \le \xi \le \frac{2}{3}\log z$,

$$|E(u)| \le \exp(H(\xi) - \xi u + 5J(\xi)).$$

Let $\frac{2}{3}\log z \ge \xi \ge \pi$ *and suppose that* $H(\xi) \ge 20H_2(\xi) + 76J(\xi) + 20$, *so that*

$$\tau := \sqrt{(5H_2(\xi) + 19J(\xi) + 5)/H(\xi)} \le 1/2.$$

Then there exist points $u_\pm$ *in the interval* $[H(\xi)(1-2\tau), H(\xi)(1+2\tau)]$ *such that*

$$E(u_+) \geq \frac{1}{20\xi H(\xi)} \exp\{H(\xi) - \xi u_+ - 5H_2(\xi) - 5J(\xi)\},$$

and

$$E(u_-) \leq -\frac{1}{20\xi H(\xi)} \exp\{H(\xi) - \xi u_- - 5H_2(\xi) - 5J(\xi)\}.$$

In Section 3b (Proposition 3.8) we will show that under certain special circumstances one can reduce length of the range for $u_\pm$ to 2.

We now record some corollaries of Theorem 3.1.

COROLLARY 3.2. *Let $z^{-\frac{1}{10}} \leq \eta \leq 1/100$ and suppose that q is composed of primes in $[z^{1-\eta}, z]$ and that*

$$\sum_{p|q} \frac{1 - f_q(p)}{p} \geq \eta^2.$$

Then for $\sqrt{z} \geq u \geq 5/\eta^2$ there exist points $u_\pm \in [u, u(1+22\eta)]$ such that

$$E(u_+) \geq \exp\Big(- u(1+25\eta) \log\Big(\frac{2u}{\eta^2}\Big)\Big),$$

and

$$E(u_-) \leq -\exp\Big(- u(1+25\eta) \log\Big(\frac{2u}{\eta^2}\Big)\Big).$$

Proof. Note that for $1 \leq \xi \leq \frac{11}{20}\log z$

$$H(\xi) = \sum_{p|q} \frac{1 - f_q(p)}{p} p^{\xi/\log z} \geq \eta^2 e^{(1-\eta)\xi},$$

and that

$$H_2(\xi) \leq \eta^2 H(\xi), \qquad \text{and} \qquad J(\xi) \leq e^{2\xi} z^{\eta-1} \leq \eta^2 H(\xi),$$

where the last inequality for $J(\xi)$ is easily checked using our lower bound for $H(\xi)$ and keeping in mind that $z^{-\frac{1}{10}} \leq \eta \leq 1/100$ and that $\xi \leq \frac{11}{20}\log z$. From these estimates it follows that if $H(\xi) \geq 5/\eta^2$ then τ (in Theorem 3.1) is $\leq 5\eta$. Therefore from Theorem 3.1 we conclude that if $H(\xi) \geq 5/\eta^2$ and $\pi \leq \xi \leq \frac{11}{20}\log z$ then there exist points $u_\pm$ in $[H(\xi)(1-10\eta), H(\xi)(1+10\eta)]$ such that

$$E(u_+) \geq \frac{1}{20\xi H(\xi)} \exp(H(\xi) - \xi u_+ - 5H_2(\xi) - 5J(\xi)) \geq e^{-\xi u_+},$$

and $E(u_-) \leq -e^{-\xi u_-}$. Renaming $H(\xi)(1-10\eta) = u$ so that $\xi \leq \frac{1}{1-\eta}\log(2u/\eta^2)$ we easily obtain the corollary. □

COROLLARY 3.3. *Suppose that q is divisible only by primes between $\sqrt{z}$ and z. Further suppose c is a positive constant such that for $1 \leq \xi \leq \frac{2}{3}\log z$*

there is $H(\xi) \geq ce^{\xi}/\xi$. *Then there is a positive constant* A (*depending only on* c) *such that for all* $e^A \leq u \ll cz^{2/3}/\log z$, *the interval* $[u(1 - A/\log u), u(1 + A/\log u)]$ *contains points* $u_\pm$ *satisfying*

$$E(u_+) \geq \exp\{-u_+(\log u_+ + \log\log u_+ + O(1))\},$$

and

$$E(u_-) \leq -\exp\{-u_-(\log u_- + \log\log u_- + O(1))\}.$$

The implied constants above depend only on c. Note that

$$\sum_{\sqrt{z} \leq p \leq z} 1/p^{1-\xi/\log z} \asymp e^{\xi}/\xi,$$

by the prime number theorem. Thus $H(\xi) \ll e^{\xi}/\xi$, and the criterion $H(\xi) \geq ce^{\xi}/\xi$ in Corollary 3.3 may be loosely interpreted as saying that, "typically", $1 - f_q(p) \gg c$.

If $H(\xi) \sim \kappa e^{\xi}/\xi$ then our bounds take the shape

$$\exp\{-u(\log(u/\kappa) + \log\log u - 1 + o(1))\}.$$

Proof of Corollary 3.3. In this situation $J(\xi) \leq \sum_{\sqrt{z} \leq p \leq z} p^{2\xi/\log z}/p^2 \ll e^{\xi}/\sqrt{z} + e^{2\xi}/z \ll e^{\xi}/\xi^3$. Further, by the prime number theorem,

$$H_2(\xi) \leq \sum_{\sqrt{z} \leq p \leq z} \frac{p^{\xi/\log z}}{p} \Big(\frac{\log(z/p)}{\log z}\Big)^2 \ll \int_{\sqrt{z}}^{z} \frac{t^{\xi/\log z}}{t\log t} \Big(\frac{\log(z/t)}{\log z}\Big)^2 dt \ll \frac{e^{\xi}}{\xi^3}.$$

The corollary now follows from Theorem 3.1, and by the fact that $u = H(\xi)$ so that $\xi = \log u + \log\log u + O(1)$. □

Corollary 3.4. *Keep the notation as in Theorem* 3.1, *and suppose* q *is divisible only by the primes between* $z/2$ *and* z. *Further suppose that* c *is a positive constant such that for* $1 \leq \xi \leq \frac{2}{3}\log z$, $H(\xi) \geq ce^{\xi}/\log z$. *Then there is a positive constant* A (*depending only on* c) *such that for all* $e^A \leq u \ll cz^{2/3}/\log z$ *the interval* $[u(1 - A/\log u), u(1 + A/\log u)]$ *contains points* $u_\pm$ *satisfying*

$$E(u_+) \geq \frac{1}{\log\log z} \exp\{-u_+(\log u_+ + \log\log z + O(1))\},$$

and

$$E(u_-) \leq -\frac{1}{\log\log z} \exp\{-u_-(\log u_- + \log\log z + O(1))\}.$$

As in Corollary 3.3, the implied constants above depend only on c. Also note that $H(\xi)$ in this case is always $\leq \sum_{z/2 \leq p \leq z} 1/p^{1-\xi/\log z} \asymp e^{\xi}/\log z$.

Proof of Corollary 3.4. In this case $J(\xi) \ll e^{2\xi} \sum_{p \geq z/2} 1/p^2 \ll e^{2\xi}/z\log z \ll e^{\xi}/\log^3 z$. Further note that $H_2(\xi) \leq (e^{\xi}/\log^2 z) \sum_{z/2 \leq p \leq z} 1/p \ll e^{\xi}/\log^3 z$.

Taking $u = H(\xi)$ so that $\xi = \log u + \log\log z + O(1)$ and thus $H(\xi) \ll e^{\xi}/\log z$, we easily deduce Corollary 3.4 from Theorem 3.1. $\square$

COROLLARY 3.5. *Keep the notation of Theorem* 3.1, *and suppose* (*as in Corollary* 3.3) *that q is divisible only by primes between $\sqrt{z}$ and z and that for $1 \le \xi \le \frac{2}{3}\log z$, $H(\xi) \ge ce^{\xi}/\xi$. Let $y = z^u$ with $1 \le u \ll cz^{2/3}/\log z$. There is a positive constant B* (*depending only on c*) *such that the interval $[1, z^{u(1+B/\log(u+1))+B}]$ contains numbers $v_\pm$ satisfying*

$$\frac{1}{y}\sum_{v_+ \le n \le v_+ + y} (f_q(n) - G_q(1)) \ge \exp\{-u(\log(u+1) + \log\log(u+2) + O(1))\},$$

and

$$\frac{1}{y}\sum_{v_- \le n \le v_- + y} (f_q(n) - G_q(1)) \le -\exp\{-u(\log(u+1) + \log\log(u+2) + O(1))\}.$$

Proof. Appealing to Corollary 3.3 we see that there is some $w = z^{u_1}$ with $u_1 \in [e^A + u(1 + D/\log(u+1)), e^A + u(1 + (D+3A)/\log(u+1))]$ (here A is as in Corollary 3.3 and D is a suitably large positive constant) such that

$$\sum_{n \le w} (f_q(n) - G_q(1)) \ge w\exp(-u_1(\log u_1 + \log\log u_1 + C_1))\Big)$$

for some absolute constant C_1.

We now divide the interval $[1, w]$ into subintervals of the form $(w - ky, w - (k-1)y]$ for integers $1 \le k \le [w/y]$, together with one last interval $[1, y_0]$ where $y_0 = w - [w/y]y = y\{w/y\}$. Put $y_0 = z^{u_0}$. Then, using the first part of Theorem 3.1 to bound $|E(u_0)|$ (taking there $\xi = \log(u_0+1) + \log\log(u_0+2)$), we get that

$$\Big|\sum_{n \le y_0} (f_q(n) - G_q(1))\Big| = y_0|E(u_0)| \le y_0\exp(-(u_0+1)(\log(u_0+1) + \log\log(u_0+2) - C_2))$$

for some absolute constant C_2.

From the last two displayed equations we conclude that if D is large enough (in terms of C_1 and C_2) then

$$\sum_{y_0 \le n \le w} (f_q(n) - G_q(1)) \ge w\exp\{-u(\log(u+1) + \log\log(u+2) + O(1))\}$$

so that the lower bound in the corollary follows with $v_+ = w - ky$ for some $1 \le k \le [w/y]$. The proof of the upper bound in the corollary is similar.

We now embark on the proof of Theorem 3.1. We will write, below, $f_q(n) = \sum_{d|n} g_q(d)$ for a multiplicative function g_q, the coefficients of the

Dirichlet series $G_q(s)$. Note that $g_q(p^k) = 0$ for $p \nmid q$, and if $p|q$ then $g_q(p^k) = f_q(p^k) - f_q(p^{k-1})$. Clearly $G_q(1) = \sum_{d=1}^{\infty} g_q(d)/d$. Let $[t]$ and $\{t\}$ denote respectively the integer and fractional part of t. Then

$$E(u) = \frac{1}{z^u} \sum_{n \le z^u} \sum_{d|n} g_q(d) - \frac{[z^u]}{z^u} G_q(1) = \frac{1}{z^u} \sum_{d=1}^{\infty} g_q(d) \Big(\Big[\frac{z^u}{d} \Big] - \frac{[z^u]}{d} \Big). \tag{3.1}$$

We begin by establishing the upper bound for $|E(u)|$ in Theorem 3.1.

PROPOSITION 3.6. *In the range* $1 \le \xi \le \frac{2}{3} \log z$,

$$|E(u)| \le \exp(H(\xi) - \xi u + 5J(\xi)\Big),$$

and also

$$\int_0^{\infty} e^{\xi u} |E(u)| du \le \frac{3}{\xi} \exp(H(\xi) + 5J(\xi)).$$

As will be evident from the proof, the condition $\xi \le \frac{2}{3} \log z$ may be replaced by $\xi \le (1 - \varepsilon) \log z$. The constants 3 and 5 will have to be replaced with appropriate constants depending only on ε.

Proof of Proposition 3.6. Since $|[z^u/d] - [z^u]/d| \le \min(z^u/d, 1)$ we obtain, from (3.1), that

$$|E(u)| \le \sum_{d \le z^u} \frac{|g_q(d)|}{z^u} + \sum_{d > z^u} \frac{|g_q(d)|}{d} \le e^{-\xi u} \sum_{d=1}^{\infty} \frac{|g_q(d)|}{d} d^{\xi/\log z};$$

and also that

$$\begin{aligned} \int_0^{\infty} e^{\xi u} |E(u)| du &\le \textstyle\sum_{d=1}^{\infty} |g_q(d)| \Big(\int_0^{\log d/\log z} \frac{e^{\xi u}}{d} du + \int_{\log d/\log z}^{\infty} \frac{e^{\xi u}}{z^u} du \Big) \\ &\le \Big(\frac{1}{\xi} + \frac{1}{\log z - \xi} \Big) \textstyle\sum_{d=1}^{\infty} \frac{|g_q(d)|}{d} d^{\xi/\log z}. \end{aligned}$$

Now, as each $|g(p^k)| \le 1$ and as $2^{1/3}/(2^{1/3} - 1) < 5$,

$$\begin{aligned} \sum_{d=1}^{\infty} \frac{|g_q(d)|}{d} d^{\xi/\log z} &\le \textstyle\prod_{p|q} \Big(1 + \frac{1 - f_q(p)}{p^{1-\xi/\log z}} + \sum_{k=2}^{\infty} \frac{1}{p^{k(1-\xi/\log z)}} \Big) \\ &\le \textstyle\prod_{p|q} \Big(1 + \frac{1 - f_q(p)}{p^{1-\xi/\log z}} \Big) \Big(1 + \frac{5}{p^{2(1-\xi/\log z)}} \Big) \end{aligned}$$

since $p \ge 2$ and $\xi \le \frac{2}{3} \log z$. The proposition follows upon taking logarithms. □

Define

$$I(s) = \int_0^{\infty} e^{-su} E(u) du.$$

From Proposition 3.6 it is clear that $I(s)$ converges absolutely in $\mathrm{Re}(s) > -\frac{2}{3}\log z$, and thus defines an analytic function in this region. Further if $\mathrm{Re}(s) > 0$ then

(3.2)
$$I(s) = \int_0^\infty \frac{e^{-su}}{z^u} \sum_{n \le z^u} (f_q(n) - G_q(1)) = \sum_{n=1}^\infty (f_q(n) - G_q(1)) \int_{\log n/\log z}^\infty \frac{e^{-su}}{z^u} du$$
$$= \frac{\zeta(1+s/\log z)}{\log z + s}(G_q(1+s/\log z) - G_q(1)).$$

By analytic continuation this identity continues to hold for all $\mathrm{Re}(s) > -\frac{2}{3}\log z$.

PROPOSITION 3.7. *For $1 \le \xi \le \frac{2}{3}\log z$ with z sufficiently large,*

$$\int_0^\infty e^{\xi u}|E(u)|du \ge \frac{\xi}{\xi^2+\pi^2}\Big(\exp\{H(\xi) - 5H_2(\xi) - 5J(\xi)\} - 1\Big).$$

Proof. Taking $s = -(\xi + i\pi)$ in (3.2) we deduce that, since $|G_q(1)| \le 1$,

$$\int_0^\infty e^{\xi u}|E(u)|du \ge |I(s)| \ge \frac{|\zeta(1+s/\log z)|}{|s+\log z|}\Big(|G_q(1+s/\log z)| - 1\Big).$$

From the formula $\zeta(w) = w/(w-1) - w\int_1^\infty \{x\}x^{-1-w}dx$, which is valid for all $\mathrm{Re}(w) > 0$, we glean that

$$\frac{|\zeta(1+s/\log z)|}{|s+\log z|} \ge \Big|\mathrm{Re}\Big(\frac{-1}{(\xi+i\pi)} - \frac{1}{\log z}\int_1^\infty \{x\}x^{-2+\xi/\log z}\cos\Big(\frac{\pi\log x}{\log z}\Big)dx\Big)\Big|.$$

For large z and $\xi \le \frac{2}{3}\log z$ we see easily that the integral above is positive,[1] and so we deduce that

$$|\zeta(1+s/\log z)|/|s+\log z| \ge \mathrm{Re}(1/(\xi+i\pi)) = \xi/(\xi^2+\pi^2).$$

Next we give a lower bound for $|G_q(1+s/\log z)|$. We claim that for $z \ge 101^6$ and for all primes p

(3.3)
$$\Big|1 + \frac{f_q(p)}{p^{1+s/\log z}} + \frac{f_q(p^2)}{p^{2(1+s/\log z)}} + \dots\Big| \ge \Big|1 + \frac{f_q(p)}{p^{1+s/\log z}}\Big|\Big(1 - \frac{103}{100}\frac{1}{p^{2-2\xi/\log z}}\Big).$$

When $p > 101^3$ we simply use that the left side of (3.3) exceeds

$$|1 + f_q(p)/p^{1+s/\log z}| - \sum_{k=2}^\infty 1/p^{k(1-\xi/\log z)}$$

[1] In fact, for $z \ge 200$.

and the claim follows. For small $p < 101^3$, set $K = [\log z/(2\log p)]$ and observe that for $k \le K$ the numbers $f_q(p^k)/p^{k(1+s/\log z)}$ all have argument in the range $[0, \pi/2]$. Hence the left side of (3.3) exceeds, when $q = 1/p^{1-\xi/\log z}$,

$$\Big|1 + \frac{f_q(p)}{p^{1+s/\log z}}\Big| - \sum_{k>K} \frac{1}{q^k} \ge \Big|1 + \frac{f_q(p)}{p^{1+s/\log z}}\Big| \left(1 - \frac{1}{q^{K-1}(q-1)^2}\right),$$

which implies (3.3) for $z \ge 101^6$.

Observe that if $|w| \le 2^{-1/3}$ then

$$\log|1+w| = \mathrm{Re}\ (w - \sum_{n=2}^{\infty}(-1)^n w^n/n) \ge \mathrm{Re}\ (w) - 5|w|^2/4.$$

From this observation and our claim (3.3) we deduce easily that

$$\log\Big|1 - \frac{1}{p^{1+s/\log z}}\Big|\Big|1 + \frac{f_q(p)}{p^{1+s/\log z}} + \dots\Big| \ge \mathrm{Re}\ \left(\frac{f_q(p)-1}{p^{1+s/\log z}}\right) - \frac{5}{p^{2(1-\xi/\log z)}}.$$

It follows that

$$\begin{aligned}
&\log|G_q(1+s/\log z)| \\
&\quad \ge -\mathrm{Re}\ \sum_{p|q}\left(\frac{1-f_q(p)}{p}\right)p^{-s/\log z} - 5J(\xi) \\
&\quad = H(\xi) + \sum_{p|q}\left(\frac{1-f_q(p)}{p}\right)p^{\xi/\log z}\Big(-1-\cos\Big(\frac{\pi\log p}{\log z}\Big)\Big) - 5J(\xi).
\end{aligned}$$

Since $-1-\cos(\pi\log p/\log z) \ge -(\pi^2/2)(\log(z/p)/\log z)^2$, we deduce the proposition. □

We are now ready to prove Theorem 3.1.

Proof of Theorem 3.1. The first part of the result was proved in Proposition 3.6. Now, let I^+ (and I^-) denote the set of values u with $E(u) \ge 0$ (respectively $E(u) < 0$). Taking $s = -\xi$ in (3.2) we deduce that for $\xi \le \frac{2}{3}\log z$

$$\Big|\int_0^\infty e^{\xi u}E(u)du\Big| \le 2\Big|\frac{\zeta(1-\xi/\log z)|}{\log z - \xi}\Big| \le \frac{6}{\xi},$$

since $0 \le G_q(1-\xi/\log z), G_q(1) \le 1$, and since (by $\zeta(w)/w = 1/(w-1) - \int_1^\infty \{x\}x^{-1-w}dw$)

$$\Big|\frac{\zeta(1-\xi/\log z)}{(\log z - \xi)}\Big| = \Big|-\frac{1}{\xi} - \frac{1}{\log z}\int_1^\infty \{x\}x^{-2+\xi/\log z}dx\Big| \le \frac{1}{\xi} + \frac{1}{\log z - \xi} \le \frac{3}{\xi}.$$

Combining this with Proposition 3.7 we deduce easily that

$$\begin{aligned}
(3.4)\quad \int_{I^\pm} e^{\xi u}|E(u)|du &\ge \frac{\xi}{2(\xi^2+\pi^2)}\Big(\exp\{H(\xi) - 5H_2(\xi) - 5J(\xi)\} - 1\Big) - \frac{3}{\xi} \\
&\ge \frac{1}{5\xi}\exp\{H(\xi) - 5H_2(\xi) - 5J(\xi)\}.
\end{aligned}$$

Put $u_1 = H(\xi)(1+2\tau)$. Then by Proposition 3.6 we get that

$$\int_{u_1}^{\infty} e^{\xi u}|E(u)|du \le e^{-\tau u_1}\int_0^{\infty} e^{(\xi+\tau)u}|E(u)|du$$
$$\le \frac{3}{\xi}\exp\{H(\xi+\tau)-\tau u_1+5J(\xi+\tau)\}.$$

Now $H(\xi+\tau)\le e^{\tau}H(\xi)\le(1+\tau+\tau^2)H(\xi)$, and $J(\xi+\tau)\le e^{2\tau}J(\xi)\le 2.8J(\xi)$. Hence $H(\xi+\tau)+5J(\xi+\tau)-\tau u_1\le H(\xi)-5H_2(\xi)-5J(\xi)-5$, and so we conclude that

$$\int_{u_1}^{\infty} e^{\xi u}|E(u)|du \le \frac{1}{20\xi}\exp\{H(\xi)-5H_2(\xi)-5J(\xi)\}. \tag{3.5}$$

Similarly note that, with $u_0 = H(\xi)(1-2\tau)$,

$$\int_0^{u_0} e^{\xi u}|E(u)|du \le e^{\tau u_0}\int_0^{\infty} e^{(\xi-\tau)u}|E(u)|du$$
$$\le \frac{3}{\xi-\tau}\exp\{H(\xi-\tau)+\tau u_0+5J(\xi-\tau)\}.$$

Now $J(\xi-\tau)\le J(\xi)$, and

$$\begin{aligned} H(\xi-\tau) &= \sum_{p|q}\frac{1-f_q(p)}{p}p^{\xi/\log z}p^{-\tau/\log z}\\ &\le \sum_{p|q}\frac{1-f_q(p)}{p}p^{\xi/\log z}\Big(1-\tau\frac{\log p}{\log z}+\frac{\tau^2}{2}\Big)\\ &= H(\xi)(1-\tau+\tau^2/2)+\tau H_1(\xi)\\ &\le H(\xi)(1-\tau+\tau^2/2)+\tau\sqrt{H(\xi)H_2(\xi)}, \end{aligned}$$

since $H_1(\xi)\le\sqrt{H(\xi)H_2(\xi)}$ by Cauchy's inequality. From these observations and our definition of τ it follows that $H(\xi-\tau)+5J(\xi-\tau)+\tau u_0\le H(\xi)-5H_2(\xi)-5J(\xi)-5$, and so

$$\int_0^{u_0} e^{\xi u}|E(u)|du \le \frac{1}{20\xi}\exp\{H(\xi)-5H_2(\xi)-5J(\xi)\}. \tag{3.6}$$

Combining (3.4), (3.5), and (3.6) we deduce that

$$\int_{I^{\pm}\cap[u_0,u_1]} e^{\xi u}|E(u)|du \ge \frac{1}{10\xi}\exp\{H(\xi)-5H_2(\xi)-5J(\xi)\}.$$

Now $u_1-u_0\le 4\tau H(\xi)\le 2H(\xi)$, so the theorem follows. □

3b. *Localization of sign changes of E.* We saw in Corollary 3.3 that (in typical situations) E changes sign in intervals of the form $[u(1-A/\log u), u(1+A/\log u)]$. We consider now the problem of providing a better localization of the sign changes of E for small values of u. Our main result of this section is the following:

PROPOSITION 3.8. *With notation as above, suppose that* $\max_{x\ge u}|E(x)|\gg 1/(G_q(1)\log z))$ *for some* $u\ge 6$. *Then there exist points* $u_+,u_-\in[u-1,u+1]$ *such that* $E(u_+),-E(u_-)\ge\max_{x\ge u}|E(x)|$.

Proposition 3.8 (which may be easily deduced from the lemmas of this section) can be used to reduce the size of the interval in Theorem 3.1. In Corollary 3.3 this is simple to state: For $e^A\le u\le\log\log z/(2\log\log\log z)$ the interval $[u-1,u+1]$ contains points $u_\pm$ satisfying the conclusions of Corollary 3.3.

LEMMA 3.9. *Uniformly for* $u>0$,

$$uE(u)+\int_u^\infty E(t)dt+\frac{1}{\log z}\sum_{p\le z}\frac{1-f_q(p)}{p}\log p\,E\Big(u-\frac{\log p}{\log z}\Big)=O\Big(\frac{1}{G_q(1)\log z}\Big).$$

Proof. Let $E_1(u):=\sum_{d>z^u}g_q(d)/d$; and note that $|E_1(u)|\le\sum_d|g_q(d)|/d\ll 1/G_q(1)$. By a result of R. R. Hall (see [13], or (4.1) of [10]) we see that

$$\frac{1}{z^u}\sum_{d\le z^u}|g_q(d)|\ll\frac{1}{u\log z}\sum_d\frac{|g_q(d)|}{d}\ll\frac{1}{G_q(1)u\log z}.$$

Therefore, from (3.1) we deduce that

$$\begin{aligned}E(u)&=-(1+O(z^{-u}))E_1(u)+O\Big(\frac{1}{z^u}\sum_{d\le z^u}|g_q(d)|\Big)\\&=-E_1(u)+O\Big(\frac{1}{G_q(1)u\log z}\Big).\end{aligned}\tag{3.7}$$

Manipulation of $E_1(u)$ yields our identity. The starting point is the observation that

$$uE_1(u)+\int_u^\infty E_1(t)dt=uE_1(u)+\sum_{d>z^u}\frac{g_q(d)}{d}\Big(\frac{\log d}{\log z}-u\Big)=\sum_{d>z^u}\frac{g_q(d)}{d}\frac{\log d}{\log z}.\tag{3.8}$$

We approximate the left side of (3.8) as follows:

$$\begin{aligned}&\Big|(uE_1(u)+\int_u^\infty E_1(t)dt)+(uE(u)+\int_u^\infty E(t)dt)\Big|\\&\quad\le u|E_1(u)+E(u)|+\int_u^\infty|E_1(t)+E(t)|dt\\&\quad\ll\frac{1}{G_q(1)\log z}+\int_u^\infty z^{-t}\Big(\frac{1}{G_q(1)}+\sum_{d\le z^u}|g_q(d)|\Big)dt\\&\quad\ll\frac{1}{G_q(1)\log z}+\frac{1}{\log z}\Big(\sum_d\frac{|g_q(d)|}{d}\Big)\ll\frac{1}{G_q(1)\log z}.\end{aligned}$$

Now $\log d = \sum_{m|d} \Lambda(m)$ so that the right side of (3.8) equals

$$\frac{1}{\log z} \sum_m \Lambda(m) \sum_{\substack{d>z^u \\ m|d}} \frac{g_q(d)}{d}.$$

The sum over m's above can be restricted to prime powers p^k for $p \le z$ (else $g_q(d) = 0$). Further the contribution of prime powers p^k with $k \ge 2$ is bounded by $\ll 1/(G_q(1)\log z)$. Finally for $m = p \le z$ we see that

$$\begin{aligned}\sum_{\substack{d>z^u \\ m|d}} \frac{g_q(d)}{d} &= \frac{g_q(p)}{p} \sum_{d>z^u/p} \frac{g_q(d)}{d} + O\Big(\frac{1}{p^2 G_q(1)}\Big) \\ &= -\frac{1-f_q(p)}{p} E_1\Big(u - \frac{\log p}{\log z}\Big) + O\Big(\frac{1}{p^2 G_q(1)}\Big).\end{aligned}$$

Therefore, by (3.7), this, taken with the estimate for the left side of (3.8), yields the result.

We call a point w *special* if $|E(w)| = \max_{x \ge w} |E(x)|$. Since $E(x) \to 0$ as $x \to \infty$ we see that there are arbitrarily large special points.

LEMMA 3.10. *Given $u \ge 2$ either $E(x) = O(1/(G_q(1)\log z))$ for all $x \ge u$ or there is a special point in $[u, u+1]$.*

Proof. Let w denote the infimum of the set of special points at least as large as u, and assume $w > u+1$ (that is, there is no special point in $[u, u+1]$). Note that $|E(w)| \ge |E(x)| + O(z^{-u})$ for any $x \ge u$. If $E(x)$ maintains the same sign for all $x \ge w$ set $v = \infty$; otherwise let v denote the infimum of those points $x \ge w$ for which $E(x)$ has the opposite sign to $E(w)$. Note that $E(v) = O(1/z^v)$. Taking Lemma 3.9 with $u = w$ and $u = v$ and subtracting we find that

(3.9)
$$\begin{aligned} wE(w) + \int_w^v E(t)dt + \frac{1}{\log z} \sum_{p \le z} \frac{1-f_q(p)}{p} \log p \, \Big(E\Big(w - \frac{\log p}{\log z}\Big) - E\Big(v - \frac{\log p}{\log z}\Big)\Big) \\ = O\Big(\frac{1}{G_q(1)\log z}\Big).\end{aligned}$$

Since $E(t)$ maintains the same sign throughout $[w, v]$ we have that

$$\Big|wE(w) + \int_w^v E(t)dt\Big| \ge w|E(w)|,$$

while on the other hand

$$\begin{aligned}&\Big|\frac{1}{\log z} \sum_{p \le z} \frac{1-f_q(p)}{p} \log p \, \Big(E\Big(w - \frac{\log p}{\log z}\Big) - E\Big(v - \frac{\log p}{\log z}\Big)\Big)\Big| \\ &\quad \le \frac{2}{\log z} \sum_{p \le z} \frac{\log p}{p} \max_{\xi \ge w-1} |E(\xi)| \le (2+o(1)) \max_{\xi \ge u} |E(\xi)| \le (2+o(1))|E(w)|,\end{aligned}$$

since w was assumed to be larger than $u+1$. We conclude that

$$(u-1+o(1))|E(w)| = O(1/(G_q(1)\log z))$$

which establishes the lemma. □

LEMMA 3.11. *If $u \geq 2$ and $E(x)$ maintains the same sign throughout $[u, u+2]$ then $E(x) = O(1/(G_q(1)\log z))$ for all $x \geq u+1$.*

Proof. Suppose not. Let w denote the infimum of the set of all special points at least as large as $u+1$. By Lemma 3.10 we know that $w \leq u+2$. Let v denote the infimum of points $x \geq u+2$ such that $E(x)$ has the opposite sign to $E(w)$; if no such point exists set $v = \infty$. Now E maintains the same sign in $[w-1, v]$ (since it is a subinterval of $[u, v]$) and so

$$\Big| wE(w) + \int_w^v E(t)dt + \frac{1}{\log z}\sum_{p\leq z}\frac{1-f_q(p)}{p}\log p\ E\Big(w - \frac{\log p}{\log z}\Big)\Big| \geq w|E(w)|;$$

on the other hand

$$\Big|\frac{1}{\log z}\sum_{p\leq z}\frac{1-f_q(p)}{p}\log p\ E\Big(v - \frac{\log p}{\log z}\Big)\Big| \leq |E(w)|(1+o(1)),$$

since $|E(v - \log p/\log z)| \leq \max_{x\geq v-1}|E(x)| \leq |E(w)|$. Therefore, by (3.9), we deduce that $(w-1+o(1))|E(w)| \leq O(1/(G_q(1)\log z))$ which proves the lemma. □

PROPOSITION 3.12. *Fix $\varepsilon > 0$. Given a special point $w > 4+\varepsilon$ either there exists a point $\xi \in [w-1, w]$ for which $E(\xi)$ and $E(w)$ have opposite signs and $|E(\xi)| \geq (w-4-\varepsilon)|E(w)|$, or $E(w) = O(1/(G_q(1)\log z))$.*

Proof. Select $v \in [w+1, w+3]$ with $E(v) = O(z^{-v})$ (if v does not exist then the proposition follows from Lemma 3.11). Choose $\delta = \pm 1$ so that $\delta E(w) > 0$. Suppose that $\delta E(x) > -(2w-v-1-\varepsilon)\delta E(w)$ for all $x \in [w-1, w]$. Then δ times the right side of (3.9) is

$$\geq \delta E(w)(w - \int_w^v 1dt - \frac{1}{\log z}\sum_{p\leq z}\frac{\log p}{p}\ (2w-v-1-\varepsilon+1)) \geq \varepsilon|E(w)|/2$$

since each $v - \log p/\log z \geq w$ so that $|E(v-\log p/\log z)| \leq |E(w)|$. The result follows from (3.9) since $2w-v-1 \geq w-4$. □

Given $u > 3+\varepsilon$ we can take w to be a special point in $[u+1, u+2]$ and then $\xi \in [u, u+2]$.

4. Proof of Theorems 2.4 and 2.5

We shall only provide the proof of Theorem 2.4, the proof of Theorem 2.5 being entirely similar. We take q to be the product of all the primes in

$(z^{1-\eta}, z)$ so that $q \le \prod_{p\le z} p \le x^{1/3+o(1)}$. Since $\mathcal{S} \subset [1, \log\log x]$ we also know that $(q, \mathcal{S}) = 1$. Since q is squarefree we check that $f_q(n)$ (as defined in Section 2) satisfies $f_q(p^k) = 1$ if $p \nmid q$ and $f_q(p^k) = h(p)(p-1)/(p-h(p))$ if $p|q$ and $k \ge 1$ (note that $f_q(p^k) \le h(p) \le 1$ in this case) . Thus $0 \le f_q(n) \le 1$ for all n, and we may apply the results of Section 3, in particular Corollary 3.2. From Corollary 3.2 we obtain that for $\sqrt{z} \ge u \ge 5/\eta^2$ there exists $\lambda \in [u, u(1+22\eta)]$ such that

$$\Big|\frac{1}{z^\lambda}\sum_{n\le z^\lambda} f_q(n) - G_q(1)\Big| \ge \exp\Big(-u(1+25\eta)\log\Big(\frac{2u}{\eta^2}\Big)\Big). \tag{4.1}$$

Using Proposition 2.2, we may easily find $\ell \in (x/(2(z^\lambda+1)), x/(2z^\lambda))$ such that ℓ is not divisible by any prime below $(\log x)/3$. Such an ℓ is coprime to q, satisfies $(\ell, \mathcal{S}) = 1$, and further, $\phi(\ell)/\ell \gg 1$. Proposition 2.2 therefore yields, by (4.1),

$$\Delta_q + \Delta_\ell \gg \exp\Big(-u(1+25\eta)\log\Big(\frac{2u}{\eta^2}\Big)\Big),$$

proving Theorem 2.4 (in the statement of which we might take $\ell = q$).

5. Limitations to the equidistribution of primes

In this section we will exploit the flexibility afforded by our general oscillation results to obtain refinements to previous results on the limitations to the equidistribution of primes. We stated in Theorem 1.5 (see Introduction) the result for primes in short intervals and we now state the analogous results for primes in arithmetic progressions.

THEOREM 5.1. *Let ℓ be large and suppose that ℓ has fewer than $(\log \ell)^{1-\varepsilon}$ prime divisors below $\log \ell$. Suppose that*

$$(\log \ell)^{1+\varepsilon} \le y \le \exp(\beta\sqrt{\log \ell}/\sqrt{2\log\log \ell})$$

for a certain absolute constant $\beta > 0$, and put $x = \ell y$. Define for integers a coprime to ℓ

$$\Delta(x;\ell,a) = \Big(\vartheta(x;\ell,a) - \frac{x}{\varphi(\ell)}\Big)\Big/\frac{x}{\varphi(\ell)}.$$

There exist numbers $x_\pm$ in the interval $(x, xy^{D/\log(\log y/\log\log \ell)})$, and integers $a_\pm$ coprime to ℓ such that

$$\Delta(x_+;\ell,a_+) \ge y^{-\delta(\ell,y)}, \qquad \text{and} \qquad \Delta(x_-;\ell,a_-) \le -y^{-\delta(\ell,y)}.$$

Here D is an absolute positive constant which depends only on ε, and $\delta(\cdot,\cdot)$ is as in Theorem 1.5.

These bounds are $\gg 1$ if $y = (\log \ell)^{O(1)}$, and $\gg y^{-\tau(1+o(1))}$ if $y = \exp((\log \ell)^\tau)$ with $0 \le \tau < 1/2$. The corresponding result in [4, Th. A1],

gives the weaker bound $y^{-(1+o(1))\tau/(1-\tau)}$ (though our bound is obtained there assuming the Generalized Riemann Hypothesis). Our constraint on the small primes dividing ℓ is less restrictive than the corresponding condition there, though our localization of the $x_\pm$ values is worse (in [4] the $x_\pm$ values are localized in intervals $(x/2, 2x)$).

Theorem 5.1 omits a thin set of moduli ℓ having very many small prime factors. We next give a weaker variant which includes all moduli ℓ.

THEOREM 5.2. *Let ℓ be large and suppose that*

$$(\log \ell)^{1+\varepsilon} \le y \le \exp(\beta\sqrt{\log \ell}/\sqrt{\log\log \ell})$$

for a certain absolute constant $\beta > 0$, and put $x = y\ell$. There exist numbers $x_\pm$ in the interval $(x, xy^{D/\log(\log y/\log\log \ell)})$, and integers $a_\pm$ coprime to ℓ such that

$$\Delta(x_+; \ell, a_+) \ge \frac{y^{-\delta_1(\ell,y)}}{\log\log\log \ell} \qquad \textit{and} \qquad \Delta(x_-; \ell, a_-) \le -\frac{y^{-\delta_1(\ell,y)}}{\log\log\log \ell},$$

where $\delta_1(x, y) = (\log\log y + O(1))/(\log\log x)$. Here D is an absolute positive constant which depends only on ε.

Theorem 5.2 should be compared with Theorem A2 of [4]. Our bound is $\gg y^{-\tau(1+o(1))}$ if $y = \exp((\log \ell)^\tau)$ with $0 < \tau < 1/2$. The corresponding result in [4, Th. A2], gives a weaker bound $y^{-(3+o(1))\tau/(1+\tau)}$, though our localization of the $x_\pm$ values is again much worse.

To prove Theorems 1.5, 5.1 and 5.2 we require knowledge of the distribution of primes in certain arithmetic progressions. We begin by describing such a result, which will be deduced as a consequence of a theorem of Gallagher [5].

For $1 \le j \le J := [\log z/(2\log 2)]$, consider the dyadic intervals $I_j = (z/2^j, z/2^{j-1}]$. Let P_j denote a subset of the primes in I_j, and let π_j denote the cardinality of P_j. We let $\mathcal{Q}$ denote the set of integers q with the following property: $q = \prod_{j=1}^J q_j$ and each q_j is the product of exactly $[\pi_j/2]$ distinct primes in P_j. It is clear that all the elements of $\mathcal{Q}$ are squarefree and lie below $Q := z^{\sum_j \pi_j/2}$, and that $|\mathcal{Q}| = \prod_{j=1}^J \binom{\pi_j}{[\pi_j/2]}$.

There is a constant c_1 such that at most one primitive L-function with modulus q between $\sqrt{T}$ and T has a zero in the region $\sigma > 1 - c_1/\log q$, and $|t| \le T$. Further if this exceptional Siegel zero exists then it is real, simple and unique (see Chapter 14 in [2]). We call the modulus of such an exceptional character a Siegel modulus. Below Q there are $\ll \log\log Q$ Siegel moduli. Denote these by $\nu_1, \nu_2, \dots, \nu_\ell$, and for each select a prime divisor $v_1, \dots, v_\ell$. Assume none of $v_1, \dots v_\ell$ belongs to $\cup_{j=1}^J P_j$, which guarantees that there are no Siegel zeros for any of the moduli d where d is a divisor of some $q \in \mathcal{Q}$.

PROPOSITION 5.3. *Suppose that* $\exp(\sqrt{\log x}) \le Q \le x^b$ *where* b *is a positive absolute constant, and let* $x\exp(-\sqrt{\log x}) \le h \le x$. *Then*

$$\frac{1}{|\mathcal{Q}|}\sum_{q\in\mathcal{Q}}\max_{(a,q)=1}\left|\frac{\vartheta(x+h;q,a)-\vartheta(x;q,a)-h/\varphi(q)}{h/\varphi(q)}\right| \ll \exp\Big(-\alpha\frac{\sqrt{\log x}}{\sqrt{\log z}}\Big),$$

where α *is a positive absolute constant.*

Proof. If $(a,q)=1$ then using the orthogonality of characters, we have

$$\begin{aligned}\vartheta(x+h;q,a)-\vartheta(x;q,a) &= \frac{1}{\varphi(q)}\sum_{\chi \pmod q}\overline{\chi(a)}\sum_{x}^{x+h}\chi(p)\log p\\ &= \frac{1}{\varphi(q)}\sum_{\substack{x\le p\le x+h\\(p,q)=1}}\log p + O\Big(\frac{1}{\varphi(q)}\sum_{\chi\ne\chi_0}\Big|\sum_{x}^{x+h}\chi(p)\log p\Big|\Big).\end{aligned}$$

By the prime number theorem the first term above is

$$h/\varphi(q)\{1+O(\exp(-c\sqrt{\log x}))\},$$

which has an acceptable error term. We now focus on estimating the second term on average.

Below the superscript $*$ will indicate a restriction to primitive characters. Observe that

$$\begin{aligned}\sum_{\chi\ne\chi_0}\Big|\sum_{x}^{x+h}\chi(p)\log p\Big| &= \sum_{\substack{d|q\\d>1}}\ \sideset{}{^*}\sum_{\chi \pmod d}\Big(\Big|\sum_{x}^{x+h}\chi(p)\log p\Big| + O\Big(\sum_{p|\frac{q}{d}}\log p\Big)\Big)\\ &= \sum_{\substack{d|q\\d>1}}\ \sideset{}{^*}\sum_{\chi \pmod d}\Big|\sum_{x}^{x+h}\chi(p)\log p\Big| + O(d(q)\log q).\end{aligned}$$

Thus

(5.1)

$$\sum_{q\in\mathcal{Q}}\sum_{\chi\ne\chi_0}\Big|\sum_{x}^{x+h}\chi(p)\log p\Big| = \sum_{1<d\le Q}\Big(\sum_{\substack{q\in\mathcal{Q}\\d|q}}1\Big)\ \sideset{}{^*}\sum_{\chi \pmod d}\Big|\sum_{x}^{x+h}\chi(p)\log p\Big| + O(|\mathcal{Q}|x^{\varepsilon}).$$

Observe that if d is to have any multiples in $\mathcal{Q}$ then we must have $d=\prod_{j=1}^{J}d_j$ with each of the d_j being composed of at most $[\pi_j/2]$ distinct primes from P_j. Therefore

$$\sum_{\substack{q\in\mathcal{Q}\\d|q}}1 \le \prod_{j=1}^{J}\binom{\pi_j-\omega(d_j)}{[\pi_j/2]-\omega(d_j)} \le \prod_{j=1}^{J}2^{-\omega(d_j)}\binom{\pi_j}{[\pi_j/2]} = 2^{-\omega(d)}|\mathcal{Q}| \le 2^{-\frac{\log d}{\log z}}|\mathcal{Q}|,$$

where $\omega(n)$ denotes the number of prime factors of n, and the final estimate follows since all prime divisors of d are below z and so $\omega(d) \geq \log d/\log z$. From these remarks we see that the right side of (5.1) is

$$\leq |\mathcal{Q}| \sideset{}{^\flat}\sum_{1<d\leq Q} 2^{-\frac{\log d}{\log z}} \sideset{}{^*}\sum_{\chi \pmod d} \Big|\sum_{x}^{x+h} \chi(p)\log p\Big| + O(|\mathcal{Q}|x^{\varepsilon}), \tag{5.2}$$

where the $\flat$ on the sum over d indicates that the sum is restricted to d as above; note that such d have no Siegel zeros.

Define $J_0 := [1, \exp(\sqrt{\log x})]$, and $J_k := (\exp(\sqrt{\log x})z^{k-1}, \exp(\sqrt{\log x})z^k]$ for $1 \leq k \leq [(\log Q - \sqrt{\log x})/\log z]$. Theorem 7 of Gallagher [5] implies that the contribution of terms $d \in J_k$ (for $k \geq 1$) is (for a positive absolute constant α)

$$\leq |\mathcal{Q}|h\exp\Big(-\alpha^2\frac{\log x}{\sqrt{\log x}+(k+1)\log z} - \frac{\sqrt{\log x}+k\log z}{2\log z}\Big)$$
$$\ll h|\mathcal{Q}|\exp\Big(-\alpha\frac{\sqrt{2\log x}}{\sqrt{\log z}}\Big),$$

and also that the contribution of the terms $d \in J_0$ is $\ll |\mathcal{Q}|h\exp(-\alpha\sqrt{\log x})$. Summing over k we deduce that the quantity in (5.2) is

$$\ll |\mathcal{Q}|h\exp(-\alpha\sqrt{\log x}/\sqrt{\log z})$$

which proves the proposition. □

Corollary 5.4. *Suppose that* $\exp(\sqrt{\log x}) \leq Q \leq x^b$ *where* b *is a positive absolute constant. Select* z *to be the largest integer such that* $\prod_{p\leq z} p \leq Q^{2-o(1)}$. *Then there exists an integer* $q \in [Q^{1-c/\log\log Q}, Q]$, *whose prime factors all lie in* $[\sqrt{z}, z]$ *with* $\sum_{p|q} 1/p^{1-\xi/\log z} \geq e^{\xi}/(10\xi)$ *for* $1 \leq \xi \leq \frac{2}{3}\log z$, *such that*

$$\Big|\vartheta(2x;q,a) - \vartheta(x;q,a) - \frac{x}{\varphi(q)}\Big| \ll \frac{x}{\varphi(q)}\exp\Big(-\beta\frac{\sqrt{\log x}}{\sqrt{\log\log x}}\Big), \tag{5.3}$$

for all $(a,q)=1$, *where* β *is a positive absolute constant.*

Proof. When z is chosen as above we have $z \sim 2\log Q$ so that $\sqrt{\log x} \ll z \ll \log x$. If $z/2^j < \sqrt{z}$ then let $P_j = \emptyset$. If $z \geq z/2^j \geq \sqrt{z}$ then let P_j be the set of primes in I_j, omitting the prime divisors $v_1, \ldots v_\ell$ of Siegel moduli; in these cases $\pi_j = \pi(z/2^{j-1}) - \pi(z/2^j) + O(\log\log x)$. By Proposition 5.3 we can select q satisfying (5.3), with $\sim z/(2^{j+1}\log(z/2^j))$ prime factors in each I_j where $j \leq [\log z/\log 4]$, so that $\sum_{p|q} 1/p^{1-\xi/\log z} \geq e^{\xi}/(10\xi)$ for $1 \leq \xi \leq \frac{2}{3}\log z$.

Corollary 5.5. *Fix* $1/2 \geq \varepsilon > 0$. *Suppose there is a large integer* ℓ *with fewer than* $(\log\ell)^{1-\varepsilon}$ *prime divisors below* $\log\ell$. *Suppose also that*

$\exp(3(\log \ell)^{1-\varepsilon}) \le Q \le \ell^b$, *and that* J *is a positive integer* $\le \exp(\sqrt{\log \ell})$. *Select* z *to be the largest integer such that* $\prod_{p\le z} p \le Q^{2-o(1)}$. *Then there exists an integer* $q \in [Q^{1-c/\log\log Q}, Q]$, *coprime to* ℓ *whose prime factors all lie in* $[\sqrt{z}, z]$ *with* $\sum_{p|q} 1/p^{1-\xi/\log z} \ge e^{\xi}/(10\xi)$ *for* $1 \le \xi \le \frac{2}{3}\log z$, *for which*

$$\sum_{j=1}^{J} \max_{(a,q)=1} \left| \frac{\vartheta((j+1)\ell/2; q, a) - \vartheta(j\ell/2; q, a) - \ell/2\varphi(q)}{\ell/2\varphi(q)} \right| \ll J \exp\Big(-\beta \frac{\sqrt{\log \ell}}{\sqrt{\log\log \ell}} \Big),$$

where β *is a positive absolute constant.*

Proof. If $j > \varepsilon(\log z)/10$ let $P_j = \emptyset$. If $1 \le j \le \varepsilon(\log z)/10$ let P_j be the set of primes in I_j, omitting the prime divisors $v_1, \dots v_\ell$ of Siegel moduli and any prime divisors of ℓ. Now, for $1 \le j \le J$ replace x by $j\ell/2$ and h by $\ell/2$ in Proposition 5.3, and sum. This yields

$$\sum_{j=1}^{J} \frac{1}{|\mathcal{Q}|} \sum_{q\in\mathcal{Q}} \max_{(a,q)=1} \left| \frac{\vartheta((j+1)\ell/2; q, a) - \vartheta(j\ell/2; q, a) - \ell/2\varphi(q)}{\ell/2\varphi(q)} \right| \ll J \exp\Big(-\alpha \frac{\sqrt{\log \ell}}{\sqrt{\log z}} \Big).$$

Thus we may choose a q as described in the result, proceeding as in the proof of Corollary 5.4.

COROLLARY 5.6. *Given a large integer* ℓ, *let* $Q = \ell^b$ *for sufficiently small* $b > 0$, *and let* J *be a positive integer* $\le \exp(\sqrt{\log \ell})$. *Select* $z = 10 \log \ell$. *Then there exists an integer* $q \in [Q^{1-c/\log\log Q}, Q]$, *coprime to* ℓ *whose prime factors all lie in* $[z/2, z]$ *with* $\sum_{p|q} 1/p^{1-\xi/\log z} \gg be^{\xi}/\log z$ *for* $1 \le \xi \le \frac{2}{3}\log z$, *for which*

$$\sum_{j=1}^{J} \max_{(a,q)=1} \left| \frac{\vartheta((j+1)\ell/2; q, a) - \vartheta(j\ell/2; q, a) - \ell/2\varphi(q)}{\ell/2\varphi(q)} \right| \ll J \exp\Big(-\beta \frac{\sqrt{\log \ell}}{\sqrt{\log\log \ell}} \Big),$$

where β *is a positive absolute constant.*

Proof. Let $P_j = \emptyset$ for $j > 1$, and let P_1 be a set of $\pi_1 = [2b \log \ell/\log\log \ell]$ primes in $I_1 = (z/2, z]$, omitting the prime divisors $v_1, \dots v_\ell$ of Siegel moduli and any prime divisors of ℓ; this is possible since I_1 contains $\sim 5 \log \ell/\log\log \ell$ primes, and we are forced to omit at most $\sim \log \ell/\log\log \ell$. From here we proceed as in the proof of Corollary 5.5.

Proof of Theorem 1.5. Take $Q = x^b$ in Corollary 5.4 to obtain q which satisfies the hypotheses of Corollary 3.5. Let $u := \log y/\log z$ and select $v_\pm$ as in Corollary 3.5. We consider the Maier matrices $\mathcal{M}_\pm$ with

$$(\mathcal{M}_\pm)_{r,s} = \begin{cases} \log(rq+s) & \text{if } rq+s \text{ is prime,} \\ 0 & \text{otherwise,} \end{cases}$$

where $x/q < r < 2x/q$ and $v_\pm \le s \le v_\pm + y$. Let $M_\pm$ denote the sum of the entries of $\mathcal{M}_\pm$. Using (5.3) to sum the entries in column s we see that

$$M_\pm = \frac{x}{\varphi(q)}\Big(1 + O\Big(\exp\Big(-\beta\frac{\sqrt{\log x}}{\sqrt{\log\log x}}\Big)\Big)\Big) \sum_{\substack{v_\pm \le s \le v_\pm + y \\ (s,q)=1}} 1.$$

Let r_+ denote the row in $\mathcal{M}_+$ whose sum is largest, and let $x_+ := qr_+ + v_+ \in (x, 2x)$. Since there are $x/q + O(1)$ rows, we have

$$\vartheta(x_+ + y) - \vartheta(x_+) \ge \frac{q}{x}(1 + O(x^{-1/2}))M_+,$$

and then Theorem 1.5 follows from the bounds in Corollary 3.5. The analogous argument works for $\mathcal{M}_-$.

Proof of Theorem 5.1. Take $Q = \ell^b$ in Corollary 5.5 to obtain q which satisfies the hypothesis of Corollary 3.3. Let $u := \log y/\log z$ and select U in Corollary 3.3 so that $U(1 - A/\log U) = u$; then put $S_\pm = [z^{U_\pm}]$, so that $S_\pm \in [z^u, z^{u+Cu/\log u}]$. We consider the Maier matrices $\mathcal{M}_\pm$ with

$$(\mathcal{M}_\pm)_{r,s} = \begin{cases} \log(rq+s\ell) & \text{if } rq+s\ell \text{ is prime,} \\ 0 & \text{otherwise,} \end{cases}$$

where $R < r < 2R$ with $R := [\ell/(2q)]$ and $1 \le s \le S_\pm$. Let $M_\pm$ denote the sum of the entries of $\mathcal{M}_\pm$. Using Corollary 5.5 to sum the entries in column s we see that

$$M_\pm = \frac{\ell}{2\varphi(q)}\Big(1 + O\Big(\exp\Big(-\beta\frac{\sqrt{\log x}}{\sqrt{\log\log x}}\Big)\Big)\Big) \sum_{\substack{s \le S_\pm \\ (s,q)=1}} 1.$$

Now, the sum of the entries in row r equals 0 if $(r,\ell) > 1$; and equals $\vartheta(\ell S_\pm + qr; \ell, qr) - \vartheta(qr; \ell, qr) = \vartheta(\ell S_\pm + qr; \ell, qr)$ if $(r,\ell) = 1$, since $qr < \ell$ and qr is not prime. The number of integers $r \in [R, 2R]$ with $(r,\ell) = 1$ is $R\varphi(\ell)/\ell + O(\tau(\ell)) = \varphi(\ell)/(2q) + O(\ell^\varepsilon)$. Therefore, denoting by r_+ the row for which $\vartheta(x_+; \ell, a_+)$, with $x_+ = \ell S_+ + qr_+$ and $a_+ = qr_+$, is maximized, we obtain

$$\vartheta(x_+; \ell, a_+) \ge \frac{2q}{\varphi(\ell)}(1 + O(\ell^{-1/2}))M_+,$$

and then Theorem 5.1 follows from the bounds in Corollary 3.3. The analogous argument works for $\mathcal{M}_-$.

Proof of Theorem 5.2. We proceed exactly as in the proof of Theorem 5.1 but replacing the use of Corollary 3.3 by Corollary 3.4, and the use of Corollary 5.5 by Corollary 5.6.

6. Further examples

6a. *Reduced residues.* Let q be square-free. Writing

$$\sum_{\substack{n\le x\\(n,q)=1\\n\equiv a \pmod{\ell}}} 1 = \sum_{d|q}\mu(d)\sum_{\substack{n\le x\\ d|n\, n\equiv a \pmod{\ell}}} 1,$$

we see that this is

$$= \begin{cases} 0 & \text{if } (a,q,\ell)>1\\ \frac{x}{\ell}\frac{\phi(q/(q,\ell))}{q/(q,\ell)} + O(\tau(q)) & \text{if } (a,q,\ell)=1. \end{cases} \tag{6.1}$$

Corollary 6.1. *Let q be a large square-free number, which satisfies* (1.3), *and define $\alpha := (\log\log q)^{-1}\sum_{p|q}(\log p)/p$ with $\eta = \min(1/100, \alpha/3)$. Then for $\eta(\log q)^{\eta/2} \ge u \ge 5/\eta^2$ there exist intervals $I_\pm \subset [q/4, 3q/4]$ of length at least $(\log q)^u$ such that*

$$\sum_{\substack{n\in I_+\\(n,q)=1}} 1 \ge \frac{\phi(q)}{q}|I_+|\Big(1+\exp\Big(-\frac{u}{\eta}(1+25\eta)\log(2u/\eta^3)\Big)\Big),$$

and

$$\sum_{\substack{n\in I_-\\(n,q)=1}} 1 \le \frac{\phi(q)}{q}|I_-|\Big(1-\exp\Big(-\frac{u}{\eta}(1+25\eta)\log(2u/\eta^3)\Big)\Big).$$

Deduction of Corollary 1.2. This follows immediately upon noting that $z \le (\log q)^\eta$ and replacing u/η by u.

Proof of Corollary 6.1. Take $a(n) = 1$ if $n \le q$ with $(n,q) = 1$ and $a(n) = 0$ otherwise. Recall that $\eta = \min(\alpha/3, 1/100)$. Since q has at most $\log q/\log\log q$ prime factors larger than $\log q$ we see that

$$\sum_{\substack{p|q\\p>\log q}} \frac{\log p}{p} \le 1.$$

Therefore from our assumption that $\sum_{p|q}\log p/p = \alpha\log\log q$ we may conclude that there exists $(\log q)^\eta \le z \le (\log q)/3$ such that

$$\sum_{\substack{p|q\\z^{1-\eta}\le p\le z}} \frac{1}{p} \ge \eta^2. \tag{6.2}$$

Take ℓ to be the product of the primes in $[z^{1-\eta}, z]$ which divide q, so that ℓ is a divisor of q and $\ell \le e^{z(1+o(1))} \le q^{\frac{1}{3}}$. Given $(\log q)^{\eta/2} \ge u \ge 5/\eta^2$ we obtain by (6.2) and Corollary 3.2 (we check readily that $\eta \ge z^{-1/10}$ using $\eta \ge 20 \log\log\log q/\log\log q$) that there exist points $u_\pm \in [u, u(1+22\eta)]$ such that, with $y_\pm = [z^{u_\pm}]$,

$$\sum_{\substack{n \le y_+ \\ (n,\ell)=1}} 1 \ge \Big(1 + \exp\Big(-u(1+25\eta)\log\Big(\frac{2u}{\eta^2}\Big)\Big)\Big)\frac{\phi(\ell)}{\ell} y_+, \tag{6.3a}$$

and

$$\sum_{\substack{n \le y_- \\ (n,\ell)=1}} 1 \le \Big(1 - \exp\Big(-u(1+25\eta)\log\Big(\frac{2u}{\eta^2}\Big)\Big)\Big)\frac{\phi(\ell)}{\ell} y_-. \tag{6.3b}$$

Consider now the "Maier matrices" $\mathcal{M}_\pm$ whose $(r,s)^{\text{th}}$ entry is $(R+r)\ell + s$ with $1 \le r \le R$ and $1 \le s \le y_\pm$, and $R = [q/(4\ell)]$. As usual we sum $a(n)$ as n ranges over the elements of this matrix. Using (6.1), note that the sth column contributes 0 unless $(s,\ell) = 1$ in which case it contributes $R\phi(q/\ell)/(q/\ell) + O(\tau(q))$. Thus the contribution of the matrix is

$$\Big(R\frac{\phi(q/\ell)}{q/\ell} + O(q^\varepsilon)\Big) \sum_{\substack{s \le y_\pm \\ (s,\ell)=1}} 1.$$

Corollary 6.1 follows immediately from (6.3 a,b). □

Proof of Corollary 1.1. Let $q = \prod_{p \in \mathcal{P}} p$; note that $\mathcal{A}$, the set of integers up to q without any prime factors from the set $\mathcal{P}$, is a subset of $[1,q]$ of density $\phi(\mathcal{P})/\mathcal{P} = \phi(q)/q$, which is strictly < 1 by hypothesis. Let $\ell = \prod_{\sqrt{z} \le p \le z/3,\ p \in \mathcal{P}} p$ so that $\ell \le q^{1-\delta+o(1)}$ for some fixed $\delta > 0$, and apply the argument in our proof of Corollary 6.1 above. In place of Corollary 3.2 we appeal to Corollary 3.3 (with ℓ in place of q, since the hypothesis on $\mathcal{P}$ implies that $H(\xi) \gg \mathrm{e}^\xi/\xi$), and see that for suitably large $u \le \sqrt{z}$ there exist integers $y_\pm \ge z^u$ such that

$$\sum_{\substack{n \le y_+ \\ (n,\ell)=1}} 1 \ge \Big(1 + \exp(-u(\log u + \log\log u + O(1))\Big)\frac{\phi(\ell)}{\ell} y_+,$$

and

$$\sum_{\substack{n \le y_- \\ (n,\ell)=1}} 1 \le \Big(1 - \exp(-u(\log u + \log\log u + O(1))\Big)\frac{\phi(\ell)}{\ell} y_-.$$

We conclude that for large $u \le \sqrt{z}$ there are intervals $I_\pm \subset [q/4, 3q/4]$ of length $\ge z^u$ such that

$$\sum_{\substack{n \in I_+ \\ (n,q)=1}} 1 \ge \frac{\phi(q)}{q}|I_+|\Big(1 + \exp(-u(\log u + \log\log u + O(1))\Big),$$

and

$$\sum_{\substack{n\in I_-\\(n,q)=1}} 1 \le \frac{\phi(q)}{q}|I_-|\Big(1-\exp(-u(\log u+\log\log u+O(1))\Big).$$

Finally, by Proposition 3.8 we find that we can take $y_\pm \le z^{u+2}$, provided that $u \le (1-\varepsilon)\log\log z/\log\log\log z$.

From the "fundamental lemma" of sieve theory (see [7]), it follows that these estimates are essentially optimal.

Example 6. Take $q=\prod_{p\le z} p$ and $\mathcal{A}$ to be the integers less than q that are coprime to q. We show how to tweak $\mathcal{A}$ to obtain a set $\mathcal{B}\subset[1,q]$ such that the symmetric difference $|(\mathcal{A}\backslash\mathcal{B})\cup(\mathcal{B}\backslash\mathcal{A})|$ is small, but such that $\mathcal{B}$ *is* well distributed in short intervals.

Let $k=[q/(\log q)^4]$ and divide $[1,q]$ into k intervals $[mh+1,(m+1)h]$ for $1\le m\le k$, and $h=q/k=(\log q)^4+O(1)$. For $1\le m\le k$ consider whether

$$\Big|\sum_{\substack{mh+1\le n\le (m+1)h\\(n,q)=1}} 1-\frac{\phi(q)}{q}h\Big| \le (\log q)^3, \tag{6.4}$$

holds or does not hold. If (6.4) holds then take $\mathcal{B}\cap[mh+1,(m+1)h]=\mathcal{A}\cap[mh+1,(m+1)h]$. Otherwise pick an arbitrary set of $[\phi(q)h/q]$ numbers in $[mh+1,(m+1)h]$ and take that to be $\mathcal{B}\cap[mh+1,(m+1)h]$.

By construction we see that for any interval $[x,x+y]\subset[1,q]$

$$\sum_{\substack{n\in\mathcal{B}\\x\le n\le x+y}} 1=\frac{\phi(q)}{q}y+O\Big(\frac{\phi(q)}{q}h+\frac{y}{\log q}\Big). \tag{6.5}$$

Thus $\mathcal{B}$ is well distributed in short intervals of length $y\ge(\log q)^5$, say.

Further note that $\mathcal{A}$ and $\mathcal{B}$ are quite close to each other. Indeed, from the theorem in Montgomery and Vaughan [13] we know that for integers $r\ge 1$,

$$\sum_{m\le k}\Big(\sum_{\substack{mh+1\le n\le (m+1)h\\(n,q)=1}} 1-\frac{\phi(q)}{q}h\Big)^{2r} \sim \frac{(2r)!}{2^r r!}\,q\Big(h\frac{\phi(q)}{q}\Big)^r. \tag{6.6}$$

It follows that the number of values m for which (6.4) does not hold is $\ll_r q/(\log q)^{2r}$. Therefore for any $r\ge 1$

$$|(\mathcal{A}\backslash\mathcal{B})\cup(\mathcal{B}\backslash\mathcal{A})| \ll_r q/(\log q)^r. \tag{6.7}$$

By (6.1) and (6.7) we therefore see that $\mathcal{B}$ is also well distributed in arithmetic progressions $a \pmod{\ell}$ provided $\ell\ll_r(\log q)^r$.

Now take $\ell=\prod_{\sqrt{w}\le p\le w} p=e^{(1+o(1))w}$ with $w\le z$ so that $\ell|q$. For $u\le\sqrt{w}$ but large, our usual Maier matrix argument then gives that one of the following statements holds:

(i) There exists $y \in [q/4, q]$ and $a \pmod{\ell}$ such that, with $\delta((a,\ell)=1)$ being 1 or 0 depending on whether $(a,\ell)=1$ or not,

$$\Big|\mathcal{B}(y;\ell,a) - \delta((a,\ell)=1)\frac{\phi(q/\ell)}{q}y\Big| \geq \exp(-u(\log u + \log\log u + O(1)))\frac{\phi(q/\ell)}{q}y.$$

(ii) There exists an interval $[x, x+y] \subset [1,q]$ with $y \geq w^u$ such that

$$\Big|\sum_{\substack{x\leq n\leq x+y\\ n\in\mathcal{B}}} 1 - \frac{\phi(q)}{q}y\Big| \geq \exp(-u(\log u + \log\log u + O(1)))y.$$

But from (6.5) we see that case (ii) cannot hold if $w^u \geq (\log q)^5$ and if $e^{-u(\log u+\log\log u+O(1))} \gg 1/\log q$. We conclude therefore that the distribution of $\mathcal{B}$ in arithmetic progressions is compromised, and that case (i) holds in this situation. In particular the expected asymptotic formula for $\mathcal{B}(y;\ell,a)$ is false for some $\ell \ll_\varepsilon \exp((\log q)^\varepsilon)$.

Our argument also places restrictions on the uniformity with which Montgomery and Vaughan's estimate (6.6) can hold. Given h and q with $h\phi(q)/q$ large, define η by $q/\phi(q) = (h\phi(q)/q)^\eta$. We now show that if (6.6) holds then $r \ll (\log(h\phi(q)/q))^{2+4\eta+o(1)}$.

Fix $\varepsilon > 0$. Choose L so that $h\phi(q)/q = L^{2+\varepsilon}$; then let

$$u = (1-\varepsilon)\log L/\log\log L \quad\text{and}\quad w = (\log L)^{3+4\eta+4\varepsilon}.$$

We follow the same argument as in Example 6, but replace "$(\log q)^3$" in (6.4) by "$(h\phi(q)/q)/L$", from which it follows that we replace "$y/\log q$" in (6.5) by "y/L", and that the upper bound in (6.7) is $\ll qh(2r/eL^\varepsilon)^r$. Case (ii) cannot hold in our range by (6.5). By the combinatorial sieve we know that $|\mathcal{A}(y;\ell,a) - \delta((a,\ell)=1)\phi(q/\ell)y/q| \ll 2^{\pi(z)}$ so that, since case (i) holds, $|(\mathcal{A}\backslash\mathcal{B})\cup(\mathcal{B}\backslash\mathcal{A})| \gg \phi(q)/\ell L$ in our range. By (6.7) we deduce that $e^{w+o(w)} = \ell L(q/\phi(q))h \gg (eL^\varepsilon/2r)^r$ so that $r \ll w/\log L = (\log L)^{2+4\eta+4\varepsilon}$, which implies the result.

6b. '*Wirsing sequences*'. Let $\mathcal{P}$ be a set of primes of logarithmic density α for a fixed number $\alpha \in (0,1)$; that is

$$\sum_{\substack{p\leq x\\ p\in\mathcal{P}}} \frac{\log p}{p} = (\alpha + o(1))\log x,$$

as $x \to \infty$. Let $\mathcal{A}$ be the set of integers not divisible by any prime in $\mathcal{P}$ and let $a(n) = 1$ if $n \in \mathcal{A}$ and $a(n) = 0$ otherwise. Wirsing proved (see page 417 of [18]) that

$$\mathcal{A}(x) \sim \frac{e^{\gamma\alpha}}{\Gamma(1-\alpha)}x\prod_{\substack{p\leq x\\ p\in\mathcal{P}}}\Big(1-\frac{1}{p}\Big). \tag{6.8}$$

Let h be the multiplicative function defined by $h(p) = 0$ if $p \in \mathcal{P}$ and $h(p) = 1$ if $p \notin \mathcal{P}$ and take $f_q(a) = h((a,q))$ and $\gamma_q = \prod_{p|q, p\in\mathcal{P}}(1-1/p)$. Naturally we may expect that $\mathcal{A}(x;q,a) \sim \frac{f_q(a)}{q\gamma_q}\mathcal{A}(x)$ and our work places restrictions on this asymptotic.

Let $u \geq \max(e^{2/\alpha}, e^{100})$ be fixed. Then for large x we see that the hypotheses of Theorem 2.4 are met with $z = (\log x)/3$ and $\eta = 1/\log u$. Combining Theorem 2.4 with (6.8) which shows that $\mathcal{A}(x)/x$ varies slowly (and therefore equals $(1+o(1))\mathcal{A}(y)/y$ for any $y \in (x/4, x)$), we attain the following conclusion.

COROLLARY 6.2. *For fixed $u \geq \max(e^{2/\alpha}, e^{100})$ and large x there exists $y \in (x/4, x)$ and an arithmetic progression $a \pmod{\ell}$ with $\ell \leq x(3/\log x)^u$ such that*

$$\Big|\mathcal{A}(y;\ell,a) - \frac{f_\ell(a)}{\ell\gamma_\ell}\mathcal{A}(y)\Big| \gg \exp(-u(\log u + O(\log\log u)))\frac{\mathcal{A}(y)}{\phi(\ell)}.$$

Similarly using Theorem 2.5 with $\eta = 1/\log u$ and $z = (\frac{1}{3}\log x)^{\frac{1}{M}}$ we obtain the following "uncertainty principle" showing that either the distribution of $\mathcal{A}$ in arithmetic progressions with small moduli, or the distribution in short intervals must be compromised.

COROLLARY 6.3. *Let $u \geq \max(e^{2/\alpha}, e^{100})$ be fixed and write $u = MN$ with both M and N at least 1. Then for each large x at least one of the following two statements is true.*

(i) *There exists $y \in (x/4, x)$ and an arithmetic progression $a \pmod{q}$ with $q \leq \exp((\log x)^{\frac{1}{M}})$ such that*

$$\Big|\mathcal{A}(y;q,a) - \frac{f_q(a)}{q\gamma_q}\mathcal{A}(y)\Big| \gg \exp(-u(\log u + O(\log\log u)))\frac{\mathcal{A}(y)}{\phi(q)}.$$

(ii) *There exists $y > (\frac{1}{3}\log x)^N$ and an interval $(v, v+y) \subset (x/4, x)$ such that*

$$\Big|\mathcal{A}(v+y) - \mathcal{A}(v) - y\frac{\mathcal{A}(v)}{v}\Big| \gg \exp(-u(\log u + O(\log\log u)))y\frac{\mathcal{A}(v)}{v}.$$

6c. *Sums of two squares and generalizations.*

Example 3, *revisited.* We return to Balog and Wooley's Example 3, the numbers that are sums of two squares. It is known that (see Lemma 2.1 of [1])

$$\mathcal{A}(x;q,a) = \frac{f_q(a)}{q\gamma_q}\mathcal{A}(x)\Big(1 + O\Big(\Big(\frac{\log 2q}{\log x}\Big)^{\frac{1}{5}}\Big)\Big). \tag{6.9}$$

Take q to be the product of primes between $\sqrt{\log x}$ and $\log x/\log\log x$. Using the Maier matrix method, (6.9) and our Corollary 3.3 we obtain that for fixed u and large x there exist $y_\pm \geq (\log x)^u$ and intervals $[v_\pm, v_\pm + y_\pm] \subset [x/4, x]$ such that

$$\sum_{v_+ \leq n \leq v_+ + y_+} a(n) \geq (1 + \exp(-u(\log u + \log\log u + O(1))))y_+ \frac{\mathcal{A}(x)}{x},$$

and

$$\sum_{v_- \leq n \leq v_- + y_-} a(n) \leq (1 - \exp(-u(\log u + \log\log u + O(1))))y_- \frac{\mathcal{A}(x)}{x}.$$

These are of essentially the same strength as the results in [1].

Further we also obtain that (for fixed u) there exists $y \in (x/4, x)$ and an arithmetic progression $a \pmod{\ell}$ with $\ell \leq x/(\log x)^u$ such that

$$\left|\mathcal{A}(y;\ell,a) - \frac{f_\ell(a)}{\ell\gamma_\ell}\mathcal{A}(y)\right| \geq \exp(-u(\log u + \log\log u + O(1)))\frac{\mathcal{A}(x)}{\phi(\ell)}.$$

Example 7. Let K be a number field with $[K:\mathbb{Q}] > 1$ and let R be its ring of integers. Let $C_1, \ldots, C_h$ be the ideal classes of R, and define $\mathcal{A}^{(i)}$ to be the set of integers which are the norms of integral ideals belonging to C_i. From the work of R. W. K. Odoni [14] we know that

$$\mathcal{A}^{(i)}(x) \sim c_i \frac{x}{(\log x)^{1-E(K)}}$$

where $c_i > 0$ is a constant and $E(K)$ denotes the density of the set of rational primes admitting in K at least one prime ideal divisor of residual degree 1. It is well known that $E(K) \geq 1/[K:\mathbb{Q}]$ and also we know that $E(K) \leq 1 - 1/[K:\mathbb{Q}]$ (see the charming article of J-P. Serre [16]).

We now describe what the natural associated multiplicative functions h and f_q should be. Define $\delta(n) = 1$ when n is the norm of some integral ideal in K and $\delta(n) = 0$ otherwise. Clearly $n \in \mathcal{A}^{(i)}$ for some i if and only if $\delta(n) = 1$. Naturally we would expect that

$$\sum_{\substack{n \leq x \\ p^k | n}} \delta(n) \approx \frac{\sum_{j \geq k} \delta(p^j)/p^j}{\sum_{j=0}^{\infty} \delta(p^j)/p^j} \sum_{n \leq x} \delta(n),$$

and so the natural definition of h is

$$\frac{h(p^k)}{p^k} = \frac{\sum_{j \geq k} \delta(p^j)/p^j}{\sum_{j=0}^{\infty} \delta(p^j)/p^j}.$$

Note that $h(p) = 1$ if $\delta(p) = 1$ (which happens if p has a prime ideal divisor in K of residual degree 1, and so occurs for a set of primes with density $E(K)$) and that $h(p) \leq 1/p + O(1/p^2)$ if $\delta(p) = 0$ (and this happens for a set of primes

of density $1 - E(K) > 0$). With the corresponding definition of $f_q(a)$ we may expect that for $(q, \mathcal{S}) = 1$ (for a finite set of bad primes $\mathcal{S}$ including all prime factors of the discriminant of K)

$$\mathcal{A}^{(i)}(x; q, a) \sim \frac{f_q(a)}{q\gamma_q}\mathcal{A}^{(i)}(x).$$

By appealing to standard facts on the zeros of zeta and L-functions over number fields one can prove such an asymptotic for small values of q (for example, if q is fixed). Our work shows that that this asymptotic fails if q is of size $x/(\log x)^u$ for any fixed u. We expect that one can understand the asymptotics of $\mathcal{A}^{(i)}(x; q, a)$ for appropriate small q in order also to conclude that the distribution of $\mathcal{A}^{(i)}$ in short intervals (of length $(\log x)^u$) is compromised. We also expect that similar results hold with R replaced with any order in K.

Example 8. Let k be a fixed integer, and choose r reduced residue classes $a_1, \ldots, a_r \pmod k$ where $1 \le r < \phi(k)$. Take $\mathcal{A}$ to be the set of integers not divisible by any prime $\equiv a_i \pmod k$ and take $\mathcal{S}$ to be the set of primes dividing k. Here h is completely multiplicative with $h(p) = 0$ if $p \equiv a_j \pmod k$ for some j and $h(p) = 1$ otherwise, and $f_q(a)$ is defined appropriately. This is a special case of a Wirsing sequence, and so (6.8) and Corollary 6.2 apply (we see easily that ℓ in Corollary 6.2 may be chosen coprime to k). Note also that Example 3 essentially corresponds to the case $k = 4$ and $a_1 = 3$. This also covers Example 7 in the case when K is an abelian extension.

We may apply standard techniques of analytic number theory to study $\mathcal{A}(x)$ and $\mathcal{A}(x; q, a)$. Consider the generating function $A(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ which converges absolutely in $\mathrm{Re}(s) > 1$ and satisfies the Euler product $\prod_{p \not\equiv a_i \pmod k}(1 - p^{-s})^{-1}$. Further using the orthogonality relations of characters $\psi \pmod k$ we see that

$$A(s) = \prod_{\psi \pmod k} L(s, \psi)^{\frac{1}{\phi(k)}\sum_{b \not\equiv a_i \pmod k}\overline{\psi(b)}} B(s),$$

where B is absolutely convergent in $\mathrm{Re}(s) > 1/2$. Further for a character $\chi \pmod q$ with $(q, k) = 1$ we get that

$$A(s, \chi) = \sum_{n=1}^{\infty} \frac{a(n)\chi(n)}{n^s} = \prod_{\psi \pmod k} L(s, \psi\chi)^{\frac{1}{\phi(k)}\sum_{b \not\equiv a_i \pmod k}\overline{\psi(b)}} B(s, \chi),$$

with $B(s, \chi)$ absolutely convergent in $\mathrm{Re}(s) > 1/2$. For large x, if $q \le \exp(\sqrt{\log x})$ with $(q, k) = 1$ is such that for all characters $\chi \pmod{qk}$ (primitive or not) $L(s, \chi)$ has no zeros in $\sigma \ge 1 - c/\log(qk(1 + |t|)$ then we may conclude by standard arguments that

$$\mathcal{A}(x; q, a) = \frac{f_q(a)}{q\gamma_q}\mathcal{A}(x) + O(x\exp(-C\sqrt{\log x})), \tag{6.10}$$

for some constant $1 > C > 0$. Since k is fixed we may suppose that no divisor of it is a Siegel modulus. Let $\nu_1, \ldots, \nu_t$ denote the Siegel moduli below $\exp(\sqrt{\log x})$ (see §5 for details, and note that $t \ll \log\log x$), and select a prime factor v_i for each ν_i. Choose q to be the product of primes between $\sqrt{w}$ and w with $w = (C/10)\sqrt{\log x}$, taking care to omit the primes $v_1, \ldots, v_t$ which fall in this range. Then (6.10) applies to this modulus q (which is of size $\exp((C/10 + o(1))\sqrt{\log x})$. Now, applying the Maier matrix method (and our Corollary 3.3) we deduce that for large $u \le \sqrt{w}$ there exists an interval $[v, v+y]$ in $[x/4, 3x/4]$ with $y \ge (\log x)^u$ such that

(6.11)
$$\Big|\mathcal{A}(v+y) - \mathcal{A}(v) - y\frac{\mathcal{A}(x)}{x}\Big| \gg \exp(-2u(\log u + \log\log u + O(1)))y\frac{\mathcal{A}(x)}{x}.$$

Arguing more carefully, using a zero density estimate as in Section 5, it may be possible to improve the right side of (6.11) to $\exp(-u(\log u + \log\log u + O(1)))y\frac{\mathcal{A}(x)}{x}$.

6d. *The multiplicative function $z^{\Omega(n)}$ for $z \in (0,1)$.* Take $a(n) = z^{\Omega(n)}$ where $\Omega(n)$ denotes the number of prime factors of n counted with multiplicity and z is a fixed number between 0 and 1. We take $\mathcal{S} = \emptyset$ and $h(n) = z^{\Omega(n)}$ and $f_q(a) = z^{\Omega((a,q))}$. For large x we know from a result of A. Selberg (see Tenenbaum [17]) that

$$\mathcal{A}(x) \sim x\frac{(\log x)^{z-1}}{\Gamma(z)}.$$

From Theorem 2.4 and the above, we deduce that for fixed $u \ge \max(e^{2/(1-z)}, e^{100})$ and large x there exists $y \in (x/4, x)$ and an arithmetic progression $a \pmod{\ell}$ with $\ell \le x(3/\log x)^u$ such that

$$\Big|\mathcal{A}(y;\ell,a) - \frac{f_\ell(a)}{\ell\gamma_\ell}\mathcal{A}(y)\Big| \gg \exp(-u(\log u + O(\log\log u)))\frac{\mathcal{A}(y)}{\phi(\ell)}.$$

Suppose $q \le \exp(\sqrt{\log x})$ is such that for every character $\chi \pmod q$ (primitive or not) $L(s,\chi)$ has no zeros in $\sigma \ge 1 - c/\log(q(|t|+2))$ for some constant $c > 0$. Then following Selberg's method we may see that for some $1 > C > 0$

$$\mathcal{A}(x;q,a) = \frac{f_q(a)}{q\gamma_q}\mathcal{A}(x) + O(x\exp(-C\sqrt{\log x})). \tag{6.12}$$

Let $\nu_1, \ldots, \nu_r$ be the Siegel moduli below $e^{\sqrt{\log x}}$ (see §5 for details; and note that $r \ll \log\log x$), and select one prime factor v_i for each ν_i. Choose q to be the product of primes between $\sqrt{w}$ and w for $w = (C/10)\sqrt{\log x}$, taking care to omit the primes $v_1, \ldots, v_r$ should they happen to lie in this interval. Then (6.12) applies to this modulus q, and using the Maier matrix method and appealing to Corollary 3.3 we find that for large $u \le \sqrt{w}$ there exists an

interval $[v, v+y] \subset [x/4, 3x/4]$ with $y \geq (\log x)^u$ such that

(6.13)
$$\Big|\mathcal{A}(v+y) - \mathcal{A}(v) - y\frac{\mathcal{A}(x)}{x}\Big| \gg \exp(-2u(\log u + \log\log u + O(1)))y\frac{\mathcal{A}(x)}{x}.$$

Taking greater care, using a zero density argument as in Section 5, it may be possible to improve the right side of (6.13) to

$$\gg \exp(-u(\log u + \log\log u + O(1)))y\mathcal{A}(x)/x.$$

7. An uncertainty principle for integral equations

E. Wirsing [18] observed that questions on mean-values of multiplicative functions can be reformulated in terms of solutions to a certain integral equation. We formalized this connection precisely in our paper [6] and we now recapitulate the salient details. Let $\chi : (0, \infty) \to \mathbb{C}$ be a measurable function with $\chi(t) = 1$ for $0 \leq t \leq 1$ and $|\chi(t)| \leq 1$ for all $t \geq 1$. Let $\sigma(u) = 1$ for $0 \leq u \leq 1$ and for $u > 1$ we define σ to be the solution to

$$u\sigma(u) = \int_0^u \chi(t)\sigma(u-t)dt. \tag{7.1}$$

In [6] we showed that there is a unique solution $\sigma(u)$ to (6.1) and that $\sigma(u)$ is continuous and $|\sigma(u)| \leq 1$ for all u. In fact $\sigma(u)$ is given by

$$\sigma(u) = 1 + \sum_{j=1}^{\infty} \frac{(-1)^j}{j!} I_j(u;\chi), \tag{7.2a}$$

where

$$I_j(u;\chi) = \int_{\substack{t_1,\dots,t_j \geq 1 \\ t_1+\dots+t_j \leq u}} \frac{1-\chi(t_1)}{t_1} \cdots \frac{1-\chi(t_j)}{t_j} dt_1 \cdots dt_j. \tag{7.2b}$$

The connection between multiplicative functions and the integral equation (7.1) is given by the following result which is Proposition 1 in [6].

Proposition 7.1. *Let f be a multiplicative function with $|f(n)| \leq 1$ for all n, and $f(n) = 1$ for $n \leq y$. Let $\vartheta(x) = \sum_{p \leq x} \log p$ and define*

$$\chi(u) = \chi_f(u) = \frac{1}{\vartheta(y^u)} \sum_{p \leq y^u} f(p)\log p.$$

Then $\chi(t)$ is a measurable function with $|\chi(t)| \leq 1$ for all t and $\chi(t) = 1$ for $t \leq 1$. Let $\sigma(u)$ be the corresponding unique solution to (7.1). Then

$$\frac{1}{y^u} \sum_{n \leq y^u} f(n) = \sigma(u) + O\Big(\frac{u}{\log y} + \frac{1}{y^u}\Big).$$

The converse to Proposition 7.1 also holds (see Proposition 1 (converse) of [6]) so that the study of these integral equations is entirely analogous to the study of mean-values of multiplicative functions. Translated into this context our oscillation results of Section 3 take the shape of an "uncertainty principle" which we will now describe.

We define the Laplace transform of a function $f : [0, \infty) \to \mathbb{C}$ by

$$\mathcal{L}(f, s) = \int_0^\infty f(t)e^{-st}dt.$$

If f grows at most sub-exponentially then the Laplace transform is well-defined for complex numbers s in the half-plane $\mathrm{Re}(s) > 0$. From equation (7.1) we obtain that for $\mathrm{Re}(s) > 0$

$$\mathcal{L}(u\sigma(u), s) = \mathcal{L}(\chi, s)\mathcal{L}(\sigma, s). \tag{7.3}$$

Moreover from (7.2b) we see that when $\mathrm{Re}(s) > 0$

$$s\mathcal{L}(\sigma, s) = \exp\Big(- \mathcal{L}\Big(\frac{1 - \chi(v)}{v}, s\Big)\Big). \tag{7.4}$$

Finally, observe that if $\int_1^\infty |1 - \chi(t)|/t \; dt < \infty$ then from (7.2b) it follows that $\lim_{u\to\infty} \sigma(u)$ exists and equals

$$\sigma_\infty := e^{-\eta} \quad \text{where} \quad \eta := \int_1^\infty \frac{1 - \chi(t)}{t} \; dt \; = \mathcal{L}\Big(\frac{1 - \chi(v)}{v}, 0\Big).$$

THEOREM 7.2. *Suppose $\sigma_\infty \neq 0$ is such that*

$$|\sigma(u) - \sigma_\infty| \leq \exp(-(u/A)\log u)$$

for some positive A and all sufficiently large u. Then either $\chi(t) = 1$ almost everywhere for $t \geq A$, or $\int_0^\infty \frac{|1-\chi(t)|}{t} e^{Ct}dt$ diverges for some $C \geq 0$.

We view this as an "uncertainty principle" since (by choosing $A = 1$) we have shown that both $|\chi(t) - 1|$ and $|\sigma(u) - \sigma_\infty|$ cannot be very small except in the case $\chi(t) = \sigma(u) = 1$.

Proof. Since $|\sigma(u) - \sigma_\infty| \leq \exp(-(u/A)\log u)$ for all large u (say, for all $u \geq U$) it follows that $\mathcal{L}(\sigma - \sigma_\infty, s)$ is absolutely convergent for all complex s. Therefore the identity

$$s\mathcal{L}(\sigma, s) = s\mathcal{L}(\sigma - \sigma_\infty, s) + \sigma_\infty,$$

which *a priori* holds for $\mathrm{Re}(s) > 0$, furnishes an analytic continuation of $s\mathcal{L}(\sigma, s)$ for all complex s. Suppose now that $\int_0^\infty \frac{|1-\chi(t)|}{t} e^{Ct}dt$ converges for all positive C. Then $\mathcal{L}(\frac{1-\chi(v)}{v}, s)$ is absolutely convergent for all $s \in \mathbb{C}$, and so defines a holomorphic function on $\mathbb{C}$. Hence the identity (7.4) now holds for all $s \in \mathbb{C}$.

If $\mathrm{Re}(s) = -\xi$ then

$$\begin{aligned}|s\mathcal{L}(\sigma, s)| &\le 1 + |s| \int_0^\infty |\sigma(u) - \sigma_\infty| e^{\xi u} du \\ &\le 1 + |s| \Big(\int_0^U 2e^{\xi u} du + \int_U^\infty \exp\Big(u\Big(\xi - \frac{\log u}{A}\Big)\Big) du \Big) \\ &\le 1 + |s| \Big(2(e^{U\xi} - 1)/\xi + \exp\Big(A(\xi+1) + e^{A\xi - 1}/A \Big) + 1 \Big),\end{aligned}$$

where we bounded the second integral by the sum of the two integrals $\int_0^{e^{A(\xi+1)}} + \int_{e^{A(\xi+1)}}^\infty$ with the same integrand. In the range of the first integral one uses $u(\xi - (\log u)/A) \le e^{A\xi - 1}/A$, and in the range of the second integral one uses $u(\xi - (\log u)/A) \le -u$. Therefore, by (7.4), if $\mathrm{Re}(s) \ge -\xi$ and $\mathrm{Im}(s) \ll e^\xi$ with ξ large, then

$$\mathrm{Re}\ -\mathcal{L}\Big(\frac{1-\chi(v)}{v}, s\Big) \ll e^{A\xi}.$$

We now apply the Borel-Caratheodory lemma[2] to $-\mathcal{L}(\frac{1-\chi(v)}{v}, s)$ taking the circles with center 1 and radii $r = \xi + 1$ and $R = \xi + 2$. Since

$$\Big| \mathcal{L}(\frac{1-\chi(v)}{v}, 1) \Big| \le \int_1^\infty \frac{2e^{-v}}{v} \le 1/2,$$

we deduce from the last two displayed estimates that

$$\Big| \mathcal{L}\Big(\frac{1-\chi(v)}{v}, -\xi\Big) \Big| \le \max_{|s-1| = \xi+1} \Big| \mathcal{L}\Big(\frac{1-\chi(v)}{v}, s\Big) \Big| \ll (\xi+1) e^{A\xi}.$$

On the other hand, for any $\delta > 0$,

$$\Big| \mathcal{L}\Big(\frac{1-\chi(v)}{v}, -\xi\Big) \Big| \ge \int_0^\infty \frac{1 - \mathrm{Re}\ \chi(v)}{v} e^{\xi v} dv \ge e^{(A+\delta)\xi} \int_{A+\delta}^\infty \frac{1 - \mathrm{Re}\ \chi(v)}{v} dv,$$

so that

$$\int_{A+\delta}^\infty \frac{1 - \mathrm{Re}\ \chi(v)}{v} dv \ll \xi e^{-\delta\xi}.$$

Taking $\delta = 2\log\xi/\xi$ and letting $\xi \to \infty$, we deduce that $\int_A^\infty \frac{1 - \mathrm{Re}\ \chi(v)}{v} dv = 0$; that is, $\chi(v) = 1$ almost everywhere for $v > A$. This proves the theorem.

Université de Montréal, Centre-Ville, Montréal, QC, Canada
E-mail address: andrew@dms.umontreal.ca

University of Michigan, Ann Arbor, MI
Current address: Stanford University, Stanford, CA
E-mail address: ksound@math.stanford.edu

[2]This says that for any holomorphic function f,

$$\max_{|z-z_0|=r} |f(z)| \le \frac{2R}{R-r} \max_{|z-z_0|=R} \mathrm{Re} f(z) + \frac{R+r}{R-r} |f(z_0)|$$

where $0 < r < R$.

References

[1] A. Balog and T. D. Wooley, Sums of two squares in short intervals, *Canad. J. Math.* **52** (2000), 673–694.

[2] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, New York, 1980.

[3] J. B. Friedlander and A. Granville, Limitations to the equi-distribution of primes I, *Ann. of Math.* **129** (1989), 363–382.

[4] J. B. Friedlander, A. Granville, A. Hildebrand, and H. Maier, Oscillation theorems for primes in arithmetic progressions and for sifting functions, *J. Amer. Math. Soc.* **4** (1991), 25–86.

[5] P. X. Gallagher, A large sieve density estimate near $\sigma = 1$, *Invent. Math.* **11** (1970), 329–339.

[6] A. Granville and K. Soundararajan, The spectrum of multiplicative functions, *Ann. of Math.* **153** (2001), 407–470.

[7] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, New York, 1974.

[8] R. R. Hall, Halving an estimate obtained from Selberg's upper bound method, *Acta Arith.* **25** (1974), 347–351.

[9] A. Hildebrand and H. Maier, Irregularities in the distribution of primes in short intervals, *J. Reine Angew. Math.* **397** (1989), 162–193.

[10] C. Hooley, On the difference of consecutive numbers prime to n, *Acta Arith.* **8** (1962/63), 343–347.

[11] H. Maier, Primes in short intervals, *Michigan Math. J.* **32** (1985), 221–225.

[12] J. Matousek and J. Spencer, Discrepancy in arithmetic progressions, *J. Amer. Math. Soc.* **9** (1996), 195–204.

[13] H. L. Montgomery and R. C. Vaughan, On the distribution of reduced residues, *Ann. of Math.* **123** (1986), 311–333.

[14] R. W. K. Odoni, On the norms of algebraic integers, *Mathematika* **22** (1975), 71–80.

[15] K. F. Roth, Remark concerning integer sequences, *Acta Arith.* **9** (1964), 257–260.

[16] J-P. Serre, On a theorem of Jordan, *Bull. Amer. Math. Soc.* **40** (2003), 429–440.

[17] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, *Cambridge Stud. in Adv. Math.* **46**, Cambridge Univ. Press, Cambridge, U.K., 1995.

[18] E. Wirsing, Das asymptotische verhalten von Summen über multiplikative Funktionen II, *Acta Math. Acad. Sci. Hung.* **18** (1967), 411–467.

(Received June 1, 2004)