Ann. Sci. Math. Québec **36**, No 1, (2012), 1–25

MULTIPLICATIVE FUNCTIONS IN ARITHMETIC PROGRESSIONS

ANTAL BALOG, ANDREW GRANVILLE AND KANNAN SOUNDARARAJAN

Dedicated to Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. Nous développons une théorie des fonctions multiplicatives (avec les valeurs sur ou à l'intérieur du cercle d'unité) en progressions arithmétiques analogues à la théorie bien connue des nombres premiers en progressions arithmétiques.

ABSTRACT. We develop a theory of multiplicative functions (with values inside or on the unit circle) in arithmetic progressions analogous to the well-known theory of primes in arithmetic progressions.

1. Introduction

1.1. Historical preliminaries

A central focus of multiplicative number theory has been the question of how primes are distributed in arithmetic progressions (see *e.g.* [4]): There are $\pi(x)$ primes up to x, of which $\pi(x;q,a)$ belong to the arithmetic progression $a \pmod q$, and

$$\pi(x;q,a) \sim \frac{\pi(x)}{\phi(q)} \tag{1.1}$$

as $x \to \infty$, whenever $(a,q)=1$. Here $\phi(q)$ stands for the Euler ϕ–function. In other words, the primes are eventually equidistributed amongst the plausible arithmetic progressions $(\mathrm{mod}\, q)$. In applications it is important to know how big x must be, as a function of q, for (1.1) to hold. Unconditionally we can only prove (1.1) for all q when x is enormous, larger than exponential of a (small) power of q, whereas we believe it holds when x is just a little bigger than q, that is $x > q^{1+\epsilon}$. We can prove a far better range for x if we ask whether (1.1), or a weakened version of it, holds for most q: Fix $\epsilon > 0$. There exists A such that

$$\left| \pi(x;q,a) - \frac{\pi(x)}{\phi(q)} \right| \le \epsilon\, \frac{\pi(x)}{\phi(q)} \tag{1.2}$$

for all $(a,q)=1$ and for all $q \le x^{1/A}$, except *possibly* those q that are multiples of some *exceptional* modulus r (which depends only on ϵ and x). We do not believe that any such r exists, but if it does then $r \ge \log x$, so the result (1.2) applies to most q. Moreover, if q is divisible by r we can still get an understanding of the distribution of

Reçu le 13 janvier 2010 et, sous forme définitive, le 30 octobre 2010.

primes in the arithmetic progressions $(\bmod\, q)$, albeit rather different from what we had expected: There exists a real character $\psi \pmod r$ such that

$$\left(\pi(x;q,a) - \frac{\pi(x)}{\phi(q)}\right) = \psi(a)\left(\pi(x;q,1) - \frac{\pi(x)}{\phi(q)}\right) + O\left(\epsilon\,\frac{\pi(x)}{\phi(q)}\right), \tag{1.3}$$

whenever $(a,q)=1$ and r divides q, with $q \le x^{1/A}$.

In the literature (*e.g.* [3, 15]) exceptional moduli are derived and discussed in terms of L-functions and egregious counterexamples to the Generalized Riemann Hypothesis known as Siegel-Landau zeros. Our goal here is to develop this same theory without L-functions and in a way that generalizes to a wide class of functions. The first step of our approach comes in recognizing that results about the distribution of prime numbers can usually be rephrased as results about mean values of the Möbius function $\mu(n)$ or the Liouville function $\lambda(n)$, both multiplicative functions (see, *e.g.* [23]), as we run through certain sequences of integers n. To see this, write the von Mangoldt function as

$$\Lambda(n) = \sum_{d\,|\,n} \mu(d)\log(n/d)$$

(where $\Lambda(p^e) = \log p$ for prime p and integer $e \ge 1$, and $\Lambda(n) = 0$ otherwise), which is deduced from $\log = 1 * \Lambda$ by Möbius inversion. Now $\log$ is a very "smooth" function, so that estimates for the sum of $\Lambda(n)$ for n in an arithmetic progression, follow from estimates for the mean value of μ in certain related arithmetic progressions. Thus (1.1) is equivalent to the statement that the mean value of μ in any arithmetic progression $(\bmod\ q)$ tends to 0 as we go further and further out in the arithmetic progression [23]; and indeed (1.2) is tantamount to the fact that

$$\left|\sum_{\substack{n\le x\\ n\equiv a \pmod q}} \mu(n)\right| \le \epsilon\,\frac{x}{q} \tag{1.2b}$$

for all $(a,q)=1$ for all $q \le x^{1/A}$, except those q that are multiples of some exceptional modulus r.

If q *is* a multiple of r then the corresponding result for $\mu(n)$ is more enlightening than (1.3). It is well known that if (1.3) holds then $L(1,\psi)$ is surprisingly small, which can hold only if $\psi(p) = -1$ for many of the "small" primes p. In other words we have $\mu(p) = \psi(p)$ for many small primes p, which implies that $\mu(n)$ displays a bias towards looking like $\psi(n)$. But then $\mu(n)$ tends to look like $\psi(n) = \psi(a)$ for $n \equiv a \pmod q$, so its mean value over such integers n tends to be like $\psi(a)$. All of these vagaries can be made more precise, but for now we content ourselves with the appropriate analogy to (1.3):

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} \mu(n) \;=\; \psi(a) \sum_{\substack{n\le x\\ n\equiv 1 \pmod q}} \mu(n) + O\left(\epsilon\,\frac{x}{q}\right) \tag{1.3b}$$

whenever $(a,q)=1$ and r divides q, with $q \le x^{1/A}$. The key point is to see that μ *pretends* to be ψ, at least at small values of the argument in this exceptional case. This notion generalizes very well.

This paper is concerned with determining, for multiplicative functions f such that $|f(n)| \le 1$ for all n, estimates for the mean values

$$\frac{1}{x/q} \sum_{\substack{n\le x \\ n\equiv a \pmod q}} f(n) \tag{1.4}$$

when $(a,q)=1$. We will show that for any fixed $\epsilon>0$ there exists A such that

$$\Bigg| \sum_{\substack{n\le x \\ n\equiv a \pmod q}} f(n) \Bigg| \le \epsilon \, \frac{x}{q} \tag{1.2c}$$

for all $(a,q)=1$ for all $q\le x^{1/A}$, except possibly those q that are multiples of some exceptional modulus r. Moreover, if such a modulus r exists, there is a character $\psi \pmod r$ such that if q is a multiple of r with $q\le x^{1/A}$, then

$$\sum_{\substack{n\le x \\ n\equiv a \pmod q}} f(n) \;=\; \psi(a) \sum_{\substack{n\le x \\ n\equiv 1 \pmod q}} f(n) + O\left(\epsilon \, \frac{x}{q}\right) \tag{1.3c}$$

whenever $(a,q)=1$.

There are examples of f for which exceptional characters *do* exist: indeed we simply let $f(n)=\psi(n)$ or even $f(n)=\psi(n)n^{it}$ for some $|t|\ll 1/\epsilon$. Thus, in this theory, exceptional characters take on a different role in that they exist for any f which pretends to be a function of the form $\psi(n)n^{it}$. This pretentiousness can be made more precise in terms of the following *distance function* $\mathbb{D}=\mathbb{D}_1$ between two multiplicative functions f and g with $|f(n)|,|g(n)|\le 1$:

$$\mathbb{D}_r(f(n),g(n);x)^2 := \sum_{\substack{p\le x \\ p\nmid r}} \frac{1-\text{Re } f(p)\overline{g(p)}}{p} \, .$$

This distance function is particularly useful since it satisfies the triangle inequality

$$\mathbb{D}_q(f_1(n),g_1(n);x)+\mathbb{D}_r(f_2(n),g_2(n);x) \ge \mathbb{D}_{qr}((f_1f_2)(n),(g_1g_2)(n);x),$$

which may be proved by squaring both sides and using the Cauchy-Schwarz inequality (see Lemma 3.1 of [15], or the general discussion in [16]).

The main thrust of this paper has been anticipated by Elliott [7]; indeed he obtains stronger results than we do here (we will give details below). However our method of proof is somewhat different, arguably easier, so it seems to be worth recording. In a further article, the second two authors [17] re-develop Elliott's original argument and are able to get best possible results in several of the results mentioned below.

1.2. More precise results

Throughout f is a multiplicative function with $|f(n)|\le 1$ for all n, and $x\ge Q$, $A\ge 1$ are given. Of all primitive characters with conductor below Q, let $\psi \pmod r$ be that character for which

$$\min_{|t|\le A} \mathbb{D}_r(f(n),\psi(n)n^{it};x)^2 \tag{1.5}$$

is a minimum.[1] Let $t = t(x, Q, A)$ denote a value of t that gives the minimum value in (1.5)

Theorem 1.1. *With the notation as above we have, when $a \pmod q$ is an arithmetic progression with $(a, q) = 1$ and $q \le Q$, that*

$$\sum_{\substack{n \le x \\ n \equiv a \pmod q}} f(n) \ll \text{Error}(x, q, A) \tag{1.2d}$$

if r does not divide q, and

$$\sum_{\substack{n \le x \\ n \equiv a \pmod q}} f(n) = \frac{\psi(a)}{\phi(q)} \sum_{\substack{n \le x \\ (n,q)=1}} f(n)\overline{\psi(n)} + O\big(\text{Error}(x, q, A)\big) \tag{1.3d}$$

if r does divide q. Here we may take either $Q = x^{1/A}$ with $\log x \ge A \ge 20$ and

$$\text{Error}(x, q, A) = \frac{x}{q} \cdot \frac{1}{\sqrt{\log A}},$$

or $Q = \log x$ and $A = \log^2 x$ with

$$\text{Error}(x, q, \log^2 x) = \frac{x}{q(\log x)^{1/3+o(1)}} + \frac{x}{(\log x)^{1-o(1)}}.$$

Throughout let χ_0 be the primitive character mod q; and here let $\chi = \chi_0$ if r does not divide q, and $\chi = \psi\chi_0$ if r does divide q. Then (1.2d) and (1.3d) can be expressed in one equation as

$$\sum_{\substack{n \le x \\ n \equiv a \pmod q}} f(n) \; - \; \chi(a) \sum_{\substack{n \le x \\ n \equiv 1 \pmod q}} f(n) \ll \text{Error}(x, q, A). \tag{1.3e}$$

We can deduce the following bound from Corollary 2.2 below, which is useful in bounding (1.3d) of Theorem 1.1:

$$\frac{1}{\phi(q)} \sum_{\substack{n \le x \\ (n,q)=1}} f(n)\overline{\psi(n)} \ll \frac{x}{q}\left((1 + \mathbb{D}_q(f(n), \psi(n)n^{it}; x)^2) e^{-\mathbb{D}_q(f(n), \psi(n)n^{it}; x)^2} + \frac{1}{(\log x)^{1/4}} \right). \tag{1.6}$$

We see that (1.2c) and (1.3c) follow immediately from this theorem. The theorem gives more than (1.2c) and (1.3c) as we get results here with some uniformity, and somewhat stronger results when x is larger than e^q.

The constant "1/3" in Theorem 1.1 cannot be improved, as we will show in [17]. To explain the idea we need to construct a multiplicative function f for which there are two different characters χ_j, $j = 1, 2$ such that

$$\mathbb{D}(f(n), \chi_j(n); x)^2 \sim \frac{1}{3} \log\log x.$$

[1] If there are several possibilities for ψ, simply pick one of those choices.

(In [17] we show that no other characters contribute much in Theorem 1.1, so that this construction indeed works.) To do this let χ be any character of order 3, and define $f(p) = 1$ when $\chi(p) = 1$, and $f(p) = -1$ otherwise. Then

$$\mathbb{D}(f(n), \chi(n); x)^2 = \mathbb{D}(f(n), \chi^2(n); x)^2 = \sum_{p \le x} \frac{2 - \chi(p) - \overline{\chi}(p)}{p} \sim \frac{1}{3} \log\log x$$

as required.

Elliott [7] gave an exponentially stronger version of our Theorem 1.1 when x is small, obtaining

$$\text{Error}(x, q, A) = \frac{x}{q} \cdot \frac{1}{A^{1/4-\epsilon}}$$

uniformly for $A \gg 1$. (Actually he proved something a little more complicated but our claim can easily be deduced from [7] and the ideas herein.) In [17] we will improve the constant "$1/4$" and further develop Elliott's ideas. It is worth noting that the same circle of ideas allowed Elliott to give a new proof of Linnik's Theorem [8] without explicit mention of zeros of Dirichlet L-functions.

Otherwise earlier work in this area focused on the equidistribution of $f(n)$ in arithmetic progressions; that is, on obtaining bounds for

$$\sum_{\substack{n \le x \\ n \equiv a \pmod q}} f(n) - \frac{1}{\phi(q)} \sum_{\substack{n \le x \\ (n,q)=1}} f(n) \tag{1.7}$$

whenever $(a, q) = 1$. Following Elliott [7] we now know that it is necessary to change focus, to key in on how "pretentious" the given characters are, since Theorem 1.1 implies that (1.7) will not necessarily be small for moduli q divisible by an exceptional modulus r (in other words, the "expected" asymptotics can be incorrect). This issue can be seen in two of the older key articles in this subject. Elliott [4, 5] showed that (1.7) is $\ll x(\log\log x/\log x)^{\frac{1}{8}}$ for all q except possibly for multiples of a certain exceptional modulus r: note that this is non-trivial only in the range $q \le (\log x)^{\frac{1}{8}+o(1)}$. Hildebrand [18] showed that (1.7) is $\ll x/(q\sqrt{\log A})$ for all $q \le x^{1/A}$ except possibly for the multiples of at most two exceptional moduli r and r'. Our result improves both of these, giving the same bound on (1.7) in the same range as Hildebrand, but at worst in terms of one exceptional moduli, and also understanding what happens when q is divisible by the (putative) exceptional modulus. Our proof derives from that of Hildebrand – our improvements here stem more from moving our focus away from bounding (1.7), to classifying when (1.4) can be large, rather than from any particular technical innovations.

One can see many of the ideas in this paper, and particularly the dichotomy between the two cases, appearing in work on elementary proofs of the prime number theorem. In particular Selberg [22] essentially shows that there is no exceptional modulus by giving (what is equivalent to) an elementary proof that the minimum in (1.5) cannot be too small. This is developed in [11] more along the lines given here.

Daboussi and Delange [3] determined when

$$\lim_{x\to\infty} \frac{1}{x/q} \sum_{\substack{n\le x\\ n\equiv a \pmod q}} f(n) \tag{1.8}$$

exists, for a given progression $a \pmod q$ with $(a,q)=1$. If $f(n)=n^{it}$ for some $t\neq 0$, or $\psi(n)n^{it}$ for some character $\psi \pmod q$ then (1.8) evidently does not exist; or even when $f(n)$ pretends to be $\psi(n)n^{it}$. Otherwise it does:

Corollary 1.2. *If f is unpretentious, that is $\mathbb{D}(f(n),\psi(n)n^{it};\infty)=\infty$ for all characters ψ and real numbers t, then*

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} f(n) = o(x) \tag{1.9}$$

as $x\to\infty$, for any $a \pmod q$ with $(a,q)=1$. If there does exist a primitive character $\psi \pmod r$ and a real number t for which $\mathbb{D}(f(n),\psi(n)n^{it};\infty)<\infty$, then ψ and t are unique. In this case (1.9) still holds if r does not divide q. However, if r divides q then

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} f(n) = \big(1+o(1)\big)\frac{\psi(a)x^{1+it}}{q(1+it)}\prod_{p\nmid q}\Big(1-\frac{1}{p}\Big)\Big(1+\frac{f(p)\overline{\psi(p)}}{p^{1+it}}+\frac{f(p^2)\overline{\psi(p^2)}}{p^{2+2it}}+\dots\Big)$$

as $x\to\infty$. In particular if f is real-valued and χ is that real character $\pmod q$ for which

$$\prod_{p}\Big(1-\frac{1}{p}\Big)\Big(1+\frac{f(p)\chi(p)}{p}+\frac{f(p^2)\chi(p^2)}{p^2}+\dots\Big)$$

is maximized,[2] *then*

$$\lim_{x\to\infty}\frac{1}{x/q}\sum_{\substack{n\le x\\ n\equiv a \pmod q}} f(n) \;=\; \chi(a)\prod_{p\nmid q}\Big(1-\frac{1}{p}\Big)\Big(1+\frac{f(p)\chi(p)}{p}+\frac{f(p^2)\chi(p^2)}{p^2}+\dots\Big).$$

1.3. Mean values of multiplicative functions, twisted by Dirichlet characters

Traditionally one estimates mean values of functions in an arithmetic progression by using characters, as in the identity

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} f(n) = \frac{1}{\phi(q)}\sum_{\chi \pmod q}\chi(a)\sum_{n\le x} f(n)\overline{\chi}(n)\,. \tag{1.10}$$

We therefore give estimates on such characters sums.

[2]Note that $|\prod_{p\le x}(1-1/p)(1+g(p)/p+g(p^2)/p^2+\dots)| \asymp \exp(-\mathbb{D}(1,g(n);x)^2)$.

Theorem 1.3. *Define ψ as above. For fixed $Q \le \sqrt{x}$ and $A = \log^2 x$ the estimate*

$$\sum_{n\le x} f(n)\overline{\chi}(n) \ll x\Big(\frac{\log Q}{\log x}\Big)^{\frac{1}{20}}$$

holds for all characters χ of conductor $q \le Q$, except perhaps those induced from ψ. Moreover the estimate

$$\sum_{n\le x} f(n)\overline{\chi}(n) \ll \frac{x}{(\log x)^{1/3+o(1)}}$$

holds for all characters χ of conductor $q \le \log x$, except perhaps those induced from ψ.

When q is small compared to x (that is $q \le \log x$) we may obtain good estimates on (1.4) by using Theorem 1.3 in (1.10). Moreover Theorem 1.3 for large moduli q suggests that Theorem 1.1 should hold for these moduli, but deriving this from (1.10) is not straightforward since many characters are now involved.

We now record one more consequence of this circle of ideas. Let f be a real-valued completely multiplicative function with $|f(n)| \le 1$ for all n. Proving a conjecture of Hall, Heath-Brown and Montgomery, Granville and Soundararajan showed in [13] that

$$\sum_{n\le x} f(n) \ge (\delta_1 + o(1))x,$$

uniformly for all f, where $o(1) \to 0$ as $x \to \infty$, and

$$\delta_1 = 1 - 2\log(1+\sqrt{e}) + 4\int_1^{\sqrt{e}} \frac{\log t}{t+1}dt = -0.656999\dots$$

Further this lower bound is best possible, and is attained when $f(\ell) = 1$ for all primes $\ell \le x^{1/(1+\sqrt{e})}$, and $f(\ell) = -1$ for $x^{1/(1+\sqrt{e})} < \ell \le x$. For any totally multiplicative function g with each $g(\ell) = 1$ or -1 and any x, there exists infinitely many primes p for which $\left(\frac{\ell}{p}\right) = g(\ell)$ for all primes $\ell \le x$, as may be proved using quadratic reciprocity and Dirichlet's theorem for primes in arithmetic progression. Thus taking $g = f$ we see that there exist primes p such that at least 17.15% of the integers below x are quadratic residues $\pmod p$. Here 17.15% is an approximation to δ_0, and this constant $\delta_0 = (1+\delta_1)/2 = 0.1715\dots$ is best possible. We now give a generalization of this result to arithmetic progressions.

Corollary 1.4. *Let $a \pmod q$ be a progression with $(a,q) = 1$. Then*

$$\liminf_{x\to\infty} \left\{ \inf_{\substack{p\\ p\nmid q}} \frac{1}{x/q} \sum_{\substack{n\le x\\ n\equiv a \pmod q}} \left(\frac{n}{p}\right) \right\} = \begin{cases} \delta_1 & \text{if } a \equiv \square \pmod q, \\ -1 & \text{if } a \not\equiv \square \pmod q. \end{cases}$$

Colloquially, if $a \equiv \square \pmod q$ then at least 17.15% of the integers $n \le x$ such that $n \equiv a \pmod q$ are quadratic residues $\pmod p$ for any prime p.

2. Hallowed Halász

Our main results rest on the large sieve and development of Halász's pioneering results on mean values of multiplicative functions, given here after incorporating significant refinements due to Montgomery and also Tenenbaum [24] (and see [14] for an explicit version).

Theorem 2.1 (Halász). *For any $T \geq 1$ we have*

$$\frac{1}{x}\sum_{n\leq x} f(n) \ll \max_{|t|\leq T} \Big(1+\mathbb{D}(f(n),n^{it};x)^2\Big)e^{-\mathbb{D}(f(n),n^{it};x)^2} + \frac{1}{\sqrt{T}}\,.$$

Halász's result shows that if the mean value of f is large, then $f(p)$ pretends to be p^{it} for some small value of t, the quantity $\mathbb{D}$ giving an appropriate measure of the distance between $f(p)$ and the values p^{it}. Note that if $f(p) = p^{it}$ then the mean value of f is indeed large since $\sum_{n\leq x} n^{it} \sim x^{1+it}/(1+it)$ as $x\to\infty$.

We need the following consequence of Theorem 2.1.

Corollary 2.2. *For $1 \leq T \leq (\log x)^{\frac{1}{2}}$ select t as in Theorem 2.1. If r is an integer, smaller than or equal to $\sqrt{x}$, then*

$$\left(\frac{1}{\frac{\phi(r)}{r}\,x}\right)\sum_{\substack{n\leq x\\(n,r)=1}} f(n) \ll \Big(1+\mathbb{D}_r(f(n),n^{it};x)^2\Big)e^{-\mathbb{D}_r(f(n),n^{it};x)^2} + \frac{1}{\sqrt{T}}\,.$$

Halász's theorem allows us to estimate $\sum_{n\leq x} f(n)\overline{\chi}(n)$, and deduce that this mean value is small unless f pretends to be $\chi(p)p^{it}$ for some small t. We will show in Lemma 3.1 below that f can pretend to be $\chi(p)p^{it}$ for at most one character $\chi \pmod q$ provided q is not too large, and hence Halász's theorem implies Theorem 1.3 for large moduli q.

Proving an old conjecture of Erdős and Wintner, Wirsing [25] showed that every real-valued multiplicative function f with $|f(n)| \leq 1$ has a mean value; and it is natural to ask whether this holds as n ranges over an arithmetic progression: that is, whether (1.8) exists? We determined this mean value in Corollary 1.2 above, and then gave the analogy to Wirsing's result for arithmetic progressions. These results rest on a further beautiful result of Halász, which gives a qualitative version of Theorem 2.1.[3]

Theorem 2.3 (Halász). *If $\mathbb{D}(f(n),n^{it};\infty) < \infty$ for some real number t, then*

$$\sum_{n\leq x} f(n) = \big(1+o(1)\big)\,\frac{x^{1+it}}{1+it}\prod_p\Big(1-\frac{1}{p}\Big)\Big(1+\frac{f(p)p^{-it}}{p}+\frac{f(p^2)p^{-2it}}{p^2}+\dots\Big),$$

as $x\to\infty$, where the $o(1)\to 0$ in a manner that depends on f. If $\mathbb{D}(f(n),n^{it};\infty)=\infty$ for all t then $\sum_{n\leq x} f(n) = o(x)$ as $x\to\infty$

[3] Although unrelated to the main topic of this paper, we take this opportunity to mention a beautiful, but not widely known consequence of these results of Halász and Wirsing. Let G be a finite abelian group, and let $f:\mathbb{N}\to G$ be multiplicative. Then for any $g\in G$ the density $\lim_{x\to\infty}\frac{1}{x}\#\{n\leq x : f(n)=g\}$ exists! This is stated as a Conjecture "of the sixteen year old Hungarian mathematician I. Ruzsa" by Erdős [9].

Let S be a subset of the unit disc such that $|\arg(1-z)| \leq \theta < \pi/2$ for all $z \in S$ (here we take the argument to always be between $-\pi$ and π). We can also deduce from Theorem 2.3 that if f is such that $f(p) \in S$ for all p, then the limit in (1.8) exists (extending Theorem 1.3).

Proof of Corollary 2.2. By Theorem 4 of [14] and the last two displayed equations in the proof of Corollary 3 of [14],[4] we have, for t selected with $\mathbb{D}_r(f(n), n^{it}; x)$ minimal and $d \leq \sqrt{x}$,

$$\sum_{n \leq x/d} f(n) = \frac{1}{d^{1+it}} \sum_{n \leq x} f(n) + O\left(\frac{x}{d} \, \frac{\log \log x}{(\log x)^{2-\sqrt{3}}} \right).$$

We deduce, from the combinatorial sieve that, for $r \leq \sqrt{x}$,

$$\begin{aligned} &\frac{r}{\phi(r)} \sum_{\substack{n \leq x \\ (n,r)=1}} f(n) \\ &\quad = \prod_{p|r} \left(1 - \frac{f(p)}{p^{1+it}}\right) \left(1 - \frac{1}{p}\right)^{-1} \sum_{n \leq x} f(n) + O\left(\left(\frac{r}{\phi(r)}\right)^2 x \, \frac{\log \log x}{(\log x)^{2-\sqrt{3}}} \right). \end{aligned}$$

There is no loss of generality in setting $f(p) = p^{it}$ for each prime p dividing r, and so we deduce the result since $2 - \sqrt{3} > 1/4$. $\square$

3. Pretentious characters are repulsive

We show that f cannot pretend to be two different functions of the form $\psi(n)n^{it}$:

Lemma 3.1. *For each primitive character ψ with conductor below $\log x$ select $|t| \leq \log^2 x$ for which $\mathbb{D}(f(n), \psi(n)n^{it}; x)$ is minimal, and then label these pairs so that (ψ_j, t_j) is that pair which gives the j-th smallest distance $\mathbb{D}(f(n), \psi_j(n)n^{it_j}; x)$. Let r_j be the conductor of ψ_j. For each $j \geq 1$ we have*

$$\mathbb{D}_{r_j}(f(n), \psi_j(n)n^{it_j}; x)^2 \geq \left(1 - \frac{1}{\sqrt{j}}\right) \log \log x + O\left(\sqrt{\log \log x}\right).$$

Proof. This is essentially Lemma 3.4 of [16], except that there we dealt with the case where f itself was a character, and took all $t_j = 0$. The same proof applies, and

[4] We take this opportunity to correct an error in the statement of those two equations: in each, one should divide the sum on the right side of the equation by the number of terms in the sum.

for completeness we give the details. Note that

$$\begin{aligned}\mathbb{D}(f(n),\psi_j(n)n^{it_j};x)^2 &\geq \frac{1}{j}\sum_{k=1}^{j}\mathbb{D}(f(n),\psi_k(n)n^{it_k};x)^2\\ &\geq \frac{1}{j}\sum_{p\leq x}\frac{1}{p}\sum_{k=1}^{j}\left(1-\mathrm{Re}f(p)\overline{\psi_k(p)p^{it_k}}\right)\\ &\geq \frac{1}{j}\sum_{p\leq x}\frac{1}{p}\Big(j-\Big|\sum_{k=1}^{j}\psi_k(p)p^{it_k}\Big|\Big).\end{aligned}$$

By Cauchy-Schwarz we have that

$$\Big(\sum_{p\leq x}\frac{1}{p}\Big|\sum_{k=1}^{j}\psi_k(p)p^{it_k}\Big|\Big)^2 \leq \Big(\sum_{p\leq x}\frac{1}{p}\Big)\Big(\sum_{p\leq x}\frac{1}{p}\Big|\sum_{k=1}^{j}\psi_k(p)p^{it_k}\Big|^2\Big).$$

The first factor above is equal to $\log\log x + O(1)$, while the second term is bounded above by

$$\sum_{p\leq x}\frac{1}{p}\Big(j+\sum_{\substack{1\leq k,\ell\leq j\\ k\neq \ell}}\psi_k(p)\overline{\psi_\ell(p)}p^{i(t_k-t_\ell)}\Big) = j\log\log x + O(j^2),$$

upon using the prime number theorem in arithmetic progressions. For the transition from $\mathbb{D}$ to $\mathbb{D}_r$ simply note that $\sum_{p|r} 1/p \ll \log\log\log\log x$. The Lemma follows. □

Corollary 3.2. *If m is a positive integer for which f^m is real-valued and*

$$\mathbb{D}(f(n),\psi(n)n^{it};x)^2 \leq \frac{1}{16m^2}\log\log x$$

with $|t| \leq \frac{1}{m}\log^2 x$, then ψ^m is real and $|t| \ll \frac{1}{m\sqrt{\log x}}$.

Proof. Let $m = 1$. Taking complex conjugates we have

$$\mathbb{D}(f(n),\psi(n)n^{it};x) = \mathbb{D}(f(n),\overline{\psi}(n)n^{-it};x).$$

By Lemma 3.1 this is impossible unless $\overline{\psi} = \psi$, that is ψ is real. Now, by the triangle inequality we have

$$\mathbb{D}(f(n)^2, n^{2it};x) \leq 2\mathbb{D}(f(n),\psi(n)n^{it};x).$$

As $f^2 \geq 0$ we have

$$\mathbb{D}(f(n)^2, n^{2it};x)^2 \geq \sum_p 1/p$$

where the sum is over those primes $p \leq x$ with $\cos(2t\log p) < 0$. Since we get the "expected" number of primes in intervals $[y, y+y^{1-\delta}]$ for some fixed $\delta > 0$, we can deduce that

$$\sum_p \frac{1}{p} \geq \frac{1}{2}\Big(\log\log x - \log(\max\{1/|t|, \log|t|\}) + O(1)\Big)$$

for $|t| \log x \geq 1$, which implies that $|t| \ll 1/\sqrt{\log x}$, as required. For larger m we use the triangle inequality to note that

$$\mathbb{D}(f(n)^m, \psi^m(n)n^{imt}; x) \leq m\mathbb{D}(f(n), \psi(n)n^{it}; x)$$

and the result then follows from the $m = 1$ case. □

Lemma 3.3. *With the hypothesis of Lemma 3.1, we have*

$$\mathbb{D}_{r_2}(f(n), \psi_2(n)n^{it_2}; x)^2 \geq \left(\frac{1}{3} + o(1)\right) \log\log x\,.$$

Proof. The proof of Lemma 3.1 gives

$$\mathbb{D}(f(n), \psi_2(n)n^{it_2}; x)^2 \geq \sum_{p \leq x} \frac{1}{p}\Big(1 - \frac{1}{2}\Big|\sum_{k=1}^{2} \psi_k(p)p^{it_k}\Big|\Big) = \sum_{p \leq x} \frac{1}{p}\Big(1 - \frac{1}{2}\Big|1 + \chi(p)p^{it}\Big|\Big),$$

taking $\chi = \psi_2\overline{\psi_1}$ and $t = t_2 - t_1$. By the prime number theorem for arithmetic progressions, this equals

$$\frac{1}{\phi(q)} \sum_{\substack{a \pmod q \\ (a,q)=1}} \int_1^{\log x} \Big(1 - \frac{1}{2}\Big|1 + \chi(a)e^{itv}\Big|\Big) \frac{\mathrm{d}v}{v} + o(\log\log x)\,.$$

If χ has order $m > 1$ then there are exactly $\phi(q)/m$ values of $j \pmod m$ for which $\chi(a) = e^{2i\pi j/m}$, and so our integral equals, taking $v = 2u$,

$$\frac{1}{m}\sum_{j=0}^{m-1} \int_1^{\log x} \Big(1 - \Big|\cos(tu + \pi j/m)\Big|\Big) \frac{\mathrm{d}u}{u} + o(\log\log x)\,. \tag{3.1}$$

Now consider $\int_1^{\log x} |\cos(tu + \beta)| du/u$ for arbitrary β. If $u \leq \epsilon/t$ then

$$\cos(tu + \beta) = \cos(\beta) + O(\epsilon)\,.$$

The contribution of u in the range $\epsilon/t < u < 1/(\epsilon t)$ to the integral is $O(1)$. For $u \geq 1/(\epsilon t)$ we cut the range up into intervals $[U, U + 2\pi/t)$, and use the fact that $1/u = 1/U + O(1/U^2 t)$, to obtain

$$\int_U^{U+2\pi/t} |\cos(tu + \beta)| \frac{\mathrm{d}u}{u} = \int_U^{U+2\pi/t} \left\{\frac{1}{2\pi}\int_{w=0}^{2\pi} |\cos w| dw + O(1/tu)\right\} \frac{\mathrm{d}u}{u}\,.$$

The total error that arises here is $\ll \int_{u \geq 1/(\epsilon t)} du/(tu^2) \ll \epsilon$. We deduce that (3.1) equals $\log\log x$ times

$$\alpha \cdot \frac{1}{2\pi}\int_{w=0}^{2\pi} (1 - |\cos w|) dw + (1 - \alpha) \cdot \frac{1}{m}\sum_{j=0}^{m-1} (1 - |\cos(\pi j/m)|) + o(1)$$

for some α in the range $0 \leq \alpha \leq 1$. Now

$$\frac{1}{2\pi}\int_{w=0}^{2\pi} (1 - |\cos w|) dw = 1 - \int_{-1/2}^{1/2} \cos(\pi\theta) d\theta = 1 - 2/\pi\,.$$

Moreover,

$$1 - \frac{1}{m} \sum_{-m/2<j\le m/2} \cos(\pi j/m) = \begin{cases} 1 - 1/(m\sin(\pi/2m) & \text{if } m \text{ is odd,} \\ 1 - 1/(m\tan(\pi/2m) & \text{if } m \text{ is even.} \end{cases}$$

The minimum occurs for $m = 3$, and the result follows. □

Our next lemma (which is essentially Proposition 7 of [16]) formulates a similar repulsion principle involving characters of substantially larger conductors, at the cost of obtaining a smaller separation.

Lemma 3.4. *Let $\chi \pmod q$ be a non-principal character (with $q \ge 3$), and $t \in \mathbb{R}$. There is an absolute constant $c > 0$ such that for all $x \ge q$ we have*

$$\mathbb{D}_q(1, \chi(n)n^{it}; x)^2 \ge \frac{1}{2}\log\left(\frac{c\log x}{\log(q(1+|t|))}\right).$$

Consequently, if f is a multiplicative function, and χ and ψ are any two characters with conductors $q, r \le Q$, respectively, such that $\chi\overline{\psi}$ is non-principal, then for $x \ge Q$ we have

$$\mathbb{D}_q(f(n), \chi(n)n^{it}; x)^2 + \mathbb{D}_r(f(n), \psi(n)n^{iu}; x)^2 \ge \frac{1}{8}\log\left(\frac{c\log x}{2\log(Q(1+|t-u|))}\right).$$

Proof. For completeness we sketch the proof. We consider

$$d_{\chi,t}(n) = \sum_{ab=n} \chi(a)a^{it}\overline{\chi}(b)b^{-it}.$$

The proof of the Pólya-Vinogradov inequality is easily modified to show that

$$\sum_{n\le N} \chi(n) \ll (\phi(q)/q)\sqrt{q}\log q\,.$$

Using this and partial summation, we see that

$$\begin{aligned}\sum_{n\le x} \chi(n)n^{it} &= x^{it}\sum_{n\le x}\chi(n) - it\int_1^x u^{it-1}\sum_{n\le u}\chi(n)du \\ &\ll \frac{\phi(q)}{q}\sqrt{q}(\log q)(1+|t|\log x)\,.\end{aligned}$$

Therefore, grouping the terms $ab = n$ according to whether $a \le \sqrt{x}$ or $b \le \sqrt{x} < a$, we obtain

$$\sum_{n\le x} d_{\chi,t}(n) \ll \left(\frac{\phi(q)}{q}\right)^2 \sqrt{qx}(\log q)(1+|t|\log x)\,. \tag{3.2}$$

We write

$$d(n) = \sum_{\ell|n} d_{\chi,t}(n/\ell)h(\ell)$$

where h is a multiplicative function with $h(p) = 2 - 2\,\mathrm{Re}(\chi(p)p^{it})$, and notice that $|h(n)| \le d_4(n)$ for all n, where $d_4(n)$ is the divisor function counting the number of factorizations of n into four factors. Then

$$x\log x + O(x) = \sum_{n\le x} d(n) = \sum_{\ell\le x} h(\ell) \sum_{n\le x/\ell} d_{\chi,t}(n)\,.$$

When $\ell \le x/(q^2(1+|t|)^2)$ we use (3.2) to bound the sum over n. For larger ℓ we use the fact that $|d_{\chi,t}(n)| \le \chi_0(n)d(n)$ where $\chi_0(n)$ is the principal character $(\bmod\, q)$. Let $B = (\log q)^{q/\phi(q)}$. Thus if $x/B \le \ell \le x$ then

$$\sum_{n\le x/\ell} |d_{\chi,t}(n)| \le \sum_{n\le x/\ell} d(n) \ll \frac{x}{\ell}\,\log(ex/\ell)$$
$$\ll \frac{x}{\ell}\,\log B \ll \frac{x}{\ell}\,\frac{q}{\phi(q)}\,\log\log q \ll \frac{x}{\ell}\,\log q\,\left(\frac{\phi(q)}{q}\right)^2,$$

since $q/\phi(q) \ll \log\log q$. Now, if $N > B$ then

$$\sum_{n\le N} \chi_0(n)d(n) = \sum_{\substack{ab\le N\\(ab,q)=1}} 1$$
$$\ll \sum_{\substack{a\le\sqrt{N}\\(a,q)=1}} \sum_{\substack{b\le N/a\\(b,q)=1}} 1 \ll \sum_{\substack{a\le\sqrt{N}\\(a,q)=1}} \frac{\phi(q)}{q}\frac{N}{a} \ll \left(\frac{\phi(q)}{q}\right)^2 N\log N$$

by the sieve which we use for ℓ in the range $x/(q(1+|t|))^2 \le \ell \le x/B$ with $N = x/\ell$. Combining these estimates we obtain

$$x\log x \;\ll \sum_{\ell\le x/(q(1+|t|))^2} |h(\ell)| \left(\frac{\phi(q)}{q}\right)^2 \sqrt{qx/\ell}\,(\log q)(1+|t|\log(x/\ell))$$
$$+ \sum_{x/(q(1+|t|))^2<\ell\le x} |h(\ell)| \left(\frac{\phi(q)}{q}\right)^2 \frac{x}{\ell}\log(q(1+|t|))$$
$$\ll \left(\frac{\phi(q)}{q}\right)^2 x\log(q(1+|t|)) \sum_{\ell\le x} \frac{|h(\ell)|}{\ell}\,.$$

Since

$$\sum_{\ell\le x} |h(\ell)|/\ell \ll \exp\Big(\sum_{p\le x} |h(p)|/p\Big) = \exp\Big(2\mathbb{D}(1,\chi(n)n^{it};x)^2\Big)$$

we obtain the first statement of the Lemma.

To obtain the second estimate note that the triangle inequality gives

$$\begin{aligned}(\mathbb{D}_q(f(n),\chi(n)n^{it};x)+\mathbb{D}_r(f(n),\psi(n)n^{iu};x))^2 \\ &\geq (\mathbb{D}_{qr}(f(n),\chi(n)n^{it};x)+\mathbb{D}_{qr}(f(n),\psi(n)n^{iu};x))^2 \\ &\geq \sum_{\substack{p\leq x\\ p\nmid qr}} \frac{1-\mathrm{Re}\,|f(p)|^2\chi(p)\overline{\psi(p)}p^{i(t-u)}}{p} \\ &\geq \frac{1}{2}\sum_{\substack{p\leq x\\ p\nmid qr}} \frac{1-\mathrm{Re}\,\chi(p)\overline{\psi}(p)p^{i(t-u)}}{p},\end{aligned}$$

and now we appeal to the first part of the Lemma. □

4. The results for small moduli

Proof of Theorem 1.3 for small moduli. Select ψ as at the start of section 1.2 with $Q=\log x$ and $A=\log^2 x$. Let χ' be the primitive character that induces $\chi \pmod q$. By assumption $\chi'\neq\psi$. By Lemma 3.3 we know that for all $|t|\leq \log^2 x$,

$$\mathbb{D}(f(n),\chi'(n)n^{it};x)^2 \geq \Big(\frac{1}{3}+o(1)\Big)\log\log x\,.$$

Plainly,

$$\begin{aligned}\mathbb{D}(f(n),\chi(n)n^{it};x)^2 &= \mathbb{D}(f(n),\chi'(n)n^{it};x)^2 + O\Big(\sum_{p|q}\frac{1}{p}\Big) \\ &\geq \Big(\frac{1}{3}+o(1)\Big)\log\log x\,.\end{aligned}$$

Theorem 1.3 for small moduli now follows from Halász's Theorem 2.1. □

Proof of Theorem 1.1 for small moduli. From the discussion above, we know that for any $\chi \pmod q$ not induced by ψ we have (for all $|t|\leq\log^2 x$) the inequality

$$\mathbb{D}(f(n),\chi(n)n^{it};x)^2 \geq \Big(\frac{1}{3}+o(1)\Big)\log\log x\,.$$

By a similar argument, Lemma 3.1 implies that for all but at most $\sqrt{\log\log x}$ characters $\pmod q$ we have

$$\mathbb{D}(f(n),\chi(n)n^{it};x)^2 \geq \log\log x + O\big(\sqrt{\log\log x}\big),$$

for all $|t|\leq \log^2 x$. Therefore, from (1.10), Halász's Theorem 2.1 and these estimates, it follows that, for $r\nmid q$, we have

$$\sum_{\substack{n\leq x\\ n\equiv a \pmod q}} f(n) \ll \frac{x}{q(\log x)^{1/3+o(1)}} + \frac{x}{(\log x)^{1-o(1)}}\,.$$

When $r \mid q$ there is an extra contribution to (1.10) from the character $\tilde{\psi} \pmod q$ which is induced by $\psi \pmod r$. Thus in this case we obtain

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} f(n) = \frac{\psi(a)}{\phi(q)} \sum_{n\le x} f(n)\overline{\tilde{\psi}(n)} + O\Big(\frac{x}{q(\log x)^{1/3+o(1)}} + \frac{x}{(\log x)^{1-o(1)}}\Big),$$

which gives the result. □

Proof of Corollary 1.2. If f is unpretentious then the result follows from Theorem 1.1 for small moduli and (1.6); and similarly if f is pretentious but r does not divide q. If f is pretentious and r divides q then the result follows from (1.3d) and Theorem 2.3. To see that ψ and t are unique, suppose we have another pair ψ' and t' so that $D(\psi'(p)p^{it'}, \psi(p)p^{it}; \infty) < \infty$ by the triangle inequality, and thus $L(s, \psi'\overline{\psi})$ has a pole at $1 + i(t' - t)$, which is false. Finally, if f is real-valued then, by taking x arbitrary large in Corollary 3.2, we discover that ψ is real, and t is zero, and the result follows. □

Proof of Corollary 1.4. If $|\sum_{n\le x, n\equiv a \pmod q} \big(\frac{n}{p}\big)| \gg x/q$, then

$$\Bigg|\sum_{n\le x, n\equiv b \pmod q} \Big(\frac{n}{p}\Big)\Bigg| \gg x/q$$

whenever $(b, q) = 1$ by two applications of (1.3e). Select $c \pmod q$ so that $\psi(c)$ is as close as possible to i and let $b \equiv a/c \pmod q$; we then deduce from (1.3e) that ψ must be real since both sums are real (see also Corollary 3.2). Therefore (1.3d) tells us that our sum is

$$(\psi(a)/\phi(q)) \sum_{n\le x} \big(\frac{n}{p}\big)\overline{\psi(n)} + o(x/q)\,.$$

This is

$$(\psi(a)/q) \sum_{n\le x} g(n) + o(x/q)$$

where g is the multiplicative function with

$$g(p) = \begin{cases} \big(\frac{n}{p}\big)\overline{\psi(p)} & \text{if } p \nmid q, \\ 1 & \text{if } p \mid q, \end{cases}$$

by Proposition 4.4 of [13] (with $\phi = \pi/2$ and $\epsilon = \log q/\log x$).

Now suppose that $a \not\equiv \Box \pmod q$, so that there is a real character $\psi \pmod q$ for which $\psi(a) = -1$. There exist infinitely many primes p for which $\big(\frac{\ell}{p}\big) = \psi(\ell)$ for any prime $\ell \nmid q$ with $\ell \le x$, by quadratic reciprocity and Dirichlet's theorem. In this case

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q}} \Big(\frac{n}{p}\Big) = \psi(a)\Big(\frac{x}{q} + O(1)\Big) = -\frac{x}{q} + O(1),$$

and so the result follows.

Now suppose that $a \equiv \Box \pmod q$. Then $\psi(a) = 1$ for all real characters $\psi \pmod q$ and so our sum is $(1/q)\sum_{n\le x} g(n) + o(x/q)$. The result then follows from

Corollary 1 of [13], the minimal value being obtained by selecting prime p so that $\left(\frac{\ell}{p}\right) = 1$ for all primes $\ell \leq x^{1/(1+\sqrt{e})}$ and $\left(\frac{\ell}{p}\right) = -1$ for $x^{1/(1+\sqrt{e})} < \ell \leq x$ as described in section 1.3, and with ψ being the trivial character $\pmod 1$, so that

$$\sum_{\substack{n\leq x\\ n\equiv a \pmod q}} \left(\frac{n}{p}\right) = \frac{1}{\phi(q)} \sum_{\substack{n\leq x\\ (n,q)=1}} \left(\frac{n}{p}\right) + o(x) = \Big(\delta_1 + o(1)\Big)\frac{x}{q}\cdot$$

(The reader can either directly verify the last equality, or consult [13].) □

5. The case of large moduli

Proof of Theorem 1.3 for large moduli. Let us take $T = (\log x/\log Q)^{\frac{1}{10}}$ in Theorem 2.1. Suppose that there exists a character ψ with conductor $\leq Q$ and

$$\Big|\sum_{n\leq x} f(n)\overline{\psi(n)}\Big| \geq x\Big(\frac{\log Q}{\log x}\Big)^{\frac{1}{20}}.$$

From Theorem 2.1 we conclude that for some real number $|t| \leq T$ we have

$$\mathbb{D}(f(n), \psi(n)n^{-it}; x)^2 \leq \Big(\frac{1}{20} + o(1)\Big) \log \frac{\log x}{\log Q}\cdot$$

From Lemma 3.4 it follows that for any character χ with conductor below Q and $\chi\overline{\psi}$ non-principal, we have

$$\mathbb{D}(f(n), \chi(n)n^{-iu}; x)^2 \geq \frac{1}{14} \log \frac{\log x}{\log Q},$$

for all $|u| \leq T$. Appealing to Theorem 2.1, we obtain Theorem 1.3 for large moduli. □

We now embark on the proof of Theorem 1.1 for large moduli. It is convenient to define

$$F(x; q, a) = \sum_{\substack{n\leq x\\ n\equiv a \pmod q}} f(n)\,.$$

We will study $F(x; q, a)$ using the large sieve. First we show that for many moduli r, the distribution of $f(n)$ for $n \leq x$, $n \equiv a \pmod q$, is uniform in sub-progressions $\pmod r$.

Proposition 5.1. *Let* $1 \leq a \leq q$*. For* $\eta > 1/\sqrt{\log x}$*, the set* $\mathcal{B}(a, \eta)$ *of bad moduli* $1 < r \leq \sqrt{x/q}$ *for which*

$$\sideset{}{^*}\sum_{\psi \pmod r} \Big|\sum_{n\leq x/q} f(nq + a)\psi(n)\Big| \geq \eta\frac{x}{q},$$

(where $\sum^*$ *denotes, as usual, a sum over primitive characters) satisfies*

$$\sum_{r\in\mathcal{B}(a,\eta)} \frac{1}{\phi(r)} \leq \frac{2}{\eta^2}\,. \tag{5.1}$$

Let $\mathcal{G}(a,\eta)$ denote the set of good moduli $r \le \sqrt{x/q}$, that is those r which are square-free and not divisible by any element in $\mathcal{B}(a,\eta)$. If $r \in \mathcal{G}(a,\eta)$ with $(r,q)=1$ then

$$F(x;q,a) = rf(r)F(x/r;q,a/r) + O\Big(\frac{x}{q}\Big(\eta d(r) + \Big(1-\frac{\phi(r)}{r}\Big)\Big)\Big).$$

Here a/r denotes the residue class $ar^{-1} \pmod q$.

Proof. By Cauchy's inequality and then the large sieve (as in Theorem 7.13 of [19]) we have

$$\begin{aligned}\sum_{r\le\sqrt{x/q}} \frac{1}{\phi(r)}\Bigg(\sideset{}{^*}\sum_{\psi \pmod r} \Big| \sum_{n\le x/q} f(nq+a)\psi(n)\Big|\Bigg)^2 &\le \sum_{r\le\sqrt{x/q}} \sideset{}{^*}\sum_{\psi \pmod r} \Big|\sum_{n\le x/q} f(nq+a)\psi(n)\Big|^2 \\ &\le 2\,\frac{x}{q}\sum_{n\le x/q} |f(nq+a)|^2 \le 2\left(\frac{x}{q}\right)^2.\end{aligned}$$

The estimate (5.1) follows at once.

Now suppose that r is a good modulus, and consider any progression $b \pmod r$ with $(b,r)=1$. Since r is square-free we check easily that

$$\sum_{\ell|r} \sideset{}{^*}\sum_{\psi \pmod \ell} \overline{\psi(b)}\psi(n) = \begin{cases} \phi(r/d) & \text{if } (n,r)=d, \text{ and } n\equiv b \pmod{r/d} \text{ for some } d \,\big|\, r, \\ 0 & \text{otherwise.}\end{cases}$$

Therefore

$$\sum_{\substack{n\le x/q \\ n\equiv b \pmod r}} f(nq+a) = \frac{1}{\phi(r)} \sum_{\ell|r} \sideset{}{^*}\sum_{\psi \pmod \ell} \overline{\psi(b)} \sum_{n\le x/q} f(nq+a)\psi(n) + O\Big(\sum_{\substack{d|r\\ d>1}} \frac{\phi(r/d)}{\phi(r)} \sum_{\substack{n\le x/q \\ d|n \\ n\equiv b \pmod{r/d}}} 1\Big).$$

The error term above is plainly

$$\ll \sum_{\substack{d|r\\ d>1}} \frac{\phi(r/d)}{\phi(r)}\,\frac{x}{qr} = \frac{(r-\phi(r))}{\phi(r)}\,\frac{x}{qr}\,.$$

Further, since r is good, if $\ell>1$ and ℓ divides r then ℓ is good so that

$$\sideset{}{^*}\sum_{\psi \pmod \ell} \overline{\psi(b)} \sum_{n\le x/q} f(nq+a)\psi(n) \ll \sideset{}{^*}\sum_{\psi \pmod \ell} \Big|\sum_{n\le x/q} f(nq+a)\psi(n)\Big| \le \eta\frac{x}{q}\,.$$

We conclude that

$$\sum_{\substack{n\le x/q\\ n\equiv b \pmod r}} f(nq+a) = \frac{1}{\phi(r)} \sum_{n\le x/q} f(nq+a) + O\left(\frac{d(r)}{\phi(r)}\eta\frac{x}{q}\right) + O\left(\frac{x}{q\phi(r)}\Big(1-\frac{\phi(r)}{r}\Big)\right).$$

If $(r,q)=1$ then we may choose b so that $bq+a\equiv 0 \pmod r$, and so the left hand side of the last displayed equation equals

$$\sum_{\substack{n\le x\\ n\equiv a \pmod q\\ r|n}} f(n) = f(r)F(x/r;q,a/r) + O\left(\frac{x}{qr}\Big(1-\frac{\phi(r)}{r}\Big)\right).$$

Hence, for good moduli r that are coprime to q we have

$$\begin{aligned} F(x;q,a) &= f(r)\phi(r)F(x/r;q,a/r) + O\left(\frac{x}{q}\left(\eta d(r) + \Big(1-\frac{\phi(r)}{r}\Big)\right)\right) \\ &= rf(r)F(x/r;q,a/r) + O\left(\frac{x}{q}\left(\eta d(r) + \Big(1-\frac{\phi(r)}{r}\Big)\right)\right), \end{aligned}$$

proving our Proposition. □

Proposition 5.2. *Let $x\ge q^{20}$ and set $A=\log x/\log q$. Let a and b be any two given reduced residues $\pmod q$. Then we have*

$$F(x;q,ab)F(x;q,1) = F(x;q,a)F(x;q,b) + O\left(\frac{x}{q}\frac{1}{\sqrt{\log A}} \max_{\substack{c \pmod q\\ (c,q)=1}} |F(x;q,c)|\right).$$

Proof. We may assume that A is large, and set $\eta = C/\sqrt{\log A}$ for some sufficiently large constant $C>0$. We will produce two numbers r and s with the following properties:

(i) both r and s have at most two prime factors and these prime factors are $\ge 1/\eta$,

(ii) r and s are both in $\mathcal{G}(1,\eta)$, $\mathcal{G}(a,\eta)$, $\mathcal{G}(b,\eta)$ and $\mathcal{G}(ab,\eta)$,

(iii) the ratio r/s lies between $1-\eta$ and $1+\eta$, and

(iv) $r\equiv bs \pmod q$.

Assuming that this can be done, let us now prove Proposition 5.2. Four applications of Proposition 5.1 give:

$$F(x;q,ab) = rf(r)F(x/r;q,ab/r) + O(\eta x/q), \tag{5.2}$$

$$F(x;q,1) = sf(s)F(x/s;q,1/s) + O(\eta x/q), \tag{5.3}$$

$$F(x;q,a) = sf(s)F(x/s;q,a/s) + O(\eta x/q), \tag{5.4}$$

$$F(x;q,b) = rf(r)F(x/r;q,b/r) + O(\eta x/q). \tag{5.5}$$

By assumption we have $a/s \equiv ab/r \pmod q$, and moreover $|r/s-1| \le \eta$. Hence

$$\begin{aligned} F(x/s;q,a/s) &= F(x/s;q,ab/r) \\ &= F(x/r;q,ab/r) + O(|x/r - x/s|/q) \\ &= F(x/r;q,ab/r) + O(\eta x/(qr)), \end{aligned}$$

and, taking $a=1$,

$$F(x/r;q,b/r) = F(x/s;q,1/s) + O(\eta x/(qr)).$$

Therefore multiplying (5.2) and (5.3), and (5.4) and (5.5) we obtain that

$$\begin{aligned} F(x;q,ab)F(x;q,1) &= rsf(r)f(s)F(x/r;q,ab/r)F(x/s;q,1/s) \\ &\qquad + O\Big(\eta \frac{x}{q} \max_{\substack{c \pmod q \\ (c,q)=1}} |F(x;q,c)|\Big) \\ &= F(x;q,a)F(x;q,b) + O\Big(\eta \frac{x}{q} \max_{\substack{c \pmod q \\ (c,q)=1}} |F(x;q,c)|\Big), \end{aligned}$$

which proves the Proposition.

It remains to show the existence of r and s. If there is no Siegel-Landau zero for a character $\pmod q$ then we can take r and s to be primes. To see this note that if there is no Siegel-Landau zero then minor modifications to the proof of Proposition 18.5 of [19] imply that there exist constants $c, B > 0$ such that

$$\sum_{\substack{z<p\le(1+\eta)z \\ p\equiv a \pmod q}} \log p = \frac{\eta z}{\phi(q)} \left\{ 1 + O\left(\frac{1}{z^{c/\log q}} + \frac{1}{\log z} \right) \right\} \tag{5.6}$$

for all $z \ge q^B$ and $(a,q)=1$. We may assume that $A \ge B^2$. Let $\mathcal{P}_1$ denote the set of primes in the interval $[q^B, \sqrt{x/q}]$ which are in the set

$$\mathcal{G}(1,\eta) \cap \mathcal{G}(a,\eta) \cap \mathcal{G}(b,\eta) \cap \mathcal{G}(ab,\eta).$$

By Proposition 5.1,

$$\sum_{p\in\mathcal{P}_1} \frac{1}{p} = \sum_{q^B \le p \le \sqrt{x/q}} \frac{1}{p} + O\Big(\frac{1}{\eta^2}\Big)\cdot \tag{5.7}$$

We divide the interval $[q^B, \sqrt{x/q}]$ into intervals of the form $(z,(1+\eta)z]$. Any two primes r and s in $\mathcal{P}_1 \cap (z,(1+\eta)z]$ meet criteria (i), (ii) and (iii) above, so it only remains to satisfy criterion (iv). If criterion (iv) does not hold then the primes in $\mathcal{P}_1 \cap (z,(1+\eta)z]$ lie in at most $\phi(q)/2$ reduced residue classes $\pmod q$. Therefore, by (5.6) we must have

$$\sum_{\substack{z<p\le(1+\eta)z \\ p\in\mathcal{P}_1}} \log p \le \frac{\eta z}{2} \left\{ 1 + O\left(\frac{1}{z^{c/\log q}} + \frac{1}{\log z} \right) \right\},$$

so that

$$\sum_{p\in\mathcal{P}_1} \frac{1}{p} \le \frac{1}{2} \sum_{q^B \le p \le \sqrt{x/q}} \frac{1}{p} + O(1),$$

which contradicts (5.7), since $\sum_{q^B \le p \le \sqrt{x/q}} 1/p \asymp \log A$.

Now assume that there is a real character $\chi \pmod q$ with a Siegel-Landau zero β. Then Proposition 18.5 of [19] yields that

$$\sum_{\substack{p\le z\\ p\equiv a \pmod q}} \log p = \frac{1}{\phi(q)}\left\{z - \chi(a)\frac{z^\beta}{\beta} + O\left(\frac{z}{\log^2 z}\right)\right\} \tag{5.8}$$

for all $z \ge q^B$ and $(a,q)=1$. Notice that the primes are concentrated in the residue classes $c \,(\mathrm{mod}\, q)$ with $\chi(c)=-1$, and it is therefore difficult to solve $r \equiv bs \,(\mathrm{mod}\, q)$ in primes r and s if $\chi(b)=-1$. However products of two primes, will now be concentrated on the residue classes $c \pmod q$ for which $\chi(c)=1$, as one may deduce directly from (5.8):

(5.9)

$$\sum_{\substack{p_1p_2\le z\\ p_1p_2\equiv a \pmod q\\ p_1>p_2\ge q^B}} \log p_1 \log p_2 = \frac{1}{\phi(q)}\ \log(\sqrt{z}/q^B)\left\{z + \chi(a)\frac{z^\beta}{\beta} + O\left(\frac{z}{\log z}\right)\right\},$$

for all $z \ge q^{3B}$ and $(a,q)=1$.

So now let $\mathcal{P}_2$ denote the set of products of two primes $p_1 > p_2 \ge q^B$ with the property that $p_1p_2 \le \sqrt{x/q}$, which are in the set

$$\mathcal{G}(1,\eta)\cap\mathcal{G}(a,\eta)\cap\mathcal{G}(b,\eta)\cap\mathcal{G}(ab,\eta),$$

and imitate as best we can the proof above. Proposition 5.1 tells us, again, that $\mathcal{P}_2$ contains lots of elements, and that we can find an interval $(z,(1+\eta)z]$ containing many elements from $\mathcal{P}_1$ and $\mathcal{P}_2$. Then criterion (iv) is met by choosing either two elements from $\mathcal{P}_1$ (when $\chi(b)=1$), or an element each from $\mathcal{P}_1$ and $\mathcal{P}_2$ (when $\chi(b)=-1$), and the proof of the Proposition is complete. Although we will not go into the details, the easiest way to formulate this proof is to combine (5.8) and (5.9) into the equation

$$\sum_{\substack{p\le z\\ p\equiv a \pmod q}} \log p + \frac{1}{\log(\sqrt{z}/q^B)} \sum_{\substack{p_1p_2\le z\\ p_1p_2\equiv a \pmod q\\ p_1>p_2\ge q^B}} \log p_1\log p_2 = \frac{2z}{\phi(q)}\left\{1 + O\left(\frac{1}{\log z}\right)\right\}, \tag{5.10}$$

for all $z \ge q^{3B}$ and $(a,q)=1$, removing the effect of the Siegel-Landau zero, so that we do not need to split this proof into cases depending on the value of $\chi(b)$. □

Remark. It is amusing to note that we cannot prove (5.10) under the assumption that there is no Siegel-Landau zero. In this case there is an additional $1/z^{c/\log q}$ in the error term, as in (5.6). It would be interesting to know whether this can be removed, so as to prove (5.10) uniformly. Note that (5.10) is a complicated formulation of Selberg's formula [22] for z sufficiently large.

The proof of Proposition 5.2 is the only proof in this paper that requires non-trivial information about the zeros of L-functions and it is pleasing to give an alternate proof that is "elementary". Thus, in the spirit of Selberg's paper, one can ask whether one can give an elementary proof of (5.10) in this range? The proof of Proposition 5.2

goes through easily with $\sim 2z/\phi(q)$ on the right side of (5.10), a formula that was proved, whether or not there is a Siegel-Landau zero, by Friedlander [10] using only sieve methods. Our proof of Proposition 5.2 can easily be modified to work provided the quantity on the right side of (5.10) is between $z/\phi(q)$ and $3z/\phi(q)$, for $z > q^B$ for some fixed $B > 0$; in fact our (non-elementary) proof gives such a result (as in the discussion of the previous paragraph) but, better, Friedlander's proof is easily modified to give this result, so that all of the results in this paper can be proved avoiding use of zeros of L-functions.

Lastly, we need a result which characterizes periodic functions that are almost multiplicative. We will show that such functions are close to being characters. L. Babai, K. Friedl and A. Lukács [1] have explored such questions in greater generality recently, but for the sake of completeness we provide a proof.

Proposition 5.3. *Let* $0 \le \epsilon < 1/2$. *Let* $g : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}$ *be a function with* $g(1) = 1$, *and* $|g(ab) - g(a)g(b)| \le \epsilon$ *for all* a *and* b *coprime to* q. *Then there exists a character* $\chi \pmod q$ *such that* $|\chi(a) - g(a)| \le \epsilon/(1-2\epsilon)$, *for all* $(a, q) = 1$.

Proof. For any character $\chi \pmod q$, define

$$\hat{g}(\chi) = \sum_{a \pmod q} g(a)\overline{\chi}(a).$$

We claim that there exists a character $\chi \pmod q$ with $|\hat{g}(\chi)| \ge (1-2\epsilon)\phi(q)$. Granting this claim, we see that for any $(a, q) = 1$

$$\begin{aligned} |(g(a) - \chi(a))\hat{g}(\chi)| &= \Big| \sum_{b \pmod q} g(a)g(b)\overline{\chi}(b) - \chi(a) \sum_{ab \pmod q} g(ab)\overline{\chi}(ab) \Big| \\ &= \Big| \sum_{b \pmod q} (g(a)g(b) - g(ab))\overline{\chi}(b) \Big| \le \epsilon\phi(q), \end{aligned}$$

which proves the Proposition.

Note that

$$\sum_{\chi \pmod q} |\hat{g}(\chi)|^2 = \phi(q) \sum_{a \pmod q}^{*} |g(a)|^2 \tag{5.11}$$

(where, as usual, $\sum^*$ denotes a sum over integers coprime with q). Further,

$$\sum_{\chi \pmod q} \hat{g}(\chi)^2 \overline{\hat{g}(\chi)} = \phi(q) \sum_{a,b}^{*} g(a)g(b)\overline{g(ab)} = \phi(q) \sum_{a,b}^{*} |g(a)g(b)|^2 + E$$

where

$$\begin{aligned} |E| &\le \phi(q) \sum_{a,b}^{*} |g(ab) - g(a)g(b)||g(a)g(b)| \\ &\le \epsilon\phi(q) \sum_{a,b}^{*} |g(a)g(b)| \le \epsilon\phi(q)^2 \sum_{a}^{*} |g(a)|^2, \end{aligned}$$

so that, by (5.11),

$$\max_{\chi \pmod q} |\hat{g}(\chi)| \cdot \phi(q) \sum_a{}^* |g(a)|^2 \geq \Big| \sum_{\chi \pmod q} \hat{g}(\chi)^2 \overline{\hat{g}(\chi)} \Big|$$
$$\geq \phi(q) \Big(\sum_a{}^* |g(a)|^2 \Big)^2 - \epsilon\phi(q)^2 \sum_a{}^* |g(a)|^2.$$

We deduce that there exists a $\chi \pmod q$ with $|g(\chi)| \geq \sum_a^* |g(a)|^2 - \epsilon\phi(q)$. Now, using Cauchy's inequality, we have

$$\sum_a{}^* |g(a)|^2 \geq \Big| \sum_a{}^* g(a)g(a^{-1}) \Big| \geq (1-\epsilon)\phi(q),$$

since $|g(1) - g(a)g(a^{-1})| \leq \epsilon$, so that we may conclude the existence of a $\chi \pmod q$ with $|\hat{g}(\chi)| \geq (1-2\epsilon)\phi(q)$, as claimed. □

Proof of Theorem 1.1 for large moduli. Select $c \pmod q$ with $(c,q) = 1$ for which $|F(x;q,c)|$ is maximized. We may suppose that

$$|F(x;q,c)| \gg \frac{x}{q} \frac{1}{\sqrt{\log A}},$$

else there is nothing to prove. With this assumption, taking $a = b = c$ in Proposition 5.2, and noting that $|F(x;q,c^2)| \leq |F(x;q,c)|$, we deduce that

$$|F(x;q,1)| \geq \frac{1}{2} |F(x;q,c)|. \tag{5.12}$$

Let us define g by setting $F(x;q,a) = g(a)F(x;q,1)$. Then g is periodic with period q, $g(1) = 1$, and by Proposition 5.2 we have

$$|g(ab) - g(a)g(b)| = O\Big(\frac{1}{\sqrt{\log A}} \frac{x}{q|F(x;q,1)|} \Big).$$

By Proposition 5.3 it follows that there is a character $\chi \pmod q$ such that for all $(a,q) = 1$

$$|g(a) - \chi(a)| = O\Big(\frac{1}{\sqrt{\log A}} \frac{x}{q|F(x;q,1)|} \Big); \tag{5.13}$$

that is

$$F(x;q,a) = \chi(a)F(x;q,1) + O\Big(\frac{x}{q} \frac{1}{\sqrt{\log A}} \Big)$$

which is (1.3e); and we also deduce that

$$\sum_{n\leq x} f(n)\overline{\chi}(n) = \sum_{a \pmod q} \overline{\chi}(a)F(x;q,a) = F(x;q,1) \sum_{a \pmod q} \overline{\chi}(a)g(a) \tag{5.14}$$
$$= \phi(q)F(x;q,1) + O\Big(\frac{1}{\sqrt{\log A}} x \frac{\phi(q)}{q} \Big).$$

If $\chi\overline{\psi}$ is non-principal then

$$\mathbb{D}_q(f, \chi(n)n^{-it}; x)^2 \geq \frac{1}{17} \log A,$$

for all $|t| \leq A$ by Lemma 3.4. Therefore by Corollary 2.2 we have

$$\sum_{n\leq x} f(n)\overline{\chi}(n) \ll \frac{\phi(q)}{q}\,\frac{x}{A^{1/20}},$$

which implies the result, using (5.12) and (5.14), when r does not divide q. If r divides q, with $\chi\overline{\psi}$ non-principal, then, proceeding as above,

$$\sum_{\substack{n\leq x\\(n,q)=1}} f(n)\overline{\psi(n)} = F(x;q,1)\sum_{\substack{a \pmod q\\(a,q)=1}} \overline{\psi(a)}g(a) = O\Big(x\frac{\phi(q)}{q}\frac{1}{\sqrt{\log A}}\Big),$$

by (5.13) and the orthogonality of the characters χ and ψ, which gives the result.

If $r \mid q$ and χ is induced by ψ then from (5.14) we get

$$\begin{aligned} F(x;q,a) = g(a)F(x;q,1) &= \chi(a)F(x;q,1) + O\Big(\frac{x}{q}\frac{1}{\sqrt{\log A}}\Big)\\ &= \frac{\psi(a)}{\phi(q)}\sum_{\substack{n\leq x\\(n,q)=1}} f(n)\overline{\psi(n)} + O\Big(\frac{x}{q}\frac{1}{\sqrt{\log A}}\Big), \end{aligned}$$

as desired. □

Acknowledgements. We are grateful to Ben Green for some interesting conversations regarding Proposition 5.3, and for drawing our attention to [1], and to John Friedlander for drawing our attention to [10]. We are also grateful to the referee for his suggestions.

The first author would like to acknowledge the support of the Hungarian National Science Foundation, as well as of the Centre de recherches mathématiques in Montréal. The second author was partially supported by a grant from Natural Sciences and Engineering Research Council of Canada. The third author is partially supported by the National Science Foundation and the American Institute of Mathematics.

REFERENCES

[1] L. Babai, K. Friedl and A. Lukács, *Near representations of finite groups*, preprint.

[2] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Second Edition, Astérisque No. 18 (1987), 103 pp.

[3] H. Daboussi and H. Delange, *Quelques propriétés des fonctions multiplicatives de module au plus égal à* 1, C. R. Acad. Sci. Paris Sér. A **278** (1974), 657–660.

[4] H. Davenport, *Multiplicative number theory*, Second edition. Revised by Hugh L. Montgomery. Graduate Texts in Mathematics, **74**, Springer-Verlag, New York-Berlin, 1980, xiii+177 pp.

[5] P. D. T. A. Elliott, *Multiplicative functions on arithmetic progressions*, Mathematika **34** (1987), no. 2, 199–206.

[6] P. D. T. A. Elliott, *Multiplicative functions on arithmetic progressions II*, Mathematika **35** (1988), no. 1, 38–50.

[7] P. D. T. A. Elliott, *Multiplicative functions on arithmetic progressions VII. Large moduli*, J. London Math. Soc. (2) **66** (2002), no. 1, 14–28.

[8] P. D. T. A. Elliott, *The least prime primitive root and Linnik's theorem*, in Number theory for the millennium, I (Urbana, IL, 2000), 393–418, A K Peters, Natick, MA, 2002.

[9] P. Erdős, *Some problems in number theory*, in Computers in Number Theory (eds. Atkin and Birch), 405–414, Academic Press, London-New York, 1971.

[10] J. B. Friedlander, *Selberg's formula and Siegel's zero*, in Recent progress in analytic number theory, Vol. 1 (Durham, 1979), 15–23, Academic Press, London-New York, 1981.

[11] A. Granville, *On elementary proofs of the prime number theorem for arithmetic progressions, without characters*, in Proceedings of the Amalfi Conference on Analytic Number Theory (Maiori, 1989), 157–194, Univ. Salerno, Salerno, 1992.

[12] A. Granville and K. Soundararajan, *Large character sums*, J. Amer. Math. Soc. **14** (2001), 365–397.

[13] A. Granville and K. Soundararajan, *The spectrum of multiplicative functions*, Ann. of Math. (2) **153** (2001), no. 2, 407–470.

[14] A. Granville and K. Soundararajan, *Decay of mean values of multiplicative functions*, Canad. J. Math. **55** (2003), no. 6, 1191–1230.

[15] A. Granville and K. Soundararajan, *Large character sums: pretentious characters and the Pólya-Vinogradov theorem*, J. Amer. Math. Soc. **20** (2007), no. 2, 357–384.

[16] A. Granville and K. Soundararajan, *Pretentious multiplicative functions and an inequality for the zeta-function*, in Anatomy of integers, 191–197, CRM Proc. Lecture Notes, **46**, Amer. Math. Soc., Providence, RI, 2008.

[17] A. Granville and K. Soundararajan, *The pretentious large sieve*, to appear.

[18] A. Hildebrand, *Multiplicative functions on arithmetic progressions*, Proc. Amer. Math. Soc. **108** (1990), no. 2, 307–318.

[19] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, **53**, American Mathematical Society, Providence, RI, 2004. xii+615 pp.

[20] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, **84**, American Mathematical Society, Providence, RI, 1994. xiv+220 pp.

[21] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math. **43** (1977), no. 1, 69–82.

[22] A. Selberg, *An elementary proof of the prime number theorem for arithmetic progressions*, Canadian J. Math. **2** (1950), 66–78.

[23] H. N. Shapiro, *Some assertions equivalent to the prime number theorem for arithmetic progressions*, Comm. Pure Appl. Math. **2** (1949), 293–308.

[24] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, **46**, Cambridge University Press, Cambridge, 1995. xvi+448 pp.

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

A. BALOG, ALFRÉD RÉNYI INST. OF MATH., POB 127, 1364 BUDAPEST, HUNGARY
balog@renyi.hu

A. GRANVILLE, DÉP. DE MATH. ET STAT., U. DE MONTRÉAL, CASE POSTALE 6128, SUCCURSALE CENTRE-VILLE, MONTRÉAL QC H3C 3J7, CANADA
andrew@dms.umontreal.ca

K. SOUNDARARAJAN, DEPT. OF MATH., 450 SERRA MALL, BLDG. 380, STANFORD U., PALO ALTO CA 94305, USA
ksound@math.stanford.edu