Chapter 1

Introduction to prime number theory

1.1 The Prime Number Theorem

In the first part of this course, we focus on the theory of prime numbers. We use the following notation: we write $f(x) \sim g(x)$ as $x \to \infty$ if $\lim_{x\to\infty} f(x)/g(x) = 1$, and denote by $\log x$ the natural logarithm. The central result is the Prime Number Theorem:

Theorem 1.1 (Prime Number Theorem, Hadamard, de la Vallée Poussin, 1896)**.** *let $\pi(x)$ denote the number of primes $\leqslant x$. Then*

$$\pi(x) \sim \frac{x}{\log x} \quad \text{as } x \to \infty.$$

This result was conjectured by Legendre in 1798. In 1851/52, Chebyshev proved that if the limit $\lim_{x\to\infty} \pi(x)\log x/x$ exists, then it must be equal to 1, but he couldn't prove the existence of the limit. However, Chebyshev came rather close, by showing that there is an x_0, such that for all $x \geqslant x_0$,

$$0.921\frac{x}{\log x} < \pi(x) < 1.056\frac{x}{\log x}.$$

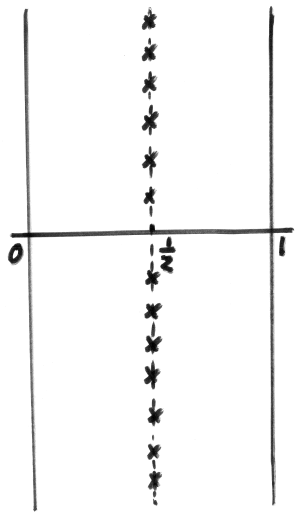
In 1859, Riemann published a very influential paper (B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Große, Monatshefte der Berliner

Akademie der Wissenschaften 1859, 671–680; also in Gesammelte Werke, Leipzig 1892, 145–153) in which he related the distribution of prime numbers to properties of the function in the complex variable s,

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

(nowadays called the Riemann zeta function). It is well-known that $\zeta(s)$ converges absolutely for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$, and that it diverges for $s \in \mathbb{C}$ with $\operatorname{Re} s \leqslant 1$. Moreover, $\zeta(s)$ defines an *analytic* (complex differentiable) function on $\{s \in \mathbb{C} : \operatorname{Re} s > 1\}$. Riemann obtained another expression for $\sum_{n=1}^{\infty} n^{-s}$ that can be defined everywhere on $\mathbb{C} \setminus \{1\}$ and defines an analytic function on this set; in fact it can be shown that it is the only analytic function on $\mathbb{C} \setminus \{1\}$ that coincides with $\sum_{n=1}^{\infty} n^{-s}$ on $\{s \in \mathbb{C} : \operatorname{Re} s > 1\}$. This analytic function is also denoted by $\zeta(s)$. Riemann proved the following properties of $\zeta(s)$:

- $\zeta(s)$ has a pole of order 1 in $s = 1$ with residue 1, that is, $\lim_{s \to 1}(s-1)\zeta(s) = 1$;
- $\zeta(s)$ satisfies a functional equation that relates $\zeta(s)$ to $\zeta(1-s)$;
- $\zeta(s)$ has zeros in $s = -2, -4, -6, \ldots$ (the trivial zeros). The other zeros lie in the *critical strip* $\{s \in \mathbb{C} : 0 < \operatorname{Re} s < 1\}$.



Riemann stated the following still unproved conjecture:

Riemann Hypothesis (RH).
All zeros of $\zeta(s)$ in the critical strip lie on the axis of symmetry of the functional equation, i.e., the line $\operatorname{Re} s = \frac{1}{2}$.

Riemann made several other conjectures about the distribution of the zeros of $\zeta(s)$, and further, he stated without proof a formula that relates

$$\theta(x) := \sum_{p \leqslant x} \log p \quad \text{(sum over all primes } \leqslant x)$$

to the zeros of $\zeta(s)$ in the critical strip. These other conjectures of Riemann were proved by Hadamard in 1893, and the said formula was proved by von Mangoldt in 1895.

Finally, in 1896, Hadamard and de la Vallée Poussin independently proved the Prime Number Theorem. Their proofs used a fair amount of complex analysis. A crucial ingredient for their proofs is, that $\zeta(s) \neq 0$ if $\operatorname{Re} s = 1$ and $s \neq 1$. In 1899, de la Vallée Poussin obtained the following *Prime Number Theorem with error term*: Let

$$\operatorname{Li}(x) := \int_2^x \frac{dt}{\log t}.$$

Then there is a constant $c > 0$ such that

$$\pi(x) = \operatorname{Li}(x) + O\Big(xe^{-c\sqrt{\log x}}\Big) \quad \text{as } x \to \infty. \tag{1.1}$$

Exercise 1.1. *a) Prove that for every integer $n \geqslant 1$,*

$$\int_2^x \frac{dt}{(\log t)^n} = O\Big(\frac{x}{(\log x)^n}\Big) \quad \textit{as } x \to \infty,$$

where the constant implied by the O-symbol may depend on n (in other words, there are $C > 0$, $x_0 > 0$, possibly depending on n, such that $|\int_2^x \frac{dt}{(\log t)^n}| \leqslant C \cdot x/(\log x)^n$ for $x \geqslant x_0$).

Hint. *Choose an appropriate function $f(x)$ with $2 < f(x) < x$, split the integral into $\int_2^{f(x)} + \int_{f(x)}^x$ and estimate both integrals from above, using $|\int_a^b g(t)dt| \leqslant (b-a)\max_{a \leqslant t \leqslant b} |g(t)|$.*

b) Prove that for every integer $n \geqslant 1$,

$$\operatorname{Li}(x) = \frac{x}{\log x} + 1!\frac{x}{(\log x)^2} + \cdots + (n-1)!\frac{x}{(\log x)^n} + O\Big(\frac{x}{(\log x)^{n+1}}\Big) \quad \textit{as } x \to \infty,$$

where the constant implied by the O-symbol may depend on n.

Hint. *Use repeated integration by parts.*

This implies that $\mathrm{Li}(x)$ is a much better approximation to $\pi(x)$ than $x/\log x$.

Corollary 1.2. $\lim_{x\to\infty} \dfrac{\pi(x)-\mathrm{Li}(x)}{\pi(x)-x/\log x} = 0.$

Proof. We combine the above exercise and (1.1) and use that

$$\frac{xe^{-c\sqrt{\log x}}}{x/(\log x)^n} = e^{n\log\log x - c\sqrt{\log x}} \to 0 \ \text{ as } x\to\infty \ \text{ for every } n>0. \tag{1.2}$$

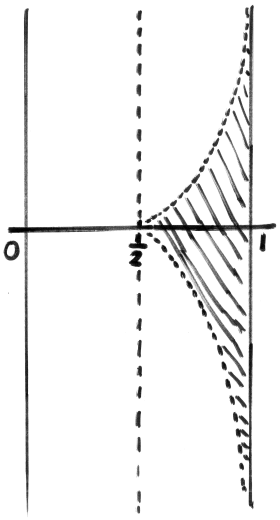
This gives

$$\begin{aligned}
\pi(x)-\frac{x}{\log x} &= \mathrm{Li}(x)-\frac{x}{\log x}+\pi(x)-\mathrm{Li}(x)\\
&= \frac{x}{(\log x)^2}+O\Big(\frac{x}{(\log x)^3}\Big)+O\Big(xe^{-c\sqrt{\log x}}\Big)\\
&= \frac{x}{(\log x)^2}+O\Big(\frac{x}{(\log x)^3}\Big) = \frac{x}{(\log x)^2}\cdot\Big(1+O\Big(\frac{1}{\log x}\Big)\Big)\\
&\sim \frac{x}{(\log x)^2} \text{ as } x\to\infty
\end{aligned}$$

and subsequently, on applying (1.1) and (1.2),

$$\frac{\pi(x)-\mathrm{Li}(x)}{\pi(x)-x/\log x} \sim \frac{\pi(x)-\mathrm{Li}(x)}{x/(\log x)^2} = O\left(\frac{xe^{-c\sqrt{\log x}}}{x/(\log x)^2}\right)\to 0 \ \text{ as } x\to\infty.$$

□



In fact, in his proof of (1.1), de la Vallée Poussin used that for some constant $c>0$,

$$\begin{aligned}&\zeta(s)\neq 0\\ &\text{for all } s \text{ with } \operatorname{Re} s > 1-\frac{c}{\log(|\operatorname{Im} s|+2)}.\end{aligned}$$

A *zero free region* for $\zeta(s)$ is a subset $\mathcal{S}$ of the critical strip of which it is known that $\zeta(s)\neq 0$ on $\mathcal{S}$. In general, a larger provable zero free region for $\zeta(s)$ leads to a better estimate for $\pi(x)-\mathrm{Li}(x)$.

In 1958, Korobov and Vinogradov independently showed that for every $\alpha > \frac{2}{3}$ there is a constant $c(\alpha) > 0$ such that

$$\zeta(s) \neq 0 \text{ for all } s \text{ with } \operatorname{Re} s > 1 - \frac{c(\alpha)}{(\log(|\operatorname{Im} s| + 2))^{\alpha}}.$$

From this, they deduced that for every $\beta < \frac{3}{5}$ there is a constant $c'(\beta) > 0$ with

$$\pi(x) = \operatorname{Li}(x) + O\Big(xe^{-c'(\beta)(\log x)^{\beta}}\Big) \text{ as } x \to \infty.$$

This has not been improved so far.

On the other hand, in 1901 von Koch proved that the Riemann Hypothesis is equivalent to

$$\pi(x) = \operatorname{Li}(x) + O\Big(\sqrt{x}(\log x)^2\Big) \text{ as } x \to \infty,$$

which is of course much better than the result of Korobov and Vinogradov.

After Hadamard and de la Vallée Poussin, several other proofs of the Prime Number theorem were given, all based on complex analysis. In the 1930's, Wiener and Ikehara proved a general so-called Tauberian theorem (from functional analysis) which implies the Prime Number Theorem in a very simple manner. In 1948, Erdős and Selberg independently found an elementary proof, "elementary" meaning that the proof avoids complex analysis or functional analysis, but definitely not that the proof is easy! In 1980, Newman gave a new, simple proof of the Prime Number Theorem, based on complex analysis. Korevaar observed that Newman's approach can be used to prove a simpler version of the Wiener-Ikehara Tauberian theorem with a not so difficult proof based on complex analysis alone and avoiding functional analysis. In this course, we prove the Tauberian theorem via Newman's method, and deduce from this the Prime Number Theorem as well as the Prime Number Theorem for arithmetic progressions (see below).

1.2 Primes in arithmetic progressions

In 1839–1842 Dirichlet (the founder of analytic number theory) proved that every arithmetic progression contains infinitely many primes. Otherwise stated, he proved that for every integer $q > 2$ and every integer a with $\gcd(a, q) = 1$, there are infinitely many primes p such that

$$p \equiv a \pmod{q}.$$

His proof is based on so-called *L-functions*. To define these, we have to introduce Dirichlet characters. A *Dirichlet character modulo* q is a function $\chi : \mathbb{Z} \to \mathbb{C}$ with the following properties:

- $\chi(1) = 1$;
- $\chi(b_1) = \chi(b_2)$ for all $b_1, b_2 \in \mathbb{Z}$ with $b_1 \equiv b_2 \pmod q$;
- $\chi(b_1 b_2) = \chi(b_1)\chi(b_2)$ for all $b_1, b_2 \in \mathbb{Z}$;
- $\chi(b) = 0$ for all $b \in \mathbb{Z}$ with $\gcd(b, q) > 1$.

The *principal character modulo* q is given by

$$\chi_0^{(q)}(a) = 1 \text{ if } \gcd(a, q) = 1, \quad \chi_0^{(q)}(a) = 0 \text{ if } \gcd(a, q) > 1.$$

Example. Let χ be a character modulo 5. Since $2^4 \equiv 1 \pmod 5$ we have $\chi(2)^4 = 1$. Hence $\chi(2) \in \{1, i, -1, -i\}$. In fact, the Dirichlet characters modulo 5 are given by χ^j $(j = 1, 2, 3, 4)$ where

$$\begin{array}{lll} \chi(b) = 1 & \text{if} & b \equiv 1 \pmod 5, \\ \chi(b) = i & \text{if} & b \equiv 2 \pmod 5, \\ \chi(b) = -1 & \text{if} & b \equiv 4 \equiv 2^2 \pmod 5, \\ \chi(b) = -i & \text{if} & b \equiv 3 \equiv 2^3 \pmod 5, \\ \chi(b) = 0 & \text{if} & b \equiv 0 \pmod 5. \end{array}$$

In general, by the Euler-Fermat Theorem, if b, q are integers with $q \geqslant 2$ and $\gcd(b, q) = 1$, then $b^{\varphi(q)} \equiv 1 \pmod q$, where $\varphi(q)$ is the number of positive integers $a \leqslant q$ that are coprime with q. Hence $\chi(b)^{\varphi(q)} = 1$.

The L-function associated with a Dirichlet character χ modulo q is given by

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}.$$

Since $|\chi(n)| \in \{0, 1\}$ for all n, this series converges absolutely for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$. Further, many of the results for $\zeta(s)$ can be generalized to L-functions:

- if χ is not a principal character, then $L(s, \chi)$ has an analytic continuation to $\mathbb{C}$, while if $\chi = \chi_0^{(q)}$ is the principal character modulo q it has an analytic continuation to $\mathbb{C} \setminus \{1\}$, with $\lim_{s \to 1}(s - 1)L(s, \chi_0^{(q)}) = \prod_{p|q}(1 - p^{-1})$.

- there is a functional equation, relating $L(s,\chi)$ to $L(1-s,\overline{\chi})$, where $\overline{\chi}$ is the complex conjugate character, defined by $\overline{\chi}(b) := \overline{\chi(b)}$ for $b \in \mathbb{Z}$.

Furthermore, there is a generalization of the Riemann Hypothesis:

Generalized Riemann Hypothesis (GRH): *Let χ be a Dirichlet character modulo q for any integer $q \geqslant 2$. Then the zeros of $L(s,\chi)$ in the critical strip lie on the line* $\operatorname{Re} s = \frac{1}{2}$.

De la Vallée Poussin managed to prove the following generalization of the Prime Number Theorem, using properties of L-functions instead of $\zeta(s)$:

Theorem 1.3 (Prime Number Theorem for arithmetic progressions)**.** *let q, a be integers with $q \geqslant 2$ and* $\gcd(a,q) = 1$. *Denote by $\pi(x;q,a)$ the number of primes p with $p \leqslant x$ and $p \equiv a \pmod q$. Then*

$$\pi(x;q,a) \sim \frac{1}{\varphi(q)} \cdot \frac{x}{\log x} \quad \text{as } x \to \infty.$$

Corollary 1.4. *Let q be an integer $\geqslant 2$. Then for all integers a coprime with q we have*

$$\lim_{x\to\infty} \frac{\pi(x;q,a)}{\pi(x)} = \frac{1}{\varphi(q)}.$$

This shows that in some sense, the primes are evenly distributed over the prime residue classes modulo q.

1.3 An elementary result for prime numbers

We finish this introduction with an elementary proof, going back to Erdős, of a weaker version of the Prime Number Theorem.

Theorem 1.5. *We have*

$$\tfrac{1}{2} \cdot \frac{x}{\log x} \leqslant \pi(x) \leqslant 2\frac{x}{\log x} \quad \text{for } x \geqslant 3.$$

The proof is based on some simple lemmas. For an integer $n \neq 0$ and a prime number p, we denote by $\operatorname{ord}_p(n)$ the largest integer k such that p^k divides n.

Further, we denote by $[x]$ the largest integer $\leqslant x$.

Lemma 1.6. *Let n be an integer $\geqslant 1$ and p a prime number. Then*

$$\mathrm{ord}_p(n!) = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right].$$

Remark. This is a finite sum.

Proof. We count the number of times that p divides $n!$. Each multiple of p that is $\leqslant n$ contributes a factor p. Each multiple of p^2 that is $\leqslant n$ contributes another factor p, each multiple of p^3 that is $\leqslant n$ another factor p, and so on. Hence

$$\mathrm{ord}_p(n!) = \sum_{j=1}^{\infty} (\text{number of multiples of } p^j \leqslant n) = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right].$$

□

Lemma 1.7. *Let a, b be integers with $a \geqslant 2b > 0$. Then*

$$\prod_{a-b+1 \leqslant p \leqslant a} p \quad \textit{divides } \binom{a}{b}.$$

Proof. We have

$$\binom{a}{b} = \frac{a(a-1)\cdots(a-b+1)}{1 \cdot 2 \cdots b}, \qquad a-b+1 > b.$$

Hence any prime with $a - b + 1 \leqslant p \leqslant a$ divides the numerator but not the denominator. □

Lemma 1.8. *Let a, b be integers with $a > b > 0$. Suppose that some prime power p^k divides $\binom{a}{b}$. Then $p^k \leqslant a$.*

Proof. Let p be a prime. By Lemma 1.6 we have

$$\begin{aligned} \mathrm{ord}_p\left(\binom{a}{b}\right) &= \mathrm{ord}_p\left(\frac{a!}{b!(a-b)!}\right) \\ &= \sum_{j=1}^{\infty} \left(\left[\frac{a}{p^j}\right] - \left[\frac{a-b}{p^j}\right] - \left[\frac{b}{p^j}\right]\right). \end{aligned}$$

Each summand is either 0 or 1. Further, each summand with $p^j > a$ is 0. Hence $\mathrm{ord}_p\left(\binom{a}{b}\right) \leqslant \alpha$, where α is the largest j with $p^j \leqslant a$. This proves our lemma. □

Lemma 1.9. *Let n be an integer $\geqslant 1$. Then*

$$\frac{2^n}{n+1} \leqslant \binom{n}{[n/2]} \leqslant 2^{n-1}.$$

Proof. $\binom{n}{[n/2]}$ is the largest among the binomial coefficients $\binom{n}{0}, \ldots, \binom{n}{n}$. Hence

$$2^n = \sum_{j=0}^{n} \binom{n}{j} \leqslant (n+1)\binom{n}{[n/2]}.$$

This establishes the lower bound for $\binom{n}{[n/2]}$. To prove the upper bound, we distinguish between the cases $n = 2k+1$ odd and $n = 2k$ even. First, let $n = 2k+1$ be odd. Then

$$\begin{aligned} \binom{n}{[n/2]} &= \binom{2k+1}{k} = \frac{1}{2}\left(\binom{2k+1}{k} + \binom{2k+1}{k+1}\right) \\ &\leqslant \frac{1}{2}\sum_{j=0}^{2k+1}\binom{2k+1}{j} = 2^{2k} = 2^{n-1}. \end{aligned}$$

Now, let $n = 2k$ be even. Then since $\binom{2k}{k-1} \geqslant \frac{1}{2}\binom{2k}{k}$ for $k \geqslant 1$,

$$\begin{aligned} \binom{n}{[n/2]} &= \binom{2k}{k} \leqslant \frac{1}{2}\left(\binom{2k}{k-1} + \binom{2k}{k} + \binom{2k}{k+1}\right) \\ &\leqslant \frac{1}{2}\sum_{j=0}^{2k}\binom{2k}{j} = 2^{2k-1} = 2^{n-1}. \end{aligned}$$

□

Proof of $\pi(x) \geqslant \frac{1}{2}x/\log x$. It is easy to check that $\pi(x) \geqslant \frac{1}{2}x/\log x$ for $3 \leqslant x \leqslant 100$. Assume that $x > 100$. Let $n := [x]$; then $n \leqslant x < n+1$.

Write $\binom{n}{[n/2]} = p_1^{k_1} \cdots p_t^{k_t}$, where the p_i are distinct primes, and the k_i positive integers. By Lemma 1.8 we have $p_i^{k_i} \leqslant n$ for $i = 1, \ldots, t$. Then also $p_i \leqslant n$ for $i = 1, \ldots, t$, hence $t \leqslant \pi(n)$. It follows that

$$\binom{n}{[n/2]} \leqslant n^{\pi(n)}.$$

So by Lemma 1.9, $n^{\pi(n)} \geqslant 2^n/(n+1)$. Consequently,

$$\begin{aligned}\pi(x) &= \pi(n) \geqslant \frac{n\log 2 - \log(n+1)}{\log n} \\ &\geqslant \frac{(x-1)\log 2 - \log(x+1)}{\log x} \geqslant \tfrac{1}{2}\frac{x}{\log x} \quad \text{for } x \geqslant 100.\end{aligned}$$

□

Proof of $\pi(x) \leqslant 2x/\log x$. Let again $n = [x]$. Since $t/\log t$ is an increasing function of t, it suffices to prove that $\pi(n) \leqslant 2 \cdot n/\log n$ for all integers $n \geqslant 3$. We proceed by induction on n.

It is straightforward to verify that $\pi(n) \leqslant 2 \cdot n/\log n$ for $3 \leqslant n \leqslant 200$. Let $n > 200$, and suppose that $\pi(m) \leqslant 2 \cdot m/\log m$ for all integers m with $3 \leqslant m < n$. If n is even, then we can use $\pi(n) = \pi(n-1)$ and that $t/\log t$ is increasing. Assume that $n = 2k+1$ is odd. Then by Lemma 1.7, we have

$$\binom{2k+1}{k} \geqslant \prod_{k+2 \leqslant p \leqslant 2k+1} p \geqslant (k+2)^{\pi(2k+1)-\pi(k+1)}.$$

Using Lemma 1.9, this leads to $(k+2)^{\pi(2k+1)-\pi(k+1)} \leqslant 2^{2k}$, or

$$\pi(2k+1) - \pi(k+1) \leqslant \frac{2k\log 2}{\log(k+2)}.$$

Finally, applying the induction hypothesis to $\pi(k+1)$ and using $k+2 > k+1 > n/2$, we arrive at

$$\begin{aligned}\pi(n) &= \pi(2k+1) \leqslant \frac{2k\log 2}{\log(k+2)} + \frac{2(k+1)}{\log(k+1)} \\ &< \frac{(\log 2 + 1)n + 1}{\log(n/2)} < 2\frac{n}{\log n} \quad \text{for } n > 200.\end{aligned}$$

□