

Analytic Number Theory

Lecture Notes

Junho Peter Whang

October 19, 2026

Seoul National University

Fall 2026

Preface

These are ongoing lecture notes for the undergraduate topics course in introductory analytic number theory taught at Seoul National University in Fall 2026. The material draws heavily from M. Ram Murty's *Problems in Analytic Number Theory* and Tom M. Apostol's *Introduction to Analytic Number Theory*.

Contents

Preface	2
1 Arithmetic functions	7
2 Summatory functions	8
3 Partial summation	9
4 Euler's formula	10
5 Bernoulli polynomials	11
6 Euler–Maclaurin formula	12
7 Applications of Euler–Maclaurin	14
8 Riemann zeta function	15
9 Basel problem	16
10 Euler's and Stirling's formulas	17
11 Dirichlet convolutions	18
12 Summatory divisor functions	19
13 Hyperbola method	20
14 Dirichlet derivative	21
15 Multiplicative functions	22
16 Dirichlet inverse	23

17 Möbius function	24
18 Möbius inversion	25
19 Summatory totient function	26
20 Formal Dirichlet series	27
21 Examples of formal Dirichlet series	28
22 Absolute convergence	29
23 Euler products	30
24 Convergence of Dirichlet series	31
25 Analyticity of Dirichlet series	32
26 Summatory bounds and Dirichlet series	33
27 Chebyshev functions	34
28 Equivalent formulations of PNT	35
29 Logarithmic average	36
30 Mertens' theorems	37
31 Bertrand's postulate	38
32 Mertens' function	39
33 Mertens' function and PNT, part I	40
34 Mertens' function and PNT, part II	41

35	Finite abelian groups and characters	42
36	Orthogonality of characters	43
37	Dirichlet characters	44
38	Dirichlet L-functions and primes	45
39	Nonvanishing of $L(1, \chi)$, part I	46
40	Nonvanishing of $L(1, \chi)$, part II	47
41	Primes in arithmetic progressions	48
42	Quadratic characters and discriminants	49
43	Quadratic reciprocity	50
44	Excursion to algebraic number theory	51
45	Gaussian integers	52
46	Dirichlet density	53
47	Splitting of polynomials mod p	54
48	$L(s, \chi) \neq 0$ for $\Re(s) = 1$, part I	55
49	$L(s, \chi) \neq 0$ for $\Re(s) = 1$, part II	56
50	PNT from Wiener–Ikehara	57
51	Fourier analysis	58
52	Monotonicity	59

53 Proof of Wiener-Ikehara	60
54 Review of contour integrals	61
55 Cauchy's theorem and residues	62
56 Perron kernel	63
57 Perron's formula	64

1 Arithmetic functions

Definition 1.1.

1. $\mathbb{N} = \{1, 2, 3, \dots\}$, $\mathbb{P} = \{p \in \mathbb{N} : p \text{ prime}\}$
2. For $x \in \mathbb{R}$, write $[x] = \max\{n \in \mathbb{Z} : n \leq x\}$ and $\{x\} = x - [x] \in [0, 1)$.

Definition 1.2. Let $X \subseteq \mathbb{R}$. Let $f, g : X \rightarrow \mathbb{C}$ be functions.

1. Assume $g \geq 0$ is real nonnegative. We write

$$f(x) = O(g(x)) \quad \text{or} \quad f(x) \ll g(x)$$

if there is a constant $K > 0$ such that $|f(x)| \leq Kg(x)$ for all $x \in X$.

2. For $a \in \mathbb{R} \cup \{\pm\infty\}$, we write:

- $f(x) = o(g(x))$ as $x \rightarrow a$ if $\lim_{x \rightarrow a} f(x)/g(x) = 0$.
- $f(x) \sim g(x)$ as $x \rightarrow a$ if $\lim_{x \rightarrow a} f(x)/g(x) = 1$.

Definition 1.3. An *arithmetic function* is a function $f : \mathbb{N} \rightarrow \mathbb{C}$.

Example 1.4.

1. Constant functions, identity function $\text{id}_{\mathbb{N}}(n) = n$.
2. Let $S \subseteq \mathbb{N}$. The characteristic function of S is given by

$$\delta_S(n) = \begin{cases} 1 & n \in S \\ 0 & \text{otherwise.} \end{cases}$$

3. Divisor function $d(n) = \#\{d \in \mathbb{N} : d \mid n\} = \sum_{d \mid n} 1$.
4. $(k \in \mathbb{N})$ $d_k(n) = \#\{(d_1, \dots, d_k) \in \mathbb{N}^k : d_1 \cdots d_k = n\}$. ($d_1 = 1$, $d_2 = d$.)
5. $(s \in \mathbb{C})$ $\sigma_s(n) = \sum_{d \mid n} d^s$. (Note. $\sigma_0 = d$.)
6. $(p \in \mathbb{P})$ $v_p(n) = \max\{k \in \mathbb{Z}_{\geq 0} : p^k \mid n\}$ p -adic valuation.
7. $\omega(n) = \#\{p \in \mathbb{P} : p \mid n\}$
8. $\Omega(n) = \sum_p v_p(n) = \#$ of prime divisors counted with multiplicity.
9. Liouville function: $\lambda(n) = (-1)^{\Omega(n)}$.

2 Summatory functions

An important theme in analytic number theory is to study the behavior of an arithmetic function on average.

Definition 2.1. The *summatory function* of $a = (a_n)_{n \in \mathbb{N}}$ is $S_a : \mathbb{R}_{\geq 0} \rightarrow \mathbb{C}$,

$$S_a(x) = \sum_{n \leq x} a_n.$$

Example 2.2.

1. $\sum_{n \leq x} 1 = [x] = x - \{x\} = x + O(1)$.
2. Suppose $\lim_{n \rightarrow \infty} a_n = \alpha \in \mathbb{C}$. Then $S_a(x) = (\alpha + o(1))x$.
3. Let $a_n = (-1)^n$. Then $S_a(x) = o(x)$.

Example 2.3. Define

$$\pi(x) = \#\{p \leq x : p \text{ prime}\} = S_{\delta_{\mathbb{P}}}(x).$$

Then prime number theorem, conjectured by Legendre and Gauss in early 1800's and proved in 1896 independently by Hadamard and de La Vallée Poussin, states that

$$\pi(x) \sim \frac{x}{\log x} \sim \int_2^x \frac{dt}{\log t} \quad \text{as } x \rightarrow \infty.$$

Definition 2.4. The Möbius function is given by

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & n \text{ squarefree (i.e., } m^2 \mid n \implies m = 1) \\ 0 & \text{otherwise.} \end{cases}$$

PNT is equivalent to $M(x) = \sum_{n \leq x} \mu(n) = o(x)$. The celebrated Riemann hypothesis is equivalent to $M(x) = O_{\epsilon}(x^{1/2+\epsilon})$.

3 Partial summation

Exercise 3.1. Let $a, b : \mathbb{N} \rightarrow \mathbb{C}$ be arithmetic functions. If $N \in \mathbb{N}$, then

$$S_{ab}(N) = S_a(N)b_N - \sum_{n < N} S_a(n)(b_{n+1} - b_n).$$

Proof. Let $T_{a,b}(N)$ be the right hand side. Clearly $S_{ab}(1) = T_{a,b}(1)$. It suffices to show that $S_{ab}(N) - S_{ab}(N-1) = T_{a,b}(N) - T_{a,b}(N-1)$ for $N \geq 2$. LHS is $a_N b_N$, while

$$\begin{aligned} T_{a,b}(N) - T_{a,b}(N-1) &= S_a(N)b_N - S_a(N-1)b_{N-1} \\ &\quad - S_a(N-1)(b_N - b_{N-1}) \\ &= (S_a(N) - S_a(N-1))b_N = a_N b_N. \quad \square \end{aligned}$$

Theorem 3.2. Let $a : \mathbb{N} \rightarrow \mathbb{C}$ be an arithmetic function. If $[y, x] \subseteq \mathbb{R}_{\geq 0}$ and $f \in C^1([y, x])$,

$$\sum_{y < n \leq x} a_n f(n) = [S_a(t)f(t)]_y^x - \int_y^x S_a(t)f'(t) dt.$$

Proof. Both sides are linear in $a_1, \dots, a_{[x]}$. We may thus assume $a_n = \delta_k(n)$ for some $k \leq x$.

1. ($k \leq y$) $0 = f(x) - f(y) - \int_y^x f'(t) dt$
2. ($y < k \leq x$) $f(k) = f(x) - \int_k^x f'(t) dt.$ $\square$

Example 3.3.

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

Proof. Let $a_n \equiv 1$ and $f(x) = \log x$. We have $S_a(x) = [x] = x + O(1)$ so

$$\begin{aligned} \sum_{n \leq x} \log n &= (x + O(1)) \log x - \int_1^x (t + O(1)) \frac{1}{t} dt \\ &= x \log x + O(\log x) - \int_1^x dt + O\left(\int_1^x \frac{1}{t} dt\right) \\ &= x \log x - x + O(\log x). \quad \square \end{aligned}$$

4 Euler's formula

Corollary 4.1 (Euler's formula). *If $[y, x] \subseteq \mathbb{R}_{\geq 0}$ and $f \in C^1([y, x])$,*

$$\sum_{y < n \leq x} f(n) = \int_y^x f(t) dt - [\{t\}f(t)]_y^x + \int_y^x \{t\}f'(t) dt.$$

Proof. Applying partial summation with $a_n \equiv 1$,

$$\begin{aligned} \sum_{y < n \leq x} f(n) &= [[t]f(t)]_y^x - \int_y^x [t]f'(t) dt \\ &= \left([tf(t)]_y^x - \int_y^x tf'(t) dt \right) - [\{t\}f(t)]_y^x + \int_y^x \{t\}f'(t) dt. \end{aligned}$$

The parenthetical expression is $\int_y^x f(t) dt$ by integration by parts. $\square$

Example 4.2. There is a constant $0 < \gamma < 1$ (called Euler's constant) such that

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right).$$

Proof.

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n} &= 1 + [\log t]_1^x - \left[\frac{\{t\}}{t} \right]_1^x - \int_1^x \frac{\{t\}}{t^2} dt \\ &= \log x + 1 - \int_1^\infty \frac{\{t\}}{t^2} dt + \int_x^\infty \frac{\{t\}}{t^2} dt + O\left(\frac{1}{x}\right). \end{aligned}$$

The result follows by setting $\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2} dt$. $\square$

Exercise 4.3. Let $N(R) = \#\{(a, b) \in \mathbb{Z}^2 : a^2 + b^2 \leq R^2\}$. Prove that

$$N(R) = \pi R^2 + O(R).$$

Conjecture 4.4 (Gauss's circle problem). $|N(R) - \pi R^2| = O_\epsilon(R^{\frac{1}{2}+\epsilon})$.

Exercise 4.5. Prove that there is a constant B such that

$$\sum_{2 \leq n \leq x} \frac{1}{n \log n} = \log \log x + B + O\left(\frac{1}{x \log x}\right).$$

5 Bernoulli polynomials

Definition 5.1. The r th Bernoulli polynomial $B_r(x)$ and the r th Bernoulli number $B_r = B_r(0)$ is given by the power series expansions

$$F(x, t) = \frac{t}{e^t - 1} e^{xt} = \sum_{r=0}^{\infty} B_r(x) \frac{t^r}{r!}, \quad \text{and} \quad \frac{t}{e^t - 1} = \sum_{r=0}^{\infty} B_r \frac{t^r}{r!}.$$

Proposition 5.2.

1. The Bernoulli polynomials are characterized by the recursive relations

$$B_0(x) = 1, \quad B'_r(x) = r B_{r-1}(x), \quad \int_0^1 B_r(x) dx = 0 \quad (r \in \mathbb{N})$$

2. For all $r \in \mathbb{N}$,

$$B_r(x+1) - B_r(x) = r x^{r-1} \quad \text{and} \quad B_r(1-x) = (-1)^r B_r(x).$$

In particular, $B_r(0) = B_r(1)$ for all $r \geq 2$, and $B_r = 0$ if $r > 1$ is odd.

Proof. (1)

$$F(x, 0) = 1, \quad \frac{\partial}{\partial x} F(x, t) = t F(x, t),$$

$$\int_0^1 F(x, t) dx = \frac{F(1, t) - F(0, t)}{t} = 1.$$

(2)

$$F(x+1, t) - F(x, t) = t e^{xt} = \frac{\partial e^{xt}}{\partial x} = \sum_{r=0}^{\infty} r x^{r-1} \frac{t^r}{r!}.$$

$$F(x, -t) = \frac{-t}{e^{-t} - 1} e^{-xt} = \frac{t}{e^t - 1} e^{(1-x)t} = F(1-x, t). \quad \square$$

Corollary 5.3. The function $B_r(\{x\})$ is continuous if $r \geq 2$.

Exercise 5.4. Prove that $B_1(x) = x - \frac{1}{2}$, $B_2(x) = x^2 - x + \frac{1}{6}$.

Exercise 5.5 (Faulhaber's formula). For all $r, N \in \mathbb{N}$,

$$\sum_{m=0}^{N-1} m^{r-1} = \frac{B_r(N) - B_r}{r}.$$

6 Euler–Maclaurin formula

Definition 6.1. Let $f, g : [y, x] \rightarrow \mathbb{C}$ be functions. The Riemann–Stieltjes integral of f with respect to g is given by

$$\int_y^x f(t) dg(t) = \lim_{n \rightarrow \infty} \sum_{i=1}^n f(c_i)(g(x_i) - g(x_{i-1})),$$

where the limit is taken over all partitions $y = x_0 < x_1 < \cdots < x_n = x$ and choices of points $c_i \in [x_{i-1}, x_i]$, as $n \rightarrow \infty$ and $\sup_i (x_i - x_{i-1}) \rightarrow 0$.

Exercise 6.2.

1. If f is continuous and g is continuous and piecewise C^1 , then $\int_y^x f(t) dg(t) = \int_y^x f(t)g'(t) dt$.
2. If f is continuous and g is of *bounded variation*, i.e., $\sup \sum_{i=1}^n |g(x_i) - g(x_{i-1})| < \infty$ where the supremum runs over all finite partitions $y = x_0 < x_1 < \cdots < x_n = x$, then

$$\int_y^x f dg = [fg]_y^x - \int_y^x g df.$$

3. If a is an arithmetic function and f is continuous on $[y, x] \subseteq \mathbb{R}_{\geq 0}$, then

$$\sum_{y < n \leq x} a_n f(n) = \int_y^x f(t) dS_a(t).$$

Theorem 6.3 (Euler–Maclaurin formula). *Let $f \in C^{k+1}([a, b])$, $a, b \in \mathbb{Z}$.*

$$\boxed{\begin{aligned} \sum_{a < n \leq b} f(n) &= \int_a^b f(t) dt + \sum_{r=0}^k \frac{(-1)^{r+1} B_{r+1}}{(r+1)!} (f^{(r)}(b) - f^{(r)}(a)) \\ &\quad + \frac{(-1)^k}{(k+1)!} \int_a^b B_{k+1}(\{t\}) f^{(k+1)}(t) dt. \end{aligned}}$$

Proof. Since $B_1(\{t\}) = \{t\} - \frac{1}{2}$, by Euler’s formula and integration by parts,

$$\begin{aligned} \sum_{a < n \leq b} f(n) &= \int_a^b f(t) d[t] = \int_a^b f(t) dt - \int_a^b f(t) dB_1(\{t\}) \\ &= \int_a^b f(t) dt - B_1 \cdot (f(b) - f(a)) + \int_a^b B_1(\{t\}) f'(t) dt. \end{aligned}$$

Iteratively integrate by parts $\int_a^b B_1(\{t\})f'(t) dt = \frac{1}{2} \int_a^b f'(t) dB_2(\{t\})$. $\square$

7 Applications of Euler–Maclaurin

Example 7.1. There exists a constant c such that for $x \in \mathbb{N}$

$$\sum_{n \leq x} \log n = x \log x - x + \frac{1}{2} \log x + c + O\left(\frac{1}{x}\right).$$

Proof. Applying the Euler–Maclaurin formula with $k = 1$, we have

$$\begin{aligned} \sum_{n \leq x} \log n &= \int_1^x \log t \, dt - B_1(\log x - \log 1) \\ &\quad + \frac{B_2}{2} \left(\frac{1}{x} - 1 \right) + \frac{1}{2} \int_1^x \frac{B_2(\{t\})}{t^2} \, dt \\ &= x \log x - x + \frac{1}{2} \log x \\ &\quad + \left(1 - \frac{B_2}{2} + \frac{1}{2} \int_1^\infty \frac{B_2(\{t\})}{t^2} \, dt \right) + O\left(\frac{1}{x}\right). \end{aligned} \quad \square$$

Example 7.2. For $x \in \mathbb{N}$ we have

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + \frac{1}{2x} - \frac{1}{12x^2} + O\left(\frac{1}{x^3}\right).$$

Proof. Apply the Euler–Maclaurin formula with $k = 2$. We have

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n} &= 1 + \int_1^x \frac{dt}{t} - B_1\left(\frac{1}{x} - 1\right) \\ &\quad + \frac{B_2}{2} \left(-\frac{1}{x^2} + 1 \right) + \frac{1}{6} \int_1^x B_3(\{t\}) \frac{-6}{t^4} \, dt \\ &= \log x + \gamma + \frac{1}{2x} - \frac{1}{12x^2} + O\left(\frac{1}{x^3}\right) \end{aligned}$$

where we use the fact that we already know $\sum_{n \leq x} \frac{1}{n} - \log x - \gamma = O(1/x)$. $\square$

8 Riemann zeta function

Remark 8.1. See Lemma 25.2 for analyticity of functions defined by a sequence or series of analytic functions.

Definition 8.2. The Riemann zeta function is the analytic function defined for $\Re(s) > 1$ by

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

Example 8.3. If $s \neq 1$, then

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n^s} &= 1 + \left[\frac{t^{1-s}}{1-s} \right]_1^x - \left[\frac{\{t\}}{t^s} \right]_1^x - s \int_1^x \frac{\{t\}}{t^{s+1}} dt \\ &= \frac{s}{s-1} + \frac{x^{1-s}}{1-s} - \{x\}x^{-s} - s \int_1^x \frac{\{t\}}{t^{s+1}} dt. \end{aligned}$$

If moreover $\Re(s) > 1$, then

$$\sum_{n \leq x} \frac{1}{n^s} = \frac{s}{s-1} - s \int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt - \left(-\frac{x^{1-s}}{1-s} - s \int_x^{\infty} \frac{\{t\}}{t^{s+1}} dt + \{x\}x^{-s} \right).$$

In particular, if $\Re(s) > 1$ then $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges absolutely and

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

The right hand side, hence $\zeta(s)$, is an analytic function of s for $\Re(s) > 0$ and $s \neq 1$, with a simple pole at $s = 1$ with $\lim_{s \rightarrow 1} (s-1)\zeta(s) = 1$.

Corollary 8.4. If $\Re(s) > 1$, then

$$\sum_{n > x} \frac{1}{n^s} = -\frac{x^{1-s}}{1-s} - s \int_x^{\infty} \frac{\{t\}}{t^{s+1}} dt + \{x\}x^{-s} = O_s(x^{1-\Re(s)}).$$

Remark 8.5. We will later see that $\zeta(s)$ extends to a meromorphic continuation to the entire complex plane.

9 Basel problem

Remark 9.1. We have $e^{iz} = \cos z + i \sin z$, so that

$$\cos z = (e^{iz} + e^{-iz})/2, \quad \sin z = (e^{iz} - e^{-iz})/(2i)$$

which gives us, writing $t = 2iz$,

$$\begin{aligned} z \cot z &= z \frac{\cos z}{\sin z} = iz \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = \frac{t e^t + 1}{2 e^t - 1} \\ &= \frac{t}{2} + \frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_{2m} \frac{t^{2m}}{(2m)!} = \sum_{m=0}^{\infty} (-1)^m 2^{2m} B_{2m} \frac{z^{2m}}{(2m)!}. \end{aligned}$$

Therefore,

$$\cot z - \frac{1}{z} = \sum_{m=1}^{\infty} \frac{(-1)^m 2^{2m} B_{2m}}{(2m)!} z^{2m-1}.$$

Theorem 9.2 (Euler).

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} \quad \text{and} \quad \zeta(2k) = (-1)^{k+1} \frac{B_{2k} (2\pi)^{2k}}{2(2k)!} \quad \forall k \in \mathbb{N}.$$

Proof. We start with Euler's product expansion

$$\frac{\sin z}{z} = \prod_{k=1}^{\infty} \left(1 - \frac{z^2}{(k\pi)^2} \right).$$

Taking the logarithmic derivative of both sides, we get

$$\cot z - \frac{1}{z} = - \sum_{k=1}^{\infty} \frac{2z/(k\pi)^2}{1 - z^2/(k\pi)^2} = - \frac{2}{z} \sum_{k=1}^{\infty} \sum_{m=1}^{\infty} \frac{z^{2m}}{(k\pi)^{2m}} = - \frac{2}{z} \sum_{m=1}^{\infty} \frac{\zeta(2m)}{\pi^{2m}} z^{2m}.$$

Compare with the previous expansion of left hand side. □

Remark 9.3. Apéry (1978) proved that $\zeta(3)$ is irrational.

Exercise 9.4. The multiple zeta function is

$$\zeta(s_1, \dots, s_k) = \sum_{n_1 > \dots > n_k > 0} \frac{1}{n_1^{s_1} \dots n_k^{s_k}}.$$

Show that $\zeta(\underbrace{2, \dots, 2}_k) = \pi^{2k}/(2k+1)!$.

10 Euler's and Stirling's formulas

Proposition 10.1 (Euler).

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

Proof sketch. Write $N \in \mathbb{N}$. One can show using trigonometric identities

$$\frac{\sin((2N+1)z)}{(2N+1)\sin z} = \prod_{k=1}^N \left(1 - \frac{\sin^2 z}{\sin^2(k\pi/(2N+1))}\right).$$

Thus

$$\frac{\sin(z)}{(2N+1)\sin(z/(2N+1))} = \prod_{k=1}^N \left(1 - \frac{\sin^2(z/(2N+1))}{\sin^2(k\pi/(2N+1))}\right).$$

As $N \rightarrow \infty$, LHS tends to $(\sin z)/z$ and each factor on RHS tends to $1 - z^2/(k\pi)^2$. Local uniform convergence follows from the tail estimate, valid for $|z| \leq M$ and $N > K$,

$$\left|1 - \prod_{k=K+1}^N \left(1 - \frac{\sin^2(z/(2N+1))}{\sin^2(k\pi/(2N+1))}\right)\right| \ll_M \sum_{k>K} k^{-2}. \quad \square$$

Corollary 10.2 (Wallis product).

$$\frac{\pi}{2} = \prod_{k=1}^{\infty} \frac{2k}{2k-1} \frac{2k}{2k+1}. \quad \square$$

Corollary 10.3 (Stirling's formula). $N! \sim \sqrt{2\pi N} \left(\frac{N}{e}\right)^N$.

Proof. By Example 7.1, $\exists C > 0$ such that $N! \sim C\sqrt{N} (N/e)^N$. So

$$\begin{aligned} p_N &= \prod_{k=1}^N \frac{2k}{2k-1} \frac{2k}{2k+1} = \prod_{k=1}^N \frac{(2k)^4}{(2k-1)(2k) \cdot (2k)(2k+1)} \\ &= \frac{2^{4N}}{2N+1} \frac{(N!)^4}{[(2N)!]^2} \sim \frac{2^{4N}}{2N+1} \frac{C^4 N^2 (N/e)^{4N}}{C^2 (2N)(2N/e)^{4N}} = \frac{C^2 N^2}{(2N+1)(2N)}. \end{aligned}$$

Using $\lim_{N \rightarrow \infty} p_N = \pi/2$, we get $C = \sqrt{2\pi}$ as desired. $\square$

11 Dirichlet convolutions

Definition 11.1. The Dirichlet convolution (or product) $f * g$ of two arithmetic functions f and g is

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d), \quad n \in \mathbb{N}.$$

Proposition 11.2. $*$ is associative and commutative, with identity δ_1 .

Proof.

$$(f * g)(n) = \sum_{ab=n} f(a)g(b) = (g * f)(n)$$

$$((f * g) * h)(n) = \sum_{abc=n} f(a)g(b)h(c) = (f * (g * h))(n)$$

$$(\delta_1 * f)(n) = f(n) = (f * \delta_1)(n). \quad \square$$

Example 11.3. $d(n) = \sum_{d|n} 1 = d = 1 * 1$. More generally,

$$d_k(n) = \#\{(d_1, \dots, d_k) \in \mathbb{N}^k : d_1 \cdots d_k = n\} = 1^{*k}(n).$$

Proposition 11.4. Let f and g be arithmetic functions. Then

$$S_{f*g}(x) = \sum_{n \leq x} f(n)S_g(x/n) = \sum_{n \leq x} g(n)S_f(x/n).$$

Proof.

$$S_{f*g}(x) = \sum_{n \leq x} \sum_{ab=n} f(a)g(b) = \sum_{ab \leq x} f(a)g(b) = \sum_{a \leq x} f(a) \sum_{b \leq x/a} g(b). \quad \square$$

Corollary 11.5. If f is an arithmetic function,

$$S_{f*1}(x) = \sum_{n \leq x} \sum_{d|n} f(d) = \sum_{n \leq x} f(n) \left[\frac{x}{n} \right] = \sum_{n \leq x} S_f\left(\frac{x}{n}\right). \quad \square$$

12 Summatory divisor functions

Recall. The divisor function is $\sigma_s(n) = \sum_{d|n} d^s$.

Example 12.1.

$$\sum_{n \leq x} d(n) = \sum_{n \leq x} \sigma_0(n) = x \log x + O(x).$$

Proof.

$$\sum_{n \leq x} d(n) = S_{1*1}(x) = \sum_{n \leq x} \left[\frac{x}{n} \right] = \sum_{n \leq x} \frac{x}{n} + O(x) = x \log x + O(x). \quad \square$$

Example 12.2.

$$\sum_{n \leq x} \sigma_1(n) = \frac{\zeta(2)}{2} x^2 + O(x \log x) \quad \text{and} \quad \sum_{n \leq x} \sigma_{-1}(n) = \zeta(2)x + O(\log x).$$

Proof.

$$\begin{aligned} \sum_{n \leq x} \sigma_1(n) &= \sum_{n \leq x} S_{\text{id}}\left(\frac{x}{n}\right) = \sum_{n \leq x} \sum_{m \leq x/n} m = \sum_{n \leq x} \left(\frac{1}{2} \left(\frac{x}{n}\right)^2 + O\left(\frac{x}{n}\right) \right) \\ &= \frac{1}{2} x^2 \sum_{n \leq x} \frac{1}{n^2} + O(x \log x) = \frac{1}{2} (\zeta(2) + O(x^{-1})) x^2 + O(x \log x). \end{aligned}$$

$$\begin{aligned} \sum_{n \leq x} \sigma_{-1}(n) &= \sum_{n \leq x} \frac{1}{n} \left[\frac{x}{n} \right] = x \sum_{n \leq x} \frac{1}{n^2} + O\left(\sum_{n \leq x} \frac{1}{n}\right) \\ &= x(\zeta(2) + O(x^{-1})) + O(\log x). \quad \square \end{aligned}$$

Exercise 12.3.

$$\sum_{n \leq x} \sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1} x^{\alpha+1} + O(x^{\max(1, \alpha)}) \quad \text{if } 1 \neq \alpha > 0.$$

$$\sum_{n \leq x} \sigma_\alpha(n) = \zeta(1-\alpha)x + O(x^{\max(0, \alpha+1)}) \quad \text{if } -1 \neq \alpha < 0.$$

13 Hyperbola method

Proposition 13.1 (Dirichlet's hyperbola method). *Let f and g be arithmetic functions. If $x = yz$ with $y, z > 0$, then*

$$S_{f*g}(x) = \sum_{a \leq y} f(a)S_g(x/a) + \sum_{b \leq z} S_f(x/b)g(b) - S_f(y)S_g(z).$$

Proof. Define

$$\begin{aligned} R &= \{(a, b) \in \mathbb{N}^2 : ab \leq x\}, \\ R_1 &= \{(a, b) \in \mathbb{N}^2 : ab \leq x, a \leq y\}, \\ R_2 &= \{(a, b) \in \mathbb{N}^2 : ab \leq x, b \leq z\}. \end{aligned}$$

Then $R = R_1 \cup R_2$ and $R_1 \cap R_2 = \mathbb{N}^2 \cap ([1, y] \times [1, z])$. We have

$$S_{f*g}(x) = \sum_{(a,b) \in R} f(a)g(b) = \sum_{R_1} + \sum_{R_2} - \sum_{R_1 \cap R_2}$$

and computing each sum gives the result. □

Theorem 13.2 (Dirichlet).

$$\sum_{n \leq x} d(n) = x \log x + (2\gamma - 1)x + O(\sqrt{x}).$$

Proof. Apply the hyperbola method with $y = z = \sqrt{x}$. Then

$$\begin{aligned} \sum_{n \leq x} d(n) &= S_{1*1}(x) = \sum_{a \leq \sqrt{x}} \left[\frac{x}{a} \right] + \sum_{b \leq \sqrt{x}} \left[\frac{x}{b} \right] - [\sqrt{x}]^2 \\ &= 2 \left(\sum_{n \leq \sqrt{x}} \frac{x}{n} + O(\sqrt{x}) \right) - x + O(\sqrt{x}) \\ &= 2x \left(\log \sqrt{x} + \gamma + O\left(\frac{1}{\sqrt{x}}\right) \right) - x + O(\sqrt{x}) \\ &= x \log x + (2\gamma - 1)x + O(\sqrt{x}). \end{aligned} \quad \square$$

Problem 13.3 (Dirichlet's divisor problem). Find infimum $\theta > 0$ such that

$$\sum_{n \leq x} d(n) = x \log x + (2\gamma - 1)x + O(x^\theta).$$

14 Dirichlet derivative

Definition 14.1. The *Dirichlet derivative* f' of $f : \mathbb{N} \rightarrow \mathbb{C}$ is given by

$$f'(n) = -f(n) \log n.$$

Exercise 14.2. We have $(f * g)' = f' * g + f * g'$.

Definition 14.3. The von Mangoldt function is given by

$$\Lambda(n) = \begin{cases} \log p & n = p^k \text{ for some prime } p \text{ and } k \in \mathbb{N} \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 14.4.

1. We have $1 * \Lambda = -1'$. In other words,

$$\sum_{d|n} \Lambda(d) = \log n.$$

2. We have

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \log([x]!) = \sum_{n \leq x} \log n.$$

3. (Legendre's identity) $[x]! = \prod_{p \leq x} p^{\alpha(p,x)}$ where $\alpha(p,x) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right]$.

Proof. First,

$$\sum_{d|n} \Lambda(d) = \sum_p \sum_{k=1}^{v_p(n)} \log p = \sum_{p|n} v_p(n) \log p = \log \left(\prod_p p^{v_p(n)} \right) = \log n.$$

Next,

$$\log([x]!) = \sum_{n \leq x} \log n = S_{1*\Lambda}(x) = \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right].$$

Legendre's identity follows from the fact that

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \sum_p \sum_{m=1}^{\infty} \log p \left[\frac{x}{p^m} \right].$$

□

15 Multiplicative functions

Definition 15.1. Let $f : \mathbb{N} \rightarrow \mathbb{C}$ be an arithmetic function.

1. f is *multiplicative* if $f(1) = 1$ and

$$f(ab) = f(a)f(b) \quad (*)$$

for all $a, b \in \mathbb{N}$ with $(a, b) = 1$.

2. f is *completely multiplicative* if moreover $(*)$ holds for all $a, b \in \mathbb{N}$.

Remark 15.2.

1. f is multiplicative iff $f(1) = 1$ and $f(n) = \prod_p f(p^{v_p(n)})$ for all $n \in \mathbb{N}$.
2. If f and g are multiplicative, $f = g$ iff $f(p^k) = g(p^k)$ for all $p \in \mathbb{P}$, $k \in \mathbb{N}$.

Proposition 15.3. *If f and g are multiplicative, then $f * g$ is multiplicative.*

Proof. Clearly $(f * g)(1) = f(1)g(1) = 1$. Write $D(n) = \{d \in \mathbb{N} : d \mid n\}$. Using the natural bijection $D(n) \simeq \prod_p D(p^{v_p(n)})$,

$$\begin{aligned} (f * g)(n) &= \sum_{d \mid n} f(d)g(n/d) = \sum_{d \mid n} \prod_p f(p^{v_p(d)})g(p^{v_p(n)-v_p(d)}) \\ &= \prod_p \left(\sum_{d \mid p^{v_p(n)}} f(p^{v_p(d)})g(p^{v_p(n)-v_p(d)}) \right) = \prod_p (f * g)(p^{v_p(n)}). \quad \square \end{aligned}$$

Corollary 15.4. *If $f : \mathbb{N} \rightarrow \mathbb{C}$ is multiplicative, so is $(1 * f)(n) = \sum_{d \mid n} f(d)$.*

Example 15.5. The divisor function $\sigma_s(n) = \sum_{d \mid n} d^s$ is multiplicative.

Example 15.6. The Liouville function $\lambda(n) = (-1)^{\Omega(n)}$ is multiplicative.

$$(1 * \lambda)(n) = \sum_{d \mid n} \lambda(d) = \delta_{\square}(n).$$

Proof. Suffice to check $(1 * \lambda)(p^k) = \sum_{0 \leq \ell \leq k} \lambda(p^\ell) = \delta_{2\mathbb{Z}}(k) = \delta_{\square}(p^k)$. $\square$

16 Dirichlet inverse

Proposition 16.1. *Let $f : \mathbb{N} \rightarrow \mathbb{C}$ be an arithmetic function. TFAE:*

1. $f(1) \in \mathbb{C}^*$.
2. *There exists $g : \mathbb{N} \rightarrow \mathbb{C}$, called Dirichlet inverse of f , such that $f * g = \delta_1$.*

Remark 16.2. If such g exists then it is unique and denoted f^{-1} .

Proof. Clearly (2) implies (1) since $f(1)g(1) = 1$. Conversely, let $g(1) = f(1)^{-1}$ and define $g(n)$ for $1 \neq n \in \mathbb{N}$ by the recursive (on $d(n)$ say) formula

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d \neq n} g(d)f(n/d).$$

Then we have $(f * g)(n) = \delta_1(n)$ for all $n \in \mathbb{N}$. □

Proposition 16.3. *If $f : \mathbb{N} \rightarrow \mathbb{C}$ is multiplicative, then f^{-1} is multiplicative.*

Proof. Let $g : \mathbb{N} \rightarrow \mathbb{C}$ be the unique multiplicative function such that for all $p \in \mathbb{P}$ and $k \in \mathbb{N}$ the recursive formula

$$g(p^k) = - \sum_{0 \leq \ell < k} f(p^{k-\ell})g(p^\ell)$$

holds. Then $(f * g)(p^k) = 0$ for all $p \in \mathbb{P}$ and $k \in \mathbb{N}$. Since $f * g$ is multiplicative, we deduce $f * g = \delta_1$. Hence $f^{-1} = g$ is multiplicative. □

Example 16.4. Let $\lambda(n) = (-1)^{\Omega(n)}$. Then $\lambda^{-1} = \delta_{\text{squarefree}}$.

Proof. For $p \in \mathbb{P}$ and $k \in \mathbb{N}$, recursive formula gives

$$\lambda^{-1}(p) = -\lambda(p) = 1, \quad \lambda^{-1}(p^2) = -\lambda(p^2)\lambda^{-1}(1) - \lambda(p)\lambda^{-1}(p) = 0,$$

and inductively $\lambda^{-1}(p^k) = -\lambda(p^k) - \lambda(p^{k-1})\lambda^{-1}(p) = 0$ for all $k \geq 3$. □

17 Möbius function

Recall. The Möbius function is

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & n \text{ is squarefree,} \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 17.1. *We have $\mu * 1 = \delta_1$. Explicitly, for any $n \in \mathbb{N}$*

$$\boxed{\sum_{d|n} \mu(d) = \delta_1(n).}$$

Proof. Since LHS is multiplicative, it suffices to show LHS is zero for $n = p^k$ with $p \in \mathbb{P}$, $k \in \mathbb{N}$. But

$$\sum_{d|p^k} \mu(d) = \sum_{0 \leq \ell \leq k} \mu(p^\ell) = \mu(1) + \mu(p) = 1 - 1 = 0. \quad \square$$

Corollary 17.2. *If $x \geq 1$, then*

$$\boxed{\sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] = S_{1*\mu}(x) = 1.}$$

Corollary 17.3. *For all $x \geq 1$ we have*

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1.$$

Proof. The statement is clear if $x < 2$, so assume $x \geq 2$. Then

$$x \left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| = \left| \sum_{n \leq x} \mu(n) \left[\frac{x}{n} \right] + \sum_{n \leq x} \mu(n) \left\{ \frac{x}{n} \right\} \right| < 1 + \{x\} + ([x] - 1) = x. \quad \square$$

Lemma 17.4. *If $\Re(s) > 1$, then*

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

Proof. Note that the LHS converges absolutely for $\Re(s) > 1$, and by Fubini

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{m=1}^{\infty} \frac{1}{m^s} \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \sum_{N=1}^{\infty} \frac{\sum_{mn=N} \mu(n)}{N^s} = 1. \quad \square$$

18 Möbius inversion

Theorem 18.1 (Möbius inversion). *Let $f, g : \mathbb{N} \rightarrow \mathbb{C}$ be arithmetic.*

$$g(n) = \sum_{d|n} f(d) \quad \forall n \in \mathbb{N} \quad \Longleftrightarrow \quad f(n) = \sum_{d|n} g(d) \mu(n/d) \quad \forall n \in \mathbb{N}.$$

Proof. $g = 1 * f \Longleftrightarrow f = \mu * g.$ □

Lemma 18.2. *If f is multiplicative, then*

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p)).$$

Proof. Since both sides are multiplicative, suffice to check formula for $n = p^k$ with $p \in \mathbb{P}$, $k \in \mathbb{N}$. But

$$\sum_{d|p^k} \mu(d) f(d) = \mu(1) f(1) + \mu(p) f(p) = 1 - f(p). \quad \square$$

Definition 18.3. Euler's totient function $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ is defined to be

$$\varphi(n) = \#\{1 \leq a \leq n : (a, n) = 1\} = \#(\mathbb{Z}/n\mathbb{Z})^*.$$

Proposition 18.4. *We have $1 * \varphi = \text{id}$, i.e., for each $n \in \mathbb{N}$,*

$$\sum_{d|n} \varphi(d) = n$$

Proof. Write $A_d(n) = \{1 \leq a \leq n : (a, n) = d\}$, so that $\varphi(n) = \#A_1(n)$. Then $\{1, \dots, n\} = \coprod_{d|n} A_d(n)$ and $A_d(n) \simeq A_1(n/d)$ under $a \mapsto a/d$. □

Corollary 18.5. *We have*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Proof. By Möbius inversion $\varphi = \mu * \text{id}$ and

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \quad \square$$

19 Summatory totient function

Theorem 19.1.

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

Proof. From $\varphi = \mu * \text{id}$ we get

$$\begin{aligned} \sum_{n \leq x} \varphi(n) &= S_{\mu * \text{id}}(x) = \sum_{n \leq x} \mu(n) S_{\text{id}}\left(\frac{x}{n}\right) = \sum_{n \leq x} \mu(n) \left(\frac{1}{2} \left(\frac{x}{n}\right)^2 + O\left(\frac{x}{n}\right) \right) \\ &= \sum_{n \leq x} \frac{\mu(n)}{2} \frac{x^2}{n^2} + O\left(\sum_{n \leq x} \frac{x}{n}\right) = \frac{x^2}{2} \left(\frac{1}{\zeta(2)} + O(x^{-1}) \right) + O(x \log x) \\ &= \frac{1}{2\zeta(2)} x^2 + O(x \log x) = \frac{3}{\pi^2} x^2 + O(x \log x). \quad \square \end{aligned}$$

Exercise 19.2. The probability that two randomly chosen integers are coprime is

$$\lim_{x \rightarrow \infty} \frac{\#\{(a, b) \in \mathbb{Z}^2 : |a|, |b| \leq x, (a, b) = 1\}}{\#\{(a, b) \in \mathbb{Z}^2 : |a|, |b| \leq x\}} = \frac{6}{\pi^2}.$$

Example 19.3. Probability that a randomly chosen $n \in \mathbb{N}$ is squarefree is

$$\lim_{x \rightarrow \infty} \frac{\#\{n \leq x : n \text{ squarefree}\}}{\#\{n \leq x\}} = \frac{6}{\pi^2}.$$

Proof. Each $n \in \mathbb{N}$ can be written uniquely as $a^2 b$ where $a \in \mathbb{N}$ and b is squarefree. Thus, we have $\delta_{\text{sqfree}} * \delta_{\square} = 1$. Note that $\delta_{\square}^{-1}(n) = \mu(\sqrt{n})$. So

$$\delta_{\text{sqfree}}(n) = \sum_{d^2 | n} \mu(d).$$

Thus,

$$\begin{aligned} S_{\text{sqfree}}(x) &= \sum_{n \leq x} \sum_{d^2 | n} \mu(d) = \sum_{d \leq \sqrt{x}} \sum_{n \leq x/d^2} \mu(d) \\ &= \sum_{d \leq \sqrt{x}} \mu(d) \left[\frac{x}{d^2} \right] = \frac{x}{\zeta(2)} + O(\sqrt{x}). \end{aligned}$$

dividing by x and letting $x \rightarrow \infty$, we get the result. $\square$

20 Formal Dirichlet series

Definition 20.1. The formal Dirichlet series associated to arithmetic function $a = (a_n)_{n \in \mathbb{N}}$ is given by

$$\mathbb{D}(a, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Remark 20.2. Formal Dirichlet series form a commutative ring under

$$\begin{aligned} \mathbb{D}(a, s) + \mathbb{D}(b, s) &= \sum_{n=1}^{\infty} \frac{a_n + b_n}{n^s} = \mathbb{D}(a + b, s), \\ \mathbb{D}(a, s)\mathbb{D}(b, s) &= \sum_{m, n \geq 1} \frac{a_m b_n}{(mn)^s} = \sum_{N=1}^{\infty} \frac{(a * b)_N}{N^s} = \mathbb{D}(a * b, s). \end{aligned}$$

with identity $1 = \mathbb{D}(\delta_1, s)$. If $a = (a_n)$ satisfies $a_1 \in \mathbb{C}^*$, then $\mathbb{D}(a, s)$ is invertible and $\mathbb{D}(a, s)^{-1} = \mathbb{D}(a^{-1}, s)$. The formal derivative

$$\mathbb{D}'(a, s) = \sum_{n=1}^{\infty} (-a_n \log n) / n^s = \mathbb{D}(a', s)$$

satisfies $(\mathbb{D}(a, s)\mathbb{D}(b, s))' = \mathbb{D}'(a, s)\mathbb{D}(b, s) + \mathbb{D}(a, s)\mathbb{D}'(b, s)$.

Example 20.3. If f is an arithmetic function and $g(n) = \sum_{d|n} f(d)$,

$$\mathbb{D}(g, s) = \mathbb{D}(f, s)\zeta(s).$$

Here, we write $\zeta(s) = \mathbb{D}(1, s)$.

Definition 20.4. Given a multiplicative function $a = (a_n)_{n \in \mathbb{N}}$, the formal Euler product expansion of its formal Dirichlet series is

$$\mathbb{D}(a, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \in \mathbb{P}} \left(1 + \frac{a_p}{p^s} + \frac{a_{p^2}}{p^{2s}} + \cdots \right).$$

If a is completely multiplicative, then we write

$$\mathbb{D}(a, s) = \prod_{p \in \mathbb{P}} \left(1 + \frac{a_p}{p^s} + \frac{a_p^2}{p^{2s}} + \cdots \right) = \prod_{p \in \mathbb{P}} \left(1 - \frac{a_p}{p^s} \right)^{-1}.$$

Remark 20.5. We may view $\mathbb{D}(a, s)$ as a function of a complex variable s where the series converges. We will write $D(a, s)$ to denote the function.

21 Examples of formal Dirichlet series

Example 21.1. Formally, we have the following.

1. $\mathbb{D}(1, s) = \zeta(s)$.
2. $\mathbb{D}(\text{id}^\alpha, s) = \sum_{n=1}^{\infty} \frac{n^\alpha}{n^s} = \zeta(s - \alpha)$.
3. $\mathbb{D}(d_k, s) = \mathbb{D}(1^{*k}, s) = \zeta(s)^k$.
4. $\mathbb{D}(\sigma_\alpha, s) = \mathbb{D}(1 * \text{id}^\alpha, s) = \zeta(s)\zeta(s - \alpha)$.
5. $\mathbb{D}(\Lambda, s) = \mathbb{D}(-1' * 1^{-1}, s) = -\zeta'(s)/\zeta(s)$.
6. $\mathbb{D}(\mu, s) = \mathbb{D}(1^{-1}, s) = \zeta(s)^{-1}$.
7. $\mathbb{D}(\varphi, s) = \mathbb{D}(\text{id} * \mu, s) = \zeta(s - 1)/\zeta(s)$.

Exercise 21.2. Let $\lambda(n) = (-1)^{\Omega(n)}$ be the Liouville function. Then

$$\mathbb{D}(\lambda, s) = \frac{\zeta(2s)}{\zeta(s)}.$$

Exercise 21.3. Let $k \in \mathbb{N}$. Define $q_k(n) = 1$ if n is k th power free and 0 otherwise. Then formally

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

Exercise 21.4. For any $a, b \in \mathbb{C}$, formally

$$\boxed{\sum_{n=1}^{\infty} \frac{\sigma_a(n)\sigma_b(n)}{n^s} = \frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)}}, \quad \boxed{\sum_{n=1}^{\infty} \frac{d(n)^2}{n^s} = \frac{\zeta(s)^4}{\zeta(2s)}}.$$

Proof. Let $n = p^k$ where $p \in \mathbb{P}$ and $k \in \mathbb{N}$. Then

$$\sum_{k=0}^{\infty} \frac{\sigma_a(p^k)\sigma_b(p^k)}{p^{ks}} = \sum_{k=0}^{\infty} \frac{1}{p^{ks}} \left(\sum_{\ell=0}^k p^{a\ell} \right) \left(\sum_{\ell=0}^k p^{b\ell} \right) = \sum_{k=0}^{\infty} \frac{p^{a(k+1)} - 1}{p^a - 1} \frac{p^{b(k+1)} - 1}{p^b - 1} \frac{1}{p^{ks}}.$$

Use Ramanujan's identity

$$\sum_{n=0}^{\infty} \left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \right) \left(\frac{\gamma^{n+1} - \delta^{n+1}}{\gamma - \delta} \right) T^n = \frac{1 - \alpha\beta\gamma\delta T^2}{(1 - \alpha\gamma T)(1 - \alpha\delta T)(1 - \beta\gamma T)(1 - \beta\delta T)}$$

and the Euler product expansion to conclude the desired result. $\square$

22 Absolute convergence

It is customary to write $\sigma = \Re s$, $t = \Im s$, and $s = \sigma + it$.

Definition 22.1. Let $f : \mathbb{N} \rightarrow \mathbb{C}$ be an arithmetic function. Then there exists $\sigma_a = \sigma_a(f) \in [-\infty, \infty]$ called abscissa of absolute convergence such that $\mathbb{D}(f, s)$ converges absolutely for all $\Re s > \sigma_a$ and does not converge absolutely for all $\Re s < \sigma_a$.

Proof. Define $\sigma_a = \sup\{\sigma : \sum_{n=1}^{\infty} |f(n)|/n^{\sigma} \text{ diverges}\}$. □

Theorem 22.2 (Uniqueness). *Let $f, g : \mathbb{N} \rightarrow \mathbb{C}$ with $\sigma_a(f), \sigma_a(g) < \infty$. Assume there is a sequence $\{s_k\}$ in $\mathbb{C}$ such that $\lim_{k \rightarrow \infty} \sigma_k = +\infty$ and $D(f, s_k) = D(g, s_k)$ for all $k \in \mathbb{N}$. Then $f = g$.*

Proof. We may assume $g = 0$. Assume there exists a least $N \in \mathbb{N}$ such that $f(N) \neq 0$. We may assume $\sigma_k > c > \sigma_a$. Since $D(f, s_k) = 0$,

$$\begin{aligned} |f(N)| &= \left| N^{s_k} D(f, s_k) - N^{s_k} \sum_{n=N+1}^{\infty} \frac{f(n)}{n^{s_k}} \right| = N^{\sigma_k} \left| \sum_{n=N+1}^{\infty} \frac{f(n)}{n^{s_k}} \right| \\ &\leq N^{\sigma_k} \sum_{n=N+1}^{\infty} \frac{|f(n)|}{n^c} n^{c-\sigma_k} \leq \left(\frac{N}{N+1} \right)^{\sigma_k} (N+1)^c D(|f|, c). \end{aligned}$$

Letting $k \rightarrow \infty$, we deduce $f(N) = 0$, a contradiction. □

Corollary 22.3. *Let $f : \mathbb{N} \rightarrow \mathbb{C}$ such that $\sigma_a(f) < \infty$. Then either $f = 0$ or there exists $c \geq \sigma_a(f)$ such that $D(f, s) \neq 0$ for all $\Re s > c$.*

Exercise 22.4. If $\sigma_a(f) < \infty$, then $\lim_{\sigma \rightarrow \infty} D(f, \sigma + it) = f(1)$ uniformly for $t \in \mathbb{R}$.

Proposition 22.5. *Let $f, g : \mathbb{N} \rightarrow \mathbb{C}$. Assume that $\sigma_a(f), \sigma_a(g) < \infty$. Then $\sigma_a(f * g) \leq \max\{\sigma_a(f), \sigma_a(g)\}$ and*

$$D(f, s)D(g, s) = D(f * g, s)$$

holds for all $\Re s > \max\{\sigma_a(f), \sigma_a(g)\}$.

Proof. By absolute convergence, we can apply Fubini's theorem. □

Example 22.6. $\mathbb{D}(\varphi, s)$ converges absolutely for $\sigma > 2$ where we have $D(\varphi, s) = \zeta(s-1)/\zeta(s)$.

23 Euler products

Theorem 23.1. *Let f be a multiplicative function. Then the Euler product*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots \right)$$

converges absolutely for $\sigma > \sigma_a(f)$. If f is completely multiplicative, then

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{f(p)}{p^s} \right)^{-1}.$$

Proof. Let $\Re s > \sigma_a(f)$. Let us write $P_s(x) = \prod_{p \leq x} (\sum_{k=0}^{\infty} f(p^k)/p^{ks})$. Then

$$\left| \sum_{n \leq x} \frac{f(n)}{n^s} - P_s(x) \right| \leq \sum_{n > x} \frac{|f(n)|}{n^{\sigma}}.$$

Since $D(f, s)$ is absolutely convergent, the right hand side tends to zero as $x \rightarrow \infty$. So $\lim_{x \rightarrow \infty} P_s(x) = D(f, s)$ pointwise. Absolute convergence comes from the fact that a product of the form $\prod_k (1 + a_k)$ is absolutely convergent if $\sum a_k$ is absolutely convergent, and we have

$$\sum_p \left| \sum_{k=1}^{\infty} \frac{f(p^k)}{p^{ks}} \right| \leq \sum_p \sum_{k=1}^{\infty} \frac{|f(p^k)|}{p^{k\sigma}} \leq \sum_{n=1}^{\infty} \frac{|f(n)|}{n^{\sigma}}. \quad \square$$

Example 23.2. We have the Euler product expansion

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s} \right)^{-1}$$

valid for $\sigma > 1$. Since $\zeta(s)$ has a simple pole at $s = 1$, the product on the right hand side must be infinite so there are infinitely many primes!

Example 23.3.

$$\sum_{n=1}^{\infty} \frac{\sigma_{\alpha}(n)}{n^s} = \zeta(s)\zeta(s - \alpha) = \prod_p \frac{1}{(1 - p^{-s})(1 - p^{-(s-\alpha)})}$$

for $\sigma > \max\{1, 1 + \Re(\alpha)\}$.

24 Convergence of Dirichlet series

Theorem 24.1. *Let $f : \mathbb{N} \rightarrow \mathbb{C}$ be an arithmetic function. If $\mathbb{D}(f, s)$ converges for some $s_0 \in \mathbb{C}$ then it also converges for all $\Re(s) > \Re(s_0)$. If it diverges for some $s_0 \in \mathbb{C}$ then it also diverges for all $\Re(s) < \Re(s_0)$.*

Proof. The second statement follows from the first. To prove the first, fix $\Re(s) > \Re(s_0)$. By assumption $\mathbb{D}(f, s_0)$ has bounded partial sums in that there exists $M > 0$ with $|\sum_{n \leq x} f(n)/n^{s_0}| \leq M$ for all $x \geq 1$. Write $g(n) = f(n)n^{-s_0}$. Then by partial summation

$$\begin{aligned} \left| \sum_{a < n \leq b} \frac{f(n)}{n^s} \right| &= \left| \sum_{a < n \leq b} \frac{g(n)}{n^{s-s_0}} \right| = \left| \left[\frac{S_g(t)}{t^{s-s_0}} \right]_a^b + (s-s_0) \int_a^b \frac{S_g(t)}{t^{s-s_0+1}} dt \right| \\ &\leq 2Ma^{\sigma_0-\sigma} + |s-s_0|M \left| \frac{b^{\sigma_0-\sigma} - a^{\sigma_0-\sigma}}{\sigma_0-\sigma} \right| \\ &\leq 2M \left(1 + \frac{|s-s_0|}{\sigma-\sigma_0} \right) a^{\sigma_0-\sigma} = Ka^{\sigma_0-\sigma} \end{aligned}$$

where K is independent of a . By Cauchy's criterion, $\mathbb{D}(f, s)$ converges. $\square$

Example 24.2. Above proof shows that if $\sum_{n \leq x} f(n)$ is bounded then $\mathbb{D}(f, s)$ converges for $\Re s > 0$. For example, the Dirichlet series

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

converges for $\Re s > 0$. It converges absolutely for $\Re s > 1$.

Definition 24.3. Let $f : \mathbb{N} \rightarrow \mathbb{C}$ be an arithmetic function. Then there exists $\sigma_c = \sigma_c(f) \in [-\infty, \infty]$ called abscissa of convergence such that $\mathbb{D}(f, s)$ converges for all $\Re s > \sigma_c$ and diverges for all $\Re s < \sigma_c$.

Proof. Take $\sigma_c = \sup\{\Re(s) : \mathbb{D}(f, s) \text{ diverges}\}$. $\square$

Proposition 24.4. *If $\sigma_c < \infty$, then $\sigma_c \leq \sigma_a \leq \sigma_c + 1$.*

Proof. Let $\Re s_0 > \sigma_c$. Since $\mathbb{D}(f, s_0)$ converges, there exists $A > 0$ such that $|f(n)/n^{s_0}| \leq A$ for all $n \in \mathbb{N}$. If $\Re(s) > \Re(s_0) + 1$ then $\mathbb{D}(f, s)$ is absolutely convergent since $|f(n)n^{-s}| \leq An^{\sigma_0-\sigma}$. $\square$

25 Analyticity of Dirichlet series

Theorem 25.1. *A Dirichlet series $\mathbb{D}(f, s)$ converges uniformly on every compact subset in the half-plane of convergence $\Re(s) > \sigma_c(f)$ and in particular is analytic there, with*

$$D'(f, s) = D(f', s) = - \sum_{n=1}^{\infty} \frac{f(n) \log n}{n^s} \quad \text{for } \Re(s) > \sigma_c(f).$$

Proof. Let $R = [\alpha, \beta] \times [c, d]$ be a compact rectangle in the complex plane with $\alpha > \sigma_c(f)$. Fix $\alpha > \sigma_0 > \sigma_c(f)$. By arguing as in the proof of Theorem 24.1, there exists $M > 0$ such that for any $s \in R$ we have

$$\left| \sum_{a < n \leq b} \frac{f(n)}{n^s} \right| \leq 2M \left(1 + \frac{|s - s_0|}{\sigma - \sigma_0} \right) a^{\sigma_0 - \sigma} \leq 2M \left(1 + \frac{\max_{s \in R} |s - s_0|}{\alpha - \sigma_0} \right) a^{\sigma_0 - \alpha}.$$

RHS is independent of $s \in R$, so $\mathbb{D}(f, s)$ converges uniformly on $s \in R$. The rest follows by Lemma 25.2 □

Lemma 25.2. *let (f_n) be a sequence of functions analytic on an open subset $S \subseteq \mathbb{C}$. Assume (f_n) converges uniformly on every compact subset of S . Then the pointwise limit $f(z) = \lim_{n \rightarrow \infty} f_n(z)$ is analytic on S and the sequence of derivatives f'_n converges uniformly on every compact subset of S to the derivative f' .*

Proof. For any $a \in S$ we have by Cauchy's integral formula

$$f_n(a) = \frac{1}{2\pi i} \oint_{\partial D} \frac{f_n(z)}{z - a} dz$$

for any compact disk $D \subset S$ with $a \in D^\circ$. By uniform convergence, interchanging limit with integral we get $f(a) = \frac{1}{2\pi i} \oint_{\partial D} \frac{f(z)}{z - a} dz$ showing f is analytic. For the derivatives we have

$$f'_n(a) = \frac{1}{2\pi i} \int_{\partial D} \frac{f_n(z)}{(z - a)^2} dz, \quad f'(a) = \frac{1}{2\pi i} \int_{\partial D} \frac{f(z)}{(z - a)^2} dz$$

which shows $f'_n \rightarrow f'$ uniformly on every compact subset of S . □

26 Summatory bounds and Dirichlet series

Proposition 26.1.

1. Let $\delta \in \mathbb{R}$. If $S_a(x) = O(x^\delta)$, then $\mathbb{D}(a, s)$ converges for $\Re(s) > \delta$ and

$$D(a, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = s \int_1^{\infty} \frac{S_a(t)}{t^{s+1}} dt.$$

2. Let $\Re(s_0) > 0$. If $\mathbb{D}(a, s_0)$ converges, then $S_a(x) = o(x^{\Re(s_0)})$.

Proof. (1) We have

$$\begin{aligned} \sum_{n \leq x} \frac{a_n}{n^s} &= a_1 + [S_a(t)t^{-s}]_1^x + s \int_1^x \frac{S_a(t)}{t^{s+1}} dt \\ &= S_a(x)x^{-s} + s \int_1^{\infty} \frac{S_a(t)}{t^{s+1}} dt - s \int_x^{\infty} \frac{S_a(t)}{t^{s+1}} dt \\ &= s \int_1^{\infty} \frac{S_a(t)}{t^{s+1}} dt + O(x^{-(\Re(s)-\delta)}). \end{aligned}$$

(2) Write $b_n = a_n/n^{s_0}$ and $\sigma_0 = \Re(s_0) > 0$. Since $\sum_{n=1}^{\infty} b_n = B$ converges, writing $r(x) = \sum_{n>x} b_n$ we have

$$\begin{aligned} S_a(x) &= \sum_{n \leq x} b_n n^{s_0} = (B - r(x))x^{s_0} - s_0 \int_1^x (B - r(t))t^{s_0-1} dt \\ &= B - r(x)x^{s_0} + s_0 \int_1^x r(t)t^{s_0-1} dt. \end{aligned}$$

Since $r(x) = o(1)$, it suffices to show that $\int_1^x r(t)t^{s_0-1} dt = o(x^{\sigma_0})$. Given $\epsilon > 0$, choose $T > 1$ such that $|r(t)| < \epsilon$ for all $t > T$. Then

$$\left| \int_1^x r(t)t^{s_0-1} dt \right| \leq O_{\epsilon, T}(1) + \frac{\epsilon}{\sigma_0} x^{\sigma_0}.$$

Thus $\limsup_{x \rightarrow \infty} \frac{|\int_1^x r(t)t^{s_0-1} dt|}{x^{\sigma_0}} \leq \frac{\epsilon}{\sigma_0}$. Letting $\epsilon \rightarrow 0$ gives the result. $\square$

Example 26.2. In the case $a_n \equiv 1$ and $\delta = 1$, we recover $\Re(s) > \delta$

$$\zeta(s) = s \int_1^{\infty} \frac{[t]}{t^{s+1}} dt = \left[\frac{s}{1-s} t^{1-s} \right]_1^{\infty} - s \int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt = \frac{s}{s-1} - s \int_1^{\infty} \frac{\{t\}}{t^{s+1}} dt.$$

27 Chebyshev functions

Definition 27.1. The first Chebyshev function is

$$\vartheta(x) = \sum_{p \leq x} \log p.$$

The second Chebyshev function is

$$\psi(x) = S_{\Lambda}(x) = \sum_{p^k \leq x} \log p = \sum_{k=1}^{\infty} \vartheta(x^{1/k}).$$

Remark 27.2. Using the trivial inequality $\vartheta(x) \leq x \log x$ we have

$$0 \leq \psi(x) - \vartheta(x) = \sum_{2 \leq k \leq \log_2 x} \vartheta(x^{1/k}) \leq \frac{\log x}{\log 2} \cdot \sqrt{x} \log \sqrt{x} = o(x).$$

Definition 27.3. Let us write $f(x) \asymp g(x)$ if $g(x) \ll f(x) \ll g(x)$.

Theorem 27.4 (Chebyshev). $\vartheta(x) \asymp x$ and $\psi(x) \asymp x$.

Proof. Suffices to show $\vartheta(n) \leq 2n \log 2 \leq \psi(2n+1)$. If $n < p \leq 2n$ and p is prime, then $p \mid \binom{2n}{n}$. Thus

$$\prod_{n < p \leq 2n} p \mid \binom{2n}{n} \leq \sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n}.$$

Taking logarithms and considering dyadic sums, first inequality follows. Next, note that (argument due to M. Nair)

$$I = \int_0^1 x^n (1-x)^n dx = \sum_{k=0}^n \binom{n}{k} (-1)^k \int_0^1 x^{n+k} dx = \sum_{k=0}^n \binom{n}{k} \frac{(-1)^k}{n+k+1} \in \mathbb{Q}_{>0}$$

and using $x(1-x) \leq 1/4$ for $x \in [0, 1]$ we get $I \leq 2^{-2n}$. On the other hand, $\text{lcm}(1, \dots, n) = e^{\psi(n)}$. Indeed, for any prime p , the p -adic valuation of both sides is $\max\{k \in \mathbb{Z}_{\geq 0} : p^k \leq n\}$. Thus we have $e^{\psi(2n+1)} I \geq 1$ and hence $\psi(2n+1) \geq \log(2^{2n}) = 2n \log 2$. $\square$

28 Equivalent formulations of PNT

Proposition 28.1.

$$\boxed{\vartheta(x) = \pi(x) \log x - \int_2^x \frac{\pi(t)}{t} dt} \quad \text{and} \quad \boxed{\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt.}$$

Proof. By partial summation, we have

$$\vartheta(x) = \log 2 + \sum_{2 < p \leq x} \log p = \log 2 + [\pi(t) \log t]_2^x - \int_2^x \frac{\pi(t)}{t} dt$$

giving the first part. The second part uses $(1/\log t)' = -1/(t(\log t)^2)$. $\square$

Theorem 28.2. *We have*

$$\boxed{\lim_{x \rightarrow \infty} \frac{\vartheta(x)}{x} = \lim_{x \rightarrow \infty} \frac{\psi(x)}{x} = \lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x}}$$

PROVIDED THAT at least one of the limits exists.

Proof. The equality of first two limits (if either exists) follows from the fact that $|\vartheta(x) - \psi(x)| = o(x)$. Now note that, for all $k \in \mathbb{N}$,

$$\int_2^x \frac{dt}{(\log t)^k} = \int_2^{\sqrt{x}} + \int_{\sqrt{x}}^x \leq \frac{\sqrt{x} - 2}{(\log 2)^k} + \frac{x - \sqrt{x}}{(\log \sqrt{x})^k} = O\left(\frac{x}{(\log x)^k}\right).$$

Suppose $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = \alpha$. We have $\pi(t)/t = O(1/\log t)$ for $t \geq 2$ so

$$\frac{\vartheta(x)}{x} = \frac{\pi(x)}{x/\log x} - \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = \alpha + o(1) + \frac{1}{x} O\left(\int_2^x \frac{1}{\log t} dt\right) = \alpha + o(1).$$

Suppose $\lim \vartheta(x)/x = \alpha$. This implies $\vartheta(t)/t = O(1)$ for $t \geq 2$ so

$$\frac{\pi(x)}{x/\log x} = \frac{\vartheta(x)}{x} + \frac{\log x}{x} \int_2^x \frac{\vartheta(t)}{t(\log t)^2} dt = \alpha + o(1) + \frac{\log x}{x} O\left(\int_2^x \frac{dt}{(\log t)^2}\right)$$

which is $\alpha + o(1)$. $\square$

Remark 28.3. Same proof gives $\vartheta(x) \asymp x$ iff $\psi(x) \asymp x$ iff $\pi(x) \asymp x/\log x$.

Theorem 28.4 (Chebyshev). $\boxed{\pi(x) \asymp x/\log x.}$

29 Logarithmic average

Definition 29.1. The logarithmic average of $a : \mathbb{N} \rightarrow \mathbb{C}$ up to x is

$$\frac{1}{\log x} \sum_{n \leq x} \frac{a_n}{n}.$$

Remark 29.2. The above is asymptotic to $(\sum_{n \leq x} a_n/n)/(\sum_{n \leq x} 1/n)$.

Proposition 29.3. *Let a be an arithmetic function. Let $\alpha \in \mathbb{C}$. Then*

$$\lim_{x \rightarrow \infty} \frac{1}{x} \sum_{n \leq x} a_n = \alpha \quad \implies \quad \lim_{x \rightarrow \infty} \frac{1}{\log x} \sum_{n \leq x} \frac{a_n}{n} = \alpha.$$

Proof. By partial summation, we have

$$\sum_{n \leq x} \frac{a_n}{n} = \frac{S_a(x)}{x} + \int_1^x \frac{S_a(t)}{t^2} dt = \int_1^x \frac{S_a(t)}{t^2} dt + O(1).$$

Let us define $y = y(x) \geq 0$ nondecreasing so that:

1. $\lim_{x \rightarrow \infty} y = \infty$, and
2. $\log y = o(\log x)$.

For instance, $y(x) = \exp((\log x)^{1/2})$. Writing $S_a(x) = \alpha x + E(x)$, we have

$$\begin{aligned} \sum_{n \leq x} \frac{a_n}{n} &= \int_1^{y(x)} \frac{S_a(t)}{t^2} dt + \int_{y(x)}^x \frac{S_a(t)}{t^2} dt + O(1) \\ &= \int_{y(x)}^x \frac{\alpha t + E(t)}{t^2} dt + O(\log y(x)) \\ &= [\alpha \log t]_{y(x)}^x + \int_{y(x)}^x \frac{E(t)}{t^2} dt + o(\log x). \end{aligned}$$

Finally, $\int_{y(x)}^x \frac{|E(t)|}{t^2} dt \leq \left(\sup_{y(x) \leq t \leq x} \frac{|E(t)|}{t} \right) \int_{y(x)}^x \frac{dt}{t} = o(\log x).$ □

Example 29.4. Suppose that $\sum_{p \leq x} \log p \sim \alpha x$ with $\alpha > 0$. Then

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

30 Mertens' theorems

Theorem 30.1 (Mertens).

1.

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

2. There is a constant M such that

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + M + O\left(\frac{1}{\log x}\right).$$

Proof. (1) Using $\log n = \sum_{d|n} \Lambda(d)$, we have

$$\sum_{n \leq x} \log n = \sum_{n \leq x} \sum_{d|n} \Lambda(d) = \sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = x \sum_{n \leq x} \frac{\Lambda(n)}{n} + O\left(\sum_{n \leq x} \Lambda(n)\right).$$

Using Chebyshev's theorem, we get

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

(2) Let $S(x) = \sum_{p \leq x} \frac{\log p}{p}$. Partial summation gives

$$\sum_{p \leq x} \frac{1}{p} = \frac{1}{2} + \left[\frac{S(t)}{\log t} \right]_2^x + \int_2^x \frac{S(t)}{t(\log t)^2} dt = 1 + \int_2^x \frac{S(t)}{t(\log t)^2} dt + O\left(\frac{1}{\log x}\right).$$

Let us write $\sum_{p \leq x} \frac{\log p}{p} = \log x + R(x)$ so that $R(x) = O(1)$. Then

$$\int_2^x \frac{S(t)}{t(\log t)^2} dt = \int_2^x \frac{1}{t \log t} dt + \int_2^x \frac{R(t)}{t(\log t)^2} dt = [\log \log t]_2^x + C + O\left(\frac{1}{\log x}\right),$$

where $C = \int_2^\infty \frac{R(t)}{t(\log t)^2} dt$ converges since $R(t) = O(1)$. $\square$

Corollary 30.2. *If the limit $\lim_{x \rightarrow \infty} \pi(x)/(x/\log x) = \alpha$ exists, then $\alpha = 1$.*

Remark 30.3. The above corollary was first proved by Chebyshev by a more elaborate method, before Mertens' theorems were available.

31 Bertrand's postulate

Theorem 31.1 (Chebyshev). *For all n sufficiently large, there exists a prime p satisfying $n \leq p \leq 2n$.*

Proof. We follow the proof by S. Ramanujan. Let $a_0 \geq a_1 \geq \dots$ be a nonincreasing sequence with $\lim_{n \rightarrow \infty} a_n = 0$. Then we have

$$a_0 - a_1 \leq \sum_{n=0}^{\infty} (-1)^n a_n \leq a_0 - a_1 + a_2.$$

Using $\log n = \sum_{d|n} \Lambda(d)$, we get

$$T(x) := \sum_{n \leq x} \log n = \sum_{n \leq x} \sum_{d|n} \Lambda(d) = \sum_{e \leq x} \psi\left(\frac{x}{e}\right).$$

We have

$$\sum_{n \leq x} (-1)^{n-1} \psi\left(\frac{x}{n}\right) = T(x) - 2T\left(\frac{x}{2}\right) = (\log 2)x + O(\log x).$$

It follows that

$$\psi(x) - \psi\left(\frac{x}{2}\right) \leq (\log 2)x + O(\log x) \leq \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right).$$

From the first inequality, we get $\psi(x) \leq 2(\log 2)x + O((\log x)^2)$. Using this to bound $\psi(x/3)$ from above and using the second inequality, we get

$$\begin{aligned} \psi(x) - \psi\left(\frac{x}{2}\right) &\geq (\log 2)x + O(\log x) - \left(2(\log 2)\frac{x}{3} + O((\log(x/3))^2)\right) \\ &= \frac{\log 2}{3}x + O((\log x)^2). \end{aligned}$$

Since $\vartheta(x) = \psi(x) + O(\sqrt{x}(\log x)^2)$ we get

$$\vartheta(x) - \vartheta\left(\frac{x}{2}\right) \geq \frac{\log 2}{3}x + O(\sqrt{x}(\log x)^2) > 0$$

for all large enough x . □

32 Mertens' function

Definition 32.1. The Mertens function is $M(x) = S_\mu(x) = \sum_{n \leq x} \mu(n)$.

Theorem 32.2. *The following are equivalent.*

1. $\sum_{n \leq x} \mu(n) = o(x)$.
2. $\sum_{n \leq x} \mu(n) \log n = o(x \log x)$.
3. $\sum_{n \leq x} \mu(n)/n = o(1)$.

Proof. Using partial summation and using $M(x) = O(x)$,

$$\sum_{n \leq x} \mu(n) \log n = M(x) \log x - \int_1^x \frac{M(t)}{t} dt = M(x) \log x + O(x)$$

proving (1) $\Leftrightarrow$ (2). The implication (1) $\Rightarrow$ (3) is left as an exercise. By partial summation, letting $A(x) = \sum_{n \leq x} \mu(n)/n$,

$$M(x) = A(x)x - \int_1^x A(t) dt$$

so for (3) $\Rightarrow$ (1) it suffices to show $\int_1^x A(t) dt = o(x)$ assuming (3). But if (3) holds, then for every ϵ we can find $c(\epsilon)$ such that $|A(t)| < \epsilon$ for $t \geq c(\epsilon)$. Since $|A(x)| \leq 1$ for all $x \geq 1$ by Cor. 17.3, we have

$$\left| \int_1^x A(t) dt \right| = \left| \int_1^{c(\epsilon)} + \int_{c(\epsilon)}^x \right| \leq c(\epsilon) - 1 + \epsilon(x - c(\epsilon)).$$

It follows that $\limsup_{x \rightarrow \infty} \frac{1}{x} \left| \int_1^x A(t) dt \right| \leq \epsilon$. The result follows. $\square$

Lemma 32.3.

$$-\sum_{n \leq x} \mu(n) \log n = \sum_{n \leq x} \mu(n) \psi\left(\frac{x}{n}\right).$$

Proof. We have

$$\Lambda(n) = \sum_{d|n} \mu(d) \log(n/d) = \delta_1(n) \log n - \sum_{d|n} \mu(d) \log d = - \sum_{d|n} \mu(d) \log d.$$

Applying Möbius inversion, we get $-\mu(n) \log n = \sum_{d|n} \mu(d) \Lambda\left(\frac{n}{d}\right)$. The desired result follows by summation. $\square$

33 Mertens' function and PNT, part I

Theorem 33.1. *The prime number theorem implies that*

$$M(x) = \sum_{n \leq x} \mu(n) = o(x).$$

Proof. Let

$$H(x) = \sum_{n \leq x} \mu(n) \psi\left(\frac{x}{n}\right).$$

By Thm 32.2, it suffices to show that $\psi(x) \sim x$ implies $H(x) = o(x \log x)$. Let $\epsilon > 0$. Choose $A > 0$ such that $|\psi(x) - x| < \epsilon x$ for all $x \geq A$. Assume now $x > A$ and write $y = [x/A]$. Then

$$H(x) = \sum_{n \leq y} \mu(n) \psi\left(\frac{x}{n}\right) + \sum_{y < n \leq x} \mu(n) \psi\left(\frac{x}{n}\right).$$

If $n \leq y \leq x/A$ then $A \leq x/n$, so we have using Cor 17.3

$$\begin{aligned} \left| \sum_{n \leq y} \mu(n) \psi\left(\frac{x}{n}\right) \right| &= \left| x \sum_{n \leq y} \frac{\mu(n)}{n} + \sum_{n \leq y} \mu(n) \left(\psi\left(\frac{x}{n}\right) - \frac{x}{n} \right) \right| \\ &< x + \epsilon \sum_{n \leq y} \frac{x}{n} < x + \epsilon x(1 + \log y) < x + \epsilon x + \epsilon x \log x. \end{aligned}$$

On the other hand, if $y < n \leq x$ then $x/n \leq x/(y+1) < A$. Thus

$$\left| \sum_{y < n \leq x} \mu(n) \psi\left(\frac{x}{n}\right) \right| \leq \psi(A) \sum_{y < n \leq x} |\mu(n)| \leq \psi(A)x.$$

Thus we have $|H(x)| < (2 + \psi(A))x + \epsilon x \log x$ if $\epsilon < 1$. Dividing by $x \log x$, we get $\limsup_{x \rightarrow \infty} \frac{1}{x \log x} |H(x)| \leq 2\epsilon$. The desired result follows. $\square$

34 Mertens' function and PNT, part II

Theorem 34.1. *Assume that $M(x) = o(x)$. Then $\psi(x) \sim x$.*

Proof. Let us define

$$f(n) = \sigma_0(n) - \log n - 2\gamma$$

where γ is Euler's constant. By Dirichlet's theorem 13.2 and Example 3.3 we have $S_f(x) = O(\sqrt{x})$. Choose $B > 0$ such that $|S_f(x)| \leq B\sqrt{x}$ for all $x \geq 1$. Note that $\mu * f = 1 - \Lambda - 2\gamma\delta_1$ since $\sigma_0 = 1 * 1$ and $-1' = 1 * \Lambda$, so

$$x - \psi(x) = S_{\mu*f}(x) + O(1).$$

It thus suffices to show $S_{\mu*f}(x) = o(x)$. Write $x = yz$ with $y, z > 0$. Note

$$\left| \sum_{a \leq y} \mu(a) S_f\left(\frac{x}{a}\right) \right| \leq \sum_{a \leq y} B \sqrt{\frac{x}{a}} \leq B\sqrt{x} \sum_{a \leq y} \frac{1}{\sqrt{a}} \leq A\sqrt{xy} = \frac{Ax}{\sqrt{z}}.$$

for some $A > B$ determined by B and independent of x, y, z . By the hyperbola method, we have

$$\begin{aligned} |S_{\mu*f}(x)| &= \left| \sum_{a \leq y} \mu(a) S_f\left(\frac{x}{a}\right) + \sum_{b \leq z} M\left(\frac{x}{b}\right) f(b) - M(y) S_f(z) \right| \\ &\leq A \frac{x}{\sqrt{z}} + \max_{b \leq z} \left| \frac{M(x/b)}{x/b} \right| x \left(\sum_{b \leq z} \frac{|f(b)|}{b} \right) + B \frac{x}{\sqrt{z}}. \end{aligned}$$

Let $\epsilon > 0$. We can fix $z > 0$ large enough so that $A/\sqrt{z} < \epsilon$. Let $W \geq 1$ be large enough so that $|M(w)/w| < \epsilon (\sum_{b \leq z} |f(b)|/b)^{-1}$ for all $w > W$. Then $|S_{\mu*f}(x)| \leq 3\epsilon x$ for all $x \geq zW$. Since ϵ was arbitrary, we are done. $\square$

35 Finite abelian groups and characters

Definition 35.1. Let A be a finite abelian group. A *character* of A is a group homomorphism $\chi : A \rightarrow \mathbb{C}^*$. The *trivial character* of A is the character $\chi_0 : A \rightarrow \mathbb{C}^*$ given by $\chi_0(a) = 1$ for all $a \in A$.

Remark 35.2. Let $n = |A|$. Then $a^n = 1$ for all $a \in A$. If χ is a character, then $\chi(a)^n = \chi(a^n) = \chi(1) = 1$ so $\chi(a)$ is an n th root of unity.

Proposition 35.3. Let A be a finite abelian group. Then the set $\widehat{A}$ of characters of A forms an abelian group under pointwise multiplication, with identity χ_0 . The inverse of a character $\chi : A \rightarrow \mathbb{C}^*$ is given by $\bar{\chi}$ where $\bar{\chi}(a) = \overline{\chi(a)}$ for all $a \in A$. $\square$

Proposition 35.4. Let A, A' be finite abelian groups.

1. There is a natural isomorphism $\widehat{A \times A'} \simeq \widehat{A} \times \widehat{A'}$.
2. The group $\widehat{A}$ is isomorphic to A . In particular, $|\widehat{A}| = |A|$.
3. If $1 \neq a \in A$, there is a character χ such that $\chi(a) \neq 1$.

Proof. (1) Let $i : A \rightarrow A \times A'$ and $i' : A' \rightarrow A \times A'$ be the inclusion homomorphisms given by $i(a) = (a, 1)$ and $i'(a') = (1, a')$ for all $a \in A$ and $a' \in A'$. Then the assignment $\chi \mapsto (\chi \circ i, \chi \circ i')$ gives us a group homomorphism $\widehat{A \times A'} \simeq \widehat{A} \times \widehat{A'}$ which is bijective (Exercise).

(2) By the classification of finitely generated abelian groups, A is a product of finitely many finite cyclic groups. By (1), it suffices to prove the claim where A is a finite cyclic group. Let a be a generator of A , and $n = |A|$. Then $A \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mu_n$ where $\mu_n = \{e^{2\pi i k/n} : 1 \leq k \leq n\} \subseteq \mathbb{C}^*$ is the group of n th roots of unity. For each $\zeta \in \mu_n$, there is a unique character $\chi_\zeta : A \rightarrow \mathbb{C}^*$ such that $\chi_\zeta(a) = \zeta$. The assignment $\zeta \mapsto \chi_\zeta$ is a bijective homomorphism $\mu_n \simeq \widehat{A}$.

(3) Suffices to treat the case A is cyclic, where the result is clear. $\square$

36 Orthogonality of characters

Proposition 36.1 (Orthogonality). *Let A be a finite abelian group.*

1. *For any $\chi \in \widehat{A}$, we have*

$$\sum_{a \in A} \chi(a) = \begin{cases} |A| & \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases}$$

2. *For any $a \in A$, we have*

$$\sum_{\chi \in \widehat{A}} \chi(a) = \begin{cases} |A| & a = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Proof. (1) We have $\sum_{a \in A} \chi_0(a) = |A|$. If $\chi \neq \chi_0$, there exists $b \in A$ such that $\chi(b) \neq 1$. Since multiplication by b permutes A , we have

$$\chi(b) \sum_{a \in A} \chi(a) = \sum_{a \in A} \chi(ba) = \sum_{a \in A} \chi(a).$$

Thus we have $(\chi(b) - 1) \sum_{a \in A} \chi(a) = 0$ and $\sum_{a \in A} \chi(a) = 0$.

(2) There are $|A|$ characters of A . If $a \neq 1$, there exists a character χ_1 such that $\chi_1(a) \neq 1$. Since multiplication by χ_1 permutes $\widehat{A}$,

$$\chi_1(a) \sum_{\chi} \chi(a) = \sum_{\chi} (\chi_1 \chi)(a) = \sum_{\chi} \chi(a).$$

Thus we have $(\chi_1(a) - 1) \sum_{\chi} \chi(a) = 0$ and $\sum_{\chi} \chi(a) = 0$. □

Corollary 36.2. *Let A be a finite abelian group.*

1. *For any $\chi, \chi' \in \widehat{A}$, we have*

$$\sum_{a \in A} \chi(a) \bar{\chi}'(a) = \begin{cases} |A| & \chi = \chi' \\ 0 & \text{otherwise.} \end{cases}$$

2. *For any $a, a' \in A$, we have*

$$\sum_{\chi \in \widehat{A}} \chi(a) \bar{\chi}(a') = \begin{cases} |A| & a = a' \\ 0 & \text{otherwise.} \end{cases}$$

37 Dirichlet characters

Definition 37.1. Let $q \in \mathbb{N}$. A *Dirichlet character* mod q is a group homomorphism

$$\chi : (\mathbb{Z}/q\mathbb{Z})^* \rightarrow \mathbb{C}^*.$$

We extend χ to a function $\chi : \mathbb{N} \rightarrow \mathbb{C}$ by setting $\chi(n) = \chi(n \bmod q)$ if $(n, q) = 1$ and $\chi(n) = 0$ otherwise. The *trivial character* mod q is the character mod q given by $\chi_0(a) = 1$ for all $(a, q) = 1$.

Exercise 37.2. A Dirichlet character χ is completely multiplicative.

Remark 37.3. By the Chinese remainder theorem, if $q = p_1^{a_1} \cdots p_k^{a_k}$ for distinct primes p_i then we have $(\mathbb{Z}/q\mathbb{Z})^* \simeq \prod_{i=1}^k (\mathbb{Z}/p_i^{a_i}\mathbb{Z})^*$. Moreover, one can show directly that:

1. If p is odd, then $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic for every $k \in \mathbb{N}$, and
2. If $a \geq 3$, then $(\mathbb{Z}/2^a\mathbb{Z})^* \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{a-2}\mathbb{Z})$.

Thus one may avoid the classification of finitely generated abelian groups when developing Dirichlet characters.

Definition 37.4. The *Dirichlet L -series* for a Dirichlet character χ is

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

Since $|\chi(n)| \leq 1$, the series converges absolutely for $\Re(s) > 1$. In particular, since χ is completely multiplicative we have

$$L(s, \chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \quad \Re(s) > 1.$$

Lemma 37.5. If χ is a nontrivial Dirichlet character, then the Dirichlet series $\sum_{n=1}^{\infty} \chi(n)/n^s$ converges for $\Re(s) > 0$.

Proof. It suffices to show that $\sum_{n \leq x} \chi(n) = O(1)$. This follows from the following orthogonality relation for a Dirichlet character χ :

$$\sum_{a \bmod q} \chi(a) = \begin{cases} \varphi(q) & \chi = \chi_0 \\ 0 & \text{otherwise.} \end{cases} \quad \square$$

38 Dirichlet L -functions and primes

Lemma 38.1.

$$\boxed{\sum_p \sum_{n=1}^{\infty} \frac{1}{np^{n\sigma}} < \infty \quad \forall \sigma > 1,} \quad \boxed{\sum_p \sum_{n=2}^{\infty} \frac{1}{np^{n\sigma}} < \infty \quad \forall \sigma > \frac{1}{2}.$$

Proof. We have a Taylor series expansion $\log(1-x) = -\sum_{n=1}^{\infty} \frac{1}{n}x^n$ that converges absolutely for $|x| < 1$. Thus, for $\sigma > 1$ we have

$$\infty > \log \zeta(\sigma) = -\sum_p \log \left(1 - \frac{1}{p^\sigma}\right) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{n\sigma}}.$$

For the second part, we have

$$\sum_p \sum_{n=2}^{\infty} \frac{1}{np^{n\sigma}} \leq \sum_p \sum_{n=2}^{\infty} \frac{1}{p^{n\sigma}} = \sum_p \frac{1}{p^{2\sigma}} \frac{1}{1 - p^{-\sigma}} \leq \frac{1}{1 - 2^{-\sigma}} \sum_p \frac{1}{p^{2\sigma}} < \infty$$

valid for all $\sigma > 1/2$. □

Proposition 38.2. *Let $(a, q) = 1$. For $s > 1$, we have*

$$\boxed{\sum_{\chi \bmod q} \overline{\chi(a)} \log L(s, \chi) = \varphi(q) \sum_{n=1}^{\infty} \sum_{p^n \equiv a \bmod q} \frac{1}{np^{ns}} \geq 0.}$$

Proof.

$$\begin{aligned} \sum_{\chi \bmod q} \overline{\chi(a)} \log L(s, \chi) &= -\sum_{\chi} \overline{\chi(a)} \sum_{(p,q)=1} \log \left(1 - \frac{\chi(p)}{p^s}\right) \\ &= \sum_{\chi} \overline{\chi(a)} \sum_{(p,q)=1} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{\chi(p)}{p^s}\right)^n \\ &= \sum_{n=1}^{\infty} \sum_{(p,q)=1} \frac{1}{np^{ns}} \sum_{\chi \bmod q} \overline{\chi(a)} \chi(p^n) \quad \text{by abs. conv.} \\ &= \varphi(q) \sum_{n=1}^{\infty} \sum_{p^n \equiv a \bmod q} \frac{1}{np^{ns}} \quad \text{by orthogonality.} \quad \square \end{aligned}$$

Corollary 38.3. $\prod_{\chi \bmod q} L(s, \chi) \geq 1$ for all $s > 1$.

Proof. Apply the previous proposition with $a = 1$. □

39 Nonvanishing of $L(1, \chi)$, part I

Proposition 39.1. *Let $q \in \mathbb{N}$. Let $\chi = \chi_0$ be the trivial character mod q .*

$$\boxed{\lim_{s \rightarrow 1^+} \log L(s, \chi_0) = +\infty,} \quad \boxed{\lim_{s \rightarrow 1^+} (s-1)L(s, \chi_0) = \frac{\varphi(q)}{q}.}$$

Proof.

$$L(s, \chi_0) = \prod_{(p,q)=1} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s) \prod_{p|q} \left(1 - \frac{1}{p^s}\right).$$

Since $\lim_{s \rightarrow 1^+} \log \zeta(s) = +\infty$ and $\lim_{s \rightarrow 1^+} (s-1)\zeta(s) = 1$, the first formula follows and we have

$$\lim_{s \rightarrow 1^+} (s-1)L(s, \chi_0) = \prod_{p|q} \left(1 - \frac{1}{p}\right) = \frac{\varphi(q)}{q}. \quad \square$$

Proposition 39.2. *There is at most one nontrivial Dirichlet character $\chi \neq \chi_0$ such that $L(1, \chi) = 0$. Moreover, any such character must be real in the sense that $\chi = \bar{\chi}$.*

Proof. Let $\chi_0, \chi_1, \dots, \chi_{\varphi(q)-1}$ be the Dirichlet characters mod q . Assume toward contradiction that $L(1, \chi_1) = L(1, \chi_2) = 0$. Then for each $j = 1, 2$ we have $L(s, \chi_j) = (s-1)g(s, \chi_j)$ for some $g(s, \chi)$ analytic near $s = 1$.

$$\lim_{s \rightarrow 1^+} \prod_{\chi \bmod q} L(s, \chi) = \lim_{s \rightarrow 1^+} (s-1)^2 L(s, \chi_0) g(s, \chi_1) g(s, \chi_2) \prod_{j \neq 0, 1, 2} L(s, \chi_j) = 0$$

which contradicts the fact that $\prod_{\chi} L(s, \chi) \geq 1$ for all $s > 1$. The second part follows from the fact that if $L(1, \chi) = 0$ then $L(1, \bar{\chi}) = \overline{L(1, \chi)} = 0$. $\square$

Lemma 39.3. *Let $s > 0$ and let χ be a nontrivial Dirichlet character. Then*

$$\sum_{n \leq x} \frac{\chi(n)}{n^s} = L(s, \chi) + O\left(\frac{1}{x^s}\right).$$

Proof. By partial summation,

$$\sum_{n \leq x} \frac{\chi(n)}{n^s} = O\left(\frac{1}{x^s}\right) + s \int_1^x \frac{S_{\chi}(t)}{t^{s+1}} dt = L(s, \chi) - s \int_x^{\infty} \frac{S_{\chi}(t)}{t^{s+1}} dt + O\left(\frac{1}{x^s}\right).$$

Conclude by noting that $\int_x^{\infty} S_{\chi}(t) dt/t^{s+1} = O(1/x^s)$. $\square$

40 Nonvanishing of $L(1, \chi)$, part II

Theorem 40.1. *Let $\chi \neq \chi_0$ be a nontrivial Dirichlet character mod q and let $f(n) = \sum_{d|n} \chi(d)$. Then*

$$\sum_{n \leq x} \frac{f(n)}{\sqrt{n}} = 2L(1, \chi)\sqrt{x} + O(1).$$

Proof. Let us write $g(n) = \chi(n)/\sqrt{n}$ and $h(n) = 1/\sqrt{n}$. Then we have

$$\frac{f(n)}{\sqrt{n}} = \frac{1}{\sqrt{n}} \sum_{ab=n} \chi(a) = \sum_{ab=n} \frac{\chi(a)}{\sqrt{a}} \frac{1}{\sqrt{b}} = (g * h)(n).$$

It follows by the hyperbola method that

$$\sum_{n \leq x} \frac{f(n)}{\sqrt{n}} = \sum_{a \leq \sqrt{x}} g(a) S_h\left(\frac{x}{a}\right) + \sum_{b \leq \sqrt{x}} \frac{1}{\sqrt{b}} \left(S_g\left(\frac{x}{b}\right) - S_g(\sqrt{x}) \right).$$

Now, there exists a constant $B \in \mathbb{R}$ such that

$$S_h(x) = \sum_{n \leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + B + O\left(\frac{1}{\sqrt{x}}\right).$$

Also, $S_g(x) = L(1/2, \chi) + O(1/\sqrt{x})$. Note that

$$\sum_{b \leq \sqrt{x}} \frac{1}{\sqrt{b}} \left(S_g\left(\frac{x}{b}\right) - S_g(\sqrt{x}) \right) = \sum_{b \leq \sqrt{x}} \frac{1}{\sqrt{b}} \left(O\left(\frac{\sqrt{b}}{\sqrt{x}}\right) + O(x^{-1/4}) \right) = O(1).$$

It follows

$$\sum_{n \leq x} \frac{f(n)}{\sqrt{n}} = \sum_{a \leq \sqrt{x}} \frac{\chi(a)}{\sqrt{a}} \left(2\sqrt{\frac{x}{a}} + B + O\left(\frac{\sqrt{a}}{\sqrt{x}}\right) \right) + O(1) = 2\sqrt{x}L(1, \chi) + O(1)$$

using $\sum_{a \leq \sqrt{x}} \frac{\chi(a)}{a} = L(1, \chi) + O(x^{-1/2})$. □

Corollary 40.2. *If χ is a real nontrivial Dirichlet character, $L(1, \chi) \neq 0$.*

Proof. Let $f = 1 * \chi$. Then $f(n) \geq 0$ for all $n \in \mathbb{N}$, and $f(n) \geq 1$ whenever n is a square (exercise: suffice to check at $n = p^k$ for $p \in \mathbb{P}$, $k \in \mathbb{N}$). Thus $\sum_{n \leq x} \frac{f(n)}{\sqrt{n}} \geq \sum_{m \leq \sqrt{x}} \frac{1}{m} \gg \log x$. This implies that $L(1, \chi) > 0$. □

41 Primes in arithmetic progressions

Theorem 41.1. *Let $(a, q) = 1$. Then there are infinitely many primes*

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

Proof. We showed that $L(1, \chi) \neq 0$ for every nontrivial Dirichlet character $\chi \neq \chi_0 \pmod{q}$. Thus, $\log L(1, \chi)$ is finite for each $\chi \neq \chi_0$ so

$$\lim_{s \rightarrow 1+} \varphi(q) \sum_{n=1}^{\infty} \sum_{p^n \equiv a \pmod{q}} \frac{1}{np^{ns}} = \lim_{s \rightarrow 1+} \sum_{\chi \pmod{q}} \overline{\chi(a)} \log L(s, \chi) = +\infty.$$

But $\sum_{n=2}^{\infty} \sum_{p^n \equiv a \pmod{q}} \frac{1}{np^{ns}} \leq \sum_{n=2}^{\infty} \sum_p \frac{1}{np^{ns}} < \infty$ for $s > 1/2$. It follows that

$$\lim_{s \rightarrow 1+} \sum_{p \equiv a \pmod{q}} \frac{1}{p^s} = +\infty$$

showing that there are infinitely many primes $p \equiv a \pmod{q}$. □

Remark 41.2. The proof establishes the stronger statement

$$\sum_{p \equiv a \pmod{q}} \frac{1}{p} = \infty.$$

42 Quadratic characters and discriminants

Definition 42.1. Let $\chi : \mathbb{N} \rightarrow \mathbb{C}$ be a Dirichlet character mod q . For $f \mid q$, we say that χ is induced by a Dirichlet character χ^* modulo f if

$$\chi(n) = \chi^*(n) \quad \text{for all } (n, q) = 1.$$

The conductor $\text{cond}(\chi)$ of χ is the least positive integer f such that χ is induced by a character modulo f . A Dirichlet character mod q is *primitive* if it has conductor q .

Example 42.2. The characters χ_{-4} , $\chi_{\pm 8}$ given by

$$\chi_{-4}(n) = (-1)^{(n-1)/2}, \quad \chi_8(n) = (-1)^{(n^2-1)/8}, \quad \chi_{-8} = \chi_{-4}\chi_8$$

for all odd $n \in \mathbb{N}$ are the only real nontrivial primitive characters of 2-power conductor, of conductor 4 for χ_{-4} and 8 for $\chi_{\pm 8}$. If $p > 0$ is an odd prime, then there is a unique real primitive Dirichlet character χ_p of conductor p given by

$$\chi_p(a) = \left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a, \\ 1 & a \text{ is a quadratic residue mod } p, \\ -1 & \text{otherwise.} \end{cases}$$

We say that $(a, p) = 1$ is a quadratic residue mod p if $x^2 \equiv a \pmod{p}$ admits a solution in $\mathbb{Z}/p\mathbb{Z}$, and a quadratic nonresidue mod p otherwise.

Definition 42.3. A fundamental discriminant is an integer of form

$$D = \begin{cases} d & d \equiv 1 \pmod{4} \text{ squarefree, or} \\ 4d & d \equiv 2, 3 \pmod{4} \text{ squarefree.} \end{cases}$$

Proposition 42.4. *There is a bijection*

$$\{\text{real primitive Dirichlet characters}\} \leftrightarrow \{\text{fundamental discriminants}\} =: \mathcal{D}$$

given by $\chi \mapsto \chi(-1) \text{cond}(\chi)$, with inverse map

$$D \mapsto \chi_D = \chi_{D,2} \prod_{\text{odd } p \mid |D|} \chi_p$$

where $\chi_{D,2} = 1$ if D is odd, χ_{-4} if $D \equiv 4 \pmod{8}$, and $\chi_{(-1)^{(m-1)/2}8}$ if $D = 8m$. □

43 Quadratic reciprocity

Definition 43.1. Let $D \in \mathcal{D}$ be a fundamental discriminant. We define $\left(\frac{D}{\cdot}\right) : \mathbb{N} \rightarrow \mathbb{C}$ by

$$\left(\frac{D}{n}\right) = \prod_{p|n} \left(\frac{D}{p}\right)^{v_p(n)}$$

where the odd-prime factors are Legendre symbols and

$$\left(\frac{D}{2}\right) = \begin{cases} 0 & 2 \mid D, \\ (-1)^{\frac{D^2-1}{8}} & 2 \nmid D. \end{cases}$$

Remark 43.2. $\left(\frac{D}{\cdot}\right)$ is clearly completely multiplicative.

Theorem 43.3 (Quadratic reciprocity). *Let p and q be odd distinct primes.*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{q}{p}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right).$$

Additionally, we have

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = \left(\frac{p}{2}\right).$$

Theorem 43.4. *We have $\chi_D = (D/-)$.*

Proof sketch. Since both sides are completely multiplicative, it suffices to show $\chi_D(p) = (D/p)$ for every $p \in \mathbb{P}$. We sketch the case where D and p are odd and $(D, p) = 1$. Then we have

$$\chi_D(p) = \chi_{D,2}(p) \prod_{\text{odd } q \mid |D|} \chi_q(p).$$

By quadratic reciprocity

$$\chi_D(p) = \prod_{q \mid D} \left(\frac{p}{q}\right) = \prod_{q \mid D} \left(\frac{(-1)^{(q-1)/2} q}{p}\right) = \left(\frac{D}{p}\right)$$

noting that $D = \prod_{q \mid |D|} (-1)^{(q-1)/2} q$. Indeed, the product has absolute value $|D|$ and is congruent to 1 modulo 4, so it equals D . The other cases are left as exercises. $\square$

44 Excursion to algebraic number theory

Let $1 \neq D \in \mathcal{D}$ be a fundamental discriminant. Let $K = \mathbb{Q}(\sqrt{D})$ and define

$$\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[\omega], \quad \omega = \frac{D + \sqrt{D}}{2}.$$

If $I \leq \mathcal{O}$ is a nonzero ideal, we write $N(I) = [\mathcal{O} : I]$. For example, if $0 \neq a \in \mathbb{Z}$ then $N(a\mathcal{O}) = a^2$. The *Dedekind zeta function* of K is given by

$$\zeta_K(s) = \sum_{0 \neq I \leq \mathcal{O}_K} \frac{1}{N(I)^s}.$$

It can be shown that $\zeta_K(s)$ converges absolutely for $\Re s > 1$. Moreover, every nonzero ideal $I \leq \mathcal{O}$ can be uniquely written as a product $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_k^{a_k}$ of nonzero prime ideals $\mathfrak{p}_i \leq \mathcal{O}$. Thus, we have

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s} \right)^{-1}$$

where the product is over the nonzero prime ideals of $\mathcal{O}$.

Proposition 44.1. *Let $D \neq 1$ be a fundamental discriminant, and let*

$$f_D(x) = x^2 - Dx + \frac{D^2 - D}{4}.$$

be the minimal polynomial of ω over $\mathbb{Q}$. Let $p \in \mathbb{P}$.

1. *If $\chi_D(p) = 0$, then $f_D(x) \equiv (x - a)^2 \pmod{p}$ for some $a \in \mathbb{Z}/p\mathbb{Z}$. Moreover, $p\mathcal{O}_K = \mathfrak{p}^2$, $\mathfrak{p} = (p, \omega - a)$, and $N(\mathfrak{p}) = p$.*
2. *If $\chi_D(p) = 1$ then $f_D(x) \equiv (x - a)(x - b) \pmod{p}$ for distinct $a, b \in \mathbb{Z}/p\mathbb{Z}$. Moreover, $p\mathcal{O}_K = \mathfrak{p}_a \mathfrak{p}_b$ where $\mathfrak{p}_a = (p, \omega - a)$ and $\mathfrak{p}_b = (p, \omega - b)$. We have $N(\mathfrak{p}_a) = N(\mathfrak{p}_b) = p$.*
3. *If $\chi_D(p) = -1$ then $f_D(x)$ is irreducible modulo p . Moreover, $p\mathcal{O}_K$ is a prime ideal and $N(p\mathcal{O}_K) = p^2$.*

Corollary 44.2. *If $1 \neq D \in \mathcal{D}$, then*

$$\zeta_K(s) = \prod_{p|D} \left(1 - \frac{1}{p^s} \right)^{-1} \prod_{(p,D)=1} \left\{ \left(1 - \frac{1}{p^s} \right) \left(1 - \frac{\chi_D(p)}{p^s} \right) \right\}^{-1} = \zeta(s) L(s, \chi_D).$$

45 Gaussian integers

Proposition 45.1. *The ring $\mathbb{Z}[i]$ is a Euclidean domain with respect to the Euclidean function $|a + bi| = \sqrt{a^2 + b^2}$, and is in particular a PID.*

Proof. Given $z, w \in \mathbb{Z}[i]$ with $z \neq 0$, let $q \in \mathbb{Z}[i]$ be the Gaussian integer that is closest to $w/z \in \mathbb{C}$ with respect to the Euclidean distance in $\mathbb{C}$. Then we see that $|w/z - q| \leq \frac{1}{\sqrt{2}}$. Writing $r = w - qz$, we find that $|r| < |z|$. $\square$

Corollary 45.2. *We have*

$$\zeta_{\mathbb{Q}(\sqrt{-1})}(s) = \sum_{a=1}^{\infty} \sum_{b=0}^{\infty} \frac{1}{(a^2 + b^2)^s} = \frac{1}{4} \sum_{n=1}^{\infty} \frac{r_2(n)}{n^s}$$

where $r_2(n) = \#\{(a, b) \in \mathbb{Z}^2 : a^2 + b^2 = n\}$.

Corollary 45.3. $\frac{1}{4}r_2(n) = \sum_{d|n} \chi_{-4}(d)$.

Proof. This follows from the above and $\zeta_{\mathbb{Q}(\sqrt{-1})}(s) = \zeta(s)L(s, \chi_{-4})$. $\square$

Theorem 45.4 (Leibniz).

$$L(1, \chi_{-4}) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots = \frac{\pi}{4}.$$

Proof. We have

$$\frac{1}{4} \sum_{n \leq x} r_2(n) = \frac{\pi}{4}x + O(x^{1/2})$$

by lattice-point estimate for a disk of radius $x^{1/2}$. On the other hand,

$$\frac{1}{4} \sum_{n \leq x} r_2(n) = \sum_{n \leq x} \chi_{-4}(n) \left[\frac{x}{n} \right] = x \sum_{n \leq x} \frac{\chi_{-4}(n)}{n} + o(x) = L(1, \chi_{-4})x + o(x).$$

Comparing the two expressions gives us the desired result. $\square$

46 Dirichlet density

Definition 46.1. The Dirichlet density of a set $S \subseteq \mathbb{P}$ of primes is

$$\delta(S) = \lim_{s \rightarrow 1^+} \frac{\sum_{p \in S} \frac{1}{p^s}}{\sum_{p \in \mathbb{P}} \frac{1}{p^s}}$$

provided that the limit exists.

Proposition 46.2. *Let $S \subseteq \mathbb{P}$. Write $\pi_S(x) = \#\{p \in S : p \leq x\}$. If the natural density $d(S) = \lim_{x \rightarrow \infty} \pi_S(x)/\pi(x)$ exists, then so does the Dirichlet density $\delta(S)$ and $d(S) = \delta(S)$.*

Proof. Let us write $\pi_S(x) = d(S)\pi(x) + r(x)$ where $r(x) = o(\pi(x))$. Since $\pi(x) = O(x)$, for $s > 1$ we have

$$\sum_{p \in S} \frac{1}{p^s} = s \int_2^\infty \frac{\pi_S(x)}{x^{s+1}} dx, \quad \sum_{p \in \mathbb{P}} \frac{1}{p^s} = s \int_2^\infty \frac{\pi(x)}{x^{s+1}} dx.$$

It therefore suffices to show, as $s \rightarrow 1^+$,

$$\int_2^\infty \frac{r(x)}{x^{s+1}} dx = o\left(\int_2^\infty \frac{\pi(x)}{x^{s+1}} dx\right).$$

Given $\epsilon > 0$, let $y(\epsilon) \geq 2$ be such that $|r(x)| \leq \epsilon\pi(x)$ for all $x \geq y(\epsilon)$. Then as $s \rightarrow 1^+$ we have

$$\left| s \int_2^\infty \frac{r(x)}{x^{s+1}} dx \right| \leq O_\epsilon(1) + \epsilon s \int_{y(\epsilon)}^\infty \frac{\pi(x)}{x^{s+1}} dx.$$

The desired result follows since $\lim_{s \rightarrow 1^+} \sum_{p \in \mathbb{P}} p^{-s} = +\infty$. □

Theorem 46.3. *Let $(a, q) = 1$. The Dirichlet density of the set $\mathbb{P}_{a,q}$ of primes $p \equiv a \pmod{q}$ is $1/\varphi(q)$.*

Proof. Our proof of Dirichlet's theorem shows that

$$\sum_{p \equiv a \pmod{q}} \frac{1}{p^s} \sim \frac{1}{\varphi(q)} \log L(s, \chi_0) \sim \frac{1}{\varphi(q)} \sum_{p \in \mathbb{P}} \frac{1}{p^s}. \quad \square$$

Remark 46.4. We will later show that $\mathbb{P}_{a,q}$ has natural density $1/\varphi(q)$.

47 Splitting of polynomials mod p

Let $f(x) = a_d x^d + \cdots + a_0 \in \mathbb{Z}[x]$ be an irreducible polynomial, $a_d \neq 0$. Given $\vec{d} = (d_1, \dots, d_r) \in \mathbb{N}^r$ with $\sum_{i=1}^r d_i = d$, let $\mathbb{P}(f, \vec{d})$ be the set of primes p coprime to $a_d \text{disc}(f)$ for which

$$f(x) \equiv a_d f_1(x) \cdots f_r(x) \pmod{p}$$

for some monic irreducible polynomials $f_i \in (\mathbb{Z}/p\mathbb{Z})[x]$ with $\deg(f_i) = d_i$.

Exercise 47.1. Let $f(x) = x^2 - a$, where $1 \neq a \in \mathbb{Z}$ is squarefree.

$$\begin{aligned} \mathbb{P}(f, (2)) &= \{p \nmid 2a : (a/p) = -1\}, \\ \mathbb{P}(f, (1, 1)) &= \{p \nmid 2a : (a/p) = 1\}. \end{aligned}$$

Combining Dirichlet's theorem on primes in arithmetic progressions and quadratic reciprocity, prove that $\delta(\mathbb{P}(f, (2))) = \delta(\mathbb{P}(f, (1, 1))) = \frac{1}{2}$.

Example 47.2. Let $f(x) = x^3 - 2$. Suppose that $p \nmid 6$. If $p \equiv 2 \pmod{3}$, then the map $(\mathbb{Z}/p\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ given by $x \mapsto x^3$ is a bijection since $(3, p-1) = 1$. Thus $x^3 = 2$ has exactly one solution mod p , and hence $p \in \mathbb{P}(f, (1, 2))$. Dirichlet's theorem gives

$$\delta(\mathbb{P}(f, (1, 2))) = \frac{1}{2}.$$

The remaining densities are $\delta(\mathbb{P}(f, (3))) = \frac{1}{3}$, $\delta(\mathbb{P}(f, (1, 1, 1))) = \frac{1}{6}$.

Theorem 47.3. Let $f \in \mathbb{Z}[x]$ be irreducible. For any $\vec{d} = (d_1, \dots, d_r) \in \mathbb{N}^r$ with $\sum_{i=1}^r d_i = d$, the set $\mathbb{P}(f, \vec{d})$ has a natural (hence Dirichlet) density.

Remark 47.4. Given f , let $K_f \subseteq \mathbb{C}$ be the field obtained by adjoining all of the roots of f . Write $\vec{1} = (1, \dots, 1)$. Then $\mathbb{P}(f, \vec{1})$ determines K_f in the sense that, if $\mathbb{P}(f_1, \vec{1})$ and $\mathbb{P}(f_2, \vec{1})$ agree except for finitely many primes, then $K_{f_1} = K_{f_2}$.

Remark 47.5. For polynomials of higher degree, the densities of the different factorization types are governed by the arithmetic symmetries of the roots. The general result is a consequence of the Chebotarev density theorem, whose proof lies beyond the scope of this course.

48 $L(s, \chi) \neq 0$ for $\Re(s) = 1$, part I

Let $q \in \mathbb{N}$, and consider

$$Z_q(s) = \prod_{\chi \bmod q} L(s, \chi).$$

The function $Z_q(s)$ extends meromorphically to $\Re(s) > 0$; it is analytic there except for a simple pole at $s = 1$. Also, $Z_1(s) = \zeta(s)$.

Lemma 48.1. *We have $L(s, \chi) \neq 0$ for all Dirichlet characters $\chi \bmod q$ and all $\Re(s) > 1$. In particular, $Z_q(s) \neq 0$ for $\Re(s) > 1$.*

Proof. For $\sigma = \Re(s) > 1$, we have

$$\sum_p \left| \frac{\chi(p)}{p^\sigma} \right| = \sum_{p \nmid q} \frac{1}{p^\sigma} \leq \sum_p \frac{1}{p^\sigma} < \infty$$

which implies that the Euler product $L(s, \chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}$ converges absolutely to a nonzero number for $\Re(s) > 1$. $\square$

Proposition 48.2. *For all $\sigma > 1$ and $t \in \mathbb{R}$,*

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

Proof. For $\sigma = \Re(s) > 1$, writing $s = \sigma + it$ we have

$$\begin{aligned} \log Z_q(s) &= \varphi(q) \sum_{k=1}^{\infty} \sum_{p^k \equiv 1 \bmod q} \frac{1}{kp^{ks}} \\ &= \varphi(q) \sum_{\substack{n \geq 2 \\ n \equiv 1 \bmod q}} \frac{\Lambda(n)}{n^\sigma \log n} (\cos(t \log n) - i \sin(t \log n)). \end{aligned}$$

So we have, writing $A(\sigma, t) = \Re \log(Z_q(\sigma)^3 Z_q(\sigma + it)^4 Z_q(\sigma + 2it))$,

$$A(\sigma, t) = \varphi(q) \sum_{\substack{n \geq 2 \\ n \equiv 1 \bmod q}} \frac{\Lambda(n)}{n^\sigma \log n} (3 + 4 \cos(t \log n) + \cos(2t \log n)).$$

Since $3 + 4 \cos \theta + \cos 2\theta = 3 + 4 \cos \theta + (2 \cos^2 \theta - 1) = 2(1 + \cos \theta)^2$ for all $\theta \in \mathbb{R}$, we deduce that $A(\sigma, t) \geq 0$ for all $\sigma > 1$ and $t \in \mathbb{R}$. Exponentiate. $\square$

49 $L(s, \chi) \neq 0$ for $\Re(s) = 1$, part II

Let $q \in \mathbb{N}$, and let $Z_q(s) = \prod_{\chi \bmod q} L(s, \chi)$ as before.

Theorem 49.1. $Z_q(1 + it) \neq 0$ for all $0 \neq t \in \mathbb{R}$.

Proof. Suppose that $Z_q(s)$ has a zero of order $m \geq 1$ at some $1 + it$ with $0 \neq t \in \mathbb{R}$. Then $\lim_{\sigma \rightarrow 1^+} (\sigma - 1)^{-m} Z_q(\sigma + it) = c$ for some $0 \neq c \in \mathbb{C}$.

$$|(\sigma - 1)^{3-4m} Z_q(\sigma)^3 Z_q(\sigma + it)^4 Z_q(\sigma + 2it)| \geq |\sigma - 1|^{3-4m}$$

for $\sigma > 1$. As $\sigma \rightarrow 1^+$, the left hand side remains bounded while the right hand side tends to infinity, a contradiction. $\square$

Corollary 49.2. *We have the following.*

1. $\zeta(1 + it) \neq 0$ and $L(1 + it, \chi_0) \neq 0$ for all $0 \neq t \in \mathbb{R}$.
2. $L(1 + it, \chi) \neq 0$ for all $t \in \mathbb{R}$ and all Dirichlet characters $\chi_0 \neq \chi \bmod q$.

Theorem 49.3. *For each Dirichlet character $\chi \bmod q$, we have*

$$D(\Lambda_\chi, s) = \sum_{n=1}^{\infty} \frac{\Lambda(n) \chi(n)}{n^s} = -\frac{L'(s, \chi)}{L(s, \chi)}$$

for all $\Re(s) > 1$. If $\chi \neq \chi_0$, then $D(\Lambda_\chi, s)$ extends to an analytic function on an open neighborhood of $\Re(s) \geq 1$. On the other hand, $D(\Lambda_{\chi_0}, s)$ extends meromorphically to an open neighborhood of $\Re(s) \geq 1$ that is analytic except for a simple pole of residue 1 at $s = 1$.

Proof. We have

$$-\frac{L'(s, \chi)}{L(s, \chi)} = -(\log L(s, \chi))' = -\left(\sum_{k=1}^{\infty} \sum_p \frac{1}{k} \frac{\chi(p)^k}{p^{ks}} \right)' = \sum_{k=1}^{\infty} \sum_p \frac{\chi(p^k) \log p}{p^{ks}}.$$

which gives the desired result. For $\chi = \chi_0$, we have for $\Re(s) > 1$

$$L(s, \chi_0) = \zeta(s) \prod_{p|q} \left(1 - \frac{1}{p^s} \right).$$

Writing $h(s) = (s - 1)\zeta(s)$, we get $h'(s)/h(s) = 1/(s - 1) + \zeta'(s)/\zeta(s)$ showing that $\zeta'(s)/\zeta(s)$ is analytic in a neighborhood of $\Re(s) \geq 1$ except for a simple pole at $s = 1$ with residue -1 . $\square$

50 PNT from Wiener–Ikehara

Theorem 50.1 (Wiener–Ikehara). *Let $D(b, s) = \sum_{n=1}^{\infty} b_n/n^s$ be a Dirichlet series with nonnegative coefficients absolutely convergent for $\Re(s) > 1$. Suppose $D(b, s)$ extends meromorphically to an open neighborhood of $\Re(s) \geq 1$ that is analytic there except for a simple pole at $s = 1$ with residue*

$$R = \lim_{s \rightarrow 1} (s - 1)D(b, s) \geq 0.$$

Then we have $S_b(x) = \sum_{n \leq x} b_n = Rx + o(x)$.

Remark 50.2. The proof using Fourier analysis is given in Section 53.

Theorem 50.3. *Let $(a, q) = 1$. Then*

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n) \sim \frac{1}{\varphi(q)} x.$$

Proof.

$$\sum_{\substack{n \geq 1 \\ n \equiv a \pmod{q}}} \frac{\Lambda(n)}{n^s} = \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \overline{\chi(a)} \sum_{n=1}^{\infty} \frac{\Lambda(n) \chi(n)}{n^s} = \frac{-1}{\varphi(q)} \sum_{\chi \pmod{q}} \overline{\chi(a)} \frac{L'(s, \chi)}{L(s, \chi)}$$

absolutely convergent for $\Re(s) > 1$. RHS extends to an analytic function in an open neighborhood of $\Re(s) \geq 1$ except for a simple pole of residue $(-1/\varphi(q))(-1) = 1/\varphi(q)$ at $s = 1$ coming from $\chi = \chi_0$. The desired follows by an application of the Wiener–Ikehara theorem. $\square$

Exercise 50.4. Let $(a, q) = 1$. Prove that

$$\pi(x; a, q) = \#\{p \in \mathbb{P} : p \leq x, p \equiv a \pmod{q}\} \sim \frac{1}{\varphi(q)} \frac{x}{\log x}.$$

51 Fourier analysis

We use the following standard facts without proof. For $f \in L^1(\mathbb{R})$, define

$$\hat{f}(t) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} f(u) e^{-iut} du.$$

Theorem 51.1.

1. (Fourier inversion) *If $f \in L^1(\mathbb{R})$ is continuous and $\hat{f} \in L^1(\mathbb{R})$, then*

$$f(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \hat{f}(t) e^{itx} dt.$$

2. (Riemann–Lebesgue) *If $f \in L^1(\mathbb{R})$, then $\hat{f}(t) \rightarrow 0$ as $|t| \rightarrow \infty$.*

3. (Parseval) *If $f, k \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$, then $\hat{f}, \hat{k} \in L^2(\mathbb{R})$ and*

$$\int_{\mathbb{R}} f(u) \overline{k(u)} du = \int_{\mathbb{R}} \hat{f}(t) \overline{\hat{k}(t)} dt.$$

Theorem 51.2 (Fejér kernel). *For $\lambda > 0$, the Fejér kernel*

$$K_{\lambda}(x) = \lambda \left(\frac{\sin(\lambda x)}{\lambda x} \right)^2, \quad K_{\lambda}(0) = \lambda,$$

belongs to $L^1(\mathbb{R}) \cap L^2(\mathbb{R})$ and satisfies

$$\widehat{K}_{\lambda}(t) = \begin{cases} \sqrt{\frac{\pi}{2}} \left(1 - \frac{|t|}{2\lambda} \right), & |t| \leq 2\lambda, \\ 0, & |t| > 2\lambda. \end{cases}$$

In particular, $K_{\lambda} \geq 0$ and $\int_{\mathbb{R}} \left(\frac{\sin x}{x} \right)^2 dx = \int_{\mathbb{R}} K_{\lambda}(x) dx = \pi$.

Corollary 51.3. *For every $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$ and $v \in \mathbb{R}$ we have*

$$\int_{\mathbb{R}} f(u) K_{\lambda}(u - v) du = \int_{\mathbb{R}} \hat{f}(t) \widehat{K}_{\lambda}(t) e^{itv} dt.$$

Proof. A change of variables gives $\widehat{K_{\lambda}(\cdot - v)}(t) = e^{-itv} \widehat{K}_{\lambda}(t)$. The boxed formula follows by Parseval's formula, using the fact that K_{λ} and $\widehat{K}_{\lambda}$ are real-valued. $\square$

52 Monotonicity

Proposition 52.1. *Let $g : \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$ be a function such that $g(u) = 0$ for $u < 0$, and $g(u)e^u$ is nondecreasing. Suppose that for every $\lambda > 0$ we have*

$$\lim_{v \rightarrow \infty} \int_0^\infty (g(u) - 1)K_\lambda(u - v) du = 0.$$

Then $\lim_{v \rightarrow \infty} g(v) = 1$.

Proof. Let us write $I(v, \lambda) = \int_{\mathbb{R}} g(v + \alpha/\lambda) \left(\frac{\sin \alpha}{\alpha}\right)^2 d\alpha$. Writing $u = v + \alpha/\lambda$, our hypothesis implies that $\lim_{v \rightarrow \infty} I(v, \lambda) = \pi$ since $\int_{\mathbb{R}} \left(\frac{\sin \alpha}{\alpha}\right)^2 d\alpha = \pi$. Let

$$J(v, \lambda) = \int_{-\sqrt{\lambda}}^{\sqrt{\lambda}} g(v + \alpha/\lambda) \left(\frac{\sin \alpha}{\alpha}\right)^2 d\alpha, \quad S(\lambda) = \int_{-\sqrt{\lambda}}^{\sqrt{\lambda}} \left(\frac{\sin \alpha}{\alpha}\right)^2 d\alpha.$$

Note that $J(v, \lambda) \leq I(v, \lambda)$ for all $v \in \mathbb{R}$ and $\lambda > 0$. For any $|\alpha| \leq \sqrt{\lambda}$,

$$g(v - 1/\sqrt{\lambda})e^{-2/\sqrt{\lambda}} \leq g(v + \alpha/\lambda) \leq g(v + 1/\sqrt{\lambda})e^{2/\sqrt{\lambda}}.$$

Taking the average of $g(v + \alpha/\lambda)$ over $[-\sqrt{\lambda}, \sqrt{\lambda}]$ with weights $(\frac{\sin \alpha}{\alpha})^2$,

$$g(v - 1/\sqrt{\lambda})e^{-2/\sqrt{\lambda}} \leq \frac{J(v, \lambda)}{S(\lambda)} \leq g(v + 1/\sqrt{\lambda})e^{2/\sqrt{\lambda}}.$$

Thus, for all $\lambda > 0$, using $\lim_{v \rightarrow \infty} I(v, \lambda) = \pi$,

$$\begin{aligned} \limsup_{v \rightarrow \infty} g(v) &= \limsup_{v \rightarrow \infty} g(v - 1/\sqrt{\lambda}) \leq \limsup_{v \rightarrow \infty} \frac{J(v, \lambda)}{S(\lambda)} e^{2/\sqrt{\lambda}} \leq \pi \frac{e^{2/\sqrt{\lambda}}}{S(\lambda)}, \\ \liminf_{v \rightarrow \infty} g(v) &= \liminf_{v \rightarrow \infty} g(v + 1/\sqrt{\lambda}) \geq \liminf_{v \rightarrow \infty} \frac{J(v, \lambda)}{S(\lambda)} e^{-2/\sqrt{\lambda}}. \end{aligned}$$

Letting $\lambda \rightarrow \infty$ in the first inequality, we deduce that $\limsup_{v \rightarrow \infty} g(v) \leq 1$ and in particular g is bounded. Let $A = \sup_v g(v)$. Then

$$0 \leq I(v, \lambda) - J(v, \lambda) \leq A \int_{|\alpha| > \sqrt{\lambda}} \left(\frac{\sin \alpha}{\alpha}\right)^2 d\alpha \leq \frac{2A}{\sqrt{\lambda}}.$$

It follows that $\liminf_{v \rightarrow \infty} g(v) \geq (\pi + O(1/\sqrt{\lambda}))e^{-2/\sqrt{\lambda}}/S(\lambda)$ and letting $\lambda \rightarrow \infty$, we find $\liminf_{v \rightarrow \infty} g(v) \geq 1$. Thus $\lim_{v \rightarrow \infty} g(v) = 1$. $\square$

53 Proof of Wiener-Ikehara

Proof. Up to replacing b_n by $b_n + 1$, we may assume $R > 0$. Also, replacing b_n by b_n/R , we may assume $R = 1$. Define $g(u) = S_b(e^u)/e^u$. With $x = e^u$,

$$D(b, s) = s \int_1^\infty \frac{S_b(x)}{x^{s+1}} dx = s \int_0^\infty \frac{e^u}{e^{us}} g(u) du.$$

Since we have $\int_0^\infty \frac{e^u}{e^{us}} du = \frac{1}{s-1}$, we have

$$E(s) := \frac{D(b, s)}{s} - \frac{1}{s-1} = \int_0^\infty (g(u) - 1) \frac{e^u}{e^{us}} du.$$

By our hypothesis on b , $E(s)$ extends to a continuous function $\Re(s) \geq 1$. For each $\delta \geq 0$, define

$$h_\delta(t) = E(1 + \delta + it), \quad \phi_\delta(u) = \begin{cases} (g(u) - 1)e^{-u\delta} & u \geq 0 \\ 0 & u < 0. \end{cases}$$

The boxed formula for $s = 1 + \delta + it$ with $\delta > 0$ becomes $h_\delta(t) = \sqrt{2\pi} \hat{\phi}_\delta(t)$. Since $S_b(x) \ll x^c$ for every $c > 1$, we see $\phi_\delta \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$ for all $\delta > 0$. By Parseval's formula, for all $v \in \mathbb{R}$, $\lambda > 0$, and $\delta > 0$,

$$\int_{-\infty}^\infty \phi_\delta(u) K_\lambda(u - v) du = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^\infty h_\delta(t) \widehat{K}_\lambda(t) e^{itv} dt.$$

By uniform convergence $h_\delta \rightarrow h_0$ on the support of $\widehat{K}_\lambda$ which is compact, the limit as $\delta \rightarrow 0$ of the right hand side exists. Limit of LHS as $\delta \rightarrow 0$ is

$$\int_0^\infty (g(u) - 1) K_\lambda(u - v) du$$

by monotone convergence applied to the g -term and dominated convergence applied to the constant term. Hence,

$$\int_0^\infty (g(u) - 1) K_\lambda(u - v) du = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^\infty h_0(t) \widehat{K}_\lambda(t) e^{itv} dt.$$

The limit as $v \rightarrow \infty$ of the right hand side is zero by the Riemann–Lebesgue lemma. Since $g(u) = 0$ for all $u < 0$ and $g(u)e^u = S_b(e^u)$ is nondecreasing, we deduce by preceding proposition that $\lim_{u \rightarrow \infty} g(u) = 1$, giving $\lim_{x \rightarrow \infty} S_b(x)/x = 1$. $\square$

54 Review of contour integrals

A *contour* is a piecewise continuously differentiable map $\gamma : [a, b] \rightarrow \mathbb{C}$. If f is continuous on the image of γ , define

$$\int_{\gamma} f(s) ds = \int_a^b f(\gamma(t)) \gamma'(t) dt.$$

The contour γ^{-1} is obtained by reversing the orientation. The length of γ is

$$L(\gamma) = \int_a^b |\gamma'(t)| dt.$$

Proposition 54.1. *If f is continuous on the image of γ ,*

$$\left| \int_{\gamma} f(s) ds \right| \leq L(\gamma) \sup_{s \in \gamma} |f(s)|.$$

Proof.

$$\left| \int_{\gamma} f(s) ds \right| \leq \int_a^b |f(\gamma(t))| |\gamma'(t)| dt \leq L(\gamma) \sup_{s \in \gamma} |f(s)|. \quad \square$$

Example 54.2. Let γ be the vertical line segment from $a + ib$ to $a + ic$. Then $L(\gamma) = |c - b|$. If $x > 0$, then $|x^s| = x^{\Re(s)} = x^a$ on γ , so

$$\left| \int_{\gamma} \frac{x^s}{s} ds \right| \leq |c - b| x^a \sup_{s \in \gamma} \frac{1}{|s|}.$$

In particular, if $a \neq 0$, then

$$\left| \frac{1}{2\pi i} \int_{\gamma} \frac{x^s}{s} ds \right| \leq \frac{|c - b| x^a}{2\pi |a|}.$$

Example 54.3. Let γ be an arc of the circle $|s| = \rho$. If $L(\gamma) \leq \theta \rho$ and $|f(s)| \leq M$ on γ , then

$$\left| \int_{\gamma} \frac{f(s)}{s} ds \right| \leq \theta M.$$

Thus the factor ρ arising from the length of the arc cancels the factor ρ^{-1} arising from $1/s$.

55 Cauchy's theorem and residues

Theorem 55.1 (Cauchy's theorem). *Let $D \subseteq \mathbb{C}$ be a simply connected domain, and let f be holomorphic on D . If γ is a closed contour in D , then*

$$\int_{\gamma} f(s) ds = 0.$$

Thus a contour may be deformed with fixed endpoints inside a region on which the integrand is holomorphic without changing its integral.

Theorem 55.2 (Cauchy's integral formula). *Let γ be a positively oriented simple closed contour, and suppose that f is holomorphic on a neighborhood of γ and its interior. If z lies inside γ , then*

$$f(z) = \frac{1}{2\pi i} \int_{\gamma} \frac{f(s)}{s - z} ds.$$

If f is meromorphic near z_0 and

$$f(s) = \sum_{n=-m}^{\infty} a_n (s - z_0)^n,$$

define $\text{Res}_{s=z_0} f(s) = a_{-1}$. For a simple pole,

$$\text{Res}_{s=z_0} f(s) = \lim_{s \rightarrow z_0} (s - z_0) f(s).$$

Theorem 55.3 (Residue theorem). *Let γ be a positively oriented simple closed contour, and suppose that f is meromorphic on a neighborhood of γ and its interior, with no poles on γ . Then*

$$\frac{1}{2\pi i} \int_{\gamma} f(s) ds = \sum_{z \text{ inside } \gamma} \text{Res}_{s=z} f(s).$$

Example 55.4. For $x > 0$, define $x^s = e^{s \log x}$. The function x^s/s has a single simple pole at $s = 0$, with $\text{Res}_{s=0} \frac{x^s}{s} = 1$. Hence, if γ is a positively oriented simple closed contour not passing through 0, then

$$\frac{1}{2\pi i} \int_{\gamma} \frac{x^s}{s} ds = \begin{cases} 1, & 0 \text{ lies inside } \gamma, \\ 0, & 0 \text{ lies outside } \gamma. \end{cases}$$

56 Perron kernel

Exercise 56.1. Let $x > 0$. If $a \neq 0$ and $b, c \in \mathbb{R}$, we have

$$\left| \frac{1}{2\pi i} \int_{a+ib}^{a+ic} \frac{x^s}{s} ds \right| \leq \frac{|c-b|}{2\pi} \frac{x^a}{|a|}, \quad \left| \frac{1}{2\pi i} \int_{b+ia}^{c+ia} \frac{x^s}{s} ds \right| \leq \frac{1}{2\pi|a|} \frac{|x^b - x^c|}{|\log x|}.$$

Define $\delta(x) = 1$ if $x > 1$, $\delta(1) = 1/2$, and $\delta(x) = 0$ if $0 < x < 1$.

Proposition 56.2. Let $c > 0$ and $x > 0$. Then

$$\left| \frac{1}{2\pi i} \int_{c-iR}^{c+iR} \frac{x^s}{s} ds - \delta(x) \right| < \begin{cases} x^c \min(1, R^{-1} |\log x|^{-1}) & x \neq 1 \\ c/R & x = 1 \end{cases}$$

Proof. Choose $a < 0$ if $x > 1$, and $a > c$ if $0 < x < 1$. With this choice $|x^a| \rightarrow 0$ as $|a| \rightarrow \infty$. Let D be the rectangle with corners $a \pm iR$, $c \pm iR$. Since x^s/s has only a simple pole of residue 1 at $s = 0$, $\frac{1}{2\pi i} \int_{\partial D} \frac{x^s}{s} ds = \delta(x)$ by Cauchy's formula. Then as $|a|$ tends to infinity,

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{c-iR}^{c+iR} \frac{x^s}{s} ds - \delta(x) \right| &\leq \frac{1}{2\pi} \left(\left| \int_{c-iR}^{a-iR} \frac{x^s}{s} ds \right| + \left| \int_{c+iR}^{a+iR} \frac{x^s}{s} ds \right| + \left| \int_{a-iR}^{a+iR} \frac{x^s}{s} ds \right| \right) \\ &\leq \frac{1}{\pi R} \frac{|x^c - x^a|}{|\log x|} + \frac{R}{\pi} \frac{x^a}{|a|} \rightarrow \frac{x^c}{\pi R |\log x|}. \end{aligned}$$

Let γ (resp. γ') be the arc of the circle centered at 0 going counterclockwise (resp. clockwise) from $c - iR$ to $c + iR$. Let $\rho = \sqrt{c^2 + R^2}$. Suppose that $0 < x < 1$. Then we have $|x^s| = x^{\Re(s)} \leq x^c$ for s on γ , so

$$\left| \frac{1}{2\pi i} \int_{c-iR}^{c+iR} \frac{x^s}{s} ds \right| = \left| \frac{1}{2\pi i} \int_{\gamma} \frac{x^s}{s} ds \right| \leq \frac{1}{2\pi} \pi \rho \cdot \frac{x^c}{\rho} < x^c.$$

Suppose now that $x > 1$. Then $|x^s| \leq x^c$ for s on γ' , so

$$\left| \frac{1}{2\pi i} \int_{c-iR}^{c+iR} \frac{x^s}{s} ds - 1 \right| = \left| \frac{1}{2\pi i} \int_{\gamma'} \frac{x^s}{s} ds \right| \leq \frac{1}{2\pi} (2\pi \rho) \cdot \frac{x^c}{\rho} = x^c.$$

For $x = 1$, letting $t = cu$ we have

$$\begin{aligned} \frac{1}{2\pi i} \int_{c-iR}^{c+iR} \frac{ds}{s} &= \frac{1}{2\pi i} \int_{-R}^R \frac{i dt}{c + it} = \frac{1}{2\pi} \int_{-R}^R \frac{c - it}{c^2 + t^2} dt = \frac{1}{\pi} \int_0^{R/c} \frac{du}{1 + u^2} \\ &= \frac{1}{2} - \frac{1}{\pi} \int_{R/c}^{\infty} \frac{du}{1 + u^2}, \quad \left| \frac{1}{\pi} \int_{R/c}^{\infty} \frac{du}{1 + u^2} \right| \leq \left| \frac{1}{\pi} \int_{R/c}^{\infty} \frac{du}{u^2} \right| < \frac{c}{R}. \end{aligned}$$

□

57 Perron's formula

Definition 57.1 (Cauchy principal value). Let f be continuous on $\Re(s) = c$. We define

$$\int_{(c)} f(s) ds = \text{p. v.} \int_{c-i\infty}^{c+i\infty} f(s) ds = \lim_{R \rightarrow \infty} \int_{c-iR}^{c+iR} f(s) ds$$

provided that the limit exists.

Theorem 57.2 (Perron's formula). *Let $a : \mathbb{N} \rightarrow \mathbb{C}$ be an arithmetic function such that $D(a, s)$ converges absolutely for $\Re(s) > \sigma$. Then for any $c > \max\{0, \sigma\}$ and $x > 0$ we have*

$$\sum'_{n \leq x} a_n = \frac{1}{2\pi i} \int_{(c)} D(a, s) \frac{x^s}{s} ds$$

where the prime indicates that the term $n = x$, when $x \in \mathbb{N}$, is counted with weight $1/2$.

Proof. Let $R > 0$. By the uniform convergence of $D(a, s)$ for $\Re(s) > \sigma$,

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

It follows that

$$\begin{aligned} & \left| \frac{1}{2\pi i} \int_{c-iR}^{c+iR} D(a, s) \frac{x^s}{s} ds - \sum'_{n \leq x} a_n \right| \\ & \leq \sum_{\substack{n \geq 1 \\ n \neq x}} \frac{|a_n|}{n^c} \min \left\{ 1, \frac{1}{R |\log(x/n)|} \right\} + \delta_{\mathbb{N}}(x) \frac{c|a_x|}{Rx^c}. \end{aligned}$$

For fixed x , the summands in the sum tend to zero as $R \rightarrow \infty$ and are dominated by $|a_n|n^{-c}$, whose sum converges. The result therefore follows from dominated convergence. $\square$

Example 57.3. For any $x > 0$ and $c > 1$,

$$\frac{1}{2\pi i} \int_{(c)} \zeta(s) \frac{x^s}{s} ds = \begin{cases} [x], & x \notin \mathbb{N}, \\ x - \frac{1}{2}, & x \in \mathbb{N}. \end{cases}$$