Analytic Number Theory

Cambridge Part III, Michaelmas 2022

Taught by Mansur Boase

Notes taken by Leonard Tomczak

Contents

0 Prelude: Cramer's Model

Let $\pi(x)$ be the number of primes $\leq x$.

Conjecture. (Gauss) $\pi(x) \sim \mathrm{li}(x)$.

Here li is the *integral logarithm*, defined by $\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}$.

Probabilistic Motivation. Suppose that the "probability" that n is a prime is $\frac{1}{\log n}$. We model this as follows: Let $X_1, X_2, \dots$ be independent random variables where

$$X_1 = 0,$$
$$X_2 = 1,$$
$$X_n = \begin{cases} 1 & \text{with probability } 1/\log n, \\ 0 & \text{otherwise.} \end{cases} \qquad \text{for } n \geq 2$$

Then let $\Pi(x) := \sum_{i \leq x} X_i$. Then

$$\mathbb{E}[\Pi(x)] = 1 + \sum_{3 \leq n \leq x} \frac{1}{\log n},$$
$$\mathrm{Var}[\Pi(x)] = \sum_{i \leq x} \mathrm{Var}[X_i] = \sum_{3 \leq n \leq x} \frac{1}{\log n} - \frac{1}{(\log n)^2}.$$

By comparing the sums with integrals we find that $\mathbb{E}[\Pi(x)] \sim \mathrm{li}(x) \sim \mathrm{Var}[\Pi(x)]$.

Furthermore, we have $\mathrm{li}(x) \sim \frac{x}{\log x}$. There are several ways to see this:

1. Write $\mathrm{li}(x) = \int_2^x \frac{dt}{\log t} = \int_2^{\sqrt{x}} + \int_{\sqrt{x}}^x \frac{dt}{\log t} = \dots$, but using this we only get $\mathrm{li}(x) \ll \frac{x}{\log x}$.
2. Apply L'Hôpital's rule to $\lim_{x\to\infty} \frac{\int_2^x \frac{dt}{\log dt}}{\frac{x}{\log x}}$.

More generally, let $\mathrm{li}_n(x) = \int_2^x \frac{dt}{(\log t)^n}$. Then one similarly finds that $\mathrm{li}_n(x) \sim \frac{x}{(\log x)^n}$.

We can find the asymptotics of $\mathrm{li}(x)$ using integration by parts:

$$\begin{aligned} \mathrm{li}(x) &= \int_2^x \frac{dy}{\log y} = \frac{y}{\log y}\Big|_2^x + \int_2^x \frac{dy}{(\log y)^2} \\ &= \frac{x}{\log x} + \Big(\frac{x}{\log x}\Big)^2 + \int_2^x \frac{2dy}{(\log y)^3} + O(1) \\ &= \frac{x}{\log x} + \cdots + \frac{(N-1)!x}{(\log x)^N} + O_N\Big(\frac{x}{(\log x)^{N+1}}\Big) \end{aligned}$$

Cramer's model is so good, because it assumes the random variables X_n to be independent, but e.g. the condition that n is prime is not independent from the condition that $n+1$ is prime.

Another key idea from probability theory used in analytic number theory is *generating functions*!

Example. We sieve out primes $p_1, p_2, \dots, p_k$ of $1 + z + z^2 + \cdots = \frac{1}{1-z}$. For any prime p we have $1 + z^p + z^{2p} + \cdots = \frac{1}{1-z^p}$, hence using the Inclusion-Exclusion principle we get

$$\frac{1}{1-z} - \sum_i \frac{1}{1-z^{p_i}} + \sum_{i<j} \frac{1}{1-z^{p_i p_j}} + \cdots + (-1)^k \frac{1}{1-z^{p_1 \cdots p_k}} = \sum_{p_1, \dots, p_k \nmid n} z^n$$

for $|z| < 1$. If there were only finitely many primes $p_1, \dots, p_k$, then this would be z^1. But letting $z \to e^{2\pi i/(p_1 \cdots p_k)}$ within $|z| < 1$ yields a contradiction.

Next we will talk more about generating functions.

1 Generating Functions

Idea. Turn a sequence $a_0, a_1, \dots \in \mathbb{C}$ into a generating function, like $\sum_{n\geq 0} a_n z^n$. Then study the function to get information about the sequence.

Note. Power series $\sum_{n\geq 0} a_n z^n$ can be viewed either formally as elements in $\mathbb{C}[\![z]\!]$ with its z-adic topology, or as genuine functions on subsets of $\mathbb{C}$ where they converge. These views are usually compatible, e.g. multipliying two power series formally and then evaluating them gives the same value as first evaluating them and then multiplying the values.

Given a power series $f = \sum_{n\geq 0} a_n z^n$ we write $[z^n]f$ for the coefficient of z^n, i.e. a_n.

Example. We prove that the number of odd partitions of a natural number n equals the number of partitions into distinct parts. The latter is $[z^n](1+z)(1+z^2)(1+z^3)\cdots$. The former is $[z^n](1+z+z^2+\cdots)(1+z^3+z^6+\cdots)\cdots = [z^n]\frac{1}{1-z}\frac{1}{1-z^3}\cdots$. In other words, we want to prove that

$$\frac{1}{1-z}\frac{1}{1-z^3}\frac{1}{1-z^5}\cdots = (1+z)(1+z^2)(1+z^3)\cdots.$$

Indeed, we have

$$\prod_{k\geq 1}(1+z^k) = \prod_{k\geq 1}\left(\frac{1-z^{2k}}{1-z^k}\right) = \prod_{k\geq 1}\frac{1}{1-z^{2k-1}}.$$

Note that this argument works purely formally in $\mathbb{C}[\![z]\!]$ (or even $\mathbb{Z}[\![z]\!]$), we could also interpret this as functions in $\{z \in \mathbb{C} \mid |z| < 1\}$.

Example (Fibonacci numbers)**.** Let F_n be the sequence defined by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$. Then let $f(z) = \sum_{n\geq 0} F_n z^n$. Then we can rewrite the reccurence relation as $f(z) - (0+z) = f(z)z + f(z)z^2$, i.e.

$$f(z) = \frac{z}{1-z-z^2}.$$

By writing out the partial fraction decomposition of the RHS, we obtain an explicit formula for the F_n.

Some identities:

- $\sum_{n=0}^{m}\binom{m}{n}x^n = (1+x)^m$
- $\sum_{n\geq 0}\binom{n+m-1}{m-1}z^n = (1-z)^{-m}$. This follows from the $m=1$ case and then differentiating.
- $\sum_{n\geq 0} p(5n+4)z^n = 5\prod_{n\geq 1}\frac{(1-z^{5n})}{(1-z^n)^6}$ where $p(k)$ is the number of partitions of k. This holds both formally in $\mathbb{C}[\![z]\!]$ and analytically in $|z| < 1$.

Often we want to relate a sequence $(a_n)_n$ with its sequence of partial sums $(A_N)_N$ given by $A_N = \sum_{n=0}^{N} a_n$. If $f(z) = \sum_{n\geq 0} a_n z^n$, then it is easily seen that $\sum_{N\geq 0} A_N z^N = \frac{f(z)}{1-z}$.

Theorem 1.1 (Abel's Limit Theorem). *Let $f(z) = \sum_{n\geq 0} a_n z^n$, $A_N = \sum_{n=0}^N a_n$. Suppose that $A_N \to A$. Then $\lim_{z\to 1^-} f(z) = A$.*

Note that since $a_n \to 0$, $f(z)$ converges in $\{|z| < 1\}$.

Proof. Let $\varepsilon > 0$. We have $\sum_{N\geq 0} A_N z^N = \frac{f(z)}{1-z}$ for $|z| < 1$. Then

$$|f(z) - A| = |(1-z)\sum_{N\geq 0}(A_N - A)z^N| \leq |1-z|\Big(\sum_{N<M_\varepsilon}|(A_N - A)z^N| + \varepsilon\sum_{N\geq M_\varepsilon}|z|^N\Big)$$

where M_ε is chosen such that $|A_N - A| < \varepsilon$ for $N \geq M_\varepsilon$. Then

$$|f(z) - A| \leq |1-z|\sum_{N<M_\varepsilon}|A_N - A||z|^n + \varepsilon.$$

Letting $z \to 1$ we see $\limsup_{z\to 1}|f(z) - A| \leq \varepsilon$. □

The converse is not true, take e.g. $a_n = (-1)^n$.

Theorem 1.2 (Tauber's First Theorem). *The converse holds as long as $a_n = o(1/n)$ as $n \to \infty$, i.e. if $f(z) = \sum_{n\geq 0} a_n z^n$ converges as $z \to 1$, then $\sum_n a_n$ converges.*

Proof. Note that $|1 - z^n| \leq n|1-z|$ for $|z| < 1$. Then for $z = 1 - \frac{1}{N}$ we have

$$|\sum_{n=0}^N a_n - f(z)| = |\sum_{n=0}^N a_n(1-z^n) - \sum_{n=N+1}^\infty a_n z^n| \leq \sum_{n=0}^N n|1-z||a_n| + \underbrace{\frac{1}{N}\sum n|a_n||z|^n}_{\leq \frac{1}{N(1-|z|)}\sup_{n>N} n|a_n|}$$

$$\leq \frac{1}{N}\sum_{n=0}^N n|a_n| + \sup_{n>N} n|a_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2}$$

for N large enough (for the first term use Cesaro-limit). □

In fact, the following is true:

Theorem 1.3 (Tauber's Second Theorem). *The converse of Abel's theorem holds if and only if $A_N - \frac{\sum_{n=0}^{N-1} A_n}{N} \to 0$ as $N \to \infty$.*

2 Smooth Sums

Theorem 2.1 (Abel's Summation Formula). *Suppose $f(n)$ is continuously differentiable and $a_0 = A_0 = 0$, then*

$$\begin{aligned}\sum_{n=1}^{N} a_n f(n) &= \sum_{n=1}^{N} f(n)(A(n) - A(n-1)) \\ &= A(N)f(N) - \sum_{n=1}^{N-1} A(n)(f(n+1) - f(n)) \\ &= A(N)f(N) - \sum_{n=1}^{N-1} \int_n^{n+1} A(x)f'(x)dx \\ &= A(N)f(N) - \int_1^N A(x)f'(x)dx\end{aligned}$$

We can write $\sum_{n=1}^{N} a_n f(n) = \int_0^N f(x)dA(x)$ (Riemann-Stieltjes Integral). Then Abel's summation formula is integration by parts for this integral.

Theorem 2.2 (Kronecker's Lemma). *Suppose $f : [0,\infty) \to (0,\infty)$ is decreasing to 0 and differentiable. If $\sum_{n\geq 0} a_n f(n)$ converges, then $f(N)\sum_{n\leq N} a_n \to 0$ as $N \to \infty$.*

Example. Let μ be the Möbius function, i.e. $\mu(n)$ is the number of prime factors of n if n is squarefree and 0 otherwise. Suppose that $\sum_{n\geq 1} \frac{\mu(n)}{n}$ converges. Then we get $\frac{1}{N}\sum_{n=1}^{N} \mu(n) \to 0$ as $N \to \infty$ and this easily implies the Prime Number Theorem (but the convergence of $\sum_{n\geq 1} \frac{\mu(n)}{n}$ is not so easy).

Proof. Let $\varepsilon > 0$. Let $A(N) = \sum_{n=1}^{N} a_n = \sum_{n\leq N} a_n f(n) \frac{1}{f(n)}$ and $S(N) = \sum_{n\leq N} a_n f(n)$. Since $S(N) \to S$, there exists N_0 such that $|S(N) - S| < \varepsilon$ for all $N \geq N_0$. By Abel summation we have

$$\begin{aligned}|A(N)| &= \left| \frac{S(N)}{f(N)} + \int_1^N S(x)\frac{f'(x)}{f(x)^2}dx \right| \\ &= \left| \int_0^N (-S(N) + S(x))\frac{f'(x)}{f(x)^2}dx + \frac{S(N)}{f(0)} \right| \\ &\leq \left| \int_0^{N_0} (-S(N) + S(x))\frac{f'(x)}{f(x)^2}dx \right| + \left| \int_{N_0}^N (-S(N) + S(x))\frac{f'(x)}{f(x)^2}dx \right| + \left| \frac{S(N)}{f(0)} \right| \\ &\leq C + 2\varepsilon \int_{N_0}^N \left| \frac{f'(x)}{f(x)^2} \right| dx \\ &= C + 2\varepsilon \left(\frac{1}{f(N)} - \frac{1}{f(N_0)} \right)\end{aligned}$$

$$\leq \frac{2\varepsilon}{f(N)} + \tilde{C}$$

Here $C, \tilde{C} > 0$ are some constants (depending on N_0). We then see that

$$\limsup_{N\to\infty} |f(N)A(N)| \leq 2\varepsilon,$$

so our claim follows. □

Theorem 2.3 (Euler's Summation Formula)**.** *For any function f with continuous derivative on $[1, n]$ we have*

$$\sum_{n=1}^{N} f(n) = \int_1^N f(x)dx + \int_1^N \{x\}f'(x)dx + f(1).$$

Here $\{x\} := x - \lfloor x \rfloor$ denotes the fractional part of x.

Proof. Let $a_n = 1$ in Abel's summation formula. Then $A(x) = \lfloor x \rfloor$, so

$$\begin{aligned}
\sum_{n=1}^{N} f(n) &= Nf(N) - \int_1^N \lfloor x \rfloor f'(x)dx \\
&= Nf(N) - \int_1^N (x - \{x\})f'(x)dx \\
&= Nf(N) - \int_1^N xf'(x)dx + \int_1^N \{x\}f'(x)dx \\
&= \int_1^N f(x)dx + \int_1^N \{x\}f'(x)dx + f(1).
\end{aligned}$$

□

Example. Take $f(x) = \frac{1}{x}$. As $\int_1^N \{x\}\frac{1}{x^2}dx$ converges as $N \to \infty$, this shows that $\sum_{n=1}^N \frac{1}{n} - \log N$ converges to a non-negative number, called *Euler-Mascheroni constant.*

An *Appell sequence* is a sequence of polynomials A_n such that $\deg A_n = n$ and $A_n'(x) = nA_{n-1}(x)$. So

$$\begin{aligned}
A_0 &= a_0 \\
A_1 &= a_0x + a_1 \\
A_2 &= a_0x^2 + 2a_1x + a_2 \\
&\cdots
\end{aligned}$$

In general there are numbers $a_0, a_1, \ldots$ such that $A_n = \sum_{k=0}^n a_k \binom{n}{k} x^{n-k}$.

Let $G(x,z) = \sum_{k=0}^{\infty} A_k(x)\frac{z^k}{k!}$ be the (exponential) generating function of $A_n(x)$. We then have

$$\frac{\partial}{\partial x}G(x,z) = \sum_{k=1}^{\infty} A_{k-1}\frac{z^k}{(k-1)!} = zG(x,z).$$

From this we get $G(x,z) = g(z)e^{zx}$ for some power series $g(z)$.

We want to find an Appell sequence $B_0, B_1, \dots$ such that $B_0 = 1$ and $\int_0^1 B_i(x)dx = 0$ for $i > 0$, so $\int_0^1 e^{zx}g(z)dx = 1$ for all z, thus $\left[g(z)\frac{e^{zx}}{z}\right]_0^1 = 1$, i.e. $g(z)\frac{e^z-1}{z} = 1$, so $g(z) = \frac{z}{e^z-1}$, and then $G(x,z) = \frac{ze^{xz}}{e^z-1}$.

We have

$$\begin{aligned} B_0 &= 1, \\ B_1(x) &= x - \frac{1}{2}, \\ B_2(x) &= x^2 - x + \frac{1}{6}, \\ B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x \end{aligned}$$

Let $B_k = B_k(0)$.

Theorem 2.4.

(i) $B_n(x) = \sum_{k=0}^{n} B_k\binom{n}{k}x^{n-k}$.

(ii) $B_k(1) = B_k(0)$ *for* $k \neq 1$. *Also* $B_1(0) = -\frac{1}{2}$, $B_1(1) = \frac{1}{2}$.

(iii) $B_{2k+1} = 0$ *for* $k \geq 1$.

(iv) $\frac{B_{k+1}(x+1) - B_{k+1}(x)}{k+1} = x^k$ *for all* $k \geq 0$.

(v) $B_k(1-x) = (-1)^k B_k(x)$ *for all* k

Proof.

(i) $\sum_{k,n\geq 0} B_k(x)\frac{z^n}{n!} = \frac{ze^{xz}}{e^z-1} = \frac{z}{e^z-1}e^{xz} = \left(\sum_{k\geq 0} B_k\frac{z^k}{k!}\right)\left(\sum_{n\geq 0}\frac{(xz)^k}{k!}\right)$. Now compare coefficients.

(ii) Follows from (iv), or directly $B_k(1)$ has generating function $\frac{e^z z}{e^z-1} = z + \frac{z}{e^z-1}$ from which our claim is immediate. Alternatively use $\int_0^1 B_k(x)dx = 0$.

(iii) Note that $\frac{z}{2} + \frac{z}{e^z-1}$ is even.

(iv) The exponential generating function of the LHS is $\frac{e^{(x+1)z}}{e^z-1} - \frac{e^{xz}}{e^z-1} = e^{xz}$ which is the exponential generating function of the RHS.

(v) For k odd this says $B_k(1-x)+B_k(x)=0$ and for k even, $B_k(1-x)-B_k(x)=0$. For $k=0$ this holds trivially, the general case follows by induction (using (ii) and (iii)).

□

Some Bernoulli numbers:

n	0	1	2	4	6	8	10	12	14
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$

We know that $\frac{z}{e^z-1}$ has its smallest singularity at $z=2\pi i$, hence

$$(2\pi)^{-1}=\limsup_{k\to\infty}\left(\frac{B_k}{k!}\right)^{1/k}.$$

We will get better bounds.

Theorem 2.5. $\sum_{n=0}^N n^k=\frac{B_{k+1}(N+1)-B_{k+1}(0)}{k+1}$

Proof.

$$\sum_{n=0}^N n^k=\sum_{n=0}^N\frac{B_{k+1}(n+1)-B_{k+1}(n)}{k+1}=\frac{B_{k+1}(N+1)-B_{k+1}(0)}{k+1}.$$

□

Let $P_k(x)=\frac{1}{k!}B_k(\{x\})$. We can then rewrite Theorem 2.3 as:

$$\sum_{n=1}^N f(n)-\int_1^N f(x)dx=\frac{f(1)+f(N)}{2}+\int_1^N P_1(x)f'(x)dx.$$

Note that since $\int_0^1 B_k(t)dt=0$, we have $\int_0^x P_k(t)dt=\frac{1}{k!}\int_0^{\{x\}}B_k(t)dt=\frac{1}{(k+1)!}(B_{k+1}(\{x\})-B_{k+1}(0))$, so $P'_{k+1}=P_k$ for all k. Therefore we have:

$$\begin{aligned}\int_1^N P_1(x)f'(x)dx&=[P_2f']_1^N-\int_1^N P_2(x)f''(x)dx\\&=\frac{B_2}{2!}(f'(N)-f'(1))-\int_1^N P_2(x)f''(x)dx\\&=\frac{B_2}{2!}(f'(N)-f'(1))-[P_3f'']_1^N+\int_1^N P_3(x)f'''(x)dx\\&=\frac{B_2}{2!}(f'(N)-f'(1))+\frac{B_4}{4!}(f'''(N)-f'''(1))-\int_1^N P_4(x)f''''(x)dx.\end{aligned}$$

To summarise:

Theorem 2.6 (Euler-MacLaurin Summation)**.** *Let* $f \in C^{2r+1}([1,N])$*. Then:*

$$\sum_{n=1}^{N} f(n) - \int_1^N f(x)dx = \frac{f(1)+f(N)}{2} + \frac{B_2}{2!}(f'(N) - f'(1)) + \frac{B_4}{4!}(f'''(N) - f'''(1)) + \cdots + \frac{B_{2r}}{(2r)!}(f^{(2r-1)}(N) - f^{(2r-1)}(1)) + \int_1^N P_{2r+1}(x) f^{(2r+1)}(x)dx.$$

To bound the integral remainder term, we want bounds on P_{2r+1}. The Fourier expansion of $P_1(x) = \{x\} - \frac{1}{2}$ is given by

$$P_1(x) = -\sum_{n=1}^{\infty} \frac{\sin(2\pi n x)}{n\pi}.$$

From this it easily follows that

$$P_{2k}(x) = (-1)^{k-1} \sum_{n=1}^{\infty} \frac{2\cos(2n\pi x)}{(2n\pi)^{2k}},$$

$$P_{2k+1}(x) = (-1)^{k-1} \sum_{n=1}^{\infty} \frac{2\sin(2n\pi x)}{(2n\pi)^{2k+1}}.$$

Plugging in $x = 0$ into $P_{2k}(x)$, gives

$$\frac{B_{2k}}{(2k)!} = (-1)^{k-1} 2 (2\pi)^{-2k} \sum_{n=1}^{\infty} \frac{1}{n^{2k}}$$

We also get the bound $|P_k(x)| \leq \frac{4}{(2\pi)^k}$ for all x.

2.1 Analytic Continuation of $\zeta(s)$

The *Riemann ζ-function* is defined by

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

for $\operatorname{Re} s > 1$. We will usually write $s = \sigma + it$. The series defining ζ converges locally uniformly in $\sigma > 1$.

Theorem 2.7. *For* $\operatorname{Re} s > 1$*,*

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{\infty} \frac{\{x\}}{x^{s+1}} dx.$$

Proof. $\zeta(s) - \int_1^{\infty} x^{-s} dx = \int_1^{\infty} \frac{-s\{x\}}{x^{s+1}} dx + 1$ by the Euler summation formula, and we are done. □

Now the integral on the right converges for $\operatorname{Re} s > 0$.

Theorem 2.8.

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \frac{s}{12} - s(s+1)(s+2)\int_1^\infty \frac{2\{x\}^3 - 3\{x\}^2 + \{x\}}{12x^{s+3}}dx.$$

This extends $\zeta(s)$ to $\operatorname{Re} s > -2$ and we get $\zeta(0) = -\frac{1}{2}$. More generally:

Theorem 2.9.

$$\zeta(s) = \frac{1}{s-1} + \frac{1}{2} + \sum_{k=1}^{r} \frac{B_{2k}}{2k}\binom{s+2k-2}{2k-1} - \int_1^\infty \frac{B_{2r+1}(\{x\})\binom{s+2r}{2r+1}}{x^{s+2r+1}}dx.$$

Proof. Let $f(x) = x^{-s}$. Then $f^{(k)}(x) = \frac{(-s)(-s-1)\ldots(-s-k)}{x^{s+k}} = \frac{(-1)^k\binom{s+k-1}{k}k!}{x^{s+k}}$. So

$$\begin{aligned}
\zeta(s) - \int_1^\infty \frac{dx}{x^s} &= \frac{1}{2} + \sum_{k=1}^{r} \frac{B_{2k}}{(2k)!}[f^{(2k-1)}(x)]_1^\infty + \int_1^\infty P_{2r+1}(x) f^{(2r+1)}(x)dx \\
&= \frac{1}{2} + \sum_{k=1}^{r} \frac{B_{2k}}{2k}\binom{s+2k-2}{2k-1} - \int_1^\infty \frac{B_{2r+1}(\{x\})\binom{s+2r}{2r+1}}{x^{s+2r+1}}dx.
\end{aligned}$$

□

This shows that ζ extends analytically to $\mathbb{C} \setminus \{1\}$ with a simple pole of residue 1 at $s = 1$.

Theorem 2.10. *Given an integer $m \geq 2$, $\zeta(1-m) = \frac{-B_m}{m}$.*

Proof. Let $r \geq m/2$ in the previous theorem. Then $\binom{1-m+2r}{2r+1} = 0$, so the integral term vanishes and then

$$\begin{aligned}
\zeta(1-m) &= \frac{-1}{m} + \frac{1}{2} + \frac{B_2}{2}\binom{1-m}{1} + \frac{B_4}{4}\binom{3-m}{3} + \ldots \\
&= \frac{-1}{m}(B_0 + B_1\binom{m}{1} + B_2\binom{m}{2} + \cdots + B_m\binom{m}{m}) \\
&= \frac{-B_m}{m}.
\end{aligned}$$

The last equality follows from $\sum_{k=0}^{n-1} B_k\binom{n}{k} = 0$ for $n > 1$. □

The Bernoulli numbers appear both in $\zeta(2k)$ and in $\zeta(1-2k)$, this suggests there might be a general connection between these values. This is indeed the case, and for this we need the Gamma function.

2.2 The Gamma Function

Euler's definition of the Gamma function:

$$\Gamma(s) = \lim_{N\to\infty} N^s \frac{(N-1)!}{s(s+1)\dots(s+N-1)}.$$

We see that $\Gamma(1) = 1$. Also note that

$$s\Gamma(s) = \lim_{N\to\infty} \frac{sN}{N+s}\Gamma(s) = \Gamma(s+1).$$

Theorem 2.11. *For* $\operatorname{Re} s > 0$*,*

$$\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt.$$

Proof idea. Write $e^{-t} = \lim_{N\to\infty}(1-t/N)^N$ and integrate by parts. See notes for details. $\square$

Some more identities:

$$\begin{aligned}\frac{1}{\Gamma(s)} &= \lim_{N\to\infty} \frac{s}{N^s}\prod_{n=1}^{N-1}\frac{s+n}{n} \\ &= \lim_{N\to\infty} s e^{(\sum_{n=1}^{N-1}\frac{1}{n}-\log N)s}\prod_{n=1}^{N-1} e^{-s/n}(1+\frac{s}{n}) \\ &= s e^{\gamma s}\prod_{n=1}^{\infty} e^{-s/n}\left(1+\frac{s}{n}\right).\end{aligned}$$

Theorem 2.12 (Complex Stirling Formula)**.**

$$\log\Gamma(s) = (s-\frac{1}{2})\log s - s + \frac{1}{2}\log 2\pi + O(|s|^{-1})$$

uniformly in $\{|\arg(s)+\pi| \geq \delta\}$*.*

Using the Gamma function we obtain another way of analytically continuing the Zeta function.

Theorem 2.13.

$$\zeta(s) = \frac{1}{\Gamma(s)}\int_0^\infty \frac{x^{s-1}dx}{e^x - 1}$$

for $\operatorname{Re} s > 1$*.*

Proof. $\int_0^\infty e^{-nx} x^{s-1} dx = \frac{\Gamma(s)}{n^s}$. Sum over these and we get

$$\sum_{n=1}^{\infty} \frac{\Gamma(s)}{n^s} = \int_0^\infty \frac{x^{s-1}}{e^x - 1} dx.$$

□

Let $G(s) = \int_\varepsilon^\infty \frac{x^{s-1}}{e^x-1} dx$ and $F(s) = \int_0^\varepsilon \frac{x^{s-1}}{e^x-1} dx$ for some fixed $\varepsilon > 0$. Then $G(s)$ is entire, so only need to deal with $F(s)$ in order to analytically continue $\zeta(s)$.

We have $\frac{1}{e^x-1} = \frac{1}{x} - \frac{1}{2} - \sum_{n=1}^\infty \frac{B_{2n}}{(2n)!} x^{2n-1}$. Then

$$\begin{aligned} F(s) &= \int_0^\varepsilon \frac{x^{s-1}}{e^x - 1} dx \\ &= \varepsilon^{s-1} \Big(\frac{1}{s-1} - \frac{\varepsilon}{2s} - \sum_{n=1}^\infty \frac{B_{2n}}{(2n)!} \frac{\varepsilon^{2n}}{2n+s-1} \Big). \end{aligned}$$

Now the RHS is analytic in $\mathbb{C} \setminus (\{0, 1\} \cup \{1 - 2n \mid n \geq 1\})$. The poles at 0 and $1 - 2n$ cancel with those of Γ, hence $\zeta(s)$ is analytic in $\mathbb{C} \setminus \{1\}$.

3 Dirichlet Series

Power series $\sum_{n\geq 0}$ are good for additive problems, since $z^n z^m = z^{n+m}$. For multiplicative problems we replace z^n by n^z, so that $n^z m^z = (nm)^z$. This leads to Dirichlet series.

A *Dirichlet series* is a series $\sum \frac{a_n}{n^s}$ associated with a sequence a_n. If $a_n = f(n)$ where $f : \mathbb{N} \to \mathbb{C}$ is an arithmetical function, we write $D(f,s) = \sum \frac{f(n)}{n^s}$. As in the case of power series, we can view Dirichlet series either as formal series or as analytic functions (where they converge),.

Note that $D(f,s) + D(g,s) = D(f+g,s)$ and $D(f,s)D(g,s) = D(f*g,s)$ where

$$(f*g)(n) = \sum_{d|n} f(d)g(n/d)$$

is the (Dirichlet) convolution of f and g.

We have $g*f = f*g$, $f*(g*h) = (f*g)*h$.

f is a *multiplicative function* if $f(nm) = f(n)f(m)$ for n,m with $(n,m) = 1$. If $f(nm) = f(n)f(m)$ for all n,m, then f is *completely multiplicative.*

It is easily seen that the convolution of multiplicative functions is again multiplicative. The set of multiplicative functions that are not constant 0 are an abelian group under $*$ with identity $\mathbb{1}(n=1)$ where $D(\mathbb{1}(n=1),s) = 1$.

The inverse f^{-1} of f can be easily determined recursively. To see that f^{-1} is again multiplicative, note that if f and $f*g$ are multiplicative, then so is g (if not, pick a minimal counterexample,...).

Nota that a multiplicative function is uniquely determined by its values on prime powers.

We define the *Möbius function* μ by $\mu(p) = 1$ and $\mu(p^k) = 0$ for primes p and $k \geq 2$ and then extend multiplicatively.

We then have the identity

$$1 * \mu = \mathbb{1}(n=1).$$

In other words

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1, \\ 0 & n > 1. \end{cases}$$

This can be seen e.g. from the inclusion exclusion principle or using the multiplicativity it suffices to check it for prime powers in which case it is obvious.

This gives the following result.

Theorem 3.1 (Möbius inversion)**.** *For functions $f,g : \mathbb{N} \to \mathbb{C}$ we have $g = 1*f$ iff $f = \mu * g$. If this holds, then $D(f,s)\zeta(s) = D(g,s)$. In particular $\zeta(s)^{-1} = D(\mu,s)$*

Theorem 3.2 (Euler Product). *If $f : \mathbb{N} \to \mathbb{C}$ is multiplicative and $f(1) = 1$, then*

$$D(f,s) = \prod_p (1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \dots).$$

E.g. $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$.

So far we only dealt with Dirichlet series formally, now we will care about convergence.

3.1 Convergence and Non-vanishing of Dirichlet Series

Theorem 3.3. *$D(f,s)$ converges absolutely iff $\sum_{m,p} \left|\frac{f(p^m)}{p^{ms}}\right|$ converges.*

Proof. $D(f,s)$ converges absolutely iff its Euler product converges absolutely, and $\prod_n (1 + a_n)$ converges absolutely iff $\sum_n |a_n|$ converges. □

In particular $\frac{1}{\zeta(s)} = \sum_{n \geq 1} \frac{\mu(n)}{n^s}$ converges absolutely for $\operatorname{Re} s > 1$, so $\zeta(s) \neq 0$ in this region. This also follows from the Euler product.

A *general Dirichlet series* has the form $\sum_{n \geq 1} a_n e^{-\lambda_n s}$ with $\lambda_n \nearrow +\infty$.

E.g. taking $\lambda_n = n$ gives $\sum a_n (e^{-s})^n = \sum a_n z^n$ with $z = e^{-s}$. And for $\lambda_n = \log n$ we get ordinary Dirichlet series.

Note that $\sum_{n \geq 1} a_n e^{-\lambda_n s} = \int_0^\infty e^{-st} dA(t)$ when $A(t) = \sum_{\lambda_n \leq t} a_n$.

Theorem 3.4. *If a Dirichlet series $\sum a_n / n^s$ converges at $s_0 \in \mathbb{C}$, then it converges uniformly in every angular sector $\frac{|s - s_0|}{\sigma - \sigma_0} \leq \frac{1}{\cos \phi}$ for every $0 \leq \phi < \pi/2$.*

Proof. By replacing a_n by $n^{s_0} a_n$ we may assume $s_0 = 0$, so $\sum_n a_n$ converges. Let $R(u) = \sum_{n > u} a_n$ so that $R(u) \to 0$ as $u \to \infty$.

$$\begin{aligned}
\sum_{n=M+1}^{N} \frac{a_n}{n^s} &= \int_M^{N^+} \frac{-1}{x^s} dR(x) \\
&= [-R(x)/x^s]_M^{N^+} + \int_M^{N^+} \frac{s}{x^{s+1}} R(x) dx \\
&= \frac{R(M)}{M^s} - \frac{R(N)}{N^s} + s \int_M^{N^+} \frac{s}{x^{s+1}} R(x) dx
\end{aligned}$$

So

$$\left| \sum_{n=M+1}^{N} \frac{a_n}{n^s} \right| \leq \varepsilon + \varepsilon + \varepsilon \left| s \int_M^\infty x^{-(s+1)} dx \right|$$

$$\leq 2\varepsilon + \varepsilon(|s|/\sigma).$$

□

This shows that for a Dirichlet series $f(s) = \sum_n a_n n^{-s}$ there exists a number $\sigma_c \in \mathbb{R} \cup \{\pm 1\}$, called the *abscissa of convergence* of f, such that $f(s)$ converges for $\operatorname{Re} s > \sigma_c$ and diverges for $\operatorname{Re} s < \sigma_c$. Similarly, there is the abscissa of absolute convergence σ_a which is the abscissa of convergence of $\sum_n |a_n| n^{-s}$.

Note that $\sigma_c \leq \sigma_a$ and $\sigma_a - \sigma_c \leq 1$. Indeed, if $\sum_n a_n n^{-s}$ converges for some s, then $|a_n n^{-s}| < 1$ for large n and then $|a_n n^{-(s+\delta+1)}| < n^{-(1+\delta)}$ for large n, hence $\sum_n a_n n^{-(s+1+\delta)}$ is absolutely convergent.

Theorem 3.5. *If $A(N) = \sum_{n=1}^N a_n = O(N^{\alpha+\varepsilon})$ for every $\varepsilon > 0$, then $\sum_{n=1}^\infty a_n n^{-s} = s\int_1^\infty \frac{A(x)}{x^{s+1}} dx$ converges for $\operatorname{Re} s > \alpha$.*

Proof.

$$\sum_{n=1}^N a_n n^{-s} = \int_{1^-}^{N^+} x^{-s} dA(x) = [A(x)x^{-s}]_1^N - \int_{1^-}^{N^+} (-s)x^{-(s+1)}A(x)dx$$

converges. □

From the theorem we get

$$\sigma_c \leq \limsup_{x\to\infty} \frac{\log A(x)}{\log x}.$$

If $\sum a_n n^{-\alpha}$ converges, then by Kronecker's Lemma $N^{-\alpha}\sum_{n=1}^N a_n \to 0$, so $\sum_{n=1}^N a_n = O(N^\alpha)$, so

$$\sigma_c = \limsup_{x\to\infty} \frac{\log A(x)}{\log x}.$$

Theorem 3.6 (Landau)**.** *If $a_n \geq 0$, then σ_c is a singularity of $f(s)$.*

Theorem 3.7 (Ramanujan)**.**

$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)} = \sum_{n=1}^\infty \frac{\sigma_a(n)\sigma_b(n)}{n^s},$$

where $\sigma_a(n) = \sum_{d|n} d^a$ and $\operatorname{Re} s > \max\{1, \operatorname{Re} a + 1, \operatorname{Re} b + 1, \operatorname{Re}(a+b)+1\}$. In particular

$$\frac{\zeta(s)^4}{\zeta(2s)} = \sum_{n\geq 1} \frac{d(n)^2}{n^s},$$

where $d(n) = \sum_{d|n} 1$ is the number of divisors of n.

Proof. Let $z = p^{-s}$. Then compare the Euler products. The LHS is

$$\prod_p \frac{1 - p^{a+b} z^2}{(1-z)(1-p^a z)(1-p^b z)(1-p^{a+b} z)}$$

and the RHS

$$\prod_p \Big(\sum_{n \geq 0} \sigma_a(p^n) \sigma_b(p^n) z^n \Big) = \prod_p \Big(\sum_{n \geq 0} \frac{p^{a(n+1)} - 1}{p^a - 1} \frac{p^{b(n+1)} - 1}{p^b - 1} z^n \Big).$$

It is now straightforward to verify these two are equal. □

Corollary 3.8. *For any $0 \neq t \in \mathbb{R}$, we have $\zeta(1+it) \neq 0$.*

Proof. Suppose $\zeta(1+it) = 0$. Then also $\zeta(1-it) = 0$. Let $a = it, b = -it$ in the previous theorem. Then

$$\frac{\zeta(s)^2 \zeta(s+it)\zeta(s-it)}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{\sigma_{it}(n)\sigma_{-it}(n)}{n^s} = \sum_{n=1}^{\infty} \frac{|\sigma_{it}(n)|^2}{n^s}.$$

Now at $s = 1$, the zeros at $\zeta(s+it)$ and $\zeta(1-it)$ cancel the double pole of $\zeta(s)^2$, hence the LHS has no poles in $(-1, \infty)$. The RHS is a Dirichlet series with non-negative real coefficients, hence by Landau's theorem it converges in $(-1, \infty)$. But this is clearly impossible. □

4 Primes in Arithmetic Progressions

Let G be a finite abelian group. Then a *character* χ of G is a homomorphism $\chi : G \to \mathbb{C}^\times$. Let $q \geq 1$ be an integer.A *Dirichlet character* $\chi : \mathbb{Z} \to \mathbb{C}^\times$ mod q is a function of the form

$$\chi(n) = \begin{cases} \tilde{\chi}(n \bmod q) & (q,n) = 1 \\ 0 & (q,n) > 1 \end{cases}$$

for some character $\tilde{\chi}$ of $(\mathbb{Z}/q\mathbb{Z})^\times$. The trivial character mod q is denoted χ_0 (i.e. $\chi_0(n) = 1$ if $(q,n) = 1$).

We recall the following basic facts about characters:

Theorem 4.1.

$$\sum_{n=1}^{q} \chi(n) = \begin{cases} \varphi(q) & \chi = \chi_0, \\ 0 & \chi \neq \chi_0. \end{cases}$$

Theorem 4.2.

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(q) & n \equiv 1 \pmod{q}, \\ 0 & n \not\equiv 1 \pmod{q}. \end{cases}$$

Corollary 4.3. *If* $(a,q) = 1$*, then*

$$\sum_{\chi} \chi(n)\overline{\chi}(a) = \begin{cases} \varphi(q) & n \equiv a \pmod{q}, \\ 0 & n \not\equiv a \pmod{q}. \end{cases}$$

Here the sums run over all characters χ mod q.

Given a Dirichlet character χ mod q, the corresponding *Dirichlet L-function* (mod q) is defined for $\operatorname{Re} s > 1$ by

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

Theorem 4.4 (Dirichlet's Theorem)**.** *There exist infinitely many primes* $\equiv a \pmod{q}$ *where* $(a,q) = 1$.

Proof. $\log L(s,\chi) = \sum_p \sum_{m \geq 1} \frac{\chi(p^m)}{mp^{ms}}$. And

$$\begin{aligned} \frac{1}{\varphi(q)} \sum_{\chi} \overline{\chi}(a) \log L(s,\chi) &= \frac{1}{\varphi(q)} \sum_p \sum_{m=1} \frac{1}{mp^{ms}} \left(\sum_{\chi} \chi(p^m)\overline{\chi}(a) \right) \\ &= \sum_p \sum_{\substack{m=1 \\ p^m \equiv a \bmod q}} \frac{1}{mp^{sm}} \end{aligned}$$

$$\leq C + \sum_{p \equiv a \bmod q} \frac{1}{p^s}.$$

We have $L(s, \chi_0) = \prod_{p|q}(1 - p^{-s})\zeta(s)$, so $\lim_{\sigma \to 1^+} \log L(\sigma, \chi_0) = \infty$. So we only need to prove that $\log L(s, \chi)$ is bounded around $s = 1$ for $\chi \neq \chi_0$. This follows from the following three theorems. □

Theorem 4.5. *For* $\chi \neq \chi_0$*,*

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = s \int_1^{\infty} \Big(\sum_{n \leq x} \chi(n) \Big) x^{-s-1} dx$$

converges for $\operatorname{Re} s > 0$*.*

Proof. By Theorem 4.1, the partial sums $\sum_{n \leq x} \chi(n)$ are bounded. Then the result follows from Theorem 3.5. □

Theorem 4.6. $L(1, \chi) \neq 0$ *if* $\chi \neq \overline{\chi}$*, i.e. if* χ *is a complex character.*

Proof. Let $Z(s) = \prod_\chi L(s, \chi)$. Suppose that $L(1, \chi) = 0$ for some $\chi \neq \bar{\chi}$. Then also $L(1, \overline{\chi}) = 0$ and the double zero of $L(s, \chi)L(s, \overline{\chi})$ cancels the pole of $L(s, \chi_0)$ at $s = 1$ and we get $Z(1) = 0$. From the above expression with $a = 1$ it is easily seen that $\frac{1}{\varphi(q)} \sum_\chi \log L(s, \chi) \geq 0$ for $\operatorname{Re} s > 1$, hence $|Z(s)| \geq 1$ for $\operatorname{Re} s > 1$ which gives a contradiction. □

We now give another proof of this which also includes the case where χ is a non-trivial real character. For this we need:

Theorem 4.7.

$$Z(s) = \prod_{p \nmid q} (1 - p^{-s \operatorname{ord}_q p})^{-\varphi(q)/\operatorname{ord}_q p}$$

for $\operatorname{Re} s > 1$*.*

Proof. Fix a prime $p \nmid q$ and let $r = \operatorname{ord}_q p$. It suffices to prove that

$$\prod_\chi (1 - \chi(p)p^{-s}) = (1 - p^{-sr})^{\varphi(q)/r}.$$

It is easy to see that as χ runs through the characters mod q, $\chi(p)$ takes on every r-th root of unity exactly $\varphi(q)/r$ times, hence

$$\prod_\chi (1 - \chi(p)p^{-s}) = \prod_{\zeta^r = 1} (1 - \zeta p^{-s})^{\varphi(q)/r} = (1 - p^{-sr})^{\varphi(q)/r}.$$

□

Theorem 4.8. *$L(1,\chi) \neq 0$ if $\chi \neq \chi_0$.*

Proof. Suppose $L(1,\chi) = 0$. Then this zero cancels the pole of $L(s,\chi_0)$ at $s = 1$ in $Z(s)$, hence Z is holomorphic at 1 and thus holomorphic in $\operatorname{Re} s > 0$. Now note that

$$Z(s) = \prod_{p \nmid q} (1 - p^{-s \operatorname{ord}_q p})^{-\varphi(q)/\operatorname{ord}_q p} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

where all c_n are real and non-negative. Hence by Landau's theorem, the Dirichlet series on the right must converge in $(0,\infty)$. Now note that for $\sigma > 1$, we have

$$Z(\sigma) \geq \prod_{p \nmid q} (1 - p^{-\varphi(q)\sigma})^{-1} = \sum_{(n,q)=1} n^{-\varphi(q)\sigma}.$$

Then it must be that the coefficients c_n are greater than or equal to those on the RHS, hence this inequality is also valid in $(0,\infty)$. But this is impossible as the series on the RHS is divergent at $\sigma = \frac{1}{\varphi(q)}$. □

4.1 Gauss Sums

Now consider an odd prime p. Let χ be a non-trivial real character mod p. Then χ is necessarily given by the Legendre symbol, i.e. $\chi(n) = \left(\frac{n}{p}\right)$. We will prove directly $L(1,\chi) \neq 0$ for χ.

Let $\zeta = \exp(2\pi i/p)$. The *Gauss sum* is

$$S_p = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^n = \sum_{k=0}^{p-1} \zeta^{k^2}.$$

One can show that $S_p^2 = p\left(\frac{-1}{p}\right)$

Now suppose $L(1,\chi) = \sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n} = 0$.

Let

$$P = \frac{\prod_{m \in \mathbb{F}_p^\times \setminus (\mathbb{F}_p^\times)^2} (1 - \zeta^m)}{\prod_{r \in (\mathbb{F}_p^\times)^2} (1 - \zeta^r)}$$

Then

$$\begin{aligned} \log P &= \sum_{n=1}^{\infty} \frac{1}{n} \Big(\sum_r \zeta^{rn} - \sum_m \zeta^{mn} \Big) \\ &= \sum_{n=1}^{\infty} \frac{1}{n} \sum_{k=1}^{p-1} \left(\frac{kn}{p}\right) \zeta^k \end{aligned}$$

$$
\begin{aligned}
&= \Big(\sum_{n=1}^{\infty} \frac{\left(\frac{n}{p}\right)}{n}\Big)\Big(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k\Big) \\
&= L(1,\chi) S_p
\end{aligned}
$$

So if $L(1,\chi) = 0$, then $P = 1$. Let c be a quadratic non-residue mod p. Then

$$
1 = P = \prod_{r \in (\mathbb{F}_p^\times)^2} \frac{1 - \zeta^{cr}}{1 - \zeta^r}.
$$

In other words, ζ is a root of $\prod_r \frac{1-x^{cr}}{1-x^r} - 1 =: g(x)$. Since the minimal polynomial of ζ over $\mathbb{Q}$ is $1 + x + \cdots + x^{p-1}$, there is $f(x) \in \mathbb{Z}[x]$ such that $g(x) = f(x)(1 + x + \cdots + x^{p-1})$. Now evaluate at $x = 1$. Then we get $c^{\frac{p-1}{2}} - 1 \equiv 0 \bmod p$, hence c is a quadratic residue mod p, a contradiction!

Now we consider Gauss sums not necessarily mod primes.

Theorem 4.9.

$$
S_n := \sum_{k=0}^{n-1} \zeta^{k^2} = \frac{1 + (-i)^n}{1 - i} \sqrt{n}
$$

where $\zeta = e^{2\pi i/n}$.

Gauss sums can be defined for any Dirichlet character. If χ is a character mod q (not necessarily prime), then we let

$$
\tau(\chi) = \sum_{n=1}^{q-1} \chi(n) e(n/q),
$$

where $e(x) = \exp(2\pi i x)$. Note that this may be viewed as the discrete Fourier transform $\widehat{\chi}(1)$ of χ. More generally, $\widehat{\chi}(r) = \sum_{n=1}^{q-1} \chi(n) e(nr/q)$. It can also be viewed as a discrete version of the Gamma function.

We say that the character χ mod q is *primitive* if it is not induced by any character χ' mod d for some proper divisor d of q.

Theorem 4.10. $|\tau(\chi)|^2 = q$ *if* χ *is primitive mod* q.

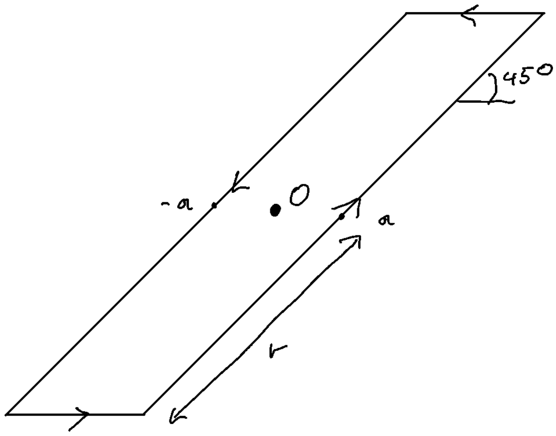
Proof. For $(r, q) = 1$, we have

$$
\begin{aligned}
\chi(r)\widehat{\chi}(r) &= \sum \chi(r)\chi(n) e(rn/q) \\
&= \sum \chi(rn) e(rn/q) \\
&= \tau(\chi).
\end{aligned}
$$

And then in particular $|\widehat{\chi}(r)| = |\tau(\chi)|$. If $(r,q) > 1$, then it is not difficult to see that $\widehat{\chi}(r) = 0$ using that χ is primitive. Now by Parseval we get

$$\varphi(q) = \sum_{n=1}^{q} |\chi(n)|^2 = \frac{1}{q} \sum |\widehat{\chi}(r)|^2 = \frac{\varphi(q)}{q} |\tau(\chi)|^2.$$

□



Contour γ_r

Proof of Theorem 4.9. Let

$$f(z) = \frac{\sum_{k=0}^{n-1} e((z+k)^2/n)}{e(z) - 1}.$$

Consider a parallellogram contour γ_r with center 0, two sides of length r tilted $\pi/4$ relative to the x-axis, two sides parallel to x axis (of length $2a$), as in the figure. Let

$$I(a; f) = \lim_{r \to \infty} \int_{-r}^{r} f(a + te^{\pi i/4}) e^{\pi i/4} dt$$

and

$$I_{\gamma_r} = \int_{\gamma_r} f(z) dz.$$

Take $a = \frac{1}{2}$. Then $z = 0$ is the only singularity of f in γ_r, so by the residue theorem,

$$I_{\gamma_r} = 2\pi i \operatorname{Res}_{z=0} f = \sum_{k=0}^{n-1} \zeta^{k^2} = S_n.$$

We want to compare $I(\frac{1}{2}; f)$ with I_{γ_r}. Note that on the horizontal lines in γ_r, $\mathrm{Re}((z+k)^2)$ will be small, hence $|f(z)|$ will be small and the integral over this part goes to 0 as $r \to \infty$. Hence

$$S_n = \lim_{r \to \infty} I_{\gamma_r} = I(\frac{1}{2}; f) - I(-\frac{1}{2}, f).$$

Now we have:

$$f(z+1)-f(z)=\frac{e((z+n)^2/n)-e(z^2/n)}{e(z)-1}=e(z^2/n)\frac{e(2z)-1}{e(z)-1}=e(z^2/n)(e(z)+1).$$

And therefore

$$S_n=I(\frac{1}{2};f)-I(-\frac{1}{2},f)=I\Big(-\frac{1}{2};e(\frac{z^2}{n})\Big)+I\Big(-\frac{1}{2};e(\frac{z^2}{n}+z)\Big).$$

Let $g(z)=e(z^2/n)$. Note that $e\big(\frac{z^2}{n}+z\big)=e\big(\frac{(z+n/2)^2}{n}\big)e(-n/4)=g(z+n/2)(-i)^n$. Since g is entire we can translate the path of integration and get

$$S_n=I(0;g(z))(1+(-i)^n)=I(0;e(z^2/n))(1+(-i)^n)$$

Now

$$I(0;e(z^2/n))=\int_{-\infty}^{\infty}e^{-2\pi t^2/n}e^{\pi i/4}dt=\sqrt{n}I(0;e(z^2))=\sqrt{n}\frac{S_1}{1+(-i)^1}.$$

Clearly $S_1=1$, hence

$$S_n=\frac{1+(-i)^n}{1-i}\sqrt{n}.$$

□

Note that the proof also gives the classical result

$$\int_{-\infty}^{\infty}e^{-\pi t^2}dt=1.$$

Alternatively one can prove Theorem 4.9 using the following facts:

Theorem 4.11. *For a continuous function f of bounded variation on $[0,1]$, we have*

$$\frac{1}{2}(f(0)+f(1))=\lim_{N\to\infty}\sum_{j=-N}^{N}\int_0^1 f(x)e^{-2\pi ijx}dx.$$

Now sum this to get:

Theorem 4.12 (Poisson Summation)**.** *For a continuous function f of bounded variation on $[0,n]$, we have*

$$\frac{1}{2}f(0)+f(1)+\cdots+f(n-1)+\frac{1}{2}f(n)=\lim_{N\to\infty}\sum_{j=-N}^{N}\int_0^n f(x)e^{-2\pi ijx}dx.$$

To get Theorem 4.9, apply this to $f(x)=e(x^2/n)$. See notes for details.

Theorem 4.13. *If χ is primitive mod q and $\chi(-1) = -1$, then*

$$L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \frac{i\pi}{q^2}\tau(\chi) \sum_{m=1}^{q} m\overline{\chi}(m).$$

Proof. Let $f(x) = \frac{1}{2} - \{x\}$. Then

$$f(x) = \sum_{n=1}^{\infty} \frac{\sin(2n\pi x)}{n\pi}$$

converges locally uniformly on $(0,1)$. Plug in $x = \frac{m}{q}$ and note $\sum_{m=1} \chi(m)\cos(2mn\pi/q) = 0$. Then

$$\begin{aligned} i\sum_{m=1}^{q} \chi(m)\Big(\frac{1}{2} - \frac{m}{q}\Big) &= \sum_{n=1}^{\infty} \frac{\sum_{m=1}^{q} \chi(m) e^{2mn\pi i/q}}{n\pi} \\ &= \sum_{n=1}^{\infty} \frac{\overline{\chi}(n)\tau(\chi)}{n\pi} \\ &= \tau(\chi)\sum_{n=1}^{\infty} \frac{\overline{\chi}(n)}{n\pi}. \end{aligned}$$

So

$$-\frac{i}{q}\sum_{m=1}^{q} m\chi(m) = \tau(\chi)\sum_{n=1}^{\infty} \frac{\overline{\chi}(n)}{n\pi}.$$

Now replace χ by $\overline{\chi}$. We have $\tau(\overline{\chi}) = \overline{\chi(-1)\tau(\chi)}$ and hence $\frac{1}{\tau(\overline{\chi})} = -\frac{\tau(\chi)}{q}$. □

Now suppose that q is prime and $q \equiv 3 \bmod 4$. Take χ to be the quadratic character. Then $\tau(\chi) = i\sqrt{q}$ by Theorem 4.9. Therefore

$$\sum_{n=1}^{\infty} \frac{\left(\frac{n}{q}\right)}{n} = -\frac{\pi}{q\sqrt{q}} \sum_{m=1}^{q-1} m\left(\frac{m}{q}\right).$$

The LHS can also be written as

$$\lim_{s\to 1^+} \sum_{n=1}^{\infty} \left(\frac{n}{q}\right) n^{-s} = \lim_{s\to 1^+} \prod_{p} (1 - \left(\frac{p}{q}\right) p^{-s})^{-1}.$$

This is clearly > 0. Hence

$$\sum_{m=1}^{q-1} m\left(\frac{m}{q}\right) < 0,$$

i.e. the sum of the quadratic non-residues exceeds the sum of the quadratic residues.

5 Chebychev's Estimates

From now on, p will always denote a prime, so e.g. $\sum_{p\le x}$ is the sum over all primes less than or equal to x.

Theorem 5.1. *There exist $a, b > 0$ such that $a < \frac{\pi(x)\log x}{x} < b$ for all $x \ge 2$.*

Proof. Note that $v_p(n!) = \sum_{j=1}^{\infty} \lfloor \frac{n}{p^j} \rfloor$, so

$$v_p\left(\binom{2n}{n}\right) = \sum_{j=1}^{\infty} \left\lfloor \frac{2n}{p^j} \right\rfloor - 2\left\lfloor \frac{n}{p^j} \right\rfloor.$$

All the terms in the sum are 0 or 1, and 1 only if $\{\frac{n}{p^j}\} \ge \frac{1}{2}$. So

$$\binom{2n}{n} \le \prod_{p\le 2n} p^{(\log 2n)/\log p} = (2n)^{\pi(2n)}$$

and also

$$\binom{2n}{n} \ge \prod_{n<p\le 2n} p \ge n^{\pi(2n)-\pi(n)}.$$

But also

$$\frac{2^{2n}}{2n+1} \le \binom{2n}{n} \le 2^{2n}.$$

From this we get

$$\pi(2n) \ge \frac{2n\log 2 - \log(2n+1)}{\log 2n},$$
$$\pi(2n) - \pi(n) \le \frac{2n\log 2}{\log n}.$$

The first inequality immediately gives $\pi(x) \ge a\frac{x}{\log x}$ for some $a > 0$. The second gives

$$\pi(x) \le \pi(\sqrt{x}) + \sum_{j=1}^{\log\sqrt{x}/\log 2} \pi(x/2^{j-1}) - \pi(x/2^j) < \frac{bx}{\log x},$$

for some $b > 0$. □

Chebychev showed that we can take $a = 0.9219\ldots$ and $b = 1.1053\ldots$ for $x \ge 30$. This was enough to show Bertrand's Postulate: There is always a prime between n and $2n$ for $n \ge 1$.

Theorem 5.2. *Let p_n denote the n-th prime number. Then $n\log n \ll p_n \ll n\log n$.*

Proof. Substitute $x = p_n$ in the previous result. Then

$$a\frac{p_n}{\log p_n} < \pi(p_n) = n < b\frac{p_n}{\log p_n}. \qquad (*)$$

We get

$$\frac{n}{b} < \frac{n}{b}\log p_n < p_n < \left(\frac{p_n}{\log p_n}\right)^2 < \left(\frac{n}{a}\right)^2.$$

Hence $\log n \ll \log p_n \ll \log n$. Substitute this back into $(*)$ to get the result. □

Theorem 5.3. $\sum_{p\leq x}\frac{\log p}{p} = \log x + O(1)$.

Proof. The Euler summation formula gives

$$\sum_{n\leq x}\log n = x\log x + -x + O(\log x) = x\log x + O(x).$$

But we also have

$$\sum_{n\leq x}\log n = \sum_{p\leq x}\log p\sum_{j=1}^{\infty}\left\lfloor\frac{x}{p^j}\right\rfloor.$$

The contribution from $j = 1$ is

$$x\sum_{p\leq x}\frac{\log p}{p} - \sum_{p\leq x}(\log p)\left\{\frac{x}{p}\right\} = x\sum_{p\leq x}\frac{\log p}{p} + O(\pi(x)\log x)$$

and $O(\pi(x)\log x) = O(x)$ by Theorem 5.1. The remaining terms contribute at most

$$x\sum_{n\leq x}(\log n)(n^{-2} + n^{-3} + \dots) = x\sum_{n\leq x}\frac{\log n}{n^2 - n} = O(x).$$

Hence the claim. □

Theorem 5.4. *There exists C such that*

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + C + O(1/\log x).$$

Proof. Apply Abel summation with $a_n = \frac{\log n}{n}$ if n is prime and $a_n = 0$ otherwise. Let $f(x) = 1/\log x$. Then

$$\sum_{p\leq x}\frac{1}{p} = \frac{A(x)}{\log x} - \int_2^x \frac{-A(x)}{t(\log t)^2}dt$$

By Theorem 5.3, $A(t) = \log t + \eta(t)$ where $\eta(t) = O(1)$. So

$$\sum_{p\leq x}\frac{1}{p} = 1 + \frac{\eta(x)}{\log x} + \int_2^x\frac{dt}{t\log t} + \int_2^x\frac{\eta(t)}{t(\log t)^2}dt$$

The result follows with $C = 1 - \log\log 2 + \int_2^\infty \frac{\eta(t)dt}{t(\log t)^2}$. □

Theorem 5.5. *There exists a constant C' such that*

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1}=C'\log x+O(1).$$

Proof. We have

$$\begin{aligned}\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1}&=\prod_{p\le x}\exp\left(-\log\left(1-\frac{1}{p}\right)\right)\\&=\prod_{p\le x}\exp\left(\frac{1}{p}+\frac{1}{2p^2}+\frac{1}{3p^3}+\dots\right)\\&=\exp\left(\sum_{p\le x}\frac{1}{p}\right)\exp\left(\sum_{p\le x}\left(\frac{1}{2p^2}+\frac{1}{3p^3}+\dots\right)\right)\end{aligned}$$

Now $D:=\sum_{p=1}^{\infty}\left(\frac{1}{2p^2}+\frac{1}{3p^3}+\dots\right)<\sum_{p=1}^{\infty}\frac{1}{2p(p-1)}$ converges and $\sum_{p>x}\frac{1}{2p(p-1)}=O(1/x)$. Then by the previous theorem:

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1}=\exp(\log\log x+C+O(1/\log x))\exp(D)\exp(O(1/x))$$

Now the result easily follows. □

Remark. Mertens showed $C'=e^{\gamma}$ where γ is the Euler Mascheroni constant.

Theorem 5.6. *If the limit*

$$\lim_{x\to\infty}\pi(x)\frac{\log x}{x}$$

exists, it must be 1.

Proof. Suppose the limit equals l. Use Abel summation with

$$a_n=\begin{cases}1 & n\text{ prime,}\\ 0 & \text{otherwise}\end{cases}$$

and $f(x)=\frac{1}{x}$. Then

$$\sum_{p\le x}\frac{1}{p}=\sum_{n\le x}a_nf(n)=\frac{\pi(x)}{x}+\int_2^x\frac{\pi(x)}{t^2}dt.$$

Now the last integral is asymptotically

$$\int_2^x\frac{l\frac{t}{\log t}+o(1)}{t^2}dt+O(1)=\int_2^x\frac{ldt}{t\log t}=l\log\log x+O(1)$$

But we already know that the sum is $\sim\log\log x$, so $l=1$. □

We define the *Chebychev functions*

$$\theta(x) = \sum_{p \le x} \log p,$$
$$\psi(x) = \sum_{p^m \le x} \log p.$$

We can write $\psi(x) = \sum_{n \le x} \Lambda(n)$ where

$$\Lambda(n) = \begin{cases} \log p & n = p^m, \\ 0 & \text{otherwise} \end{cases}$$

is the *von Mangoldt function*.

Theorem 5.7.

$$\pi(x) = \frac{\theta(x)}{\log x} + O\Big(\frac{x}{\log x^2}\Big).$$

So the Prime Number Theorem $\pi(x) \sim x/\log x$ is equivalent to $\psi(x) \sim x$. Also $\psi(x) \sim x$ iff $x \sim \theta(x)$ as $\psi(x) = \theta(x) + O(\sqrt{x})$.

Proof. Apply Abel summation with $a_n = \log n$ if n is prime and 0 otherwise, and $f(x) = \frac{1}{\log x}$. We get

$$\pi(x) = \sum_{p \le x} 1 = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t(\log t)^2} dt.$$

Since $\pi(x) \ll \frac{x}{\log x}$, we get $\theta(t) \ll t$. Furthermore, $\int_2^x \frac{dt}{(\log t)^2} \sim \frac{x}{(\log x)^2}$ as in Chapter 0. □

Given an arithmetic function $f : \mathbb{N} \to \mathbb{C}$, we define $f' : \mathbb{N} \to \mathbb{C}$ by $f'(n) = f(n) \log n$. Note that $\frac{d}{ds} D(f, s) = -D(f', s)$. We also have $f' + g' = (f + g)'$ and $(f * g)' = f' * g + f * (g')$. Indeed,

$$\begin{aligned}(f * g)'(n) &= \sum_{d|n} f(d)g(n/d) \log n = \sum_{d|n} f(d)g(n/d)(\log d + \log(n/d)) \\ &= \sum_{d|n} f(d)g(n/d) \log d + \sum_{d|n} f(d)g(n/d) \log(n/d)) \\ &= (f' * g)(n) + (f * g')(n).\end{aligned}$$

Theorem 5.8.

$$\Lambda * 1 = 1'$$

Proof.

$$(\Lambda * 1)(n) = \sum_{d|n} \Lambda(d) = \sum_{p^m|n} \log p = \log n.$$

□

Theorem 5.9 (Selberg's Identity)**.**

$$\Lambda(n)\log n+\sum_{d|n}\Lambda(d)\Lambda(n/d)=\sum_{d|n}\mu(d)(\log(n/d))^2.$$

Proof. From $\Lambda*1=1'$ we get

$$1''=\Lambda'*1+\Lambda*1'=\Lambda'*1+\Lambda*(\Lambda*1).$$

Convoluting with μ gives $\Lambda'+\Lambda*\Lambda=\mu*1''$ which is the claim. □

Theorem 5.10.

$$\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}=\frac{-\zeta'(s)}{\zeta(s)}.$$

Proof. The equation $\zeta(s)\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}=-\zeta'(s)$ is equivalent to $1*\Lambda=1'$. Alternatively use the Euler product of ζ and write out $(-\log\zeta(s))'$. □

Theorem 5.11. *Let $M(x)=\sum_{n\le x}\mu(n)$. Suppose that $M(x)=O_A(x/(\log x)^A)$ for all A. Then $\psi(x)=x+O_A(x/(\log x)^A)$ for all A.*

Proof. From $1*\Lambda=1'$ we get $\Lambda=\mu*1'$. Then

$$\begin{aligned}\psi(x)&=\sum_{n\le x}\Lambda(n)=\sum_{n\le x}\sum_{d|n}\mu(d)\log(n/d)\\&=\sum_{dn\le x}\mu(d)\log n=\sum_{d\le\sqrt{x}}\mu(d)\Big(\sum_{n\le x/d}\log n\Big)+\sum_{n\le\sqrt{x}}\log n\Big(\sum_{\sqrt{x}<d\le x/n}\mu(d)\Big)\\&=\sum_{d\le\sqrt{x}}\mu(d)\Big(\frac{x}{d}\log\frac{x}{d}-\frac{x}{d}+O(\log(x/d))\Big)+\sum_{n\le\sqrt{x}}\frac{\log n}{n}O\Big(\frac{x}{(\log x)^A}\Big)\\&=\sum_{d\le\sqrt{x}}\mu(d)\Big(\frac{x}{d}\log\frac{x}{d}-\frac{x}{d}+O(\log(x/d))\Big)+\sum_{n\le\sqrt{x}}\frac{1}{n(\log n)^2}O\Big(\frac{x}{(\log x)^{A-3}}\Big)\\&=\sum_{d\le\sqrt{x}}\mu(d)\Big(\frac{x}{d}\log\frac{x}{d}-\frac{x}{d}+O(\log(x/d))\Big)+O\Big(\frac{x}{(\log x)^{A-3}}\Big)\end{aligned}$$

We have $\sum_{d\ge1}\frac{\mu(d)}{d}=0$ as this is $\lim_{s\to1^+}\frac{1}{\zeta(s)}=0$. Next consider $x\sum_{d\le\sqrt{x}}\frac{\mu(d)}{d}\log d$. We have

$$\sum_{d\ge1}\frac{\mu(n)\log n}{n}=\lim_{s\to1}\sum_{d\ge1}\frac{\mu(n)\log n}{n^s}=\lim_{s\to1}(1/\zeta(s))'=1.$$

We have to check how fast these sums are convergent.

$$\sum_{n>y}\frac{\mu(n)}{n}\log n=\int_y^{\infty}\sum_{y<n\le t}\mu(n)\Big(\frac{\log t-1}{t^2}\Big)dt$$

$$= O\Big(\frac{1}{(\log t)^A}\Big)$$

Therefore:

$$\begin{aligned}
\psi(x) &= x\Big(1 - 0 - \sum_{d>\sqrt{x}} \frac{\mu(d)\log(x/d)}{d} - \frac{\mu(d)}{d}\Big) + \sum_{d\le\sqrt{x}} \mu(d) O(\log(x/d)) + O\Big(\frac{x}{(\log x)^{A-3}}\Big) \\
&= x + O\Big(\frac{x}{(\log x)^{A-3}}\Big).
\end{aligned}$$

□

6 Functional Equation for ζ

Theorem 6.1. *The Riemann zeta function can be extended to a meromorphic function on $\mathbb{C}$ and satisfies*

$$\zeta(s) = 2^s \pi^{s-1} \sin(\pi s/2) \Gamma(1-s) \zeta(1-s).$$

Proof. We have

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{\{x\}}{x^{s+1}} dx = \frac{1}{s-1} + \frac{1}{2} + s\int_1^\infty \frac{\frac{1}{2} - \{x\}}{x^{s+1}} dx$$

which is valid in $\sigma > -1$. Note that

$$f(x) := \frac{1}{2} - \{x\} = \sum_{n=1}^\infty \frac{\sin(2\pi n x)}{n\pi}$$

is uniformely convergent for $\{x\} \in [\varepsilon, 1-\varepsilon]$. Also note that

$$\frac{1}{s-1} + \frac{1}{2} = s\int_0^1 \frac{\frac{1}{2} - \{x\}}{x^{s+1}} dx$$

when $-1 < \sigma < 0$.

Hence

$$\zeta(s) = s\int_0^\infty \frac{f(x)}{x^{s+1}} dx.$$

For $-1 < \sigma < 0$ we then have:

$$\begin{aligned}
\zeta(s) &= s\int_0^\infty \frac{\{x\} - \frac{1}{2}}{x^{s+1}} dx \\
&= s\int_0^\infty \frac{\sum_{n=1}^\infty \frac{\sin 2n\pi x}{n\pi}}{x^{s+1}} dx = \frac{s}{\pi}\sum_{n=1}^\infty \frac{1}{n}\int_0^\infty \frac{\sin 2n\pi x}{x^{s+1}} dx \\
&= \frac{s}{\pi}\sum_{n=1}^\infty \frac{(2\pi n)^s}{n}\int_0^\infty \frac{\sin x}{x^{s+1}} dx \\
&= \frac{s}{\pi}(2\pi)^s \zeta(1-s)\int_0^\infty \frac{\sin x}{x^{s+1}} dx \\
&= \frac{s}{\pi}(2\pi)^s \zeta(1-s)(-\Gamma(-s)\sin(\pi s/2)) \qquad (*) \\
&= \frac{s}{\pi}(2\pi)^s (-\Gamma(-s))\sin(\pi s/2)\zeta(1-s) \\
&= 2^s \pi^{s-1}\Gamma(1-s))\sin(\pi s/2)\zeta(1-s)
\end{aligned}$$

That we can interchange integral and sum in the third equality is not completely obvious, to see it split the integral up into $\{x\} \in [\varepsilon, 1-\varepsilon]$ and $\notin [\varepsilon, 1-\varepsilon]$ and do some stuff, see notes for details.

Proof of $(*)$:

$$\int_0^\infty \frac{\sin x}{x^{s+1}}dx = \frac{1}{2i}\left(\int_0^\infty \frac{e^{iy}}{y^{s+1}}dy - \int_0^\infty \frac{e^{-iy}}{y^{s+1}}dy\right)$$

Now consider a contour as follows: $\varepsilon > 0, R > 0$. Then go from ε to R, then on a quarter circle from R to iR. Then to $i\varepsilon$, and then along a small quarter circle back to ε. Integrate $\frac{e^{iz}}{z^{s+1}}$ over this contour. We have

$$\left|\int_{i\varepsilon}^{\varepsilon} \frac{e^{iz}}{z^{s+1}}dz\right| \le C\int_0^{\pi/2} \frac{\varepsilon}{\varepsilon^{s+1}}dt \xrightarrow{\varepsilon\to 0} 0,$$

$$\begin{aligned}\left|\int_R^{iR} \frac{e^{iz}}{z^{s+1}}dz\right| &\le \frac{1}{R^{s+1}}\int_0^{\pi/4} e^{-R\sin\theta}Rd\theta \\ &\le \frac{1}{R^{s+1}}\int_0^{\pi/4} e^{-R\frac{2}{\pi}\theta}Rd\theta \xrightarrow{R\to\infty} 0\end{aligned}$$

Since the integral over the whole contour is 0, we get

$$\int_0^\infty \frac{e^{iy}}{y^{s+1}}dy = -\int_\infty^0 \frac{e^{-y}}{(iy)^{s+1}}idy = i\int_0^\infty \frac{e^{-y}}{(iy)^{s+1}}dy$$

Similarly, one shows by integrating over the mirrored contour in the lower half plane that

$$\int_0^\infty \frac{e^{-iy}}{y^{s+1}}dy = i\int_0^\infty \frac{e^{-y}}{(-iy)^{s+1}}dy$$

Therefore

$$\begin{aligned}\int_0^\infty \frac{\sin x}{x^{s+1}}dx &= \frac{1}{2}\left(\int_0^\infty \frac{e^{-y}}{(iy)^{s+1}}dy - \int_0^\infty \frac{e^{-y}}{(-iy)^{s+1}}dy\right) \\ &= \frac{1}{2}\Gamma(-s)(i^{-s-1} + (-i)^{-s-1}) \\ &= \frac{1}{2}\Gamma(-s)(e^{-si\pi/2}i^{-1} + (-i)^{-1}e^{si\pi/2}) \\ &= -\Gamma(-s)\sin(\pi s/2).\end{aligned}$$

□

Theorem 6.2. $\zeta'(0) = -\frac{1}{2}\log(2\pi)$

Proof. We have

$$\zeta(s) = \frac{1}{s-1} + 1 - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt = \frac{1}{s-1} + \gamma + O(s-1).$$

Therefore $\lim_{s\to 1^+}(\zeta(s)(s-1))' = \gamma$. Now compare this with the other side of the functional equation. □

Remark. If $\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$, then $\xi(s) = \xi(1-s)$.

7 Perron's Formula

Given a sequence a_n, we associate to it the Dirichlet series $D(s) = \sum a_n n^{-s}$. How do we get information about the a_n from properties of D? Let $A^*(x) = \sum_{n \le x} a_n$ if x is not an integer and $A^*(x) = \sum_{n<x} a_n + \frac{1}{2} a_x$ if x is an integer. Let σ_c be the abscissa of convergence of D.

Theorem 7.1 (Perron's formula, ineffective version)**.** *If $a > 0, a > \sigma_c$, then for all $x \ge 0$:*

$$A^*(x) = \frac{1}{2\pi i} \int_{a-i\infty}^{a+i\infty} D(s) \frac{x^s}{s} ds := \frac{1}{2\pi i} \lim_{T \to \infty} \int_{a-iT}^{a+iT} D(s) \frac{x^s}{s} ds.$$

Theorem 7.2 (Perron's formula, effective version)**.** *If $a > 0, a > \sigma_c$, then for all $x \ge 0$:*

$$A^*(x) = \frac{1}{2\pi i} \int_{a-iT}^{a+iT} D(s) \frac{x^s}{s} ds + R(T)$$

where $|R(T)| \le \frac{x^a}{T} \sum_{n=1}^{\infty} \frac{|a_n|}{n^a |\log \frac{x}{n}|}$.

In the case $D(s) = 1$, this says

$$\frac{1}{2\pi i} \lim_{T \to \infty} \int_{a-iT}^{a+iT} \frac{x^s}{s} ds = \begin{cases} 0 & 0 \le x < 1, \\ \frac{1}{2} & x = 1, \\ 1 & x > 1. \end{cases}$$

Note that since $|x^s/s| = x^a/|s|$, the integral does not converge absolutely.

Let $I_T = \int_{a-iT}^{a+iT} \frac{x^s}{s} ds$. Then we have $I_T = \frac{x^s}{s \log x}\Big|_{a-iT}^{a+iT} + \frac{1}{\log x} \int_{a-iT}^{a+iT} \frac{x^s}{s^2} ds$ and this does converge absolutely for $T \to \infty$. We have $\left| \frac{x^{a \pm iT}}{(a \pm iT) \log x} \right| = \frac{x^a}{\sqrt{a^2+T^2} \log x} = O(x^a/(T \log x)) = o(1)$.

We now prove Perron's formula for $D(s) = 1$. Consider the following contour, the Bronwich contour.

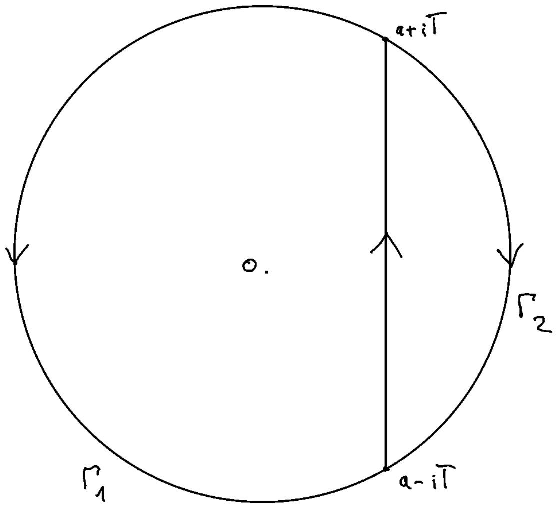
Suppose first that $x > 1$. Then on Γ_1 we have $|x|^s > x^a$. The residue of $\frac{x^s}{s^2}$ at $s = 0$ is $\log x$. Then

$$\frac{1}{2\pi i} \int_{a-iT}^{a+iT} \frac{x^s}{s^2} ds = \log x - \frac{1}{2\pi i} \int_{\Gamma_1} \frac{x^s}{s^2} ds.$$

Let $\rho = \sqrt{a^2 + T^2}$ be the radius of the circle. Then on Γ_1 we have $|x^s/s^2| < |x^a/\rho^2|$, hence the integral on the RHS is $O(1/\rho) = o(1)$ as $T \to \infty$. Then we have

$$\frac{1}{2\pi i} \int_{a-iT}^{a+iT} \frac{x^s}{s} ds = O(x^a/(T \log x)) + 1 + O(1/T) = o(1) + 1.$$

In the case $x < 1$ one similarly finds the claim by integrating over Γ_2 instead of Γ_1.



Bronwich contour

The case $x = 1$ can be done directly.

The same argument shows the following more general version:

Theorem 7.3.

$$\frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty}\frac{x^s dx}{s(s+1)\cdots(s+k)} = \begin{cases} 0 & x \le 1, \\ \frac{1}{k!}\left(1-\frac{1}{x}\right)^k & x \ge 1. \end{cases}$$

Proof of Theorem 7.1 and Theorem 7.2. If $a > \sigma_a$, then we can just swap integral and sum in $\int_{a-i\infty}^{a+i\infty} D(s)\frac{x^s}{s}ds$ and the result follows from the special case $D(s) = 1$. For $\sigma_c < a \le \sigma_a$, we need to do a bit more, see notes for details. □

We now give a version of Perron's formula that gets rid of the difficulty of non-absolute convergence.

Let $A_1(x) = \int_0^x A(t)dt = \sum_{n\le x} a_n(x-n)$. Then we have:

Theorem 7.4. *For any $c > \max(0, \sigma_a)$ and any $x > 1$,*

$$A_1(x) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} D(s)\frac{x^{s+1}}{s(s+1)}ds.$$

Proof. It is easy to see that the RHS is absolutely convergent, hence can swap sum and integral and apply Theorem 7.4:

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} D(s)\frac{x^{s+1}}{s(s+1)}ds = \frac{1}{2\pi i}\sum_{n=1}^{\infty} a_n \int_{c-i\infty}^{c+i\infty}\frac{\left(\frac{x}{n}\right)^s x}{s(s+1)}ds$$

$$
\begin{aligned}
&= \sum_{n \le x} a_n x \left(1 - \frac{n}{x}\right) \\
&= A_1(x).
\end{aligned}
$$

□

8 The Prime Number Theorem

Theorem 8.1. *For* $\operatorname{Re} s \geq 1$*, we have* $\zeta(s) \neq 0$*.*

Proof. For $\operatorname{Re} s > 1$, this is easy. E.g. it follows from the convergence of the Euler product or from $\frac{1}{\zeta(s)} = \sum_{n\geq 1} \frac{\mu(n)}{n^s}$. So suppose $s = 1 + it$ where $0 \neq t \in \mathbb{R}$. We already proved this case in Corollary 3.8. Here is another proof using the 3-4-1 trick. For $\operatorname{Re} s = \sigma > 1$, we have

$$\log \zeta(s) = -\sum_p \log(1 - p^{-s}) = \sum_p \sum_{k\geq 1} \frac{1}{kp^{ks}}.$$

And

$$\log |\zeta(s)| = \operatorname{Re} \log \zeta(s) = \sum_p \sum_{k\geq 1} \frac{\cos(t \log p^k)}{kp^{k\sigma}}.$$

Now for $\theta \in \mathbb{R}$ we have

$$3 + 4\cos\theta + \cos 2\theta = 2(1 + \cos\theta)^2 \geq 0.$$

Hence

$$3 \log |\zeta(\sigma)| + 4 \log |\zeta(\sigma + it)| + \log |\zeta(\sigma + 2it)| \geq 0$$

for any $t \in \mathbb{R}, \sigma > 1$. Therefore

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

Now let $\sigma \to 1^+$. Then $\zeta(1 + it) \neq 0$, otherwise the term $\zeta(\sigma + it)^4$ would dominate over the triple pole of $\zeta(\sigma)^3$, contradicting the inequality above.

Yet another method: We have $0 \leq (1 + p^{it} + p^{-it})^2 = 3 + 2p^{it} + 2p^{-it} + p^{2it} + p^{-2it}$ Now consider

$$\log |\zeta(\sigma)^3 \zeta(\sigma + it)^2 \zeta(\sigma - it)^2 \zeta(\sigma + 2it) \zeta(\sigma - 2it)|.$$

□

Plan. Perron's formula relates $\int_0^x \psi(x)dt$ and $\int_{c-i\infty}^{c+i\infty} \frac{x^{s+1}}{s(s+1)} ds$ for $c > 1$. We want to shift the integral contour to $c = 1$ and then calculate it. For this we need bounds on ζ.

Theorem 8.2. *If* $\log |t| \geq 4$ *and* $\sigma \geq 1 - \frac{2}{\log |t|}$*, we have*

$$\zeta(s) < c \log |t|$$

for some constant c*.*

Proof. For $\sigma > 1$ we can write

$$\zeta(s) - \sum_{n=1}^{N} \frac{1}{n^s} = \sum_{n>N} \frac{1}{n^s} = \int_N^\infty \frac{1}{t} d\lfloor t \rfloor = \frac{t^{1-s}}{1-s}\Big|_N^\infty - \int_N^\infty t^{-s} d\{t\}$$
$$= \frac{-N^{1-s}}{1-s} - \frac{1}{2}N^{-s} + s\int_N^\infty \frac{f(x)}{x^{s+1}}dx$$

where $f(x) = \frac{1}{2} - \{x\}$. Now the RHS is also convergent in $\sigma > 0$, hence by the identity theorem, the equality is also valid in this region. Then

$$|\zeta(s)| \leq \sum_{n=1}^{N} \frac{1}{n^\sigma} + \frac{N^{1-\sigma}}{|t|} + \frac{1}{2}N^{-\sigma} + \frac{1}{2}|s|\frac{1}{\sigma}\frac{1}{N^\sigma}.$$

Now put $N = \lfloor |t| \rfloor + 1$ and $\rho = 1 - \frac{2}{\log |t|}$. Then

$$\sum_{n=1}^{N} \frac{1}{n^\sigma} < \sum_{n=1}^{N} \frac{1}{n^\rho} \leq 1 + \int_1^N t^{-\rho} dt = \frac{N^{1-\rho}}{1-\rho} \ll \log |t|.$$

Also $\frac{N^{1-\sigma}}{|t|} \ll 1$ and $\frac{1}{2}N^{-\sigma} \ll 1$. Finally for the last term:

$$\frac{1}{2}|s|\sigma^{-1}N^{-\sigma} \ll |t|N^{-\sigma} \ll |t||t|^{\frac{2}{\log t}-1} \ll 1.$$

Hence we get the bound

$$|\zeta(s)| \ll \log |t|.$$

□

Theorem 8.3. *We have*

$$\zeta^{(k)}(s) < c(\log |t|)^{k+1}.$$

for all s with $\sigma > 1 - \frac{1}{\log |t|}$ and $\log |t - \frac{1}{4}| \geq 4$.

Proof. Let $r = \frac{1}{\log |t|}$. Then by Cauchy's integral formula,

$$\zeta^{(k)}(s) = \frac{k!}{2\pi i}\int_{|z|=r} \frac{\zeta(s+z)}{z^{k+1}} dz$$

Now $s + z$ is in the range of the previous theorem, so we get $|\zeta(s + z)| \ll \log |t|$. Now plug this into the formula. □

Theorem 8.4. *We have*

$$\left|\frac{\zeta'(s)}{\zeta(s)}\right| \ll (\log |t|)^{10}$$

for $\sigma \geq 1$ and t sufficiently large.

Proof. Wlog $1 \leq \sigma \leq 2$, because $\left|\frac{\zeta'(s)}{\zeta(s)}\right| = |\sum_{n\geq 1} \Lambda(n) n^{-s}| \leq \left|\frac{\zeta'(2)}{\zeta(2)}\right|$ for $\sigma \geq 2$.

Let $\sigma' = \sigma + \frac{1}{(\log|t|)^{10}}$. Recall from the 3-4-1 trick that

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

Since $|\zeta(\sigma' + 2it)| \ll \log|t|$ and $\zeta(\sigma') \ll (\sigma' - 1)^{-1}$, we get

$$|\zeta(\sigma' + it)|^4 \gg \frac{(\sigma' - 1)^3}{\log|t|} \gg \frac{1}{(\log|t|)^{31}}.$$

Then

$$|\zeta(\sigma' + it)| \gg (\log|t|)^{-31/4}.$$

Also $|\zeta(\sigma + it) - \zeta(\sigma' + it)| = \left|\int_\sigma^{\sigma'} \zeta'(u + it) dt\right| \ll (\sigma' - \sigma)(\log|t|)^2 = (\log|t|)^{-8}$. Hence

$$|\zeta(\sigma + it)| \gg (\log|t|)^{-31/4}$$

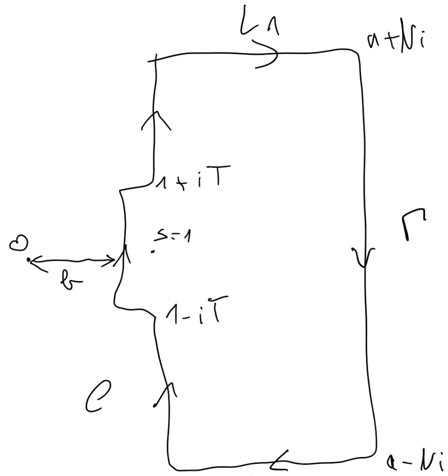
and then

$$\left|\frac{\zeta'}{\zeta}(s)\right| \ll \frac{(\log|t|)^2}{(\log|t|)^{-31/4}} \ll (\log|t|)^{10}.$$

□

Theorem 8.5.

$$\int_0^x \psi(u) du \sim \frac{1}{2} x^2.$$



Proof. Consider the contour as in the figure. Let C be the left part of the contour. Choose T and b so that there are no zeros of ζ in the interior of the contour. Let $\Phi(s) = \frac{\zeta'(s)}{\zeta(s)} \frac{x^{s+1}}{s(s+1)}$. Note that by the residue theorem

$$\frac{1}{2\pi i} \int_{C+L_1+L_2+\Gamma} \Phi(s)ds = \frac{1}{2}x^2.$$

Also

$$\frac{1}{2\pi i} \int_{\Gamma} \Phi(s)ds = o(1) + \int_0^x \psi(u)du \quad \text{as } N \to \infty,$$

by the smoothed Perron's formula, Theorem 7.4. So to prove the claim, we just have to show that the integrals over L_1, L_2, C are $o(x^2)$.

We have

$$\left| \int_{L_i} \Phi(s)ds \right| \le \int_{L_i} |\Phi(s)|\, ds \le \int_{L_i} \frac{c(\log N)^{10} \max(1, x^{a+1})}{N(N-1)} ds$$
$$\le (a-1) \frac{c(\log N)^{10} \max(1, x^{a+1})}{N(N-1)} \xrightarrow{N\to\infty} 0.$$

Now on the line segments from $1+iT$ to $1+iN$ and $1-iN$ to $1-iT$, we have $\left|\frac{\Phi(1+it)}{x^2}\right| < \frac{c(\log|t|)^{10}}{|t|^2}$, so

$$\left| \int_{1+iT}^{1+iN} + \int_{1-iN}^{1-iT} \right| < \frac{\varepsilon}{2} x^2$$

for T sufficiently large. On the indented rectangle, the integral is bounded by

$$Mx^2 \left(\int_{-T}^{T} x^{b-1} dt + 2 \int_b^1 x^{\sigma-1} d\sigma \right)$$

where $M = \sup \left| \frac{\zeta'}{\zeta} \frac{1}{s(s+1)} \right|$. This is

$$< x^2 M \Big(2Tx^{b-1} + \left[\frac{2}{\log x} e^{(\sigma-1)\log x} \right]_b^1 \Big) = Mx^2 \Big(2Tx^{b-1} + \frac{2}{\log x}(1 - x^{b-1}) \Big) = o(x^2).$$

Remark by L.T.: The order in which we choose N, T, x seems somewhat problematic here. For our bound on $\int_{L_i} \Phi(s)ds$ we need x fixed. Then we choose N large enough, then we choose T large enough. But then why is $M2Tx^{b-1}$ small? Also we might want to use an effective version of Perron's formula in the beginning to see how the $o(1)$-term depends on x. ∎

Theorem 8.6 (Prime Number Theorem)**.**

$$\psi(x) \sim x.$$

And hence $\pi(x) \sim \frac{x}{\log x}$ by Theorem 5.7.

Proof. ψ is increasing and so

$$\frac{1}{h}\int_{x-h}^{x} \psi(u)du < \psi(x) < \frac{1}{h}\int_{x}^{x+h} \psi(u)du.$$

Therefore

$$x - \frac{1}{2}h + o(x^2/h) < \psi(x) < x + \frac{1}{2}h + o(x^2/h).$$

Now choose $h = \delta x$, so that

$$x(1 - \frac{1}{2}\delta + o(x/\delta)) < \psi(x) < x(1 + \frac{1}{2}\delta + o(x/\delta)).$$

Then for large enough x,

$$x(1-\delta) < \psi(x) < x(1+\delta).$$

□

9 Hadamard's Factorisation Theorem

An entire function f is *of finite order* if for some $\alpha \geq 0$, we have $|f(z)| = O(e^{|z|^\alpha})$ as $|z| \to \infty$. The inf of such α is called the *order* of f.

Theorem 9.1 (Hadamard's Factorisation Theorem)**.** *Suppose f is entire of order α, $f(0) \neq 0$. Then $f(z) = e^{Q(z)}P(z)$, where Q is a polynomial of degree $\leq \lfloor \alpha \rfloor$, and*

$$P(z) = \prod_{n=1}^{\infty} \Big(1 - \frac{z}{\rho_n}\Big) \exp\Big(\sum_{m=1}^{\lfloor \alpha \rfloor} \frac{1}{m} (\frac{z}{\rho_n})^m\Big)$$

where $\rho_1, \rho_2, \dots$ is an enumeration of the zeros of f. The product converges locally uniformly in $\mathbb{C}$. Moreover, for $R > 1$,

$$\#\{\rho_n \mid |\rho_n| \leq R\} \ll_\varepsilon R^{\alpha+\varepsilon}.$$

Conversely, given a sequence ρ_n satisfying this bound, the expression $e^{Q(z)}P(z)$ defines an entire function of order $\leq \alpha$.

Define the *primary factors* $E(u, 0) = 1 - u$ and $E(u, k) = (1 - u) \exp(u + \frac{u^2}{2} + \dots + \frac{u^k}{k})$ for $k \geq 1$. Then $\log E(u, k) = -\frac{u^{k+1}}{k+1} - \frac{u^{k+2}}{k+2} - \dots$ and for $|u| < 1$, $|\log E(u, k)| < \frac{|u|^{k+1}}{1-|u|}$. So $P(z)$ in the theorem can be written as $\prod_{n=1}^{\infty} E(u/\rho_n, \lfloor \alpha \rfloor)$.

Theorem 9.2. *Given any set $\{\rho_n\}_{n\in\mathbb{N}}$ in $\mathbb{C}$ with no limit points, there is an entire function with roots exactly the ρ_n.*

Proof. Set $r_n = |\rho_n|$. After reordering we may assume $r_1 \leq r_2 \leq \dots$. We can also assume $r_1 \neq 0$. Let $f(z) = \prod_{n=1}^{\infty} E(\frac{z}{\rho_n}, n-1)$. If $|z| < \frac{r_n}{2}$, then $|\log E(z/\rho_n, n-1)| < \frac{(|z|/r_n)^n}{1-(|z|/r_n)} < \frac{1}{2^{n-1}}$, hence for $|z| \leq R$, $\sum_{r_n > 2R} \log E(z/\rho_n, n-1)$ is absolutely and uniformly convergent, so f is analytic ain $|z| \leq R$ and its zeros in this region are precisely those of the remainding product $\prod_{r_n \leq 2R} E(z/\rho_n, n-1)$. □

We see from the proof that we can replace $n-1$ in $E(z/\rho_n, n-1)$ by a_n where a_n is such that $\sum r_n^{-a_n-1}$ converges.

Theorem 9.3 (Weierstraß Factorisation Theorem)**.** *Let f be entire with $f(0) \neq 0$. Then $f(z) = f(0)e^{g(z)}P(z)$ where P is a product of primary factors and g is entire.*

Proof. Form $P(z)$ as in Theorem 9.2 with the set of roots of f as the ρ_n (with multiplicities). Then $\frac{f(z)}{P(z)}$ has no zeros, hence admits a logarithm. Alternatively, let $\phi(z) = \frac{f'(z)}{f(z)} - \frac{P'(z)}{P(z)}$. Then ϕ is entire, hence we can define $g(z) = \int_0^z \phi(t)dt$. □

Proof of Theorem 9.1. Suppose first that f has no zeros. Then by Weierstraß we may write $f = e^g$ where g is entire. Since $|f(z)| \ll e^{|z|^{\alpha+\varepsilon}}$ for all $\varepsilon > 0$, we get $e^{\operatorname{Re} g(z)} \ll e^{|z|^{\alpha+\varepsilon}}$, hence $\operatorname{Re} g(z) \ll |z|^{\alpha+\varepsilon}$. In fact $|g(z)| \ll |z|^{\alpha} + \varepsilon$ by the Borel-Caratheodory lemma. It then follows from Liouville's theorem that g is a polynomial of degree $\leq \lfloor \alpha \rfloor$.

To also cover the case when f has zeros, we need some more results. □

Theorem 9.4 (Borel-Caratheodory)**.** *Suppose f is analytic on $|z| \leq R$ such that $f(0) = 0$ and $\operatorname{Re} f(z) \leq M$. Then for any $r < R$,*

$$\sup_{|z|=r} |f(z)| \leq \frac{2r}{R-r} M.$$

Proof. Let $g(z) = \frac{f(z)}{z(2M-f(z))}$, so g is analytic on $|z| \leq R$ and satisfies $|g(z)| \leq \frac{1}{R}$ on $|z| = R$. By the maximum modulus principle, $|g(z)| \leq \frac{1}{R}$ also for $|z| = r$. So $R|f(z)| \leq 2Mr + r|f(z)|$ and the result follows. □

Suppose f is analytic in $|z| < R + \varepsilon$ and $f(0) \neq 0$. Then

$$|f(0)| \leq \Big(\prod_{|\rho_n|<R} \frac{|\rho_n|}{R} \Big) \sup_{|z|=R} |f(z)|.$$

This follows from Jensen's formula:

Theorem 9.5 (Jensen)**.** *Suppose f is analytic in $|z| < R + \varepsilon$ and $f(z) \neq 0$ in $R \leq |z| \leq R + \varepsilon$ and $f(0) \neq 0$. Then*

$$\frac{1}{2\pi} \int_0^{2\pi} \log |f(Re^{i\theta})| d\theta = \log |f(0)| + \log \frac{R^n}{|\rho_1| \cdots |\rho_n|}$$

where $\rho_1, \ldots, \rho_n$ denote the roots of f inside $|z| < R$ with multiplicity.

Proof. Write $f(z) = C g_1(z) \cdots g_n(z) F(z)$ where F has no zeros in $|z| < R$ and $g_i(z) = \frac{R(z-\rho_i)}{R^2 - \bar{\rho}_i z}$ and C is chosen so that $F(0) = 1$. Note that g_i is analytic in $|z| < R + \varepsilon$. Then $\frac{\log F(z)}{z}$ is analytic in $|z| < R + \varepsilon$, hence $\int_{|z|=R} \frac{\log F(z)}{z} dz = 0$, so $\int_0^{2\pi} \log F(Re^{i\theta}) i d\theta = 0$. Taking imaginary part of both sides gives the result for F in place of f. For $|z| = R$ we have $|g_i(z)| = \left| \frac{R(z-\rho_i)}{R^2 - \bar{\rho}_i z} \right| = 1$. Also $g_i(0) = \frac{\rho_i}{R}$. Then the formula also holds for g_i. It clearly holds for the constant function C. It is easy to see that it then also holds for the product f. □

Theorem 9.6. *Let f be entire, $f(0) \neq 0$. Let $n(r)$ denote the number of zeros of f in $|z| \leq r$. Then*

$$\frac{1}{2\pi} \int_0^{2\pi} \log |f(Re^{i\theta})| d\theta - \log |f(0)| = \log \Big(\frac{R^n}{r_1 \cdots r_n} \Big) = \int_0^R \frac{n(r)}{r} dr$$

where $r_1, \ldots, r_n$ are the zeros in $|z| < R$.

Theorem 9.7. *If f is of order α, then for $\alpha' > \alpha$, $\sum_n r_n^{-\alpha'}$ converges.*

Using this it is possible to complete the proof of Theorem 9.1, see notes for details.

9.1 Application to $\zeta(s)$

Let $\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s) = (s-1)\pi^{-s/2}\Gamma(1+s/2)\zeta(s)$. This is an entire function and $\log|\xi(s)| \ll s\log|s|$, but not $\ll |s|$. So from the Hadamard factorisation theory, $\sum \frac{1}{|\rho|}$ diverges where the sum runs over the roots of ξ (see notes for details).

Theorem 9.8.

$$\frac{\zeta'(s)}{\zeta(s)} = B - \frac{1}{s-1} + \frac{1}{2}\log\pi - \frac{1}{2}\frac{\Gamma'(1+s/2)}{\Gamma(1+s/2)} + \sum_{\rho}\Big(\frac{1}{s-\rho} + \frac{1}{\rho}\Big)$$

where the sum is taken over the zeros ρ of ζ in $0 < \sigma < 1$.

In fact, $B = -\frac{\gamma}{2} - 1 - \frac{1}{2}\log 4\pi$.

Proof. By Hadamard, $\xi(s) = e^{A+Bs}\prod_\rho\big(1-\frac{s}{\rho}\big)e^{s/\rho}$. Now take logarithmic derivatives. □