SUMS OF MULTIPLICATIVE FUNCTIONS

Andrew Granville

Abstract. In these six hours of lectures we will discuss three themes that have been central to multiplicative number theory in the last few years: The uncertainty principle, bounds for character sums, and mean values of multiplicative functions. I will discuss many recent developments, in historical context, involving some proofs. The notes here are "pieced together" from several old articles of mine (mostly with Soundararajan, some alone, and some with Friedlander), so apologies to the reader for any disjointedness.

1. The Uncertainty Principle, in the twentieth century[1]

1.1. The distribution of Primes. 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

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 changes sign infinitely often (see, e.g. [GM]). 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 1859, Riemann, in a now famous memoir, illustrated how the question of estimating $\pi(x)$ could be turned into a question in analysis: Define $\zeta(s) := \sum_{n\ge1} n^{-s}$ for $\mathrm{Re}(s) > 1$, and then analytically continue $\zeta(s)$ to the rest of the complex plane. We have, for sufficiently large x,

$$x^{b-\epsilon} \ll \max_{y\le x} |\pi(y) - \mathrm{Li}(y)| \ll x^{b+\epsilon} \quad \text{where } b := \sup_{\zeta(\beta+i\gamma)=0} \beta. \tag{1.1}$$

The (as yet unproven) *Riemann Hypothesis* (RH) asserts that $b = 1/2$ (in fact that $\beta = 1/2$ whenever $\zeta(\beta + i\gamma) = 0$ with $0 \le \beta \le 1$) leading to the sharp estimate

$$\pi(x) \;=\; \mathrm{Li}(x) + O(x^{1/2}\log x)\ . \tag{1.2a}$$

[1] This section is an edited version of [Gr1].

It was not until 1896 that HADAMARD and DE LA VALLÉE POUSSIN independently proved that $\beta < 1$ whenever $\zeta(\beta + i\gamma) = 0$, which implies *The Prime Number Theorem*: that is, GAUSS's prediction that

$$\pi(x) \ \sim \ \mathrm{Li}(x) \ \sim \ \frac{x}{\log x}.$$

The best version known has an error term in which we do not even save a power of x:

$$\pi(x) = \mathrm{Li}(x) + O\left(x \Big/ \exp\left(\frac{c(\log x)^{3/5}}{(\log\log x)^{1/5}}\right)\right).$$

In 1914, LITTLEWOOD showed, unconditionally, that

$$\pi(x) - \mathrm{Li}(x) = \Omega_{\pm}\left(x^{1/2} \ \frac{\log\log\log x}{\log x}\right), \tag{1.2b}$$

the first proven 'irregularities' in the distribution of primes[2].

Since GAUSS's vague 'density assertion' was so prescient, CRAMÉR [Cra] decided, in 1936, to interpret GAUSS's statement more formally in terms of probability theory, to try to make further predictions about the distribution of prime numbers: Let $Z_2, Z_3, \ldots$ be a sequence of independent random variables with

$$\mathrm{Prob}(Z_n = 1) \ = \ \frac{1}{\log n} \quad \text{and} \quad \mathrm{Prob}(Z_n = 0) \ = \ 1 - \frac{1}{\log n} \ .$$

Let S be the space of sequences $T = z_2, z_3, \ldots$ and, for each $x \geq 2$ define

$$\pi_T(x) \ = \ \sum_{2 \leq n \leq x} z_n \ .$$

The sequence $P = \pi_2, \pi_3, \ldots$, where $\pi_n = 1$ if and only if n is prime, belongs to S. CRAMÉR wrote: "*In many cases it is possible to prove that,* with probability *1, a certain relation R holds for sequences in S ... Of course we cannot in general conclude that R holds for the particular sequence P, but results suggested in this way may sometimes afterwards be rigorously proved by other methods.*" For example CRAMÉR was able to show, with probability 1, that

$$\max_{y \leq x} |\pi_T(y) - \mathrm{Li}(y))| \sim \sqrt{2x \cdot \frac{\log\log x}{\log x}},$$

which corresponds well with the estimates in (1.2); and if true for $T = P$ implies RH, by (1.1).

GAUSS's assertion was really about primes in short intervals, and so is best applied to $\pi(x+y) - \pi(x)$, where y is "small" compared to x. The binomial random variables Z_n are more-or-less the same for all integers n in such an interval. If we take $y = \lambda \log x$ so that

[2] $f(x) = \Omega_{\pm}(g(x))$ means that there exists a constant $c > 0$ such that $f(x_+) > cg(x_+)$ and $f(x_-) < -cg(x_-)$ for certain arbitrarily large values of $x_{\pm}$.

the 'expected' number of primes, λ, in the interval is fixed then we would expect that the number of primes in such intervals should follow a Poisson distribution. Indeed, we can prove that for any fixed $\lambda > 0$ and integer $k \geq 0$, we have

$$\#\{\text{integers } x \leq X : \quad \pi_T(x + \lambda \log x) - \pi_T(x) = k\} \sim e^{-\lambda} \frac{\lambda^k}{k!} X \tag{1.3}$$

as $X \to \infty$, with probability 1 for $T \in S$. In 1976, GALLAGHER [Ga2] showed that this holds for the sequence of primes (that is, for P) under the assumption of a reasonable "uniform" version of HARDY AND LITTLEWOOD's *Prime k-tuplets conjecture* . This conjecture is the case where we take each $f_j(x)$ to be a linear polynomial in SCHINZEL AND SIERPIŃSKI's

Hypothesis H. *Let $F = \{f_1(x), f_2(x), \dots, f_k(x)\}$ be a set of irreducible polynomials with integer coefficients. Then the number of integers $n \leq x$ for which each $|f_j(n)|$ is prime is*

$$\pi_F(x) = \{C_F + o(1)\} \frac{x}{\log |f_1(x)| \log |f_2(x)| \dots \log |f_k(x)|}$$
$$\text{where} \quad C_F = \prod_{p \text{ prime}} \left(1 - \frac{\omega_F(p)}{p}\right) \Big/ \left(1 - \frac{1}{p}\right)^k,$$

and $\omega_F(p)$ counts the number of integers n, in the range $1 \leq n \leq p$, for which $f_1(n) f_2(n) \dots f_k(n) \equiv 0 \pmod p$[3] [,4].

Estimates analogous to (1.2a) should hold for the number of primes in intervals of various lengths, if we believe that what almost always occurs in S, should also hold for P. Specifically, if $10 \log^2 x \leq y \leq x$ then

$$\pi_T(x + y) - \pi_T(x) \;=\; \mathrm{Li}(x + y) - \mathrm{Li}(x) + O(y^{1/2}) \tag{1.4}$$

with probability 1 for $T \in S$. In 1943 SELBERG [Sl1] showed that primes do, on the whole, behave like this by proving, under the assumption of RH, that

$$\pi(x + y) - \pi(x) \sim \frac{y}{\log x} \tag{1.5}$$

for 'almost all' integers x, provided $y/\log^2 x \to \infty$ as $x \to \infty$.

CRAMÉR's model does seem to accurately predict what we already believe to be true about primes for more substantial reasons[5]. To be sure, one can find small discrepancies[6]

[3]Elementary results on prime ideals guarantee that the product defining C_F converges if the primes are taken in ascending order.

[4]The asymptotic formula proposed here for $\pi_F(x)$ has a 'local part' C_F, which has a factor corresponding to each rational prime p, and an 'analytic part' $x/\prod_i \log |f_i(x)|$. This reminds one of formulae which arise when counting points on varieties.

[5]Though HARDY AND LITTLEWOOD remarked thus on probabilistic models: "*Probability is not a notion of pure mathematics, but of philosophy or physics*"

[6]As has been independently pointed out to me by SELBERG, MONTGOMERY and PINTZ: for example, PINTZ noted that the mean square of $|\psi(y) - y|$ for $y \leq x$, is $\gg x^{2b-\varepsilon}$ (with b as in (1.1)), in fact $\asymp x$ assuming RH, whereas the probabilistic model predicts $\asymp x \log x$.

but the probabilistic model usually gives one a strong indication of the truth. CRAMÉR made one conjecture, based on his model, which does not seem to be attackable by other methods: If $p_1 = 2 < p_2 = 3 < p_3 = 5 < \dots$ is the sequence of prime numbers then

$$\max_{p_n \le x} (p_{n+1} - p_n) \sim \log^2 x.$$

This statement (or the weaker $O(\log^2 x)$) is known as '*Cramér's Conjecture*'; there is some computational evidence to support it:

p_n	$p_{n+1} - p_n$	$(p_{n+1} - p_n)/\log^2 p_n$
31397	72	.6715
370261	112	.6812
2010733	148	.7025
20831323	210	.7394
25056082087	456	.7953
2614941710599	652	.7975
19581334192423	766	.8177
218209405436543	906	.8311
1693182318746371	1132	.9206

Record-breaking gaps between primes, up to 5×10^{16}

In 1985 MAIER [Mai] surprisingly proved that, despite SELBERG showing (1.5) holds 'almost all' the time when $y = \log^B x$ (assuming RH) for fixed $B > 2$, it cannot hold all of the time for such y. This not only radically contradicts what is predicted by the probabilistic model, but also what most researchers in the field had believed to be true, whether or not they had faith in the probabilistic model. Specifically, MAIER showed the existence of a constant $\delta_B > 0$ such that for occasional, but arbitrarily large, values of x_+ and x_-,

$$\begin{aligned} &\pi(x_+ + \log^B x_+) - \pi(x_+) \ > \ (1+\delta_B)\log^{B-1} x_+ \ , \\ \text{and} \qquad &\pi(x_- + \log^B x_-) - \pi(x_-) \ < \ (1-\delta_B)\log^{B-1} x_-. \end{aligned} \tag{1.6}$$

Outline of the Proof. There are $\sim e^{-\gamma} x/\log z$ integers $\le x$, all of whose prime factors are $> z$, provided z is not too large. Among these we have all but $\pi(z)$ of the primes $\le x$, and so the probability that a randomly chosen such integer is prime is $\sim e^{\gamma}\log z/\log x$. Thus in a specific interval $(x, x+y]$ we should 'expect' $\sim e^{\gamma}\Phi \log z/\log x$ primes, where Φ is the number of integers in the interval that are free of prime factors $\le z$. Now if we can select our interval so that $\Phi \not\sim e^{-\gamma} y/\log z$ then our new prediction is not the same as that in (1.5).

If x is divisible by $P = \prod_{p \le z} p$ then

$$\Phi = \Phi(y,z) := \#\{1 \le n \le y : \ p|n \Rightarrow p > z\} \sim \omega(u)\frac{y}{\log z}$$

for $y = z^u$ with u fixed, where $\omega(u)$, the *Buchstab function*, equals 0 if $0 < u < 1$ and satisfies the differential-delay equation $u\,\omega(u) = 1 + \int_1^{u-1} \omega(t)\mathrm{d}t$ if $u \ge 1$. Obviously

$\lim_{u\to\infty}\omega(u)=\mathrm{e}^{-\gamma}$. IWANIEC showed that $\omega(u)-\mathrm{e}^{-\gamma}$ oscillates, crossing zero either once or twice in every interval of length 1. Thus if we fix $u>B$, chosen so that $\omega(u)>\mathrm{e}^{-\gamma}$ or $<\mathrm{e}^{-\gamma}$ (as befits the case of (1.6)), select $y=\log^B x$ and $z=y^{1/u}$, and 'adjust' x so that it is divisible by P, then we expect (1.5) to be false.

1.2. Maier matrices. To convert this heuristic into a proof, MAIER considered a progression of intervals of the form $(rP, rP+y]$, with $R\le r<2R$ for a suitable value of R. Visualizing this as a 'matrix', with each such interval represented by a different row, we see that the primes in the matrix are all contained in those columns j for which $(j,P)=1$.

$RP+1$	$RP+2$	$RP+3$	$\cdots$	$RP+y$
$(R+1)P+1$	$(R+1)P+2$	$(R+1)P+3$	$\cdots$	$(R+1)P+y$
$(R+2)P+1$	$(R+2)P+2$	$\cdot$	$\cdot$	$\vdots$
$(R+3)P+1$	$\vdots$	(i,j)th entry : $(R+i)P+j$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\cdot$	$\vdots$	$\vdots$
$(2R-1)P+1$	$(2R-1)P+2$	$\cdots$	$\cdots$	$(2R-1)P+y$

The 'Maier Matrix' for $\pi(x+y)-\pi(x)$

Now, for any integer $q>1$, the primes are roughly equi-distributed amongst those arithmetic progressions $a \pmod q$ with $(a,q)=1$: in fact up to x we expect that the number of such primes

$$\pi(x;q,a)\ \sim\ \frac{\pi(x)}{\phi(q)}. \tag{1.7}$$

If so, then the number of primes in the jth column, when $(j,P)=1$, is

$$\pi(2X;P,j)-\pi(X;P,j)\sim\frac{1}{\phi(P)}\frac{X}{\log X}\quad\text{where } X=RP.$$

To get the total number of primes in the matrix we sum over all such j, and then we can deduce that, on average, a row contains

$$\sim\ \frac{\Phi(y,z)}{R}\frac{1}{\phi(P)}\frac{RP}{\log RP}\ \sim\ \omega(u)\frac{y}{\log z}\frac{P}{\phi(P)}\frac{1}{\log RP}\ \sim\ \mathrm{e}^{\gamma}\omega(u)\frac{y}{\log RP}$$

primes. MAIER's result follows provided we can prove a suitable estimate in (1.7)

In general, it is desirable to have an estimate like (1.7) when x is not too large compared to q. It has been proved that (1.7) holds uniformly for[7]

i) All $q\le\log^B x$ and all $(a,q)=1$, for any fixed $B>0$ (SIEGEL-WALFISZ).[8]

[7]We believe, but cannot prove, that (1.7) holds uniformly for all $q\le x^{1-\epsilon}$ based on what computations appear to reveal.

[8]It is impossible to give all the constants explicitly in the resulting version of (1.7) because the proof works in two parts: first, if GRH is true, and second, by using a putative counterexample to GRH, if one exists. Hence if GRH is true but remains unproved one cannot, by the very nature of this proof, determine the constants involved. An alternate argument does provide all the constants involved in the more limited range $B\le 2$.

ii) All $q \le \sqrt{x}/\log^{2+\epsilon} x$ and all $(a,q)=1$, assuming GRH[9]. In fact (1.7) then holds with error term $O\left(\sqrt{x}\log^2(qx)\right)$.
iii) Almost all $q \le \sqrt{x}/\log^{2+\epsilon} x$ and all $(a,q)=1$ (Bombieri-Vinogradov)[10].
iv) Almost all $q \le x^{1/2+o(1)}$ with $(q,a)=1$, for fixed $a \ne 0$ (Bombieri-Friedlander-Iwaniec, Fouvry)
v) Almost all $q \le x/\log^{2+\epsilon} x$ and almost all $(a,q)=1$ (Barban-Davenport-Halberstam, Montgomery, Hooley).

Thus, when GRH is true, we get a good enough estimate in (1.7) with $R = P^2$ to complete Maier's proof. However Maier, in the spirit of the Bombieri-Vinogradov Theorem, showed how to pick a '*good*' value for P, so that (1.7) is off by, at worst, an insignificant factor when R is a large, but fixed, power of P (thus proving his result unconditionally).

In [GS7], we extended the range for y in the proof above, establishing that there are intervals $(x, x+y]$ in every interval $[X, 2X]$ for which (1.4) fails to hold for some $y > \exp\left(c(\log x/\log\log x)^{1/2}\right)$.

It is plausible that (1.5) holds uniformly if $\log y/\log\log x \to \infty$ as $x \to \infty$; and that (1.4) holds uniformly for $T = P$ if $y > \exp\left((\log x)^{1/2+\epsilon}\right)$ (at least, we can't disprove these statements as yet). We conjecture, presumably safely, that (1.4) and (1.5) hold uniformly when $y > x^{\epsilon}$.

One can show that there are more than $x/\exp\left((\log x)^{c_B}\right)$ integers $x_{\pm} \le x$ satisfying the unexpected inequalities in (1.6).

Maier's work suggests that Cramér's model should be adjusted to take into account divisibility of n by 'small' primes[11]. It is plausible to define 'small' to mean those primes up to a fixed power of $\log n$. Then we are led to conjecture that there are infinitely many primes p_n with $p_{n+1} - p_n > 2e^{-\gamma}\log^2 p_n$, contradicting Cramér's conjecture, as $2e^{-\gamma} > 1$.[12]

If we analyze the distribution of primes in arithmetic progressions using a suitable analogue of Cramér's model, then we would expect (1.7), and even

$$\pi(x;q,a) \;=\; \frac{\pi(x)}{\phi(q)} + O\left(\left(\frac{x}{q}\right)^{1/2}\log(qx)\right)\;, \tag{1.7$'$}$$

to hold uniformly when $(a,q)=1$ in the range

$$q \le Q = x/\log^B x\;, \tag{1.8}$$

for any fixed $B > 2$. However the method of Maier is easily adapted to show that neither (1.7) nor (1.7′) cannot hold in at least part of the range (1.8): For any fixed

[9]The *Generalized Riemann Hypothesis* (GRH) states that if $\beta+i\gamma$ is a zero of *any* Dirichlet L-function then $\beta \le 1/2$

[10]This result is often referred to as 'GRH on average'. See section 6.4 for another result of this type.

[11]One has to be careful about the meaning of 'small' here, since if we were to take into account the divisibility of n by all primes up to $\sqrt{n}$, then we would conclude that there are $\sim \mathrm{e}^{-\gamma}x/\log x$ primes up to x.

[12]It is unclear what the 'correct conjecture' here should be since, to get at it with this approach, we would need more precise information on 'sifting limits' than is currently available.

$B > 0$ there exists a constant $\delta_B > 0$ such that for any modulus q, with 'not too many small prime factors', there exist arithmetic progressions $a_\pm \pmod q$ and values $x_\pm \in [\phi(q)\log^B q, 2\phi(q)\log^B q]$ such that

$$\pi(x_+;q,a_+) \ > \ (1+\delta_B)\frac{\pi(x_+)}{\phi(q)} \quad \text{and} \quad \pi(x_-;q,a_-) \ < \ (1-\delta_B)\frac{\pi(x_-)}{\phi(q)} \ . \tag{1.9}$$

The proof is much as before, though now using a modified 'Maier matrix':

RP	$RP+q$	$RP+2q$	$\cdots$	$RP+yq$
$(R+1)P$	$(R+1)P+q$	$(R+1)P+2q$	$\cdots$	$(R+1)P+yq$
$(R+2)P$	$(R+2)P+q$	$\cdot$	$\cdot$	$\vdots$
$(R+3)P$	$\vdots$	(i,j)th entry : $(R+i)P+jq$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\cdot$	$\vdots$	$\vdots$
$(2R-1)P$	$(2R-1)P+q$	$\cdots$	$\cdots$	$(2R-1)P+yq$

The Maier Matrix for $\pi(yq;q,a)$

The Bombieri-Vinogradov Theorem is usually stated in a stronger form than above: For any given $A > 0$, there exists a value $B = B(A) > 0$ such that

$$\sum_{q\le Q} \max_{(a,q)=1} \max_{y\le x} \left|\pi(y;q,a) - \frac{\pi(y)}{\phi(q)}\right| \ll \ \frac{x}{\log^A x} \tag{1.10}$$

where $Q = \sqrt{x}/\log^B x$. It is possible [FG1] to take the same values of R and P in the Maier matrix above for many different values of q, and thus deduce that there exist arbitrarily large values of a and x for which

$$\left| \sum_{\substack{Q\le q\le 2Q\\(q,a)=1}} \left\{\pi(x;q,a) - \frac{\pi(x)}{\phi(q)}\right\} \right| \gg x; \tag{1.11}$$

thus refuting the conjecture that for any given $A > 0$, (1.10) should hold in the range (1.8) for some $B = B(A) > 0$. In [FG2] we showed that (1.10) even fails with

$$Q \ = \ x/\exp\big((A-\epsilon)(\log\log x)^2/(\log\log\log x)\big) \, .$$

In [GS7] we showed that, for any $q \ge x/\exp\big((\log x)^{1/2-\epsilon}\big)$, the bound (1.7′) cannot hold for every integer a prime to q.

It seems plausible that (1.7) holds uniformly if $\log(x/q)/\log\log q \to \infty$ as $q \to \infty$; and that (1.10) holds uniformly for $Q < x/\exp\big((\log x)^{1/2+\epsilon}\big)$. At least we can't disprove

these statements as yet, though we might play it safe and conjecture only that they hold uniformly for $q, Q < x^{1-\epsilon}$.

Notice that in the proof described above, the values of a increase with x, leaving open the possibility that (1.7) might hold uniformly for all $(a, q) = 1$ in the range (1.8) if we fix a.[13] However, in [FG3] we observed that when a is fixed one can suitably modify the Maier matrix, by forcing the elements of the second column to all be divisible by P:

1	$1+(RP-1)$	$1+2(RP-1)$	$\cdots$	$1+y(RP-1)$
1	$1+((R+1)P-1)$	$1+2((R+1)P-1)$	$\cdots$	$1+y((R+1)P-1)$
1	$1+((R+2)P-1)$	$\cdot$	$\cdot$	$\vdots$
1	$\vdots$	(i,j)th entry : $1+j((R+i)P-1)$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\cdot$	$\vdots$	$\vdots$
1	$1+((2R-1)P-1)$	$\cdots$	$\cdots$	$1+y((2R-1)P-1)$

The Maier Matrix for $\pi(yq; q, 1)$

Notice that the jth column here is now part of an arithmetic progression with a varying modulus, namely $1 - j \pmod{jP}$. With this type of Maier matrix we can deduce that, for almost all $0 < |a| < x/\log^B x$ (including all fixed $a \neq 0$), there exist $q \in (x/\log^B x, 2x/\log^B x]$, coprime to a, for which (1.7) does not hold. However (1.7) cannot be false too often (like in (1.11)), since this would contradict the Barban-Davenport-Halberstam Theorem. So for which a is (1.7) frequently false? It turns out that the answer depends on the number of prime factors of a: In [FG5], extending the results of [BFI], we show that for any given $A > 1$ there exists a value $B = B(A) > 0$ such that, for any $Q \le x/\log^B x$ and any integer a which satisfies $0 < |a| < x$ and has $\ll \log\log x$ distinct prime factors[14], we have

$$\left| \sum_{\substack{Q \le q \le 2Q \\ (q,a)=1}} \left\{ \pi(x; q, a) - \frac{\pi(x)}{\phi(q)} \right\} \right| \ll \frac{x}{\log^A x}. \tag{1.12}$$

On the other hand, assuming GRH, for every given $A, B > 0$, there exists $Q \le x/\log^B x$ and an integer a for which (1.12) does not hold, where $0 < |a| < x$ and a has $< (\log\log x)^{1+\epsilon}$ distinct prime factors.

Finding primes in $(x, x+y]$ is equivalent to finding integers $n \le y$ for which $f(n)$ is prime, where $f(t)$ is the polynomial $t + x$. Similarly, finding primes $\le x$ which belong to the arithmetic progression $a \pmod q$, is equivalent to finding integers $n \le y := x/q$ for which $f(n)$ is prime, where $f(t)$ is the polynomial $qt + a$. Define the *height*, $h(f)$, of a given

[13] Which would be consistent with the Barban-Davenport-Halberstam Theorem.

[14] which includes almost all integers a once the inexplicit constant here is > 1 (by a famous result of Hardy and Ramanujan).

polynomial $f(t) = \sum_i c_i t^i$ to be $h(f) := \sqrt{\sum_i c_i^2}$. In the cases above, in which the degree is always 1, we proved that we do not always get the asymptotically expected number of prime values $f(n)$ with $n \le y = \log^B h(f)$, for any fixed $B > 0$. In [FG4] we showed that this is true for polynomials of arbitrary degree d, which is somewhat ironic since it is not known that *any* polynomial of degree ≥ 2 takes on infinitely many prime values, nor that the prime values are ever 'well-distributed'. Nair and Perelli [NP] showed that some of the polynomials $F_R(n) = n^d + RP$ attain more than, and others attain less than, the number of prime values expected in such a range, by considering the following Maier matrix:

$F_R(1)$	$F_R(2)$	$F_R(3)$	$\cdots$	$F_R(y)$
$F_{R+1}(1)$	$F_{R+1}(2)$	$F_{R+1}(3)$	$\cdots$	$F_{R+1}(y)$
$F_{R+2}(1)$	$F_{R+2}(2)$	.	.	$\vdots$
$F_{R+3}(1)$	$\vdots$	(i,j)th entry : $F_{R+i}(j)$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	.	$\vdots$	$\vdots$
$F_{2R-1}(1)$	$F_{2R-1}(2)$	$\cdots$	$\cdots$	$F_{2R-1}(y)$

The Maier Matrix for $\pi_F(y)$

Notice that the jth column here is part of the arithmetic progression $j^d \pmod P$.

Using Maier matrices it is possible to prove 'bad equi-distribution' results for primes in other interesting sequences, such as the values of binary quadratic forms, and of prime pairs. For example, if we fix $B > 0$ then, once x is sufficiently large, there exists a positive integer $k \le \log x$ such that there are at least $1 + \delta_B$ times as many prime pairs $p, p + 2k$, with $x < p \le x + \log^B x$, as we would expect from assuming that the estimate in Hypothesis H holds uniformly for $n \ll \log^B h((t + x)(t + (x + 2k)))$.

We have now seen that the asymptotic formula in Hypothesis H fails when x is an arbitrary fixed power of $\log h(F) (:= \sum_i \log h(f_i))$, for many different non-trivial examples F. Presumably the asymptotic formula *does* hold uniformly as $\log x / \log\log h(F) \to \infty$. However, to be safe, we only make the following prediction:

Conjecture. *Fix $\varepsilon > 0$ and positive integer k. The asymptotic formula in Hypothesis H holds uniformly for $x > h(F)^\varepsilon$ as $h(F) \to \infty$.*

Our work here shows that the 'random-like' behaviour exhibited by primes in many situations does not carry over to *all* situations. It remains to discover a model that will always accurately predict how primes are distributed, since it seems that minor modifications of Cramér's model will not do. We thus agree that:

> *"It is evident that the primes are randomly distributed but, unfortunately, we don't know what 'random' means."* — R.C. Vaughan (February 1990).

1.3. And beyond. Armed with Maier's ideas it seems possible to construct incorrect conclusions from, more-or-less, any variant of Cramér's model. This flawed model may still be used to make conjectures about the distribution of primes, but one should be very cautious of such predictions!

There are no more than $O(x^2/\log^{3B} x)$ arithmetic progressions $a \pmod q$, with $1 \le a < q < x/\log^B x$ and $(a,q) = 1$, for which (1.7) fails, by the Barban-Davenport-Halberstam Theorem. However our methods here may be used to show that (1.7) does fail for more than $x^2/\exp((\log x)^\epsilon)$ such arithmetic progressions.

Maier's matrix has been used in other problems too: Konyagin used it to find unusually large gaps between consecutive primes. Maier used it to find long sequences of consecutive primes, in which there are longer than average gaps between each pair. Shiu has used it to show that every arithmetic progression $a \pmod q$ with $(a,q) = 1$ contains arbitrarily long strings of consecutive primes. Recently Thorne[15] generalized these ideas to function fields, and to Gaussian primes.

Despite the efforts of several mathematicians we have still not got a particularly good model to replace the now discredited model of Cramér. Certainly not a well-motivated one, so there are still many questions about the distribution of primes in which we cannot even guess at the right answer with much confidence. This is not a new complaint:

> *"Mathematicians have tried in vain to discover some order in the sequence of prime numbers but we have every reason to believe that there are some mysteries which the human mind will never penetrate."*
>
> — L. Euler (1770).

2. The Uncertainty Principle, in the twenty-first century

2.1. A general phenomenon. I ended my 1994 ICM talk with Euler's quote – it seemed fitting since these counterintuitive extensions of Maier's results seemed to be something to do with Euler's observation that primes refuse, in almost every way, to be easily understood. There was a hiatus in developments in this subject, until a paper of Balog and Wooley [BW] appeared in 2000. There they applied the same circle of ideas to the integers that are the sum of two squares, and proved an analogous result to that of Maier. My first reaction when I heard about their work was that it was nice they had generalized things beyond primes, but was this really so interesting? Especially as it was probably technically easier than Maier's work on primes? They sent me a reprint of their paper and it sat unread on my desk for an embarrassingly long time. After two years I picked it up and almost immediately realized that what they had done was a big surprise and their work surely pointed the way to an important phenomenon ... The point is that I had thought that irregularities in the distribution of primes came about because primes are always "strange", but here Balog and Wooley had taken a relatively civilized sequence, one with very predictable multiplicative structure even, and found similar irregularities in the distribution. This meant that Maier's proof was surely nothing to do with primes and must be the harbinger of a *much more general phenomenon*. Indeed this intuition was correct and Sound and I were able to prove a very general "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.

[15] In his 2008 Ph.D. at Madison.

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 our sequence coming from arithmetic. Sieve theory already provides a framework for considering analytic properties of "arithmetic sequences", so this is our starting point:

$\mathcal{A}$ could be a set of integers but, more generally, let $\mathcal{A}$ denote a sequence $a(n)$ of non-negative real numbers, and $\mathcal{A}(x) = \sum_{n\le x} a(n)$. If the $a(n)$ are well-distributed in short intervals then we expect

$$\mathcal{A}(x+y) - \mathcal{A}(x) \approx y\frac{\mathcal{A}(x)}{x}, \tag{2.1}$$

for suitable y.

Suppose that the proportion of $\mathcal{A}$ which is divisible by d is approximately $h(d)/d$ where $h(.)$ is a non-negative multiplicative function; in other words,

$$\mathcal{A}_d(x) := \sum_{\substack{n\le x\\ d|n}} a(n) \approx \frac{h(d)}{d}\mathcal{A}(x), \tag{2.2}$$

for each d.[16] 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 any integer d_2 which is coprime with d_1.

If the asymptotic behavior of $\mathcal{A}$ in the arithmetic progression $a \pmod q$, depends only on (a,q) when $(q,\mathcal{S})=1$ then, by (2.2), we arrive at the prediction that, for $(q,\mathcal{S})=1$,

$$\mathcal{A}(x;q,a) := \sum_{\substack{n\le x\\ n\equiv a \pmod q}} a(n) \approx \frac{f_q(a)}{q\gamma_q}\mathcal{A}(x), \tag{2.3}$$

where $\gamma_q = \prod_{p|q}((p-1)/(p-h(p)))$ and $f_q(a)$ is a certain non-negative multiplicative function of a for which $f_q(a) = f_q((a,q))$ (thus $f_q(a)$ is periodic $\pmod q$).[17]

Example 1. We take $a(n)=1$ for all n, so that $h(n)=1$ for all n. Then $f_q(a)=1$ for all q and all a, and $\gamma_q = 1$. Clearly both (2.3) and (2.1) 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, so that $h(n)=1$ 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 (2.3) 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 (2.3), and Maier's result sets limitations to (2.1).

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 (2.1).

A weak form of our main results are given in the next two Theorems:

[16] Or perhaps when $(d,\mathcal{S})=1$, where $\mathcal{S}$ is a finite set of 'bad' primes.

[17] We prove this in section 2.2 below, giving an explicit description of f_q in terms of h.

Theorem 2.1. *Let $\mathcal{A}$, $\mathcal{S}$, h, f_q and γ_q be as above. For given $\alpha > 0$ there exist constants $c' > 0$, $c > 1$ such that, for sufficiently large x, if either*

$$\sum_{p \le \log x} \frac{\max\{0, 1 - h(p)\}}{p} \log p \ge \alpha \log\log x, \tag{2.4}$$

or there exists $n \le x$ with $h(n) \ge (\log x)^{c'}$, and if $1 \ll u \ll (\log x)^{c'}$ then 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

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

The condition (2.4) ensures that $h(p)$ is not always close to 1; this is essential in order to eliminate the very well behaved Example 1.

One can show that $\frac{\mathcal{A}(x)}{\phi(\ell)} \ge \frac{1}{\ell\gamma_\ell} y \frac{\mathcal{A}(x)}{x}$. It is good to not have $f_\ell(a)$ in the lower bound since it may well be 0.

Theorem 2.1 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 also applies to any subset of the primes:

Example 4. Let $\mathcal{A}$ be *any* subset of the primes. Fix $u \ge 1$. For any x there exists $y \in (x/4, x)$ such that either

$$|\mathcal{A}(y)/y - \mathcal{A}(x)/x| \gg_u \mathcal{A}(x)/x \tag{2.5a}$$

(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

$$\Big|\mathcal{A}(y; \ell, a) - \frac{\mathcal{A}(y)}{\phi(\ell)}\Big| \gg_u \frac{\mathcal{A}(x)}{\phi(\ell)}. \tag{2.5b}$$

In other words, we find "Maier type" irregularities in the distribution of *any subset of the primes*.[18] A similar result holds for any subset of the numbers that are sums of two squares.

Let $\mathcal{S}_\epsilon$ be the set of integers n having no prime factors in the interval $[(\log n)^{1-\epsilon}, \log n]$, so that $\mathcal{S}_\epsilon(N) \sim (1 - \epsilon)N$. Notice that the primes are a subset of $\mathcal{S}_\epsilon$. Theorem 2.1 with $\alpha \ge \epsilon + o(1)$ implies that any subset $\mathcal{A}$ of $\mathcal{S}_\epsilon$ is poorly distributed in that for any x there exists $y \in (x/4, x)$ such that either (2.5a) 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 (2.5b) holds (that is with $\phi(\ell)$ replaced by $\ell \prod_{p|\ell,\ (\log x)^{1-\epsilon} < p < \log x}(1 - 1/p)$).

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

[18] 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 $(\ell, \mathcal{S}) = 1$", where $(\ell, \mathcal{S}) = 1$ means that $(\ell, p) = 1$ for all $p \in \mathcal{S}$.

Theorem 2.2. *Let $\mathcal{A}$, $\mathcal{S}$, h, f_q and γ_q be as above. For given $\alpha > 0$ there exist constants $c' > 0$, $c > 1$ such that, for sufficiently large x, if either (2.4) holds or there exists $n \le x$ with $h(n) \ge (\log x)^{c'}$, and if $1 \ll u \ll (\log x)^{c'}$ then 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*

$$\Big|\mathcal{A}(v+y) - \mathcal{A}(v) - y\frac{\mathcal{A}(x)}{x}\Big| \gg u^{-cu} y\frac{\mathcal{A}(x)}{x}.$$

(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*

$$\Big|\mathcal{A}(y; q, a) - \frac{f_q(a)}{q\gamma_q} y\frac{\mathcal{A}(x)}{x}\Big| \gg u^{-cu}\frac{\mathcal{A}(x)}{\phi(q)}.$$

This is aptly named an "uncertainty principle" for we can construct sequences which are well distributed in short intervals (and then must have fluctuations in arithmetic progressions), and primes are known to be well-distributed in these long arithmetic progressions (and so exhibit fluctuations in short intervals).

Our proofs develop Maier's "matrix method": 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 (as we will discuss in section 2.3). In section 3.4 we will prove an analogy of such oscillation results for a wide class of related integral equations, which has the flavor of a classical "uncertainty principle" from Fourier analysis (and hence the nomenclature).

2.2. The new framework. We may assume that $h(p^k) < p^k$ for all prime powers p^k without any significant loss of generality.

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. Writing $(q, a) = m$, since $|\{b \pmod q : (b, q) = m\}| = \varphi(q/m)$, we then guess that

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

Using now (2.2) we would guess that

$$\mathcal{A}(x; q, a) \approx \mathcal{A}(x)\frac{1}{\varphi(q/m)} \sum_{d|\frac{q}{m}} \mu(d)\frac{h(dm)}{dm} =: \frac{f_q(a)}{q\gamma_q}\mathcal{A}(x), \tag{2.6}$$

where

$$\gamma_q = \prod_{p|q} \Big(\frac{1 - h(p)/p}{1 - 1/p}\Big)^{-1} = \prod_p \Big(1 - \frac{1}{p}\Big)\Big(1 + \frac{f_q(p)}{p} + \frac{f_q(p^2)}{p^2} + \dots\Big), \tag{2.7}$$

and $f_q(a)$, a multiplicative function with $f_q(a) = f_q((a,q))$ so that it has period q, is defined as follows: $f_q(p^k) = 1$ if $p \nmid q$. If p divides q, indeed if p^e is the highest power of p dividing q then

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

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

We may assume that $0 \leq h(n) \leq 1$ for all n, since such results are easy if $h(p) > 1$ often:[19]

Proposition 2.3. *Suppose that $q \leq x$ is an integer for which $h(q) > 6$. Then either*[20]

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

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

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

Proof. If the first option fails then

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

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,

$$\begin{aligned}\sum_{n\leq N}\frac{f_\ell(nq)}{\ell\gamma_\ell} &= \sum_{\substack{n\leq N\\ \ell\nmid n}}\frac{1}{\ell\gamma_\ell} + \sum_{\substack{n\leq N\\ \ell | n}}\frac{h(\ell)}{\ell} \\ &= \frac{1}{\ell-1}([N] - [N/\ell]) - \frac{h(\ell)}{\ell(\ell-1)}(\ell\{N/\ell\} - \{N\}) \leq \frac{N+1}{\ell}.\end{aligned}$$

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

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

[19] Proposition 2.3 implies Theorems 2.1 and 2.2 when there exists $n \leq x$ with $h(n) \geq (\log x)^{c'}$.

[20] Note that this criterion is equivalent to $|\mathcal{A}_q(x) - (h(q)/q)\mathcal{A}(x)| \geq \frac{1}{2}(h(q)/q)\mathcal{A}(x)$, since $f_q(0)/q\gamma_q = f_q(q)/q\gamma_q = h(q)/q$.

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

From now on assume $0 \le h(n) \le 1$ for all n. Suppose that $(q, \mathcal{S}) = 1$ and define $\Delta_q = \Delta_q(x)$ by

$$\Delta_q(x) := \max_{x/4 \le y \le x} \max_{a \pmod q} \Big| \mathcal{A}(y; q, a) - \frac{f_q(a)}{q\gamma_q} \frac{y}{x} \mathcal{A}(x) \Big| \Big/ \frac{\mathcal{A}(x)}{\phi(q)}. \tag{2.8}$$

We can now formulate our main principle.

Proposition 2.4. *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 $S := [x/(2\ell)] < \sqrt{x}/2$. We sum the values of $a(n)$ as n varies over the integers in the following $R \times S$ "Maier matrix."

$(R+1)q + \ell$	$(R+1)q + 2\ell$	$\cdots$	$(R+1)q + S\ell$
$(R+2)q + \ell$	$(R+2)q + 2\ell$	$\cdots$	$(R+2)q + S\ell$
$(R+3)q + \ell$	$\cdot$	$\cdot$	$\vdots$
$(R+4)q + \ell$	$\vdots$	(r,s)th entry : $(R+r)q + s\ell$	$\vdots$
$\vdots$	$\vdots$	$\cdot$	$\vdots$
$2Rq + \ell$	$\cdots$	$\cdots$	$2Rq + S\ell$

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 r-th row contributes $\mathcal{A}((R+r)q + \ell S; \ell, (R+r)q) - \mathcal{A}((R+r)q; \ell, (R+r)q)$. Using (2.8), and noting that $f_\ell((R+r)q) = f_\ell(R+r)$ as $(\ell, q) = 1$, this is

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

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

$$\frac{\ell S}{x} \mathcal{A}(x) \sum_{r=R+1}^{2R} \frac{f_\ell(r)}{\ell\gamma_\ell} + O\Big(\frac{\Delta_\ell}{\phi(\ell)} \mathcal{A}(x) R \Big). \tag{2.9a}$$

The contribution of column s is $\mathcal{A}(2Rq + \ell s; q, \ell s) - \mathcal{A}(Rq + \ell s; q, \ell s)$. By (2.8), 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

$$\frac{Rq}{x}\mathcal{A}(x)\sum_{s=1}^{S}\frac{f_q(s)}{q\gamma_q}+O\Big(\frac{\Delta_q}{\phi(q)}\mathcal{A}(x)S\Big). \tag{2.9b}$$

Comparing (2.9a) and (2.9b) we deduce that

$$\frac{1}{S\gamma_q}\sum_{s=1}^{S}f_q(s)+O\Big(\frac{q\Delta_q}{\phi(q)}\Big)=\frac{1}{R\gamma_\ell}\sum_{r=R+1}^{2R}f_\ell(r)+O\Big(\frac{\ell\Delta_\ell}{\phi(\ell)}\Big). \tag{2.10}$$

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

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

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 (2.10) we obtain the Proposition.

In Proposition 2.4 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

$$\tilde\Delta(y,x):=\max_{(v,v+y)\subset(x/4,x)}\Big|\mathcal{A}(v+y)-\mathcal{A}(v)-y\frac{\mathcal{A}(x)}{x}\Big|\Big/\,y\frac{\mathcal{A}(x)}{x}. \tag{2.11}$$

Proposition 2.5. *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 2.4, starting with an $R\times y$ "MAIER matrix" (again $R=[x/(4q)]$) whose (r,s)-th entry is $(R+r)q+s$. We omit the details.

2.3. Oscillations in mean-values of multiplicative functions. Assume that q is an integer all of whose prime factors are less than or equal to large 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

$$F_q(s) = \sum_{n=1}^{\infty} \frac{f_q(n)}{n^s} = \zeta(s)G_q(s), \qquad \text{where } \ G_q(s) = \prod_{p|q} \Big(1-\frac{1}{p^s}\Big)\Big(1+\frac{f_q(p)}{p^s}+\frac{f_q(p^2)}{p^{2s}}+\dots\Big).$$

To start with, F_q is defined in $\mathrm{Re}(s) > 1$, but the above furnishes a meromorphic continuation to $\mathrm{Re}(s) > 0$. Now $\gamma_q = G_q(1)$, and define

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

which is what we need to consider in Propositions 2.2 and 2.3 above. For complex number ξ, let $H(\xi) := H_0(\xi)$ where

$$H_j(\xi) := \sum_{p|q} \frac{1 - f_q(p)}{p^{1-\xi/\log z}} \Big(\frac{\log(z/p)}{\log z}\Big)^j \text{ for each } j \ge 0, \quad \text{and } J(\xi) := \sum_{p|q} \frac{1}{p^{2(1-\xi/\log z)}}.$$

One can easily show that for $\pi \le \xi \le \frac{2}{3}\log z$ one has

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

The new development is to show that if

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

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

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

This gives us, in some generality, a best possible oscillation result up to a small factor. We will not prove this result here, but we will later (in section 3.4) indicate how we proved it, though first (in section 3) we will need to discuss the theory of mean values of multiplicative functions in some detail.

By a judicious choice of ξ, one can deduce Theorems 2.1 and 2.2 from Propositions 2.4 and 2.5 respectively.

2.4. More Examples.

• **Sieves**. 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

hypothesis for $\mathcal{B}, \mathcal{P}$ and $u := \log x/\log z$. The fundamental lemma of sieve theory (see [HR1]) implies (for example, when $\mathcal{B}$ is the set of integers in an interval) that

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

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: We proved in [GS7] that if $\mathcal{P}$ is a given set of primes for which $\#\{p\in\mathcal{P}:\ p\le y\} \gg \pi(y)$ for all $y\in(\sqrt{z},z]$, then there exists a constant $c>0$ such that for any $u \ll \sqrt{z}$ there exist intervals $I_\pm$ of length $\ge z^u$ for which

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

$$\text{and}\quad \mathcal{S}(\mathcal{I}_-,\mathcal{P},z) \le \left\{1-\Big(\frac{c}{u\log u}\Big)^u\right\}|I_-|\prod_{p\in\mathcal{P},p\le z}\Big(1-\frac{1}{p}\Big).$$

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

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 Hooley, and of Montgomery and Vaughan [MV2] 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 $h\ge\log^2 q$. However, by a modification of our argument, we can show that 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 fact Montgomery and Vaughan showed that

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

for integers $r\ge 1$. Our work places restrictions on the uniformity with which this estimate can hold: Given h and q with $h\phi(q)/q$ large, define η by $q/\phi(q) = (h\phi(q)/q)^\eta$. If the above holds then $r \ll (\log(h\phi(q)/q))^{2+4\eta+o(1)}$.

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

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

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 that (see page 417 of [Ten])

$$\mathcal{A}(x) \sim \frac{e^{\gamma\alpha}}{\Gamma(1-\alpha)} x \prod_{\substack{p \le x \\ p \in \mathcal{P}}} \Big(1 - \frac{1}{p}\Big). \tag{2.12}$$

We can show oscillatory results for any such $\mathcal{A}$: Fix $u \ge \max(e^{2/\alpha}, e^{100})$ and suppose x is sufficiently large. Then there exists $y \in (x/4, x)$ and an arithmetic progression $a \pmod{\ell}$ with $\ell \le x(3/\log x)^u$ such that

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

Moreover suppose $MN = u$ with $M, N \ge 1$. Then at least one of the following is true:

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

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

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

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

Examples of Wirsing sequences include sums of two squares, in fact norms of integral ideals belonging to a given ideal class (in a given number field).

3. HALÁSZ'S THEOREM

3.1. The Halász-Montgomery theorem. Given a multiplicative function f with $|f(n)| \le 1$ for all n, define

$$\Theta(f, x) := \prod_{p \le x} \Big(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \dots\Big)\Big(1 - \frac{1}{p}\Big).$$

We are concerned with understanding the mean value of f up to x, that is $\frac{1}{x}\sum_{n \le x} f(n)$. For real-valued f it turns out that

$$\frac{1}{x}\sum_{n \le x} f(n) \to \Theta(f, \infty) \ \text{ as } x \to \infty. \tag{3.1a}$$

In 1944 WINTNER proved this when $\Theta(f, \infty) \ne 0$, which is equivalent to the hypothesis that $\sum_p (1 - f(p))/p$ converges. In 1967, WIRSING [Wrs] settled the harder remaining case

when $\Theta(f,\infty)=0$, thereby establishing an old conjecture of Erdős and Wintner that every multiplicative function f with $-1\le f(n)\le 1$ has a mean-value.

On the other hand not all complex valued multiplicative functions have a mean value tending to a limit; for example, the function $f(n)=n^{i\alpha}$, with $\alpha\in\mathbb{R}\setminus\{0\}$, since $\frac{1}{x}\sum_{n\le x} n^{i\alpha}\sim x^{i\alpha}/(1+i\alpha)$. In the early seventies, Gábor Halász [Hal1, Hal2] brilliantly realized that the correct question to ask is whether $\sum_p(1-\mathrm{Re}(f(p)p^{-i\alpha}))/p$ converges for all real numbers α. His fundamental result states:

(I) If $\sum_p(1-\mathrm{Re}(f(p)/p^{i\alpha}))/p$ diverges for all α then $\frac{1}{x}\sum_{n\le x} f(n)\to 0$ as $x\to\infty$.

(II) If there exists α for which $\sum_p(1-\mathrm{Re}(f(p)/p^{i\alpha}))/p$ converges then

$$\frac{1}{x}\sum_{n\le x} f(n)\sim \frac{x^{i\alpha}}{1+i\alpha}\Theta(f_\alpha,x) \tag{3.1b}$$

where $f_\alpha(n):=f(n)/n^{i\alpha}$. Now $|\Theta(f_\alpha,x)|\to|\Theta(f_\alpha,\infty)|$ as $x\to\infty$ so we can rewrite the above as

$$\frac{1}{x}\sum_{n\le x} f(n)\sim \frac{x^{i\alpha}}{1+i\alpha}|\Theta(f_\alpha,\infty)|e^{ir(x)}$$

where $r(x)=\arg\Theta(f_\alpha,x)$ (which varies very slowly, for example $r(x^2)=r(x)+o(1)$). Also note that if $\sum_p|1-f(p)/p^{i\alpha}|/p$ converges then (II) holds and $\Theta(f_\alpha,x)\to\Theta(f_\alpha,\infty)$ as $x\to\infty$.

Moreover one should note the Corollary that if (II) holds then for any real number β one has

$$\frac{1}{x}\sum_{n\le x} f(n)n^{i\beta}\sim \frac{x^{i(\alpha+\beta)}}{1+i(\alpha+\beta)}\Theta(f_\alpha,x).$$

In case (I), Halász also quantified how rapidly the limit is attained. His method was modified and refined by Montgomery [Mon], Tenenbaum [Ten, p.343], and Sound and I [GS4]: Throughout define

$$M(x,T):=\min_{|y|\le 2T}\sum_{p\le x}\frac{1-\mathrm{Re}(f(p)p^{-iy})}{p}. \tag{3.2}$$

Theorem (Halász-Montgomery). *Let f be a multiplicative function with $|f(n)|\le 1$ for all n. Let $x\ge 3$ and $T\ge 1$ be real numbers, and let $M=M(x,T)$. If f is completely multiplicative then*

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big|\le \Big(M+\frac{12}{7}\Big)e^{\gamma-M}+O\Big(\frac{1}{T}+\frac{\log\log x}{\log x}\Big).$$

If f is multiplicative then

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big|\le \prod_p\Big(1+\frac{2}{p(p-1)}\Big)\Big(M+\frac{4}{7}\Big)e^{\gamma-M}+O\Big(\frac{1}{T}+\frac{\log\log x}{\log x}\Big).$$

This is essentially "best possible" (up to a factor 10) in that for any given sufficiently large m_0, we can construct f and x such that $M = M(x,\infty) = m_0 + O(1)$ and $|\sum_{n\le x} f(n)| \ge (M+12/7)e^{\gamma-M}x/10$.

If the minimum in (3.2) occurs for $y = y_0$ then one might expect that $f(n)$ looks roughly like n^{iy_0}, so that the mean-value of $f(n)$ should be around size $|x^{iy_0}/(1+iy_0)| \asymp 1/(1+|y_0|)$. In fact we proved that if the minimum in (3.2) with $T = \log x$ is attained at $y = y_0$ then

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big| \ll \frac{1}{1+|y_0|} + \frac{(\log\log x)^{1+2(1-\frac{2}{\pi})}}{(\log x)^{1-\frac{2}{\pi}}}.$$

Taking $f(n) = n^{iy_0}$ we see that this is best possible in terms of y_0 though, in this case $M = 0$. Next we proved a hybrid bound between the last two results, obtaining, for $M = M(x,\log x)$,

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big| \ll (M+1)\frac{e^{\gamma-M}}{\sqrt{1+y_0^2}} + \frac{\log\log x}{(\log x)^{2-\sqrt{3}}}.$$

The right hand side of (3.1b) has size $\asymp e^{-M}/(1+|y_0|)$, implying that there is little room to reduce the bound in Theorem 2b. In fact for any given α and m_0 we can determine f, such that $M = m_0 + O(1)$, $y_0 = \alpha$ and the bound here is too big by at most a constant factor.

The minimum in (3.2) can be unwieldy to determine, so it is desirable to get similar decay estimates in terms of $\sum_{p\le x}(1-\mathrm{Re}(f(p)))/p$ (or equivalently $|F(1)|$). However, in light of case (II) above, this is only possible if we have some additional information on f, since the $\sum_p(1-\mathrm{Re}(f(p)))/p$ may diverge while the absolute value of the mean value may converge. One can avoid case (II) altogether by insisting that all $f(p)$ lie in some closed convex subset D of the unit disc $\mathbb{U}$ (this is a natural restriction for many applications, such as when f is a Dirichlet character of a given order), as in Halász [Hal1, Hal2], Hall and Tenenbaum [HT], and Hall [Hl2]. The result of Hall is the most general, perhaps qualitatively definitive. To describe it we require some information on the geometry of D:

Throughout we let D be a closed, convex subset of $\mathbb{U}$ with $1 \in D$, and define $\nu = \nu(D) = \max_{\delta\in D}(1-\mathrm{Re}(\delta))$. For $\alpha \in [0,1]$ define

$$\hbar(\alpha) = \frac{1}{2\pi}\int_0^{2\pi} \max_{\delta\in D} \mathrm{Re}((1-\delta)(\alpha - e^{-i\theta}))\, d\theta, \tag{3.3}$$

which is a continuous, increasing, convex function of α. Note that $\hbar(0) = \lambda(D)/2\pi$, where $\lambda(D)$ is the length of the boundary of D. Define $\kappa = \kappa(D)$ to be the largest value of $\alpha \in [0,1]$ such that $\hbar(\alpha) \le 1$, which exists since $\hbar(0) \le 1$. When $0 \in D$, Hall showed that $\kappa(D) = 0$ only when $D = \mathbb{U}$, and $\kappa(D) = 1$ only when $D = [0,1]$. He also proved that

$$\kappa(D) \ge \min\Big(1, \frac{1-\hbar(0)}{\hbar(1)-\hbar(0)}\Big) \ge \min\Big(1, \frac{1}{\nu(D)}\Big(1-\frac{\lambda(D)}{2\pi}\Big)\Big).$$

Moreover $\kappa(D)\nu(D) \le 1$ for all D, with equality holding if and only if $D = [0,1]$.

Theorem (Hall). *Let D be a closed, convex subset of $\mathbb{U}$ with $1 \in D$, and define $\kappa(D)$ as above. Let f be a multiplicative function with $|f(n)| \le 1$ and $f(p) \in D$ for all primes p. Then*

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big| \ll_D \exp\Big(-\kappa(D)\sum_{p\le x}\frac{1-\mathrm{Re}(f(p))}{p}\Big). \tag{3.4}$$

Hall proved that the constant $\kappa(D)$ here is optimal for *every* D, in that it cannot be replaced by any larger value.

One would also like to bound how averages of multiplicative functions vary, for example that

$$\frac{1}{x}\sum_{n\le x} f(n) - \frac{w}{x}\sum_{n\le x/w} f(n) \ll \Big(\frac{\log 2w}{\log x}\Big)^{\beta}, \tag{3.5}$$

for all $1 \le w \le x$, with as large an exponent β as possible; the only problem is that this is not true as the ubiquitous example $f(n) = n^{i\alpha}$ reveals. On the other hand Elliott proved that the *absolute value* of the mean of a given multiplicative function does vary slowly, and using the method here one can improve his result to:

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big| - \frac{w}{x}\Big|\sum_{n\le x/w} f(n)\Big| \ll \left(\frac{\log 2w}{\log x}\right)^{1-\frac{2}{\pi}} \log\left(\frac{\log x}{\log 2w}\right) + \frac{\log\log x}{(\log x)^{2-\sqrt{3}}} \tag{3.6}$$

for $1 \le w \le x/10$ and any multiplicative function f with $|f(n)| \le 1$ for all n. If the minimum in (3.2) occurs when $y = 0$ then we can remove the absolute value signs here, and have a result like the one proposed, (3.5). In the special case that $f(n)$ is non-negative we improved the $1 - 2/\pi$ to $1 - 1/\pi$, see [GS6].

An application of such an estimate, as Hildebrand [Hi3] observed, is to extend slightly the range of validity of Burgess' famous character sum estimate. For characters χ with cubefree conductor q, one can show that $\sum_{n\le N}\chi(n) = o(N)$ for $N > q^{1/4-o(1)}$ rather than $N > q^{1/4+o(1)}$.

Our proofs are based on the following key Proposition, which we establish by a variation of Halász' method.

Proposition 3.1. *For $x \ge 3, T \ge 1$, and*

$$F(s) = F_x(s) := \prod_{p\le x}\Big(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots\Big)$$

for any complex number s with $Re(s) > 0$, we have

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big| \le \frac{2}{\log x}\int_0^1 \Big(\frac{1-x^{-2\alpha}}{2\alpha}\Big)\Big(\max_{|y|\le T}|F(1+\alpha+iy)|\Big)d\alpha + O\Big(\frac{1}{T} + \frac{\log\log x}{\log x}\Big).$$

Sketch of deduction of the HALÁSZ-MONTGOMERY *theorem.* Whenever $0 < \alpha < 1$ we have $z^{-\alpha} = \frac{1}{\pi}\int_{-T}^{T} \frac{\alpha}{\alpha^2+\xi^2} z^{-i\xi} d\xi + O(\frac{\alpha}{T})$. We easily deduce that

$$\frac{1}{\log x} \max_{|y|\le T} |F(1+\alpha+iy)| \le L + O\Big(\frac{\alpha}{T}\Big) \text{ where } L := \frac{1}{\log x}\Big(\max_{|y|\le 2T} |F(1+iy)|\Big),$$

a bound we use in the range $\alpha \le 1/L\log x$. For larger α we have $|F(1+\alpha+iy)| \le \zeta(1+\alpha) \le 1/\alpha + O(1)$. Substituting these estimates into Proposition 3.1, it is now a manipulation of some integrals to show that

$$\frac{1}{x}\Big|\sum_{n\le x} f(n)\Big| \le L\Big(\log\frac{e^\gamma}{L} + \frac{12}{7}\Big) + O\Big(\frac{1}{T} + \frac{\log\log x}{\log x}\Big).$$

If f is completely multiplicative then, by Mertens' theorem,

$$\begin{aligned} |F(1+iy)| &= (e^\gamma \log x + O(1)) \prod_{p\le x} \Big|1 - \frac{f(p)}{p^{1+iy}}\Big|^{-1}\Big(1-\frac{1}{p}\Big) \\ &= (e^\gamma \log x + O(1)) \exp\Big(-\sum_{\substack{p\le x\\ k\ge 1}} \frac{1-\mathrm{Re}(f(p^k)p^{-iky})}{kp^k}\Big), \end{aligned}$$

so that $L \le e^{\gamma - M} + O(1/\log x)$, and the result follows. If f is multiplicative then the result follows similarly after noting that

$$\Big|1 + \frac{f(p)}{p^{1+iy}} + \frac{f(p^2)}{p^{2+2iy}} + \dots\Big|\Big|1 - \frac{f(p)}{p^{1+iy}}\Big| \le 1 + \frac{2}{p(p-1)},$$

since $|f(p^k)| \le 1$ for all k.

3.2. Integral delay equations – a model for mean values. Proofs of Proposition 3.1 (as in [GS4]) can be rather complicated and seem unmotivated. It is our intention to give the proof of an analogous result about integral delay equations which can be modified to give a proof of Proposition 3.1. We now discuss what the connection is with integral delay equations, before getting more precise later.

WIRSING [Wrs] observed that questions on mean-values of multiplicative functions can be reformulated in terms of solutions to a related integral equation. We formalized this connection precisely in our paper [GS1] and we now recapitulate the salient details. Throughout we suppose that f is a multiplicative function with $|f(n)| \le 1$ for all n. Two classes of multiplicative functions with non-zero mean values are easily dealt with in the literature, those with $f(p) = 1$ for all of the "small" primes p, and those with $f(p) = 1$ for all of the "large" primes p:

• An example with $f(p) = 1$ for all of the "small" primes p. It is known that there are $\sim \rho(u)y^u$ integers up to y^u which only have prime factors $\le y$ (the "y-smooth" or

"y-friable" integers). Here $\rho(u) = 1$ for $u \le 1$, obviously, and $\rho(u) = (1/u)\int_0^1 \rho(u-t)dt$ for $u > 1$. In general suppose that $f(p) = 1$ for all primes $p \le y$. Define

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

so that $\chi(t)$ is a measurable function with $|\chi(t)| \le 1$ for all t and $\chi(t) = 1$ for $t \le 1$. Let $\sigma(u)$ be defined as $\sigma(u) = 1$ for $0 \le u \le 1$, and

$$\sigma(u) = \frac{1}{u}\int_0^u \chi(t)\sigma(u-t)dt \tag{3.7}$$

for $u > 1$. Then

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

In the y-smooth numbers example we had $f(p) = 1$ if $p \le y$ and $f(p) = 0$ if $p > y$ so that $\chi(t) = 1$ for $t \le 1$ and 0 for $t > 1$, so that (3.7) gives us $\rho(u) = (1/u)\int_0^1 \rho(u-t)dt$.

In fact whenever $\chi : (0, \infty) \to \mathbb{C}$ is measurable function with $\chi(t) = 1$ for $0 \le t \le 1$ and $|\chi(t)| \le 1$ for all $t \ge 1$, there is a unique solution $\sigma(u)$ to (3.7) which is continuous, with $|\sigma(u)| \le 1$ for all u.

• An example with $f(p) = 1$ for all of the "large" primes p. Let P be a set of primes $\le y$ where $y = x^{o(1)}$. It is known from sieve theory that the number of integers up to x with no prime factors from the set P is $\sim \prod_{p \in P}(1 - 1/p) \cdot x$. In general suppose that $f(p) = 1$ for all primes $p \in (y, x]$. We saw in (3.1b) that

$$\frac{1}{x} \sum_{n \le x} f(n) \to \Theta(f, x) = \Theta(f, y) = \prod_{p \le y} \Big(1 - \frac{1}{p}\Big)\Big(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \dots\Big);$$

In our example, f is totally multiplicative with $f(p) = 0$ if $p \in P$, and $f(p) = 1$ otherwise.

What about f without such helpful structure? By Halász's theorem we see that the mean value $\to 0$ unless there exists α such that $f_\alpha(p) := f(p)/p^{i\alpha}$ is mostly close to 1. In that case, by partial summation and (3.1b) (and the discussion after), we deduce that

$$\sum_{n \le x} f(n) \sim \frac{x^{i\alpha}}{1 + i\alpha} \sum_{n \le x} f_\alpha(n),$$

and we will study this latter mean value. We know that $\sum_{p \le x} \frac{1 - \mathrm{Re}(f_\alpha(p))}{p}$ is bounded and, in particular, there exists extremely small $\epsilon > 0$ such that $\sum_{x^{\epsilon^2} < p \le x^\epsilon} \frac{1 - \mathrm{Re}(f_\alpha(p))}{p} < \epsilon$. Now let $g(p) = 1$ for all $p \le x^\epsilon$ and $g(p) = f_\alpha(p)$ otherwise, and $h(p) = f_\alpha(p)$ for all $p \le x^{\epsilon^2}$, and $h(p) = 1$ otherwise. By an inclusion-exclusion argument it is easy to show that

$$\frac{1}{x} \sum_{n \le x} f_\alpha(n) = \frac{1}{x} \sum_{n \le x} g(n) \cdot \frac{1}{x} \sum_{n \le x} h(n) + O(\epsilon),$$

so now we can proceed to determine the mean value of f, using what we have discussed above about multiplicative functions like $g(.)$ that are 1 on all the small primes, and those like $h(.)$ that are 1 on all the large primes .

What we have proved is that if the mean value of f is not too small in absolute value, then it can be written as a product, of $\frac{x^{i\alpha}}{1+i\alpha}$ for some $|\alpha| < \log x$, times an Euler product, times the solution to an integral delay equation like (3.7). This is a strong version of the *Structure Theorem* of [GS1]. Although this is, we believe, the first such formal statement in the literature, such ideas have been used implicitly for a long time – certainly it had been recognized that in many problems, the extreme cases are easily modeled by an integral delay equation. Note that for any particular α, an admissible value for the Euler product, and an admissible χ, it is not difficult to construct examples $f(.)$ that come close to these values. Hence from our model we can construct arithmetic examples.

Typically the $\frac{x^{i\alpha}}{1+i\alpha}$ and the Euler product are easy to determine, but the solution to the integral delay equation is difficult to determine. The advantage of the structure theorem is that it allows the researcher to move away from the rather difficult arithmetic issues and focus instead on a cleaned up pure analysis question about integral delay equations. I prefer to try to explain most of the proofs here in these terms (however, as one referee wrote, it is usual to do these kind of calculations in rough and then "translate" the argument to the arithmetic setting, which is often quite challenging). To start with let me justify Halász's theorem in this way. Formally I am going in circles since we used Halász's theorem to prove the Structure Theorem, but in fact the proof that we now sketch can be re-written with multiplicative functions (see [GS4]) though with several additional complications.

3.3. An integral delay equation version of Proposition 3.1. By a typical sieve iteration argument one can easily show that

$$\sigma(u) = 1 + \sum_{j=1}^{\infty} \frac{(-1)^j}{j!} I_j(u;\chi), \tag{3.8a}$$

where

$$I_j(u;\chi) = \int_{\substack{t_1,\dots,t_j\ge 1\\ t_1+\dots+t_j\le u}} \frac{1-\chi(t_1)}{t_1}\cdots\frac{1-\chi(t_j)}{t_j} dt_1\cdots dt_j. \tag{3.8b}$$

In fact if $\chi(t) \in \mathbb{R}$ for all t then we have the inclusion-exclusion relations, $\sigma_{2k+1}(u) \le \sigma(u) \le \sigma_{2k}(u)$ where[21]

$$\sigma_k(u) := 1 + \sum_{j=1}^{k} \frac{(-1)^j}{j!} I_j(u;\chi).$$

The Laplace transform of a function $f : [0,\infty) \to \mathbb{C}$ is defined by

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

[21]Looking back at our papers (particularly Proposition 3.6 of [GS1]) we did not, but should have, proved that $\sigma_{2k+1}(u)$ is non-decreasing in k, and that $\sigma_{2k}(u)$ is non-increasing in k.

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 (3.7) we obtain that for $\mathrm{Re}(s) > 0$

$$\mathcal{L}(u\sigma(u), s) = \mathcal{L}(\chi, s)\mathcal{L}(\sigma, s). \tag{3.9}$$

Moreover from (3.8) we see that when $\mathrm{Re}(s) > 0$

$$s\mathcal{L}(\sigma, s) = \exp\Big(- \mathcal{L}\Big(\frac{1-\chi(v)}{v}, s\Big)\Big). \tag{3.10}$$

Finally, observe that if $\int_1^\infty |1-\chi(t)|/t\, dt < \infty$ then from (3.8b) it follows that $\lim_{u\to\infty} \sigma(u)$ exists and equals

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

We now give our integral equations version of Proposition 3.1.

Proposition 3.2. *Fix $u \geq 1$, and define for $t > 0$*

$$M_+(t) = \int_u^\infty \frac{e^{-tv}}{v}\, dv + \min_{y\in\mathbb{R}} \int_0^u \frac{1 - \mathrm{Re}(\chi(v)e^{-ivy})}{v}\, e^{-tv}\, dv.$$

Then

$$|\sigma(u)| \leq \frac{1}{u}\int_0^\infty \left(\frac{1-e^{-2tu}}{t}\right)\frac{\exp(-M_+(t))}{t} dt.$$

Since $M_+(t) \geq \max(0, -\log(tu) + O(1))$ we see that the integral in this Proposition converges.

Proof. Define $\hat{\chi}(v) = \chi(v)$ if $v \leq u$, and $\hat{\chi}(v) = 0$ if $v > u$. Let $\hat{\sigma}$ denote the corresponding solution to (3.7). Note that $\hat{\sigma}(v) = \sigma(v)$ for $v \leq u$. Thus

$$\begin{aligned} |\sigma(u)| = |\hat{\sigma}(u)| &\leq \frac{1}{u}\int_0^u |\hat{\sigma}(v)| dv = \frac{1}{u}\int_0^u 2v|\hat{\sigma}(v)| \int_0^\infty e^{-2tv} dt dv \\ &= \frac{1}{u}\int_0^\infty \left(\int_0^u 2v|\hat{\sigma}(v)|e^{-2tv} dv\right) dt. \end{aligned} \tag{3.11}$$

By Cauchy's inequality

$$\begin{aligned} \left(\int_0^u 2v|\hat{\sigma}(v)|e^{-2tv} dv\right)^2 &\leq \left(4\int_0^u e^{-2tv} dv\right)\left(\int_0^\infty |v\hat{\sigma}(v)|^2 e^{-2tv} dv\right) \\ &= 2\, \frac{1-e^{-2tu}}{t} \int_0^\infty |v\hat{\sigma}(v)|^2 e^{-2tv} dv. \end{aligned} \tag{3.12}$$

By Plancherel's formula (Fourier transform is an isometry on L^2)

$$\int_0^\infty |v\hat{\sigma}(v)|^2 e^{-2tv} dv = \frac{1}{2\pi}\int_{-\infty}^\infty |\mathcal{L}(v\hat{\sigma}(v), t+iy)|^2 dy$$

and, using (3.9), this is

$$= \frac{1}{2\pi}\int_{-\infty}^{\infty} |\mathcal{L}(\hat\sigma, t+iy)|^2 |\mathcal{L}(\hat\chi, t+iy)|^2 dy \le \left(\max_{y\in\mathbb{R}} |\mathcal{L}(\hat\sigma, t+iy)|^2\right) \frac{1}{2\pi}\int_{-\infty}^{\infty} |\mathcal{L}(\hat\chi, t+iy)|^2 dy.$$

Applying Plancherel's formula again, we get

$$\frac{1}{2\pi}\int_{-\infty}^{\infty} |\mathcal{L}(\hat\chi, t+iy)|^2 dy = \int_0^{\infty} |\hat\chi(v)|^2 e^{-2tv} dv \le \int_0^u e^{-2tv} dv = \frac{1-e^{-2tu}}{2t}.$$

Hence

$$\int_0^{\infty} |v\hat\sigma(v)|^2 e^{-2tv} dv \le \frac{1-e^{-2tu}}{2t} \max_{y\in\mathbb{R}} |\mathcal{L}(\hat\sigma, t+iy)|^2. \tag{3.13}$$

By (3.10), we have

$$\mathcal{L}(\hat\sigma, t+iy) = \frac{1}{t+iy} \exp\left(-\mathcal{L}\left(\frac{1-\hat\chi(v)e^{-ivy}}{v}, t\right) + \mathcal{L}\left(\frac{1-e^{-ivy}}{v}, t\right)\right).$$

Now, we have the identity

$$\mathrm{Re}\left(\mathcal{L}\left(\frac{1-e^{-ivy}}{v}, t\right)\right) = \log|1+iy/t|$$

which is easily proved by differentiating both sides with respect to y. Using this we obtain

$$t|\mathcal{L}(\hat\sigma, t+iy)| = \exp\left(-\mathrm{Re}\left(\mathcal{L}\left(\frac{1-\hat\chi(v)e^{-ivy}}{v}, t\right)\right)\right),$$

from which it follows that

$$\max_{y\in\mathbb{R}} |\mathcal{L}(\hat\sigma, t+iy)| = \frac{\exp(-M_+(t))}{t}.$$

Inserting this in (3.13), and that into (3.12), and then (3.11), we obtain the Proposition.

Now imagine doing all this with χ and σ replaced by the appropriate mean values and you can see that it is likely to get quite a bit more complicated!

3.4. An uncertainty principle for integral equations. We need to give an idea of the proofs that Propositions 2.4 and 2.5 lead to Theorems 2.1 and 2.2, which use the results described in section 2.3. The proofs of these results are too detailed to give here but, again, they are modeled on an uncertainty principle for integral delay equations, which we now describe.

Theorem 3.3. *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 $|\chi(t)-1|$ and $|\sigma(u)-\sigma_\infty|$ cannot both 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 (3.10) now holds for all $s \in \mathbb{C}$.

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

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

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 $u(\xi - (\log u)/A) \leq e^{A\xi-1}/A$, and in the range of the second integral one uses $u(\xi - (\log u)/A) \leq -u$. Therefore, by (3.10), if $\mathrm{Re}(s) \geq -\xi$ and $\mathrm{Im}(s) \ll e^\xi$ with ξ large, then

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

We now apply the Borel-Caratheodory lemma[22] 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

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

[22]This says that for any holomorphic function f we have

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

where $0 < r < R$.

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 $\delta > 0$ we have

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

so that

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

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

3.5. Spectra. It is interesting, and applicable, to understand what are the possible mean values of multiplicative functions that take their values of the kth roots of unity. From our structure theorem we know that we can break this down into a study of Euler products, and integral delay equations. Here we need χ to be measurable, and its values to belong to the convex hull of the kth roots of unity. In fact for any subset S of the unit disk we can ask to determine the *spectrum* $\Gamma(S)$ of possible mean values:[23] We can again apply the structure theorem where χ is now allowed to be anywhere in the convex hull of S. We may assume that S is closed with no loss of generality. This implies that if $1 \notin S$ then $\Gamma(S) = \{0\}$, so we may assume that $1 \in S$ henceforth, and hence $1 \in \Gamma(S)$.

It is easy to show that $\Gamma([0,1]) = [0,1]$. It was the main point of our paper [GS1] to show that $\Gamma([-1,1]) = [\delta_1, 1]$ where

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

One amusing consequence of this result is that, once x is sufficiently large, at least 17.15% of the integers up to x are quadratic residues mod p, for each prime p, and that this percentage is attained.[24]

If S is the unit disc $\mathbb{U} := \{|z| \le 1\}$ then $\Gamma(\mathbb{U}) = \mathbb{U}$ as may be deduced by taking $f(p) = p^{i\alpha}$ for smaller and smaller. A similar proof holds if there is an infinite sequence of points of S approaching 1, whose angle with 1 becomes increasingly vertical. In other words if

$$\text{Ang}(S) := \sup_{\substack{v\in S\\ v\neq 1}} |\arg(1-v)|$$

equals $\frac{\pi}{2}$. So henceforth we may assume that $0 \le \text{Ang}(S) < \frac{\pi}{2}$.

[23] Really we are asking for the set of limit points so $\Gamma(S)$ is always closed, and $\Gamma(S) = \Gamma(\overline{S})$.

[24] Notice that x does not depend on p. Also that .1715 is an approximation for $(1+\delta_1)/2$.

There are two obvious subsets of $\Gamma(S)$, the Euler products

$$\Gamma_\Theta(S) := \lim_{x\to\infty} \{\Theta(f,x) : f \in \mathcal{F}(S)\} = \{\Theta(f,\infty) : f \in \mathcal{F}(S)\}$$

(this last equality since $\mathrm{Ang}(S) < \frac{\pi}{2}$) which is a closed subset of $\Gamma(S)$, and the solutions to integral delay equations

$$\Lambda(S) := \{\sigma(u) \text{ from (3.7)} : \ u \geq 0,\ \chi(t) \in \mathrm{ConvexHull}(S) \text{ for all } t \geq 0\}.$$

Our structure theorem implies that $\Gamma(S) = \Gamma_\Theta(S) \times \Lambda(S)$. It is not hard to get a good understanding of $\Gamma_\Theta(S)$ but $\Lambda(S)$ remains largely elusive.

By constructing f with $f(p) = \alpha \in S$ for lots of large primes p we see that the spiral $\{e^{-t(1-\alpha)} : \ t \geq 0\}$ connecting 0 to 1, belongs to $\Gamma_\Theta(S)$; and similarly one can show that $\mathcal{E}(S) := \{e^{-t(1-\alpha)} : \ t \geq 0,\ \alpha \in \mathrm{ConvexHull}(S)\} \subset \Gamma_\Theta(S)$.

• In most cases of interest S contains a real point other than 1 which we will assume from now on. If so then $\Gamma_\Theta(S) = \mathcal{E}(S) = \mathcal{E}(S)\times[0,1]$ and a more precise description is given by taking the union of the interiors of the two curves $\{e^{-t(1-z_\pm)} : \ 0 \leq t \leq 2\pi/|\mathrm{Im}(z_\pm)|\}$ where $z_\pm$ is chosen so that $\pm\mathrm{Im}(z_\pm) > 0$ with $\mathrm{Ang}(z_\pm)$ maximal.

Note that $\Gamma(S)$ inherits some of these properties through the structure theorem. In particular $\Gamma(S) = \Gamma(S) \times \mathcal{E}(S)$ so that the spectrum of S is connected, and one can show that $\Gamma(S) = \Lambda(S)$. In fact $\Gamma(S)$ is contained inside a ball of radius $1 - A$ centered at $A := (28/411)\cos^2(\mathrm{Ang}(S))$. We deduce that it only touches the unit circle at 1, so that one can generalize Hall's theorem to all such sets S (i.e. that a mean value, if it is real, is $\geq -(1-2A)$).

In [GS1] we proved and conjectured several things about the geometry of the spectra:

We conjecture that $\mathrm{Ang}(\Gamma(S)) = \mathrm{Ang}(S)$ (and also equals $\mathrm{Ang}(\Lambda(S)), \mathrm{Ang}(\Gamma_\Theta(S))$ and $\mathrm{Ang}(\mathcal{E}(S))$): We can prove only that $\mathrm{Ang}(\Gamma(S)) \ll \mathrm{Ang}(S) \leq \mathrm{Ang}(\Gamma(S)) \leq \frac{1}{2}(\pi - \sin(\frac{\pi}{2} - \mathrm{Ang}(S)))$.

The projection of a complex number z in the direction $e^{i\alpha}$ is $\mathrm{Re}(e^{-i\alpha}z)$. We define the maximal projection of the spectrum $\Gamma(S)$ of a set $S \subset \mathbb{T}$ as $\max_{1\neq\zeta\in S} \max_{z\in\Gamma(S)} \mathrm{Re}(\zeta^{-1}z)$, and conjecture that this *equals* $1 - (1+\delta_1)\cos^2(\mathrm{Ang}(S))$. It is easy to establish that the maximal projection is $\geq 1 - (1+\delta_1)\cos^2(\mathrm{Ang}(S))$ (by taking $f(p) = 1$ for $p \leq x^{1/(1+\sqrt{e})}$, and $f(p) = \zeta$ otherwise), and that it is $< 1 - (56/411)\cos^2(\mathrm{Ang}(S))$. Moreover we know that the conjecture is true for $S = \{1,-1\}$ and for $S = \{1,-1,i,-i\}$.

3.6. Sieving extrema. Fix $u > 1$. Suppose that we have a set of primes $\mathcal{P}$ up to x for which $\prod_{p\in\mathcal{P}}(1-1/p) \sim 1/u$. Typically we would expect the number of integers up to x, free of prime factors from the set $\mathcal{P}$, to be $\sim x\prod_{p\in\mathcal{P}}(1-1/p) \sim x/u$. However some sets $\mathcal{P}$ may behave rather differently, so we ask what are the maximum and minimum possible values for the proportion of the integers up to x that are free of prime factors from a set $\mathcal{P}$ of primes with $\prod_{p\in\mathcal{P}}(1-1/p) \sim 1/u$?

For the minimum a good candidate is to take $\mathcal{P}$ to be the set of primes $> x^{1/u}$ since then we are counting the number of $x^{1/u}$-smooth numbers up to x, and we saw in section 3.2 that this is $\sim \rho(u)x$, where $\rho(u) = 1/u^{u+o(u)}$ is remarkably tiny. That $\rho(u)$ is the minimum proportion was first proved by Hildebrand in [Hi4]. To reprove this, we

[GS6] used the structure theorem (taking $f(p) = 0$ if $p \in \mathcal{P}$ and $f(p) = 1$ otherwise), to decompose f, observed that the small primes only have the predictable effect (since their contribution belongs to the Euler product) so one could focus on $\mathcal{P}$ with only large prime factors and thus solve an associated optimization problem for a certain class of integral delay equations.

Hall [Ha1] rather elegantly got the upper bound $\le e^\gamma/u + o_{x\to\infty}(1)$ on the proportion; we again used the structure theorem so we could study an associated class of integral delay equations to prove that the maximum proportion equals $e^\gamma/u - 1/u^{2+o(1)}$.

One might ask the same questions for arbitrary intervals of a given width, that is: Fix $u > 1$. For x sufficiently large, what are the maximum and minimum possible values for the proportion of the integers in an interval of length x that are free of prime factors from a set $\mathcal{P}$ of primes with $\prod_{p\in\mathcal{P}}(1 - 1/p) \sim 1/u$? Our methods do not seem to apply to this question. I would guess that the lower bound of $\rho(u)$ will be hard to beat, but the upper bound may be attackable (and that there are examples with a larger proportion of unsieved integers).

4. Character Sums

A central problem in analytic number theory is to gain an understanding of character sums

$$\sum_{n\le x} \chi(n),$$

where χ is a non-principal Dirichlet character $\chi \pmod q$.

4.1. The Pólya-Vinogradov Theorem. It is easy to show that such characters sums are always $\le q$ in absolute value, while Pólya and I.M. Vinogradov [Pol, Vin] improved this to $\le \sqrt{q}\log q$ around 1919. To prove this we begin with the fact that if $(n, q) = 1$ then

$$\sum_{a \pmod q} \chi(a) e\left(\frac{an}{q}\right) = \overline{\chi}(n) \sum_{a \pmod q} \chi(an) e\left(\frac{an}{q}\right) = \overline{\chi}(n)\tau(\chi),$$

where $\tau(\chi) := \sum_{b \pmod q} \chi(b) e\left(\frac{b}{q}\right)$ is the Gauss sum, which is well-known to be $\sqrt{q}$ in absolute value. Hence

$$\sum_{n\le x} \overline{\chi}(n) = \frac{1}{\tau(\chi)} \sum_{a \pmod q} \chi(a) \sum_{n\le x} e\left(\frac{an}{q}\right).$$

Now, if x is an integer then $\sum_{n\le x} e\left(\frac{an}{q}\right) = e\left(\frac{a}{q}\right) \cdot \frac{e\left(\frac{ax}{q}\right)-1}{e\left(\frac{a}{q}\right)-1}$. Writing $e\left(\frac{a}{q}\right) - 1 = \frac{2i\pi a}{q}(1 + O(\frac{a}{q}))$ we get, after some manipulation, Pólya's Fourier expansion

$$\sum_{n\le x} \chi(n) = \frac{\tau(\chi)}{2\pi i} \sum_{\substack{h=-H \\ h\ne 0}}^{H} \frac{\overline{\chi}(h)}{h}(1 - e(-\tfrac{hx}{q})) + O\left(1 + \frac{q\log q}{H}\right). \tag{4.1}$$

Taking $H = q$ and bounding every term by its absolute value we get the bound $|\sum_{n\le x}\chi(n)| \le \frac{\sqrt{q}}{2\pi}\sum_{0<|h|<q}\frac{2}{|h|}+O(\log q) \ge \frac{2}{\pi}\sqrt{q}(\log q+O(1)) \le \sqrt{q}\log q$ for q sufficiently large,[25] as desired.

Montgomery and Vaughan [MV1] improved this bound to $\ll \sqrt{q}\log\log q$ assuming the Generalized Riemann Hypothesis (GRH), in 1977. We now reprove their result by somewhat different means: It is well-known (see, e.g. page 120 of [Dav]) that for any non-principal character $\psi \pmod m$, we have

$$\sum_{n\le x}\psi(n)\Lambda(n) \ll \sqrt{x}\log x\log(mx). \tag{4.2}$$

assuming GRH. Then by partial summation we obtain

$$\sum_{p\le x}\psi(p) \ll \sqrt{x}\log(mx).$$

For any $\theta \in [0,1)$ there exists integers $b \le r \le x^{2/3}$ such that $|r\theta - b| \le 1/x^{2/3}$. First we estimate $\sum_{p\le x}\chi(p)e(pb/r)$ by expanding $e(pb/r)$ in terms of characters mod r and using (4.2), and then we proceed by partial summation to deduce that if $\chi \pmod q$ is a primitive character mod q and $x < q^{3/2}$ then

$$\sum_{p\le x}\chi(p)e(p\theta) \ll x^{5/6}\log q. \tag{4.3}$$

Now if we write each integer n as pm where p is the largest prime factor of n, we can use (4.3) to show that those n with $p > y$ contribute only to the error term in

$$\sum_{n\le x}\chi(n)e(n\alpha) = \sum_{\substack{n\le x\\ p|n \Longrightarrow p\le y}}\chi(n)e(n\alpha) + O(xy^{-1/6}\log q). \tag{4.4}$$

By partial summation we deduce that

$$\sum_{n\le q}\frac{\overline{\chi}(n)e(n\theta)}{n} = \sum_{\substack{n\le q\\ p|n \Longrightarrow p\le y}}\frac{\overline{\chi}(n)e(n\theta)}{n} + O(y^{-1/6}\log^2 q).$$

Substitute this with $y = (\log q)^{12}$ and $\theta = 0, \pm\frac{x}{q}$ into (4.1) (with $H = q$), to obtain

$$\sum_{n\le x}\chi(n) = \frac{\tau(\chi)}{2\pi i}\sum_{\substack{0<|h|<q\\ p|h \Longrightarrow p\le(\log q)^{12}}}\frac{\overline{\chi}(h)}{h}(1-e(-\tfrac{hx}{q})) + O(\log q). \tag{4.5}$$

[25] A bound is easily determined from this proof.

Taking the absolute value of each term this is

$$\le \frac{2\sqrt{q}}{\pi} \prod_{p\le (\log q)^{12}} \left(1-\frac{1}{p}\right)^{-1} + O(\log q) \le (24e^\gamma + o(1))\sqrt{q}\log\log q.$$

With some work [GS8] the constant "$24e^\gamma$" here can be improved to "$\frac{2e^\gamma}{\pi}$", and we conjecture that "$\frac{e^\gamma}{\pi}$" is the maximum possible.[26] Certainly there are constants this large since an argument of Paley [Pal], from 1932, can be used to show that there exist characters sums (with real, quadratic characters), that are $\ge \frac{(e^\gamma+o(1))}{\pi}\cdot\sqrt{q}\log\log q$: Let $x=q/2$ in (4.5), which means we will need $\chi(-1)=-1$ to avoid having the hth and $-h$th term cancelling, to obtain

$$\sum_{n\le q/2}\chi(n) = \frac{2\tau(\chi)}{\pi i} \sum_{\substack{h\le q\\ p|h \Longrightarrow 2<p\le (\log q)^{12}}} \frac{\overline{\chi}(h)}{h} + O(\log q),$$

and the main term here can be shown to be

$$\sim \frac{2\tau(\chi)}{\pi i} \prod_{2<p\le (\log q)^{12}} \left(1-\frac{\overline{\chi}(p)}{p}\right)^{-1}.$$

Now let $m = 4\prod_{2<p\le y} p$ and select a prime $q\equiv -1 \pmod m$ and $\chi(.) = (./q)$, so that $\chi(-1)=-1$. Note that we can find such a q by Dirichlet's theorem, and that $(p/q) = (-q/p) = 1$ for all odd primes $p\le y$. We expect that we can take $y=(\log q)^{1+o(1)}$. When we average over such q we find that the contribution of the primes $p>y$ to the Euler product here is negligible, so we expect the size above to be

$$\sim \frac{2\sqrt{q}}{\pi} \prod_{2<p\le \log q} \left(1-\frac{1}{p}\right)^{-1} \sim \frac{e^\gamma\sqrt{q}}{\pi}\log\log q$$

as desired.

Vinogradov conjectured that the least quadratic non-residue mod q is $\ll q^\epsilon$ for each prime q. This conjecture is not resolved, though it is widely believed to be true (see [Gr6] for a lengthy discussion). The best result known has $\epsilon = 1/4\sqrt{e} \approx .15163$. Now, suppose that Vinogradov's conjecture is false, that there are an infinite sequence of $q\equiv 3 \pmod 4$ for which the least quadratic non-residue mod q is $\gg q^c$ for some $c>0$. By the discussion at the end of the last paragraph we might then expect the values of the character sum up to $q/2$ to be $\asymp c\sqrt{q}\log q$. Hence if we cannot prove Vinogradov's conjecture then we cannot expect to significantly improve the Pólya-Vinogradov Theorem.

In [GS8] we also showed that for any given angle $\theta\in(-\pi,\pi]$ there are at least $q^{1-\epsilon}$ characters $\chi \pmod q$ for which $\sum_{n\le x}\chi(n) \sim e^{i\theta}\ \frac{e^\gamma\sqrt{q}}{\pi}\log\log q$ for some x. Hence there are many character sums of this size.

[26] This factor of 2 difference between upper and lower bounds is entirely analogous with Littlewood's famous work on the size of $L(1,\chi)$.

4.2. Burgess's Theorem. In many applications one is interested in when

$$\left|\sum_{n\le x}\chi(n)\right| = o(x). \tag{4.6}$$

In 1957, Burgess [Bu1] used ingenious combinatorial methods together with the "Riemann Hypothesis for hyperelliptic curves" to establish (4.6) whenever $x > q^{\frac14+o(1)}$, for any quadratic character mod q, with q prime.[27] Recently Friedlander and Iwaniec [FI] have supplied a different proof of Burgess's result, and Hildebrand [Hi3] observed that one can "extrapolate" Burgess's bound to the range $x > q^{\frac14-o(1)}$. However, Burgess's range has not been substantially improved over the last forty years although it is widely believed that such an estimate should hold for $x \gg_\epsilon q^\epsilon$.

Assuming GRH we have by (4.4) with $\alpha = 0$ and $y = (\log q)^7$ that $|\sum_{n\le x}\chi(n)|$ is bounded by the number of y-smooth integers up to x plus $o(x)$, that is $\le (\rho(u/7)+o(1))x$.[28] Hence we get (4.6) if $\log x/\log\log q \to \infty$. On the other hand, if we construct χ as in Paley's example in the previous subsection, we can show that the contribution of integers n containing larger prime factors to the sum in (4.4) is negligible on average, so that $\sum_{n\le x}\chi(n) \sim x\rho(u)$. In particular (4.6) does not hold if $x = (\log q)^u$, for some fixed u.[29] In fact $\rho(u) = 1/u^{u+o(u)}$. In [GS2] we went on to show that for any fixed $A > 0$, for any given angle θ, there are non-principal characters χ modulo any prime q for which the character sum up to $\log^A q$ equals $\{e^{i\theta}+o(1)\}\rho(A)\log^A q$, putting this on the same footing as the Pólya-Vinogradov problem (see the last remark in the previous subsection).

In [GS2] we improved on (4.4) when $\alpha = 0$, at the cost of more work, obtaining roughly $x(\log q)(\log x)/y^{1/2}$ in the error term. In fact we showed that the character sum up to x is bounded by a constant multiple of the number of $(\log q)^2(\log\log q)^{20}$-smooth numbers up to x. In particular this implies that

$$\left|\sum_{n\le x}\chi(n)\right| \ll \sqrt{x}\cdot q^{(5+o(1))\frac{\log\log\log q}{\log\log q}}. \tag{4.7}$$

We conjectured that the character sum up to x is bounded by a constant multiple of the number of $(\log^2 x+\log q)(\log\log q)^C$-smooth numbers up to x for some $C > 0$. This would lead to the "5" in (4.7) being replaced by "$C/4$". One can prove that one cannot replace this by $(\frac{1}{4e^2}\log^2 x + c\log q\log\log q)$-smooths, for small $c > 0$; it seems to be a rather delicate issue to guess the correct bound in (4.7). In [GS2] we showed that for every q there exists a non-principal character χ, and x, such that $|\sum_{n\le x}\chi(n)|/\sqrt{x} \gg \exp\left(c\sqrt{\frac{\log q}{\log\log q}}\right)$, and this may well be about as large as it gets.

Recently it has been realized that the proof of Burgess's theorem can be somewhat generalized in the framework of *additive combinatorics*.[30] For finite sets A and B, we define $A+B = \{a+b:\ a\in A, b\in B\}$ and $r_{A+B}(n) = \#\{a\in A, b\in B:\ a+b=n\}$. Moreover we let $E_\times(A,B) = \#\{a,a'\in A, b,b'\in B:\ ab = a'b'\}$.

[27] And subsequently generalized this to any non-principal character $\chi \pmod q$ when q is cubefree; with the smaller range $x > q^{\frac38+o(1)}$ otherwise.

[28] See section 3.2 for the definition of ρ, from which it can be deduced that $\rho(v) = o_{v\to\infty}(1)$.

[29] Our proof here uses GRH, but this can be proved unconditionally — see [GS2].

[30] Much of the argument here is implicit in much earlier work of Friedlander and Iwaniec [FI].

Proposition 4.1. *For any sets $B, U, V \subset \mathbb{F}_q$ we have*

$$\frac{1}{|B|}\left|\sum_{n\in B}\chi(n)\right| \le \left(\left(\frac{r^{2r}q}{|V|^r}+2r\sqrt{q}\right)\frac{E_\times(B,U)}{|B|^2|U|^2}\right)^{\frac{1}{2r}} + 2\left(1-\frac{1}{|B||U||V|}\#\{u\in U, v\in V, b,b'\in B : b-b'=uv\}\right). \tag{4.8}$$

Remark. To get a non-trivial result, we must have $2r\sqrt{q}E_\times(B,U)/|B|^2|U|^2 < 1$. Now $E_\times(B,U) \le |B||U|$ and $|U| \le |B|$ with $r \ge 1$, so we *must have* $|B| \ge q^{1/4}$.

Proof. Since

$$\left|\sum_{n\in B}\chi(n) - \sum_{n\in B}\chi(n+t)\right| \le 2|B\setminus(B+t)| = 2(|B| - r_{B-B}(t)),$$

we deduce that

$$\left|\sum_{n\in B}\chi(n) - \frac{1}{|T|}\sum_{t\in T}\sum_{n\in B}\chi(n+t)\right| \le 2\left(|B| - \frac{1}{|T|}\sum_{t\in T} r_{B-B}(t)\right).$$

If $T = UV$ counting multiplicities then

$$\left|\frac{1}{|T|}\sum_{t\in T}\sum_{n\in B}\chi(n+t)\right| \le \frac{1}{|U||V|}\sum_{\substack{n\in B\\ u\in U}}\left|\sum_{v\in V}\chi(nu^{-1}+v)\right| = \frac{1}{|U||V|}\sum_m r_{B/U}(m)\left|\sum_{v\in V}\chi(m+v)\right|.$$

By Holder's inequality this is

$$\le \frac{1}{|U||V|}\left(\sum_m r_{B/U}(m)\right)^{1-\frac{1}{r}}\left(\sum_m r_{B/U}(m)^2\right)^{\frac{1}{2r}}\left(\sum_m\left|\sum_{v\in V}\chi(m+v)\right|^{2r}\right)^{\frac{1}{2r}}.$$

Now $\sum_m r_{B/U}(m) = |B||U|$ and $\sum_m r_{B/U}(m)^2 = E_\times(B,U)$. Expanding the $2r$th power in the last term of the line above we obtain

$$\sum_{v_1,\dots,v_{2r}\in V}\sum_{n\in\mathbb{F}_q}\chi\left(\frac{(n+v_1)\dots(n+v_r)}{(n+v_{r+1})\dots(n+v_{2r})}\right).$$

By Weil's theorem we know that if χ has order $k > 1$ and $f(x)$ is not a kth power then

$$\sum_{n\in\mathbb{F}_q}\chi(f(n)) \le (\#\{\text{distinct roots of } f\} - 1)\sqrt{q}.$$

Evidently if our rational function is a kth power then the numerator is of the form $g(n)^k f(n)$ and the denominator is of the form $G(n)^k f(n)$ for some polynomials f, g, G. Hence the number of possible rational functions of this type that are kth powers is (counting over polynomials g of degree d), where each $v_i \in V$,

$$\leq \sum_{d=0}^{[r/k]} |V|^{2d+(r-dk)} \left(\frac{r!}{k!^d}\right)^2 \leq r^{2r}|V|^r,$$

and each contributes $\leq q$. The other $\leq |V|^{2r}$ terms each contribute $\leq (2r-1)\sqrt{q}$ by Weil's theorem, so in total our sum is

$$\leq r^{2r}|V|^r q + |V|^{2r}(2r-1)\sqrt{q}.$$

Combining all this info yields (4.8).

We now show how to recover Burgess's theorem.

Corollary 4.2. *Fix integer $r \geq 1$. If $N \geq q^{\frac{r+1}{4r}}$ then, for any integer M, we have*

$$\frac{1}{N}\left|\sum_{M<n\leq M+N}\chi(n)\right| \lesssim \left(\frac{q^{\frac{r+1}{4r}}}{N}\right)^{\frac{2}{2r+1}}(1+(\log q)^{\frac{1}{2r}})$$

Proof. Let B be the set of integers in the interval $(M, M+N]$ of length N, V the set of integers $\leq r^2 q^{1/2r}$ and U be the set of primes in the interval $q \in (Q, 2Q]$ where $Q = (2/3r^2)\cdot(N^{2r-1}/q^{1/2})^{\frac{1}{2r+1}}$. We first need to determine $E_\times(B,U)$, that is the number of solutions to $bq = b'q'$. If $q = q'$ then $b = b'$ and so there are $N|U|$ such diagonal solutions. If $q \neq q'$ then $b = nq'$ and $b' = nq$ for some integer n in an interval of length $N/\max\{q, q'\} \leq N/Q$, so that there are $\leq |U|^2 N/Q = o(N|U|)$ such solutions. Hence $E_\times(B,U) \sim NQ/\log Q$. If $t > 0$ then $|B| - r_{B-B}(t) \leq t$ (with equality for $t \leq |B|$), so (4.8) becomes

$$\frac{1}{N}\left|\sum_{M<n\leq M+N}\chi(n)\right| \lesssim \left(\frac{\sqrt{q}}{NQ/\log Q}\right)^{\frac{1}{2r}} + \frac{3r^2 q^{1/2r}Q}{2N}$$

which yields the result.

Recently Henri Cohen posted a question about bounds for character sums over squarefree integers on the number theory listserve. One can apply Proposition 4.1, by restricting elements of V to be divisible by $(\prod_{p\leq y} p)^2$, to obtain a non-trivial upper bound for all intervals of length $> q^{1/4+o(1)}$.

4.3. Improving Burgess's Theorem? Integral delay equations. Suppose that the least quadratic non-residue of the quadratic character $\pmod q$ is of size $q^{1/(4\sqrt{e})+o(1)}$, for an infinite sequence of primes q, which is large as it can be. If so that $(n/q) = 1$ for all $n \le q^{1/(4\sqrt{e})+o(1)}$. In particular if $\chi(t) = \chi_{(./q)}(t)$ where $y = q^{1/(4\sqrt{e})}$ then $\chi(t) = \sigma(t) = 1$ for $t \le 1$, and $\sigma(u) = 0$ for all $u \ge \sqrt{e}$ by Burgess's Theorem. By (3.8) we have, for $1 \le u \le 2$ that $\sigma(u) = 1 - \int_1^u \frac{1-\chi(t)}{t}dt \ge 1 - \int_1^u \frac{2}{t}dt = 1 - 2\log u$, so $\chi(t) = -1$ for all $1 \le t \le \sqrt{e}$ as $\sigma(\sqrt{e}) = 0$. Therefore

$$\sigma(u) = \begin{cases} 1 & \text{for } u \le 1; \\ 1 - 2\log u & \text{for } 1 \le u \le \sqrt{e}; \\ 0 & \text{for } u \ge \sqrt{e}. \end{cases} \tag{4.9}$$

A simple calculation reveals that,

$$(s + \log y)\mathcal{L}(\sigma, s) \approx L(1 + s/\log y, (./q)),$$

so that we can hunt for zeros of the Dirichlet L-function just inside the critical strip by looking for zeros of $\mathcal{L}(\sigma, s)$ with $\mathrm{Re}(s) < 0$. Now by (4.9) and then integrating by parts,

$$\mathcal{L}(\sigma, z) = \int_0^{\sqrt{e}} e^{-uz}du - \int_1^{\sqrt{e}} 2(\log u)e^{-uz}du = \frac{1}{z} - \frac{2}{z}\int_1^{\sqrt{e}} \frac{e^{-uz}}{u}du.$$

Multiplying through by z and integrating by parts twice more gives

$$1 - 2\int_1^{\sqrt{e}} \frac{e^{-uz}}{u}du = 1 - 2\frac{e^{-z\sqrt{e}}}{z\sqrt{e}} + O\left(\frac{e^R}{|z|} + \frac{e^{R\sqrt{e}}}{|z|^2}\right),$$

where $\mathrm{Re}(z) = -R$. Substituting in $z_k(\phi)\sqrt{e} = -\log(\pi k) \pm 2i\pi(k - 1/4) - \log(1 - \delta e^{i\phi})$ for a large integer k we obtain

$$z\mathcal{L}(\sigma, z) = \delta e^{i\phi} + O\left(\frac{1}{k^{1-1/\sqrt{e}}} + k\epsilon^{\eta/3}\right) + o(k) = \delta e^{i\phi} + O\left(\frac{1}{k^{1-1/\sqrt{e}}}\right),$$

since $0 < k \le (1/\epsilon)^{\eta/6}$. Taking, say, $\delta = 1/k^{1/3}$ we see by the argument principle that $\mathcal{L}(\sigma, z)$ has exactly one zero z_k satisfying $\sqrt{e}z_k = -\log(\pi k) \pm 2i\pi(k - 1/4) + O(1/k^{1/3})$, and thus we have proved that

$$L(s, (./q_i)) = 0 \quad \text{for} \quad s = 1 - \frac{z_k + o_k(1)}{\log(q_i^{1/4})},$$

where $z_k = \log(\pi k) \pm 2\pi i(k - 1/4)$. It is possible to prove an analogous result (see [GS12]) whenever $|\sum_{n \le x} \chi_i(n)| \gg x$ for an infinite sequence of primitive characters $\chi_i \pmod{q_i}$ of order r, with $x = q_i^\theta$, using Halász's theorem: In this case we have only been able to prove that we have an infinite sequence of such complex numbers z_k, although we believe that they also satisfy a similar growth condition.

This same circle of ideas has led us to prove in [GS12] that if χ is a real, primitive character $\pmod q$, and one hundred percent of the zeros of $L(s, \chi)$ up to height 1 lie on the critical line, then (4.6) holds uniformly for all $x > q^\epsilon$ (and a similar but weaker result for complex characters).

5. Pretentiousness

In the last few years we have introduced the word *pretentiousness* into this literature. A multiplicative function f is called ψ-pretentious if it is very similar to ψ; i.e. if $f(p) \approx \psi(p)$ for "most" primes p up to some given point z. The prototype for pretentiousness is Halász's theorem which, in this language, states that if a multiplicative function f, with each $|f(n)| \leq 1$, has large mean value up to x then $f(n)$ must be n^{it}-pretentious for some "small" t. Let us begin by defining a distance function: If f and g are two multiplicative functions with values inside or on the unit circle define

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

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

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

Then Halász's theorem states that if the mean value up to x of a multiplicative function f, with each $|f(n)| \leq 1$, is $\gg 1$, then there exists $t \in \mathbb{R}$ with $|t| \ll 1$ such that $\mathbb{D}(f(n), n^{it}; x) \ll 1$. Actually one find "pretentious proofs" in many places in the analytic number theory literature, perhaps most strikingly the original

5.1. Proof of the prime number theorem. By 1896 researchers only needed to show that $\zeta(1+it) \neq 0$ 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 [Da]. 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 and hence $\zeta(1+2it)=\infty$. In other words, if $\lambda(n)$ is n^{it}-pretentious then 1 is n^{2it}-pretentious, which is clearly false.[31] Justifying this argument was rather complicated, and every textbook repeats the rather elegant, subsequent argument of Mertens which avoids many technicalities rather cleverly.[32]

The usual proof that $\zeta(1+it) \neq 0$ for all non-zero real t: Suppose $\zeta(1+it)=0$ for some real $t \neq 0$. Since ζ is analytic there, one may suppose the zero is of order $r \geq 1$ so that, using the Taylor series, we have $\zeta(1+\Delta+it) \approx c\Delta^r$ for $|\Delta|$ sufficiently small. We also know that $\zeta(s)$ has a pole of order 1 at $s=1$, so that $\zeta(1+\Delta) \approx 1/\Delta$. Now the clever observation of Mertens (1898) was to use the inequality

$$|\zeta(\sigma)\zeta(\sigma+it)^4\zeta(\sigma+2it)^3| \geq 1,$$

which holds for all real $\sigma > 1$ and $t \neq 0$. (We'll re-establish this in the next subsection.) Substituting in $\sigma = 1+\Delta$ with $\Delta > 0$ small, we have

$$|\Delta^{4r-1}\zeta(1+\Delta+2it)^3| \gg 1.$$

[31] Here $\lambda(n)$ is Liouville's function, totally multiplicative with $\lambda(p)=-1$ for every prime p.

[32] For more on the history of the prime number theorem, read Narkiewicz's superb book [Nar].

As $\Delta \to 0$ the left side will go to zero unless $\zeta(s)$ has a pole of order $\geq \frac{4r-1}{3} \geq 1$ at $s = 1 + 2it$. This contradicts the fact that $\zeta(s)$ is analytic at $s = 1 + 2it$.

Our pretentious proof that $\zeta(1+it) \neq 0$ for all non-zero real t: We obtain $\zeta(1+\Delta+it) \approx c\Delta^r$ for $|\Delta|$ sufficiently small as above, now taking $\Delta = \frac{1}{\log x}$ for sufficiently large x. One can show that this is equivalent to

$$\prod_{p\leq x}\Big(1-\frac{1}{p^{1+it}}\Big)^{-1} \asymp \frac{1}{(\log x)^r};$$

i.e. the extra $\frac{1}{\log x}$ in the exponent means the contribution of the primes $> x$ to the product is uniformly bounded, and the contribution of $p^{1/\log x}$ to the term for each prime $p < x$ is too small to significant change the value of the product. Our product can be rewritten as

$$\prod_{p\leq x}\Big(1+\frac{e^{-it\log p}}{p}\Big) \asymp \frac{1}{(\log x)^r}.$$

Now

$$\frac{1}{(\log x)^r} \gg \Big|\prod_{p\leq x}\Big(1+\frac{e^{-it\log p}}{p}\Big)\Big| \geq \prod_{p\leq x}\Big(1-\frac{1}{p}\Big) \gg \frac{1}{\log x}$$

by Mertens' theorem so that $r = 1$, and hence

$$\prod_{p\leq x}\Big(1+\frac{1+e^{-it\log p}}{p}\Big) \asymp \prod_{p\leq x}\Big(1-\frac{1}{p}\Big)^{-1}\cdot\prod_{p\leq x}\Big(1+\frac{e^{-it\log p}}{p}\Big) \asymp 1.$$

Taking logarithms of each side we see that $p^{-it} = e^{-it\log p}$ pretends to be -1; more precisely that $\mathbb{D}(p^{-it}, -1; x)$ is bounded. Now the triangle inequality yields $\mathbb{D}(p^{-2it}, 1; x) \leq 2\mathbb{D}(p^{-it}, -1; x)$ so is also bounded, and hence, repeating the steps above gives

$$\zeta(1+\Delta+2it) \asymp \prod_{p\leq x}\Big(1-\frac{1}{p^{1+2it}}\Big)^{-1} \asymp \prod_{p\leq x}\Big(1-\frac{1}{p}\Big)^{-1} \asymp \log x.$$

This implies that $\zeta(s)$ has a pole of order 1 at $s = 1 + 2it$, contradicting the fact that it is analytic at this point.

5.2. Interlude: Distance and beyond. Consider the space $\mathbb{U}^{\mathbb{N}}$ of vectors $\mathbf{z} = (z_1, z_2, \dots)$ where each z_i lies on the unit disc $\mathbb{U} = \{|z| \leq 1\}$. The space is equipped with a product obtained by multiplying componentwise: that is, $\mathbf{z} \times \mathbf{w} = (z_1w_1, z_2w_2, \dots)$. Suppose we have a sequence of functions $\eta_j : \mathbb{U} \to \mathbb{R}_{\geq 0}$ for which $\eta_j(zw) \leq \eta_j(z) + \eta_j(w)$ for any z, $w \in \mathbb{U}$. Then we may define a 'norm' on $\mathbb{U}^{\mathbb{N}}$ by setting

$$\|\mathbf{z}\| = \Big(\sum_{j=1}^{\infty}\eta_j(z_j)^2\Big)^{\frac{1}{2}},$$

assuming that the sum converges. The key point is that such a norm satisfies the triangle inequality

$$\|\mathbf{z}\times\mathbf{w}\|\le\|\mathbf{z}\|+\|\mathbf{w}\|,$$

since

$$\|\mathbf{z}\times\mathbf{w}\|^2=\sum_{j=1}^{\infty}\eta_j(z_jw_j)^2\le\sum_{j=1}^{\infty}(\eta_j(z_j)^2+\eta_j(w_j)^2+2\eta_j(z_j)\eta_j(w_j))$$
$$\le\|\mathbf{z}\|^2+\|\mathbf{w}\|^2+2\Big(\sum_{j=1}^{\infty}\eta_j(z_j)^2\Big)^{\frac12}\Big(\sum_{j=1}^{\infty}\eta_j(w_j)^2\Big)^{\frac12}=(\|\mathbf{z}\|+\|\mathbf{w}\|)^2,$$

using the Cauchy-Schwarz inequality.

A nice class of examples is provided by taking $\eta_j(z)^2=a_j(1-\text{Re }z)$ where the a_j are non-negative constants with $\sum_{j=1}^{\infty}a_j<\infty$. This last condition ensures the convergence of the sum in the definition of the norm. To verify that $\eta_j(zw)\le\eta_j(z)+\eta_j(w)$, note that $1-\text{Re }(e^{2i\pi\theta})=2\sin^2(\pi\theta)$ and $|\sin(\pi(\theta+\phi))|\le|\sin(\pi\theta)\cos(\pi\phi)|+|\sin(\pi\phi)\cos(\pi\theta)|\le|\sin(\pi\theta)|+|\sin(\pi\phi)|$. This settles the case where $|z|=|w|=1$, and one can extend this to all pairs $z,w\in\mathbb{U}$.

Now we show how to use such norms to study multiplicative functions. Let f be a completely multiplicative function. Let $q_1<q_2<\dots$ denote the sequence of prime powers, and we identify f with the element in $\mathbb{U}^{\mathbb{N}}$ given by $(f(q_1),f(q_2),\dots)$. Take $a_j=\Lambda(q_j)/(q_j^{\sigma}\log q_j)$ for $\sigma>1$, and $\eta_j(z)^2=a_j(1-\text{Re }z)$. Then our norm is

$$\|f\|^2=\sum_{j=1}^{\infty}\frac{\Lambda(q_j)}{q_j^{\sigma}\log q_j}(1-\text{Re }f(q_j))=\log\frac{\zeta(\sigma)}{|F(\sigma)|},$$

where $F(s)=\sum_{n=1}^{\infty}f(n)n^{-s}$.

Let f and g be completely multiplicative functions with $|f(n)|\le1$ and $|g(n)|\le1$, and $F\otimes G(s)=\sum_{n=1}^{\infty}f(n)g(n)n^{-s}$. Then by the triangle inequality we have

$$\sqrt{\log\frac{\zeta(\sigma)}{|F(\sigma)|}}+\sqrt{\log\frac{\zeta(\sigma)}{|G(\sigma)|}}\ge\sqrt{\log\frac{\zeta(\sigma)}{|F\otimes G(\sigma)|}},\tag{5.1a}$$

for $\sigma>1$, and, taking $(-1)^{\Omega(n)}f(n)$ and $(-1)^{\Omega(n)}g(n)$ in place of f and g we obtain

$$\sqrt{\log|\zeta(\sigma)F(\sigma)|}+\sqrt{\log|\zeta(\sigma)G(\sigma)|}\ge\sqrt{\log\frac{\zeta(\sigma)}{|F\otimes G(\sigma)|}}.\tag{5.1b}$$

Taking $f(n)=n^{-it_1}$ and $g(n)=n^{-it_2}$ we are led to the following curious inequalities for the zeta-function which we have not seen before:

$$\sqrt{\log\frac{\zeta(\sigma)}{|\zeta(\sigma+it_1)|}}+\sqrt{\log\frac{\zeta(\sigma)}{|\zeta(\sigma+it_2)|}}\ge\sqrt{\log\frac{\zeta(\sigma)}{|\zeta(\sigma+it_1+it_2)|}},$$

and

$$\sqrt{\log|\zeta(\sigma)\zeta(\sigma+it_1)|}+\sqrt{\log|\zeta(\sigma)\zeta(\sigma+it_2)|}\ge\sqrt{\log\frac{\zeta(\sigma)}{|\zeta(\sigma+it_1+it_2)|}}.$$

If we take $t_1=t_2$ in this last inequality, square out and simplify, we obtain the classical inequality $\zeta(\sigma)^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)|\ge 1$ of Mertens used in the last section. It is conceivable that the more flexible inequalities here could lead to numerically better zero-free regions for $\zeta(s)$, but our initial approaches in this direction were unsuccessful.

Taking $f(n)=\chi(n)n^{-it_1}$ and $g(n)=\psi(n)n^{-it_2}$ in (5.1) leads to similar inequalities for Dirichlet L-functions: for example,

$$\sqrt{\log\frac{\zeta(\sigma)}{|L(\sigma+it_1+it_2,\chi\psi)|}}\le\sqrt{\log\frac{\zeta(\sigma)}{|L(\sigma+it_1,\chi)|}}+\sqrt{\log\frac{\zeta(\sigma)}{|L(\sigma+it_2,\psi)|}}.$$

Thus the classical inequalities leading to zero-free regions for Dirichlet L-functions can be put in this framework of triangle inequalities. We wonder if similar useful inequalities could be found for other L-functions.

It is no more difficult to conclude from (5.1) that

$$\sqrt{\pm\mathrm{Re}\Big(\frac{F'(\sigma)}{F(\sigma)}\Big)-\frac{\zeta'(\sigma)}{\zeta(\sigma)}}+\sqrt{\pm\mathrm{Re}\Big(\frac{G'(\sigma)}{G(\sigma)}\Big)-\frac{\zeta'(\sigma)}{\zeta(\sigma)}}\ge\sqrt{\mathrm{Re}\Big(\frac{(F\otimes G)'(\sigma)}{(F\otimes G)(\sigma)}\Big)-\frac{\zeta'(\sigma)}{\zeta(\sigma)}}.$$

Again taking $F=G$ and squaring we obtain:

$$3\frac{\zeta'(\sigma)}{\zeta(\sigma)}\pm 4\mathrm{Re}\left(\frac{F'(\sigma)}{F(\sigma)}\right)+\mathrm{Re}\left(\frac{(F\otimes F)'(\sigma)}{(F\otimes F)(\sigma)}\right)\le 0.$$

There is probably a lot waiting to be done with these new identities!

5.3. A new (and easy) application of pretentiousness. Suppose that we cannot improve Burgess's theorem, in that there exist arbitrarily large q and $x=q^c$ such that $|\sum_{n\le x}\chi(n)|\gg x$. By Halász's theorem we know that $\chi(n)$ must be n^{it}-pretentious for some small t and so $\chi^2(n)$ must be n^{2it}-pretentious. Hence we might expect that $|\sum_{n\le y}\chi^2(n)|$ is large for some values of y close to x:

Define $\phi=M+\log(1+|t|)+O(1)$ where t is the value of y in (3.2) and $M=M(x,t)$. We will prove (as in [GS12]) that there exists y in the range $x^{1/(\phi e^\phi)}\le y\le x$ such that

$$\left|\sum_{n\le y}f(n)\right|>e^{-\phi}y. \tag{5.2}$$

Proof of (5.2). Let $\eta=1/(\phi e^\phi)$ and $\delta=\phi/\log x$. Let $g(.)$ be that totally multiplicative function for which $g(p)=f(p)$ for all primes $p\le x$, and $g(p)=0$ for all primes $p>x$. Now

$$\sum_{n\ge1}\frac{g(n)}{n^{1+\delta+it}}=\prod_{p\le x}\left(1-\frac{f(p)}{p^{1+\delta+it}}\right)^{-1}$$

which, in absolute value, is

$$\asymp \prod_{p\le x}\left(1-\frac{1}{p^{1+\delta}}\right)^{-1}\exp\left(-\sum_{p\le x}\frac{1-\mathrm{Re}(f(p)/p^{it})}{p^{1+\delta}}\right) \gg \frac{\log x}{\phi}\ e^{-M} \tag{5.3}$$

by the prime number theorem. On the other hand

$$\sum_{n\ge 1}\frac{g(n)}{n^{1+\delta+it}} = (1+\delta+it)\int_1^\infty \frac{1}{y^{2+\delta+it}}\sum_{n\le y} g(n)dy.$$

Assuming that $|\sum_{n\le y} f(n)| \le e^{-\phi}y$ for all $x^\eta \le y \le x$, and using the the trivial bound $|\sum_{n\le y} g(n)| \le y$ otherwise, we find that the absolute value of the integral here is

$$\begin{aligned}&\ll \int_1^{x^\eta}\frac{dy}{y^{1+\delta}} + e^{-\phi}\int_{x^\eta}^x \frac{dy}{y^{1+\delta}} + \int_x^\infty \frac{dy}{y^{1+\delta}}\\ &= \frac{\log x}{\phi}\left((1-e^{-\eta\phi}) + e^{-\phi}(e^{-\eta\phi}-e^{-\phi}) + e^{-\phi}\right) \le 3e^{-\phi}\ \frac{\log x}{\phi}\end{aligned}$$

which yields a contradicts (5.3) if the "$O(1)$" in the choice of ϕ is chosen sufficiently large.

Using the triangle inequality it is now easy to prove the result claimed in the first paragraph of this subsection, and much more: For example if we have large character sums for two different characters, then we do for their product.

In section 4.3 we saw that a large character sum for quadratic character χ, contradicting an improvement to Burgess, tells us about many zeros of $L(s,\chi)$ close to the 1-line (in fact these notions are more-or-less equivalent). If we have two (distinct) such characters then, by what we have just done, we know that there is a large character sum for their product, which is also a character of order 2. Hence zeros of two L-functions tell us about zeros of another, third, L-function, at least in the unlikely situation that Burgess cannot be significantly improved. This is the first time such a phenomenon has been observed.

5.4. Pólya-Vinogradov revisited. A real number $\alpha \in [0,1)$ lies on a *major arc* if it is within a "small" distance of a rational number with small denominator; otherwise α lies on a *minor arc*. The arcs are so named because in many integrals on the circle that arise in number theory, it is the part of the integral on the major arcs (that is, at angles close to $2\pi a/b$ for small b) which contribute the main term to the overall integral, and the minor arcs just contribute to the error. This was confirmed by Montgomery and Vaughan [MV1] who showed that one can always get non-trivial upper bounds on $\sum_{n\le N} f(n)e(\alpha n)$ assuming α lies on a minor arc. This is enough to deduce that if x/q is on a minor arc then the contribution of the terms involving $e(\frac{-hx}{q})$ in (4.1) is small; hence the character sum is large if and only if $\sum_h \overline{\chi}(h)/h = (1-\chi(-1))L(1,\overline{\chi})$ is large. It is straightforward to show[33] that this is large if and only if $\chi(-1)=-1$ and χ is 1-pretentious.

[33] And should be done as an exercise

If x/q is near to a rational a/b with small denominator then the character sum up to x is determined by the right side of (4.1), which will be determined by the value of the right side of (4.1) with x/q replaced by a/b. But $e(\frac{\cdot}{b})$ can be re-written as sum over characters $\psi \pmod b$, with fixed coefficients which have denominators around size $\sqrt{b}$.[34] Therefore we can re-write the value of (4.1) as a linear combination of sums of the form $\sum_h \overline{\chi}(h)\psi(h)/h$. Such a sum can be large if and only if χ is ψ-pretentious, and $\chi(-1)\psi(-1) = -1$. Moreover b must be bounded for the right side of (4.1) to be large, because of the denominator $\sqrt{b}$. (Notice that the special case at the end of the last paragraph is simply an example, $\psi = 1$, of what we have here.)

So can χ a character mod q, be ψ-pretentious for a character ψ of bounded conductor? Certainly this would contradict the Riemann Hypothesis for $L(s, \chi\overline{\psi})$. One can easily show that χ cannot be pretentious for more than one such character;[35] and so we can deduce a significant improvement to the Pólya-Vinogradov theorem simply by assuming the Riemann Hypothesis for $L(s, \chi\overline{\psi})$.[36]

We can again multiply characters together for which there is a large character sum: We have seen that there is a large character sum for χ_j if and only if χ_j is ψ_j-pretentious, and $\chi_j(-1)\psi_j(-1) = -1$ for some character ψ_j of small conductor. But then $\chi := \chi_1\chi_2\chi_3$ is $\psi := \psi_1\psi_2\psi_3$-pretentious, and $\chi(-1)\psi(-1) = -1$, so we have a large character sum for $\chi_1\chi_2\chi_3$. (This can all be quantified quite precisely; see [GS8] for details.) In particular if we have a large character sum for χ then we do for χ^k for any fixed odd integer k. For example, if χ, a primitive character of order 6 mod q, has a large character sum, then so does $(./q)$. As in the last section this idea that strange behaviour by one character implies the same for another character appears to be a quite new phenomenon.

Now let's prove that one cannot have a large character sum for any primitive character χ of order 3: Note that $\chi(-1) = \chi^3(-1)/(\chi(-1))^2 = 1/(\pm 1)^2 = 1$, and so if we do have a large character sum then χ is ψ-pretentious, where $\psi(-1) = -1$ for some character ψ of small conductor b. But then for most small primes $p \equiv -1 \pmod b$ we have that $\chi(p)$, which equals $1, e(\frac{1}{3})$ or $e(\frac{2}{3})$ must be close to $\psi(p) = \psi(-1) = -1$, which is blatantly false, contradiction. A similar proof works for characters of any fixed odd order.

As we noted at the end of section 4.1 there is little hope of significantly improving the Pólya-Vinogradov theorem, either unconditionally or assuming GRH, for characters of order 2. However from the argument of the last paragraph we obtained the following improvement [GS8] for primitive characters $\chi \pmod q$ of odd order $g > 1$:

$$\left|\sum_{n\le x} \chi(n)\right| \ll_g \begin{cases} \sqrt{q}(\log q)^{1-\frac{\delta_g}{2}+o(1)} & \text{unconditionally, and} \\ \sqrt{q}(\log\log q)^{1-\frac{\delta_g}{2}+o(1)} & \text{assuming GRH,} \end{cases}$$

where $\delta_g = 1 - \frac{g}{\pi}\sin\frac{\pi}{g}$.[37] The argument of two paragraphs above implies that we can

[34] Another exercise!

[35] Fun exercise: Prove this, ie that "*pretentiousness is repulsive*."

[36] Our original objective was to try to reprove Montgomery and Vaughan's result using just the Riemann Hypothesis for $L(s, \chi)$, not the whole of GRH like they did. We now understand that we had the wrong objective — it is surprising that a character sum over χ-values should depend on the Riemann Hypothesis for a quite different character, $\chi\overline{\psi}$.

[37] It should be possible to significantly improve the exponents given here – I do not think our tech-

significantly improve the Pólya-Vinogradov theorem for primitive characters of even order $2^k\ell$, where ℓ is odd, if we can do so for primitive characters of order 2^k.

Leo Goldmakher [Gol] recently observed that one can apply these ideas to significantly improve the Pólya-Vinogradov theorem for characters belonging to certain special classes of conductors: His key observation is to note that if χ is 1-pretentious for the primes up to y, then $L\left(1+\frac{1}{\log y},\chi\right) \gg \log y$, and then to get upper bounds on the L-function value using known bounds for character sums. In particular, using bounds of Postnikov-Gallagher-Iwaniec [Iw] on characters whose conductor q has small *radical* $\mathrm{rad}(q) := \sum_{p|q} \log p$ one can show that

$$\left|\sum_{n\le x} \chi(n)\right| \ll \sqrt{q}\left((\log q)^{1/2}(\log \mathrm{rad}(q))^{1/2} + (\log q)^{7/8}(\log\log q)^{3/8}\right),$$

which is $o(\sqrt{q}\log q)$ provided $\mathrm{rad}(q) = q^{o(1)}$. Goldmakher also proved that

$$\left|\sum_{n\le x} \chi(n)\right| \ll \sqrt{q}\left((\log q)^{3/4}(\log P(q)d(q))^{1/4} + \frac{\log q}{(\log\log q)^{1/2}}\right),$$

where $P(q)$ is the largest prime divisor of q, and $d(q)$ is the number of divisors, which is $o(\sqrt{q}\log q)$ provided $P(q) = q^{o(1)}$.

6. Recent work

6.1. Pretentiousness is indeed repulsive. In [GS11] we prove that there is an absolute constant $c > 0$ such that if f is a multiplicative function, and χ and ψ are any two distinct primitive characters with conductor below Q, then for $x \ge Q$ we have

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

hence one of the two distances must be large. In fact we can put the distances from any given character to the set of characters of small conductor in order and get some good lower bounds: Given a primitive character $\chi \pmod q$ organize the primitive characters $\psi_j \pmod{m_j}$ with $m_j \le \log y$, so the distances $\mathbb{D}(\chi, \psi_j; y)$ are in ascending order. Then

$$\mathbb{D}(\chi, \psi_j; y)^2 \ge \left(1 - \frac{1}{\sqrt{j}} + o(1)\right)\log\log y,$$

for $1 \le j \ll 1$.

niques were optimized – a good research problem.

6.2. Multiplicative functions in arithmetic progressions. Halász's theorem states 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: In [BGS], Balog, Sound and I showed that if the mean value of f is "large" in an arithmetic progression mod q then $f(n)$ is $\chi(n)n^{it}$-pretentious for some Dirichlet character χ mod q and some "small" real t. From what we just stated about pretentiousness being repulsive, there can only be one such χ and t.

It would be interesting to know what could be said about when

$$\frac{1}{\pi(N)}\sum_{p\le N} f(p-1)$$

is large? Certainly if $f(n)=n^{it}$ then this is $\sim N^{it}/(1+it)$. Also if $f(p)=\chi(p)$ whenever $p\nmid q$ then the mean-value is $\sim -\chi(-1)/\phi(q)$. Perhaps if the mean-value is large then $f(n)$ must be $\chi(n)n^{it}$-pretentious for some Dirichlet character $\chi \pmod q$, where q and t are both small?

6.3. Exponential sums. If $\left|\sum_{n\le x} f(n)e^{2i\pi n\alpha}\right|$ is large then Montgomery and Vaughan [MV1] showed that α is on a major arc; i.e. α is close to some rational a/b with b "small". In [GS13] we show, in addition, that $f(n)$ is $\psi(n)n^{it}$-pretentious where ψ is a character of conductor b and t is "small".

This result 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 $(1+\delta_1)^3$, where this is the δ_1 we encountered in section 3.5. One corollary states that for sufficiently large x, for each prime p at least $\frac{1}{2}\%$ of the solutions to $a+b=c\le x$ give rise to Pythagorean triangles mod p (that is $a+b=c$ where a,b and c are squares mod p).

More generally, if f,g,h are three totally multiplicative functions whose values all lie in $\mathbb{U}$, such that

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

then $f(n), g(n), h(n)$ 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 $\psi_1\psi_2\psi_3$ principal

6.4. The prime number theorem in terms of multiplicative functions. Since $\zeta(s)^{-1} = \sum_{n\geq 1} \mu(n)/n^s$, one can show that the prime number theorem is of the same depth as proving that $\sum_{n\leq x} \mu(n) = o(x)$ or, equivalently, that $\sum_{n\leq x} \lambda(n) = o(x)$.[38] Hence we may write the prime number theorem as: 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

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

whenever $(a, q) = 1$. As we noted way back on page 6, we only know this, unconditionally with $x_{\epsilon,q}$ exponential in a power of q, which is not useful in many applications. It was a great breakthrough when Bombieri and Vinogradov showed how to get $x_{\epsilon,q}$ just a touch bigger than q^2, for "most" q. A beautiful and more explicit version of this theorem, though with a slightly smaller range, was given by a result of Gallagher [Ga1]: Given $\epsilon > 0$ there exists $A > 1$ such that

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

for all $(a, q) = 1$ and all $q \leq x^{1/A}$, except those q that are multiples of some exceptional modulus r. In this case there exists a character $\psi \pmod r$ such that

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

whenever $(a, q) = 1$ and r divides q, with $q \leq x^{1/A}$. 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 $L(\psi, s)$ lying very close to $s = 1$. We already know

[38] This equivalence can be obtained by entirely elementary means by summing over the identity $\sum_{n=ab} \mu(a) \log b = \log n$ if n is a prime power, 0 otherwise.

that there cannot be two such characters ψ because pretentiousness is repulsive. That there cannot be two such characters has typically been proved in the past by noting that if there were then they would both have zeros close to 1, and hence to each other, but zeros of Dirichlet L-functions "repel" according to the DEURING-HEILBRONN phenomenon.[39] The (unique) exceptional zero is known as a "Siegel zero" or "Landau-Siegel zero", and is typically believed to lie deep in the theory of Dirichlet L-functions.

In [BGS] we have generalized GALLAGHER's theorem, from λ to *all* multiplicative functions f with all $|f(n)| \le 1$: 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 those q that are multiples of some exceptional modulus r. In this case there exists 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.[40]

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.[41] Moreover GALLAGHER's theorem no longer appears to lie deep in the theory of Dirichlet L-functions but instead is a rather general phenomenon. In fact, given the generality of this new result, one might expect a proof that is entirely combinatorial and has little to do with the analytic number theory of zeta functions. In our proof we require, for some fixed 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 $[q^C, 2q^C]$.

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 $\psi(n) = 1$.

[39] Hence our terminology, "repulsion".

[40] We have quite consciously written out a version of Gallagher's theorem which is, word-for-word, the example $f = \lambda$ of this theorem.

[41] Analytic number theorists tend to think of mean value theorems for the coefficients of Dirichlet series (like $L(f,s) := \sum_{n\ge1} f(n)/n^s$) as coming from so-called Tauberian theorems. Yet here we see a quite developed theory of mean values of $L(f\chi, s)$, with little chance of proving these results by Tauberian methods, since the $L(f\chi, s)$ are not so likely to be provably analytic on the line $\mathrm{Re}(s) = 1$ nor a little to the left of it.

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 [Sl2] 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 [Fr1] conveniently showed this for all $x \ge q^{3B}$, which is what allows us to prove our result avoiding deep facts about L-functions.

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

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

For small q, that is $q \le (\log x)^C$, onee 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.

6.5. Periodic functions pretending to be characters. One step of the proof is rather entertaining: If $g : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}$ is a function with $g(1)=1$, and $|g(ab)-g(a)g(b)| \le \epsilon (< \frac{1}{2})$ 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 $(a,q)=1$. Such problems are explored in much greater generality in [BFL].

References

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

[BGS] A. Balog, A. Granville and K. Soundararajan, *Multiplicative Functions in Arithmetic Progressions* (to appear).

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

[Bo] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque **18** (1987/1974), 103 pp.

[BFI] E. Bombieri, J.B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli III*, J. Amer. Math. Soc. **2** (1989), 215-224.

[Bu1] D.A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika Soc **4** (1957), 106-112.

[Bu2] ———, *On character sums and L-series, I*, Proc. London Math. Soc **12** (1962), 193-206; II, Proc. London Math. Soc **13** (1963), 524-536.

[Cra] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2** (1936), 23-46.

[Dav] H. Davenport, *Multiplicative number theory*, Springer Verlag, New York, 1980.

[Fr1] 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.

[FG1] J.B. Friedlander and A. Granville, *Limitations to the equi–distribution of primes I*, Ann. Math. **129** (1989), 363-382.
[FG2] ———, A. Hildebrand and H. Maier, *Oscillation theorems for primes in arithmetic progressions and for sifting functions*, J. Amer. Math. Soc. **4** (1991), 25-86.
[FG3] ———, *Limitations to the equi–distribution of primes III*, Comp. Math. **81** (1992), 19-32.
[FG4] ———, *Limitations to the equi–distribution of primes IV*, Proc. Royal Soc. A **435** (1991), 197-204.
[FG5] ———, *Relevance of the residue class to the abundance of primes*, Proc. Amalfi Conf. on Analytic Number Theory (E. Bombieri, A. Perelli, S. Salerno, U. Zannier, eds.), Salerno, Italy, 1993, pp. 95-104.
[FI] J.B. Friedlander and H. Iwaniec, *A note on character sums*, Contemp. Math. J **166** (1994), 295-299.
[Gal] P.X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math **11** (1970), 329–339.
[Ga2] ———, *On the distribution of primes in short intervals*, Mathematika **23** (1976), 4-9.
[Gol] Leo Goldmakher, *Character sums to smooth moduli are small* (to appear).
[GR] S.W. Graham and C.J. Ringrose, *Lower bounds for least quadratic non-residues*, Prog. Math **85** (1990), Birkhäuser, Boston, 269-309.
[Gr1] A. Granville, *Unexpected irregularities in the distribution of prime numbers,*, Proceedings of the International Congress of Mathematicians (1995), 388–399..
[Gr2] ———, *Harald Cramér and the distribution of prime numbers*, Act. J. Scand. **1** (1995), 12–28.
[Gr3] ———, *On integers, without large prime factors, in arithmetic progressions I*, Acta Mathematica **170** (1993), 255–273.
[Gr4] ———, *On integers, without large prime factors, in arithmetic progressions II Philosophical Transactions of the Royal Society* **345** *(1993), 349–362.*
[Gr5] ———, *Pretentiousness in analytic number theory* (to appear).
[Gr6] ———, *Smooth numbers: Computational number theory and beyond*, Proceedings, MSRI workshop, Berkeley 2000 (to appear).
[GM] A. Granville and G. Martin, *Prime Number Races*, Amer. Math. Monthly **113** (2006), 1–33.
[GS1] A. Granville and K. Soundararajan, *The Spectrum of Multiplicative Functions*, Ann. of Math **153** (2001), 407–470.
[GS2] ———, *Large Character Sums*, J. Amer. Math. Soc **14** (2001), 365–397.
[GS3] ———, *Upper bounds for* $|L(1,\chi)|$, Quarterly Journal of Mathematics, Oxford **53** (2002), 265–284.
[GS4] ———, *Decay of mean-values of multiplicative functions*, Canadian Journal of Mathematics **55** (2003) 1191–1230..
[GS5] ———, *Distribution of values of* $L(1,\chi_d)$, Geometric and Functional Analysis **13** (2003) 992–1028.
[GS6] ———, *The number of unsieved integers up to* x, Acta Arithmetica **115** (2004), 305–328..
[GS7] ———, *An uncertainty principle for arithmetic sequences*, Annals of Mathematics **165** (2007), 593–635..
[GS8] ———, *Large Character sums: pretentious characters and the Pólya-Vinogradov theorem*, J. Amer. Math. Soc. **20** (2007), 357–384.
[GS9] ———, *Extreme values of* $|\zeta(1+it)|$, Proceedings, Bangalore Conference, 2003.
[GS10] ———, *Negative values of truncations to* $L(1,\chi)$, "Analytic Number Theory: A Tribute to Gauss and Dirichlet" Clay Mathematics Proceedings, **7** (2007)..
[GS11] ———, *Pretentious multiplicative functions and an inequality for the zeta-function*, Proceedings, Anatomy of Integers workshop, Montreal 2006.
[GS12] ———, *Large Character Sums: pretentious characters, Burgess's theorem and the location of zeros* (to appear).
[GS13] ———, *Exponential sums with multiplicative coefficients* (to appear).
[Hal1] G. Halász, *On the distribution of additive and mean-values of multiplicative functions*, Stud. Sci. Math. Hungar **6** (1971), 211-233.
[Hal2] ———, *On the distribution of additive arithmetic functions*, Acta Arith. **27** (1975), 143-152.
[HR1] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.
[HR2] ———, *On a result of R. R. Hall*, J. Number Theory **11** (1979), 76-89.
[Hl1] R.R. Hall, *Halving an estimate obtained from Selberg's upper bound method*, Acta Arith **25** (1974), 347-351.

[Hl2] ———, *A sharp inequality of Halász type for the mean value of a multiplicative arithmetic function*, Mathematika **42** (1995), 144-157.
[HT] R.R. Hall and G. Tenenbaum, *Effective mean value estimates for complex multiplicative functions*, Math. Proc. Camb. Phil. Soc. **110** (1991), 337-351.
[Hi1] A. Hildebrand, *Fonctions multiplicatives et équations intégrales*, Séminaire de Théorie des Nombres de Paris, 1982-83 (M.-J. Bertin, ed.), Birkhäuser, 1984, pp. 115-124.
[Hi2] ———, *Quantitative mean value theorems for nonnegative multiplicative functions I*, J. London Math. Soc **30** (1984), 394-406-260.
[Hi3] ———, *A note on Burgess's character sum estimate*, C.R. Acad. Sci. Roy. Soc. Canada **8** (1986), 35-37.
[Hi4] ———, *Quantitative mean value theorems for nonnegative multiplicative functions II*, Acta Arith. **XLVIII** (1987), 209-260.
[HM] A. Hildebrand and H. Maier, *Irregularities in the distribution of primes in short intervals*, J. Reine Angew. Math. **397** (1989), 162-193.
[Iw] H. Iwaniec, *On zeros of Dirichlet's L-series*, Invent. math. **23** (1974), 97-104.
[IK] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer Math Soc, Providence, Rhode Island, 2004.
[Mai] H. Maier, *Primes in short intervals*, Michigan Math. J. **32** (1985), 221-225.
[Mon] H.L. Montgomery, *A note on the mean values of multiplicative functions*, Inst. Mittag-Leffler, (Report # 17).
[MV1] H.L. Montgomery and R.C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math **43** (1977), 69-82.
[MV2] ———, *On the distribution of reduced residues*, Annals of Math **123** (1986), 311–333.
[MV3] ———, *Mean-values of multiplicative functions*, Periodica Math. Hung. **43** (2001), 188-214.
[NP] M. Nair and A. Perelli, *On the prime ideal theorem and irregularities in the distribution of primes* (1994) (to appear).
[Nar] W. Narkiewicz, *The development of prime number theory (from Euclid to Hardy and Littlewood)*, Springer., 2000.
[Pal] R.E.A.C. Paley, *A theorem on characters*, J. London Math. Soc **7** (1932), 28-32.
[Pol] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Göttingen Nachrichten (1918), 21-29.
[Sl1] A. Selberg, *On the normal density of primes in small intervals and the difference between consecutive primes*, Arch. Math. Naturvid. J. **47** (1943), 87-105.
[Sl2] ———, *An elementary proof of the prime number theorem for arithmetic progressions*, Can. J. Math **2** (1950), 66-78.
[Shi] D.K.L. Shiu, *Strings of congruent primes*, J. London Math. Soc **61** (2000), 359–373.
[Ten] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics **46**, Cambridge University Press, Cambridge, 1995.
[Vin] I.M. Vinogradov, *Über die Verteilung der quadratischen Reste und Nichtreste*, J. Soc. Phys. Math. Univ. Permi **2** (1919), 1-14.
[Wrs] E. Wirsing, *Das asymptotische verhalten von Summen über multiplikative Funktionen II*, Acta Math. Acad. Sci. Hung. **18** (1967), 411-467.

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