PRETENTIOUSNESS IN ANALYTIC NUMBER THEORY

Andrew Granville

Abstract. In this report, prepared specially for the program of the *XXVième Journées Arithmétiques*, we describe how, in joint work with K. Soundararajan and Antal Balog, we have developed the notion of "pretentiousness" to help us better understand several key questions in analytic number theory.

The prime number theorem, I

As a boy of 15 or 16, Gauss determined, by studying tables of primes, that the primes occur with density $\frac{1}{\log x}$ at around x. This translates into the guess that

$$\pi(x) := \#\{\text{primes} \le x\} \approx \mathrm{Li}(x) \quad \text{where} \quad \mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}.$$

The existing data lend support to Gauss's guesstimate:

x	$\pi(x) = \#\{\text{primes} \le x\}$	Overcount: $[\mathrm{Li}(x) - \pi(x)]$
10^8	5761455	753
10^9	50847534	1700
10^{10}	455052511	3103
10^{11}	4118054813	11587
10^{12}	37607912018	38262
10^{13}	346065536839	108970
10^{14}	3204941750802	314889
10^{15}	29844570422669	1052618
10^{16}	279238341033925	3214631
10^{17}	2623557157654233	7956588
10^{18}	24739954287740860	21949554
10^{19}	234057667276344607	99877774
10^{20}	2220819602560918840	222744643
10^{21}	21127269486018731928	597394253
10^{22}	201467286689315906290	1932355207
10^{23}	1925320391606803968923	7250186214

L'auteur est partiellement soutenu par une bourse de la Conseil de recherches en sciences naturelles et en génie du Canada. Thanks to K. Soundararajan for his comments on an earlier draft of this article.

Notice how the entries in the final column are always positive and always about half the width of the entries in the middle column: So it seems that Gauss's guess is always an overcount by about $\sqrt{x}$. We believe that this observation is both right and wrong: Although the last column looks to be positive and growing we believe that it eventually turns negative, and subsequently changes sign infinitely often (see, e.g. [7]). On the other hand we believe that the error in Gauss's guess is never much more than $\sqrt{x}$ — correctly formulated this statement is equivalent to the Riemann Hypothesis.

In this talk we only need the weaker statement that $\pi(x) \sim x/\log x$, the *Prime Number Theorem*. We state this in a slightly cumbersome way, as this fits better the perspective developed herein.

The Prime Number Theorem (version 1). *For any $\epsilon > 0$ there exists x_ϵ such that if $x \ge x_\epsilon$ then*

$$\left|\pi(x) - \frac{x}{\log x}\right| \le \epsilon \frac{x}{\log x}.$$

Let $\pi(x; q, a)$ denote the number of primes $\le x$ that are $\equiv a \pmod q$. An analogous proof reveals that if $(a, q) = 1$ and $x \ge x_{\epsilon,q}$ then

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

A key question is to determine how small we can take $x_{\epsilon,q}$, for a given ϵ. Calculations reveal that one should be able to take $x_{\epsilon,q}$ just a tiny bit larger than q, say $q^{1+\delta}$ for any fixed $\delta > 0$ (once q is sufficiently large). However the best results known [4] have $\log x_{\epsilon,q}$ a power of q, way off from what is expected. If we are prepared to assume the unproven *Generalized Riemann Hypothesis* we do far better, being able to take $x_{\epsilon,q}$ just a tiny bit larger than q^2, though notice that this is still some way off from what we expect to be true.

Our research in this area centres around the distribution of mean values of multiplicative functions, that is functions f on the positive integers, for which

$$f(mn) = f(m)f(n) \quad \text{whenever} \quad (m, n) = 1.$$

Typically we will assume $f : \mathbb{N} \to \mathbb{U}$ where $\mathbb{U} := \{z \in \mathbb{C} : \ |z| \le 1\}$ and that f is totally multiplicative (that is when $f(mn) = f(m)f(n)$ for all $m, n \ge 1$, not just those pairs of integers m, n that are coprime). Key examples include $f(n) = 1$ and $f(n) = n^{it}$ for some $t \in \mathbb{R}$, as well as the Dirichlet characters: If χ is a Dirichlet character of order m then $\chi : (\mathbb{Z}/q\mathbb{Z})^* \to G \subset \mathbb{U}$ where G is the set of mth roots of unity, a finite group. So what is the connection between the two subjects? The Mőbius function $\mu(n)$ is multiplicative and we have the remarkably useful identity

$$\sum_{n=ab} \mu(a)\log b = \begin{cases} \log p & \text{if } n = p^e \\ 0 & \text{otherwise} \end{cases}$$

where the sum is over all pairs of positive integers a, b satisfying $ab = n$, and the first case is for all powers (with $e \geq 1$) of a prime p. If we sum this identity over all $n \leq x$ we obtain the identity

$$\sum_{p^e \leq x} \log p = \sum_{ab \leq x} \mu(a) \log b.$$

The contribution of the prime powers p^e with $e \geq 2$ to the left hand side are easily shown to be negligible, and a good estimate for the remaining sum can easily be shown, via partial summation, to be equivalent to a good estimate for $\pi(x)$.[1] Therefore a good estimate for the right hand side must be equivalent to the prime number theorem. One can approach the right hand side by fixing a and then summing over b; this is easy since $\sum_{b \leq B} \log b = \log B!$ which can be very accurately estimated using Stirling's formula. This leaves us with a sum over a, something like

$$x \sum_{a \leq x} \frac{\mu(a)}{a} \left(\log(x/a) - 1\right),$$

which can be estimated accurately, via partial summation, provided $\sum_{a \leq A} \mu(a)$ can be for various values of A. Thus we have sketched a justification that the prime number theorem is "equivalent" to proving that

$$\sum_{n \leq N} \mu(n) = o(N).$$

(See, e.g. section 2.1 of [14] for a proof that these really are equivalent.) Of course μ is a multiplicative function, but not a totally multiplicative function, which would be easier to work with. This is easily remedied by replacing μ by Liouville's function $\lambda(n)$ which equals $\mu(n)$ when n is squarefree and in general is given by

$$\lambda(n) = (-1)^{\#\{\text{prime powers } p^e | n\}}.$$

One can also show that the prime number theorem is equivalent to proving that

$$\sum_{n \leq N} \lambda(n) = o(N). \tag{1}$$

As above we state it in the following form:

The Prime Number Theorem (version 2). *For any $\epsilon > 0$ there exists x_ϵ such that if $x \geq x_\epsilon$ then*

$$\left| \sum_{n \leq x} \lambda(n) \right| \leq \epsilon x.$$

Moreover if $x \geq x_{\epsilon,q}$ then

$$\left| \sum_{\substack{n \leq x \\ n \equiv a \pmod q}} \lambda(n) \right| \leq \epsilon \frac{x}{q}$$

[1] Indeed $\sum_{p^e \leq x} \log p \sim x$ if and only if $\pi(x) \sim x/\log x$.

whenever $(a,q)=1$.

Now, (1) can be restated as

$$\lim_{N\to\infty}\ \frac{1}{N}\ \sum_{n\le N}\lambda(n)=0.$$

Since $\lambda(n)=1$ or -1 for every integer n, this is equivalent to the assertion that, asymptotically, half the values of $\lambda(n)$ are 1, and half are -1. In other words

$$\lim_{N\to\infty}\ \frac{1}{N}\ \#\{n\le N:\ \lambda(n)=1\}\quad\text{and}\quad\lim_{N\to\infty}\ \frac{1}{N}\ \#\{n\le N:\ \lambda(n)=-1\}$$

both exist and equal $\frac12$.

Mean values of multiplicative functions

More generally one can ask, for any given totally multiplicative $f:\mathbb{N}\to G$, where G is a given finite group, whether

$$\lim_{N\to\infty}\ \frac{1}{N}\ \#\{n\le N:\ f(n)=g\} \tag{2}$$

exists, for each $g\in G$. The answer is "yes", something that could have been proved directly from results of Wirsing and Halasz in the early 70s had they been aware of this nice question of Ruzsa. Once one knows that the limit in (2) always exists one can ask whether one can obtain upper and lower bounds that depend only on the group G. For example if $f(n)=1$ for all n then the value in (2) is 0 if $g\neq 1$, and equals 1 if $g=1$. One can thus ask whether it is possible to get the limit 1 in (2) when $g\neq 1$, and whether it is possible to get the limit 0 in (2) when $g=1$? To better understand, let's focus on the case $G=\{-1,1\}$. Evidently we cannot have $f(n)=-1$ for all n, since $f(1)=1$, and also $f(4)=f(9)=f(16)=\ldots=1$ since the square of both 1 and -1 equals 1. But even more, we cannot have all three of $f(2), f(3)$ and $f(6)$ equal to -1, since $f(6)=f(2)f(3)$, and indeed the same remark applies for any three multiplicatively dependent integers. In the 1980s Hall showed that for any totally multiplicative $f:\mathbb{N}\to\{-1,1\}$, we must have $f(n)=1$ for at least a positive proportion of the integers n up to any given point (so that the answer to both questions above is "no"). His proof can be extended to show that the answer to both questions above is "no" for any finite group G; that is, there exists a constant $c_G>0$ such that the proportion of integers $n\le N$ with $f(n)=1$ is always $\ge c_G$. Heath-Brown and Montgomery then asked for the minimum possible proportion of $f(n)$-values that equal 1 when $G=\{-1,1\}$. In 2001 Soundararajan and I proved [8] that at least 17.15% of the $f(n)$-values must equal 1, where 17.15% is an approximation for

$$1-\frac{\pi^2}{6}-\log(1+\sqrt{e})\log\frac{e}{1+\sqrt{e}}+2\sum_{n=1}^{\infty}\frac{1}{n^2}\frac{1}{(1+\sqrt{e})^n}=.1715004931\ldots,$$

and this is "best possible". It would be nice to have a combinatorial interpretation as to why this particular constant comes up here.

As the limit in (2) exists, we can deduce that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\le N} f(n) \tag{3}$$

exists whenever $f : \mathbb{N} \to G$, a finite group. This leads naturally to the question as to whether (3) exists for all totally multiplicative $f : \mathbb{N} \to \mathbb{U}$? Let us study the example $f(n) = n^{it}$ for given real number t: Here the mean value is

$$\frac{1}{N} \sum_{n\le N} n^{it} \approx \frac{1}{N} \int_0^N u^{it} dt = \frac{1}{N} \frac{N^{1+it}}{1+it} = \frac{N^{it}}{1+it},$$

for sufficiently large N. This equals $1/\sqrt{1+t^2}$ in absolute value, but varies in angle with N. That is,

$$\lim_{N\to\infty} \left| \frac{1}{N} \sum_{n\le N} f(n) \right| \tag{4}$$

exists but not (3). In fact, in general, (4) exists for all totally multiplicative $f : \mathbb{N} \to \mathbb{U}$, but (3) does not necessarily exist, as we have just seen.

Next we might ask, when is

$$\left| \frac{1}{N} \sum_{n\le N} f(n) \right| \tag{5}$$

large? That is, when is there not very much cancellation between different values of $f(n)$? Evidently (5) is large when $f(n) = 1$ for all $n \ge 1$, and, as we have just seen, more generally when $f(n) = n^{it}$ for all $n \ge 1$. Moreover we would not expect the mean value (5) to change much if we simply alter the values of f by a suitably small amount (though keeping f totally multiplicative). In other words if $f(n)$ is more-or-less n^{it} for some small real t then we would expect the mean value to be "large"; or, more colloquially, if $f(n)$ *pretends* to be n^{it}. Are there any other examples of f for which this mean value (5) is large? The remarkable result of Halasz [9,10] states that the answer to this question is "no":

Halasz (1975). *If the mean value of f is "large" in absolute value then $f(n)$ pretends to be n^{it} for some "small" real t.*

As you might expect Halasz was a little more precise in his formulation, but here we can make do with "large" meaning $> \epsilon$, "small" meaning $|t| \ll 1/\epsilon$, and "pretends" meaning that

$$\sum_{p\le N} \frac{1 - \mathrm{Re}(f(p)/p^{it})}{p} \quad \text{is bounded.} \tag{6}$$

This last quantity is worth discussing in a little more detail: If $f(n) = n^{it}$ for all $n \le N$ then $f(p) = p^{it}$ for all $p \le N$, that is $f(p)/p^{it} = 1$, or $1 - \mathrm{Re}(f(p)/p^{it}) = 0$. In other words, the quantity in (6) above would equal 0. As $f(n)$ varies more from n^{it}, we see that the quantity in (6) grows. We can extend this to define a useful distance function for pairs of multiplicative functions: If f and g are two multiplicative functions with values inside or on the unit circle define

$$\mathbb{D}(f, g; x)^2 := \sum_{p \le x} \frac{1 - \mathrm{Re}(f(p)\overline{g}(p))}{p}.$$

This has the desirable properties that $\mathbb{D}(f, g; x) = 0$ if and only if $f(p) = g(p)$ and $|f(p)| = 1$ for all primes $p \le x$, and that it satisfies the triangle inequality

$$\mathbb{D}(f, g; x) + \mathbb{D}(F, G; x) \ge \mathbb{D}(fF, gG; x).$$

Large character sums, I

One is interested in proving, for a non-principal character $\chi \pmod q$, that

$$\sum_{n \le x} \chi(n) = o(x) \tag{7}$$

in as wide a range for x as possible. Burgess [3] showed that (7) holds uniformly for $x > q^{1/4+o(1)}$, and the outstanding question in this area is to show that (7) holds uniformly for $x \ge q^{\epsilon}$. In [9] we showed that (7) holds whenever $\log x/\log\log q \to \infty$, assuming the Generalized Riemann Hypothesis; and that (7) cannot hold for smaller x, that is when $x = (\log q)^A$ for any fixed $A > 0$.

Now suppose that (7) fails for some character χ. By Halasz's theorem we know that $\chi(n)$ pretends to be n^{it} for some suitably small t. Hence $\chi^2(n)$ pretends to be n^{2it} and we might expect (7) to fail with χ replaced by χ^2. Indeed, in [11], we prove that if (7) fails for $\chi = \chi_i \pmod q$ for some $x_i > q^{\epsilon}$ for $i = 1$ and 2, then (7) fails for $\chi = \chi_1\chi_2$ for some $x > q^{\delta}$ with $\delta = \delta(\epsilon) > 0$.

The prime number theorem, II

Now that we have seen what pretentious means, a potentially complicated function looking very much like something far simpler, let us study an early example from the history of analytic number theory. By 1896 researchers only needed to show that $\zeta(1 + it) \ne 0$ for all non-zero real t, in order to complete the proof of the Prime Number Theorem. Both Hadamard and de la Vallée Poussin established that if $\zeta(1 + it) = 0$ then $\zeta(1 + 2it) = \infty$ contradicting the fact that $\zeta(s)$ is analytic except at $s = 1$. In his book [4], Davenport explains this by noting that if $\zeta(1 + it) = 0$ then the p^{it} would "predominantly" point towards -1, so that the p^{2it} would "predominantly" point towards 1. A clever identity of Mertens allows one to establish this connection rather elegantly, but here we go back to the original heuristic and see that it can be viewed as an early example of pretentiousness.

A pretentious proof of the Prime Number Theorem: We know that $\zeta(s)$ is analytic in $\mathrm{Re}(s) > 1$ except at $s = 1$. Suppose that $\zeta(1+it) = 0$ and that the zero at $1+it$ has order $r \geq 1$. Then $\zeta(1+\Delta+it) \approx c\Delta^r$ for some non-zero constant c when $|\Delta|$ is sufficiently small, as may be proved by studying the Taylor series for $\zeta(s)$ around $1+it$. Taking $\Delta = 1/\log x$ for sufficiently large x one can show that this is equivalent (see Appendix 1) to

$$\prod_{p\leq x}\left(1-\frac{1}{p^{1+it}}\right)^{-1} \approx \frac{c_1}{(\log x)^r},$$

which can be rewritten as

$$\prod_{p\leq x}\left(1+\frac{e^{-it\log p}}{p}\right) \approx \frac{c_2}{(\log x)^r},$$

for some non-zero constants c_1, c_2. Now Mertens' theorem states that

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x}.$$

Since $|1-1/p^{1+it}| \geq 1-1/p$, the last two estimates are incompatible unless $r = 1$. In that case we can directly compare the two estimates to deduce that $p^{-it} = e^{-it\log p}$ pretends to be -1; more precisely that $\mathbb{D}(p^{-it}, -1; x)$ is bounded. Squaring, we find that p^{-2it} pretends to be $(-1)^2 = 1$ (or, more precisely, $\mathbb{D}(p^{-2it}, 1; x) \leq 2\mathbb{D}(p^{-it}, -1; x)$ is bounded), and then reversing all of the steps above we deduce that $\zeta(1+\Delta+2it) \approx c''/\Delta$ for $\Delta > 0$ sufficiently small, that is $\zeta(s)$ diverges at $s = 1+2it$, contradicting the fact that it is analytic at this point. □

In this proof we deduced that p^{-it} pretends to be -1; we note that, if that were the case then n^{it} pretends to be $\lambda(n)$.

Large character sums, II

Let χ be a character mod $q > 1$. How large can

$$\max_{\chi}\left|\sum_{n\leq x}\chi(n)\right|$$

be? By periodicity we know that this is $\leq q$. The first important result on this question is the 1919 Pólya-Vinogradov inequality [17,19] which states that

$$\left|\sum_{n\leq x}\chi(n)\right| \leq \sqrt{q}\log q,$$

which was improved by Montgomery and Vaughan in 1977 [15], assuming the Generalized Riemann Hypothesis, to

$$\left|\sum_{n\le x}\chi(n)\right| \ll \sqrt{q}\log\log q. \tag{8}$$

In 1932 Paley [16] showed that this bound is best possible, up to the evaluation of the constant, by constructing quadratic characters $\chi \pmod q$ which pretend to be 1 for the primes $p \le c\log q$. Similarly if there are quadratic characters $\chi \pmod q$ which pretend to be 1 for the primes $p \le q^\epsilon$ then the Pólya-Vinogradov inequality cannot be improved.[2]

So when can $|\sum_{n\le x}\chi(n)|$ be large? Say $> \sqrt{q}(\log q)^{1-\delta}$ for some fixed small $\delta > 0$. Soundararajan and I [10] proved that if the character sum is this large then χ pretends to be a character $\psi \pmod m$ where $m \le (\log q)^{1/3}$. In fact $\chi(p) \approx \psi(p)$ for a surprisingly large proportion of the primes $p \le q$, which is surely impossible, though that is hard to prove.

One extra observation: If one has such a large character sum then one can show that $\chi(-1)\psi(-1) = -1$. This allows us to get a contradiction for χ of fixed, odd order.

Proof sketch when χ has order 3. In this case $\chi(n) = 0, 1, \omega$ or ω^2 for all integers n. Now $\chi(-1)^2 = \chi(1)^2 = 1$ so that $\chi(-1) = 1$, as χ cannot take the value -1. Therefore $\psi(-1) = 1\cdot\psi(-1) = \chi(-1)\cdot\psi(-1) = -1$. Hence for most small primes $p \equiv -1 \pmod m$ we have $\chi(p) \approx \psi(p) = \psi(-1) = -1$, which is impossible since none of $0, 1, \omega$ or ω^2 are close to -1.

In [10] we proved the following result:

Theorem. *If $\chi \pmod q$ has odd order $g > 1$ then*

$$\left|\sum_{n\le x}\chi(n)\right| \ll \sqrt{q}(\log q)^{1-\delta_g+o(1)},$$

where $\delta_g = \frac12(1 - \frac{\sin(\pi/g)}{\pi/g}) > 0$ (for example $1 - \delta_3 \approx 11/12$). Moreover, assuming the Generalized Riemann Hypothesis we have

$$\left|\sum_{n\le x}\chi(n)\right| \ll \sqrt{q}(\log\log q)^{1-\delta_g}.$$

A surprising revelation was that Montgomery and Vaughan's result (8) does not require the Generalized Riemann Hypothesis nor the Riemann Hypothesis for $L(s,\chi)$ but rather the Riemann Hypothesis for $L(s,\chi\overline{\psi})$. Note that $\chi\overline{\psi}$ is a character with large conductor which pretends to be 1.

[2]We do not believe that such q exist, but we do not know how to prove that they don't.

Suppose that we have a large character sum for χ, so that χ pretends to be ψ, a character with relatively small modulus, and $\chi(-1)\psi(-1) = -1$. Then χ^2 pretends to be ψ^2 with $\chi^2(-1)\psi^2(-1) = (-1)^2 = 1$, and χ^3 pretends to be ψ^3 with $\chi^3(-1)\psi^3(-1) = (-1)^3 = -1$, so we might guess that there is a a large character sum for χ^3. More generally, we prove in Theorem 2 of [10] that if characters χ_1, χ_2 and $\chi_3 \pmod q$ have large character sums then so does $\chi_1\chi_2\chi_3$. In particular note that if we have a big character sum for $\chi \pmod q$ of order 6, then we do for $\chi^3 \pmod q$ which has order 2.

Multiplicative functions in arithmetic progressions

Earlier we saw that if $\left|\frac{1}{N}\sum_{n\le N} f(n)\right|$ is large then $f(n)$ is n^{it}-pretentious for some "small" real t. What about if

$$\left|\frac{1}{N}\sum_{\substack{n\le N\\ n\equiv a \pmod q}} f(n)\right|$$

is large? There are several obvious examples for which this sum is large, for examples $f(n) = n^{it}$, and $f(n) = \chi(n)$ where χ is a Dirichlet character mod q (since then $f(n) = \chi(n) = \chi(a)$ for each n in the sum). One also has the two multiplied together, that is $f(n) = \chi(n)n^{it}$, and no more (as shown in [1]):

Theorem. *If the mean value of f is "large" in an arithmetic progression mod q then $f(n)$ pretends to be $\chi(n)n^{it}$ for some Dirichlet character χ mod q and some "small" real t.*

Pretentiousness is repulsive

Can a multiplicative function f be pretentious in more than one way? In other words, can there exist two characters ψ and χ with small conductors such that $f(n) \approx \psi(n)n^{it}$ and $f(n) \approx \chi(n)n^{iu}$ for most $n \le x$? If so then $\chi(n)n^{iu} \approx \psi(n)n^{it}$ for most $n \le x$, and hence $(\chi\overline{\psi})(n) \approx n^{i(u-t)}$ for most $n \le x$, which we know is impossible as $\chi\overline{\psi}$ is itself a character with small conductor. More precisely we have

$$\mathbb{D}(f(n), \chi(n)n^{iu}; x) + \mathbb{D}(f(n), \psi(n)n^{it}; x) \ge \mathbb{D}((\chi\overline{\psi})(n), n^{i(u-t)}; x) \gg (\log\log x)^{1/2}.$$

Exponential sums

If $\left|\sum_{n\le x} f(n)e^{2i\pi n\alpha}\right|$ is large then

- α is close to some rational a/b with b "small" (by [15]);
- $f(n)$ pretends to be $\psi(n)n^{it}$ where ψ is a character of conductor b and t is "small".

This characterization (given in [11]) has tremendous impact on questions that can be attacked by the circle method. For example, the number of solutions to

$$a + b = c$$

in integers $a, b, c \le x$ with $f(a) = f(b) = f(c) = 1$ where $f : \mathbb{N} \to \{-1, 1\}$, is

$$\ge \frac{1}{2}\% \text{ of } \#\{a, b, c \in \mathbb{N} : \ a, b, c \le x \text{ and } a + b = c\}.$$

Here $\frac{1}{2}\%$ is really $(17.15\%)^3$, where we have the 17.15% from before.

More generally, if f_1, f_2, f_3 are three totally multiplicative functions whose values all lie in $\mathbb{U}$, such that

$$\left| \sum_{\substack{a,b,c \le N \\ a+b=c}} f_1(a) f_2(b) f_3(c) \right| \ge \epsilon \frac{N^2}{2}$$

then $f_1(n), f_2(n), f_3(n)$ pretend to be $\psi_1(n)n^{it_1}, \psi_2(n)n^{it_2}, \psi_3(n)n^{it_3}$, respectively, where the t_i are bounded, the ψ_i are characters to small moduli, and $\psi_1\psi_2\psi_3$ is principal.

Prime number theorem for arithmetic progressions

We saw earlier that the primes up to x are equi-distributed in the arithmetic progressions mod q provided $x \ge x_{\epsilon,q}$, and that this has been proved unconditionally only for $x_{\epsilon,q}$ exponential in a power of q. However, in the late 1960s, Bombieri and Vinogradov [2] proved that one can take $x_{\epsilon,q}$ just a little bigger than q^2 for "most" q. It takes a little explanation to give the precise definition of "most" here, so we shall instead describe a variant, due to Gallagher, which is useful in many applications since it gives an explicit description of the exceptional moduli q if there are any:

Theorem. (Gallagher, 1970) *Let λ be Liouville's function. Given $\epsilon > 0$ there exists $A > 1$ such that*

$$\left| \sum_{\substack{n \le x \\ n \equiv a \pmod q}} \lambda(n) \right| \le \epsilon \frac{x}{q}$$

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

$$\left| \sum_{\substack{n \le x \\ n \equiv a \pmod q}} \lambda(n) \ - \ \psi(a) \sum_{\substack{n \le x \\ n \equiv 1 \pmod q}} \lambda(n) \right| \le \epsilon \frac{x}{q}$$

whenever $(a, q) = 1$ and r divides q, with $q \le x^{1/A}$. If this occurs then $\lambda(n)$ is $\psi(n)n^{it}$–pretentious for some small real t.

If this last case occurs, it would contradict the Generalized Riemann Hypothesis. In fact since $\lambda(n)$ is real-valued one can deduce that $t = 0$, that ψ must be a real-valued character, and that there is a zero of the $L(s, \psi)$ lying very close to $s = 1$. This exceptional zero is known as a "Siegel zero", and is typically believed to lie deep in the theory of Dirichlet L-functions.

We have proved the following generalization of Gallagher's theorem in [1]:

Theorem. (Balog, Soundararajan, Granville) *Let $f : \mathbb{N} \to \mathbb{U}$ be any totally multiplicative function. Given $\epsilon > 0$ there exists $A > 1$ such that*

$$\left| \sum_{\substack{n \le x \\ n \equiv a \pmod q}} f(n) \right| \le \epsilon \frac{x}{q}$$

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

$$\left| \sum_{\substack{n \le x \\ n \equiv a \pmod q}} f(n) \; - \; \psi(a) \sum_{\substack{n \le x \\ n \equiv 1 \pmod q}} f(n) \right| \le \epsilon \frac{x}{q}$$

whenever $(a, q) = 1$ and r divides q, with $q \le x^{1/A}$. If this occurs then $f(n)$ is $\psi(n)n^{it}$–pretentious for some small real t.

Gallagher's theorem is the special case $f(n) = \lambda(n)$ of this theorem. If we let $f(n) = \psi(n)n^{it}$ then the second case of the theorem does occur quite naturally. I am not sure what this implies about Siegel zeros, except to say that we are unlikely to rule out the possibility of their existence from an approach involving only the arithmetic theory of multiplicative functions.

This result gives mean value theorems for the coefficients of the Dirichlet series $L(s, f\chi)$ (where $L(s, f) := \sum_{n \ge 1} f(n)/n^s$) with proofs quite different from the usual "Tauberian methods" (indeed I can not see how these can be applied here).

One can write down a more precise version of our theorem: For $x^c \ge x^{1/A} \ge 3$ one can take

$$\epsilon = \frac{1}{\sqrt{\log A}}.$$

For small q, that is $q \le (\log x)^C$, one can take

$$\epsilon = \frac{1}{(\log x)^{1/3+o(1)}} + \frac{q}{(\log x)^{1+o(1)}};$$

and we can show that $1/3 + o(1)$ cannot be replaced by 1.

One step in the proof of this theorem is reminiscent of some of the recent developments in additive combinatorics. It can be paraphrased as "if a periodic function looks like a character then it more-or-less is a character". Specifically, if g has period q, with $g(1) = 1$ and $|g(ab) - g(a)g(b)| \le \epsilon$ $(\le 1/4)$ whenever $(a, b) = 1$ then there exists a character $\chi \pmod q$ such that $|\chi(a) - g(a)| \le 2\epsilon$ whenever $(a, q) = 1$.

How deep is the proof of our theorem? Given how far it generalizes Gallagher's theorem one might believe that it is necessary to use even deeper facts about the zeros of Dirichlet L-functions. On the other hand, given the generality of the result, one might

expect a proof that is more combinatorial in nature and less tied in with the distribution of prime numbers:

In our proof we require, for B and C sufficiently large and for each $(a,q)=1$, "lots" of primes $\equiv a \pmod q$ in an interval $[q^B, 2q^B]$, or "lots" of P2s $\equiv a \pmod q$ in an interval $[q^C, 2q^C]$ (where a "P2" is the product of two different primes.)

Our original proof used the theory of L-functions non-trivially: We noted that by Gallagher's theorem we have enough such primes except when there is a Siegel zero for some character $\psi \pmod q$ and $\psi(a)=1$. In that case almost all primes of this size satisfy $\psi(p)=-1$, so that most of the P2s n made up of these primes satisfy $\psi(n)=1$.

Subsequently we observed that our result follows if something like

$$\log x \sum_{\substack{p\le x\\ p\equiv a \pmod q}} \log p + \sum_{\substack{p_1p_2\le x\\ p_1p_2\equiv a \pmod q}} \log p_1 \log p_2 \sim \frac{2x\log x}{\phi(q)}$$

holds for each $(a,q)=1$ for a suitable value of x. Selberg [18] showed this for $x\ge e^q$ in his elementary proof of the prime number theorem for arithmetic progressions, a value of x which is far too large for our purposes. However in 1981 Friedlander [5] conveniently showed something close to this for all $x\ge q^{3B}$ using sieve methods, which means that our theorem can be proven, avoiding deeper consideration of the zeros of L-functions.

Appendix 1: Truncating Euler products

If $\Delta = 1/\log x$ then $\Delta>0$ so that $\zeta(1+\Delta+it)=\prod_p(1-1/p^{1+\Delta+it})^{-1}$. Hence $\log(\zeta(1+\Delta+it)\prod_{p\le x}(1-1/p^{1+it}))$ equals

$$\sum_{p\le x}\log\left((1-1/p^{1+it}))(1-1/p^{1+\Delta+it})^{-1}\right) - \sum_{p>x}\log\left(1-1/p^{1+\Delta+it}\right).$$

The absolute value of this is

$$\begin{aligned}
&\le \sum_{p\le x}\frac{1}{|p^{1+it}|}\left(1-\frac{1}{p^\Delta}\right)+\sum_{p>x}\frac{1}{p^{1+\Delta}}+2\sum_p\frac{1}{p^2}\\
&\ll \sum_{p\le x}\frac{\Delta\log p}{p}+\int_{u>x}\frac{du}{u^{1+\Delta}\log u}+1\\
&\ll \Delta\log x+\frac{x^{-\Delta}}{\Delta\log x}+1\ll 1.
\end{aligned}$$

Hence

$$\zeta(1+\Delta+it)\asymp\prod_{p\le x}\left(1-\frac{1}{p^{1+it}}\right)$$

References

1. A. Balog, A. Granville and K. Soundararajan, *Multiplicative Functions in Arithmetic Progressions* (to appear).
2. E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque **18** (1987/1974), 103 pp.
3. D.A. Burgess, *On character sums and L-series, I*, Proc. London Math. Soc **12** (1962), 193-206; II, Proc. London Math. Soc **13** (1963), 524-536.
4. H. Davenport, *Multiplicative number theory*, Springer Verlag, New York, 1980.
5. J.B. Friedlander, *Selberg's formula and Siegel's zero*, Recent progress in analytic number theory, Vol. 1 (Durham, 1979), Academic Press, London-New York, 1981, pp. 15–23.
6. P.X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math **11** (1970), 329–339.
7. A. Granville and G. Martin, *Prime Number Races*, Amer. Math. Monthly **113** (2006), 1–33.
8. A. Granville and K. Soundararajan, *The Spectrum of Multiplicative Functions*, Ann. of Math **153** (2001), 407–470.
9. _____, *Large Character Sums*, J. Amer. Math. Soc **14** (2001), 365–397.
10. _____, *Large Character sums: pretentious characters and the Pólya-Vinogradov theorem*, J. Amer. Math. Soc. **20** (2007), 357–384.
11. _____, *Large Character Sums: pretentious characters, Burgess's theorem and the location of zeros* (to appear).
12. G. Halász, *On the distribution of additive and mean-values of multiplicative functions*, Stud. Sci. Math. Hungar **6** (1971), 211-233.
13. _____, *On the distribution of additive arithmetic functions*, Acta Arith. **27** (1975), 143-152.
14. H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer Math Soc, Providence, Rhode Island, 2004.
15. H.L. Montgomery and R.C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math **43** (1977), 69-82.
16. R.E.A.C. Paley, *A theorem on characters*, J. London Math. Soc **7** (1932), 28-32.
17. G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Göttingen Nachrichten (1918), 21-29.
18. A. Selberg, *An elementary proof of the prime number theorem for arithmetic progressions*, Can. J. Math **2** (1950), 66-78.
19. I.M. Vinogradov, *Über die Verteilung der quadratischen Reste und Nichtreste*, J. Soc. Phys. Math. Univ. Permi **2** (1919), 1-14.

Département de Mathématiques et Statistique, Université de Montréal, CP 6128 succ Centre-Ville, Montréal, QC H3C 3J7, Canada

E-mail address: andrew@dms.umontreal.ca