

Different Approaches to the Distribution of Primes

Andrew Granville

Abstract. In this lecture celebrating the 150th anniversary of the seminal paper of Riemann, we discuss various approaches to interesting questions concerning the distribution of primes, including several *that do not involve the Riemann zeta-function*.

1. The prime number theorem, from the beginning

By studying tables of primes, Gauss understood, as a boy of 15 or 16 (in 1792 or 1793), that the primes occur with density $\frac{1}{\log x}$ at around x . In other words

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

The existing data lends support to Gauss's belief (see Table 1.1).

When we integrate by parts we find that a first approximation to $\text{Li}(x)$ is given by $x/(\log x)$ so we can formulate a guess for the number of primes up to x :

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1,$$

which we write as

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

I would like to thank the anonymous referee, Alex Kontorovich and Youness Lamzouri for their comments on an earlier draft of this article. L'auteur est partiellement soutenu par une bourse du Conseil de recherches en sciences naturelles et en génie du Canada.

x	$\pi(x) = \#\{\text{primes} \leq x\}$	Overcount: $[\text{Li}(x) - \pi(x)]$
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

TABLE 1.1. The number of primes up to various x .

This may also be formulated more elegantly by weighting each prime p with a $\log p$, to give

$$\sum_{p \leq x} \log p \sim x.$$

These equivalent estimates, known as the *Prime Number Theorem*, were all proved in 1896, by Hadamard and de la Vallée Poussin, following a program of study laid out almost forty years earlier by Riemann:¹

Riemann's idea was to use a formula of Perron to extend this last sum to be over all primes p , while picking out only those that are $\leq x$. The special case of Perron's formula that we need here is

$$\frac{1}{2i\pi} \int_{s: \text{Re}(s)=2} \frac{t^s}{s} ds = \begin{cases} 0 & \text{if } t < 1, \\ 1 & \text{if } t > 1, \end{cases}$$

¹One may make more precise guesses from the data in Table 1.1. For example one can see that the entries in the final column are always positive and are always about half the width of the entries in the middle column. So perhaps Gauss's guess is always an overcount by about \sqrt{x} ? This observation is, we now believe, both correct and incorrect, as we will discuss in what follows.

for positive real t . We apply this with $t = x/p$, when x is not itself a prime, which gives us a characteristic function for numbers $p < x$. Hence

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \text{ prime}}} \log p &= \sum_{p \text{ prime}} \log p \cdot \frac{1}{2i\pi} \int_{s: \operatorname{Re}(s)=2} \frac{(x/p)^s}{s} ds \\ &= \frac{1}{2i\pi} \int_{s: \operatorname{Re}(s)=2} \sum_{p \text{ prime}} \frac{\log p}{p^s} \frac{x^s}{s} ds. \end{aligned}$$

Here we were able to safely swap the infinite sum and the infinite integral since the terms are sufficiently convergent as $\operatorname{Re}(s) = 2$. The sum $\sum_p (\log p)/p^s$ is almost itself a recognizable function; that is, it is almost

$$\sum_{p \text{ prime}} \sum_{m \geq 1} \frac{\log p}{p^{ms}} = -\frac{\zeta'(s)}{\zeta(s)},$$

where

$$\zeta(s) := \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right). \quad (1.1)$$

So, by a minor alteration, one obtains the closed formula

$$\sum_{\substack{p \text{ prime} \\ p^m \leq x \\ m \geq 1}} \log p = -\frac{1}{2i\pi} \int_{s: \operatorname{Re}(s)=2} \frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} ds.$$

To evaluate this, Riemann proposed moving the contour from the line $\operatorname{Re}(s) = 2$, far to the left, and using the theory of residues to evaluate the integral. What a beautiful idea! However before one can possibly succeed with that plan one needs to know many things, for instance whether $\zeta(s)$ makes sense to the left, that is one needs an *analytic continuation* of $\zeta(s)$. Riemann was able to do this based on an extraordinary identity of Jacobi. Next, to use the residue theorem, one needs to be able to identify the poles of $\zeta'(s)/\zeta(s)$, that is the zeros and poles of $\zeta(s)$. The poles are not so hard, there is just the one, a simple pole at $s = 1$ with residue 1, so the contribution of that pole to the above formula is

$$-\lim_{s \rightarrow 1} (s-1) \frac{\zeta'(s)}{\zeta(s)} \frac{x^s}{s} = -\lim_{s \rightarrow 1} (s-1) \left(\frac{-1}{(s-1)} \right) \frac{x^1}{1} = x,$$

the expected main term. The locations of the zeros of $\zeta(s)$ are much more mysterious. Moreover, even if we do have some idea of where they are, in order to complete Riemann's plan, one needs to be able to bound the

contribution from the discarded contour when one moves the main line of integration to the left, and hence one needs bounds on $|\zeta(s)|$ throughout the plane. We do this in part by having a pretty good idea of how many zeros there are of $\zeta(s)$ up to a certain height, and there are many other details besides. These all had to be worked out (see, eg [13], for further details), after Riemann's initial plan – this is what took forty years! At the end, if all goes well, one has an approximation,

$$\sum_{p \leq x} \log p - x = - \sum_{\rho: \zeta(\rho)=0} \frac{x^\rho}{\rho} + \text{a bounded error.} \quad (1.2)$$

(One counts a zero with multiplicity m_ρ , m_ρ times in this sum). It became apparent, towards the end of the nineteenth century, that to prove the prime number theorem it was sufficient to prove that all of the zeros of $\zeta(s)$ lie to the left of the line $\operatorname{Re}(s) = 1$.² Riemann himself suggested that, more than that, all of the non-trivial zeros lie on the line $\operatorname{Re}(s) = \frac{1}{2}$,³ the so-called *Riemann Hypothesis*, which implies an especially strong form of the prime number theorem, using (1.2), that

$$\left| \sum_{p \leq x} \log p - x \right| \leq 2\sqrt{x} \log^2 x,$$

for $x \geq 100$, or, equivalently,⁴

$$|\pi(x) - \operatorname{Li}(x)| \leq 3\sqrt{x} \log x.$$

This reflects what we observed from the data in Table 1.1, that the difference should be this small; and what an extraordinary way to prove it, seemingly so far removed from counting the primes themselves. Is it really *necessary* to go to the theory of complex functions to count primes? And to work there with the zeros of an analytic continuation of a function, not even the function itself? This was something that was hard to swallow in the 19th century but gradually people came to believe it, seeing in (1.2) an equivalence, more-or-less, between questions about the distribution of primes and questions about the distribution of zeros of $\zeta(s)$. This is discussed in the introduction of Ingham's book [42]: “*Every known proof of the prime number theorem is based on a certain property of the complex*

²That there are none to the right is trivial, using the Euler product in (1.1).

³The “trivial zeros” lie at $s = -2, -4, -6, \dots$

⁴But not trivially equivalent.

zeros of $\zeta(s)$, and this conversely is a simple consequence of the prime number theorem itself. It seems therefore clear that this property must be used (explicitly or implicitly) in any proof based on $\zeta(s)$, and it is not easy to see how this is to be done if we take account only of real values of s . For these reasons, it was long believed that it was impossible to give an elementary proof of the prime number theorem.

Riemann remarked in a letter to Goldschmidt that

$$\pi(x) < \text{Li}(x) \tag{1.3}$$

for all $x < 3 \times 10^6$; and (1.3) is now known to be true for all $x < 10^{23}$ (as one might surmise from the data above). One might guess that this is always so but, in 1914, Littlewood [49] showed that this is not the case, proving that $\pi(x) - \text{Li}(x)$ infinitely often changes sign. Since (1.3) holds (easily) as far as we can compute primes, we might ask, in light of Littlewood's result, whether we can predict when $\pi(x) - \text{Li}(x)$ is first non-negative? A few years ago, Bays and Hudson [5] used the first million zeros, in an analogy to (1.2) for $\pi(x) - \text{Li}(x)$, to predict that the smallest x for which $\pi(x) > \text{Li}(x)$ is around 1.3982×10^{316} . In fact they can prove something like this as an upper bound on the smallest such x , but no-one knows how to use this method to get a lower bound since, to do so, one would need to rule out the extraordinary possibility of a conspiracy of high zeros. These issues are discussed in more detail in [32].

Let $\pi(x; q, a)$ denote the number of primes $\leq x$ that are $\equiv a \pmod{q}$. A proof analogous to that proposed by Riemann, reveals that if $(a, q) = 1$ then

$$\pi(x; q, a) \sim \frac{\pi(x)}{\phi(q)}, \tag{1.4}$$

once x is sufficiently large. However in many application one wants to know just how large x needs to be for the primes to be equi-distributed in arithmetic progressions mod q . Calculations reveal that the primes up to x are equi-distributed amongst the arithmetic progressions mod q , once x is just a tiny bit larger than q , say $x \geq q^{1+\delta}$ for any fixed $\delta > 0$ (once q is sufficiently large). However the best proven results have x bigger than the exponential of a power of q , far larger than what we expect. If we are prepared to assume the unproven *Generalized Riemann Hypothesis* we do much better, being able to prove that the primes up to $q^{2+\delta}$ are equally distributed amongst the arithmetic progressions mod q , for q sufficiently large, though notice that this is still somewhat larger than what we expect to be true.

So what are the consequences if (1.4) does not hold until x is bigger than the exponential of a power of q ? For one thing one can then deduce that the Generalized Riemann Hypothesis is false but, as we shall see, there are other easier to understand, and more elementary, consequences. We shall return to this a little later.

2. Selberg's formula

It is not difficult to show that the prime number theorem implies that

$$\log x \sum_{\substack{p \leq x \\ p \text{ prime}}} \log p + \sum_{\substack{p_1 p_2 \leq x \\ p_1 < p_2 \text{ both prime}}} \log p_1 \log p_2 \sim 2x \log x. \quad (2.1)$$

(We call an integer which is either a prime p , or the product of two primes, $p_1 p_2$, a “P2”.) Selberg [57] gave an elementary proof that (2.1) is true using sieve methods, and then Erdős [17, 18] was able to deduce the prime number theorem from (2.1),⁵ contrary to the aforementioned beliefs of Ingham and others.⁶ How can a formula like (2.1) hold without any hint of the zeros of $\zeta(s)$? Well, as a consequence of (1.2) one can show that

$$\frac{1}{\log x} \sum_{\substack{p_1 p_2 \leq x \\ p_1 < p_2 \text{ both prime}}} \log p_1 \log p_2 - x = \sum_{\rho: \zeta(\rho)=0} \frac{x^\rho}{\rho} + \text{small error},$$

and when we add this to (1.2) we get (2.1), the contribution of the zeros canceling.

There is also an analogous formula for primes in arithmetic progressions:

$$\log x \sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \log p + \sum_{\substack{p_1 p_2 \leq x \\ p_1 p_2 \equiv a \pmod{q}}} \log p_1 \log p_2 \sim \frac{2x \log x}{\phi(q)}, \quad (2.2)$$

which holds for each $(a, q) = 1$ for all suitably large values of x . This formed the start of Selberg's elementary proof [59] of the prime number theorem for

⁵There is a considerable controversy as to whether Erdős behaved appropriately in quickly deducing the prime number theorem upon hearing of Selberg's formula. My view is that the controversy reflects two different perspectives on what is appropriate when one hears about the latest research of others, and what is not. For more on the controversy, you can read Selberg's own words [2], or accounts by Goldfeld [26], or by Strauss [64] who was caught up in the controversy at the time.

⁶Though see Ingham's Math Review [43] of Selberg's and Erdős's papers for a thorough explanation of the ideas in the elementary proof.

arithmetic progressions. Selberg's proof implies that (2.2) holds for $x \geq e^q$.⁷ So what happens if (1.4) fails to be true (for q , and for no smaller modulus)? It is then not hard to deduce from (2.2) that the distribution of primes mod q depends on their quadratic character mod q . That is, one can show that almost all primes congregate in the arithmetic progressions $a \pmod{q}$ for which $\left(\frac{a}{q}\right) = -1$, or more precisely:

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} \log p = \begin{cases} \{2 + o(1)\} \frac{x}{\phi(q)} & \text{if } \left(\frac{a}{q}\right) = -1; \\ o\left(\frac{x}{\phi(q)}\right) & \text{if } \left(\frac{a}{q}\right) = 1. \end{cases}$$

In other words, almost all primes p up to this point satisfy $\left(\frac{p}{q}\right) = -1$. But then how can (2.2) be true? Well if most $\left(\frac{p}{q}\right) = -1$ then most $\left(\frac{p_1 p_2}{q}\right) = (-1) \times (-1) = 1$, so we find that

$$\frac{1}{\log x} \sum_{\substack{p_1 p_2 \leq x \\ p_1 p_2 \equiv a \pmod{q}}} \log p_1 \log p_2 = \begin{cases} o\left(\frac{x}{\phi(q)}\right) & \text{if } \left(\frac{a}{q}\right) = -1; \\ \{2 + o(1)\} \frac{x}{\phi(q)} & \text{if } \left(\frac{a}{q}\right) = 1. \end{cases}$$

Thus Selberg's formula (2.2) follows by adding together the last two displayed equations. We see that Selberg's formula (2.2) somehow takes account of the possibility of this, the only feasible rogue behaviour — amazing! Note though that this case cannot be true for all x , else $L\left(1, \left(\frac{\cdot}{q}\right)\right) = 0$ (since $\left(\frac{p}{q}\right) = -1$ for most primes if this held for all x) which we know to be untrue thanks to Dirichlet. In fact Dirichlet's class number formula implies that $L\left(1, \left(\frac{\cdot}{q}\right)\right) \gg 1/\sqrt{q}$, and so (1.4) cannot fail for x bigger than $e^{\sqrt{q}}$.⁸

This discussion is still quite deep and analytic — after all what else is $L\left(1, \left(\frac{\cdot}{q}\right)\right)$ but a special value of a function defined by an infinite sum?⁹ However we can show that x needs to be very large for (1.4) to hold, without infinite series, if the class number of the quadratic field $\mathbb{Q}(\sqrt{-q})$ is small. To do so, we follow an argument of Ankeny and Chowla [1]: We consider

⁷In 1981 Friedlander [19] showed that (2.2) holds for all $x \geq q^B$ as $B \rightarrow \infty$, using sieve methods.

⁸So long as (2.2) is valid in the wide range given by Friedlander [59].

⁹Though in this case, the definition of $L(s, (\cdot/q))$ is valid for all s to the right of $\text{Re}(s) = 0$, where we sum $\chi(n)/n^s$ in the natural order of ascending integer n -values.

the binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $-q = b^2 - 4ac$.¹⁰ Two forms are said to be $\mathrm{SL}(2, \mathbb{Z})$ -equivalent if there is a transformation from one to the other by making the substitution $\begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$ where $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$. Gauss's work implies that in each $\mathrm{SL}(2, \mathbb{Z})$ -equivalence class there is an unique reduced form,¹¹ and that there are only finitely many; we denote the number of classes by $h(-q)$. If p is a prime for which $\left(\frac{p}{q}\right) = 1$ then there are a total of two representations of p as the value of a reduced binary quadratic form of discriminant $-q$. If $N \geq q$ then there are $\ll N/\sqrt{q}$ values $\leq N$ taken by each binary quadratic form of discriminant $-q$, and so

$$\begin{aligned} \#\left\{p \leq N : \left(\frac{p}{q}\right) = 1\right\} &\leq \frac{1}{2} \sum_{f \text{ reduced}} \#\{m, n \in \mathbb{Z} : f(m, n) \leq N\} \\ &\ll h(-q) \frac{N}{\sqrt{q}}. \end{aligned}$$

Therefore if a positive proportion of the primes up to N satisfy $\left(\frac{p}{q}\right) = 1$ then we deduce that

$$N \gg e^{c\sqrt{q}/h(-q)}$$

for some constant $c > 0$. In particular if $h(-q) \leq q^{1/2-\epsilon}$ then $N \gg e^{q^\epsilon}$. Moreover if we know that a positive proportion of the primes up to q^2 satisfy $\left(\frac{p}{q}\right) = 1$ then $h(-q) \gg \sqrt{q}/\log q$.

3. Primes in Arithmetic Progressions, without L -functions

Selberg [58] proved (1.4), the prime number theorem for arithmetic progressions, based on his formula (2.1). His proof (easily) yields the result for $x > e^{cq}$, and with Friedlander's improved range of validity [19], one can

¹⁰The classical theory of Gauss and Dirichlet tells us that there is a 1-to-1 correspondence between the binary quadratic forms $ax^2 + bxy + cy^2$ and the ideals $(2a, -b + \sqrt{-q})$. We shall discuss things here in the language of quadratic forms but there is an equivalent theory of ideals.

¹¹ $ax^2 + bxy + cy^2$ is *reduced* if $-a < b \leq a \leq c$, and if $b \geq 0$ when $a = c$.

deduce (1.4) when $x > e^{c\sqrt{q}}$. It is unlikely that one can do much better directly without gaining some understanding of the class number of $\mathbb{Q}(\sqrt{-q})$. Indeed, as we discussed just above, if (1.4) is true then $x \gg e^{c\sqrt{q}/h(-q)}$.

Let us suppose for now that $h(-q) \gg \sqrt{q}/\log q$.¹² In this case there are now two elementary proofs that

$$\pi(x; q, a) = \{1 + o_{u \rightarrow \infty}(1)\} \frac{\pi(x)}{\phi(q)} \quad \text{where } x = q^u, \quad (3.1)$$

for any $(a, q) = 1$. That is (1.4) holds for $x = q^u$ as $u \rightarrow \infty$, and in particular one can deduce that there exists a constant $A > 0$ such that there is a prime $\ll q^A$ in every arithmetic progression $a \pmod{q}$ with $(a, q) = 1$.¹³ The most recent such proof, to appear in a forthcoming book of Friedlander and Iwaniec [22], uses elementary but difficult small sieve methods. The first elementary proof, due to Elliott [14] (and strengthened in [4]), is based on the *pretentious large sieve* which implies that there exists a character $\chi \pmod{q}$ such that if $x = q^u \geq q^{1+\delta}$ then

$$\pi(x; q, a) = \frac{\pi(x)}{\phi(q)} + \frac{\chi(a)}{\phi(q)} \sum_{p \leq x} \bar{\chi}(p) + o_{u \rightarrow \infty} \left(\frac{\pi(x)}{\phi(q)} \right); \quad (3.2)$$

and we may remove the χ term unless χ is a real-valued character. This fails to imply (3.1) if and only if $\chi(p)$ is not equally often 1 and -1 as we run through the primes p up to x .

The key idea in proving (3.2) is that $\sum_{rs=n} \mu(r) \log s$ equals 0 unless n is a power of some prime p , in which case it equals $\log p$. Hence counting primes up to x that are $\equiv a \pmod{q}$ is equivalent to estimating $\sum_{rs \leq x, rs \equiv a \pmod{q}} \mu(r) \log s$, and since \log is such a smooth function, this is equivalent to showing that $\mu(r)$ is $o(1)$ on average as r runs through any arithmetic progression \pmod{q} (see section 2.1 of [46] for more details on this equivalence).

It turns out that the $\sum_{p \leq x} \bar{\chi}(p)$ term is large in (3.2) if and only if $\chi(p) = \mu(p)$ for “almost all” primes $p \leq x$. The “pretentious methods” in the proof of (3.2) do not use, at all, the fact that $\mu(p) = -1$ for all primes p . In fact the only assumption is that μ is an example of a multiplicative function f such that $|f(n)| \leq 1$ for all $n \geq 1$. In this generality one can

¹²As is believed, and as certainly follows from the Generalized Riemann Hypothesis.

¹³When using zeros of L -functions this is a tough thing to prove since one needs various difficult explicit estimates. Linnik’s original proof [48] (see also [7]) is a tour-de-force.

show that for a given x , and for all $q \leq Q = x^{1/u}$, we either have

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} f(n) = o_{u \rightarrow \infty} \left(\frac{x}{q} \right)$$

whenever $(a, q) = 1$, or there exists a primitive character χ of conductor r such that in the cases where $r|q$ we have

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} f(n) = \frac{\chi(a)}{\phi(q)} \sum_{\substack{n \leq x \\ (n, q) = 1}} f(n) \overline{\chi(n)} + o_{u \rightarrow \infty} \left(\frac{x}{q} \right)$$

whenever $(a, q) = 1$. This theorem, first proved for μ by Gallagher [23] though in the language of prime counting, has long been considered to lie deep and to be intimately connected with the distribution of zeros of Dirichlet L -functions. The generality of the new result suggests that this cannot be so deep (indeed it can be proved using only elementary methods). Although we do not believe that this exceptional character χ exists for μ , it does exist for certain f , for example if we take $f = \chi$, so the effect of a putative exceptional character certainly needs to be accounted for in any theorem of this generality about the distribution of multiplicative functions in arithmetic progressions.

It remains to give a proof of (1.4), or something like it, in the case that $h(-q)$ is small, that is $h(-q) \ll \sqrt{q}/\log q$. From what we noted above, (1.4) cannot hold unless $N \gg e^{c\sqrt{q}/h(-q)}$, which will be surprisingly large in this case. In the proofs involving zeros of L -functions one gets an explicit formula, in this case, of the shape

$$\pi(x; q, a) = \frac{1}{\phi(q)} \frac{x - \overline{\chi}(a) \frac{x^\beta}{\beta}}{\log x} \{1 + o_{u \rightarrow \infty}(1)\}, \tag{3.3}$$

where β is a real zero of $L(s, \chi)$ that is close to 1. This will be large unless $\chi(a) = 1$. In this case if $u \rightarrow \infty$ but is not too large (that is $u(1 - \beta) \log q = o(1)$) then the main term becomes

$$\sim \frac{x - x^\beta}{\phi(q) \log x} \sim \frac{(1 - \beta)x}{\phi(q)},$$

which is not the same as (1.4), though it does provide a lower bound for $\pi(x; q, a)$ in this case. Note that we obtain (1.4) from (3.3) when $u(1 - \beta) \log q \rightarrow \infty$.

Without using of zeros of L -functions we can prove something similar by reverting to the theory of binary quadratic forms of discriminant $-q$:

If $p|f(m, n)$ where $\chi(p) = -1$ then $p|(m, n)$. If $p|f(m, n)$ where $\chi(p) = 1$ then the ratio $m : n \pmod{p}$ lies in two of the $p + 1$ possibilities. Hence if there are surprisingly few primes p with $\chi(p) = 1$ we can use the small sieve on the values of the binary quadratic form that are $\equiv a \pmod{q}$. In this way we prove that there are $\sim \kappa N$ prime values of the quadratic form up to N which are $\equiv a \pmod{q}$, for some constant $\kappa > 0$, and so complete the proof of Linnik's theorem.¹⁴ From Gauss's theory, we know that each prime with $\chi(p) = 1$ is represented exactly twice in total over all the reduced binary quadratic forms of discriminant $-q$, and so we can deduce, now in an elementary manner, that $\pi(x; q, a) \sim \kappa' x / \phi(q)$, for some constant $\kappa' > 0$, provided $u \rightarrow \infty$ and is not too large. Hence $1 - \beta \sim \kappa'$ where κ' is derived as a sieving constant. This allows us to recover a version of the result of Goldfeld [25].

It is still an open question whether one can recover precisely the formula (3.3) by elementary means, though I showed in [28], starting now from (2.2), that the transition between when $\pi(x; q, a)$ looks like $\kappa' x / \phi(q)$, and when it looks like $\pi(x) / \phi(q)$, is more-or-less exponential, that is there exist constants $0 < \beta_-, \beta_+ < 1$ such that

$$\frac{x^{\beta_-}}{\beta_-} \ll x - \phi(q)\pi(x; q, a) \log x \ll \frac{x^{\beta_+}}{\beta_+}.$$

4. Primes in Short Intervals

Riemann's approach gives a good way to determine the number of primes up to x , but Gauss was looking for primes in intervals around x . So we can ask whether we can estimate the number of primes in intervals $[x, x + y]$? The Riemann Hypothesis allows us to find the number of primes in intervals with $y \geq \sqrt{x} \log x$. If we add in some plausible hypotheses about the vertical distribution of the zeros of $\zeta(s)$ then we can improve this [39] to $y \geq \epsilon \sqrt{x \log x}$, but we know of no approach to prove that there are primes in all intervals $[x, x + \sqrt{x}]$. The outstanding question in this area, which beautifully highlights our ignorance, asks

Is there a prime in the interval
 $(n^2, (n + 1)^2)$
for all integers $n \geq 1$?

¹⁴The elementary proofs given for this case in [14, 22] can be interpreted as sieving on the union, counting multiplicities, of the set of values of all reduced binary quadratic forms of discriminant $-q$.

If we cannot prove something like this for all intervals, maybe we can show that there are primes in “almost all” short intervals? This was accomplished by Selberg [57] in 1949, proving that

$$\pi(x+y) - \pi(x) \sim \frac{y}{\log x} \quad (4.1)$$

when $y = y(x) > (\log x)^{2+\epsilon}$, for almost all x . It was believed that this would surely be true for all x , a belief supported by a widely quoted heuristic of Cramér [12]. However this is *not true*. In 1984, Maier [50] gave a delightful sieve theory argument to show that for any constant $A > 2$ there exists a constant $\delta_A > 0$ such that there are arbitrarily large integers x and X for which

$$\begin{aligned} \pi(x + \log^A x) - \pi(x) &\geq (1 + \delta_A) \log^{A-1} x, \text{ and} \\ \pi(X + \log^A X) - \pi(X) &\leq (1 - \delta_A) \log^{A-1} X. \end{aligned}$$

This type of poor distribution result is true for all “arithmetic sequences” [33].

Cramér’s heuristic (see [29] for a discussion, and [53] for a different perspective) led him to conjecture that there is always a prime in the interval $[x, x + \{1 + o(1)\} \log^2 x]$. More precisely, if $p_1 = 2, p_2 = 3, \dots$ is the sequence of primes then

$$\limsup_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\log^2 p_n} = 1.$$

The latest best data is as follows:

p_n	$p_{n+1} - p_n$	$(p_{n+1} - p_n) / \log^2 p_n$
113	14	.6264
1327	34	.6576
31397	72	.6715
370261	112	.6812
2010733	148	.7026
20831323	210	.7395
25056082087	456	.7953
2614941710599	652	.7975
19581334192423	766	.8178
218209405436543	906	.8311
1693182318746371	1132	.9206

TABLE 4.1. (Known) record-breaking gaps between primes.

Evidently the record-breaking values in the last column are slowly creeping upwards but will they ever reach 1? Based on Maier's ideas, I showed [29] that Cramér's heuristic should be modified to conjecture an even bigger constant, that

$$\limsup_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\log^2 p_n} \geq 2e^{-\gamma} \approx 1.1229 \dots$$

It is hard to conclude from the data which conjecture is correct, if either.

5. Sieve methods

I have mentioned sieve methods several times already without properly saying what they are. They all derive from the sieve of Eratosthenes: In the sieve of Eratosthenes one deletes every second integer up to x after 2, then keeps the first undeleted integer > 2 , which is 3, and then deletes every third integer up to x after 3, then keeps the first undeleted integer > 3 , which is 5, and then deletes every fifth integer up to x after 5, etc. This leaves the primes up to x and suggests a way to guess at how many there are: After sieving by 2 one is left with roughly half the integers up to x ; after sieving by 3, one is left with roughly two-thirds of those that had remained and continuing like this we expect to have about

$$x \prod_{p \leq y} \left(1 - \frac{1}{p}\right)$$

integers left by the time we have sieved with all the primes up to y . Once $y = \sqrt{x}$ the undeleted integers are 1 and the primes up to x , since every composite has a prime factor no bigger than its square-root. However this does not turn out to be such a good approximation for the number of primes up to x when $y = \sqrt{x}$, because the heuristic was based on an assumption of independence of divisibility by different primes, that is divisibility by $d = p_1 p_2 \dots p_k$, which is not exactly correct (as is clear when we take $d > x$). To be more precise, the error term in our approximation is something like $2^{\pi(y)}$, which is enormous for the sort of y -values that we are talking about. To make such a method useful it needs to be modified so that the effect of large divisors d is less pronounced.

The first successful approach, a clever version of “the principle of inclusion-exclusion”, was initially developed by Brun, and led to his famous proof that

$$\sum_{p, p+2 \text{ both prime}} \frac{1}{p} < \infty.$$

Brun’s method was used in many interesting ways by Paul Erdős, and the theory was significantly developed by Rosser, and more recently by Iwaniec, e.g., [45].

The other key modification is due to Selberg [60]–[63], who introduced various general weights and clever identities to reduce the effect of the large d . Selberg formulated sieve problems with abstract hypotheses, allowing him to remove the number theory so as to completely resolve the abstract problem using the “calculus of variations”. This has the great benefit that such problems can be completely solved, but has the disadvantage of being somewhat removed from the original number theory problems, and indeed only attack a restricted class of questions. For example, Selberg’s methods cannot distinguish between integers with an even or odd number of prime factors, the so-called “parity problem”. (This can be seen in Selberg’s identity (2.1) which counts P^2 ’s, the number of integers with *at most* two prime factors). This issue has been largely misunderstood in the literature — if one reformulates Selberg’s sieve hypotheses then one might be able to overcome this difficulty, though too many people have mistaken this to mean that such problems cannot be overcome by sieve methods.

Iwaniec [44] was the first to circumvent these issues so as to use sieve methods to show that there are infinitely many primes in an interesting infinite sequence, namely the integers represented by any given two variable polynomial where every monomial has degree ≤ 2 . We will discuss other more recent work of this type, a little later.

6. Gaps between primes

The number $n! + k$ is divisible by k whenever $1 \leq k \leq n$, and so each of $n!+2, n!+3, \dots, n!+n$ is composite. Hence if p_r is the largest prime $\leq n!+1$ then $p_{r+1} \geq n! + n + 1$ and so $p_{r+1} - p_r \geq n$. Therefore $\limsup_{r \rightarrow \infty} p_{r+1} - p_r = \infty$. This proof can be found in many elementary textbooks, and if we use Stirling’s formula to recall that $\log n! \sim n \log n$ then this proof gives $p_{r+1} - p_r \gtrsim \log p_r / \log \log p_r$. We can do a little better quantitatively by

replacing $n!$ with $\prod_{p \leq n} p$ and using much the same argument to obtain $p_{r+1} - p_r \gtrsim \log p_r$.

With the prime number theorem we can also obtain this, the largest gap being at least as big as the average:

$$\max_{p_r \leq x} (p_{r+1} - p_r) \geq \frac{1}{\pi(x)} \sum_{p_r \leq x} (p_{r+1} - p_r) \geq \frac{p_{R+1} - 2}{\pi(x)} \geq \frac{x - 1}{\pi(x)} \sim \log x,$$

where p_R is the largest prime $\leq x$. So next one might ask whether gaps between primes get significantly larger; for example, is it true that

$$\limsup_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\log p_n} = \infty ?$$

In 1931 Westzynthuis [65] proved this using a slightly more sophisticated version of our argument above, and his argument has been gradually improved until now [16, 52] we know that there are infinitely many n such that

$$p_{n+1} - p_n \gtrsim 2e^\gamma \log p_n \frac{\log \log p_n}{(\log \log \log p_n)^2} \log \log \log \log p_n. \quad (6.1)$$

The constant in front, $2e^\gamma$, is the culmination of many improvements appearing in a series of papers over the last 70 years; Erdős long ago offered ten thousand dollars to anyone who could show that one can take an arbitrarily large constant here, his most lucrative prize.¹⁵

We believe that there are infinitely many twin primes, that is prime pairs $p, p + 2$, but we seem to be far from proving that. The smallest gaps between primes around x are obviously smaller than the average, that is

$$\min_{x < p_r \leq 2x} (p_{r+1} - p_r) \lesssim \log x,$$

and we might ask whether we can prove that

$$\liminf_{n \rightarrow \infty} \frac{p_{n+1} - p_n}{\log p_n} = 0 ? \quad (6.2)$$

(the average result gives that this is ≤ 1 .) This question inspired Bombieri and Davenport [6] to develop the large sieve yet for all their extraordinary ingenuity they simply improved the upper bound to $\leq .466\dots$ ¹⁶ Subsequent work by Huxley [41] and Maier [51] improved this to just a little better than $\leq \frac{1}{4}$.

¹⁵Given Cramér's conjecture, we believe that far more is true, but the complicated function on the right side of (6.1) seems to be the limit of *this* method.

¹⁶Of course, this work of Bombieri and Davenport has had a big impact on so many important questions!

The general belief was that this is a tough question that would not succumb to a simple proof so it came as rather a shock when, in 2009, Goldston, Pintz and Yildirim [27] proved (6.2) using a simple variant of the Selberg sieve. This was especially surprising as they used their sieve method to identify primes, yet the “parity principle” seemed to suggest that this was impossible with Selberg’s method. However, as we explained above, this misbelief stems from a mis-conception of the precise formulation of Selberg’s sieve method.

More recently, Goldston, Pintz and Yildirim, together with Sid Graham, have also gone beyond Selberg’s methods by proving many things about the distribution of integers with *exactly* two prime factors, rather than P2s (which are the integers with *at most* two prime factors).

Goldston, Pintz and Yildirim not only proved (6.2) but developed an approach that, perhaps for the first time, makes one feel that the twin prime conjecture can perhaps be tackled by current methods: They prove that if (1.4) holds for all $(a, q) = 1$ whenever $x \geq q^{1.05}$ then there are infinitely many p_n such that

$$p_{n+1} - p_n \leq 16.$$

In fact one deduce this under the weaker assumption that (1.4) holds for “almost all” q in this range.

7. The asymptotic sieve

Selberg’s parity principle implies that it is difficult to use sieve methods to identify primes; somehow one has to circumvent the issues identified by Selberg. It was Bombieri [8] who suggested an “asymptotic sieve” that would do so, provided certain additional hypotheses are satisfied. Developing Bombieri’s idea [21] led Friedlander and Iwaniec in 1998 to show that there are infinitely many primes of the form $m^2 + n^4$ [20]. Subsequently Heath-Brown and Moroz [40] showed that for any irreducible binary cubic form $f(x, y) \in \mathbb{Z}[x, y]$ with no fixed divisor, there are infinitely many pairs of integers m, n such that $f(m, n)$ is prime. Stunning!

The most desired open problem in this area is to show that

$$4a^3 + 27b^2$$

is prime for infinitely many pairs of integers a, b (this is of interest because if $4a^3 + 27b^2$ is prime then it is usually the conductor of the elliptic curve $y^2 = x^3 + ax + b$).

8. Primes in what (polynomial) sequences ?

One can ask many questions of this type:

- Are there infinitely many pairs of twin primes $p, p + 2$?
- How about primes of the form $n^2 + 1$?
- Is it true that for any integer $N \geq 3$ there is a pair of primes $p, 2N - p$?
- Are there infinitely many pairs of *Sophie Germain* twin primes $p, 2p+1$?
- Are there infinitely many primes of the form $a^2+b^3+c^5$? Or $4a^3+27b^2$?

We believe we know the answer to all of these questions and any questions like this. To state the general conjecture we must first see when there are only finitely many primes in such sequences. For example there can only be finitely many pairs of primes $p, p + 1$ because one of these must be even, similarly there can only be finitely many triples of primes $p, p + 2, p + 10$ because one of these must be divisible by 3. Another good example is $n^2 - 3n + 4$, which is always even. So we have to avoid these *local* difficulties; and the conjecture is that if we can then we have infinitely many tuples of such primes. To be more precise, suppose that $f_1, f_2, \dots, f_k \in \mathbb{Z}[x_1, \dots, x_n]$ are all irreducible, and that there is no fixed prime divisor of $f_1 f_2 \dots f_k$ (that is, for any prime p , one can substitute in integer values for the variables so that the product is not divisible by p). Then we call our set of polynomials *admissible*, and conjecture that there are infinitely n -tuples of integers a_1, a_2, \dots, a_n such that

$$f_j(a_1, a_2, \dots, a_n) \text{ is prime for each } j \text{ in the range } 1 \leq j \leq k.$$

The only cases in which unconditional results have been proven, have all of the f_j linear. For example it has long been known that there are infinitely many triples of primes in arithmetic progression, which corresponds to the triple of polynomials $x, x + y, x + 2y$. A little more complicated is the lovely example due to Balog [3], of a 3-by-3 array of primes, with each row and column in arithmetic progression, that is that there are infinitely many simultaneous prime values of the nine polynomials

$$\begin{array}{ccc} x, & x + y, & x + 2y, \\ x + z, & x + w, & x + 2w - z, \\ x + 2z, & x + 2w - y, & x + 4w - 2z - 2y; \end{array}$$

(notice that each row and each column is a three term arithmetic progression), for example forming the two dimensional 3-by-3 array of primes,

11	17	23
59	53	47
107	89	71

He also showed that there are infinitely many three dimensional 3-by-3-by-3 arrays of primes in arithmetic progression such as

47	383	719	149	401	653	251	419	587
179	431	683	173	347	521	167	263	359
311	479	647	197	293	389	83	107	131

(Here each row and each column of each 3-by-3 square, which is a layer of the 3-by-3-by-3 Balog cube, is an arithmetic progression of primes, and also the (i, j) th elements of each of the three 3-by-3 squares form an arithmetic progression of primes for each fixed $1 \leq i, j \leq 3$: for example, for $i = 1, j = 3$ we have 719, 653, and 587.) and even with an arbitrary number of dimensions.

For many years there did not seem to be methods to go further than three term arithmetic progressions of primes. That all changed with the seminal paper of Green and Tao [34] in 2008 when they showed that there are infinitely many k -term arithmetic progressions of primes and much else besides. One of my favorite consequences (see [31] for this and more) is a neatening up of Balog's theorem, so that the 3-by-3 array can be taken to be the polynomials $x + iy + jz$, $0 \leq i, j \leq 2$ such as

5	17	29		29	41	53
47	59	71		59	71	83
89	101	113	and	89	101	113

Moreover one can extend the length of the sides to be length 4, such as

503	1721	2939	4157
863	2081	3299	4517
1223	2441	3659	4877
1583	2801	4019	5237

and even to be of arbitrary side length N , as well as an arbitrary number of dimensions D , for any $N, D \geq 2$.

Legendre observed that the polynomial $X^2 + X + 41$ is prime for $X = 0, 1, 2, \dots, 39$, and although no polynomial can always be prime, one can ask whether there are quadratic polynomials whose first N values are prime. This indeed follows from the work of Green and Tao, though not (yet) for a monic quadratic polynomial.

Green and Tao have also proposed a program [34]–[36] to prove a large chunk of the conjecture for linear polynomials: If their program works out then we will know that any set of admissible linear polynomials, such that no two are linearly dependent over the integers,¹⁷ simultaneously take on prime values infinitely often.

9. A strange polynomial

There is one *reducible* polynomial worth mentioning in this context, namely

$$\begin{aligned}
 F(a, b, \dots, z) := & (k+2) \times \left(1 - (n+l+v-y)^2 - (2n+p+q+z-e)^2 \right. \\
 & - (16(k+1)^3(k+2)(n+1)^2 + 1 - f^2)^2 \\
 & - ((gk+2g+k+1)(h+j) + h-z)^2 \\
 & - (z+pl(a-p) + t(2ap-p^2-1) - pm)^2 \\
 & - (p+l(a-n-1) + b(2an+2a-n^2-2n-2) - m)^2 \\
 & - (wz+h+j-q)^2 - (q+y(a-p-1) \\
 & + s(2ap+2a-p^2-2p-2) - x)^2 - (ai+k+1-l-i)^2 \\
 & - ((a^2-1)l^2 + 1 - m^2)^2 - ((a^2-1)y^2 + 1 - x^2)^2 \\
 & - (e^3(e+2)(a+1)^2 + 1 - o^2)^2 - (16r^2y^4(a^2-1) + 1 - u^2)^2 \\
 & \left. - (((a+u^2(u^2-a))^2 - 1)(n+4dy)^2 + 1 - (x+cu)^2)^2 \right),
 \end{aligned}$$

constructed by several logicians [47] based on ideas of Matijasevic. This polynomial has the remarkable property that, although it is not often positive, when it is, it is prime valued, and every prime is a value of the polynomial. However, from my perspective the polynomial is an artificial construct, indeed it is even reducible, so it is hard to see how this could be of much use to someone exploring the analytic properties of primes, but you have to admire its beauty!

10. Fast growing sequences

- Are there infinitely many primes of the form $2^n - 1$?

¹⁷That is, satisfying a linear equation $af_i + bf_j = c$, with $a, b, c \in \mathbb{Z}$.

- Are there infinitely many primes of the form $2^n + 1$?
- How about numbers of the form 1111...1111, that is of the form $(10^n - 1)/9$?
- Are there infinitely many Fibonacci primes F_n , the n th Fibonacci number?

These are all examples of sequences that grow exponentially fast and we really don't know what to expect. In the first case, Father Mersenne showed that if $2^n - 1$ is prime then n is prime, and the participants of Great Internet Mersenne Prime Search (GIMPS) continue to identify primes of this sort. In the second case one can show that if $2^n + 1$ is prime then n is a power of 2. The first five elements of this sequence are prime, and Fermat conjectured that they all are, but Euler showed that that is false; in fact no other primes have been identified in this sequence.

Despite not even knowing how to conjecture the right answer in these cases of exponential growth, there has been spectacular progress recently for other types of sequences that grow very fast. Indeed Bourgain, Gamburd and Sarnak [9, 10] consider the co-ordinates of points under the action of matrices generated by words constructed from a finite set of matrices. In this case it is not so clear how to order the points (in that there are several candidates) so, instead, if the points lie on a variety, their goal is to show that points with prime co-ordinates are Zariski dense on that variety. At the moment, they have some beautiful results for certain expanders, showing that points whose co-ordinates have a bounded number of prime factors are indeed Zariski dense. The key inputs come from the theory of expanders and from sieve methods.

Take any three touching circles each with rational radii r_j . Then select the smallest positive integer m such that each m/r_j is an integer, and call that the *curvature*. In certain cases the largest circle that can be inscribed in the "lune" in-between the three given circles also has integer curvature. Then one can inscribe a largest circle in each of the resulting four lunes, each of which also has integer curvature, etc. This gives rise to an infinite sequence of circles of integer curvature, and one can ask about arithmetic properties of their curvatures! Sarnak [55] proves the striking result that infinitely many of these curvatures are prime numbers, and even that there are infinitely many pairs of touching circles each with prime curvature. The mathematics behind this involves the co-ordinates of points under the action of matrices generated by words constructed from four simple matrices in $SL(4, \mathbb{Z})$, namely three that involve swapping the first co-ordinate

with any other, and also the matrix whose first column is $(-1, 2, 2, 2)$ and otherwise looks like the identity. Delightful!

There has been a very recent and startling development due to Bourgain and Kontorovich [11]: Suppose that S is a subgroup of $\mathrm{SL}(2, \mathbb{Z})$ such that the limit set, in the reals, of the orbit of any point in the upper plane, under the action of S , is of Hausdorff dimension $> 1 - \eta$ for some $\eta > 0$. Then almost all admissible¹⁸ primes appear in the bottom right hand corner of some matrix of S . What's more, almost every admissible integer appears in the bottom right hand corner of some matrix of S .

References

- [1] N.C. Ankeny and S. Chowla, *The relation between the class number and the distribution of primes*. Proc. Amer. Math. Soc. **1** (1950), 775–776.
- [2] N.A. Baas and C.F. Skau, *The lord of the numbers, Atle Selberg. On his life and mathematics*. Bull. Amer. Math. Soc. **45** (2008), 617–649.
- [3] A. Balog, *The prime k -tuples conjecture on average*. Analytic Number Theory (ed. B.C. Berndt, H.G. Diamond, H. Halberstam, A. Hildebrand), Birkhäuser, Boston, 1990, 165–204.
- [4] A. Balog, A. Granville and K. Soundararajan, *Multiplicative Functions in Arithmetic Progressions*. To appear.
- [5] C. Bays and R.H. Hudson, *A new bound for the smallest x with $\pi(x) > \mathrm{Li}(x)$* . Math. Comp. **69** (2000), 1285–1296.
- [6] E. Bombieri and H. Davenport, *Small differences between prime numbers*. Proc. Roy. Soc. Ser. A **293** (1966), 1–18.
- [7] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*. Astérisque **18** (1987/1974), 103.
- [8] E. Bombieri, *The asymptotic sieve*. Rend. Accad. Naz. dei XL, **1/2** (1977), 243–269.
- [9] J. Bourgain, A. Gamburd, and P. Sarnak, *Sieving and expanders*. C. R. Math. Acad. Sci. Paris **343** (2006), 155–159.
- [10] J. Bourgain, A. Gamburd, and P. Sarnak, *Affine linear sieve, expanders, and sum-product*. To appear.
- [11] J. Bourgain, and A. Kontorovich, *On representations of integers in thin subgroups of $\mathrm{SL}(2, \mathbb{Z})$* . To appear.
- [12] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*. Acta Arith. **2** (1936), 23–46.

¹⁸That is, that satisfy certain obvious local conditions.

- [13] H. Davenport, *Multiplicative number theory*. Springer Verlag, New York, 1980.
- [14] P.D.T.A. Elliott, *Multiplicative functions on arithmetic progressions. VII. Large moduli*. J. London Math. Soc. **66** (2002), 14–28.
- [15] P.D.T.A. Elliott, *The least prime primitive root and Linnik’s theorem*. Number theory for the millennium, I (Urbana, IL, 2000), 393–418. A. K. Peters, Natick, MA, 2002.
- [16] P. Erdős, *On the difference of consecutive primes*. Quart. J. Math. Oxford **6** (1935), 124–128.
- [17] P. Erdős, *On a new method in elementary number theory which leads to an elementary proof of the Prime Number Theorem*. Proc. Nat. Acad. Sci. **35** (1949), 374–384.
- [18] P. Erdős, *On a Tauberian theorem connected with the new proof of the Prime Number Theorem*. J. Ind. Math. Soc. **13** (1949), 133–147.
- [19] J.B. Friedlander, *Selberg’s formula and Siegel’s zero*. Recent progress in analytic number theory, Academic Press, London—New York, 1981, 15–23.
- [20] J.B. Friedlander and H. Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes*. Ann. of Math. **148** (1998), 945–1040.
- [21] J.B. Friedlander and H. Iwaniec, *Asymptotic sieve for primes*. Ann. of Math. **148** (1998), 1041–1065.
- [22] J.B. Friedlander and H. Iwaniec, *Opera de Cribro*. To appear.
- [23] P.X. Gallagher, *A large sieve density estimate near $\sigma = 1$* . Invent. Math. **11** (1970), 329–339.
- [24] D. Goldfeld, *A simple proof of Siegel’s theorem*. Proc. Nat. Acad. Sci. USA **71** (1974), 1055.
- [25] D. Goldfeld, *An asymptotic formula relating the Siegel zero and the class number of quadratic fields*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. **2** (1975), 611–615.
- [26] D. Goldfeld, *The elementary proof of the prime number theorem: An historical perspective*. Number Theory (New York 2003), Springer, New York, 2004, 179–192.
- [27] D. A. Goldston, J. Pintz, C. Y. Yildirim, *Primes in Tuples I*. Ann. of Math. **170** (2009), 819–862.
- [28] A. Granville, *On elementary proofs of the Prime Number Theorem for arithmetic progressions, without characters*. Proceedings of the Amalfi Conference on Analytic Number Theory, Salerno, Italy, 1993, 157–194.
- [29] A. Granville, *Harald Cramér and the distribution of prime numbers*. Scandinavian Actuarial J. **1** (1995), 12–28.

- [30] A. Granville, *Unexpected irregularities in the distribution of prime numbers*. Proceedings of the International Congress of Mathematicians (Zurich, Switzerland, 1994) **I** (1995), 388–399.
- [31] A. Granville, *Prime number patterns*. Amer. Math. Monthly **115** (2008), 279–296.
- [32] A. Granville and G. Martin, *Prime Number Races*. Amer. Math. Monthly **113** (2006), 1–33.
- [33] A. Granville and K. Soundararajan, *An uncertainty principle for arithmetic sequences*. Ann. of Math. **165** (2007), 593–635.
- [34] B. Green and T. Tao, *The primes contain arbitrarily long arithmetic progressions*. Ann. of Math. **167** (2008), 481–547.
- [35] B. Green and T. Tao, *Quadratic uniformity of the Möbius function*. Ann. Inst. Fourier (Grenoble) **58** (2008), 1863–1935.
- [36] B. Green and T. Tao, *Linear equations in primes*. Ann. of Math. To Appear.
- [37] B. Green and T. Tao, *The Möbius function is strongly orthogonal to nilsequences*. To Appear.
- [38] D.R. Heath-Brown, *Siegel zeros and the least prime in an arithmetic progression*. Quart. J. Math. Oxford **41** (1990), 405–418.
- [39] D.R. Heath-Brown and D.A. Goldston, *A note on the differences between consecutive primes*. Math. Ann. **266** (1984), 317–320.
- [40] D.R. Heath-Brown and B.Z. Moroz, *Primes represented by binary cubic forms*. Proc. London Math. Soc. **84** (2002), 257–288.
- [41] M.N. Huxley, *Small differences between consecutive primes*. Mathematika **20** (1973), 229–232.
- [42] A.E. Ingham, *The distribution of prime numbers*. Cambridge Math Library, Cambridge, 1932.
- [43] A.E. Ingham, MR0029410/29411. Mathematical Reviews **10** (1949), 595–596.
- [44] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*. Acta Arith. **24** (1973/74), 435–459.
- [45] H. Iwaniec, *A new form of the error term in the linear sieve*. Acta Arith. **37** (1980), 307–320.
- [46] H. Iwaniec and E. Kowalski, *Analytic number theory*. Amer. Math. Soc. Providence, Rhode Island, 2004.
- [47] J.P. Jones, D. Sato, H. Wada, and D. Wiens, *Diophantine representation of the set of prime numbers*. Amer. Math. Monthly **83** (1976), 449–464.
- [48] U.V. Linnik, *On the least prime in an arithmetic progression. II. The Deuring-Heilbronn phenomenon*. Rec. Math. [Mat. Sb.] N.S. **15** (1944), 347–368.

- [49] J.E. Littlewood, *Distribution des nombres premiers*. C. R. Acad. Sci. Paris **158** (1914), 1869–1872.
- [50] H. Maier, *Primes in short intervals*. Michigan Math. J. **32** (1985), 221–225.
- [51] H. Maier, *Small differences between prime numbers*. Michigan Math. J. **35** (1988), 323–344.
- [52] J. Pintz, *Very large gaps between consecutive primes*. J. Number Theory **63** (1997), 286–301.
- [53] J. Pintz, *Cramér vs. Cramér. On Cramér’s probabilistic model for primes*. Funct. Approx. Comment. Math. **37** (2007), 361–376.
- [54] M. Rubinstein and P. Sarnak, *Chebyshev’s bias*. Experiment. Math. **3** (1994), 173–197.
- [55] P. Sarnak, *Letter to Jeff Lagarias, 2007*. www.math.princeton.edu/sarnak/.
- [56] A. Selberg, *On the normal density of primes in small intervals and the difference between consecutive primes*. Arch. Math. Naturvid **47** (1943), 87–105.
- [57] A. Selberg, *An elementary proof of the Prime Number Theorem*. Ann. of Math. **50** (1949), 305–313.
- [58] A. Selberg, *On elementary methods in prime number-theory and their limitations*. Cong. Math. Scand. Trondheim **11** (1949), 13–22.
- [59] A. Selberg, *An elementary proof of the prime number theorem for arithmetic progressions*. Can. J. Math. **2** (1950), 66–78.
- [60] A. Selberg, *The general sieve-method and its place in prime number theory*. Proceedings of the International Congress of Mathematicians, Cambridge, Mass. **1** (1950), 286–292. Amer. Math. Soc. Providence, R.I., 1952.
- [61] A. Selberg, *Sieve methods*. Proc. Sympos. Pure Math (StonyBrook, 1969) **20**, 311–351. Amer. Math. Soc. Providence, R.I., 1971.
- [62] A. Selberg, *Remarks on sieves*. Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972), 1972, 205–216.
- [63] A. Selberg, *Sifting problems, sifting density, and sieves*. Number theory, trace formulas and discrete groups (Oslo, 1987), 467–484. Academic Press, Boston, MA, 1989.
- [64] J. Spencer and R. Graham, *The elementary proof of the prime number theorem*. Math Intelligencer **31** (2009). To appear.
- [65] E. Westzynthius, *Über die verteilung der zahlen die zu den n ersten primzahlen teilerfremd sind*. Comm. Phys. Math. Helingsfors **5:5** (1931), 1–37.

Andrew Granville

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

e-mail: andrew@dms.umontreal.ca