THE DISTRIBUTION OF PRIMES: CONJECTURES vs. HITHERTO PROVABLES

C. Y. YILDIRIM

Department of Mathematics, Boğaziçi University
& Feza Gürsey Institute for Fundamental Sciences,
İstanbul, Turkey
E-mail: yalciny@boun.edu.tr

We present the main results, conjectures and ideas concerning the distribution of primes. We recount only the most important milestones and we do not go into technical details. Instead, suggestions for further reading are provided.

Keywords: Distribution of prime numbers.

1. Introduction

Here I endeavour to give an exposition of what are 'known' about the distribution of prime numbers. Of course, there is more than one meaning of 'known'. In the strictest sense a statement is known if there is a proof agreed upon by all mathematicians; in a lenient sense instead of a proof there could be numerical data or heuristic arguments or evidence of other sorts which indicate the truth of a statement and these may be sufficient for some people to accept the assertion. Number theory is rife with long-standing questions, ranging from completely solved claims to problems about which not even conjectures can be formulated. In what follows we will dwell upon the main results and conjectures concerning the distribution of prime numbers, skipping most of the intermediate developments which along with other relevant questions not mentioned here can be tracked down from the references.

Notation

For two natural numbers a and b we denote by (a, b) their greatest common divisor. For a natural number n, Euler's totient $\phi(n)$ is the number of positive integers less than or equal to n and relatively prime to n. The letter p will always stand for a prime number. By p_n, the n-th largest prime is

meant (so that $p_1 = 2$, $p_2 = 3, \ldots$). On some occasions γ will denote Euler's constant, and on some other occasions it will denote the imaginary part of a zero of the Riemann zeta-function. In general ϵ will mean an arbitrarily small positive real number, the letters $A, C, c, \ldots$ will be used for constants, and these need not have the same value at each occurrence.

For two functions f, g we write $f(x) = O(g(x))$, or equivalently $f(x) \ll g(x)$, if there is a constant C such that $|f(x)| \leq Cg(x)$ on the common domain where both f and g are defined. If C depends on a parameter α, we write $f = O_\alpha(g)$ or $f \ll_\alpha g$. When x tends to a limit, $f(x) \sim g(x)$ means $\lim f(x)/g(x) = 1$, and $f(x) = o(g(x))$ means $\lim f(x)/g(x) = 0$. We write $f(x) = \Omega(g(x))$ in place of $\limsup |f(x)|/g(x) > 0$, and $f(x) = \Omega_\pm(g(x))$ if $\limsup f(x)/g(x) > 0$ and $\liminf f(x)/g(x) < 0$.

2. The dawn: Up until the 19th century

We can't pinpoint at which epoch and where some person(s) first hit upon the property that some of the counting numbers are prime. The most ancient records we are aware of are the almost 4000 years old clay tablets by mathematicians of the Sumer-Akkad civilization who compiled tables of factors of integers and also studied equations and extraction of square roots involving primes. One of the oldest known mathematical proofs, the proof of irrationality of $\sqrt{2}$ attributed to Pythagoras's school (6th century B.C.), relies on the concepts of divisibility and primes. Euclid (4th century B.C.), upon giving the fundamental theorem of arithmetic, proved the existence of infinitely many primes which we regard as the oldest result on the distribution of primes. Eratosthenes (3rd century B.C.) described the basic sieve method for determining the primes up to a given bound. Eratosthenes's method evolved to powerful sieve methods which played key roles in almost all of the strongest results in number theory obtained in the 20th century.

A most influential mathematician of antiquity Diophantus (circa 3rd century A.D.) was mostly occupied with finding integer or rational solutions to various equations, but his books were lost in the fire that destroyed the library of Alexandria. Some of Diophantus's books were found in the 15th century, and then translated into Latin by Bachet (1621). Fermat and Mersenne, upon studying Bachet's publication, announced new results on divisibility, primes and Diophantine equations. From their works the branches of (as they are now called) elementary number theory, algebraic number theory, Diophantine equations, elliptic curves ... developed. The 20th century witnessed several culminations of these developments, the completion of the proof of Fermat's Last Theorem by Wiles, and appli-

cations of primes and factorization to cryptography to name two.

As far as we know after Euclid and Eratosthenes the next mathematician to produce results on the distribution of primes was Euler (1737). The only still problematic statement from the times in between is that every even number is a sum of one, two or three primes due to Descartes. *Euler's product identity*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p:\,\text{prime}} (1 - \frac{1}{p^s})^{-1}, \tag{1}$$

valid for $s > 1$, is an analytic way of expressing the unique factorization of natural numbers into a product of primes. Euler had no scruples about using this identity with $s = 1$, whereupon he deduced that the sum of the reciprocals of the primes diverges. He also corresponded with Goldbach, who conjectured that every number > 2 can be written as a sum of three primes and every even number > 2 is a sum of two primes. (These statements are believed to be true, with the obvious modification to > 5 in the first statement, according to the present understanding that 1 is not a prime number contrary to Goldbach and many mathematicians before him who at times took 1 as a prime. We can immediately notice some properties which distinguish 1 from the primes: 1 is the multiplicative unit of the ring of integers and divisibility by 1 is not a special feature of any integer. Moreover, the value of any multiplicative arithmetic function at 1 is 1, whereas $\phi(p) = p - 1$ for example, so that unnecessary inconvenience in the definitions of arithmetic functions is avoided by excluding 1 from the set of primes. Some information about the status of Goldbach's still unproved statements will be given in §9).

Gauss mentioned much later in his life that around 1792, upon examining tables of primes, he conjectured that a good approximation to

$$\pi(x) := \sum_{p \le x} 1 \tag{2}$$

is given by the logarithmic integral

$$\mathrm{li}(x) := \int_2^x \frac{dt}{\log t}, \tag{3}$$

and that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1 \tag{4}$$

which is equivalent to $p_n \sim n \log n$. A similar but slightly wrong conjecture was in fact first published in 1798 and 1808 by Legendre, also on empirical

grounds. Gauss also stated that the number of integers $\leq x$ which are products of two distinct primes (we call these E_2-*numbers*) is approximately $x \log\log x / \log x$.

3. The launch of rigorous analytic methods for primes

Euler stated that an arithmetic progression with the first term 1 contains infinitely many primes. Elementary number theory textbooks contain examples of generalizations of Euclid's theorem to some arithmetic progressions, i.e. sequences of the form $a + kq$ where a and q are fixed relatively prime positive integers and k runs through all natural numbers, for example, that the progressions $3 + 4k, 1 + 4k, 1 + 3k, 5 + 6k...$ each contain an infinitude of primes. Some of these are proved by simple modifications in Euclid's proof, and some require other elementary ingredients. M.R. Murty [88], defining a Euclidean proof for the arithmetic progression $a + kq$ via the existence of an irreducible polynomial $f(x)$ with integer coefficients such that all but finitely many prime divisors of the values $f(n)$, $n \in \mathbb{Z}$ are either $\equiv 1 (\mathrm{mod}\, q)$ or $\equiv a (\mathrm{mod}\, q)$, proved that a Euclidean proof exists if and only if $a^2 \equiv 1 (\mathrm{mod}\, q)$. (The 'if' part of this theorem had been proved by I. Schur).

The full generalization of Euclid's theorem that if a and q are relatively prime natural numbers, then there are infinitely many primes of the form $a + kq$ was conjectured by Legendre (1788) and proved by Dirichlet (1837-1840) in some memoirs which are regarded as the origin of analytic number theory. Dirichlet's idea was to adapt Euler's method to the case when the primes are restricted to the residue class $a (\mathrm{mod}\, q)$. The proof uses the so-called *Dirichlet's L-functions*, defined by

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1 - \frac{\chi(p)}{p^s})^{-1} \tag{5}$$

in $s > 1$ where the series and the product are absolutely convergent. Here χ is a *Dirichlet's character to the modulus* q, a function of an integer variable n which is multiplicative and periodic with period q. It follows that if $(n, q) = 1$, then $\chi(n)$ is a root of unity. For $(n, q) > 1$, it is apt to define $\chi(n) = 0$. The character χ_0 which assumes the value 1 at all n coprime to q is called the *principal character* in which case (5) differs from (1) by the finite factor $\prod_{p|q}(1 - \frac{1}{p^s})$. It could be that for values of n coprime to q, the least period of a nonprincipal $\chi(n)$ is not q but a divisor of q, in which case χ is called an *imprimitive* character, and otherwise *primitive*. There are $\phi(q)$ characters in all to the modulus q, which form an abelian group (defining $\chi_1\chi_2(n) =$

$\chi_1(n)\chi_2(n)$) isomorphic to the group of those residue classes which are relatively prime to the modulus q. The characters to the modulus q satisfy

$$\sum_{n(\bmod q)} \chi(n) = \begin{cases} \phi(q) & \text{if} \quad \chi = \chi_0, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\sum_{\chi(\bmod q)} \chi(n) = \begin{cases} \phi(q) & \text{if} \quad n \equiv 1 \,(\bmod q), \\ 0 & \text{otherwise.} \end{cases}$$

From a given set of integers those belonging to a particular residue class $a(\bmod q)$ can be selected by invoking

$$\frac{1}{\phi(q)} \sum_{\chi(\bmod q)} \overline{\chi}(a)\chi(n) = \begin{cases} 1 & \text{if} \quad n \equiv a \,(\bmod q) \quad \text{and } (a,q) = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

For nonprincipal χ the series in (5) is conditionally convergent for $0 < s \leq 1$ so that $L(s,\chi)$ is regular at $s = 1$. Dirichlet's proof of the infinitude of primes of the form $a + kq$ hinges on the fact that for χ nonprincipal, $\log L(s,\chi)$ is bounded as $s \to 1^+$.

Dirichlet's innovations were wonderful, but the challenge of estimating the number of primes up to x, as $x \to \infty$, was not overcome yet. Around 1849 Chebyshev made advances in this problem. He showed that if $\lim_{x\to\infty} \pi(x)/x \log x$ exists it should be 1, and found lower and upper bounds to this limit as 0.92.. and 1.10.. by an argument based on equating the Stirling formula estimate for $\log n!$ with the expression of $\log n!$ as a sum over the logarithms of primes up to n. But Chebyshev's method would not pin down the limit to 1.

Mertens (1874) went further along Chebyshev's lines and established the following asymptotic formulae:

$$\sum_{p\leq x} \frac{\log p}{p} = \log x + O(1), \tag{7}$$

$$\sum_{p\leq x} \frac{1}{p} = \log\log x + A + O(\frac{1}{\log x}), \tag{8}$$

$$\prod_{p\leq x} (1 - \frac{1}{p})^{-1} = e^{\gamma} \log x + O(1). \tag{9}$$

Mertens also showed that if χ is a nonprincipal character then $\sum_p \frac{\chi(p)}{p}$ converges (Dirichlet had used $\lim_{\sigma\to 1^+} \sum_p \frac{\chi(p)}{p^\sigma}$ is finite), wherefrom he ob-

tained the generalization of the second of his formulas given above, a quantified form of Dirichlet's theorem:

$$\sum_{\substack{p\le x\\ p\equiv a(\bmod q)}} \frac{1}{p} = \frac{\log\log x}{\phi(q)} + A(q,a) + O(\frac{1}{\log x}). \tag{10}$$

4. Riemann's revolution

It is indeed interesting that partial summation applied to (7) or (8) is of no avail for obtaining an asymptotic formula for $\pi(x)$. In between Chebyshev and Mertens there was a development which turned out to be of utmost importance, not only for the goal of settling (4), but also for the impact on the theory of functions of a complex variable. In an article published in 1859, Riemann [98] took the quantity given by either of the two expressions in the Euler product identity (1) as a function of a complex variable $s = \sigma + it \in \mathbb{C},\ \sigma, t \in \mathbb{R}$. In this way the *Riemann zeta-function* $\zeta(s)$ was defined in the half-plane $\sigma > 1$ where both sides of (1) are absolutely convergent and therefore make sense. He started from the well-known equation $\displaystyle\int_0^\infty e^{-nx}x^{s-1}\,dx = \frac{\Gamma(s)}{n^s}$, which upon summing over n gives $\displaystyle\zeta(s) = \frac{1}{\Gamma(s)}\int_0^\infty \frac{x^{s-1}}{e^x-1}\,dx$ for $\sigma > 1$. Riemann's remarkable insight to take $s \in \mathbb{C}$ allowed him to apply the methods of complex integration, and upon using the functional equation for a Jacobi theta function he obtained the representation

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \frac{1}{s(s-1)} + \int_1^\infty (x^{\frac{s}{2}-1} + x^{-\frac{s+1}{2}})(\sum_{n=1}^\infty e^{-n^2\pi x})\,dx\,, \tag{11}$$

where the integral converges absolutely for any s, and uniformly in compact subsets of the s-plane. Thus Riemann showed that from its original domain of definition $\zeta(s)$ can be continued analytically over the whole complex plane as a single-valued and meromorphic function with its only pole at $s = 1$, a simple pole with residue 1. Since the right-hand side of (11) is unchanged when $1-s$ is used in place of s, this also revealed the *functional equation of* $\zeta(s)$:

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\zeta(1-s). \tag{12}$$

The value of $\zeta(s)$ can be calculated at any s with $\sigma > 1$ to any desired accuracy from the expressions in (1). Then, by the functional equation, $\zeta(s)$ can also be calculated for any s with $\sigma < 0$. It is clear from the product

in (1) that $\zeta(s) \neq 0$ in $\sigma > 1$, and it is immediate from (12) that at the negative even integers where $\Gamma(\frac{s}{2})$ has simple poles, $\zeta(s)$ vanishes - these are called the *trivial zeros*. In the rather mysterious region $0 \leq \sigma \leq 1$, the so-called *critical strip*, one may use (11) or

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty (x)x^{-s-1}\,dx \quad (\sigma > 0), \tag{13}$$

where (x) is the fractional part of x. In this formula which is obtained by applying partial summation to the series in (1), the integral converges absolutely for $\sigma > 0$ and uniformly for $\sigma \geq \delta > 0$, so that we have an analytic continuation of $\zeta(s)$ to $\sigma > 0$.

Riemann also made several assertions on the zeros of $\zeta(s)$, and provided sketches of the proofs for some. The matter of justifying Riemann's statements inspired Hadamard's work on general results for entire functions. Hadamard (1893) showed that the entire function $\xi(s) := \frac{1}{2}s(s-1)\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$ is bounded in size by $\exp(C|s|\log|s|)$ as $|s| \to \infty$, from which he deduced that $\zeta(s)$ has infinitely many *nontrivial zeros* in the critical strip. The nontrivial zeros must be situated symmetrically with respect to the real axis, and with respect to the point $\frac{1}{2}$. Applying the argument principle to $\xi(s)$, von Mangoldt (1895) gave the proof of Riemann's assertion that the number of nontrivial zeros $\rho = \beta + i\gamma$ with $0 < \gamma \leq T$ is $\frac{T}{2\pi}\log T - \frac{T}{2\pi} + O(\log T)$, as $T \to \infty$.

Riemann's expression for $\pi(x)$ in terms of the zeros of $\zeta(s)$, and a related formula we will now dwell upon, were also fully proved by von Mangoldt. Logarithmic differentiation of the product expression of $\zeta(s)$ gives

$$\frac{\zeta'}{\zeta}(s) = -\sum_{n=2}^{\infty}\frac{\Lambda(n)}{n^s} \quad (\sigma > 1), \tag{14}$$

where $\Lambda(n)$ is *von Mangoldt's function*

$$\Lambda(n) := \begin{cases} \log p & \text{if} \quad n = p^a, \quad p\text{: prime, } a \in \mathbb{N}\ , \\ 0 & \text{otherwise.} \end{cases} \tag{15}$$

Most researchers find it more convenient to work with

$$\psi(x) := \sum_{n \leq x}\Lambda(n) = \sum_{p^m \leq x}\log p \tag{16}$$

and then convert a result involving $\psi(x)$ to a result for $\pi(x)$ than working straightforwardly with $\pi(x)$. For instance, (4) is equivalent to $\psi(x) \sim x$.

From (14) one has

$$\psi_0(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty}[-\frac{\zeta'}{\zeta}(s)]\frac{x^s}{s}\,ds \quad (c>1), \tag{17}$$

where $\psi_0(x) = \psi(x) - \dfrac{\Lambda(x)}{2}$. Considering the integral from $c-iT$ to $c+iT$, and moving the line of integration all the way to the left in the complex plane one obtains, by the residue theorem, for any $x \geq 2$,

$$\psi_0(x) = x - \sum_{|\gamma|<T}\frac{x^\rho}{\rho} - \frac{\zeta'}{\zeta}(0) - \frac{1}{2}\log(1-x^{-2}) \tag{18}$$
$$+ O(\frac{x\log^2(xT)}{T}) + O(\log x \min(1, \frac{x}{T\langle x\rangle}))$$

(here $\langle x\rangle$ denotes the distance from x to the nearest prime power - other than x itself in case x is a prime power). This is known as the *Riemann-von Mangoldt formula* or the *explicit formula*: it provides an explicit link between a (weighted) count of the primes and a sum over the nontrivial zeros of $\zeta(s)$. The more elegant form obtained by taking the limit $T \to \infty$ in (18),

$$\psi_0(x) = x - (\lim_{T\to\infty}\sum_{|\gamma|<T}\frac{x^\rho}{\rho}) - \frac{\zeta'}{\zeta}(0) - \frac{1}{2}\log(1-x^{-2}) \tag{19}$$

which is valid for $x > 1$, is less useful in applications.

The time was ripe, in 1896 Hadamard and de la Vallée-Poussin proved independently that $\zeta(s)$ has no zeros on the line $\sigma = 1$, from which they reached (4), the *prime number theorem*. (In fact, the non-vanishing of $\zeta(s)$ on the line $\sigma = 1$ is equivalent to the prime number theorem).

It is clear from the explicit formula that the more we know about the location of the zeta zeros, the more we can say about $\psi(x) - x$. So de la Vallée-Poussin's (1899) result $\zeta(s) \neq 0$ for $\sigma > 1 - c/\log(|t|+2)$ for the *zero-free region of* $\zeta(s)$ yielded the prime number theorem with the error term $\psi(x) = x + O(x\exp[-c(\log x)^{\frac{1}{2}}])$. This can be seen by an argument which combines the fact that $3\dfrac{\zeta'}{\zeta}(\sigma) + \Re[4\dfrac{\zeta'}{\zeta}(\sigma+it) + \dfrac{\zeta'}{\zeta}(\sigma+2it)] \leq 0$ (a consequence of $3 + 4\cos\theta + \cos 2\theta \geq 0$, $\forall\theta \in \mathbb{R}$) with simple inequalities obtained from the partial fraction expansion of $\dfrac{\zeta'}{\zeta}(s)$.

The hope for an elementary, i.e. without recourse to the theory of functions of a complex variable and in fact to any infinite summation, though not necessarily easy, proof of the prime number theorem seemed to fade.

Hardy [54] said in 1921 "No elementary proof is known, and one may ask whether it is reasonable to expect one. Now we know that the theorem is roughly equivalent to a theorem about an analytic function, the theorem that Riemann's zeta-function has no zeros on a certain line. A proof of such a theorem, not fundamentally dependent upon the ideas of the theory of functions, seems to me extraordinarily unlikely. It is rash to assert that a mathematical theorem cannot be proved in a particular way; but one thing seems quite clear. We have certain views about the logic of the theory; we think that some theorems, as we say, 'lie deep', and others nearer to the surface. If anyone produces an elementary proof of the prime number theorem, he will show that these views are wrong, that the subject does not hang together in the way we have supposed, and that it is time for the books to be cast aside and for the theory to be rewritten". A century after Chebyshev, Selberg [103] succeeded in giving an elementary proof based on *Selberg's identity*

$$\sum_{n\leq x}\Lambda(n)\log n+\sum_{mn\leq x}\Lambda(m)\Lambda(n)=2x\log x+O(x) \tag{20}$$

(and Erdös [20] too; Goldfeld [32] has told the story of the dispute over their roles in the proof). Being a kind of Stirling's formula of higher degree, (22) leads to achieving more than Chebyshev's results. There is some folklore to the effect that in fact Selberg might have been inspired by zeta function theory in arriving at his identity (Ingham, in his review [68] of Selberg's and Erdös's articles pointed out that it is quicker to obtain the identity starting out from equating coefficients in the Dirichlet series expression for $(\frac{\zeta'}{\zeta}(s))'+(\frac{\zeta'}{\zeta}(s))^2=\frac{\zeta''}{\zeta}(s))$, but Selberg presented an argument which avoids these. Selberg [104] also gave an elementary proof of Dirichlet's theorem on the infinitude of primes in an arithmetic progression.

Using I.M. Vinogradov's method for strong majorizations of *exponential sums* (i.e. sums of the kind $\sum_{a<n\leq b} g(n)e^{2\pi i f(n)}$), in 1958 Korobov and Vinogradov independently established that the region

$$\sigma>1-\frac{c}{(\log(3+|t|))^{2/3}(\log\log(3+|t|))^{1/3}}. \tag{21}$$

is free of zeta zeros. This implies the prime number theorem with the smallest proved error term

$$\pi(x)=\operatorname{li}x+O(x\exp[-c\frac{(\log x)^{\frac{3}{5}}}{(\log\log x)^{\frac{1}{5}}}]). \tag{22}$$

5. The Riemann Hypothesis

In view of the fact that zeta zeros do exist in the critical strip and they are situated symmetrically with respect to the critical line, the strongest improvement on the zero-free region (21) one can ever hope for is $\sigma > \frac{1}{2}$. Of all the assertions in Riemann's memoir the guess that *'all of the nontrivial zeros lie on the critical line* $\sigma = \frac{1}{2}$*'* is the only one that still awaits a proof. This statement which has turned out to be very profound is known as the *Riemann Hypothesis* (RH). Riemann wrote that after some fleeting futile attempts he put it aside, correctly assessing that it wasn't necessary for his immediate aim of reaching the prime number theorem.

Other than the point of view that it is esthetically pleasing and ideally desirable to have all of the zeros of a function which is deeply related to the primes and which has a simple Dirichlet series in the sense that all of the coefficients are 1, lie on one line (and are simple), there is considerable evidence in favour of RH.

Beginning with Riemann himself, computations have now reached to cover the first 10^{13} zeros, as well as millions of zeros in certain intervals at ordinates up to 10^{24}, and they are all simple zeros on the critical line ([46]). By the theoretical studies of Hardy and Littlewood, Selberg, Levinson, and finally Conrey [10], it is now known that more than 40 % of the zeros of $\zeta(s)$ lie on the critical line $\sigma = \frac{1}{2}$ and are simple. This result was attained by the *mollifier method*, in which a suitable *Dirichlet polynomial* (an expression of the kind $\sum_{n \leq y} \frac{a_n}{n^s}$), producing the effect of smoothing out the irregularities, is introduced in the integrands involving $\zeta(s)$ of the integrals needed for the application of the argument principle. There are also *zero-density estimates* which are upper bounds for $N(\sigma, T) := \{\rho : \zeta(\rho) = 0, \sigma < \beta, 0 < \gamma \leq T\}$. Zero-density estimates are useful in tackling many problems of analytic number theory unconditionally (i.e. not assuming the truth of RH or any other unproved hypotheses). It is known that $N(\sigma, T) \ll T^{3(1-\sigma)/(2-\sigma)} \log^5 T$ uniformly for $\sigma > \frac{1}{2}$. (This result due to Ingham (1940) has been improved for some σ by later researchers). The density estimates say that exceptions to RH, if ever they exist, are rare and become rarer as σ moves away from $\frac{1}{2}$.

The importance of $\zeta(s)$ is not limited by its connections to the distribution of primes and other applications in analytic number theory by virtue of its Euler product being a key tool in dealing with similar products arising from multiplicative functions. The Riemann zeta-function is the protoype of a class of functions, *global L-functions*, associated with various algebraic,

arithmetic or geometric objects (as well as some which are not directly associated as such). These functions are Dirichlet series possessing a product representation of the Euler type, they can be analytically continued from their original domain of definition in keeping with a functional equation, and a version of RH can be stated for them. The existence of these functions and the properties satisfied by them have enormous implications in many areas. In many cases some parts of these conditions have been shown to hold, the rest remain conjectural. There are numerical data concerning some cases which confirm the hypotheses. For no global L-function the truth or falsity of RH has been established. However, for many problems the implications of the relevant form of RH have been proved by independent means. Thus global L-functions can be regarded to provide additional belief in the truth of RH by dint of the (mostly hypothetical) coherence in the big picture which includes many theories. Furthermore, for the zeta functions of algebraic varieties over finite fields, the analogue of RH has been proved.

Other mostly hypothetical support comes from additional conjectures which predict results that are confirmed by numerical computations. There are even problems for which predictions were not possible before. The predictions from these conjectures on already proved results coincide with them. We will say a little more about these in §7.

There are diverse statements, in complex analysis and functional analysis, formulated as tests or equivalent conditions for the truth of RH, and nothing that points to the falsity of RH has come up.

The following probabilistic argument supports RH. Consider the Möbius function $\mu(n)$ defined on the natural numbers as follows. First of all, as all multiplicative arithmetic functions, $\mu(1) = 1$. If $n = p_{\alpha_1} \cdots p_{\alpha_k}$ is a product of k distinct primes, then $\mu(n) = (-1)^k$. If n is divisible by the square of a prime, then $\mu(n) = 0$. It is easy to see that

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \quad (\sigma > 1), \tag{23}$$

and that

$$M(x) := \sum_{n \leq x} \mu(n) = O(x^{\frac{1}{2}+\epsilon}) \Longleftrightarrow \text{RH is true.} \tag{24}$$

The sequence $\{\mu(n)\}_{n=1}^{\infty}$ seems to be quite random in the long run, and for almost all random sequences of entries 0 or ± 1, the summatory function is bounded as $O(x^{\frac{1}{2}+\epsilon})$. (We note that Mertens' original conjecture that $|M(x)| \leq x^{\frac{1}{2}}$ was refuted by Odlyzko and te Riele [91] who showed

that $\limsup_{x\to\infty} M(x)x^{-\frac{1}{2}} > 1.06$ and $\liminf_{x\to\infty} M(x)x^{-\frac{1}{2}} < -1.009$. Ingham [67] proved that if at most a finite number of sums of the type $\sum_{n\leq N} c_n\gamma_n$, with integers c_i having greatest common divisor 1, are 0, then the just mentioned lim inf and lim sup are ∞ and $-\infty$ respectively. Here $\gamma_1, \gamma_2, \ldots$ denote the imaginary parts of the distinct nontrivial zeros of $\zeta(s)$. Bateman et. al. [2] weakened the condition demanded by Ingham's theorem to having $|c_n| \leq 2$ with at most one of the $|c_n| = 2$ and not all of them 0).

If RH is false, then the distribution of primes would have to exhibit irregularities much wilder than expected, and the first zeta zero off the critical line would be a very significant mathematical constant.

If RH is true, then all the ρ have real part $\frac{1}{2}$, and knowing the count of zeta zeros it is easy to deduce from the explicit formula that

$$\psi(x) = x + O(x^{\frac{1}{2}}\log^2 x) \quad \text{and} \quad \pi(x) = \operatorname{li} x + O(x^{\frac{1}{2}}\log x) \tag{25}$$

with a much smaller error term than (22). The exponent $\frac{1}{2}$ in the error term is the best possible because there are zeta zeros on the critical line.

6. More about the error term in the prime number theorem

Littlewood (1914) used Dirichlet's theorem on Diophantine approximation to show that the sum over ρ cannot be very small at all x, and proved that

$$\psi(x) - x = \Omega_{\pm}(x^{\frac{1}{2}}\log\log\log x) \quad \text{and} \quad \pi(x) - \operatorname{li} x = \Omega_{\pm}(\frac{x^{\frac{1}{2}}\log\log\log x}{\log x}). \tag{26}$$

This also answers Riemann's [98] thoughts on whether it could always be that $\pi(x) < \operatorname{Li} x := \int_0^{\infty} \frac{dt}{\log t}$ for $x > 2$. However, Pintz [93] proved that $\int_2^X (\pi(t) - \operatorname{Li} t)dt < 0$ for all sufficiently large X if and only if RH holds, and that $\pi(x) - \operatorname{Li} x$ is negative in a particular average sense. Furthermore, considerations based on some basic beliefs about the zeta zeros suggest that the probability that $\pi(x) > \operatorname{li} x$ is about $2.6 \cdot 10^{-7}$ (see [99]). Montgomery [84] suggested on a probabilistic argument, assuming RH and the linear independence over rational numbers of the imaginary parts of the nontrivial zeros above the real axis so that linear forms in the γ don't take on very small values, that the sharpest form of the prime number theorem can be

$$\overline{\lim}\frac{\psi(x) - x}{x^{\frac{1}{2}}(\log\log\log x)^2} = \pm\frac{1}{2\pi}, \quad (x \to \infty). \tag{27}$$

Note that even under (27), Legendre's conjecture that there is always a prime between n^2 and $(n+1)^2$ for any positive integer n is inaccessible.

Averages of the error term in the prime number theorem are also of great relevance in studying the distribution of primes. For brevity call

$$R(x) := \psi(x) - x\,. \tag{28}$$

By (26) it is known that, as $x \to \infty$, $R(x)$ changes sign infinitely many times. Cramér [14] showed that on RH

$$\int_1^X \frac{(R(u))^2}{u}\,du = O(X), \tag{29}$$

and

$$\int_1^X (\frac{R(u)}{u})^2\,du \sim C\log X\,. \tag{30}$$

Gallagher's article [31] contains compact proofs of such results. Pintz [92] has shown that for all sufficiently large X

$$\frac{X^{\frac{3}{2}}}{400} \le \int_1^X |R(u)|\,du \le X^{\frac{3}{2}}\,, \tag{31}$$

where the lower bound is unconditional and the upper bound depends essentially on RH. Jurkat [73], by developing concepts on almost-periodic functions proved upon RH that,

$$\int_x^{x+\frac{x}{\log\log x}} \frac{R(u)}{u^{\frac{3}{2}}}\,du = \Omega_{\pm}(\frac{\log\log\log x}{\log\log x}) \tag{32}$$

(with the implied constants $\pm\frac{1}{2}$), and that this cannot be improved upon much for he also showed that the left-hand side of (32) is $O((\log\log\log x)^2/\log\log x)$. This result contains Littlewood's result (26). From (31) and (25) we see that as $x \to \infty$, $|R(x)|$ spends most of its time roughly around the value $x^{\frac{1}{2}}$ (instead of much smaller values), and (32) reveals the existence of quite long intervals throughout which $|R(x)|$ is almost as large as possible.

7. Pair correlation of zeta zeros and primes

In 1972 H. L. Montgomery [83], assuming RH, found a way of looking into the distribution of the nontrivial zeros on the line $\sigma = \frac{1}{2}$. Upon developing a new version of the explicit formula, Montgomery was led to define

$$F(\alpha, T) = (\frac{T}{2\pi}\log T)^{-1} \sum_{0<\gamma,\gamma'\le T} \frac{4}{4+(\gamma-\gamma')^2} T^{i\alpha(\gamma-\gamma')}, \tag{33}$$

where $\frac{1}{2}+i\gamma$ and $\frac{1}{2}+i\gamma'$ run through the zeros of $\zeta(s)$. It is easily seen that $F(\alpha,T)=F(-\alpha,T)$, and from the count of zeta zeros that $F(\alpha,T)\ll \log T$ for any $\alpha\in\mathbb{R}$. By using the mean-value result for Dirichlet series (see [86])

$$\int_0^T |\sum_n a_n n^{-it}|^2\,dt=\sum_n |a_n|^2(T+O(n)) \tag{34}$$

(with a_n's composed of the von Mangoldt function $\Lambda(n)$ in this application), Montgomery showed that upon RH one can obtain

$$F(\alpha,T)=(1+o(1))T^{-2\alpha}\log T+\alpha+o(1),\quad (0\le\alpha\le 1), \tag{35}$$

as $T\to\infty$. What is in question here is the size of

$$\int_0^T |\frac{1}{T^\alpha}\sum_{n\le T^\alpha}\Lambda(n)n^{\frac{1}{2}-it}+T^\alpha\sum_{n>T^\alpha}\Lambda(n)n^{-\frac{3}{2}-it}-\frac{2T^{\alpha(\frac{1}{2}-it)}}{(\frac{1}{2}+it)(\frac{3}{2}-it)}|^2\,dt.$$

For $\alpha>1$ the estimate for the contribution of the nondiagonal terms become large enough to prevent an asymptotic estimate. Montgomery, drawing upon the conjectured size of expressions of the kind $\sum_{n\le x}\Lambda(n)\Lambda(n+h)$ (see §9), conjectured that

$$F(\alpha,T)=1+o(1),\qquad (1\le\alpha\le A). \tag{36}$$

In (35) and (36) the estimates are uniform in the respective domains of α, and $A>1$ is arbitrary but fixed. Here the condition that A is fixed cannot be relaxed, since from Dirichlet's theorem on Diophantine approximation it can be seen that there exist large $\alpha=\alpha(T)$ for which $F(\alpha,T)$ is close to $F(0,T)\sim\log T$. We expect that $F(\alpha,T)\ll 1$ holds on average, for Goldston [34] proved, assuming RH, that for sufficiently large T,

$$\int_c^{c+1}F(\alpha,T)<\frac{8}{3}+\epsilon,\quad \int_{c-1}^{c+1}F(\alpha,T)>\frac{2}{3}-\epsilon,$$

uniformly for any $c\in\mathbb{R}$ (c may even be a function of T).

Using convolutions of $F(\alpha,T)$ with appropriate kernels $\hat{r}(\alpha)$ so that

$$\sum_{0<\gamma,\gamma'\le T} r((\gamma-\gamma')\frac{\log T}{2\pi})w(\gamma-\gamma')=(\frac{T}{2\pi}\log T)\int_{-\infty}^{\infty}F(\alpha,T)\hat{r}(\alpha)\,d\alpha$$

where r and $\hat{r}$ are Fourier transforms of each other, from (35) and (36) Montgomery obtained

$$\sum_{\substack{0<\gamma,\gamma'\le T\\ \frac{2\pi\alpha}{\log T}<\gamma-\gamma'\le\frac{2\pi\beta}{\log T}}} 1\sim(\frac{T\log T}{2\pi})\{\int_\alpha^\beta 1-(\frac{\sin\pi u}{\pi u})^2\,du+\delta(\alpha,\beta)\}, \tag{37}$$

as $T \to \infty$ for fixed $\alpha < \beta$ (here $\delta(\alpha, \beta) = 1$ if $0 \in [\alpha, \beta]$ and $\delta(\alpha, \beta) = 0$ if $0 \notin [\alpha, \beta]$). The assertions (36) or (37) are essentially equivalent, they are known as the *pair correlation conjecture* (PC), and from either it is easy to deduce that almost all zeta zeros are simple. Since on RH, $F(\alpha, T)$ can be calculated for $|\alpha| \leq 1$ as in (35), one can use an $\hat{r}(\alpha)$ supported in $[-1, 1]$ to see the implications of RH. By taking $r(u) = (\frac{\sin \pi\alpha u}{\pi\alpha u})^2$, Montgomery deduced that on RH at least $\frac{2}{3}$ of the zeros of $\zeta(s)$ are simple. We also note that for $M(x)$ defined in (24), the *Mertens hypothesis* in the weaker form

$$\int_1^X \big(\frac{M(x)}{x}\big)^2 \, dx = O(\log X), \tag{38}$$

implies that all zeros of $\zeta(s)$ which are on the critical line are simple (see [110, §14.29]).

The emergence of $1-(\frac{\sin \pi u}{\pi u})^2$ as the pair correlation function of the zeta zeros has turned out to be very fruitful for the unleashing of new methods for studying $\zeta(s)$ and functions allied to it. F. J. Dyson told Montgomery that this is precisely the same pair correlation function for the eigenvalues of large order random Hermitian matrices, specifically the Gaussian Unitary Ensemble (GUE). From the random matrix model many details about $\zeta(s)$ (such as the moments of $\zeta(s)$ on the critical line, the maximal size of $\arg \zeta(\frac{1}{2} + it)$, the maximal and minimal gaps between zeta zeros) which were formerly inaccessible even by heuristics can now be predicted. Furthermore, random matrix models for general L-functions are also being thoroughly investigated in tandem with the philosophy of studying ensembles of such functions rather than regarding each one, and in particular their prototype $\zeta(s)$, as an isolated object. Over the last three decades considerable numerical and theoretical evidence pointing to the validity of random matrix models have accumulated. All these add to our belief in the existence of a linear operator whose eigenvalues characterize the zeros of $\zeta(s)$ (and similarly for other L-functions), an idea that legend dates back to Hilbert and Pólya (see [90]). We refer the reader to Conrey's surveys [12] and [13] for a detailed exposition of this research area.

Goldston and Montgomery [39] proved an equivalence between the pair correlation conjecture (36) and the asymptotic estimate for the second moment for primes (note that the first moment for primes is easily obtained from the prime number theorem). The result is, setting $x = T^\alpha$ and

$F_T(x) = \dfrac{T\log T}{2\pi}F(\alpha,T)$ and assuming RH, as follows:

$$\int_1^x \{\psi((1+\delta)y) - \psi(y) - \delta y\}^2\,dy \sim \frac{1}{2}\delta x^2(\log 1/\delta) \tag{39}$$

holds uniformly for $x^{-B_2} \le \delta \le x^{-B_1}$ where $0 < B_1 \le B_2 \le 1$, provided that

$$F_T(x) \sim \frac{T\log T}{2\pi} \tag{40}$$

is true uniformly for $x^{B_1}(\log x)^{-3} \le T \le x^{B_2}(\log x)^3$; conversely, if (39) holds uniformly in $x^{-1/A_1}(\log x)^{-3} \le \delta \le x^{-1/A_2}(\log x)^3$ where $1 \le A_1 \le A_2 < \infty$, then (40) is true uniformly for $T^{A_1} \le x \le T^{A_2}$.

Heath-Brown [57] showed that from RH and (36) in the weaker form $F_T(x) = o(T\log^2 T)$ for $1 \le \alpha \le A$ it follows that

$$\psi(x) = x + o(x^{\frac{1}{2}}\log^2 x). \tag{41}$$

The effect of assuming PC on top of RH can be assessed by comparing (41) with (25)-(27). With the support of PC one would expect to obtain nontrivial estimates on sums such as $\sum_\rho \dfrac{x^\rho}{\rho}$. For instance, Heath-Brown derived from the representation

$$\int_{-\infty}^{\infty} e^{-2|u|}\Big|\sum_{0<\gamma\le T} x^{i\gamma}e^{i\gamma u}\Big|^2\,du = F_T(x) \tag{42}$$

(which incidentally reveals that $F_T(x) \ge 0$ for all x), that

$$\sum_{0<\gamma\le T} x^{i\gamma} \ll T^{\frac{1}{2}}\{\max_{t\le T} F_t(x)\}^{\frac{1}{2}} \tag{43}$$

whereas the trivial bound is

$$\sum_{0<\gamma\le T} x^{i\gamma} \ll T\log T. \tag{44}$$

Since $\psi_0(x)$ is discontinuous at the prime powers, so is $\sum_\rho \dfrac{x^\rho}{\rho}$ $(= \lim_{T\to\infty}\sum_{|\gamma|<T}\dfrac{x^\rho}{\rho})$ by the explicit formula (19); the series is boundedly convergent in fixed intervals $1 < a \le x \le b$. The sum $\sum_{0<\gamma\le T} x^\rho$ too is discontinuous at the prime powers. By considering $\displaystyle\int \frac{\zeta'(s)}{\zeta(s)}x^s\,ds$ taken around an

appropriate rectangular contour, Gonek [45] proved a uniform (in both x and T) version of an old result of Landau, that for $x, T > 1$,

$$\sum_{0<\gamma\le T} x^\rho = -\frac{T}{2\pi}\Lambda(x) + O(x\log 2xT\,\log\log 3x) \tag{45}$$
$$+O(\log x\min(T, \frac{x}{\langle x\rangle})) + O(\log 2T\min(T, \frac{1}{\log x})).$$

If one assumes RH, then (45) implies for $x, T > 1$ that

$$\sum_{0<\gamma\le T} x^{i\gamma} \ll Tx^{-\frac{1}{2}}\log 2x + x^{\frac{1}{2}}\log 2x\log\log 3x. \tag{46}$$

Comparison with (44) shows that (46) is nontrivial for $2 \le x \le T^{2-\epsilon}$. If one assumes further that the $x^{i\gamma}$ behave like independent random variables, then one may expect that for almost all $x > 1$,

$$\sum_{0<\gamma\le T} x^{i\gamma} \ll T^{\frac{1}{2}+\epsilon}. \tag{47}$$

However, by Dirichlet's theorem on Diophantine approximation there exist arbitrarily large x for which

$$\sum_{0<\gamma\le T} x^{i\gamma} \gg T\log T, \tag{48}$$

so (47) doesn't hold for all $x > 1$. The observation (47) along with the heuristics of using $n/\log n$ in place of γ_n in $\sum x^{i\gamma}$ led Gonek to conjecture that

$$\sum_{0<\gamma\le T} x^{i\gamma} \ll (Tx^{-\frac{1}{2}+\epsilon} + T^{\frac{1}{2}}x^\epsilon), \quad (x, T \ge 2). \tag{49}$$

This would imply that, for $1 \le h \le x$,

$$\psi(x+h) - \psi(x) = h + O(h^{\frac{1}{2}}x^\epsilon), \tag{50}$$

which in turn yields

$$p_{n+1} - p_n \ll p^\epsilon. \tag{51}$$

For comparison we note the results on difference between consecutive primes under various conditions:

$$\begin{aligned} p_{n+1} - p_n &\ll p_n^{0.525} && \text{(unconditional)} \quad [1] \\ p_{n+1} - p_n &\ll p_n^{\frac{1}{2}}\log p_n && \text{(on RH)} \quad [14] \\ p_{n+1} - p_n &= o\big((p_n\log p_n)^{\frac{1}{2}}\big) && \text{(on RH \& PC)} \quad [38] \end{aligned} \tag{52}$$

8. Primes in arithmetic progressions

The theory of Dirichlet L-functions parallels that of $\zeta(s)$ for the most part although $L(s,\chi)$ doesn't have a pole at $s=1$ for nonprincipal χ. But a major trouble is encountered in the calculation of the zero-free region. The analogue of the inequality used for $\zeta(s)$ is $3\frac{L'}{L}(\sigma,\chi_0)+\Re[4\frac{L'}{L}(\sigma+it,\chi)+\frac{L'}{L}(\sigma+2it,\chi^2)]\leq 0$. If χ is a real character, so that $\chi^2=\chi_0$, the argument doesn't work completely, and one cannot rule out the possibility of a real *exceptional zero* $\beta\in(1-\frac{c}{\log q},1)$ where c is an absolute constant, which can occur for at most one of the real nonprincipal characters modulo q. Of course, this often creates complications and limitations in dealing with many problems. It is believed that exceptional zeros don't exist, and the *Generalized Riemann Hypothesis* (GRH) states that all zeros of Dirichlet's L-functions lie on the line $\sigma=\frac{1}{2}$.

Analogous to (16), let

$$\psi(x;q,a):=\sum_{\substack{n\leq x\\ n\equiv a\ (\mathrm{mod}\ q)}}\Lambda(n). \tag{53}$$

We will take $(a,q)=1$ all throughout this section. Writing

$$\psi(x,\chi):=\sum_{n\leq x}\chi(n)\Lambda(n), \tag{54}$$

we have by (6),

$$\psi(x;q,a)=\frac{1}{\phi(q)}\sum_{\chi\ (\mathrm{mod}\ q)}\overline{\chi}(a)\psi(x,\chi). \tag{55}$$

Here one aims for a *prime number theorem for arithmetic progressions* of the type $\psi(x;q,a)=\frac{x}{\phi(q)}(1+o(1))$. Proceeding as in the proof of the prime number theorem, an explicit formula for $\psi(x,\chi)$ is obtained leading to

$$\psi(x;q,a)=\frac{x}{\phi(q)}-\frac{\overline{\chi_1}(a)x^{\beta_1}}{\phi(q)\beta_1}+O(xe^{-C'\sqrt{\log x}}) \tag{56}$$

uniformly for $q\leq\exp[C\sqrt{\log x}]$, where C' is a positive constant depending only on C, and χ_1 is the only real character to the modulus q, if it exists, for which $L(s,\chi_1)$ has an exceptional zero β_1. If the exceptional zero β (for characters to the modulus q) exists, then it is known to satisfy $1-\beta\gg\frac{1}{\sqrt{q}(\log q)^2}$ with a specifiable constant, and this leads to

$$\psi(x;q,a)=\frac{x}{\phi(q)}+O(xe^{-c\sqrt{\log x}}) \tag{57}$$

valid for $q \leq (\log x)^{1-\delta}$ for some fixed $\delta > 0$. This result is effective in the sense that the numerical value of both of the constants in (57) can be determined if the value of δ is given. Siegel showed that for any $\epsilon > 0$ there exists a positive number $C = C(\epsilon)$ such that $L(s, \chi) \neq 0$ for $s > 1 - Cq^{-\epsilon}$. The upper bound for β is thus greatly improved in a sense but by the nature of its proof this result is noneffective (i.e. it is not known how to assign a value to C corresponding to a given value of ϵ). It leads to the *Siegel-Walfisz theorem* (1936), the best unconditionally established result that (57) holds uniformly for $q \leq (\log x)^N$ for any fixed $N > 0$ with a constant $c = c(N)$ which is unspecifiable. Assuming GRH, one easily gets

$$\psi(x; q, a) = \frac{x}{\phi(q)} + O(x^{\frac{1}{2}} \log^2 x), \quad (q \leq x), \tag{58}$$

which is an asymptotic relation for q almost up to $x^{\frac{1}{2}}$.

The main inquiry is: For which ranges of the relevant variables are the primes evenly distributed in the permissible congruence classes modulo q, and to what extent and in which sense is this distribution regular? When various averages over q and a are taken, results that hold in greater ranges of the parameters can be obtained. The *Bombieri-Vinogradov theorem* (1965) says that given any constant $A > 0$, we have

$$\sum_{q \leq Q} \max_{y \leq x} \max_{\substack{a \\ (a,q)=1}} |\psi(y; q, a) - \frac{y}{\phi(q)}| \ll \frac{x}{(\log x)^A} \tag{59}$$

with $Q = \dfrac{x^{\frac{1}{2}}}{(\log x)^B}$ where $B = B(A)$. The meaning of the Bombieri-Vinogradov theorem is that the asymptotic formula for $\psi(x; q, a)$ usually holds for q roughly as large as $x^{\frac{1}{2}}$, almost the same extent GRH delivers for an individual $\psi(y; q, a)$.

The important ingredients in the now standard version of the proof of the Bombieri-Vinogradov theorem include the Siegel-Walfisz theroem, a so-called *large-sieve* result

$$\sum_{q \leq Q} \frac{q}{\phi(q)} \sum_{\chi}^{*} |\sum_{M+1}^{M+N} a_n \chi(n)|^2 \ll (N + Q^2) \sum_{M+1}^{M+N} |a_n|^2$$

(here $\sum_{\chi}^{*}$ denotes a sum over all primitive characters $\chi(\mathrm{mod} q)$), the *Pólya-Vinogradov inequality*

$$\sum_{M+1}^{M+N} \chi(n) \ll q^{\frac{1}{2}} \log q$$

for a nonprincipal character to the modulus q, and a simple identity due to Vaughan which simplifies Vinogradov's method for evaluating sums of the sort $\sum_{p\leq N} f(p)$ when f is oscillatory but not multiplicative. (For monotonic f the prime number theorem and partial summation usually suffices; for multiplicative f arguments involving Perron's summation formula such as (4) and the knowledge about the zero-free regions for $\zeta(s)$ and $L(s,\chi)$ are employed). The original proof of the Bombieri-Vinogradov theorem also used zero-density estimates for Dirichlet L-functions, it was Gallagher who first essentially avoided arguments that involve the critical strip, and then Vaughan's method provided further simplification.

The Bombieri-Vinogradov theorem is a very deep and useful result in number theory. So it was natural when Elliott and Halberstam [19] wondered whether it is possible that this theorem is valid for larger values of Q, in particular up to $x/(\log x)^B$. Friedlander and Granville [27], upon proving that this is not possible, cast the present form of the *Elliott-Halberstam conjecture* as the hope that the Bombieri-Vinogradov theorem is valid for Q up to $x^{1-\epsilon}$. They also conjectured the uniform estimates (with any fixed $\epsilon > 0$)

$$\psi(x;q,a) = \frac{x}{\phi(q)} + O((\frac{x}{q})^{\frac{1}{2}} x^{\epsilon}), \quad (q < x), \tag{60}$$

and

$$\psi(x;q,a) \ll_{\epsilon} \frac{x}{\phi(q)}, \quad (q < \frac{x}{(\log x)^{2+\epsilon}}). \tag{61}$$

With further averaging over the permissible residue classes a for each q, one has the *Barban-Davenport-Halberstam theorem* which reads in its asymptotic form (proved by Montgomery)

$$\sum_{q\leq Q} \sum_{\substack{1\leq a\leq q \\ (a,q)=1}} |\psi(x;q,a) - \frac{x}{\phi(q)}|^2 \sim Qx\log x, \quad (\frac{x}{(\log x)^A} \leq Q \leq x), \tag{62}$$

where $A > 0$ is any fixed number ([82, Thm. 17.2]). Upon GRH this holds for $x^{\frac{1}{2}}\log^2 x \leq Q \leq x$ ([25], [44]). Here the range of q is much longer than that for the Bombieri-Vinogradov theorem, but the mean-square error in the prime number theorem for arithmetic progressions is considered instead of the maxima in (59). For the average taken only over a there is Hooley's result [64], depending on GRH, that

$$\sum_{\substack{1\leq a\leq q \\ (a,q)=1}} \max_{u\leq x} |\psi(u;q,a) - \frac{u}{\phi(q)}|^2 \ll x(\log x)^4, \quad (q \leq x). \tag{63}$$

Hooley conjectured that this sum without the max behaves asymptotically as $x \log q$ in some ranges of q, and provided [63] evidence for his guess. The results of Friedlander and Goldston [25] also support this conjecture. Hooley [65] also did some work for the third moment

$$\sum_{q \le Q} \phi(q) \sum_{\substack{1 \le a \le q \\ (a,q)=1}} (\psi(x;q,a) - \frac{x}{\phi(q)})^3,$$

and showed that as $x \to \infty$ this quantity is

$$\ll (Qx \log x)^{\frac{3}{2}} + \frac{x^3}{(\log^A x)} \quad \text{if } Q = o(\frac{x}{\log x}),$$

and

$$= \frac{3}{\pi^2} Q^2 x \log^2 x + O(Q^2 x \log x \log^2(\frac{2x}{Q})) \quad \text{if } \frac{x}{\log x} \le Q \le x.$$

These results are consistent with the belief that

$$(\psi(x;q,a) - \frac{x}{\phi(q)}) \ll (\frac{x \log x}{\phi(q)})^{\frac{1}{2}}$$

in most cases for q up to $x/\log x$, and that $\psi(x;q,a) - \frac{x}{\phi(q)}$ is symmetrically distributed about its zero mean.

Although the asymptotic values of $\psi(x;q,a_1)$ and $\psi(x;q,a_2)$ are the same, estimates for their difference (or with $\pi(x;q,a)$ which is defined by the same summation as in (53) but with the summand 1) are also of interest. Chebyshev observed that $\pi(x;4,3) - \pi(x;4,1)$ is more often positive than negative. One simple reason for this is that 1 is a square modulo 4, and 3 isn't. Studies in this direction were taken up by Hardy and Littlewood, Landau, Pólya and continued by Turán, Knapowski, Staś and Wiertelak. In their works q is mostly taken to be either fixed or very small compared to x. For these we refer the reader to Ingham's tract [66], Turán's Collected Works Vol. 3 [111] and Pintz's review articles therein. Rubinstein and Sarnak [99], assuming GRH and that for each q the collection of nontrivial zeros of all $L(s,\chi)$ for primitive $\chi \pmod q$ are linearly independent over the rational numbers, characterized the moduli and residue classes for which Chebyshev type bias occurs and calculated the logarithmic densities for the set of x giving $\pi(x;q,a) - \pi(x;q,b) > 0$ for $q \ge 3$, $(ab,q) = 1$. As a continuation of these results and methods, Bays, Ford, Hudson and Rubinstein [3] examined the connections between small zeros of L-functions, class numbers of imaginary quadratic fields and Chebyshev's bias.

A very important result concerning the distribution of primes in arithmetic progressions is the unconditional *Brun-Titchmarsh theorem*

$$\pi(x;q,a) \leq \frac{cx}{\phi(q)\log(x/q)}, \quad (1 \leq q < x). \tag{64}$$

Here c is a constant (the theorem is known to hold with $c = 2$), and x is assumed to be sufficiently large. For $1 \leq q \leq x^{1-\epsilon}$ the upper-bound is at the expected order of magnitude. For $q > \sqrt{x}$, (64) says more than (58) which depends upon GRH. There has been considerable effort for proving (64) with smaller values of c (the theorem should be true with any $c > 1$). The critical barrier of $c = 2$ has been overcome for $x^{\alpha} < q < x^{\beta}$ for any fixed $0 < \alpha < \beta < 1$ (see Friedlander-Iwaniec [28]). From a similar improvement for small q, the nonexistence of exceptional zeros would follow as can be seen from (56).

Another famous problem in this topic is determining the size of the least prime in an arithmetic progression, denoted as $p_{\min}(a,q) := \min\{p : p \equiv a(\mathrm{mod}\, q)\}$. The Siegel-Walfisz theorem gives a very weak estimate. Upon discounting the small contribution of proper prime powers to $\psi(x;q,a)$ in (58), we see that GRH implies $p_{\min}(a,q) \ll q^2 \log^5 q$. In a pioneering deep work Linnik obtained $p_{\min}(a,q) \ll q^C$ with effectively computable constant. The best known value for the Linnik constant is $C = 5.5$ due to Heath-Brown [60]. It is conjectured that $C = 1 + \epsilon$ would work; it is easy to see that $p_{\min}(a,q) \ll o(q \log q)$ is false.

9. Additive questions about the primes

It has long been believed but not yet proved that there exist infinitely many twin primes, i.e. p and $p+2$ both prime. Brun (1919) showed that the series formed by the reciprocals of twin primes is convergent. His method involved the truncation of certain sums which arise in Legendre's formulation of Eratosthenes's sieve. This not only rendered the Eratosthenes sieve usable for his purpose, but also opened the way for the development of various sieve methods to be applied to many formerly unapproachable problems. For example, it is now known that $\pi_{(0,2)}(x)$, the number of prime $p \leq x$ such that $p+2$ is also prime, is $\lesssim 6.84 \prod_{p>2}(1 - \frac{1}{(p-1)^2})\frac{x}{(\log x)^2}$. (Of course for the twin primes problem one needs a lower bound which tends to infinity with x. A curious result due to Heath-Brown [58] is that the existence (in an appropriate sense) of exceptional zeros implies the infinitude of twin primes).

Hardy and Littlewood's [55] *prime r-tuples conjecture* for the number $\pi_{\mathbf{d}}(N)$ of positive integers $n \le N$ for which $n+d_1, \dots, n+d_r$ are all prime (here r is fixed, $d_1, \dots, d_r$ are distinct integers and $\mathbf{d} = (d_1, \dots, d_r)$) in the form of an asymptotic formula is

$$\pi_{\mathbf{d}}(N) \sim \mathfrak{S}(\mathbf{d}) \frac{N}{\log^r N}, \quad (N \to \infty) \tag{65}$$

when $\mathfrak{S}(\mathbf{d}) \neq 0$, where

$$\mathfrak{S}(\mathbf{d}) = \prod_p \frac{p^{r-1}(p - \nu_{\mathbf{d}}(p))}{(p-1)^r}, \tag{66}$$

and $\nu_{\mathbf{d}}(p)$ is the number of distinct residue classes modulo p occupied by $d_1, \dots, d_r$. A strong form of the conjecture with an error term is

$$\sum_{n=1}^{N} \prod_{i=1}^{r} \Lambda(n+d_i) = \mathfrak{S}(\mathbf{d}) N + E_r(N, \mathbf{d}), \quad E_r(N, \mathbf{d}) \ll_{\epsilon, r} N^{\frac{1}{2}+\epsilon}, \tag{67}$$

uniformly for $|d_i| \le N$. The $r = 1$ case of (65) is the prime number theorem. For $r \ge 2$ the conjecture remains unproved for any $\mathbf{d}$. The heuristics for arriving at the r-tuples conjecture in the case $r = 2$, $d_1 = 0$, $d_2 = 2$ (see Hardy and Wright [56, §22.20]), is based on counting the number of positive integers $\le x$ which are relatively prime to $\prod_{p \le \sqrt{x}} p$ in two ways, using Mertens's result (9) and using the prime number theorem, that leads to a discrepancy by a factor of $2e^{-\gamma}$. The error lies in the calculation that uses (9), because it involves the assumption that the number of such integers in an interval is always proportional to the length of the interval, even if the interval is very short as in this application. The conjectural step comes in when this reasoning is adopted for pairs of such integers, and the square of the correction factor $e^{\gamma}/2$ is introduced. Let us also mention in this context, that Hensley and Richards [62] proved that the conjecture $\pi(x+y) \le \pi(x) + \pi(y)$ is incompatible with the prime r-tuples conjecture.

Assuming that for each r, (65) holds uniformly for $1 \le d_1, \dots, d_r \le h$, Gallagher [30] showed that if $P_k(h, N)$ is the number of integers $n \le N$ for which the interval $(n, n+h]$ contains exactly k primes, then $P_k(\lambda \log N, N) \sim N \frac{e^{-\lambda} \lambda^k}{k!}$ as $N \to \infty$, i.e. the distribution tends to the Poisson distribution with parameter λ. Numerical studies [109] indicate that small primes seem to obey Gaussian Orthogonal Ensemble statistics and as more primes are included there is a transition towards Poisson statistics.

Assuming the conjecture (67) for $1 \le r \le K$, Montgomery and Soundararajan [85] calculated the K-th moment for the primes in short

intervals as

$$\sum_{n=1}^{N}(\psi(n+h)-\psi(n)-h)^K = \mu_K h^{\frac{K}{2}} \int_1^N (\log(\frac{x}{h}+b)^{\frac{K}{2}}\, dx \qquad (68)$$
$$+O(N(\log N)^{\frac{K}{2}} h^{\frac{K}{2}} (\frac{h}{\log N})^{-\frac{1}{8K}} + h^K N^{\frac{1}{2}+\epsilon}),$$

uniformly for $\log N \leq h \leq N^{\frac{1}{K}}$, where $\mu_K = 1 \cdot 3 \cdots (K-1)$ if K is even, and $\mu_K = 0$ if K is odd, and $b = 1 - \gamma - \log 2\pi$. We notice that in the case $K = 1$ the assumption is equivalent to RH, and for $K = 2$ the assumption is equivalent to a strong form of PC. Later on Chan [8] obtained the same result under the weaker assumption that for $N \geq h$,

$$\sum_{\substack{1 \leq d_i \leq h \\ i=1,\ldots,r}} E_r(N, \mathbf{d})^2 \ll_r N^{1+\epsilon} h^r.$$

Montgomery and Soundararajan conjectured that the right-hand side of (68) continues to be $(\mu_K + o(1))N(h \log N/h)^{K/2}$ uniformly for $(\log N)^{1+\delta} \leq h \leq N^{1-\delta}$, and that this conjecture is equivalent to

$$\int_1^X (\sum_{0<\gamma\leq T} \cos(\gamma \log x))^k\, dx = (\mu_k + o(1))X(\frac{T}{4\pi}\log T)^{\frac{k}{2}},$$

where the γ run through the ordinates of the zeta zeros.

One of the oldest unsolved problems concerning primes is the *Goldbach conjecture* (1742) that every even number > 2 is the sum of two prime numbers. Beginning with the work of Brun on sieve methods the furthest achievement in this direction is the theorem of Chen from 1966 [9], that every sufficiently large even number can be expressed as the sum of a prime and a number which has at most two prime factors - counted with multiplicity. Pintz [94], making a great improvement over former results, has shown that the number of even integers $\leq x$ which are not expressible as a sum of two primes is $O(x^{\frac{2}{3}})$. In this context we note that Schnirelman (1930) proved by developing a quite simple method that there exists a constant C such that every natural number > 1 can be expressed as a sum of at most C primes. Ramaré's work [96] shows that $C = 7$ suffices. Vinogradov (1937), using his method of estimating exponential sums, proved that every sufficiently large odd number can be expressed as a sum of three primes (see [16]), from which it immediately follows that every sufficiently large integer can be expressed as a sum of at most 4 primes. As for conditional results, it is known that RH implies $C = 6$ is fine, while GRH allows Vinogradov's result for all odd numbers > 5 and this makes $C = 4$ sufficient.

The root of the difficulty in such conjectures is that they involve constraints of an additive nature on the primes which are defined in terms of the operation of multiplication. So what needs to be understood deeply is the relation between the operations of addition and multiplication, which are linked only by the distributive law. Some mathematicians, e.g. Knuth [75], think that Goldbach's conjecture may well be true but there is no rigourous way to prove it. It might be one of the unprovable assertions that Gödel showed exist (and it is known that in some sense almost all correct statements about mathematics are unprovable).

Schinzel formulated two grand conjectures which embody the Goldbach and twin-prime conjectures as well as many other questions. Let $P_i(n)$ $(i = 1, \ldots, r)$ be distinct irreducible polynomials in $\mathbb{Z}[x]$ having positive leading coefficients such that the product $P = P_1 \cdots P_r$ has no fixed prime divisor. The first conjecture is: There exist infinitely many $n \in \mathbb{Z}$ such that each $P_i(n)$ is prime. The second conjecture is: Let $N \in \mathbb{N}$ and $G \in \mathbb{Z}[x]$ be another polynomial with positive leading coefficient such that $N - G$ is irreducible, and also such that $(N - G)P$ has no fixed prime divisor. For all sufficiently large N, there exists $n \in \mathbb{Z}^+$ such that $N - G(n) > 0$ and each of $N - G(n), P_1(n), \ldots, P_r(n)$ is prime. Iwaniec [70] showed that any inhomogeneous irreducible quadratic polynomial in two variables which depends essentially on both of the variables, and whose coefficients are integers without a common factor takes infinitely many prime values. Iwaniec also proved an asymptotic formula for the number of these primes $\leq z$ as $z \to \infty$. In this case, as well as in the previously dealt cases of the prime number theorem and binary quadratic forms, the number $N(z)$ of the values of the argument of the polynomial for which the value of the polynomial is $\leq z$ satisfies $N(z) \gg z$. Fouvry and Iwaniec [21] proved an asymptotic formula for the number of primes represented by $x^2 + p^2$ (where p is a prime), in which case $N(z) \ll z/\log z$. In a later development, Friedlander and Iwaniec [29] settled the problem for $x^2 + y^4$, which is a quite sparse sequence with $N(z) = O(z^{\frac{3}{4}})$. More recently Heath-Brown [61] worked out the problem for the even sparser sequence $x^3 + 2y^3$ with $N(z) = O(z^{\frac{2}{3}})$ in which case the homogeneity of the polynomial is helpful. In the case of $x^2 + 1$, Iwaniec [71] showed that it is infinitely often a number having at most two (not necessarily distinct) prime factors.

A recent major development in a question of additive nature took place when Green and Tao [51] showed that the primes contain arbitrarily long arithmetic progressions. Their proof makes use of combinatorial methods, harmonic analysis and ergodic theory in addition to methods of analytic

number theory.

10. Primes in short intervals

After the prime number theorem it is natural to ask for which functions $\Phi(x)$, as $x \to \infty$,

$$\pi(x + \Phi(x)) - \pi(x) \sim \frac{\Phi(x)}{\log x}. \tag{69}$$

Here one would try to find $\Phi(x)$ as slowly increasing as possible. Heath-Brown [59] proved that one can take $\Phi(x) = x^{\frac{7}{12}-\epsilon(x)}$ ($\epsilon(x) \to 0$, as $x \to \infty$), and $\Phi(x) = x^{\frac{1}{2}+\epsilon}$ is allowed if RH is assumed. The gap between these upper-bounds and the known lower-bounds is huge. We know due to Rankin [97] that (69) doesn't hold with

$$\Phi(x) = c\frac{\log x \log\log x \log\log\log\log x}{(\log\log\log x)^2}, \tag{70}$$

because Rankin showed that there exists a sequence of values of x tending to ∞ with intervals around x of length given in (70) which don't contain a prime. This is the best proved order of magnitude for the largest gaps between consecutive primes. Maier [77] generalized this to the existence, for any fixed k, of k consecutive gaps between primes each of size at the order of magnitude (70). (This in turn was generalized to the case of arithmetic progressions by Shiu [105]). On the other hand Selberg [102] showed assuming RH that, (69) holds for almost all x if $\dfrac{\Phi(x)}{(\log x)^2} \to \infty$ as $x \to \infty$. Here what is meant by 'almost all x' is that, while $X \to \infty$ the measure of the set of $x \in [0, X]$ for which (69) doesn't hold is $o(X)$. Without assuming RH, this almost-all result is known to hold with $\Phi(x) = x^{\frac{1}{6}-\epsilon}$ (Zaccagnini [114]). Whether Selberg's result is true without exceptions or not was answered by Maier [78] who showed that exceptions to (69) exist with $\Phi(x)$ as large as $(\log x)^\lambda$ with any fixed $\lambda > 1$, i.e.

$$\limsup_{x\to\infty} \frac{\pi(x + (\log x)^\lambda) - \pi(x)}{(\log x)^{\lambda-1}} > 1, \ \liminf_{x\to\infty} \frac{\pi(x + (\log x)^\lambda) - \pi(x)}{(\log x)^{\lambda-1}} < 1. \tag{71}$$

By the prime number theorem the difference between consectuive primes, $p_{n+1} - p_n$ is on average $\sim \log p_n$. Cramér [15] conjectured upon probabilistic reasoning that the largest possible gap between consecutive primes satisfies $\limsup_{n\to\infty} \dfrac{p_{n+1} - p_n}{(\log p_n)^2} = 1$, but now it is widely thought that

$$p_{n+1} - p_n = O(\log^2 p_n) \tag{72}$$

is a safer conjecture. Cramér's reasoning was based on the simple model that the probability of n being a prime is approximately $1/\log n$, and that this can be taken into account independently for different integers (which is the basic flaw in Cramér's model; for example, n and $n+2$ both being primes are not independent events: if n is even we automatically know that $n+2$ can't be prime). Since Rankin's estimate (70), only the value of the constant c in (70) has been improved (see [80]). The estimates in (51) and (52), even under very strong conjectures for the zeta zeros, fall dismally short of (72). Naturally the more that is known or assumed about the zeta zeros, the stronger results are deduced on the distribution of primes, notwithstanding the zeta zeros by themselves do not pertain steadfastly to primes as

$$\zeta^*(s) = \prod_{n=1}^{\infty}(1-\frac{1}{q_n^s})^{-1} \quad (p_n \le q_n \le p_{n+1}),$$

considered by Grosswald and Schnitzer [52], reveals. This product converges absolutely for $\sigma > 1$ where it doesn't vanish, it can be analytically continued to $\sigma > 0$ and then it is seen that $\zeta^*(s)$ has the same zeros as $\zeta(s)$ in $\sigma > 0$. But some significant properties of $\zeta(s)$ are not valid for $\zeta^*(s)$, namely the analytic continuation is not possible beyond $\sigma > 0$ so that for $\zeta^*(s)$ there is no functional equation, and it has a simple pole at $s = 1$ with residue r, $\frac{1}{2} \le r \le 1$.

As for small gaps between primes, there has been considerable progress recently. In the 1990's Goldston [35] developed a method which gives lower bounds of the correct order of magnitude in many problems about the distribution of primes. This method rested upon using short divisor sum approximations to the von Mangoldt function such as

$$\Lambda_R(n) := \sum_{d|n,\, d\le R} \mu(d)\log(\frac{R}{d}),$$

with a parameter R to be chosen as large as possible in an application because without the condition $d \le R$ this sum is equal to $\Lambda(n)$ for $n > 1$. After a sequence of works by Goldston et. al. either concerning various applications or for improving the results by employing better approximants, Goldston, Pintz and the author in [40] and [42] have reached

$$\liminf_{n\to\infty} \frac{p_{n+r}-p_n}{\log p_n} \le e^{-\gamma}(\sqrt{r}-1)^2 \tag{73}$$

for any fixed positive integer r. With $r = 1$ this shows that for any fixed $\epsilon > 0$, there are infinitely many consecutive primes differing by less than ϵ

times the average gap. Through a more refined analysis in [41] the sharper result

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\sqrt{\log p_n}(\log\log p_n)^2} \leq \infty \tag{74}$$

was obtained. The method also allows a generalization of (73) to primes in arithmetic progressions where the modulus q can grow with the size N of the primes subject to $q \ll_A (\log\log N)^A$. Furthermore, it turns out somewhat surprisingly, the assumption that (59) holds with $Q = x^{\theta-\epsilon}$ for any fixed $\theta \in (\frac{1}{2}, 1]$ implies that there exist bounded gaps between primes infinitely often, the size of the gaps being a function of θ. This is an instance revealing the importance and strength of the Bombieri-Vinogradov theorem, and that showing its result continues to hold beyond $\theta = \frac{1}{2}$ will be an utmost breakthrough.

Together with Graham the same authors applied their methods to the problem of small gaps between E_2-numbers q_n. Corresponding to (73), it was shown in [36] that

$$\liminf_{n\to\infty} q_{n+r} - q_n \leq C(r) \tag{75}$$

for a constant $C(r)$, in particular $C(1) = 6$. The ideas involved in this work also yielded in [37] stronger variants of the Erdös-Mirsky conjecture: There are infinitely many integers n which simultaneously satisfy $d(n) = d(n+1)$, $\Omega(n) = \Omega(n+1)$, $\omega(n) = \omega(n+1)$, even by specifying the value of these functions along with generalizations to shifts $n+b$ with an arbitrary positive integer b (here $d(n)$, $\Omega(n)$, $\omega(n)$ denote respectively the number of positive integer divisors of n, the number of prime divisors of n counted with multiplicity, and the number of distinct prime divisors of n).

Suggestions for further reading

In addition to the articles and books cited in the text we suggest the following works for a presentation of the topics and the proofs.

Section 2: Dickson's three volume set [17] is a compendium of results in number theory up to approximately 1920. The book by Hardy and Wright [56] is a standard reference for most topics of elementary number theory.

Sections 3, 4 & 8: For detailed introductions to the topics of these sections we refer the reader to the books by Davenport [16], and by Montgomery and Vaughan [87].

Sections 4 & 5: Titchmarsh's book (with notes added by Heath-Brown for the 2nd edition) [110] is a classic treatise on the Riemann zeta-function.

There are other treatises devoted to the theory of $\zeta(s)$, notably those of Edwards [18], Ivic [69], Karatsuba and Voronin [74]. The last two books contain a proof of (21) and (22). Elementary proofs of the prime number theorem are given in Hardy and Wright [56], and in the introductory level book by Tenenbaum and Mendes-France [108]. The articles by Bombieri [6], Sarnak [101], and Conrey [11] are recent essays on the Riemann Hypothesis by three of the leading experts in the field.

Section 6: A classical book on the subject which includes the proof of (26) is Ingham's tract [66].

Section 7: For further details on the pair correlation conjecture and prime numbers we refer the reader to Goldston's survey article [33]. The n-level correlations of zeros of $\zeta(s)$ were studied by Bogomolny and Keating [4] using heuristic arguments and based on the Hardy-Littlewood conjecture (equations (65)-(66) above with $r = 2$), and rigorously by Rudnick and Sarnak [100]. For the theory of random matrices, correlation functions and relations of zeta zeros to eigenvalues of a Hermitian operator the reader may consult the book by Mehta [81].

Section 8: The survey article by Iwaniec [72] gives an overview of the current directions in prime number theory. In a series of three papers, the last being [7], Bombieri, Friedlander and Iwaniec obtained improvements in some directions (not including the version stated in §8) on the Bombieri-Vinogradov theorem. Concerning the Barban-Davenport-Halberstam theorem there are the works of Hooley titled 'On the Barban - Davenport - Halberstam theorem I – XVIII'), and of Friedlander and Goldston [26]. The books by Montgomery [82], and Bombieri [5] contain further treatment of most of the topics of this section. For the Brun-Titchmarsh theorem see Friedlander's survey article [22].

Section 9: The methods of attacking problems having an additive nature, sieve methods, and the conjectures on the distribution of primes mentioned in this section can be found at an introductory level in Friedlander [24], Greaves [49] and Nathanson [89]. At more advanced levels there are the books of Greaves [50], Halberstam and Richert [53], and Vaughan [112]. The article by Kra [76] presents an introduction to the ideas in Green and Tao's work.

Section 10: Maier's papers listed in the references brought forth important developments in prime number theory. For comments on the error terms in the prime number theorem for arithmetic progressions, and for the consequences of Maier's work we refer the reader to Friedlander's survey article [23]. For Cramér's model, Maier's method and related matters on

the distribution of primes we refer the reader to the articles by Granville [47], [48], Pintz [95] and Soundararajan [106], [107]. The last of these articles is mainly concerned with the problem of small gaps between primes. The developments leading to the results of Goldston, Pintz and Yıldırım are recounted in [43].

It is much easier to find the articles of Riemann, Hardy, Littlewood and Selberg from their collected works. Some of the original articles which have shaped the development of the theory in the 20th century have been collected in a book edited by Wang [113]. And most of the recent articles can be found in the websites of the authors.

References

1. R. C. Baker, G. Harman and J. Pintz, *Proc. London Math. Soc. (3)* **83**, 532-562 (2001).
2. P. T. Bateman, J. W. Brown, R. S. Hall, K. E. Kloss and R. M. Stemmler, Linear relations connecting the imaginary parts of the zeros of the zeta function, in *Computers in Number Theory* (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969), Academic Press, London, 1971, pp. 1-19.
3. C. Bays, K. Ford, R. H. Hudson and M. Rubinstein, *J. Number Theory* **87**, 54-76 (2001).
4. E. B. Bogomolny and J. P. Keating, *Nonlinearity* **9**, 911-935 (1996).
5. E. Bombieri, *Le grand crible dans la théorie analytique des nombres*; *Astérisque* **18** (1987/1974), (Société Mathématique de France, 1987).
6. E. Bombieri, (2000), `http://www.claymath.org/library/MPP.pdf`, pp. 99-111.
7. E. Bombieri, J. B. Friedlander and H. Iwaniec, *J. Amer. Math. Soc.* **2**, no. 2, 215-224 (1989).
8. T. H. Chan, *Int. J. Number Theory* **2**, no.1, 105-110 (2006).
9. J. Chen, *Sci. Sinica* **16**, 157-176 (1973).
10. J. B. Conrey, *J. Reine Angew. Math.* **399**, 1-26 (1989).
11. J. B. Conrey, *Notices Amer. Math. Soc.* **50**, no.3, 341-353 (2003).
12. J. B. Conrey, L-functions and random matrices, in *Mathematics unlimited - 2001 and beyond*, Springer-Verlag, Berlin, 2001, pp. 331-352.
13. J. B. Conrey, Notes on L-functions and random matrix theory, in *Frontiers in Number Theory, Physics and Geometry I*, Springer-Verlag, Berlin, 2006, pp. 107-162.
14. H. Cramér, *Ark. Mat. Astronom. Fys.* **15**, 1-32 (1920).
15. H. Cramér, *Acta Arith.* **2**, 23-46 (1936).
16. H. Davenport, *Multiplicative number theory*, 3rd edn., revised and with a preface by H. L. Montgomery, Springer-Verlag, New York, 2000.
17. L. E. Dickson, *History of the theory of numbers* (3 vol.s), 1923, reprinted, Amer. Math. Soc., Providence, 2002.
18. H. M. Edwards, *Riemann's zeta function*, 1974, reprinted, Dover, New York, 2001.

19. P. D. T. A. Elliott and H. Halberstam, *Symposia Mathematica* **4** (INDAM, Rome, 1968/69), Academic Press, London, 1970, pp. 59-72.
20. P. Erdös, *Proc. Nat. Acad. Sci.* **35**, 374-384 (1949).
21. E. Fouvry and H. Iwaniec, *Acta Arith.* **79**, no. 3, 249-287 (1997).
22. J. B. Friedlander, On the Brun-Titchmarsh theorem, in *Number Theory, Trace Formulas and Discrete Groups* (Selberg Symposium, Oslo, 1987) (eds. Aubert, Bombieri and Goldfeld), Academic Press, Boston, 1989, pp 219-228.
23. J. B. Friedlander, Irregularities in the distribution of primes, in *Advances in number theory* (Kingston, ON, 1991), (ed.s Gouvêa and Yui) Oxford Univ. Press, New York, 1993, pp. 17-30.
24. J. B. Friedlander, Topics in analytic number theory, in *Number Theory and its Applications* (Ankara, 1996), (ed.s Yıldırım and Stepanov), Lecture Notes in Pure and Applied Math. **204**, Marcel Dekker, New York, 1999, pp. 47-64.
25. J. B. Friedlander and D. A. Goldston, *Quart. J. Math. Oxford (2)* **47**, 313-336 (1995).
26. J. B. Friedlander and D. A. Goldston, Note on a variance in the distribution of primes, in *Number theory in progress, Vol. 2* (Zakopane, 1997), (ed.s György, Iwaniec and Urbanowicz), de Gruyter, Berlin, 1999, pp. 841-848.
27. J. B. Friedlander and A. Granville, *Ann. of Math.(2)* **129**, no. 2, 363-382 (1989).
28. J. B. Friedlander and H. Iwaniec, The Brun-Titchmarsh theorem, in *Analytic number theory (Kyoto 1996)*, London Math. Soc. Lect. Note Ser. **247**, Cambridge Univ. Press, 1997, pp. 85-93.
29. J. B. Friedlander and H. Iwaniec, *Ann. of Math. (2)* **148**, no. 3, 945-1040 (1998).
30. P. X. Gallagher, *Mathematika* **23**, 4-9 (1976).
31. P. X. Gallagher, *Acta Arithmetica* **37**, 339-343 (1980).
32. D. Goldfeld, `http://www.math.columbia.edu/~goldfeld/ErdosSelbergDispute.pdf`
33. D. A. Goldston, `http://aimath.org/preprints.html`, Preprint 2004-28.
34. D. A. Goldston, *J. Number Theory* **27**, no. 2, 149-177 (1987).
35. D. A. Goldston, *Expo. Math.* **13**, 366-376 (1995).
36. D. A. Goldston, S. W. Graham, J. Pintz and C. Y. Yıldırım, `http://arxiv.org/PS_cache/arxiv/pdf/0609/0609615v1.pdf`
37. D. A. Goldston, S. W. Graham, J. Pintz and C. Y. Yıldırım, `http://arxiv.org/PS_cache/arxiv/pdf/0803/0803.2636v1.pdf`
38. D. A. Goldston and D. R. Heath-Brown, *Math. Ann.* **266**, 317-320 (1984).
39. D. A. Goldston and H. L. Montgomery, Pair correlation of zeros and primes in short intervals, in *Analytic Number Theory and Diophantine Problems, Proc. of a conference at Oklahoma State Univ. 1984*, (ed.s Adolphson, Conrey, Ghosh and Yager), Birkhäuser Boston 1987, pp. 183-203.
40. D. A. Goldston, J. Pintz and C. Y. Yıldırım, to appear in *Ann. of Math.* `http://arxiv.org/PS_cache/arxiv/pdf/0508/0508185v1.pdf`
41. D. A. Goldston, J. Pintz and C. Y. Yıldırım, `http://arxiv.org/PS_cache/arxiv/pdf/0710/0710.2728v1.pdf`
42. D. A. Goldston, J. Pintz and C. Y. Yıldırım, *Funct. Approx. Comment.*

Math. **35**, 79-89 (2006).
43. D. A. Goldston, J. Pintz and C. Y. Yıldırım, The path to recent progress on small gaps between primes, in *Analytic Number Theory, Clay Math. Proc.* **7**, Amer. Math. Soc., Providence, 2007, pp. 129-139.
44. D. A. Goldston and R. C. Vaughan, On the Montgomery-Hooley asymptotic formula, in *Sieve methods, exponential sums, and their applications to number theory (Cardiff, 1995)* London Math. Soc. Lecture Note Ser. **237**, Cambridge Univ. Press, 1997, pp. 117-142.
45. S. M. Gonek, An explicit formula of Landau and its applications to the theory of the zeta-function, in *A tribute to Emil Grosswald: Number theory and related analysis* (ed.s Knopp and Sheingorn) Contemporary Math. **143**, Amer. Math. Soc., Providence, 1993, pp. 395-413.
46. X. Gourdon, (2004), `http://numbers.computation.free.fr/Constants/Miscellaneous/zetazeros1e13-1e24.pdf`
47. A. Granville, *Scand. Actuarial J.*, no.1, 12-28 (1995).
48. A. Granville, Unexpected irregularities in the distribution of prime numbers, in *Proc. International Congress of Mathematicians, Zurich 1994*, Birkäuser, Basel, 1995, pp. 388-399.
49. G. Greaves, Sieve methods, in *Number Theory and its Applications* (Ankara, 1996), (ed.s Yıldırım and Stepanov), Lecture Notes in Pure and Applied Math. **204**, Marcel Dekker, NY, 1999, 65-107.
50. G. Greaves, *Sieves in Number Theory*, Springer-Verlag, Berlin, 2001.
51. B. Green and T. Tao, *Ann. of Math. (2)* **167**, no. 2, 481-547 (2008).
52. E. Grosswald and F. J. Schnitzer, *Pacific J. Math.* **74**, no.2, 357-364 (1978).
53. H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.
54. G. H. Hardy, *Matematisk Tidsskrift B*, 1-16 (1922).
55. G. H. Hardy and J. E. Littlewood, *Acta Mathematica* **44**, 1-70 (1922).
56. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., Oxford Univ. Press, 1985.
57. D. R. Heath-Brown, *Acta Arithmetica* **XLI**, 85-99 (1982).
58. D. R. Heath-Brown, *Proc. London Math. Soc. (3)* **47**(2), 193-224 (1983).
59. D. R. Heath-Brown, *J. Reine Angew. Math.* **389**, 22-63 (1988).
60. D. R. Heath-Brown, *Proc. London Math. Soc. (3)* **64**(2), 265-338 (1992).
61. D. R. Heath-Brown, *Acta Math.* **186** no. 1, 1-84 (2001).
62. D. Hensley and I. Richards, On the incompatibility of two conjectures concerning primes, in *Proc. Symp. Pure Math.* **24**, Amer. Math. Soc., Providence, 1973, pp. 181-193.
63. C. Hooley, *J. London Math. Soc. (2)* **11**, 399-407 (1975).
64. C. Hooley, *J. London Math. Soc. (2)* **13**, 57-64 (1976).
65. C. Hooley, *J. Reine Angew. Math.* **499**, 1-46 (1998).
66. A. E. Ingham, *The distribution of prime numbers*, 1932, reprinted with a foreword by R. C. Vaughan, Cambridge Univ. Press, 1992.
67. A. E. Ingham, *Amer. J. Math.* **64**, 313-319 (1942).
68. A. E. Ingham, (1949), `http://www.ams.org/mathscinet/pdf/29411.pdf`
69. A. Ivic, *The Riemann zeta-function*, 1985, reprinted, Dover, New York, 2003.

70. H. Iwaniec, *Acta Arith.* **24**, 435-459, (1973/74).
71. H. Iwaniec, *Invent. Math.* **47** no. , 171-188, (1973/74).
72. H. Iwaniec, Prime numbers and L-functions, in *Proc. International Congress of Mathematicians, Madrid, 2006*, Eur. Math. Soc., Zurich, 2007, pp. 279-306.
73. W. B. Jurkat, The Mertens conjecture and related general Ω-theorems, in *Proc. Symp. Pure Math.* **24** (Amer. Math. Soc., Providence, 1973), pp. 147-158.
74. A. A. Karatsuba and S. M. Voronin, *The Riemann zeta-function* (translated from the Russian by N. Koblitz), de Gruyter, Berlin, 1992.
75. D. Knuth, *Notices Amer. Math. Soc.* **49**, no. 3, 318-324 (2002).
76. B. Kra, *Bull. Amer. Math. Soc. (N.S.)* **43**, no. 1, 3-23 (2006).
77. H. Maier, *Adv. in Math.* **39**, no. 3, 257-269 (1981).
78. H. Maier, *Michigan Math. J.* **32**, no. 2, 221-225 (1985).
79. H. Maier, *Michigan Math. J.* **35**, (1988), no. 3, 323-344.
80. H. Maier and C. Pomerance, *Trans. Amer. Math. Soc.* **322**, no. 1, 201-237 (1990).
81. M. L. Mehta, *Random Matrices*, 3rd ed., Elsevier/Academic Press, 2004.
82. H. L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Math. **227**, Springer, Berlin, 1971.
83. H. L. Montgomery, The pair correlation of zeros of the zeta function, in *Proc. Symp. Pure Math.* **24**, Amer. Math. Soc., Providence, 1973, pp. 181-193.
84. H. L. Montgomery, The zeta function and prime numbers in *Proc. Queen's Number Theory Conference, 1979*, Queen's Papers in Pure and Appl. Math. **54**, Queen's University, Kingston, Ont., 1980, pp. 1-31.
85. H. L. Montgomery and K. Soundararajan, *Commun. Math. Phys.* **252**, 589-617 (2004).
86. H. L. Montgomery and R. C. Vaughan, *J. London Math. Soc. (2)* **8**, 73-82, (1974).
87. H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge University Press, 2007.
88. M. R. Murty, *J. Madras Univ.*, 161–169 (1988);
or `http://www.math.mast.queensu.ca/~murty/index2.html`
89. M. B. Nathanson, *Additive Number Theory, The Classical Bases*, Springer-Verlag, New York, 1996.
90. A. M. Odlyzko, `http://www.dtc.umn.edu/~odlyzko/`
91. A. M. Odlyzko and H. J. J. te Riele, *J. Reine Angew. Math.* **357**, 138-160 (1985).
92. J. Pintz, On the remainder term of the prime number formula and the zeros of Riemann's zeta-function, in *Lec. Notes in Math.* **1068** (ed. H. Jager), Springer-Verlag, Berlin, 1984, pp. 186-197.
93. J. Pintz, *Acta Math. Hungar.* **58** no. 3-4, 383-387 (1991).
94. J. Pintz, Approximations to the Goldbach and twin prime problem and gaps between consecutive primes, in *Adv. Studies in Pure Math.* **43**, Int. Conference on Probability and Number Theory, Kanazawa, 2005, (2006), pp. 1-40.

95. J. Pintz, *Functiones et Approximatio* **XXXVII.2**, 361-376 (2007).
96. O. Ramaré, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* **22**, 645-706, (1995).
97. R. A. Rankin, *J. London Math. Soc.* **13**, 242-247 (1938).
98. B. Riemann, *Monatsberichte d. Preuss. Akad. d. Wissens.*, 671–680 (1859).
99. M. Rubinstein and P. Sarnak, *Experimental Math.* **3**, 173-197 (1994).
100. Z. Rudnick and P. Sarnak, *C.R. Acad. Sci. Paris* **319**, Série I, 1027-1032 (1994).
101. P. Sarnak, (2004), `http://www.claymath.org/library/04report_sarnak.pdf`
102. A. Selberg, *Arch. Math. Naturvid.* **47**, no. 6, 87-105 (1943).
103. A. Selberg, *Ann. of Math.* **50**, 305-313 (1949).
104. A. Selberg, *Ann. of Math.* **50**, 297-304 (1949).
105. D. K. L. Shiu, *J. London Math. Soc. (2)* **61**, no. 2, 359-373 (2000).
106. K. Soundararajan, The distribution of prime numbers, in *Equidistribution in number theory, an introduction*, NATO Sci. Ser. II. Math. Phys. Chem. **237**, Springer, Dordrecht, 2007, pp. 59-83.
107. K. Soundararajan, *Bull. Amer. Math. Soc. (N.S.)* **44**, no. 1, 1-18 (2007).
108. G. Tenenbaum and M. Mendes-France, *The prime numbers and their distribution* (translated from the French), Amer. Math. Soc, Providence, 2000.
109. T. K. Timberlake and J. M. Tucker, (2008), `http://arxiv.org/PS_cache/arxiv/pdf/0708/0708.2567v2.pdf`
110. E. C. Titchmarsh, *The theory of the Riemann zeta-function*, 2nd ed. revised by D.R. Heath-Brown, Oxford Univ. Press, 1986.
111. P. Turán, *Collected papers of Paul Turán, Vol. 3*, ed. P. Erdös Akademiai Kiado, Budapest, 1990.
112. R. C. Vaughan, *The Hardy-Littlewood method*, 2nd ed., Cambridge Univ. Press, 1997.
113. Y. Wang (editor), *The Goldbach Conjecture*, 2nd ed., World Scientific, Singapore, 2002.
114. A. Zaccagnini, *Acta Arith.* **84**, no. 3, 225-244, (1998).