# An Introduction to Analytic Number Theory

*Ilan Vardi*
IHES, Bures-sur-Yvette

December 14, 1998

[summary by Cyril Banderier and Ilan Vardi]

## 1. Introduction

> "Le plus court chemin entre deux vérités dans le domaine réel passe par le domaine complexe.[1] "
>
> J. Hadamard.

The above quote captures the depth analysis can bring when one is confronted by number theoretic questions. The oldest and most fundamental of such questions is the study of prime numbers. The first question to be answered is: Are there an infinite number of primes? This can be answered by a number of simple proofs:

- Euclid: Assume there are a finite number of primes $p_1, \ldots, p_n$, then $p_1 p_2 \cdots p_n + 1$ is not divisible by any of the $p_i$'s, so any of its prime divisors yields a new prime number (Euclid only considered the case $n = 3$).
- Pólya: The Fermat numbers $F_n = 2^{2^n} + 1$ are pairwise relatively prime, so the set of their prime divisors must be infinite.
- Erdős: Fix $x$ and consider the primes $p_1, \ldots, p_n \le x$. Since every integer is the product of a perfect square and a squarefree number, one can write every integer $m \le x$ as $m = p_1^{e_1} \ldots p_n^{e_n} Q^2$, where $e_i \in \{0, 1\}$ and $Q^2 \le x$. There are $2^n$ choices for the $e_i$ and $\sqrt{x}$ choices for $Q$, so it follows that $n \ge \frac{\ln(x)}{2\ln(2)}$.
- Euler: One has the formal identity

$$\sum_n \frac{1}{n^s} = \prod_{p \,\text{prime}} \frac{1}{1 - p^{-s}} \tag{1}$$

which in fact holds for $\Re(s) > 1$. As $s \to 1$, the left hand side of (1) tends to $\infty$ since the harmonic series diverges, so there must be an infinite number of factors on the right.

This proof can be modified by noting that $\zeta(2) = \pi^2/6$, where $\zeta(s) = \sum 1/n^s$. If there were only a finite number of primes, then (1) would imply that $\pi^2$ is rational, proved false by Legendre in 1797, see also [6]. Several other proofs are given in [7].

A stronger version of this is due to Mertens: The finite version of (1) gives

$$\prod_p \frac{1}{1 - p^{-1}} > \sum_{n<x} \frac{1}{n} \sim \ln(x)\,,$$

[1] "The shortest path between two truths in the real domain passes through the complex domain."

and taking logs will give

$$\sum_{p<x} \frac{1}{p} \sim \ln\ln(x)\,, \tag{2}$$

and so there are an infinite number of primes.

Which of these is the "best" proof? One argument would say that it is the one which allows the best generalisation. For example, Euclid's proof easily shows that there are an infinite number of primes of the form $4k+3$ (consider $4p_1\cdots p_n - 3$), but seems to fall flat when trying to prove that the same holds for primes of the form $4k+1$ (one has to consider $4(p_1\cdots p_n)^2+1$). In general, one wants to demonstrate Dirichlet's assertion (that he proved in 1837, in [3]) "there are an infinite number of primes of the form $ak+b$, where $a$ and $b$ are relatively prime." It turns out that the proof of this deep fact uses a generalisation of Euler's method, i.e., equation (2):

$$\sum_{p\equiv a \pmod q} \frac{1}{p} = \infty \Leftrightarrow \text{ there are an infinite number of primes in } ak+q.$$

## 2. Dirichlet's theorem

Let $\chi$ be a multiplicative character, with period $q$, that it is to say a complex valued function $\chi(n)$ satisfying $\chi(mn)=\chi(m)\chi(n)$ and $\chi(0)=0$ (this implies that if $\chi(n)\neq 0$, then it is a root of unity and so has norm one). An example is the Legendre (or Jacobi if $q$ is not a prime) symbol

$$\chi(n) := \left(\frac{n}{q}\right) = \begin{cases} 0 & \text{if } q|n, \\ 1 & \text{if } x^2 \equiv n \pmod q \text{ for some } x \\ -1 & \text{otherwise.} \end{cases}$$

In fact, for odd $q$, there are exactly $\phi(q)$ multiplicative characters modulo $q$, all given by $\chi(n) := e^{2ik\pi\nu(n)/\phi(q)}$ for $0 \le b \le \phi(q)-1$ and where $n \equiv g^{\nu(n)} \pmod q$ for any fixed primitive root $g$ of the group of inversible elements. When $q$ is a power of 2, the definition is a little more cumbersome and for general $q$, it is the product of the characters of the odd and even factors of $q$.

The importance of characters is seen by the following *orthogonality relation*:

$$\frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)}\chi(n) = \begin{cases} 1 & \text{whenever } n \equiv a \pmod q, \\ 0 & \text{otherwise.} \end{cases} \tag{3}$$

which allows one to pick out an arithmetic progression. For his proof, Dirichlet introduced what are nowadays called Dirichlet $L$-functions, defined by

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

Taking logarithm leads to $\ln L(s,\chi) = \sum_p -\ln(1-\chi(p)p^{-s})$, thus one has

$$\frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \ln L(s,\chi) = \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \sum_p -\ln(1-\chi(p)p^{-s})$$

$$= \sum_p \sum_{k\ge 1} \frac{1}{\phi(q)} \sum_{\chi} \overline{\chi(a)} \frac{\chi(p^k)p^{-sk}}{k}$$

and a simple application of relation (3) gives

$$\frac{1}{\phi(q)}\sum_{\chi}\overline{\chi}(a)\ln L(s,\chi)=\sum_{p}\sum_{\substack{k\geq 1\\ p^k\equiv a \pmod q}}\frac{p^{-sk}}{k}=\sum_{p\equiv a \pmod q}p^{-s}+O(1)\qquad ,s\to 1^{+}.$$

Then, by splitting the sum in real and complex characters, one gets

$$\sum_{p\equiv a \pmod q}p^{-1}=\frac{1}{\phi(q)}\left(\sum_{\chi=\chi_0}+\sum_{\chi=\left(\frac{n}{q}\right)}+\sum_{\chi\text{ complex}}\right)\overline{\chi}(a)\ln L(1,\chi)+O(1). \tag{4}$$

$\chi_0$ is called the principal character and equals 1 whenever $n\not\equiv 0 \pmod q$ and 0 otherwise. The first sum (over $\chi_0$) is $+\infty$, as $L(s,\chi_0)=\zeta(s)\prod_{p|q}(1-p^{-s})$. This infinite term should imply that there are an infinite number of primes in the arithmetic progression. The only problem is that one of the other terms could cancel this one by being $-\infty$ at $s=1$. Abel summation criterion shows that $L(1,\chi)$ is finite. One therefore has to show that $L(1,\chi)\neq 0$.

This is definitely true for complex characters since otherwise, by setting $a=1$ and taking the exponential in 2, one has $\prod_{\chi}|L(1,\chi)|>1$ which is incompatible with a zero of weight 2 (coming from $L(1,\chi)=0$ and $L(1,\overline{\chi})=0$) versus a single pole in $s=1$. Hence the last sum in relation (4) is bounded.

The real problem is then to bound the middle sum in relation (4), that is to say to show that $L(1,(\cdot/q))\neq 0$. Dirichlet proved this result by a very ingenious method: He evaluated this number in closed form! This is now known as Dirichlet's class number formula:

$$0\neq L\left(1,(\cdot/q)\right)=\begin{cases}\frac{\pi h}{w\sqrt{q}} & \text{when } q\equiv 1 \pmod 4\\ \frac{2h\ln\epsilon}{\sqrt{q}} & \text{when } q\equiv 3 \pmod 4\end{cases}$$

where $h$ is the class number of $\mathbf{Q}(\sqrt{(-1)^{(q+1)/2}q})$, $\epsilon$ its fundamental unit and $w$ the number of roots of unity in this field (see the canonical reference [2]). Since each of these quantities counts something, they are positive, and the result now follows:

$$\sum_{p\equiv a \pmod q}p^{-1}=+\infty.$$

Simpler proofs using only complex analysis are also possible. The idea is to use Landau's theorem that a Dirichlet series with positive terms has a pole at its abscissa of convergence and apply it to $\prod_{\chi \bmod q}L(s,\chi)$ which has just been shown to have positive coefficients.

## 3. The Prime Number Theorem

The distribution of primes is quite irregular, so it is easier to study their statistical behaviour. In this direction, let $\pi(x)$ be the number of primes $\leq x$. Gauss conjectured that $\pi(x)\sim\int_2^x\frac{dt}{\ln t}=:\mathrm{Li}(x)$. This assertion simply says: "the probability that $n$ is prime is about $1/\ln n$." This result was finally proved by Hadamard and La Vallée Poussin in 1896. Both of them used fundamental ideas of Riemann who was the first to introduce complex analysis in the study of the distribution of prime numbers.

Using Perron's formula, namely

$$\sum_{p^n\leq x}\ln(p)=\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\frac{-\zeta'(s)}{\zeta(s)}\frac{x^s ds}{s}$$

and using residues, Riemann essentially found what is perhaps the most important formula in analytic number theory (the von Mangoldt explicit formula):

$$\sum_{p^n\le x}\ln(p) = x - \frac{\zeta'(0)}{\zeta(0)} - \sum_{\zeta(\rho)=0}\frac{x^\rho}{\rho} = x - \ln(2\pi) - \sum_{\Re(\rho)>0}\frac{x^\rho}{\rho} - \frac{1}{2}\ln(1-x^{-2}), \tag{5}$$

where sum on the right is over the zeroes of the Riemann $\zeta$ function. These zeroes can be split up into two types: The *trivial* zeroes at $-2,-4,-6,\ldots$, and the zeroes with $0\le\Re\le 1$ (the right hand side of (5) reflects this dichotomy). This formula has many interesting properties and reflects the following principles of analytic number theory:

1. Primes should always be counted with weight $\ln(p)$;
2. Primes and prime powers should be counted together;
3. There are much less prime powers than primes;
4. The zeroes of the $\zeta$ function are the "fundamental frequencies" of the primes, and in this sense are dual to the primes.

Following Chebyshev, one defines $\theta(x)=\sum_{p\le x}\ln(p)$ and $\psi(x)=\sum_{p^n\le x}\ln(p)=\sum_{n\le x}\Lambda(n)$, where $\Lambda(n)=\ln(p)$ when $n=p^m$, and zero otherwise. A fairly straightforward partial summation shows that the prime number theorem is equivalent to $\psi(x)\sim x$ (note that trivially, $\psi(x)=\theta(x)+O(\sqrt{x})$), and that more generally,

$$\psi(x)=x+R(x)\Longleftrightarrow \pi(x)\sim \mathrm{Li}(x)+O(R(x)/\ln(x)).$$

One can then see from the explicit formula (5) that the prime number theorem would follow if one can bound $\Re\rho<1$, since each error term would then be of order $<x$. The prime number theorem would then be equivalent to showing that $\zeta(1+it)\neq 0$ for $t\neq 0$. In fact, this is an equivalence (as was later shown by Wiener) and Hadamard and La Vallée Poussin were able to prove that $\zeta(1+it)\neq 0$ using some ingenious trigonometric identities. We will give a proof due to Mertens, in 1898. Set $\rho=1+it$, then $\zeta(\rho)=0\Longrightarrow \Re\ln\zeta(\sigma+it)\to-\infty$ when $\sigma\to 1$ (we restrict to $\Re(\sigma)>1$). But, by the Euler identity, one has $\ln\zeta(s)=\sum_p\sum_{m\ge 1}m^{-1}p^{-m\sigma}\exp(-itm\ln(p))$ and so

$$\Re\ln\zeta(s)=\sum_p\sum_{m\ge 1}m^{-1}p^{-m\sigma}\cos(-tm\ln(p)).$$

Mertens' trick consists in noticing that $2(1+\cos\beta)^2=3+4\cos\beta+\cos 2\beta\ge 0$, thus $3\ln\zeta(\sigma)+4\Re\ln\zeta(\sigma+it)+\Re\ln\zeta(\sigma+2it)\ge 0$, hence $\zeta^3(\sigma)|\zeta^4(\sigma+it)\zeta(\sigma+2it)|\ge 1$.
But, as $\sigma\to 1$, one has $\zeta(\sigma)\sim(\sigma-1)^{-1}$ and $|\zeta(\sigma+it)|\sim A(\sigma-1)$ for a some constant $A$ (by analicity). So one should have $\zeta(\sigma+2it)\to\infty$, this contradicts the fact that $\zeta(1+2it)$ is bounded (by the Abel summation criterion) . In conclusion, the $\zeta$ function has no zero with $\Re(\rho)=1$, the PNT is proved. An elementary (i.e. without complex analysis) proof of the PNT was subsequently found by Erdős and Selberg in 1949 (see [4] and [9]).

## 4. Chebyshev's bias

All numerical evidence shows that $\pi(x)<\mathrm{Li}(x)$ and it was long believed that this would be true for all $x$. Similarly, Chebyshev noted that the number of primes of the form $4k+3$ seemed to be more abundant than the primes of the form $4k+1$, more precisely, let $\pi_{q,a}(x)=|\{p\le x:\ p\equiv a \pmod q\}|$ then $\pi_{4,3}(x)\ge\pi_{4,1}(x)$.

In fact, Littlewood proved in 1914 that $\pi(x)-\mathrm{Li}(x)$ changes sign infinitely often and the same is true for $\pi_{4,3}(x)-\pi_{4,1}(x)$. In 1957 Leech showed that $\pi_{4,1}(x)>\pi_{4,3}(x)$ is first true for $x=26861$. That the similar inequality $\pi_{3,1}(x)>\pi_{3,2}(x)$ is first true for $x=608981813029$ was shown by Bays and Hudson in 1978. No example of $\pi(x) > \mathrm{Li}(x)$ is known. Skewes first gave an upper bound $e^{e^{e^5}}$ which was later reduced by Sherman–Lehman and then te Riele [10] who gave an upper bound of $10^{370}$.

This behaviour can easily be explained using explicit formulas. In the case of $\pi(x)$, the point is the following: The explicit formula (5) expresses $\psi(x)$ as a sum of powers $x^\rho$. Assuming the Riemann Hypothesis, one can write this as

$$\psi(x) = x - x^{1/2}\left(\sum_{\zeta(1/2+i\gamma)=0} \frac{x^{i\gamma}}{1/2+i\gamma}\right) + o(x^{1/2})\,.$$

One can now see the reason for the bias: The function $\psi(x)$ does not count primes but prime powers so what one really wants is the behaviour of $\theta(x)$ which is given by

$$\theta(x) = \psi(x) - \theta(\sqrt{x}) + O(x^{1/3})\,,$$

so that

$$\theta(x) = x - x^{1/2}\left(1 + \sum_{\zeta(1/2+i\gamma)=0} \frac{x^{i\gamma}}{1/2+i\gamma}\right) + o(x^{1/2})\,.$$

The function

$$\sum_{\zeta(1/2+i\gamma)=0} \frac{e^{i\gamma\ln(x)}}{1/2+i\gamma}\,,$$

is a very slowly oscillating trigonometric series which should be zero on average, so the extra term biases $\theta(x)$ to be smaller than $x$ on average. A simple description is that $\mathrm{Li}(x)$ counts the number of prime powers $\leq x$, so the number of primes should be slightly less since the number of prime squares is of the same order as the error term.

There is a similar explanation for the bias in arithmetic progressions. There is an explicit formula

$$\sum_{p^n\leq x} \chi(n)\ln(p) = -x^{1/2}\left(\sum_{L(1/2+i\gamma_\chi,\chi)=0} \frac{x^{i\gamma_\chi}}{1/2+i\gamma_\chi}\right) + o(x^{1/2})\,,$$

where the *Generalised Riemann Hypothesis* has been assumed (there is no $x$ term since $L(1,\chi)$ is no longer a pole if $\chi \neq \chi_0$). As before one has

$$\psi_{q,a}(x) = \sum_{\substack{p^n\equiv a \ (\mathrm{mod}\, q)\\ p^n\leq x}} \ln(p) = \frac{x}{\phi(q)} - \frac{x^{1/2}}{\phi(q)} \sum_{\chi \bmod q} \overline{\chi(a)} \sum_{L(1/2+i\gamma_\chi)=0} \frac{x^{i\gamma_\chi}}{1/2+i\gamma_\chi}$$

but one really wants to look at

$$\theta_{q,a}(x) = \sum_{\substack{p\equiv a \ (\mathrm{mod}\, q)\\ p\leq x}} \ln(p) = \psi_{q,a}(x) - \sum_{\substack{p^2\equiv a \ (\mathrm{mod}\, q)\\ p^2\leq x}} \ln(p) + O(x^{1/3}) = \psi_{q,a}(x) - c_{q,a}x^{1/2} + O(x^{1/3})\,,$$

where $c_{q,a}$ is the number of solutions of $y^2 \equiv a \pmod q$. In particular, the same argument shows that there will always be fewer primes in the progression $qn + a$ when $a$ is a residue than when $a$ is a nonresidue. Simply put, the "balanced" count is the set of prime powers $\equiv a \pmod q$ so there are fewer primes $\equiv a \pmod q$ when $a$ is quadratic residue since the number of prime squares congruent to $a$ is of the same order as the error term in the analytic formulas.

In 1994, Rubinstein and Sarnak [8] were able to make Chebyshev's bias precise. Assuming GRH (if this is false, then there is no bias) and also the Grand Simplicity Hypothesis (GSH: All the ordinates of zeroes of $L$-function are linearly independent over $\mathbb{Q}$), then

$$\frac{1}{\ln(x)} \sum_{\substack{\pi(n)>\mathrm{Li}\, n \\ n\le x}} \to .00000026, \qquad \frac{1}{\ln(x)} \sum_{\substack{\pi_{4,3}(n)>\pi_{4,1}(n) \\ n\le x}} \to .9959.$$

### References


[1] Daboussi (Hédi). – Sur le théorème des nombres premiers. *Comptes Rendus des Séances de l'Académie des Sciences. Série I. Mathématique*, vol. 298, n° 8, 1984, pp. 161–164.

[2] Davenport (Harold). – *Multiplicative Number Theory.* – Springer-Verlag, New York, 1980, second edition, xiii+177p. Revised by Hugh L. Montgomery.

[3] Dirichlet (L.). – Beweis des Satzes, das jede unbegrenzte arithmetische Progression... *Abh. Kőnig. Preuss. Akad.*, vol. 34, 1837, pp. 45–81.

[4] Erdős (P.). – On a New Method in Elementary Number Theory which leads to an Elementary Proof of the Prime Number Theorem. *Proceedings of the National Academy of Sciences. U.S.A.*, vol. 35, 1949, pp. 374–384.

[5] Friedlander (John) and Iwaniec (Henryk). – Using a Parity-Sensitive Sieve to Count Prime Values of a Polynomial. *Proceedings of the National Academy of Sciences. U.S.A.*, vol. 94, n° 4, 1997, pp. 1054–1058.

[6] Niven (Ivan). – A Simple Proof that $\pi$ is Irrational. *Bulletin of the American Mathematical Society*, vol. 53, 1947, p. 509.

[7] Ribenboim (Paulo). – *The New Book of Prime Number Records.* – Springer-Verlag, New York, 1996, xxiv+541p.

[8] Rubinstein (Michael) and Sarnak (Peter). – Chebyshev's Bias. *Experimental Mathematics*, vol. 3, n° 3, 1994, pp. 173–197.

[9] Selberg (Atle). – An Elementary Proof of the Prime-Number Theorem. *Annals of Mathematics (2)*, vol. 50, 1949, pp. 305–313.

[10] te Riele (Herman J. J.). – On the Sign of the Difference $\pi(x) - \mathrm{Li}(x)$. *Mathematics of Computation*, vol. 48, n° 177, 1987, pp. 323–328.

[11] Tenenbaum (Gérald) and Mendès France (Michel). – *Les nombres premiers.* – Presses Universitaires de France, Paris, 1997, 128p.