Otto Forster:

Analytic Number Theory

Lecture notes of a course given in the Winter Semester 2001/02
at the Department of Mathematics, LMU Munich, Germany

Contents

0. Notations and Conventions

Standard notations for sets

$\mathbb{Z}$ ring of all integers

$\mathbb{N}_0$ set of all integers ≥ 0

$\mathbb{N}_1$ set of all integers ≥ 1

$\mathbb{P}$ set of all primes $= \{2, 3, 5, 7, 11, \ldots\}$

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote the fields of rational, real and complex numbers respectively

A^* multiplicative group of invertible elements of a ring A

$[a, b],]a, b[\,, [a, b[\,,]a, b]$ denote closed, open and half-open intervals of $\mathbb{R}$

$\mathbb{R}_+ = [0, \infty[$ set of non-negative real numbers

$\mathbb{R}_+^* = \mathbb{R}_+ \cap \mathbb{R}^*$ multiplicative group of positive real numbers

$\lfloor x \rfloor$ greatest integer $\leq x \in \mathbb{R}$

Landau symbols *O, o*

For two functions $f, g : [a, \infty[\to \mathbb{C}$, one writes

$$f(x) = O(g(x)) \quad \text{for } x \to \infty,$$

if there exist constants $C > 0$ and $x_0 \geq a$ such that

$$|f(x)| \leq C|g(x)| \quad \text{for all } x \geq x_0.$$

Similarly,

$$f(x) = o(g(x)) \quad \text{for } x \to \infty$$

means that for every $\varepsilon > 0$ there exists $R \geq a$ such that

$$|f(x)| \leq \varepsilon|g(x)| \quad \text{for all } x \geq R.$$

For functions $f, g :]a, b[\to \mathbb{C}$ the notions

$$f(x) = O(g(x)) \quad \text{for } x \searrow a,$$

and

$$f(x) = o(g(x)) \quad \text{for } x \searrow a,$$

are defined analogously.

$$f(x) = f_0(x) + O(g(x))$$

is defined as $f(x) - f_0(x) = O(g(x))$.

Asymptotic equality

Two functions $f, g : [a, \infty[\to \mathbb{C}$ are said to be asymptotically equal for $x \to \infty$, in symbols

$$f(x) \sim g(x) \quad \text{for } x \to \infty,$$

if $g(x) \neq 0$ for $x \geq x_0$ and

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Analogously, for two sequences $(a_n)_{n\geqslant n_0}$ and $(b_n)_{n\geqslant n_0}$,

$$a_n \sim b_n$$

means $\lim\limits_{n\to\infty} \dfrac{a_n}{b_n} = 1$. A famous example for asymptotic equality is the Stirling formula

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n,$$

which we will prove in theorem 9.8.

Miscellaneous

We sometimes write ‘iff’ as an abbreviation for ‘if and only if’.

1. Divisibility. Unique Factorization Theorem

1.1. Definition. Let $x, y \in \mathbb{Z}$ be two integers. We define

$$x \mid y \qquad \text{(read: } x \textit{ divides } y\text{)},$$

iff there exists an integer q such that $y = qx$. We write $x \nmid y$, if this is not the case.

1.2. We list some simple properties of divisibility for numbers $x, y, z \in \mathbb{Z}$.

i) $(x \mid y \ \wedge \ y \mid z) \implies x \mid z$.

ii) $x \mid 0$ for all $x \in \mathbb{Z}$.

iii) $0 \mid x \implies x = 0$.

iv) $1 \mid x$ and $-1 \mid x$ for all $x \in \mathbb{Z}$.

v) $(x \mid y \ \wedge \ y \mid x) \implies x = \pm y$.

1.3. Definition. A *prime number* is an integer $p \geq 2$ such that there doesn't exist any integer x with $1 < x < p$ and $x \mid p$.
So the only positive divisors of a prime number p are 1 and p. Note that by definition 1 is not a prime number.

Every integer $x \geq 2$ is either a prime or a product of a finite number of primes. This can be easily proved by induction on x. The assertion is certainly true for $x = 2$. Let now $x > 2$, and assume that the assertion has already been proved for all integers $x' < x$. If x is a prime, we are done. Otherwise there exists a decomposition $x = yz$ with integers $2 \leq y, z < x$. By induction hypothesis, y and z can be written as products of primes

$$y = \prod_{i=1}^{n} p_i, \quad z = \prod_{j=1}^{m} q_j, \qquad (m, n \geq 1, \ p_i, q_j \text{ prime})$$

Multiplying these two formulas gives the desired prime factorization of x.
Using the convention that an empty product (with zero factors) equals 1, we can state that any positive integer x is a product of primes

$$x = \prod_{i=1}^{n} p_i, \quad n \geq 0, \ p_i \text{ primes}.$$

We can now state and prove Euclid's famous theorem on the infinitude of primes.

1.4. Theorem (Euclid). *There exist infinitely many prime numbers.*
Proof. Assume to the contrary that there are only finitely many primes and that

$$p_1 := 2, \ p_2 := 3, \ p_3, \ldots, p_n$$

Chap. 1 last revised: 2003-04-14

is a complete list of all primes. The integer

$$x := p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$$

must be a product of primes, hence must be divisible by at least one of the p_i, $i = 1, \ldots, n$. But this is impossible since

$$\frac{x}{p_i} = (\text{integer}) + \frac{1}{p_i}$$

is not an integer. Hence the assumption is false and there exist infinitely many primes.

Whereas the existence of a prime factorization was easy to prove, the uniqueness is much harder. For this purpose we need some preparations.

1.5. Definition. Two integers $x, y \in \mathbb{Z}$ are called *relatively prime* or *coprime* (G. *teilerfremd*) if they are not both equal to 0 and there does not exist an integer $d > 1$ with $d \mid x$ and $d \mid y$.
This is equivalent to saying that x and y have no common prime factor.
In particular, if p is a prime and x an integer with $p \nmid x$, then p and x are relatively prime.

1.6. Theorem. *Two integers x, y are coprime iff there exist integers n, m such that*

$$nx + my = 1.$$

Proof. "$\Leftarrow$" If $nx + my = 1$, every common divisor d of x and y is also a divisor of 1, hence $d = \pm 1$. So x and y are coprime.
"$\Rightarrow$" Suppose that x, y are coprime. Without loss of generality we may assume $x, y \geq 0$. We prove the theorem by induction on $\max(x, y)$.
The assertion is trivially true for $\max(x, y) = 1$.
Let now $N := \max(x, y) > 1$ und suppose that the assertion has already been proved for all integers x', y' with $\max(x', y') < N$. Since x, y are coprime, we have $x \neq y$, so we may suppose $0 < x < y$. Then $(x, y - x)$ is a pair of coprime numbers with $\max(x, y - x) < N$. By induction hypothesis there exist integers n, m with

$$nx + m(y - x) = 1,$$

which implies $(n - m)x + my = 1$, q.e.d.

1.7. Theorem. *Let $x, y \in \mathbb{Z}$. If a prime p divides the product xy, then $p \mid x$ or $p \mid y$.*

Proof. If $p \mid x$, we are done. Otherwise p and x are coprime, hence there exist integers n, m with $np + mx = 1$. Multiplying this equation by y and using $xy = kp$ with an integer k, we obtain

$$y = npy + mxy = npy + mkp = p(ny + mk).$$

This shows $p \mid y$, q.e.d.

1.8. Theorem (Unique factorization theorem). *Every positive integer can be written as a (finite) product of prime numbers. This decomposition is unique up to order.*

Proof. The existence of a prime factorization has already been proved, so it remains to show uniqueness. Let

$$x = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m \tag{$*$}$$

be two prime factorizations of a positive integer x. We must show that $m = n$ and after rearrangement $p_i = q_i$ for all i. We may assume $n \leq m$. We prove the assertion by induction on n.

a) If $n = 0$, it follows $x = 1$ and $m = 0$, hence the assertion is true in this case.

b) *Induction step* $n-1 \to n$, $(n \geq 1)$. We have $p_1 \mid q_1 \cdot \ldots \cdot q_m$, hence by theorem 1.7, p_1 must divide one of the factors q_i and since q_i is prime, we must have $p_1 = q_i$. After reordering we may assume $i = 1$. Dividing equation $(*)$ by p_1 we get

$$p_2 \cdot \ldots \cdot p_n = q_2 \cdot \ldots \cdot q_m.$$

By induction hypothesis we have $n = m$ and, after reordering, $p_i = q_i$ for all i, q.e.d.

If we collect multiple occurrences of the same prime, we can write every positive integer in a unique way as

$$x = \prod_{i=1}^{n} p_i^{e_i}, \quad p_1 < p_2 < \ldots < p_n \text{ primes}, \ n \geq 0, e_i > 0.$$

This is called the canonical prime factorization of x.

Sometimes a variant of this representation is useful. For an integer $x \neq 0$ and a prime p we define

$$\mathrm{ord}_p(x) := \sup\{e \in \mathbb{N}_0 : p^e \mid x\}.$$

Then every nonzero integer x can be written as

$$x = \mathrm{sign}(x) \prod_p p^{\mathrm{ord}_p(x)}$$

where the product is extended over all primes. Note that $\mathrm{ord}_p(x) = 0$ for all but a finite number of primes, so there is no problem with the convergence of the infinite product.

1.9. Definition (Greatest common divisor). Let $x, y \in \mathbb{Z}$. An integer d is called *greatest common divisor* of x and y, if the following two conditions are satisfied:

i) d ist a common divisor of x and y, i.e. $d \mid x$ and $d \mid y$.

ii) If d_1 is any common divisor of x and y, then $d_1 \mid d$.

If d_1 and d_2 are two greatest common divisors of x and y, then $d_1 \mid d_2$ and $d_2 \mid d_1$, hence by 1.2.v) we have $d_1 = \pm d_2$. Therefore the greatest common divisor is (in case of existence) uniquely determined up to sign. The positive one is denoted by $\gcd(x, y)$. The existence can be seen using the prime factor decomposition. For $x \neq 0$ and $y \neq 0$,

$$\gcd(x, y) = \prod_p p^{\min(\mathrm{ord}_p(x), \mathrm{ord}_p(y))}$$

and $\gcd(x, 0) = \gcd(0, x) = |x|$, $\gcd(0, 0) = 0$.

Two integers x, y are relatively prime iff $\gcd(x, y) = 1$.

The following is a generalization of theorem 1.6.

1.10. Theorem. *Let $x, y \in \mathbb{Z}$. An integer d is greatest common divisor of x and y iff*

i) *d is a common divisor of x and y, and*

ii) *there exist integers n, m such that*

$$nx + my = d.$$

Proof. The case when at least one of x, y equals 0 is trivial, so we may suppose $x \neq 0$, $y \neq 0$.

"$\Rightarrow$" If d is greatest common divisor of x and y, then x/d and y/d are coprime, hence by theorem 1.6 there exist integers n, m with

$$n\frac{x}{d} + m\frac{y}{d} = 1,$$

which implies ii).

The implication "$\Leftarrow$" is trivial.

1.11. Definition (Least common multiple). Let $x, y \in \mathbb{Z}$. An integer m is called *least common multiple* of x and y, if the following two conditions are satisfied:

i) m ist a common multiple of x and y, i.e. $x \mid m$ and $y \mid m$.

ii) If m_1 is any common multiple of x and y, then $m \mid m_1$.

As in the case of the greatest common divisor, the least common multiple of x and y is uniquely determined up to sign. The positive one is denoted by $\mathrm{lcm}(x, y)$. For $x \neq 0$ and $y \neq 0$ the following equation holds

$$\mathrm{lcm}(x, y) = \prod_p p^{\max(\mathrm{ord}(x), \mathrm{ord}(y))}$$

and $\mathrm{lcm}(x, 0) = \mathrm{lcm}(0, x) = \mathrm{lcm}(0, 0) = 0$.

The definitions of the greatest common divisor and least common multiple can be extended in a straightforward way to more than two arguments. One has

$$\begin{aligned} \gcd(x_1, \ldots, x_n) &= \gcd(\gcd(x_1, \ldots, x_{n-1}), x_n), \\ \mathrm{lcm}(x_1, \ldots, x_n) &= \mathrm{lcm}(\mathrm{lcm}(x_1, \ldots, x_{n-1}), x_n). \end{aligned}$$

2. Congruences. Chinese Remainder Theorem

2.1. Definition. Let $m \in \mathbb{Z}$. Two integers x, y are called *congruent modulo* m, in symbols

$$x \equiv y \bmod m,$$

if m divides the difference $x - y$, i.e. $x - y \in m\mathbb{Z}$.

Examples. $20 \equiv 0 \bmod 5, \quad 3 \equiv 10 \bmod 7, \quad -4 \equiv 10 \bmod 7.$

$x \equiv 0 \bmod 2$ is equivalent to "x is even",

$x \equiv 1 \bmod 2$ is equivalent to "x is odd".

Remarks. a) x, y are congruent modulo m iff they are congruent modulo $-m$.

b) $x \equiv y \bmod 0$ iff $x = y$.

c) $x \equiv y \bmod 1$ for all $x, y \in \mathbb{Z}$.

Therefore the only interesting case is $m \geq 2$.

2.2. Proposition. *The congruence modulo m is an equivalence relation, i.e. the following properties hold:*

i) *(Reflexivity)* $x \equiv x \bmod m$ *for all* $x \in \mathbb{Z}$

ii) *(Symmetry)* $x \equiv y \bmod m \implies y \equiv x \bmod m$.

iii) *(Transitivity)* $(x \equiv y \bmod m) \wedge (y \equiv z \bmod m) \implies x \equiv z \bmod m$.

2.3. Lemma (Division with rest). *Let $x, m \in \mathbb{Z}$, $m \geq 2$. Then there exist uniquely determined integers q, r satisfying*

$$x = qm + r, \quad 0 \leq r < m.$$

Remark. The equation $x = qm + r$ implies that $x \equiv r \bmod m$. Therefore every integer $x \in \mathbb{Z}$ is equivalent modulo m to one and only one element of

$$\{0, 1, \ldots, m-1\}.$$

2.4. Definition. Let m be a positive integer. The set of all equivalence classes of $\mathbb{Z}$ modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$ or briefly by $\mathbb{Z}/m$.

From the above remark we see that

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\},$$

where $\overline{x} = x \bmod m$ is the equivalence class of x modulo m. If there is no danger of confusion, we will often write simply x instead of $\overline{x}$.

Chap. 2 last revised: 2001-10-20

Equivalence modulo m is compatible with addition and multiplication, i.e.

$$x \equiv x' \bmod m \quad \text{and} \quad y \equiv y' \bmod m \implies$$
$$x + y \equiv x' + y' \bmod m \quad \text{and} \quad xy \equiv x'y' \bmod m.$$

Therefore addition and multiplication in $\mathbb{Z}$ induces an addition and multiplication in $\mathbb{Z}/m$ such that $\mathbb{Z}/m$ becomes a commutative ring and the canonical surjection

$$\mathbb{Z} \longrightarrow \mathbb{Z}/m, \quad x \mapsto x \bmod m,$$

is a ring homomorphism.

Example. In $\mathbb{Z}/7$ one has

$$\overline{3} + \overline{4} = \overline{7} = \overline{0}, \quad \overline{3} + \overline{5} = \overline{8} = \overline{1}, \quad \overline{3} \cdot \overline{5} = \overline{15} = \overline{1}.$$

The following are the complete addition and multiplication tables of $\mathbb{Z}/7$.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	2	2
6	0	6	5	4	3	2	1

2.5. Theorem. *Let m be a positive integer. An element $\overline{x} \in \mathbb{Z}/m$ is invertible iff* $\gcd(x, m) = 1$.

Proof. "$\Leftarrow$" Suppose $\gcd(x, m) = 1$. By theorem 1.6 there exist integers ξ, μ such that

$$\xi x + \mu m = 1.$$

This implies $\xi x \equiv 1 \bmod m$, hence $\overline{\xi}$ is an inverse of $\overline{x}$ in $\mathbb{Z}/m$.

"$\Rightarrow$" Suppose that $\overline{x}$ is invertible, i.e. $\overline{x} \cdot \overline{y} = \overline{1}$ for some $\overline{y} \in \mathbb{Z}/m$. Then $xy \equiv 1 \bmod m$, hence there exists an integer k such that $xy - 1 = km$. Therefore $yx - km = 1$, which means by theorem 1.6 that x and m are coprime, q.e.d.

2.6. Corollary. *Let m be a positive integer. The ring $\mathbb{Z}/m$ is a field iff m is a prime.*

Notation. If p is a prime, the field $\mathbb{Z}/p$ is also denoted by $\mathbb{F}_p$.
For any ring A with unit element we denote its multiplicative group of invertible elements by A^*. In particular we use the notations $(\mathbb{Z}/m)^*$ and $\mathbb{F}_p^*$.

Example. For $p = 7$ we have the field $\mathbb{F}_7 = \mathbb{Z}/7$ with 7 elements. From the above multiplication table we can read off the inverses of the elements of $\mathbb{F}_7^* = \mathbb{F}_7 \smallsetminus \{0\}$.

x	1	2	3	4	5	6
x^{-1}	1	4	5	2	3	6

2.7. *Direct Products.* For two rings (resp. groups) A_1 and A_2, the cartesian product $A_1 \times A_2$ becomes a ring (resp. a group) with component-wise defined operations:

$$\begin{aligned}(x_1, x_2) + (y_1, y_2) &:= (x_1 + y_1, x_2 + y_2)\\ (x_1, x_2) \cdot (y_1, y_2) &:= (x_1 y_1, x_2 y_2).\end{aligned}$$

If A_1, A_2 are two rings with unit element, then $(0, 0)$ is the zero element and $(1, 1)$ the unit element of $A_1 \times A_2$. For the group of invertible elements the following equation holds:

$$(A_1 \times A_2)^* = A_1^* \times A_2^*.$$

Note that if A_1 and A_2 are fields, the direct product $A_1 \times A_2$ is a ring, but not a field, since there are zero divisors:

$$(1, 0) \cdot (0, 1) = (0, 0).$$

2.8. Theorem (Chinese remainder theorem). *Let m_1, m_2 be two positive coprime integers. Then the map*

$$\phi : \mathbb{Z}/m_1 m_2 \longrightarrow \mathbb{Z}/m_1 \times \mathbb{Z}/m_2, \quad \overline{x} \mapsto (x \bmod m_1, x \bmod m_2)$$

is an isomorphism of rings.

Proof. It is clear that ϕ is a ring homomorphism. Since $\mathbb{Z}/m_1 m_2$ and $\mathbb{Z}/m_1 \times \mathbb{Z}/m_2$ have the same number of elements (namely $m_1 m_2$), it suffices to prove that ϕ is injective.

Suppose $\phi(\overline{x}) = 0$. This means that $x \equiv 0 \bmod m_1$ and $x \equiv 0 \bmod m_1$, i.e. $m_1 \mid x$ and $m_2 \mid x$. Since m_1 and m_2 are coprime, it follows that $m_1 m_2 \mid x$, hence $\overline{x} = 0$ in $\mathbb{Z}/m_1 m_2$, q.e.d.

Remark. The classical formulation of the Chinese remainder theorem is the following (which is contained in theorem 2.8):

Let m_1, m_2 be two positive coprime integers. Then for every pair a_1, a_2 of integers there exists an integer a such that

$$a \equiv a_i \bmod m_i \quad \text{for } i = 1, 2.$$

This integer a is uniquely determined modulo $m_1 m_2$.

2.9. Definition (Euler phi function). Let m be a positive integer. Then $\varphi(m)$ is defined as the number of integers $k \in \{0, 1, \ldots, m-1\}$ which are coprime to m. Using theorem 2.5, this can also be expressed as

$$\varphi(m) := \#(\mathbb{Z}/m)^*,$$

where $\#S$ denotes the number of elements of a set S.

For small m, the φ-function takes the following values

m	1	2	3	4	5	6	7	8	9	10
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4

It is obvious that for a prime p one has $\varphi(p) = p-1$. More generally, for a prime power p^k it is easy to see that

$$\varphi(p^k) = p^k - p^{k-1} = p^k\Big(1 - \frac{1}{p}\Big).$$

If m and n are coprime, it follows from theorem 2.8 that

$$(\mathbb{Z}/mn)^* \cong (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*,$$

hence $\varphi(mn) = \varphi(n)\varphi(m)$. Using this, we can derive

2.10. Theorem. *For every positive integer n the following formula holds:*

$$\varphi(n) = n\prod_{p|n}\Big(1 - \frac{1}{p}\Big),$$

where the product is extended over all prime divisors p of n.

Proof. Let $n = \prod_{i=1}^r p_i^{e_i}$ be the canonical prime decomposition of n. Then

$$\varphi(n) = \prod_{i=1}^r \varphi(p_i^{e_i}) = \prod_{i=1}^r p_i^{e_i}\Big(1 - \frac{1}{p_i}\Big) = n\prod_{i=1}^r\Big(1 - \frac{1}{p_i}\Big), \qquad \text{q.e.d.}$$

2.11. Theorem (Euler). *Let m be an integer ≥ 2 and a an integer with* $\gcd(a, m) = 1$. *Then*

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Proof. We use some notions and elementary facts from group theory. Let G be a finite group, written multiplicatively, with unit element e. The order of an element $a \in G$ is defined as

$$\operatorname{ord}(a) := \min\{k \in \mathbb{N}_1 : a^k = e\}.$$

The order of the group is defined as the number of its elements,

$$\operatorname{ord}(G) := \#G.$$

Then, as a special case of a theorem of Lagrange, one has

$$\operatorname{ord}(a) \mid \operatorname{ord}(G) \quad \text{for all } a \in G.$$

We apply this to the group $G = (\mathbb{Z}/m)^*$. By definition $\operatorname{ord}((\mathbb{Z}/m)^*) = \varphi(m)$. Let r be the order of $\overline{a} \in (\mathbb{Z}/m)^*$. Then $\varphi(m) = rs$ with an integer s and we have in $(\mathbb{Z}/m)^*$

$$\overline{a}^{\varphi(m)} = \overline{a}^{rs} = (\overline{a}^r)^s = \overline{1}^s = \overline{1}, \quad \text{q.e.d.}$$

2.12. Corollary (Little Theorem of Fermat). *Let p be a prime and a an integer with $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \bmod p.$$

3. Arithmetical Functions. Möbius Inversion Theorem

3.1. Definition. a) An *arithmetical function* is a map

$$f : \mathbb{N}_1 \longrightarrow \mathbb{C}.$$

b) The function f is called *multiplicative* if it is not identically zero and

$$f(nm) = f(n)f(m) \quad \text{for all } n, m \in \mathbb{N}_1 \text{ with } \gcd(n, m) = 1.$$

c) The function f is called *completely multiplicative* or *strictly multiplicative* if it is not identically zero and

$$f(nm) = f(n)f(m) \quad \text{for all } n, m \in \mathbb{N}_1 \text{ (without restriction).}$$

Remark. A multiplicative arithmetical function $a : \mathbb{N}_1 \to \mathbb{C}$ satisfies $a(1) = 1$. This can be seen as follows: Since $\gcd(1, n) = 1$, we have $a(n) = a(1)a(n)$ for all n. Therefore $a(1) \neq 0$, (otherwise a would be identically zero), and $a(1) = a(1)a(1)$ implies $a(1) = 1$.

3.2. Examples

i) The Euler phi function $\varphi : \mathbb{N}_1 \to \mathbb{N}_1 \subset \mathbb{C}$, which was defined in (2.9), is a multiplicative arithmetical function. It is not completely multiplicative, since for a prime p we have

$$\varphi(p^2) = p^2 - p = (p-1)p \;\neq\; \varphi(p)^2 = (p-1)^2.$$

ii) Let $\alpha \in \mathbb{C}$ be an arbitrary complex number. We define a function

$$p_\alpha : \mathbb{N}_1 \longrightarrow \mathbb{C}, \quad n \mapsto p_\alpha(n) := n^\alpha = e^{\alpha \log(n)}.$$

Then p_α is a completely multiplicative arithmetical function.

iii) Let $f : \mathbb{N}_1 \to \mathbb{Z} \subset \mathbb{C}$ be defined by $f(p) := 1$ for primes p and $f(n) = 0$ if n is not prime. This is an example of an arithmetical function which is not multiplicative.

Remark. A multiplicative arithmetical function $f : \mathbb{N}_1 \to \mathbb{C}$ is completely determined by its values at the prime powers: If $n = \prod_{i=1}^r p_i^{e_i}$ is the canonical prime decomposition of n, then

$$f(n) = \prod_{i=1}^r f(p_i^{e_i}).$$

3.3. Divisor function $\tau : \mathbb{N}_1 \to \mathbb{N}_1$. This function is defined by

$$\tau(n) := \text{number of positive divisors of } n.$$

Thus $\tau(p) = 2$ and $\tau(p^k) = 1 + k$ for primes p. (The divisors of p^k are $1, p, p^2, \ldots, p^k$).

The divisor function is multiplicative. This can be seen as follows: Let $m_1, m_2 \in \mathbb{N}_1$ be a pair of coprime numbers and $m := m_1 m_2$. Looking at the prime decompositions one sees that the product $d := d_1 d_2$ of divisors $d_1 \mid m_1$ and $d_2 \mid m_2$ is a divisor of m and conversely every divisor $d \mid m$ can be uniquely decomposed in this way. This can be also expressed by saying that the map

$$\mathrm{Div}(m_1) \times \mathrm{Div}(m_2) \longrightarrow \mathrm{Div}(m_1 m_2), \quad (d_1, d_2) \mapsto d_1 d_2$$

is bijective, where $\mathrm{Div}(n)$ denotes the set of positive divisors of n. This implies immediately the multiplicativity of τ.

3.4. Divisor sum function $\sigma : \mathbb{N}_1 \to \mathbb{N}_1$. This function is defined by

$$\sigma(n) := \text{sum of all positive divisors of } n.$$

Thus for a prime p we have $\sigma(p) = 1 + p$ and

$$\sigma(p^k) = 1 + p + p^2 + \ldots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

The divisor sum function is also multiplicative.
Proof. Let $m_1, m_2 \in N_1$ be coprime numbers. Then

$$\begin{aligned}\sigma(m_1 m_2) &= \sum_{d \mid m_1 m_2} d = \sum_{d_1 \mid m_1, d_2 \mid m_2} d_1 d_2 = \Big(\sum_{d_1 \mid m_1} d_1\Big)\Big(\sum_{d_2 \mid m_2} d_2\Big) \\ &= \sigma(m_1)\sigma(m_2).\end{aligned}$$

3.5. Definition. A *perfect number* (G. *vollkommene Zahl*) is a number $n \in \mathbb{N}_1$ such that $\sigma(n) = 2n$.
The condition $\sigma(n) = 2n$ can also be expressed as

$$\sum_{d \mid n, d < n} d = n,$$

i.e. a number n is perfect if the sum of its proper divisors equals n. The smallest perfect numbers are

$$\begin{aligned} 6 &= 1 + 2 + 3, \\ 28 &= 1 + 2 + 4 + 7 + 14. \end{aligned}$$

The next perfect numbers are 496, 8128. The even perfect numbers are characterized by the following theorem.

Theorem. a) (Euclid) *If q is a prime such that $2^q - 1$ is prime, then $n := 2^{q-1}(2^q - 1)$ is a perfect number.*

b) (Euler) *Conversely, every even perfect number n may be obtained by the construction in* a).

The prove is left as an exercise.

The above examples correspond to $q = 2, 3, 5, 7$. For $q = 11$, $2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime.
It is not known whether there exist odd perfect numbers.

3.6. Möbius function $\mu : \mathbb{N}_1 \to \mathbb{Z}$. This rather strange looking, but important function is defined by

$$\mu(n) := \begin{cases} 1, & \text{for } n = 1, \\ 0, & \text{if there exists a prime } p \text{ with } p^2 \mid n, \\ (-1)^r, & \text{if } n \text{ is a product of } r \text{ different primes.} \end{cases}$$

This leads to the following table

n	1	2	3	4	5	6	7	8	9	10
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1

It follows directly from the definition that μ is multiplicative.

3.7. Definition. Let $f : \mathbb{N}_1 \to \mathbb{C}$ be an arithmetical function. The *summatory function* of f is the function $F : \mathbb{N}_1 \to \mathbb{C}$ defined by

$$F(n) := \sum_{d|n} f(d),$$

where the sum is extended over all positive divisors d of n.

3.8. Examples. i) The divisor sum function

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

is the summatory function of the identity map

$$\iota : \mathbb{N}_1 \longrightarrow \mathbb{N}_1, \quad \iota(n) := n.$$

ii) The divisor function $\tau : \mathbb{N}_1 \to \mathbb{N}_1$ can be written as

$$\tau(n) = \sum_{d|n} 1.$$

Therefore τ is the summatory function of the constant function

$$u : \mathbb{N}_1 \longrightarrow \mathbb{N}_1, \quad u(n) := 1 \text{ for all } n.$$

3.9. Theorem (Summatory function of the Euler phi function). *For all* $n \in N_1$

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

This means that the summatory function of the Euler phi function is the identity map $\iota : \mathbb{N}_1 \to \mathbb{N}_1$.

Proof. The set $M_n := \{1, 2, \ldots, n\}$ is the disjoint union of the sets

$$A_d := \{m \in M_n : \gcd(m, n) = d\}, \quad d \mid n.$$

Therefore $n = \sum_{d|n} \# A_d$. We have $\gcd(m, n) = d$ iff $d \mid m$, $d \mid n$ and $\gcd(m/d, n/d) = 1$. It follows that $\# A_d = \varphi(n/d)$, hence

$$n = \sum_{d|n} \# A_d = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d), \quad \text{q.e.d.}$$

3.10. Theorem (Summatory function of the Möbius function).

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

Therefore the summatory function of the Möbius function is the function

$$\delta_1 : \mathbb{N}_1 \longrightarrow \mathbb{Z}, \quad \delta_1(n) := \begin{cases} 1 & \text{for } n = 1, \\ 0 & \text{for all } n > 1. \end{cases}$$

Proof. The case $n = 1$ is trival.
Now suppose $n \geq 2$ and let $n = \prod_{j=1}^{r} p_j^{e_j}$ be the canonical prime factorization of n. For $0 \leq s \leq r$ we denote by D_s the set of all divisors $d \mid n$ which are the product of s different primes $\in \{p_1, \ldots, p_r\}$, ($D_0 = \{1\}$). For all $d \in D_s$ we have $\mu(d) = (-1)^s$; but $\mu(d) = 0$ for all divisors of n that do not belong to any of the D_s. Therefore

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{s=0}^{r} \sum_{d \in D_s} \mu(d) = \sum_{s=0}^{r} (-1)^s \# D_s = \sum_{s=0}^{r} (-1)^s \binom{r}{s} \\ &= (1 + (-1))^r = 0, \end{aligned}$$

where we have used the binomial theorem. This proves our theorem.

3.11. Definition (Dirichlet product). For two arithmetical functions $f, g : \mathbb{N}_1 \to \mathbb{C}$ one defines their Dirichlet product (or Dirichlet convolution) $f * g : \mathbb{N}_1 \to \mathbb{C}$ by

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

This can be written in a symmetric way as

$$(f * g)(n) = \sum_{k\ell=n} f(k)g(\ell),$$

where the sum extends over all pairs $k, \ell \in \mathbb{N}_1$ with $k\ell = n$. This shows that $f*g = g*f$ and $(f * g)(n) = \sum_{d|n} f(n/d)g(d)$.

Example. $(f * g)(6) = f(1)g(6) + f(2)g(3) + f(3)g(2) + f(6)g(1)$.

Remark. Let f be an arbitrary arithmetical function and u the constant function $u(n) = 1$ for all $n \in \mathbb{N}_1$. Then

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

Thus the summatory function of an arithmetical function f is nothing else than the Dirichlet product $u * f$.

3.12. Theorem. *If the arithmetical functions $f, g : \mathbb{N}_1 \to \mathbb{C}$ are multiplicative, their Dirichlet product $f * g$ is again multiplicative.*

Example. Since the constant function $u(n) = 1$ is clearly multiplicative, the summatory function of every multiplicative arithmetical function is multiplicative.

Proof. Let $m_1, m_2 \in \mathbb{N}_1$ be two coprime numbers. Then

$$\begin{aligned}
(f * g)(m_1 m_2) &= \sum_{d|m_1 m_2} f(d)g\Big(\frac{m_1 m_2}{d}\Big) = \sum_{d_1|m_1, d_2|m_2} f(d_1 d_2)g\Big(\frac{m_1 m_2}{d_1 d_2}\Big) \\
&= \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1)f(d_2)g\Big(\frac{m_1}{d_1}\Big)g\Big(\frac{m_2}{d_2}\Big) \\
&= \sum_{d_1|m_1} f(d_1)g\Big(\frac{m_1}{d_1}\Big) \sum_{d_2|m_2} f(d_2)g\Big(\frac{m_2}{d_2}\Big) \\
&= (f * g)(m_1)(f * g)(m_2), \quad \text{q.e.d.}
\end{aligned}$$

3.13. Theorem. *The set $\mathcal{F}(\mathbb{N}_1, \mathbb{C})$ of all arithmetical functions $f : \mathbb{N}_1 \to \mathbb{C}$ is a commutative ring with unit element when addition is defined by*

$$(f + g)(n) := f(n) + g(n) \quad \textit{for all } n \in \mathbb{N}_1$$

and multiplication is the Dirichlet product. The unit element is the function $\delta_1 : \mathbb{N}_1 \to \mathbb{C}$ defined by

$$\delta_1(1) := 1, \quad \delta_1(n) = 0 \quad \textit{for all } n > 1.$$

Remark. The notation δ_1 is motivated by the Kronecker δ-symbol

$$\delta_{ij} = \begin{cases} 1 & \text{for } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Using this, one can write $\delta_1(n) = \delta_{1n}$.

Proof. That δ_1 is the unit element is seen as follows

$$(\delta_1 * f)(n) = \sum_{d|n} \delta_1(d) f\Big(\frac{n}{d}\Big) = \delta_1(1) f\Big(\frac{n}{1}\Big) = f(n).$$

All ring axioms with exception of the associative law for multiplication are easily verified. Proof of associativity:

$$\begin{aligned} ((f * g) * h)(n) &= \sum_{\substack{k,\ell \\ k\ell = n}} (f * g)(k) h(\ell) = \sum_{\substack{k,\ell \\ k\ell = n}} \sum_{\substack{i,j \\ ij = k}} f(i) g(j) h(\ell) \\ &= \sum_{\substack{i,j,\ell \\ ij\ell = n}} f(i) g(j) h(\ell) = \sum_{\substack{i,m \\ im = n}} \sum_{\substack{j,\ell \\ j\ell = m}} f(i) g(j) h(\ell) \\ &= \sum_{\substack{i,m \\ im = n}} f(i) (g * h)(m) = (f * (g * h))(n), \quad \text{q.e.d.} \end{aligned}$$

3.14. Theorem (Möbius inversion formula). *Let $f : \mathbb{N}_1 \to \mathbb{C}$ be an arithmetical function and $F : \mathbb{N}_1 \to \mathbb{C}$ its summatory function,*

$$F(n) = \sum_{d|n} f(d) \quad \text{for all } n \in \mathbb{N}_1. \tag{$*$}$$

Then f can be reconstructed from F by the formula

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) F(d) \quad \text{for all } n \in \mathbb{N}_1. \tag{$**$}$$

Conversely, $(**)$ implies $(*)$.

Proof. The formula $(*)$ can be written as

$$F = u * f,$$

where u is the constant function $u(n) = 1$ for all n. Theorem 3.10 says that u is the Dirichlet inverse of the Möbius function:

$$u * \mu = \mu * u = \delta_1.$$

Therefore

$$\mu * F = \mu * (u * f) = (\mu * u) * f = \delta_1 * f = f,$$

which is formula $(**)$. Conversely, from $f = \mu * F$ one obtains

$$u * f = u * (\mu * F) = (u * \mu) * F = \delta_1 * F = F,$$

that is formula $(*)$, q.e.d.

3.15. Examples. i) Applying the Möbius inversion formula to the summatory function of the Euler phi function (theorem 3.9)

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

yields $\varphi = \mu * \iota$, i.e.

$$\varphi(n) = \sum_{d|n} \mu(d)\, \iota\Big(\frac{n}{d}\Big) = \sum_{d|n} \frac{n}{d}\, \mu(d).$$

This can also be written as

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

ii) Example 3.8.i) says $u * \iota = \sigma$ which implies $\iota = \mu * \sigma$, i.e.

$$\sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, \sigma(d) = n.$$

iii) Example 3.8.ii) says $u * u = \tau$, hence $u = \mu * \tau$, i.e.

$$\sum_{d|n} \mu\Big(\frac{n}{d}\Big)\, \tau(d) = 1 \quad \text{for all } n \geq 1.$$

We now state a second Möbius inversion formula for functions defined on the real interval

$$I_1 := \{x \in \mathbb{R} : x \geq 1\}.$$

3.16. Theorem. *For a function $f : I_1 \to \mathbb{C}$ define $F : I_1 \to \mathbb{C}$ by*

$$F(x) = \sum_{k \leqslant x} f\Big(\frac{x}{k}\Big) \quad \text{for all } x \geq 1, \tag{$\diamond$}$$

where the sum extends over all positive integers $k \leq x$. Then

$$f(x) = \sum_{k \leqslant x} \mu(k) F\Big(\frac{x}{k}\Big) \quad \text{for all } x \geq 1. \tag{$\diamond\diamond$}$$

Conversely, $(\diamond\diamond)$ implies $(\diamond)$.

Example. If f is the constant function $f(x) = 1$ for all $x \geq 1$, then $F(x) = \lfloor x \rfloor =$ greatest integer $\leq x$. The theorem implies the remarkable formula

$$\sum_{k \leqslant x} \mu(k) \left\lfloor \frac{x}{k} \right\rfloor = 1 \quad \text{for all } x \geq 1.$$

E.g. for $x = 5$ this reads

$$5\mu(1) + 2\mu(2) + \mu(3) + \mu(4) + \mu(5) = 1.$$

To prove theorem 3.16, we put it first into an abstract context.

3.17. Let $\mathcal{F}(I_1, \mathbb{C})$ denote the vector space of all functions $f : I_1 = [1, \infty[\to \mathbb{C}$. We define an operation of the ring of all arithmetical functions on this vector space

$$\mathcal{F}(\mathbb{N}_1, \mathbb{C}) \times \mathcal{F}(I_1, \mathbb{C}) \longrightarrow \mathcal{F}(I_1, \mathbb{C}), \quad (\alpha, f) \mapsto \alpha \triangleright f,$$

where

$$(\alpha \triangleright f)(x) := \sum_{k \leqslant x} \alpha(k) f\Big(\frac{x}{k}\Big).$$

3.18. Theorem. *With the above operation, $\mathcal{F}(I_1, \mathbb{C})$ becomes a module over the ring $\mathcal{F}(\mathbb{N}_1, \mathbb{C})$.*

Proof. It is clear that $\mathcal{F}(I_1, \mathbb{C})$ is an abelian group with respect to pointwise addition $(f+g)(x) = f(x)+g(x)$. So it remains to verify the following laws (for $\alpha, \beta \in \mathcal{F}(\mathbb{N}_1, \mathbb{C})$ and $f, g \in \mathcal{F}(I_1, \mathbb{C})$).

i) $\alpha \triangleright (f + g) = \alpha \triangleright f + \alpha \triangleright g$,

ii) $(\alpha + \beta) \triangleright f = \alpha \triangleright f + \beta \triangleright f$,

iii) $\alpha \triangleright (\beta \triangleright f) = (\alpha * \beta) \triangleright f$,

iv) $\delta_1 \triangleright f = f$.

The assertions i) and ii) are trivial. The associative law iii) can be seen as follows

$$\begin{aligned}
(\alpha \triangleright (\beta \triangleright f))(x) &= \sum_{k \leqslant x} \alpha(k)(\beta \triangleright f)\Big(\frac{x}{k}\Big) = \sum_{k \leqslant x} \alpha(k) \sum_{\ell \leqslant x/k} \beta(\ell) f\Big(\frac{x}{k\ell}\Big) \\
&= \sum_{k\ell \leqslant x} \alpha(k)\beta(\ell) f\Big(\frac{x}{k\ell}\Big) \\
&= \sum_{n \leqslant x} \sum_{k\ell = n} \alpha(k)\beta(\ell) f\Big(\frac{x}{n}\Big) \\
&= \sum_{n \leqslant x} (\alpha * \beta)(n) f\Big(\frac{x}{n}\Big) = ((\alpha * \beta) \triangleright f)(x).
\end{aligned}$$

Proof of iv):

$$(\delta_1 \triangleright f)(x) = \sum_{k \leqslant x} \delta_1(k) f\left(\frac{x}{k}\right) = \delta_1(1) f\left(\frac{x}{1}\right) = f(x), \quad \text{q.e.d.}$$

3.19. Now we take up the proof of theorem 3.16. Equation ($\diamond$) can be written as

$$F = u \triangleright f$$

with the constant function $u(n) = 1$. Multiplying this equation by the Möbius function yields

$$\mu \triangleright F = \mu \triangleright (u \triangleright F) = (\mu * u) \triangleright f = \delta_1 \triangleright f = f,$$

which is equation ($\diamond\diamond$). Conversly, from $f = \mu \triangleright F$ it follows

$$u \triangleright f = u \triangleright (\mu \triangleright F) = (u * \mu) \triangleright F = \delta_1 \triangleright F = F,$$

which is equation ($\diamond$), q.e.d.

4. Riemann Zeta Function. Euler Product

4.1. Definition. For a complex $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, the Riemann zeta function is defined by the series

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

Let us first study the convergence of this infinite series. Following an old tradition, we denote the real and imaginary part of s by σ resp. t, i.e.

$$s = \sigma + it, \quad \sigma, t \in \mathbb{R}.$$

We have

$$\frac{1}{n^s} = n^{-s} = e^{-s\log n} = e^{-\sigma\log(n) - it\log n} = \frac{1}{n^\sigma} e^{-it\log n},$$

therefore

$$\left|\frac{1}{n^s}\right| = \frac{1}{n^\sigma}.$$

Since $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^\sigma}$ converges for all real $\sigma > 1$, we see that the zeta series converges absolutely and uniformly in every halfplane $\overline{H(\sigma_0)}$, $\sigma_0 > 1$, where

$$H(\sigma_0) := \{s \in \mathbb{C} : \mathrm{Re}(s) > \sigma_0\}.$$

It follows by a theorem of Weierstrass that ζ is a holomorphic (= regular analytic) function in the halfplane

$$H(1) = \{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}.$$

We will see later that ζ can be continued analytically to a meromorphic function in the whole complex plane $\mathbb{C}$, which is holomorphic in $\mathbb{C} \setminus \{1\}$ and has a pole of first order at $s = 1$. A weaker statement is

4.2. Proposition. $\displaystyle\lim_{\sigma \searrow 1} \zeta(\sigma) = \infty.$

Proof. Let $R > 0$ be any given bound. Since $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$, there exists an $N > 1$ such that

$$\sum_{n=1}^{N} \frac{1}{n} \geq R + 1.$$

Chap. 4 last revised: 2003-04-14

The function $\sigma \mapsto \sum_{n=1}^{N} \frac{1}{n^\sigma}$ is continuous on $\mathbb{R}$, hence there exists an $\varepsilon > 0$ such that

$$\sum_{n=1}^{N} \frac{1}{n^\sigma} \geq R \quad \text{for all } \sigma \text{ with } \sigma < 1 + \varepsilon.$$

A fortiori we have $\sum_{n=1}^{\infty} \frac{1}{n^\sigma} \geq R$ for all $1 < \sigma < 1 + \varepsilon$. This proves the proposition.

4.3. Theorem (Euler product). *For all* $s \in \mathbb{C}$ *with* $\mathrm{Re}(s) > 1$ *one has*

$$\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}},$$

where the product is extended over the set $\mathbb{P}$ *of all primes.*

Proof. Since $|p^{-s}| < 1/p \leq 1/2$, we can use the geometric series

$$\frac{1}{1 - p^{-s}} = \sum_{k=0}^{\infty} \frac{1}{p^{ks}},$$

which converges absolutely. If $\mathcal{P} \subset \mathbb{P}$ is any finite set of primes, the product

$$\prod_{p \in \mathcal{P}} \Big(\sum_{k=0}^{\infty} \frac{1}{p^{ks}} \Big) = \prod_{p \in \mathcal{P}} \Big(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots \Big)$$

can be calculated by termwise multiplication and we obtain

$$\prod_{p \in \mathcal{P}} \Big(\sum_{k=0}^{\infty} \frac{1}{p^{ks}} \Big) = \sum_{n \in \mathbb{N}(\mathcal{P})} \frac{1}{n^s},$$

where $\mathbb{N}(\mathcal{P})$ is the set of all positive integers n whose prime decomposition contains only primes from the set $\mathcal{P}$. (Here the unique prime factorization is used.) Letting $\mathcal{P} = \mathcal{P}_m$ be set of all primes $\leq m$ and passing to the limit $m \to \infty$, we obtain the assertion of the theorem.

Remark. The Euler product can be used to give another proof of the infinitude of primes. If the set $\mathbb{P}$ of all primes were finite, the Euler product $\prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1}$ would be continuous at $s = 1$, which contradicts the fact that $\lim_{\sigma \searrow 1} \zeta(\sigma) = \infty$.

4.4. We recall some facts from the theory of analytic functions of a complex variable about infinite products. Let $G \subset \mathbb{C}$ be an open set. For a continuous function $f : G \to \mathbb{C}$ and a compact subset $K \subset G$ we define the maximum norm

$$\|f\|_K := \sup\{|f(z)| : z \in K\} \in \mathbb{R}_+.$$

(The supremum is $< \infty$ since f is continous.) Let now $f_\nu : G \to \mathbb{C}$, $\nu \geq 1$, be a sequence of holomorphic functions. The infinite product

$$F(z) := \prod_{\nu=1}^{\infty} (1 + f_\nu(z))$$

is said to be *normally convergent* on a compact subset $K \subset G$, if

$$\sum_{\nu=1}^{\infty} \|f_\nu\|_K < \infty.$$

In this case, the product converges absolutely and uniformly on K. (The converse is not true, as can be seen by taking the constant functions $f_\nu = -\frac{1}{2}$ for all ν.) The product is said to be normally convergent in G if it converges normally on any compact subset of $K \subset G$. The limit F of a normally convergent infinite product of holomorphic functions $1 + f_\nu$ is again holomorphic and $F(z_0) = 0$ for a particular point $z_0 \in G$ if and only if one of the factors vanishes in z_0.

4.5. Theorem. *The Riemann zeta function has no zeroes in the half plane*

$$H(1) = \{s \in \mathbb{C} : \operatorname{Re}(s) > 1\}.$$

For its inverse one has

$$\frac{1}{\zeta(s)} = \prod_{p \in \mathbb{P}} \Big(1 - \frac{1}{p^s}\Big) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

where μ is the Möbius function.

Proof. The first assertion follows from the fact that the Euler product for the zeta function converges normally in $H(1)$ and all factors $(1 - p^{-s})^{-1}$ have no zeroes in $H(1)$. Inverting the product representation for $1/\zeta(s)$ yields $1/\zeta(s) = \prod(1 - p^{-s})$. To prove the last equation, let $\mathcal{P}$ a finite set of primes and $\mathbb{N}'(\mathcal{P})$ the set of all positive integers n that can be written as a product $n = p_1 p_2 \cdot \ldots \cdot p_r$ of distinct primes $p_j \in \mathcal{P}$, $(r \geq 0)$. Then, since $(-1)^r = \mu(p_1 \cdot \ldots \cdot p_r)$,

$$\prod_{p \in \mathcal{P}} \Big(1 - \frac{1}{p^s}\Big) = \sum_{n \in \mathbb{N}'(\mathcal{P})} \frac{\mu(n)}{n^s}.$$

Letting $\mathcal{P} = \mathcal{P}_m$ be set of all primes $\leq m$ and passing to the limit $m \to \infty$, we obtain the assertion of the theorem. Note that $\mu(n) = 0$ for all $n \in \mathbb{N}_1 \smallsetminus \bigcup_m \mathbb{N}'(\mathcal{P}_m)$.

4.6. We recall now some facts about the logarithm function. (By logarithm we always mean the natural logarithm with basis $e = 2.718\ldots$.) We have the Taylor expansion

$$\log(1 + z) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{z^n}{n} \quad \text{for all } z \in \mathbb{C} \text{ with } |z| < 1.$$

From this follows

$$\log\Big(\frac{1}{1-z}\Big) = \sum_{n=1}^{\infty} \frac{z^n}{n} \quad \text{for all } z \in \mathbb{C} \text{ with } |z| < 1.$$

(Of course here the principal branch of the logarithm with $\log(1) = 0$ is understood.)

If $f : G \to \mathbb{C}$ is a holomorphic function without zeroes in a simply connected domain $G \subset \mathbb{C}$, then there exists a holomorphic branch of the logarithm of f, i.e. a holomorphic function

$$\log f : G \to \mathbb{C} \quad \text{with} \quad e^{(\log f)(z)} = f(z) \text{ for all } z \in G.$$

This function $\log f$ is uniquely determined up to an additive constant $2\pi i n$, $n \in \mathbb{Z}$.

Since the zeta function has no zeroes in the simply connected halfplane $H(1)$, we can form the logarithm of the zeta function, where we select the branch of $\log \zeta$ that takes real values on the real half line $]1, \infty[$.

4.7. Theorem. *For the logarithm of the zeta function in the halfplane $H(1)$, the following equation holds:*

$$\log \zeta(s) = \sum_{p \in \mathbb{P}} \frac{1}{p^s} + \sum_{k=2}^{\infty} \frac{1}{k} \sum_{p \in \mathbb{P}} \frac{1}{p^{ks}}.$$

The function

$$F(s) := \sum_{k=2}^{\infty} \frac{1}{k} \sum_{p \in \mathbb{P}} \frac{1}{p^{ks}}$$

is bounded in $H(1)$.

Remark. If one defines the *prime zeta function* by

$$P(s) := \sum_{p \in \mathbb{P}} \frac{1}{p^s} \quad \text{for } s \in H(1),$$

the formula of the theorem may be written as

$$\log \zeta(s) = \sum_{k=1}^{\infty} \frac{P(ks)}{k} = P(s) + F(s), \quad \text{where} \quad F(s) = \sum_{k=2}^{\infty} \frac{P(ks)}{k}.$$

Proof. Using the Euler product we obtain

$$\begin{aligned} \log \zeta(s) &= \sum_{p \in \mathbb{P}} \log\Big(\frac{1}{1-p^{-s}}\Big) = \sum_{p \in \mathbb{P}} \sum_{k=1}^{\infty} \frac{1}{kp^{ks}} = \sum_{k=1}^{\infty} \sum_{p \in \mathbb{P}} \frac{1}{kp^{ks}} \\ &= \sum_{p \in \mathbb{P}} \frac{1}{p^s} + \sum_{k=2}^{\infty} \frac{1}{k} \sum_{p \in \mathbb{P}} \frac{1}{p^{ks}}. \end{aligned}$$

To prove the boundedness of

$$F(s) = \sum_{k=2}^{\infty} \frac{1}{k} \sum_{p\in\mathbb{P}} \frac{1}{p^{ks}} = \sum_{k=2}^{\infty} \frac{P(ks)}{k}$$

in $H(1)$, we use the estimate (with $\sigma = \mathrm{Re}(s) > 1$)

$$\begin{aligned} |P(ks)| \, &\leq \, P(k\sigma) \leq P(k) = \sum_{p\in\mathbb{P}} \frac{1}{p^k} \leq \sum_{n=2}^{\infty} \frac{1}{n^k} \\ &\leq \sum_{n=2}^{\infty} \int_{n-1}^{n} \frac{dx}{x^k} = \int_{1}^{\infty} \frac{dx}{x^k} = \frac{1}{k-1} \end{aligned}$$

and obtain for all $s \in H(1)$

$$|F(s)| \leq \sum_{k=2}^{\infty} \frac{1}{k(k-1)} = 1, \quad \text{q.e.d.}$$

4.8. Corollary (Euler).

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots = \infty.$$

Proof. Since the difference $|P(s) - \log\zeta(s)|$ is bounded for $\mathrm{Re}(s) > 1$ we get, using proposition 4.2,

$$\lim_{\sigma\searrow 1} P(\sigma) = \lim_{\sigma\searrow 1} \Big(\sum_{p\in\mathbb{P}} \frac{1}{p^\sigma} \Big) = \infty.$$

This implies the assertion.

Remark. The corollary gives another proof that there are infinitely many primes, but says more. Comparing with

$$\sum_{n=1}^{\infty} \frac{1}{n^2} < \infty,$$

we can conclude that the density of primes is in some sense greater than the density of square numbers.

The following theorem is a variant of theorem 4.7 and gives an interesting formula for the difference between $P(s)$ and $\log\zeta(s)$.

4.9. Theorem. *We have the following representation of the prime zeta function for* $\mathrm{Re}(s) > 1$

$$P(s) = \sum_{p\in\mathbb{P}} \frac{1}{p^s} = \log\zeta(s) + \sum_{k=2}^{\infty} \frac{\mu(k)}{k} \log\zeta(ks).$$

Proof. We start from the formula of theorem 4.7

$$\log\zeta(s) = \sum_{k=1}^{\infty}\frac{P(ks)}{k}.$$

We have as in the proof of theorem 4.7 the estimate

$$|P(ks)| \le P(k\sigma) \le \frac{1}{k\sigma - 1} \le \frac{2}{k\sigma}, \qquad \text{(where } \sigma = \mathrm{Re}(s)),$$

which implies

$$|\log\zeta(s)| \le \sum_{k=1}^{\infty}\frac{2}{k^2\sigma} = \frac{2}{\sigma}\sum_{k=1}^{\infty}\frac{1}{k^2} = \frac{2\zeta(2)}{\sigma} =: \frac{c}{\sigma}$$

with the constant $c = 2\zeta(2)$. Therefore the series $\sum_{k=1}^{\infty}(\mu(k)/k)\log\zeta(ks)$ converges absolutely:

$$\sum_{k=1}^{\infty}\left|\frac{\mu(k)}{k}\log\zeta(ks)\right| \le \sum_{k=1}^{\infty}\frac{1}{k}\cdot\frac{c}{k\sigma} = \frac{c\zeta(2)}{\sigma} < \infty.$$

Substituting $\log\zeta(ks) = \sum_{\ell=1}^{\infty}P(k\ell s)/\ell$ we get

$$\begin{aligned}
\sum_{k=1}^{\infty}\frac{\mu(k)}{k}\log\zeta(ks) &= \sum_{k,\ell=1}^{\infty}\frac{\mu(k)P(k\ell s)}{k\ell} = \sum_{n=1}^{\infty}\sum_{k\ell=n}\mu(k)\frac{P(k\ell s)}{k\ell}\\
&= \sum_{n=1}^{\infty}\sum_{k|n}\mu(k)\frac{P(ns)}{n} = \sum_{n=1}^{\infty}\delta_1(n)\frac{P(ns)}{n}\\
&= P(s), \qquad \text{q.e.d.}
\end{aligned}$$

We conclude this chapter with an interesting application of therem 4.5.

4.10. Theorem. *The probability that two random numbers $m, n \in \mathbb{N}_1$ are coprime is $6/\pi^2 \approx 61\%$, more precisely: For real $x \ge 1$ let*

$$\mathrm{Copr}(x) := \{(m,n) \in \mathbb{N}_1 \times \mathbb{N}_1 : m, n \le x \text{ and } m, n \text{ coprime}\}.$$

Then

$$\lim_{x\to\infty}\frac{\#\mathrm{Copr}(x)}{x^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Proof. Let $A(x)$ be the set of all pairs m, n of integers with $1 \le m, n \le x$ and

$$A_k(x) := \{(n,m) \in A(x) : \gcd(m,n) = k\}.$$

Then $A(x)$ is the disjoint union of all $A_k(x)$, $k = 1, 2, \ldots, \lfloor x \rfloor$, and for every k we have a bijection

$$\mathrm{Copr}\Big(\frac{x}{k}\Big) \longrightarrow A_k(x), \quad (m, n) \mapsto (km, kn).$$

Therefore

$$\sum_{k \leqslant x} \#\mathrm{Copr}\Big(\frac{x}{k}\Big) = \lfloor x \rfloor^2.$$

Now we can apply the inversion formula of theorem 3.16 and obtain

$$\#\mathrm{Copr}(x) = \sum_{k \leqslant x} \mu(k) \Big\lfloor \frac{x}{k} \Big\rfloor^2.$$

Since $0 \le (x/k) - \lfloor x/k \rfloor < 1$, it follows that $(x/k)^2 - \lfloor x/k \rfloor^2 < 2x/k$, hence

$$\bigg| \#\mathrm{Copr}(x) - \sum_{k \leqslant x} \mu(k) \Big(\frac{x}{k}\Big)^2 \bigg| \le 2x \sum_{k \leqslant x} \frac{1}{k} \le 2x(1 + \log x) = O(x \log x),$$

so we can write

$$\frac{\#\mathrm{Copr}(x)}{x^2} = \sum_{k \leqslant x} \frac{\mu(k)}{k^2} + O\Big(\frac{\log x}{x}\Big).$$

On the other hand $\sum_{k=1}^{\infty} \mu(k)/k^2 = 1/\zeta(2)$ by theorem 4.5, hence

$$\bigg| \sum_{k \leqslant x} \frac{\mu(k)}{k^2} - \frac{1}{\zeta(2)} \bigg| \le \sum_{k > x} \frac{1}{k^2} = O\Big(\frac{1}{x}\Big).$$

Combining this with the previous estimate yields

$$\frac{\#\mathrm{Copr}(x)}{x^2} = \frac{1}{\zeta(2)} + O\Big(\frac{\log x}{x}\Big),$$

which implies the assertion of the theorem.

Remark. The fact $\zeta(2) = \dfrac{\pi^2}{6}$ will be proven in the next chapter.

5. The Euler-Maclaurin Summation Formula

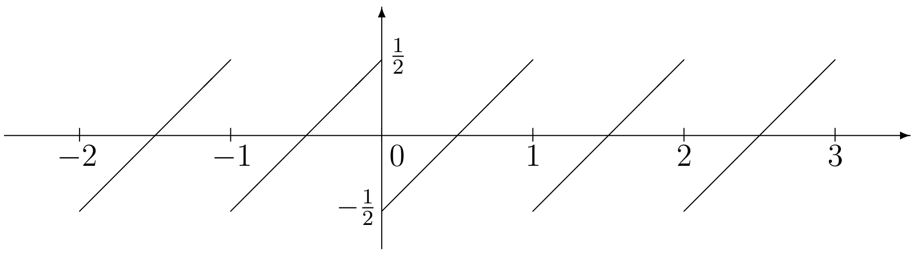
5.1. We define a periodic function

$$\mathrm{saw} : \mathbb{R} \longrightarrow \mathbb{R}$$

with period 1 by

$$\mathrm{saw}(x) := x - \lfloor x \rfloor - \tfrac{1}{2}$$

This is a kind of sawtooth function, see figure.



With this function, we can state a first form of the Euler-Maclaurin summation formula. This formula shows how a sum can be approximated by an integral and gives an exact error term.

5.2. Theorem (Euler-Maclaurin I). *Let x_0 be a real number and $f : [x_0, \infty[\; \to \mathbb{C}$ a continuously differentiable function. Then we have for all integers $n \geq m \geq x_0$*

$$\sum_{k=m}^{n} f(k) = \tfrac{1}{2}(f(m) + f(n)) + \int_m^n f(x)dx + \int_m^n \mathrm{saw}(x) f'(x)dx.$$

Proof. We have

$$\sum_{k=m}^{n} f(k) - \tfrac{1}{2}(f(m) + f(n)) = \sum_{k=m}^{n-1} \tfrac{1}{2}(f(k) + f(k+1)).$$

On the other hand we get by partial integration

$$\begin{aligned}
\int_k^{k+1} \mathrm{saw}(x) f'(x)dx &= \int_k^{k+1} (x - k - \tfrac{1}{2}) f'(x)dx \\
&= (x - k - \tfrac{1}{2}) f(x)\Big|_k^{k+1} - \int_k^{k+1} f(x)dx \\
&= \tfrac{1}{2}(f(k+1) + f(k)) - \int_k^{k+1} f(x)dx.
\end{aligned}$$

Summing up from $k = m$ to $n - 1$ yields the assertion of the theorem.

Using this theorem, we can construct an analytic continuation of the zeta function.

5.3. Theorem. *The Riemann zeta function can be analytically continued to a meromorphic function in the halfplane* $H(0) = \{s \in \mathbb{C} : \mathrm{Re}(s) > 0\}$ *with a single pole of order 1 at* $s = 1$*. The continued function can be represented in* $H(0)$ *as*

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

Proof. Applying theorem 5.2 to the function $f(x) = 1/x^s$ we get

$$\sum_{n=1}^{N} \frac{1}{n^s} = \tfrac{1}{2}\Big(1 + \frac{1}{N^s}\Big) + \int_1^N \frac{dx}{x^s} - s\int_1^N \frac{\mathrm{saw}(x)}{x^{s+1}} dx.$$

For $\mathrm{Re}(s) > 1$ we have $\lim\limits_{N\to\infty} 1/N^s = 0$ and

$$\lim_{N\to\infty} \int_1^N \frac{dx}{x^s} = \lim_{N\to\infty} \frac{1}{1-s}\Big(\frac{1}{N^{s-1}} - 1\Big) = \frac{1}{s-1}.$$

Therefore we can pass to the limit $N \to \infty$ in the formula above and get for $\mathrm{Re}(s) > 1$

$$\zeta(s) = \frac{1}{2} + \frac{1}{s-1} - s\int_1^\infty \frac{\mathrm{saw}(x)}{x^{s+1}} dx. \tag{$*$}$$

We will now show that the integral

$$F(s) := \int_1^\infty \frac{\mathrm{saw}(x)}{x^{s+1}}\, dx$$

exists for all $s \in \mathbb{C}$ with $\sigma := \mathrm{Re}(s) > 0$ and represents a holomorphic function in the halfplane $H(0)$. This will then complete the proof of the theorem, since the right hand side of the formula $(*)$ defines a meromorphic continuation of the zeta function to $H(0)$ with a single pole at $s = 1$.

The existence of the integral follows from the estimate

$$\Big|\frac{\mathrm{saw}(x)}{x^{s+1}}\Big| \le \frac{1}{2} \cdot \frac{1}{x^{\sigma+1}},$$

since $\int_1^\infty (1/x^{\sigma+1})\, dx < \infty$ for $\sigma > 0$. To prove the holomorphy of F it suffices by the theorem of Morera to show that for all compact rectangles $R \subset H(0)$

$$\int_{\partial R} F(s) ds = 0.$$

This can be seen as follows: Since $\partial R \subset H(0)$ is compact, there exist a $\sigma_0 > 0$ such that $\mathrm{Re}(s) \ge \sigma_0$ for all $s \in \partial R$. Therefore we have on $\partial R \times [1, \infty[$ the majorization

$$\Big|\frac{\mathrm{saw}(x)}{x^{s+1}}\Big| \le \frac{1}{2} \cdot \frac{1}{x^{\sigma_0+1}}$$

and we can apply the theorem of Fubini

$$\int_{\partial R} F(s)\,ds = \int_{\partial R}\int_1^\infty \frac{\mathrm{saw}(x)}{x^{s+1}}\,dx\,ds$$
$$= \int_1^\infty \mathrm{saw}(x)\underbrace{\Big(\int_{\partial R}\frac{1}{x^{s+1}}\,ds\Big)}_{=0}\,dx = 0, \quad \text{q.e.d.}$$

There exists also a proof of the holomorphy of F without recourse to Lebesgue integration theory: We write

$$F(s) = \int_1^\infty \frac{\mathrm{saw}(x)}{x^{s+1}}\,dx = \sum_{n=1}^\infty \int_n^{n+1}\frac{\mathrm{saw}(x)}{x^{s+1}}\,dx = \sum_{n=1}^\infty f_n(s)$$

with

$$f_n(s) = \int_n^{n+1}\frac{\mathrm{saw}(x)}{x^{s+1}}\,dx = \int_n^{n+1}\frac{x-n-\frac{1}{2}}{x^{s+1}}\,dx.$$

The function f_n is holomorphic in $\mathbb{C}$ (it is easily checked directly that $g(z) = \int_a^b t^z\,dt$ is holomorphic in the whole z-plane) and satisfies an estimate

$$|f_n(s)| \le \frac{1}{2n^{\sigma_0+1}} \quad \text{for all } s \in \overline{H(\sigma_0)}$$

Since $\sum_{n=1}^\infty 1/n^{\sigma_0+1} < \infty$ for all $\sigma_0 > 0$, the series $F = \sum_{n=1}^\infty f_n$ converges uniformly on every compact subset of $H(0)$. By a theorem of Weierstraß, the limit function F is holomorphic in $H(0)$.

5.4. Definition. The *Euler-Mascheroni* constant is defined as the limit

$$C := \lim_{N\to\infty}\Big(\sum_{n=1}^N \frac{1}{n} - \log N\Big).$$

The existence of this limit can be proved using the Euler-Maclaurin summation formula (5.2). This is left to the reader as an exercise.

5.5. Theorem. *There exist uniquely determined functions*

$$\beta_k : \mathbb{R} \longrightarrow \mathbb{R}, \quad k \in \mathbb{N}_1,$$

with the following properties:

i) All functions β_k are periodic with period 1, i.e. $\beta_k(x+n) = \beta_k(x)$ for all $n \in \mathbb{Z}$, and the functions β_k with $k \ge 2$ are continuous.

ii) $\beta_1 = \mathrm{saw}$.

iii) β_k is differentiable in $]0,1[$ and

$$\beta_k'(x) = \beta_{k-1}(x) \quad \text{for all } 0 < x < 1 \text{ and } k \geq 2.$$

iv) $\displaystyle\int_0^1 \beta_k(x)dx = 0$ for all $k \geq 1$

Proof. By condition iii), the function β_k is uniquely determined in the intervall $]0,1[$ by β_{k-1} up to an additive constant. This constant is uniquely determined by condition iv). Thus by ii)-iv), all β_k are uniquely determined in $]0,1[$, and by periodicity even in $\mathbb{R} \setminus \mathbb{Z}$. It remains to be shown that the definition of β_k, $k \geq 2$ can be extended continuously across the integer points. This is equivalent with

$$\lim_{\varepsilon \searrow 0} \beta_k(\varepsilon) = \lim_{\varepsilon \searrow 0} \beta_k(1-\varepsilon).$$

For $k \geq 2$ one has

$$\beta_k(1-\varepsilon) - \beta_k(\varepsilon) = \int_\varepsilon^{1-\varepsilon} \beta_{k-1}'(x)dx,$$

hence by iv)

$$\lim_{\varepsilon \searrow 0} (\beta_k(1-\varepsilon) - \beta_k(\varepsilon)) = \int_0^1 \beta_{k-1}'(x)dx = 0, \quad \text{q.e.d.}$$

Example. Let us calculate β_2. The condition

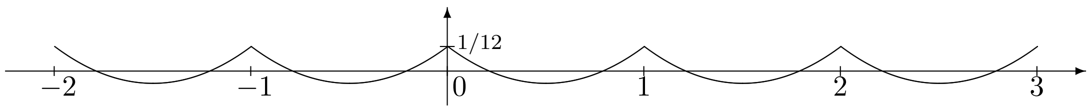
$$\beta_2'(x) = \beta_1(x) = x - \tfrac{1}{2} \quad \text{for } 0 < x < 1$$

leads to $\beta_2(x) = \frac{1}{2}x^2 - \frac{1}{2}x + c$ with an integration constant c. Since

$$\int_0^1 (\tfrac{1}{2}x^2 - \tfrac{1}{2}x)dx = \tfrac{1}{6} - \tfrac{1}{4} = -\tfrac{1}{12},$$

we have $c = \frac{1}{12}$, i.e.

$$\beta_2(x) = \tfrac{1}{2}x^2 - \tfrac{1}{2}x + \tfrac{1}{12} = \tfrac{1}{2}x(x-1) + \tfrac{1}{12} \quad \text{for } 0 \leq x \leq 1.$$



Graph of β_2

5.6. Theorem. *The functions β_n have the following Fourier expansions*

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

$$\beta_{2k+1}(x) = (-1)^{k-1} 2 \sum_{n=1}^{\infty} \frac{\sin(2\pi n x)}{(2\pi n)^{2k+1}}, \quad k \geq 1, \tag{2}$$

which converge uniformly on $\mathbb{R}$.
Formula (2) *is also valid for* $k = 0$ *and* $x \in \mathbb{R} \smallsetminus \mathbb{Z}$.

Proof. a) We first calculate the Fourier series $\sum_{n\in\mathbb{Z}} c_n e^{inx}$ of β_2. The coefficients c_n are given by the integral

$$c_n = \int_0^1 \beta_2(x) e^{-2\pi i n x}\, dx.$$

By theorem 5.5.iv) we have $c_0 = 0$. Let now $n \neq 0$. Using partial integration we get

$$\int_0^1 x e^{-2\pi i n x} dx = -\frac{1}{2\pi i n} x e^{-2\pi i n x}\Big|_0^1 + \frac{1}{2\pi i n}\int_0^1 e^{-2\pi i n x} dx = \frac{i}{2\pi n}$$

and

$$\int_0^1 x^2 e^{-2\pi i n x} dx = -\frac{1}{2\pi i n} x^2 e^{-2\pi i n x}\Big|_0^1 + \frac{2}{2\pi i n}\int_0^1 x e^{-2\pi i n x} dx = \frac{i}{2\pi n} + \frac{2}{(2\pi n)^2},$$

hence

$$c_n = \int_0^1 \left(\tfrac{1}{2}x^2 - \tfrac{1}{2}x + \tfrac{1}{12}\right) e^{-2\pi i n x} dx = \frac{1}{(2\pi n)^2}.$$

Thus we have the Fourier series

$$\beta_2(x) = \sum_{n\in\mathbb{Z}\smallsetminus 0} \frac{e^{2\pi i n}}{(2\pi n)^2} = \sum_{n=1}^{\infty} \frac{e^{2\pi i n x} + e^{-2\pi i n x}}{(2\pi n)^2} = 2\sum_{n=1}^{\infty} \frac{\cos(2\pi n x)}{(2\pi n)^2}.$$

By the general theory of Fourier series, the convergence is with respect to the L^2-norm $\|f\|_{L^2} = (\int_0^1 |f(x)|^2 dx)^{1/2}$, but since $\sum_{n=1}^{\infty} 1/n^2 < \infty$ and β_2 is continuous, we have even uniform convergence.

b) Since the right hand sides of the formulae of the theorem satisfy the same recursion and normalization relations (5.5.iii-iv) as the functions β_k, it follows that the given Fourier expansions are valid for all β_k, $k \geq 2$. To prove the formula for

$$\beta_1(x) = \mathrm{saw}(x) = -2\sum_{n=1}^{\infty} \frac{\sin(2\pi n x)}{2\pi n}, \quad x \in \mathbb{R} \smallsetminus \mathbb{Z},$$

it suffices to show that the series $\sum_{n=1}^{\infty} \frac{\sin(2\pi nx)}{2\pi n}$ converges uniformly on every interval $[\delta, 1-\delta]$, $0 < \delta < \frac{1}{2}$, since then termwise differentiation of the Fourier series of β_2 is allowed. To simplify the notation we will prove the equivalent statement

$$\sum_{n=1}^{\infty} \frac{\sin nx}{n} \quad \textit{converges uniformly on } [\delta, 2\pi-\delta],\ (0<\delta<\pi).$$

Define

$$S_m(x) := \sum_{n=1}^{m} \sin nx = \operatorname{Im}\Big(\sum_{n=1}^{m} e^{inx}\Big).$$

For $\delta \le x \le 2\pi - \delta$ we have

$$|S_m(x)| \le \Big|\sum_{n=1}^{m} e^{inx}\Big| = \Big|\frac{e^{imx}-1}{e^{ix}-1}\Big| \le \frac{2}{|e^{ix/2}-e^{-ix/2}|} = \frac{1}{\sin\frac{x}{2}} \le \frac{1}{\sin\frac{\delta}{2}}.$$

It follows for $m \ge k > 0$

$$\begin{aligned}
\Big|\sum_{n=k}^{m} \frac{\sin nx}{n}\Big| &= \Big|\sum_{n=k}^{m} \frac{S_n(x)-S_{n-1}(x)}{n}\Big| \\
&\le \Big|\sum_{n=k}^{m} S_n(x)\Big(\frac{1}{n}-\frac{1}{n+1}\Big) + \frac{S_m(x)}{m+1} - \frac{S_{k-1}(x)}{k}\Big| \\
&\le \frac{1}{\sin\frac{\delta}{2}}\Big(\frac{1}{k}-\frac{1}{m+1}+\frac{1}{m+1}+\frac{1}{k}\Big) \le \frac{2}{k\sin\frac{\delta}{2}},
\end{aligned}$$

hence also

$$\Big|\sum_{n=k}^{\infty} \frac{\sin nx}{n}\Big| \le \frac{2}{k\sin\frac{\delta}{2}} \quad \text{for all } x \in [\delta, 2\pi-\delta],$$

which proves the asserted uniform convergence and thereby completes the proof of the theorem.

5.7. Definition. It follows immediately from (5.5.iii-iv) that β_n, restricted to the open interval $]0,1[$, is a polynomial of degree n with rational coefficients. The n-th *Bernoulli polynomial* $B_n(X) \in \mathbb{Q}[X]$ is defined by

$$\frac{B_n(x)}{n!} = \beta_n(x) \quad \text{for } 0<x<1,\ n \ge 1$$

and $B_0(X) = 1$. The *Bernoulli numbers*[1] B_k are defined by

$$B_n := B_n(0), \quad n \ge 0.$$

[1] Strictly speaking, it is not correct to use the same symbol B_k for the Bernoulli polynomials and the Bernoulli numbers. However this notation is the usual one. To avoid confusion, we will always indicate the variable when we are dealing with Bernoulli polynomials.

We know already the first Bernoulli polynomials

$$B_1(X) = X - \tfrac{1}{2} \quad \text{and} \quad B_2(X) = X(X-1) + \tfrac{1}{6},$$

hence $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$.

An easy consequence of theorem 5.6 is

5.8. Theorem. *For the Bernoulli numbers the following relations hold:*

i) $B_{2k+1} = 0$ for all $k \geq 1$.

ii) $B_{2k} = (-1)^{k-1} \dfrac{2(2k)!}{(2\pi)^{2k}} \displaystyle\sum_{n=1}^{\infty} \frac{1}{n^{2k}}$, hence

$$\zeta(2k) = \frac{(2\pi)^{2k}}{2(2k)!} |B_{2k}| \quad \text{for all } k \geq 1.$$

iii) $\operatorname{sign}(B_{2k}) = (-1)^{k-1}$ for all $k \geq 1$.

Remarks. a) Formula ii) of the theorem says in particular

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6},$$

which was already used in the previous chapter.

b) Since $\lim\limits_{\sigma \to \infty} \zeta(\sigma) = 1$, formula ii) shows the asymptotic growth of the Bernoulli numbers B_{2k}

$$|B_{2k}| \sim \frac{2(2k)!}{(2\pi)^{2k}} \quad \text{for } k \to \infty.$$

5.9. Theorem (Generating function for the Bernoulli polynomials). *For fixed $x \in \mathbb{R}$, the function $\dfrac{te^{xt}}{e^t - 1}$ is a complex analytic function of t with a removable singularity at $t = 0$. The Taylor expansion at $t = 0$ of this function has the form*

$$\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} t^n.$$

In particular, for $x = 0$ one has

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n.$$

Proof. Define $B_n(x)$ by the above Taylor expansions. We will show that

(a) $B_0(x) = 1,\;\; B_1(x) = x - \frac{1}{2}$,

(b) $B_n'(x) = nB_{n-1}(x),\;\; (n \geq 1)$,

(c) $\int_0^1 B_n(x)dx = 0,\;\; (n \geq 1)$.

Then theorem 5.5 implies $\dfrac{B_n(x)}{n!} = \beta_n(x)$ for $0 < x < 1$ and all $n \geq 1$.

Proof of (a)

$$\begin{aligned} \frac{te^{xt}}{e^t - 1} &= \frac{t(1 + xt + O(t^2))}{t + \frac{1}{2}t^2 + O(t^3)} = \frac{1 + xt + O(t^2)}{1 + \frac{1}{2}t + O(t^2)} \\ &= (1 + xt)(1 - \tfrac{1}{2}t) + O(t^2) = 1 + (x - \tfrac{1}{2})t + O(t^2), \end{aligned}$$

which shows $B_0(x) = 1$ and $B_1(x) = x - \frac{1}{2}$.

Proof of (b) We calculate $\dfrac{\partial}{\partial x}\dfrac{te^{xt}}{e^t - 1}$ in two ways

$$\frac{\partial}{\partial x}\frac{te^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n'(x)}{n!}\, t^n$$

and

$$\frac{\partial}{\partial x}\frac{te^{xt}}{e^t - 1} = \frac{t^2e^{xt}}{e^t - 1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!}\, t^{n+1} = \sum_{n=1}^{\infty} \frac{B_{n-1}(x)}{(n-1)!}\, t^n$$

Comparing coefficients we get $B_n'(x) = nB_{n-1}(x)$.

Proof of (c)

$$\int_0^1 \frac{te^{xt}}{e^t - 1}\, dx = \frac{e^{xt}}{e^t - 1}\bigg|_{x=0}^{x=1} = \frac{e^t}{e^t - 1} - \frac{1}{e^t - 1} = 1.$$

On the other hand

$$\int_0^1 \frac{te^{xt}}{e^t - 1}\, dx = \sum_{n=1}^{\infty} \Big(\int_0^1 B_n(x)dx\Big)\frac{t^n}{n!}.$$

Comparing coefficients, we get $\int_0^1 B_n(x)dx = 0$ for all $n \geq 1$, q.e.d.

5.10. Recursion formula. Theorem 5.9 can be used to derive a recursion formula for the Bernoulli numbers. Since $(e^t - 1)/t = \sum\limits_{n=1}^{\infty} t^{n-1}/n!$, we have

$$\Big(\sum_{k=0}^{\infty} \frac{B_k}{k!}\, t^k\Big)\Big(\sum_{\ell=0}^{\infty} \frac{1}{(\ell+1)!}\, t^\ell\Big) = 1.$$

The Cauchy product $\sum_{n=0}^{\infty} c_n t^n$ of the two series has coefficients

$$c_n = \sum_{k=1}^{n} \frac{B_k}{k!(n-k+1)!} = \frac{1}{(n+1)!} \sum_{k=0}^{n} \binom{n+1}{k} B_k.$$

Hence comparing coefficients we get $B_0 = 1$ and

$$\sum_{k=0}^{n} \binom{n+1}{k} B_k = 0 \quad \text{for all } n \geq 1.$$

With this formula one can recursively calculate all B_n. The first non zero coefficients are

k	0	1	2	4	6	8	10	12	14	16
B_k	1	$-\frac{1}{2}$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{6}{7}$	$-\frac{3617}{510}$

5.11. Theorem (Euler-Maclaurin II). *Let x_0 be a real number and $f : [x_0, \infty[\to \mathbb{C}$ a $2r$-times continuously differentiable function. Then we have for all integers $n \geq m \geq x_0$ and all $r \geq 1$*

$$\begin{aligned}\sum_{k=m}^{n} f(k) &= \tfrac{1}{2}(f(m) + f(n)) + \int_m^n f(x)dx \\ &\quad + \sum_{k=1}^{r} \frac{B_{2k}}{(2k)!} \left(f^{(2k-1)}(n) - f^{(2k-1)}(m)\right) - \int_m^n \frac{\widetilde{B}_{2r}(x)}{(2r)!} f^{(2r)}(x)dx\end{aligned}$$

Here $\widetilde{B}_{2r}(x)$ is the periodic function defined by $\widetilde{B}_{2r}(x) := B_{2r}(x - \lfloor x \rfloor) = (2r)!\beta_{2r}(x)$.

Proof. We start with theorem 5.2

$$\sum_{k=m}^{n} f(k) = \tfrac{1}{2}(f(m) + f(n)) + \int_m^n f(x)dx + \int_m^n \mathrm{saw}(x) f'(x)dx.$$

and evaluate the last integral by partial integration.

Since $\beta_2'(x) = \mathrm{saw}(x)$ for $k < x < k+1$ and β_2 is continuous and periodic, we get

$$\begin{aligned}\int_m^n \mathrm{saw}(x) f'(x)dx &= \sum_{k=m}^{n-1} \int_k^{k+1} \mathrm{saw}(x) f'(x)dx \\ &= \sum_{k=m}^{n-1} \beta_2(x) f'(x)\Big|_k^{k+1} - \sum_{k=m}^{n-1} \int_k^{k+1} \beta_2(x) f''(x)dx \\ &= \sum_{k=m}^{n-1} \left(\beta_2(k+1) f'(k+1) - \beta_2(k) f'(k)\right) - \int_m^n \beta_2(x) f''(x)dx \\ &= \frac{B_2}{2!}(f'(n) - f'(m)) - \int_m^n \beta_2(x) f''(x)dx.\end{aligned}$$

This proves the case $r = 1$ of the theorem. The general case is proved by induction.
Induction step $r \to r+1$.

$$\begin{aligned}
-\int_m^n \beta_{2r}(x) f^{(2r)}(x)dx &= -\beta_{2r+1}(x) f^{(2r)}(x)\Big|_m^n + \int_m^n \beta_{2r+1}(x) f^{(2r+1)}(x)dx \\
&= \int_m^n \beta_{2r+1}(x) f^{(2r+1)}(x)dx \qquad \left[\text{since } \beta_{2r+1}(k) = \frac{B_{2r+1}}{(2r+1)!} = 0\right] \\
&= \beta_{2r+2}(x) f^{(2r+1)}(x)\Big|_m^n - \int_m^n \beta_{2r+2}(x) f^{(2r+2)}(x)dx \\
&= \frac{B_{2r+2}}{(2r+2)!}(f^{(2r+1)}(n) - f^{(2r+1)}(m)) - \int_m^n \beta_{2r+2}(x) f^{(2r+2)}(x)dx.
\end{aligned}$$

This proves the assertion for $r+1$.

Remark. If f is infinitely often differentiable and we pass to the limit $r \to \infty$, the "error term"

$$\int_m^n \frac{\widetilde{B}_{2r}(x)}{(2r)!} f^{(2r)}(x)dx$$

will in general not converge to 0. In case f is real and $f^{(2r)}$ does not change sign in the interval $[m, n]$, one has the following estimate

$$\Big|\int_m^n \frac{\widetilde{B}_{2r}(x)}{(2r)!} f^{(2r)}(x)dx\Big| \le \frac{|B_{2r}|}{(2r)!}\Big|\int_m^n f^{(2r)}(x)dx\Big| = \frac{|B_{2r}|}{(2r)!}|f^{(2r-1)}(n) - f^{(2r-1)}(m)|,$$

which means that the error of the approximation

$$\sum_{k=m}^n f(k) \approx \tfrac{1}{2}(f(m)+f(n)) + \int_m^n f(x)dx + \sum_{k=1}^r \frac{B_{2k}}{(2k)!}\left(f^{(2k-1)}(n) - f^{(2k-1)}(m)\right)$$

is by absolute value not larger than the last term of the sum. Hence by increasing r one gets better approximations as long as the absolute values of the added terms decrease.

5.12. Theorem. *The Riemann zeta function can be analytically continued to a meromorphic function in the whole plane $\mathbb{C}$ with a single pole of order 1 at $s = 1$. For* $\mathrm{Re}(s) > 1 - 2r$, *the continued function can be represented as*

$$\begin{aligned}
\zeta(s) = \frac{1}{2} + \frac{1}{s-1} &+ \sum_{k=1}^r \frac{B_{2k}}{(2k)!} s(s+1)\cdot\ldots\cdot(s+2k-2) \\
&- s(s+1)\cdot\ldots\cdot(s+2r-1)\int_1^\infty \frac{\widetilde{B}_{2r}(x)}{(2r)!}\cdot\frac{1}{x^{s+2r}}\,dx.
\end{aligned}$$

Proof. This is proved by applying theorem 5.11 to the sum $\sum_{k=1}^n 1/k^s$ and passing to the limit $n \to \infty$. That the last integral defines a holomorphic function for $\mathrm{Re}(s) > 1-2r$, follows from the fact that the function $\widetilde{B}_{2r}(x)$ is bounded and

$$\Big|\frac{1}{x^{s+2r}}\Big| \le \frac{1}{x^{1+\delta}} \quad \text{for all } s \in \mathbb{C} \text{ with } \mathrm{Re}(s) \ge 1 - 2r + \delta.$$

6. Dirichlet Series

6.1. Definition. A *Dirichlet series* is a series of the form

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad (s \in \mathbb{C}),$$

where $(a_n)_{n\geqslant 1}$ is an arbitrary sequence of complex numbers.

The *abscissa of absolute convergence* of this series is defined as

$$\sigma_a := \sigma_a(f) := \inf\{\sigma \in \mathbb{R} : \sum_{n=1}^{\infty} \frac{|a_n|}{n^\sigma} < \infty\} \in \mathbb{R} \cup \{\pm\infty\}.$$

If $\sum_{n=1}^{\infty}(|a_n|/n^\sigma)$ does not converge for any $\sigma \in \mathbb{R}$, then $\sigma_a = +\infty$, if it converges for all $\sigma \in \mathbb{R}$, then $\sigma_a = -\infty$.

An analogous argument as in the case of the zeta function shows that a Dirichlet series with abscissa of absolute convergence σ_a converges absolutely and uniformly in every halfplane $\overline{H(\sigma)}$, $\sigma > \sigma_a$.

Example. The Dirichlet series

$$g(s) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}$$

has $\sigma_a(g) = 1$. We will see however that the series converges for every $s \in H(0)$. Of course the convergence is only conditional and not absolute if $0 < \mathrm{Re}(s) \leq 1$.

We need some preparations.

6.2. Lemma (Abel summation). *Let $(a_n)_{n\geqslant 1}$ and $(b_n)_{n\geqslant 1}$ be two sequences of complex numbers and set*

$$A_n := \sum_{k=1}^{n} a_k, \qquad A_0 = 0 \text{ (empty sum)}.$$

Then we have for all $n \geq m \geq 1$

$$\sum_{k=m}^{n} a_k b_k = A_n b_n - A_{m-1} b_m - \sum_{k=m}^{n-1} A_k (b_{k+1} - b_k).$$

Remark. This can be viewed as an analogon of the formula for partial integration

$$\int_a^b F'(x) g(x) dx = F(b)g(b) - F(a)g(a) - \int_a^b F(x) g'(x) dx.$$

Chap. 6 last revised: 2001-11-21

Proof.

$$\begin{aligned}\sum_{k=m}^{n} a_k b_k &= \sum_{k=m}^{n}(A_k - A_{k-1})b_k = \sum_{k=m}^{n} A_k b_k - \sum_{k=m-1}^{n-1} A_k b_{k+1} \\ &= A_n b_n + \sum_{k=m}^{n-1} A_k b_k - \sum_{k=m}^{n-1} A_k b_{k+1} - A_{m-1} b_m \\ &= A_n b_n - A_{m-1} b_m - \sum_{k=m}^{n-1} A_k (b_{k+1} - b_k), \quad \text{q.e.d.}\end{aligned}$$

6.3. Lemma. *Let $s \in \mathbb{C}$ with $\sigma := \mathrm{Re}(s) > 0$. Then we have for all $m, n \geq 1$*

$$\left|\frac{1}{n^s} - \frac{1}{m^s}\right| \;\leq\; \frac{|s|}{\sigma} \cdot \left|\frac{1}{n^\sigma} - \frac{1}{m^\sigma}\right|.$$

Proof. We may assume $n \geq m$. Since $\dfrac{d}{dx}\Big(\dfrac{1}{x^s}\Big) = -s \cdot \dfrac{1}{x^{s+1}}$,

$$-s \int_m^n \frac{dx}{x^{s+1}} = \frac{1}{n^s} - \frac{1}{m^s}\,.$$

Taking the absolute values, we get the estimate

$$\left|\frac{1}{n^s} - \frac{1}{m^s}\right| \leq |s| \int_m^n \frac{dx}{x^{\sigma+1}} = \frac{|s|}{\sigma} \cdot \left|\frac{1}{n^\sigma} - \frac{1}{m^\sigma}\right|, \quad \text{q.e.d.}$$

Remark. For $s_0 \in \mathbb{C}$ and an angle α with $0 < \alpha < \pi/2$, we define the *angular region*

$$\mathrm{Ang}(s_0, \alpha) := \{s_0 + re^{i\phi} : r \geq 0 \text{ and } |\phi| \leq \alpha\}.$$

For any $s \in \mathrm{Ang}(s_0, \alpha) \smallsetminus \{s_0\}$ we have

$$\frac{|s - s_0|}{\mathrm{Re}(s - s_0)} = \frac{1}{\cos\phi} \leq \frac{1}{\cos\alpha}\,,$$

hence the estimate in lemma 6.3 can be rewritten as

$$\left|\frac{1}{n^s} - \frac{1}{m^s}\right| \;\leq\; \frac{1}{\cos\alpha} \cdot \left|\frac{1}{n^\sigma} - \frac{1}{m^\sigma}\right| \quad \text{for all } s \in \mathrm{Ang}(0, \alpha).$$

6.4. Theorem. *Let*

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

be a Dirichlet series such that for some $s_0 \in \mathbb{C}$ *the partial sums* $\sum_{n=1}^{N} \dfrac{a_n}{n^{s_0}}$ *are bounded for* $N \to \infty$*. Then the Dirichlet series converges for every* $s \in \mathbb{C}$ *with*

$$\mathrm{Re}(s) > \sigma_0 := \mathrm{Re}(s_0).$$

The convergence is uniform on every compact subset

$$K \subset H(\sigma_0) = \{s \in \mathbb{C} : \mathrm{Re}(s) > \sigma_0\}.$$

Hence f *is a holomorphic function in* $H(\sigma_0)$*.*

Proof. Since

$$f(s) = \sum_{n=1}^{\infty} \frac{1}{n^{s_0}} \cdot \frac{a_n}{n^{s-s_0}} = \sum_{n=1}^{\infty} \frac{\tilde{a}_n}{n^{s-s_0}} \quad \text{where } \tilde{a}_n := \frac{a_n}{n^{s_0}},$$

we may suppose without loss of generality that $s_0 = 0$. By hypothesis there exists a constant $C_1 > 0$ such that

$$\Big|\sum_{n=1}^{N} a_n\Big| \le C_1 \quad \text{for all } N \in \mathbb{N}.$$

The compact set K is contained in some angular region $\mathrm{Ang}(0, \alpha)$ with $0 < \alpha < \pi/2$. We define

$$C_\alpha := \frac{1}{\cos\alpha} \quad \text{and} \quad \sigma_* := \inf\{\mathrm{Re}(s) : s \in K\} > 0.$$

Now we apply the Abel summation lemma 6.2 to the sum $\sum a_n \cdot (1/n^s)$, $s \in K$. Setting $A_N := \sum_{n=1}^{N} a_n$, we get for $N \ge M \ge 1$

$$\sum_{n=M}^{N} \frac{a_n}{n^s} = A_N \frac{1}{N^s} - A_{M-1} \frac{1}{M^s} + \sum_{n=M}^{N-1} A_n \Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big).$$

This leads to the estimate (with $\sigma = \mathrm{Re}(s)$)

$$\begin{aligned}
\Big|\sum_{n=M}^{N} \frac{a_n}{n^s}\Big| &\le 2C_1 \Big|\frac{1}{M^s}\Big| + C_1 \sum_{n=M}^{N-1} \Big|\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big| \\
&\le 2C_1 \frac{1}{M^\sigma} + C_1 C_\alpha \sum_{n=M}^{N-1} \Big(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma}\Big) \\
&= 2C_1 \frac{1}{M^\sigma} + C_1 C_\alpha \Big(\frac{1}{M^\sigma} - \frac{1}{N^\sigma}\Big) \\
&\le \frac{C_1}{M^\sigma}\Big(2 + C_\alpha\Big) \le \frac{C_1(2 + C_\alpha)}{M^{\sigma_*}}.
\end{aligned}$$

This becomes arbitrarily small if M is sufficently large. This implies the asserted uniform convergence on K of the Dirichlet series.

6.5. Theorem. *Let*

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

be a Dirichlet series which converges for some $s_0 \in \mathbb{C}$. Then the series converges uniformly in every angular region $\mathrm{Ang}(s_0, \alpha)$*, $0 < \alpha < \pi/2$. In particular*

$$\lim_{s \to s_0} f(s) = f(s_0),$$

when s approaches s_0 within an angular region $\mathrm{Ang}(s_0, \alpha)$.

Proof. As in the proof of theorem 6.4 we may suppose $s_0 = 0$. Set $C_\alpha := 1/\cos\alpha$. Let $\varepsilon > 0$ be given. Since $\sum_{n=1}^{\infty} a_n$ converges, there exists an $n_0 \in \mathbb{N}$, such that

$$\Big|\sum_{n=M}^{N} a_n\Big| < \varepsilon_1 := \frac{\varepsilon}{1 + C_\alpha} \quad \text{for all } N \geq M \geq n_0.$$

With $A_{Mn} := \sum_{k=M}^{n} a_k$, $A_{M,M-1} = 0$, we have by the Abel summation formula

$$\sum_{n=M}^{N} \frac{a_n}{n^s} = A_{MN}\frac{1}{N^s} + \sum_{n=M}^{N-1} A_{Mn}\Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big).$$

From this, we get for all $s \in \mathrm{Ang}(0, \alpha)$, $\sigma := \mathrm{Re}(s)$, and $N \geq M \geq n_0$ the estimate

$$\begin{aligned}
\Big|\sum_{n=M}^{N} \frac{a_n}{n^s}\Big| &\leq \varepsilon_1 \frac{1}{|N^s|} + \varepsilon_1 \sum_{n=M}^{N-1} \Big|\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big| \\
&\leq \varepsilon_1 + \varepsilon_1 C_\alpha \sum_{n=M}^{N-1} \Big(\frac{1}{n^\sigma} - \frac{1}{(n+1)^\sigma}\Big) \\
&= \varepsilon_1 + \varepsilon_1 C_\alpha \Big(\frac{1}{M^\sigma} - \frac{1}{N^\sigma}\Big) \leq \varepsilon_1 + \varepsilon_1 C_\alpha = \varepsilon.
\end{aligned}$$

This shows the uniform convergence of the Dirichlet series in $\mathrm{Ang}(0, \alpha)$. Therefore f is continuous in $\mathrm{Ang}(0, \alpha)$, which implies the last assertion of the theorem.

6.6. Definition. Let $f(s) = \sum\limits_{n=1}^{\infty} \dfrac{a_n}{n^s}$ be a Dirichlet series. The *abscissa of convergence* of f is defined by

$$\sigma_c := \sigma_c(f) := \inf\,\{\mathrm{Re}(s) : \sum_{n=1}^{\infty} \frac{a_n}{n^s} \text{ converges }\}.$$

By theorem 6.4 this is the same as

$$\sigma_c = \inf\{\mathrm{Re}(s) : \sum_{n=1}^{N} \frac{a_n}{n^s} \text{ is bounded for } N \to \infty\}$$

and it follows that the series converges to a holomorphic function in the halfplane $H(\sigma_c)$.

Examples. Consider the three Dirichlet series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad g(s) := \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}, \qquad \frac{1}{\zeta}(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

We have $\sigma_a(\zeta) = \sigma_a(g) = \sigma_a(1/\zeta) = 1$. Clearly $\sigma_c(\zeta) = 1$ and $\sigma_c(g) = 0$, since the partial sums $\sum_{n=1}^{N}(-1)^{n-1}$ are bounded. The abscissa of convergence $\sigma_c(1/\zeta)$ is not known; of course $\sigma_c(1/\zeta) \le 1$. One conjectures that $\sigma_c(1/\zeta) = \frac{1}{2}$, which is equivalent to the *Riemann Hypothesis*, which we will discuss in a later chapter.

Remark. Multiplying the zeta series by 2^{-s} yields $2^{-s}\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{(2n)^s}$. Hence

$$g(s) = (1 - 2^{1-s})\zeta(s).$$

6.7. Theorem. *If the Dirichlet series $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ has a finite abscissa of convergence σ_c, then for the abscissa of absolute convergence σ_a the following estimate holds:*

$$\sigma_c \le \sigma_a \le \sigma_c + 1.$$

Proof. Without loss of generality we may suppose $\sigma_c = 0$. Then $\sum_{n=1}^{\infty} \frac{a_n}{n^{\varepsilon}}$ converges for every $\varepsilon > 0$. We have to show that

$$\sum_{n=1}^{\infty} \frac{|a_n|}{n^{\sigma_*}} < \infty \qquad \text{for all } \sigma_* > 1.$$

To see this, write $\sigma_* = 1 + 2\varepsilon$, $\varepsilon > 0$. Then

$$\frac{|a_n|}{n^{\sigma_*}} = \frac{|a_n|}{n^{\varepsilon}} \cdot \frac{1}{n^{1+\varepsilon}}$$

Since $|a_n|/n^{\varepsilon}$ is bounded for $n \to \infty$ and $\sum_{n=1}^{\infty} 1/n^{1+\varepsilon} < \infty$, the assertion follows.

Remarks. a) It can be easily seen that $\sigma_c = -\infty$ implies $\sigma_a = -\infty$.

b) The above examples show that the cases $\sigma_a = \sigma_c$ and $\sigma_a = \sigma_c + 1$ do actually occur.

c) That σ_a and σ_c may be different is quite surprising if one looks at the situation for power series: If a power series $\sum_{n=0}^{\infty} a_n z^n$ converges for some $z_0 \neq 0$, it converges absolutely for every z with $|z| < |z_0|$.

6.8. Theorem (Landau). *Let*

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

be a Dirichlet series with non-negative coefficients $a_n \geq 0$ and finite abscissa of absolute convergence $\sigma_a \in \mathbb{R}$. Then the function f, which is holomorphic in the halfplane $H(\sigma_a)$, cannot be continued analytically as a holomorphic function to any neighborhood of σ_a.

Proof. Assume to the contrary that there exists a small open disk D around σ_a such that f can be analytically continued to a holomorphic function in $H(\sigma_a) \cup D$, which we denote again by f. Then the Taylor series of f at the point $\sigma_1 := \sigma_a + 1$ has radius of convergence > 1. Since

$$f^{(k)}(\sigma_1) = \sum_{n=1}^{\infty} \frac{(-\log n)^k a_n}{n^{\sigma_1}},$$

the Taylor series has the form

$$f(s) = \sum_{k=0}^{\infty} \frac{f^{(k)}(\sigma_1)}{k!}(s - \sigma_1)^k = \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(-\log n)^k a_n}{k!\, n^{\sigma_1}}(s - \sigma_1)^k.$$

By hypothesis there exists a real $\sigma < \sigma_a$ such that the Taylor series converges for $s = \sigma$. We have

$$f(\sigma) = \sum_{k=0}^{\infty} \sum_{n=1}^{\infty} \frac{(\log n)^k a_n (\sigma_1 - \sigma)^k}{k!\, n^{\sigma_1}} = \sum_{n=1}^{\infty} \sum_{k=0}^{\infty} \frac{(\log n)^k (\sigma_1 - \sigma)^k}{k!} \cdot \frac{a_n}{n^{\sigma_1}},$$

where the reordering is allowed since all terms are non-negative. Now

$$\sum_{k=0}^{\infty} \frac{(\log n)^k (\sigma_1 - \sigma)^k}{k!} = e^{(\log n)(\sigma_1 - \sigma)} = \frac{1}{n^{\sigma - \sigma_1}},$$

hence we have a convergent series

$$f(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^{\sigma - \sigma_1}} \cdot \frac{a_n}{n^{\sigma_1}} = \sum_{n=1}^{\infty} \frac{a_n}{n^{\sigma}}.$$

Thus the abscissa of absolute convergence is $\leq \sigma < \sigma_a$, a contradiction. Hence the assumption is false, which proves the theorem.

6.9. Theorem (Identity theorem for Dirichlet series). *Let*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad \text{and} \quad g(s) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}$$

be two Dirichlet series that converge in a common halfplane $H(\sigma_0)$. If there exists a sequence $s_\nu \in H(\sigma_0)$, $\nu \in \mathbb{N}_1$, with $\lim_{\nu\to\infty} \mathrm{Re}(s_\nu) = \infty$ and

$$f(s_\nu) = g(s_\nu) \quad \text{for all } \nu \geq 1,$$

then $a_n = b_n$ for all $n \geq 1$.

Proof. Passing to the difference $f - g$ shows that it suffices to prove the theorem for the case where g is identically zero. So we suppose that

$$f(s_\nu) = 0 \quad \text{for all } \nu \geq 1.$$

If not all $a_n = 0$, then there exists a minimal k such that $a_k \neq 0$. We have

$$f(s) = \frac{1}{k^s}\Big(a_k + \sum_{n>k} \frac{a_n}{(n/k)^s}\Big).$$

It suffices to show that there exists a $\sigma_* \in \mathbb{R}$ such that

$$\Big|\sum_{n>k} \frac{a_n}{(n/k)^s}\Big| \leq \frac{|a_k|}{2} \quad \text{for all } s \text{ with } \mathrm{Re}(s) \geq \sigma_*,$$

for this would imply $f(s) \neq 0$ for $\mathrm{Re}(s) \geq \sigma_*$, contradicting $f(s_\nu) = 0$ for all ν. The sum $\sum_{n>k} \frac{a_n}{(n/k)^{\sigma'}}$ converges absolutely for some $\sigma' \in \mathbb{R}$. Therefore we can find an $M \geq k$ such that

$$\sum_{n>M} \frac{|a_n|}{(n/k)^{\sigma'}} \leq \frac{|a_k|}{4}.$$

Further there exists a $\sigma'' \in \mathbb{R}$ such that

$$\sum_{k<n\leqslant M} \frac{|a_n|}{(n/k)^{\sigma''}} \leq \frac{|a_k|}{4}.$$

Combining the last two estimates shows

$$\Big|\sum_{n>k} \frac{a_n}{(n/k)^s}\Big| \leq \frac{|a_k|}{2} \quad \text{for all } s \text{ with } \mathrm{Re}(s) \geq \max(\sigma', \sigma''), \quad \text{q.e.d.}$$

Remark. A similar theorem is not true for arbitrary holomorphic functions in halfplanes. For example, the sine function satisfies

$$\sin(\pi n) = 0 \quad \text{for all integers } n,$$

without being identically zero. This shows also that not every function holomorphic in a halfplane $H(\sigma)$ can be expanded in a Dirichlet series.

6.10. Theorem. *Let $a, b : \mathbb{N}_1 \to \mathbb{C}$ be two arithmetical functions such that the Dirichlet series*

$$f(s) := \sum_{n=1}^{\infty} \frac{a(n)}{n^s} \quad \textit{and} \quad g(s) := \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$$

converge absolutely in a common halfplane $H(\sigma_0)$. Then we have for the product

$$f(s)g(s) = \sum_{n=1}^{\infty} \frac{(a * b)(n)}{n^s}.$$

This Dirichlet series converges absolutely in $H(\sigma_0)$.

Proof. Since the series for $f(s)$ and $g(s)$ converge absolutely for $s \in H(\sigma_0)$, they can be multiplied term by term

$$\begin{aligned} f(s)g(s) &= \sum_{k=1}^{\infty} \frac{a(k)}{k^s} \sum_{\ell=1}^{\infty} \frac{b(\ell)}{\ell^s} = \sum_{k,\ell \geqslant 1} a(k)b(\ell) \frac{1}{k^s \ell^s} \\ &= \sum_{n=1}^{\infty} \sum_{k\ell=n} a(k)b(\ell) \frac{1}{(k\ell)^s} = \sum_{n=1}^{\infty} \frac{(a * b)(n)}{n^s}, \end{aligned}$$

and the product series converges absolutely, q.e.d.

Examples. i) The zeta function $\zeta(s) = \sum\limits_{n=1}^{\infty} \dfrac{1}{n^s}$ is the Dirichlet series associated to the constant arithmetical function $u(n) = 1$. Since $u * \mu = \delta_1$, it follows

$$\Big(\sum_{n=1}^{\infty} \frac{1}{n^s}\Big)\Big(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\Big) = \sum_{n=1}^{\infty} \frac{\delta_1(n)}{n^s} = 1,$$

which gives a new proof of

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \qquad \text{(cf. theorem 4.5).}$$

ii) The Dirichlet series associated to the identity map $\iota : \mathbb{N}_1 \to \mathbb{N}_1$ is

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

which converges absolutely for $\operatorname{Re}(s) > 2$. For the divisor sum function σ we have $u * \iota = \sigma$, cf. (3.15.iii), which implies

$$\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s} \quad \text{for } \operatorname{Re}(s) > 2.$$

iii) In a similar way, the formula $\varphi = \mu * \iota$ for the Euler phi function, cf. (3.15.i), yields

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} \quad \text{for } \operatorname{Re}(s) > 2.$$

6.11. Theorem (Euler product for Dirichlet series). *Let $a : \mathbb{N}_1 \to \mathbb{C}$ be a* multiplicative *arithmetical function such that the Dirichlet series*

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

has abscissa of absolute convergence $\sigma_a < \infty$.
a) *Then we have in $H(\sigma_a)$ the product representation*

$$f(s) = \prod_{p \in \mathbb{P}} \Big(\sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}} \Big) = \prod_{p \in \mathbb{P}} \Big(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \frac{a(p^3)}{p^{3s}} + \cdots \Big),$$

where the product is extended over the set $\mathbb{P}$ of all primes.
b) *If the arithmetical function a is* completely *multiplicative, this can be simplified to*

$$f(s) = \prod_{p \in \mathbb{P}} \Big(1 - \frac{a(p)}{p^s} \Big)^{-1}.$$

Proof. Let $\mathcal{P} \subset \mathbb{P}$ be a finite set of primes and $\mathbb{N}(\mathcal{P})$ the set of all positive integers whose prime decomposition contains only primes from the set $\mathcal{P}$. Since a is multiplicative, we have for an integer n with prime decomposition $n = p_1^{k_1} p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$

$$a(n) = a(p_1^{k_1}) a(p_2^{k_2}) \cdot \ldots \cdot a(p_r^{k_r}).$$

It follows by multiplying the infinite series term by term that

$$\prod_{p \in \mathcal{P}} \Big(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \frac{a(p^3)}{p^{3s}} + \cdots \Big) = \sum_{n \in \mathbb{N}(\mathcal{P})} \frac{a(n)}{n^s}.$$

Letting $\mathcal{P} = \mathcal{P}_m$ be set of all primes $\le m$ and passing to the limit $m \to \infty$, we obtain part a) the theorem.

If a is completely multiplicative, then $a(p^k) = a(p)^k$, hence

$$\sum_{k=0}^{\infty} \frac{a(p^k)}{p^{ks}} = \sum_{k=0}^{\infty} \Big(\frac{a(p)}{p^s}\Big)^k = \Big(1 - \frac{a(p)}{p^s}\Big)^{-1},$$

proving part b).

Examples. i) The Euler product for the zeta function

$$\zeta(s) = \prod_{p \in \mathbb{P}} \Big(1 - \frac{1}{p^s}\Big)^{-1}$$

is a special case of this theorem.

ii) Since $\mu(p) = -1$ and $\mu(p^k) = 0$ for $k \geq 2$, the formula for the inverse of the zeta function

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = \prod_{p \in \mathbb{P}} \Big(1 - \frac{1}{p^s}\Big) = \frac{1}{\zeta(s)}$$

also follows from this theorem.

7. Group Characters. Dirichlet L-series

7.1. Definition (Group characters). Let G be a group. A *character* of G is a group homomorphism

$$\chi : G \longrightarrow \mathbb{C}^*.$$

If G is a finite group (written multiplicatively), then every element $x \in G$ has finite order, say $r = \operatorname{ord}(x)$. It follows that

$$\chi(x)^r = \chi(x^r) = \chi(e) = 1,$$

hence $\chi(x)$ is a root of unity for all $x \in G$.

Example. Let G be a cyclic group of order r and $g \in G$ a generator of G, i.e.

$$G = \{e = g^0, g = g^1, g^2, g^3, \ldots, g^{r-1}\} =: \langle g \rangle, \qquad (g^r = e).$$

If $\chi : G \to \mathbb{C}^*$ is a character, $\chi(g)$ is an r-th root of unity, hence there exits an integer k, $0 \le k < r$, with $\chi(g) = e^{2\pi i k/r}$. Conversely, for any such k,

$$\chi_k(g^s) := e^{2\pi i ks/r}$$

defines indeed a group character of G.

7.2. Theorem. *Let G be a group.*

a) *The set of all group characters $\chi : G \to \mathbb{C}^*$ is itself a group if one defines the multiplication of two characters χ_1, χ_2 by*

$$(\chi_1\chi_2)(x) := \chi_1(x)\chi_2(x) \quad \text{for all } x \in G.$$

This group is called the *character group* of G and is denoted by $\widehat{G}$.

b) *If G is a finite abelian group, then the character group $\widehat{G}$ is isomorphic to G.*

Proof. a) The easy verification is left to the reader.

b) Consider first the case when $G = \langle g \rangle$ is a cyclic group of order r. Let

$$E_r := \{e^{2\pi i k/r} : 0 \le k < r\}$$

be the group of r-th roots of unity. E_r is itself a cyclic group of order r and the map

$$\widehat{G} \longrightarrow E_r, \quad \chi \mapsto \chi(g),$$

is easily seen to be an isomorphism. To prove the general case, we use the fact that every finite abelian group G is isomorphic to a direct product of cyclic groups:

$$G \cong C_1 \times \ldots \times C_m.$$

Chap. 7 last revised: 2003-04-14

From $\widehat{G} \cong \widehat{C}_1 \times \ldots \times \widehat{C}_m$ the assertion follows.

7.3. Theorem. *Let G be a finite abelian group of order r.*
a) *Let $\chi \in \widehat{G}$ be a fixed character. Then*

$$\sum_{x \in G} \chi(x) = \begin{cases} r, & \text{if } \chi \text{ is the unit character } \chi \equiv 1, \\ 0 & \text{else.} \end{cases}$$

b) *Let $x \in G$ be a fixed element. Then*

$$\sum_{\chi \in \widehat{G}} \chi(x) = \begin{cases} r, & \text{if } x = e, \\ 0 & \text{else.} \end{cases}$$

Proof. a) The formula is trivial for the unit character. If χ is any group character different from the unit character, there exists an $x_0 \in G$ with $\chi(x_0) \neq 1$. If x runs through all group elements, also $x_0 x$ runs through all group elements. Therefore

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(x_0 x) = \chi(x_0) \sum_{x \in G} \chi(x).$$

It follows

$$(1 - \chi(x_0)) \sum_{x \in G} \chi(x) = 0 \quad \Longrightarrow \quad \sum_{x \in G} \chi(x) = 0, \quad \text{q.e.d.}$$

b) The formula is trivial for the unit element e. If x is a group element different from e, there exists a group character $\psi \in \widehat{G}$ with $\psi(x) \neq 1$. Otherwise all group characters would be constant on the subgroup $H \subset G$ generated by x, hence could be regarded as characters of the quotient group G/H, which contradicts theorem 7.2.b). If χ runs through all elements of $\widehat{G}$, so does $\psi\chi$. Hence

$$\sum_{\chi \in \widehat{G}} \chi(x) = \sum_{\chi \in \widehat{G}} (\psi\chi)(x) = \psi(x) \sum_{\chi \in \widehat{G}} \chi(x).$$

It follows

$$(1 - \psi(x)) \sum_{\chi \in \widehat{G}} \chi(x) = 0 \quad \Longrightarrow \quad \sum_{\chi \in \widehat{G}} \chi(x) = 0, \quad \text{q.e.d.}$$

7.4. Definition (Dirichlet characters). Let m be an integer ≥ 2. An arithmetical function $\chi : \mathbb{N}_1 \longrightarrow \mathbb{C}$ is called a Dirichlet character modulo m, if χ is induced by a group character

$$\tilde{\chi} : (\mathbb{Z}/m)^* \longrightarrow \mathbb{C}^*,$$

which means that

$$\chi(n) = \begin{cases} \tilde{\chi}(\overline{n}), & \text{if } \gcd(n,m) = 1, \\ 0, & \text{if } \gcd(n,m) > 1. \end{cases}$$

(Here $\overline{n}$ denotes the residue class of n modulo m).

The *principal* Dirichlet character modulo m is the Dirichlet character induced by the unit character $1 : (\mathbb{Z}/m)^* \to \mathbb{C}$. We denote this principal character by χ_{0m} or briefly by χ_0, if the value of m is clear by the context. Hence we have

$$\chi_{0m}(n) = \begin{cases} 1, & \text{if } \gcd(n,m) = 1, \\ 0, & \text{if } \gcd(n,m) > 1. \end{cases}$$

It is clear that a Dirichlet character is completely multiplicative. It is easy to see that an arithmetical function $f : \mathbb{N}_1 \to \mathbb{C}$ is a Dirichlet character modulo m iff it has the following properties:

i) f is completely multiplicative.

ii) $f(n) = f(n')$ whenever $n \equiv n' \bmod m$.

iii) $f(n) = 0$ for all n with $\gcd(n,m) > 1$.

7.5. Definition (Dirichlet L-series). Let $\chi : \mathbb{N}_1 \to \mathbb{C}$ be a Dirichlet character. The L-series associated to χ is the Dirichlet series

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

This series converges absolutely for every $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$.

Examples. Let $m = 4$.

i) The principal Dirichlet character modulo 4 has $\chi_{0,4}(n) = 1$ for n odd and $\chi_{0,4}(n) = 0$ for n even. Therefore

$$L(s,\chi_{0,4}) = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^s} = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \ldots$$

Since $2^{-s}\zeta(s) = \sum\limits_{k=1}^{\infty} \dfrac{1}{(2k)^s}$, we have

$$L(s,\chi_{0,4}) = (1 - 2^{-s})\zeta(s),$$

which shows that $L(s,\chi_{0,4})$ can be analytically continued to the whole plane $\mathbb{C}$ as a meromorphic function with a single pole at $s = 1$.

ii) Since $(\mathbb{Z}/4)^* = \{\overline{1}, \overline{3}\}$ has two elements, there is exactly one non-principal Dirichlet character χ_1 modulo 4, namely

$$\chi_1(n) = \begin{cases} 0 & \text{for } n \text{ even,} \\ (-1)^{(n-1)/2} & \text{for } n \text{ odd.} \end{cases}$$

Therefore

$$L(s, \chi_1) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \frac{1}{9^s} - + \ldots$$

This Dirichlet series converges to a holomorphic function for $\mathrm{Re}(s) > 0$. For $s = 1$ one gets the well known Leibniz series, hence

$$L(1, \chi_1) = \frac{\pi}{4}.$$

7.6. Theorem. *Let $\chi : \mathbb{N}_1 \to \mathbb{C}$ be a Dirichlet character modulo m. Then*
a) *For* $\mathrm{Re}(s) > 1$ *one has a product representation*

$$L(s, \chi) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \chi(p)p^{-s}}.$$

b) *If $\chi = \chi_{0m}$ is the principal character, then*

$$L(s, \chi_{0m}) = \Big(\prod_{p|m} (1 - p^{-s})\Big) \zeta(s),$$

where the product is extended over all prime divisors of m. Hence $L(s, \chi_{0m})$ can be analytically continued to the whole plane $\mathbb{C}$ as a meromorphic function with a single pole at $s = 1$.

c) *If χ is not the principal character, the L-series $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)/n^s$ has abscissa of convergence $\sigma_c = 0$, hence represents a holomorphic function in the halfplane $H(0)$.*

Proof. a) This follows directly from theorem 6.11 since χ is completely multiplicative.
b) From part a) and the definition of the principal character one gets

$$L(s, \chi_{0m}) = \prod_{p \nmid m} \frac{1}{1 - p^{-s}} = \prod_{p|m} (1 - p^{-s}) \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}}.$$

Since the last product is the Euler product of the zeta function, the assertion follows.
c) By theorem 6.4 it suffices to show that the partial sums $\sum_{n=1}^{N} \chi(n)$ remain bounded as $N \to \infty$. This can be seen as follows: Write $N = qm + r$ with integers q, r, $0 \le r < m$. By theorem 7.3.a) one has $\sum\limits_{n=1}^{qm} \chi(n) = 0$, hence

$$\Big|\sum_{n=1}^{N} \chi(n)\Big| = \Big|\sum_{n=qm+1}^{qm+r} \chi(n)\Big| \le \sum_{n=qm+1}^{qm+r} |\chi(n)| \le \varphi(m), \quad \text{q.e.d.}$$

The next theorem is an analogon of theorem 4.7.

7.7. Theorem. *Let m be an integer ≥ 2 and $\chi : \mathbb{N}_1 \to \mathbb{C}$ a Dirichlet character modulo m. We define the following generalization of the prime zeta function:*

$$P(s,\chi) := \sum_{p\in\mathbb{P}} \frac{\chi(p)}{p^s}.$$

This series converges absolutely in the halfplane $H(1) := \{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$ and one has

$$P(s,\chi) = \log L(s,\chi) + F_\chi(s),$$

where $F_\chi(s)$ is a bounded function in $H(1)$.

Proof. From the Euler product of the L-function we get for $\mathrm{Re}(s) > 1$

$$\begin{aligned} \log L(s,\chi) &= \sum_{p\in\mathbb{P}} \log \frac{1}{1-\chi(p)p^{-s}} = \sum_{p\in\mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi(p)^k}{kp^{ks}} \\ &= \sum_{p\in\mathbb{P}} \frac{\chi(p)}{p^s} + \sum_{k=2}^{\infty} \frac{1}{k} \sum_{p\in\mathbb{P}} \frac{\chi(p)^k}{p^{ks}}. \end{aligned}$$

The theorem follows with

$$F_\chi(s) = -\sum_{k=2}^{\infty} \frac{1}{k} \sum_{p\in\mathbb{P}} \frac{\chi(p)^k}{p^{ks}},$$

since for $\mathrm{Re}(s) > 1$ we have

$$\Big|\sum_{p\in\mathbb{P}} \frac{\chi(p)^k}{p^{ks}}\Big| \leq \sum_{n=2}^{\infty} \frac{1}{n^k} \leq \frac{1}{k-1},$$

hence

$$|F_\chi(s)| \leq \sum_{k=2}^{\infty} \frac{1}{k(k-1)} = 1.$$

8. Primes in Arithmetic Progressions

8.1. Definition (Dirichlet density). For any subset $A \subset \mathbb{P}$ of the set $\mathbb{P}$ of all primes, we define the function

$$P_A(s) := \sum_{p \in A} \frac{1}{p^s}.$$

The sum converges at least for $\mathrm{Re}(s) > 1$ and defines a holomorphic function in the halfplane $H(1) = \{s \in \mathbb{C} : \mathrm{Re}(s) > 1\}$. For $A = \mathbb{P}$ we get the prime zeta function $P(s)$ already discussed in (4.7). If the limit

$$\delta_{\mathrm{Dir}}(A) := \lim_{\sigma \searrow 1} \frac{P_A(\sigma)}{P(\sigma)}$$

exists, it is called the *Dirichlet density* or *analytic density* of the set A. It is clear that, if the Dirichlet density of A exists, one has

$$0 \le \delta_{\mathrm{Dir}}(A) \le 1.$$

The Dirichlet density of the set of all primes is 1, and any finite set of primes has density 0. Hence $\delta_{\mathrm{Dir}}(A) > 0$ implies that A is infinite.
An equivalent definition of the Dirichlet density is

$$\delta_{\mathrm{Dir}}(A) = \lim_{\sigma \searrow 1} P_A(\sigma) \Big/ \log\Big(\frac{1}{\sigma - 1}\Big).$$

This comes from the fact that

$$\lim_{\sigma \searrow 1} P(\sigma)/\log \zeta(\sigma) = 1$$

by theorem 4.7, and

$$\lim_{\sigma \searrow 1} \log \zeta(\sigma) \Big/ \log\Big(\frac{1}{\sigma - 1}\Big) = 1,$$

since $\zeta(s) = 1/(s-1) + (\text{holomorphic function})$.

8.2. Arithmetic progressions. Let m, a be integers, $m \ge 2$. The set of all $n \in \mathbb{N}_1$ with

$$n \equiv a \bmod m$$

is called an arithmetic progression. We want to study the distribution of primes in arithmetic progressions. Clearly if $\gcd(a, m) > 1$, there exist only finitely many primes in the arithmetic progression of numbers congruent $a \bmod m$. So suppose $\gcd(a, m) = 1$. Dirichlet has proved that there exist infinitely many primes $p \equiv a \bmod m$, more

Chap. 8 last revised: 2003-04-14

precisely: The set of all such primes has Dirichlet density $1/\varphi(m)$, which means that the Dirichlet density of primes in all arithmetic progressions $a \bmod m$, $\gcd(a,m) = 1$, is the same. To prove this, we have, according to definition 8.1, to study the functions

$$P_{a,m}(s) := \sum_{p \equiv a \bmod m} \frac{1}{p^s},$$

where the sum is extended over all primes $\equiv a \bmod m$. It was Dirichlet's idea to use instead the functions

$$P(s,\chi) := \sum_{p \in \mathbb{P}} \frac{\chi(p)}{p^s},$$

where $\chi : \mathbb{N}_1 \to \mathbb{C}$ is a Dirichlet character modulo m. These functions were already introduced in theorem 7.7. The relation between the functions $P_{a,m}(s)$ and $P(s,\chi)$ is given by the following lemma.

8.3. Lemma. *Let m be an integer ≥ 2 and a an integer coprime to m. Then we have for all $s \in \mathbb{C}$ with* $\operatorname{Re}(s) > 1$

$$P_{a,m}(s) = \frac{1}{\varphi(m)} \sum_{\chi} \overline{\chi}(a) P(s,\chi).$$

Here the sum is extended over all Dirichlet characters χ modulo m and $\overline{\chi}(a)$ denotes the complex conjugate of $\chi(a)$.

Proof. We have

$$\sum_{\chi} \overline{\chi}(a) P(s,\chi) = \sum_{p \in \mathbb{P}} \Big(\sum_{\chi} \overline{\chi}(a)\chi(p) \Big) \cdot \frac{1}{p^s} = \sum_{p \in \mathbb{P}} \frac{\alpha_p}{p^s},$$

where

$$\alpha_p := \sum_{\chi} \overline{\chi}(a)\chi(p).$$

Since a is coprime to m, there exists an integer b with $ab \equiv 1 \bmod m$, hence $\chi(a)\chi(b) = 1$. On the other hand $|\chi(a)| = 1$, which implies $\chi(b) = \overline{\chi}(a)$. Therefore by theorem 7.3.b)

$$\alpha_p = \sum_{\chi} \chi(b)\chi(p) = \sum_{\chi} \chi(bp) = \begin{cases} \varphi(m) & \text{if } bp \equiv 1 \bmod m, \\ 0 & \text{otherwise.} \end{cases}$$

But $bp \equiv 1 \bmod m$ is equivalent to $p \equiv a \bmod m$, hence

$$\sum_{p \in \mathbb{P}} \frac{\alpha_p}{p^s} = \varphi(m) \sum_{p \equiv a \bmod m} \frac{1}{p^s},$$

which proves the lemma.

In the proof of the Dirichlet theorem on primes in arithmetic progressions, the following theorem plays an essential role.

8.4. Theorem. *Let m be an integer ≥ 2 and χ a non-principal Dirichlet character modulo m. Then*

$$L(1, \chi) \neq 0.$$

Recall that for a non-principal character χ the function $L(s, \chi)$ is holomorphic for $\mathrm{Re}(s) > 0$ (theorem 7.6.c).

Example. For the non-principal character χ_1 modulo 4 one has (cf. 7.4)

$$L(1, \chi_1) = 1 - \frac{1}{3} + \frac{1}{5} + \frac{1}{7} - \frac{1}{9} \pm \ldots = \frac{\pi}{4}.$$

Before we prove this theorem, we show how Dirichlet's theorem can be derived from it.

8.5. Theorem (Dirichlet). *Let a, m be coprime integers, $m \geq 2$. Then the set of all primes $p \equiv a \bmod m$ has Dirichlet density $1/\varphi(m)$.*

Proof. For the principal Dirichlet character χ_{0m} it follows from theorem 7.6.b) that

$$\lim_{\sigma \searrow 1} \log L(\sigma, \chi_{0m}) / \log \zeta(\sigma) = \lim_{\sigma \searrow 1} \log L(\sigma, \chi_{0m}) \Big/ \log\Big(\frac{1}{\sigma - 1}\Big) = 1.$$

On the other hand, if χ is a non-principal character, then we have by theorem 8.4

$$\lim_{\sigma \searrow 1} \log L(\sigma, \chi) \Big/ \log\Big(\frac{1}{\sigma - 1}\Big) = 0.$$

By theorem 7.7 this implies

$$\lim_{\sigma \searrow 1} P(\sigma, \chi_{0m}) \Big/ \log\Big(\frac{1}{\sigma - 1}\Big) = 1$$

and

$$\lim_{\sigma \searrow 1} P(\sigma, \chi) \Big/ \log\Big(\frac{1}{\sigma - 1}\Big) = 0$$

for all non-principal characters χ. Therefore

$$\lim_{\sigma \searrow 1} \Big(\sum_{\chi} \overline{\chi}(a) P(\sigma, \chi) \Big) \Big/ \log\Big(\frac{1}{\sigma - 1}\Big) = \overline{\chi}_{0m}(a) = 1.$$

Now using lemma 8.3 we get

$$\lim_{\sigma \searrow 1} P_{a,m}(\sigma) \Big/ \log\Big(\frac{1}{\sigma - 1}\Big) = \frac{1}{\varphi(m)},$$

which proves our theorem.

8.6. *Proof of theorem 8.4.* We have to show that

$$L(1,\chi) \neq 0$$

for every non-principal Dirichlet character χ modulo m.
Assume to the contrary that there exists at least one non-principal character χ with $L(1,\chi) = 0$. We define the function

$$\zeta_m(s) := \prod_{\chi} L(s,\chi),$$

where the product is extended over *all* Dirichlet characters modulo m. For the principal character the function $L(s,\chi_{0m})$ has a pole of order 1 at $s = 1$. This pole is canceled by the assumed zero of one of the functions $L(s,\chi)$, $\chi \neq \chi_{0m}$. Therefore, under the assumption, ζ_m would be holomorphic everywhere in the halfplane $H(0) = \{s \in \mathbb{C} : \mathrm{Re}(s) > 0\}$. We will show that this leads to a contradiction.
Using the Euler product for the L-functions (theorem 7.6), we get

$$\zeta_m(s) = \prod_{\chi} \prod_{p\in\mathbb{P}} \frac{1}{1-\chi(p)p^{-s}} = \prod_{p\in\mathbb{P}} \frac{1}{\prod_\chi (1-\chi(p)p^{-s})}.$$

By lemma 8.7 below, for every $p \nmid m$ there exist integers $f(p), g(p) \geq 1$ with $f(p)g(p) = \varphi(m)$ such that

$$\prod_{\chi} (1-\chi(p)p^{-s}) = (1-p^{-f(p)s})^{g(p)}.$$

Therefore

$$\frac{1}{\prod_\chi (1-\chi(p)p^{-s})} = \Big(\sum_{k=0}^{\infty} \frac{1}{p^{f(p)ks}}\Big)^{g(p)}$$

is a Dirichlet series with non-negative coefficients and we have

$$\Big(\sum_{k=0}^{\infty} \frac{1}{p^{f(p)ks}}\Big)^{g(p)} \succ \sum_{k=0}^{\infty} \frac{1}{p^{\varphi(m)ks}},$$

where the relation $\sum_n a_n/n^s \succ \sum_n b_n/n^s$ between two Dirichlet series is defined as $a_n \geq b_n$ for all n. It follows that $\zeta_m(s)$ is a Dirichlet series with non-negative coefficients and

$$\zeta_m(s) \succ \prod_{p\nmid m} \Big(\sum_{k=0}^{\infty} \frac{1}{p^{\varphi(m)ks}}\Big) = \sum_{\gcd(n,m)=1} \frac{1}{n^{\varphi(m)s}}.$$

The last Dirichlet series has abscissa of absolute convergence $= 1/\varphi(m)$. Therefore $\sigma_a(\zeta_m) \geq 1/\varphi(m)$. But by the theorem of Landau (6.8) this contradicts the assumption that ζ_m is holomorphic in the halfplane $H(0)$. Therefore the assumption is false, which proves $L(1,\chi) \neq 0$ for all non-principal characters χ.

8.7. Lemma. *Let G be a finite abelian group of order r and let $g \in G$ be an element of order $k \mid r$. Then we have the following identity in the polynomial ring $\mathbb{C}[T]$*

$$\prod_{\chi \in \widehat{G}} (1 - \chi(g)T) = \big(1 - T^k\big)^{r/k}.$$

Proof. Let $H \subset G$ be the subgroup generated by the element g. H is a cyclic group of order k. For every character $\chi \in \widehat{G}$, the restriction $\chi \mid H$ is a character of H. Two characters $\chi_1, \chi_2 \in \widehat{G}$ have the same restriction to H iff the character $\chi := \chi_1\chi_2^{-1}$ is identically 1 on H, which implies that χ induces a character on the quotient group G/H. Since G/H has r/k elements, there can be at most r/k characters of G which restrict to the unit character on H. This means that the restriction of the r characters of G yield at least k different characters of H. But we know that there are exactly k characters of H. Hence every character ψ of H is the restriction of a character of G and there are exactly r/k characters of G which restrict to ψ. Now

$$\prod_{\psi \in \widehat{H}} (1 - \psi(g)T) = \prod_{\nu=0}^{k-1} (1 - e^{2\pi i\nu/k}T) = 1 - T^k$$

and

$$\prod_{\chi \in \widehat{G}} (1 - \chi(g)T) = \Big(\prod_{\psi \in \widehat{H}} (1 - \psi(g)T)\Big)^{r/k} = \big(1 - T^k\big)^{r/k}, \quad \text{q.e.d.}$$

9. The Gamma Function

9.1. Definition. The *Gamma function* is defined for complex z with $\mathrm{Re}(z) > 0$ by the Euler integral

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

Since with $x := \mathrm{Re}(z)$ one has $|t^{z-1}e^{-t}| = t^{x-1}e^{-t}$, the convergence of this integral follows from the corresponding fact in the real case (which we suppose known) and we have the estimate

$$|\Gamma(z)| \le \Gamma(\mathrm{Re}(z)) \quad \text{for } \mathrm{Re}(z) > 0.$$

Since the integrand depends holomorphically on z, it follows further that Γ is holomorphic in the halfplane $H(0) = \{z \in \mathbb{C} : \mathrm{Re}(z) > 0\}$. As in the real case one proves by partial integration the functional equation

$$z\Gamma(z) = \Gamma(z+1),$$

which together with $\Gamma(1) = 1$ shows that $\Gamma(n+1) = n!$ for all $n \in \mathbb{N}_0$. Applying the functional equation $n+1$ times yields

$$\Gamma(z) = \frac{\Gamma(z+n+1)}{z(z+1)\cdot\ldots\cdot(z+n)}.$$

The right hand side of this formula, which was derived for $\mathrm{Re}(z) > 0$, defines a meromorphic function in the halfplane $H(-n-1) = \{z \in \mathbb{C} : \mathrm{Re}(z) > -n-1\}$ having poles of first order at the points $z = -k$, $k = 0, 1, \ldots, n$. Therefore we can use this formula to continue the Gamma function analytically to a meromorphic function in the whole plane $\mathbb{C}$, with poles of first order at $z = -n$, $n \in \mathbb{N}_0$, and holomorphic elsewhere. From now on, by Gamma function we understand this meromorphic function in $\mathbb{C}$.

The Gamma function can be characterized axiomatically as follows:

9.2. Theorem. *Let F be a meromorphic function in $\mathbb{C}$ with the following properties:*

i) *F is holomorphic in the halfplane $H(0) = \{z \in \mathbb{C} : \mathrm{Re}(z) > 0\}$.*

ii) *F satisfies the functional equation $zF(z) = F(z+1)$.*

iii) *F is bounded in the strip $\{z \in \mathbb{C} : 1 \le \mathrm{Re}(z) \le 2\}$.*

Then there exists a constant $c \in \mathbb{C}$ such that

$$F(z) = c\,\Gamma(z).$$

Proof. It is clear that Γ satisfies the properties i) to iii). We set $c := F(1)$ and

$$\Phi(z) := F(z) - c\,\Gamma(z).$$

Chap. 9 last revised: 2001-12-01

Then Φ is also a function satisfying i) to iii) and $\Phi(1) = 0$. From the functional equation $\Phi(z) = \Phi(z+1)/z$ it follows that Φ is holomorphic at $z = 0$ and that Φ is bounded in the strip $\{z \in \mathbb{C} : 0 \leq \mathrm{Re}(z) \leq 1\}$. Therefore the function

$$\varphi(z) := \Phi(z)\Phi(1-z)$$

is bounded in the same strip. We have

$$\varphi(z+1) = \Phi(z+1)\Phi(-z) = z\Phi(z)\Phi(-z) = -\Phi(z)\Phi(-z+1) = -\varphi(z).$$

From this it follows that φ is periodic with period 2 and bounded everywhere, hence holomorphic in $\mathbb{C}$. By the theorem of Liouville φ must be constant. Since $\varphi(1) = -\varphi(0)$, this constant is 0. The equation $0 = \Phi(z)\Phi(1-z)$ shows that also Φ is identically 0, but this means $F(z) = c\,\Gamma(z)$, q.e.d.

9.3. Theorem. a) *For every* $z \in \mathbb{C} \setminus \{n \in \mathbb{Z} : n \leq 0\}$ *we have*

$$\Gamma(z) = \lim_{n\to\infty} \frac{n!\, n^z}{z(z+1)\cdot\ldots\cdot(z+n)}$$

(Gauß representation of the Gamma function)

b) $1/\Gamma$ *is an entire holomorphic function with product representation*

$$\frac{1}{\Gamma(z)} = e^{Cz} z \prod_{n=1}^{\infty}\Big(1+\frac{z}{n}\Big)e^{-z/n}, \qquad (C = \text{Euler-Mascheroni constant}).$$

This product converges normally in $\mathbb{C}$.

Proof.

9.4. Lemma. *Let* $f : \mathbb{C} \to \mathbb{C}$ *be an entire holomorphic function and let* $\rho, C, R_0 \in \mathbb{R}_+$ *be non-negative constants such that*

$$\mathrm{Re}(f(z)) \leq C|z|^\rho \quad \text{for } |z| \geq R_0.$$

Then f *is a polynomial of degree* $\leq \rho$.

Note that no lower bound for $\mathrm{Re}(f(z))$ is required.

Proof. The Taylor series $f(z) = \sum_{n=0}^\infty a_n z^n$ converges for all $z \in \mathbb{C}$. Setting $z = Re^{it}$, we get Fourier series

$$f(Re^{it}) = \sum_{n=0}^{\infty} a_n R^n e^{int} \quad \text{and} \quad \overline{f(Re^{it})} = \sum_{n=0}^{\infty} \overline{a}_n R^n e^{-int},$$

hence

$$\mathrm{Re}(f(Re^{it})) = \mathrm{Re}(a_0) + \tfrac{1}{2}\sum_{n=1}^{\infty} R^n(a_n e^{int} + \overline{a}_n e^{-int}).$$

Multiplying this equation by e^{-ikt} and integrating from 0 to 2π yields

$$a_k = \frac{1}{\pi R^k} \int_0^{2\pi} \operatorname{Re}\left(f(Re^{it})\right) e^{-ikt} dt \quad \text{for } k > 0$$

and (for $k = 0$)

$$\operatorname{Re}(a_0) = \frac{1}{2\pi} \int_0^{2\pi} \operatorname{Re}\left(f(Re^{it})\right) dt.$$

The hypothesis on the growth of $\operatorname{Re}(f(z))$ implies

$$|\operatorname{Re}(f(z))| \le 2C|z|^\rho - \operatorname{Re}(f(z)) \quad \text{for } |z| \ge R_0,$$

(note this is true also if $\operatorname{Re}(f(z)) < 0$). Therefore we get the estimate

$$|a_k| \le \frac{1}{\pi R^k} \int_0^{2\pi} \left|\operatorname{Re}(f(re^{it}))\right| dt \le \frac{1}{R^k} \left(4CR^\rho - 2\operatorname{Re}(a_0)\right).$$

Letting $R \to \infty$, we see that $a_k = 0$ for $k > \rho$, q.e.d.

9.5. Theorem. *The Gamma function satisfies the following relations:*

a) $$\frac{1}{\Gamma(z)\Gamma(1-z)} = \frac{\sin(\pi z)}{\pi},$$

b) $$\Gamma\left(\frac{z}{2}\right)\Gamma\left(\frac{z+1}{2}\right) = 2^{1-z}\sqrt{\pi}\,\Gamma(z).$$

Example. Setting $z = \frac{1}{2}$ in formula a) yields

$$\Gamma(\tfrac{1}{2}) = \sqrt{\pi}.$$

The same result can also be obtained from formula b) for $z = 1$.

Proof. a) We first consider the meromorphic function

$$\Phi(z) := \Gamma(z)\Gamma(1-z).$$

It has poles of order 1 at the points $z = n$, $n \in \mathbb{Z}$, and is holomorphic elsewhere. It satisfies the relations

$$\Phi(z+1) = -\Phi(z) \quad \text{and} \quad \Phi(-z) = -\Phi(z).$$

Since $\Gamma(z)$ is bounded on $1 \le \operatorname{Re}(z) \le 2$ and

$$\Gamma(z) = \frac{\Gamma(1+z)}{z}, \quad \Gamma(1-z) = \frac{\Gamma(2-z)}{(1-z)},$$

it follows that Φ is bounded on the set

$$S_1 := \{z \in \mathbb{C} : 0 \le \mathrm{Re}(z) \le 1,\ |\mathrm{Im}(z)| \ge 1\}.$$

As $\sin(\pi z)$ has zeroes of order 1 at $z = n$, $n \in \mathbb{Z}$, the product

$$F(z) := \sin(\pi z)\Phi(z) = \sin(\pi z)\Gamma(z)\Gamma(1-z)$$

is holomorphic everywhere in $\mathbb{C}$ and without zeroes. We can write

$$F(z) = \frac{\sin(\pi z)}{z}\,\Gamma(1+z)\Gamma(1-z),$$

hence $F(0) = \pi$. Furthermore F is periodic with period 1 and an even function, i.e. $F(-z) = F(z)$. From the boundedness of Φ on S_1 we get an estimate

$$|F(z)| \le Ce^{\pi|z|} \quad \text{for } z \in S_1 \text{ and some constant } C > 0.$$

Since F is continuous and periodic, such an estimate holds in the whole plane $\mathbb{C}$. We can write F as $F(z) = e^{f(z)}$ with some holomorphic function $f : \mathbb{C} \to \mathbb{C}$. From $|F(z)| = e^{\mathrm{Re}(z)}$ we get an estimate

$$\mathrm{Re}(f) \le C'|z| \quad \text{for } |z| \ge R_0 \text{ and some constant } C' > 0.$$

By lemma 9.4, f must be a linear polynomial, hence

$$F(z) = e^{a+bz}, \quad (a, b \in \mathbb{C}).$$

Since F is an even function, we have $b = 0$, so the function F is a constant, which must be $F(0) = \pi$. This proves part a) of the theorem.

b) This is proved by applying theorem 9.2 to the function

$$F(z) := 2^z\,\Gamma\Big(\frac{z}{2}\Big)\Gamma\Big(\frac{z+1}{2}\Big).$$

...

9.6. Corollary (Sine product). *For all $z \in \mathbb{C}$ one has*

$$\sin(\pi z) = \pi z \prod_{n=1}^{\infty}\Big(1 - \frac{z^2}{n^2}\Big).$$

9.7. Corollary (Wallis product).

a) $$\frac{\pi}{2} = \prod_{n=1}^{\infty} \frac{(2n)^2}{(2n-1)(2n+1)},$$

b) $$\sqrt{\pi} = \lim_{n\to\infty} \frac{1}{\sqrt{n}} \cdot \frac{2^{2n}(n!)^2}{(2n)!}.$$

Proof. Formula a) follows directly from the sine product with $z = \frac{1}{2}$.
To prove formula b), we rewrite a) as

$$\begin{aligned}\pi &= 2 \lim_{n\to\infty} \prod_{k=1}^{n} \frac{(2k)^2}{(2k-1)(2k+1)} \\ &= \lim_{n\to\infty} \frac{2}{2n+1} \cdot \frac{2^{2n}(n!)^2}{1\cdot 3\cdot 3\cdot 5\cdot 5\cdot \ldots \cdot (2n-1)(2n-1)}\end{aligned}$$

hence

$$\begin{aligned}\sqrt{\pi} &= \lim_{n\to\infty} \sqrt{\frac{2}{2n+1}} \cdot \frac{2^n n!}{1\cdot 3\cdot 5\cdot \ldots \cdot (2n-1)} \\ &= \lim_{n\to\infty} \sqrt{\frac{2}{2n+1}} \cdot \frac{2^{2n}(n!)^2}{(2n)!}.\end{aligned}$$

Since $\lim\limits_{n\to\infty} \sqrt{2n}/\sqrt{2n+1} = 1$, the assertion follows.

9.8. Theorem (Stirling formula). *We have the following asymptotic relation*

$$n! \sim \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n.$$

Proof. We apply the Euler-Maclaurin summation formula to

$$\log(n!) = \sum_{k=1}^{n} \log k$$

and obtain

$$\begin{aligned}\log(n!) &= \tfrac{1}{2}\log n + \int_1^n \log x\,dx + \int_1^n \frac{\mathrm{saw}(x)}{x}\,dx \\ &= \tfrac{1}{2}\log n + n(\log n - 1) + 1 + \int_1^n \frac{\mathrm{saw}(x)}{x}\,dx.\end{aligned}$$

Taking the exponential function of both sides we get

$$n! = \sqrt{n}\Big(\frac{n}{e}\Big)^n e^{\alpha_n},$$

where

$$\alpha_n = 1 + \int_1^n \frac{\mathrm{saw}(x)}{x}\,dx = 1 + \frac{B_2}{2}\cdot\frac{1}{x}\Big|_1^n + \int_1^n \frac{\widetilde{B}_2(x)}{2}\cdot\frac{1}{x^2}\,dx.$$

This last representation shows that

$$\alpha := \lim_{n\to\infty} \alpha_n = 1 + \int_1^\infty \frac{\operatorname{saw}(x)}{x}\,dx$$

exists and we have the asymptotic relation

$$n! \sim \sqrt{n}\Big(\frac{n}{e}\Big)^n e^\alpha.$$

It remains to prove that $e^\alpha = \sqrt{2\pi}$. This can be done as follows. Dividing the asymptotic relations

$$(n!)^2 \sim n\Big(\frac{n}{e}\Big)^{2n} e^{2\alpha} \qquad \text{and} \qquad (2n)! \sim \sqrt{2n}\Big(\frac{2n}{e}\Big)^{2n} e^\alpha$$

yields

$$e^\alpha = \lim_{n\to\infty} \frac{(n!)^2 e^{2n}}{n^{2n+1}} \cdot \frac{(2n)^{2n+1/2}}{(2n)!e^{2n}} = \lim_{n\to\infty} \frac{(n!)^2 \cdot 2^{2n+1/2}}{(2n)!\sqrt{n}} = \lim_{n\to\infty} \sqrt{\frac{2}{n}} \cdot \frac{2^{2n}(n!)^2}{(2n)!}.$$

Now corollary 9.7 shows $e^\alpha = \sqrt{2\pi}$, q.e.d.

For later use we note that we have hereby proved

$$1 + \int_1^\infty \frac{\operatorname{saw}(x)}{x}\,dx = \log\sqrt{2\pi}.$$

9.9. Theorem (Asymptotic expansion of the Gamma function). *For every integer $r \geq 1$ and every $z \in \mathbb{C} \smallsetminus \{x \in \mathbb{R} : x \leq 0\}$ one has*

$$\begin{aligned}\log\Gamma(z) \;&=\; (z - \tfrac{1}{2})\log z - z + \log\sqrt{2\pi} + \sum_{k=1}^r \frac{B_{2k}}{(2k-1)2k} \cdot \frac{1}{z^{2k-1}} \\ &\quad + \int_0^\infty \frac{\widetilde{B}_{2r}(t)}{2r} \cdot \frac{1}{(z+t)^{2r}}\,dt.\end{aligned}$$

Here $\log\Gamma(z)$ and $\log z$ are those branches of the logarithm which take real values for positive real arguments.

Example. For $r = 5$, the value of the sum is

$$\sum_{k=1}^5 \frac{B_{2k}}{(2k-1)2k} \cdot \frac{1}{z^{2k-1}} = \frac{1}{12z} - \frac{1}{360z^3} + \frac{1}{1260z^5} - \frac{1}{1680z^7} + \frac{1}{1188z^9}$$

Proof. We use the Gauß representation of the Gamma function (theorem 9.3.a) and get

$$\log\Gamma(z) = \lim_{n\to\infty}\Big(z\log n + \sum_{k=1}^n \log k - \sum_{k=0}^n \log(z+k)\Big).$$

By Euler-Maclaurin (theorem 5.2)

$$\begin{aligned}\sum_{k=1}^{n} \log k &= \tfrac{1}{2}\log n + \int_1^n \log t\,dt + \int_1^n \frac{\operatorname{saw}(t)}{t}dt \\ &= \tfrac{1}{2}\log n + n\log n - n + 1 + \int_1^n \frac{\operatorname{saw}(t)}{t}dt\end{aligned}$$

and

$$\begin{aligned}\sum_{k=0}^{n} \log(z+k) &= \tfrac{1}{2}(\log z + \log(z+n)) + \int_0^n \log(z+t)dt + \int_0^n \frac{\operatorname{saw}(t)}{z+t}dt \\ &= \tfrac{1}{2}(\log z + \log(z+n)) + (z+n)\log(z+n) - z\log z - n \\ &\quad + \int_0^n \frac{\operatorname{saw}(t)}{z+t}dt.\end{aligned}$$

Therefore

$$\begin{aligned}&z\log n + \sum_{k=1}^{n}\log k - \sum_{k=0}^{n}\log(z+k) \\ &= (z-\tfrac{1}{2})\log z - (z+n+\tfrac{1}{2})\log\left(1+\frac{z}{n}\right) + 1 \\ &\quad + \int_1^n \frac{\operatorname{saw}(t)}{t}dt - \int_0^n \frac{\operatorname{saw}(t)}{z+t}dt.\end{aligned}$$

Since

$$\lim_{n\to\infty}(z+n+\tfrac{1}{2})\log\left(1+\frac{z}{n}\right) = z$$

and

$$\lim_{n\to\infty}\left(1+\int_1^n \frac{\operatorname{saw}(t)}{t}dt\right) = \log\sqrt{2\pi} \quad \text{(see above)},$$

we get

$$\log\Gamma(z) = (z-\tfrac{1}{2})\log z - z + \log\sqrt{2\pi} - \int_0^\infty \frac{\operatorname{saw}(t)}{z+t}dt.$$

The rest is proved as in theorem 5.11.

10. Functional Equation of the Zeta Function

10.1. Theorem (Functional equation of the theta function).
The theta series is defined for real $x > 0$ by

$$\theta(x) := \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x}.$$

It satisfies the following functional equation

$$\theta\Big(\frac{1}{x}\Big) = \sqrt{x}\theta(x) \qquad \text{for all } x > 0,$$

i.e.

$$\sum_{n\in\mathbb{Z}} e^{-\pi n^2 x} = \frac{1}{\sqrt{x}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/x}.$$

Remarks. a) The theta series, as well as its derivatives, converge uniformly on every interval $[\varepsilon, \infty[$, $\varepsilon > 0$; hence θ is a $\mathcal{C}^\infty$-function on $]0, \infty[$.
b) In the theory of elliptic functions one defines more general theta functions of two complex variables. For $\tau \in \mathbb{C}$ with $\mathrm{Im}(\tau) > 0$ and $z \in \mathbb{C}$ one sets

$$\vartheta(\tau, z) := \sum_{n\in\mathbb{Z}} e^{i\pi n^2 \tau} e^{2\pi i n z}.$$

For fixed τ this is an entire holomorphic function in z, which can be used to construct doubly periodic functions with respect to the lattice $\mathbb{Z} + \mathbb{Z}\tau$. As a function of τ, it is holomorphic in the upper halfplane. The relation to the theta series of theorem 10.1 is

$$\theta(t) = \vartheta(it, 0).$$

Proof. For fixed $x > 0$, we consider the function $F : \mathbb{R} \to \mathbb{R}$,

$$F(t) := \sum_{n\in\mathbb{Z}} e^{-\pi(n-t)^2 x}.$$

The series converges uniformly on $\mathbb{R}$ together with all its derivatives, hence represents a $\mathcal{C}^\infty$-function on $\mathbb{R}$. It is periodic with period 1, i.e. $F(t + 1) = F(t)$ for all $t \in \mathbb{R}$. Therefore we can expand F as a uniformly convergent Fourier series

$$F(t) = \sum_{n\in\mathbb{Z}} c_n e^{2\pi i n t}$$

where the coefficients c_n are the integrals

$$c_n = \int_0^1 F(t) e^{-2\pi i n t} dt = \sum_{k\in\mathbb{Z}} \int_0^1 e^{-\pi(k-t)^2 x} e^{-2\pi i n t} dt.$$

Now $\int_0^1 e^{-\pi(k-t)^2 x} e^{-2\pi i n t} dt = \int_k^{k+1} e^{-\pi t^2 x} e^{-2\pi i n t} dt$ (substitution $\tilde{t} = t - k$), hence

$$c_n = \int_{-\infty}^{\infty} e^{-\pi t^2 x} e^{-2\pi i n t} dt.$$

For $n = 0$ this is the well known integral of the Gauss bell curve

$$\begin{aligned} c_0 &= \int_{-\infty}^{\infty} e^{-\pi t^2 x} dt = 2\int_0^{\infty} e^{-\pi t^2 x} dt = \frac{2}{\sqrt{\pi x}} \int_0^{\infty} e^{-t^2} dt \\ &= \frac{1}{\sqrt{\pi x}} \int_0^{\infty} u^{-1/2} e^{-u} du = \frac{1}{\sqrt{\pi x}} \Gamma\Big(\frac{1}{2}\Big) = \frac{1}{\sqrt{x}}. \end{aligned}$$

For general n we write

$$-\pi t^2 x - 2\pi i n t = -\pi\Big(t\sqrt{x} + \frac{in}{\sqrt{x}}\Big)^2 - \frac{\pi n^2}{x}.$$

This leads to

$$c_n = e^{-\pi n^2/x} \int_{-\infty}^{\infty} e^{-\pi(t\sqrt{x} + in/\sqrt{x})^2} dt.$$

We will prove

$$\int_{-\infty}^{\infty} e^{-\pi(t\sqrt{x} + in/\sqrt{x})^2} dt = \frac{1}{\sqrt{x}} \int_{-\infty}^{\infty} e^{-\pi t^2} dt = \frac{1}{\sqrt{x}}. \tag{$*$}$$

Assuming this for a moment, we get

$$F(t) = \frac{1}{\sqrt{x}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/x} e^{2\pi i n t}.$$

Setting $t = 0$, it follows

$$F(0) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x} = \frac{1}{\sqrt{x}} \sum_{n\in\mathbb{Z}} e^{-\pi n^2/x},$$

which is the assertion of the theorem.

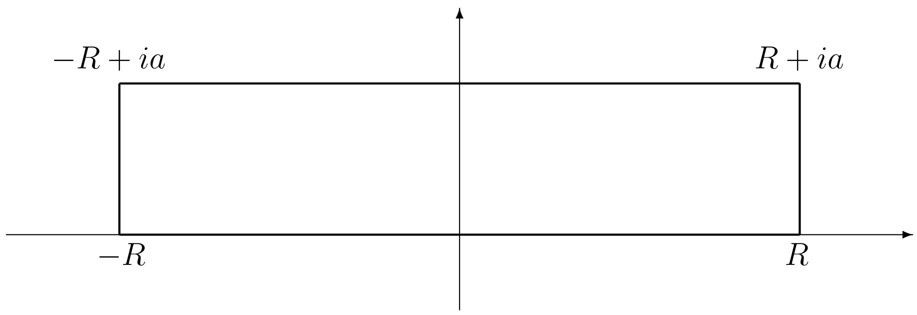
It remains to prove the formula $(*)$. Using the substitution $\tilde{t} = t\sqrt{x}$ we see that

$$\int_{-\infty}^{\infty} e^{-\pi(t\sqrt{x} + in/\sqrt{x})^2} dt = \frac{1}{\sqrt{x}} \int_{-\infty}^{\infty} e^{-\pi(t + in/\sqrt{x})^2} dt$$

With the abbreviation $a := n/\sqrt{x}$ we have to show that

$$\int_{-\infty}^{\infty} e^{-\pi(t+ia)^2} dt = \int_{-\infty}^{\infty} e^{-\pi t^2} dt. \tag{$**$}$$

To this end we integrate the holomorphic function $f(z) := e^{-\pi z^2}$ over the boundary of the rectangle with corners $-R, R, R + ia, -R + ia$, where R is a positive real number.



By the residue theorem the whole integral is zero, hence

$$\int_{-R}^{R} f(z)dz = \int_{-R+ia}^{R+ia} f(z)dz - \int_{R}^{R+ia} f(z)dz + \int_{-R}^{-R+ia} f(z)dz$$

Now

$$\begin{aligned}
\int_{-R}^{R} f(z)dz &= \int_{-R}^{R} e^{-\pi t^2} dt, \\
\int_{-R+ia}^{R+ia} f(z)dz &= \int_{-R}^{R} e^{-\pi(t+ia)^2} dt, \\
\int_{\pm R}^{\pm R+ia} f(z)dz &= i\int_0^a e^{-\pi(R^2-t^2)\mp 2\pi iRt} dt = ie^{-\pi R^2}\int_0^a e^{\pi t^2 \mp 2\pi iRt} dt.
\end{aligned}$$

We have the estimate

$$\Big|\int_{\pm R}^{\pm R+ia} f(z)dz\Big| \leq e^{-\pi R^2}|a|e^{\pi|a|^2},$$

which tends to 0 as $R \to \infty$. This implies

$$\lim_{R\to\infty}\int_{-R}^{R} e^{-\pi t^2} dt = \lim_{R\to\infty}\int_{-R}^{R} e^{-\pi(t+ia)^2} dt,$$

which proves $(**)$ and therefore $(*)$. This completes the proof of the functional equation of the theta function.

10.2. Corollary. *The theta function* $\theta(x) := \sum_{n\in\mathbb{Z}} e^{-\pi n^2 x}$ *defined in the preceding theorem satifies*

$$\theta(x) = O\Big(\frac{1}{\sqrt{x}}\Big) \quad \text{as } x \searrow 0.$$

10.3. Proposition. *For all* $s \in \mathbb{C}$ *with* $\mathrm{Re}(s) > 1$ *one has*

$$\Gamma\Big(\frac{s}{2}\Big)\zeta(s) = \pi^{s/2}\int_0^\infty t^{s/2}\Big(\sum_{n=1}^{\infty} e^{-\pi n^2 t}\Big)\frac{dt}{t}.$$

Remark. The function

$$\psi(t) := \sum_{n=1}^{\infty} e^{-\pi n^2 t}$$

decreases exponentially as $t \to \infty$. One has $\theta(t) = 1 + 2\psi(t)$, hence $\psi(t) = \frac{1}{2}(\theta(t) - 1)$, so corollary 10.2 implies

$$\psi(t) = O\Big(\frac{1}{\sqrt{t}}\Big) \qquad \text{for } t \searrow 0.$$

This shows that the integral exists for $\mathrm{Re}(s) > 1$.

Proof. We start with the Euler integral for $\Gamma(s/2)$,

$$\Gamma\Big(\frac{s}{2}\Big) = \int_0^\infty t^{s/2} e^{-t} \frac{dt}{t},$$

and apply the substitution $\tilde{t} = \pi n^2 t$, where $n \in \mathbb{N}_1$. Since $d\tilde{t}/\tilde{t} = dt/t$, we get

$$\Gamma\Big(\frac{s}{2}\Big) = n^s \pi^{s/2} \int_0^\infty t^{s/2} e^{-\pi n^2 t} \frac{dt}{t}.$$

For $\mathrm{Re}(s) > 1$ we have

$$\begin{aligned}
\Gamma\Big(\frac{s}{2}\Big)\zeta(s) &= \sum_{n=1}^{\infty} \Gamma\Big(\frac{s}{2}\Big)\frac{1}{n^s} = \sum_{n=1}^{\infty} \pi^{s/2} \int_0^\infty t^{s/2} e^{-\pi n^2 t} \frac{dt}{t} \\
&= \pi^{s/2} \int_0^\infty t^{s/2} \Big(\sum_{n=1}^{\infty} e^{-\pi n^2 t}\Big) \frac{dt}{t}.
\end{aligned}$$

The interchange of summation and integration is allowed by the theorem of majorized convergence for Lebesgue integrals.

10.4. Theorem (Functional equation of the zeta function).
a) *The function*

$$\xi(s) := \pi^{-s/2}\, \Gamma(s/2)\, \zeta(s),$$

which is a meromorphic function in $\mathbb{C}$, satisfies the functional equation

$$\xi(1-s) = \xi(s).$$

b) *For the zeta function itself one has*

$$\zeta(1-s) = 2^{1-s} \pi^{-s}\, \Gamma(s) \cos(\tfrac{\pi s}{2})\, \zeta(s).$$

Proof. By the preceding theorem

$$\xi(s) = \int_0^\infty t^{s/2}\psi(t)\frac{dt}{t} \quad \text{with} \quad \psi(t) = \sum_{n=1}^\infty e^{-\pi n^2 t}.$$

The functional equation of the theta function implies for $\psi(t) = \frac{1}{2}(\theta(t) - 1)$

$$\psi(t) = t^{-1/2}\psi(1/t) - \tfrac{1}{2}(1 - t^{-1/2}).$$

We substitute this expression in the integral from 0 to 1:

$$\int_0^1 t^{s/2}\psi(t)\frac{dt}{t} = \int_0^1 t^{(s-1)/2}\psi\Big(\frac{1}{t}\Big)\frac{dt}{t} + \tfrac{1}{2}\int_0^1 (t^{(s-1)/2} - t^{s/2})\frac{dt}{t}.$$

The last integral can be evaluated explicitly (recall that $\mathrm{Re}(s) > 1$):

$$\tfrac{1}{2}\int_0^1 (t^{(s-1)/2} - t^{s/2})\frac{dt}{t} = \frac{1}{s-1} - \frac{1}{s}.$$

For the first integral on the right hand side we use the substitution $\tilde{t} = 1/t$ and obtain

$$\int_0^1 t^{(s-1)/2}\psi\Big(\frac{1}{t}\Big)\frac{dt}{t} = \int_1^\infty t^{(1-s)/2}\psi(t)\frac{dt}{t}.$$

Putting everything together we get

$$\xi(s) = \int_0^\infty t^{s/2}\psi(t)\frac{dt}{t} = \int_1^\infty \big(t^{(1-s)/2} + t^{s/2}\big)\,\psi(t)\frac{dt}{t} + \Big(\frac{1}{s-1} - \frac{1}{s}\Big).$$

The integral on the right hand side converges for all $s \in \mathbb{C}$ to a holomorphic function in $\mathbb{C}$. Thus we have got a representation of the function $\xi(s)$ valid in the whole plane. This representation is invariant under the map $s \mapsto 1-s$, proving $\xi(1-s) = \xi(s)$, i.e. part a) of the theorem.

To prove part b), we use the equation we just proved:

$$\pi^{-(1-s)/2}\Gamma\Big(\frac{1-s}{2}\Big)\,\zeta(1-s) = \pi^{-s/2}\Gamma\Big(\frac{s}{2}\Big)\,\zeta(s),$$

yielding

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

By theorem 9.5.a) we have

$$\Gamma\Big(\frac{1-s}{2}\Big)\Gamma\Big(\frac{1+s}{2}\Big) = \frac{\pi}{\sin(\pi\frac{1+s}{2})} = \frac{\pi}{\cos(\frac{\pi s}{2})},$$

therefore

$$\zeta(1-s) = \pi^{-1/2-s}\Gamma\Big(\frac{s}{2}\Big)\Gamma\Big(\frac{1+s}{2}\Big)\cos(\tfrac{\pi s}{2})\,\zeta(s).$$

Now by theorem 9.5.b)

$$\Gamma\Big(\frac{s}{2}\Big)\Gamma\Big(\frac{1+s}{2}\Big) = 2^{1-s}\sqrt{\pi}\,\Gamma(s),$$

which implies

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\Gamma(s)\cos(\tfrac{\pi s}{2})\,\zeta(s), \qquad \text{q.e.d.}$$

10.5. Corollary. a) *For every integer $k > 0$*

$$\zeta(-2k) = 0.$$

These are the only zeroes of the zeta function in the halfplane $\mathrm{Re}(s) < 0$.

b) $\qquad \zeta(0) = -\frac{1}{2}$.

c) *For every integer $k > 0$*

$$\zeta(1-2k) = -\frac{B_{2k}}{2k}.$$

Proof. a) We use the functional equation

$$\zeta(1-s) = 2^{1-s}\pi^{-s}\Gamma(s)\cos\tfrac{\pi s}{2}\,\zeta(s)$$

$\mathrm{Re}(1-s) < 0$ is equivalent to $\mathrm{Re}(s) > 1$. Since $\zeta(s) \neq 0$ for $\mathrm{Re}(s) > 1$ (theorem 4.5), the only zeroes of the right hand side for $\mathrm{Re}(s) > 1$ come from the cosine function. Now

$$\cos\tfrac{\pi s}{2} = 0 \quad \iff \quad s = 1 + 2k \quad \text{with } k \in \mathbb{Z}$$

This implies assertion a)

c) From the functional equation we get

$$\zeta(1-2k) = 2^{1-2k}\pi^{-2k}\Gamma(2k)\cos(\pi k)\zeta(2k) = \frac{2}{(2\pi)^{2k}}(2k-1)!\,(-1)^k\zeta(2k).$$

By theorem 5.8.ii)

$$\zeta(2k) = (-1)^{k-1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k}.$$

Substituting this in the equation above yields

$$\zeta(1-2k) = -\frac{B_{2k}}{2k}.$$

b) We write the functional equation in the form $\zeta(1-s) = f_1(s)f_2(s)$ with

$$f_1(s) := 2^{1-s}\pi^{-s}\Gamma(s) \quad \text{and} \quad f_2(s) := \cos\tfrac{\pi s}{2}\,\zeta(s).$$

f_1 is holomorphic in a neighborhood of $s = 1$ and $f_1(1) = 1/\pi$. The function f_2 is likewise holomorphic in a neighborhood of $s = 1$, since the pole of the zeta function is cancelled by the zero of the cosine. To calculate $f_2(1)$, we determine the first terms of the Taylor resp. Laurent expansions of the factors.

$$\begin{aligned}\cos\tfrac{\pi s}{2} &= \cos\left(\tfrac{\pi}{2}(s-1)+\tfrac{\pi}{2}\right) = -\sin\left(\tfrac{\pi}{2}(s-1)\right) = -\tfrac{\pi}{2}(s-1) + O((s-1)^3),\\ \zeta(s) &= \frac{1}{s-1} + (\text{holomorphic function}).\end{aligned}$$

Multiplying both expressions yields $f_2(s) = -\frac{\pi}{2} + O(s-1)$, hence $f_2(1) = -\frac{\pi}{2}$. Therefore

$$\zeta(0) = f_1(1)f_2(1) = -\tfrac{1}{2}, \quad \text{q.e.d.}$$

10.6. Theorem. *For all $t \in \mathbb{R}$*

$$\zeta(1+it) \neq 0.$$

Proof. We use the inequality

$$3 + 4\cos t + \cos 2t \geq 0 \qquad \text{for all } t \in \mathbb{R}.$$

This is proved as follows: Since $\cos 2t = \cos^2 t - \sin^2 t = 2\cos^2 t - 1$, we have

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

Let now $s = \sigma + it$ be a complex number with $\mathrm{Re}(s) = \sigma > 1$. Then

$$\log\zeta(s) = \sum_{p\in\mathbb{P}} \log\frac{1}{1-p^{-s}} = \sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}\frac{1}{k}\cdot\frac{1}{p^{ks}} = \sum_{n=1}^{\infty}\frac{a_n}{n^s},$$

where

$$a_n = \begin{cases} 1/k, & \text{if } n = p^k \text{ for some prime } p,\\ 0 & \text{otherwise.}\end{cases}$$

Since $\log|z| = \mathrm{Re}(\log z)$ for every $z \in \mathbb{C}^*$,

$$\log|\zeta(s)| = \sum_{n=1}^{\infty} a_n \mathrm{Re}(n^{-s}) = \sum_{n=1}^{\infty}\frac{a_n}{n^\sigma}\cos(t\log n).$$

Using a trick of v. Mangoldt (1895) we form the expression

$$\log\Big(|\zeta(\sigma)|^3|\zeta(\sigma+it)|^4|\zeta(\sigma+2it)|\Big)$$
$$= \sum_{n=1}^{\infty}\frac{a_n}{n^\sigma}\Big(\underbrace{3+4\cos(t\log n)+\cos(2t\log n)}_{\geq 0}\Big) \geq 0.$$

Therefore

$$\big|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)\big| \geq 1 \quad \text{for all } \sigma>1 \text{ and } t\in\mathbb{R}.$$

Assume that $\zeta(1+it)=0$ for some $t\neq 0$. Then the function $s\mapsto\zeta(s)^3\zeta(s+it)^4$ has a zero at $s=1$, since the pole of order 3 of the function $\zeta(s)^3$ is compensated by the zero of order ≥ 4 of the function $\zeta(s+it)^4$. Therefore

$$\lim_{\sigma\searrow 1}\big|\zeta(\sigma)^3\zeta(\sigma+it)^4\zeta(\sigma+2it)\big| = 0,$$

contradicting the above estimate. Hence the assumption is false, which proves the theorem.

10.7. Riemann Hypothesis. It follows from theorem 10.6 and the functional equation that $\zeta(s)\neq 0$ for all $s\in\mathbb{C}$ with $\mathrm{Re}(s)=0$. Therefore, besides the trivial zeroes of the zeta function at $s=-2k$, $k\in\mathbb{N}_1$, all other zeroes of the zeta function must satisfy $0<\mathrm{Re}(s)<1$. It was conjectured by Riemann in 1859 that all non-trivial zeroes of the zeta function actually have $\mathrm{Re}(s)=\frac{1}{2}$. This is the famous Riemann hypothesis which is still unproven today.

11. The Chebyshev Functions Theta and Psi

11.1. Definition (Prime number function). For real $x > 0$ we denote by $\pi(x)$ the number of all primes $p \le x$. This can be also written as

$$\pi(x) = \sum_{p \leqslant x} 1.$$

$\pi(x)$ is a step function with jumps of height 1 at all primes. Of course $\pi(x) = 0$ for all $x < 2$. Some other values are

x	10	100	1000	10^4	10^5	10^6	10^7
$\pi(x)$	4	25	168	1229	9592	78498	664579

The prime number theorem, which we will prove in chapter 13, describes the asymptotic behavior of $\pi(x)$ for $x \to \infty$, namely

$$\pi(x) \sim \frac{x}{\log x},$$

meaning that the quotient $\pi(x)/\frac{x}{\log x}$ converges to 1 for $x \to \infty$. For the proof of the prime number theorem, some other functions, introduced by Chebyshev, are useful.

11.2. Definition (Chebyshev theta function). This function is defined for real $x > 0$ by

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

(Of course this has nothing to do with the theta series and theta functions considered in the previous chapter.)

We will see that the prime number theorem is equivalent to the fact that the asymptotic behavior of the Chebyshev theta function is $\vartheta(x) \sim x$ for $x \to \infty$.

A first rough estimate is given by the following proposition.

11.3. Proposition. *For all $x > 0$ one has*

$$\vartheta(x) < x \log 4,$$

in particular $\vartheta(x) = O(x)$ for $x \to \infty$.

Proof. Of course it suffices to prove the assertion for $x = n \in \mathbb{N}_1$. The assertion is equivalent to

$$F(n) := \prod_{p \leqslant n} p \;<\; 4^n.$$

Chap. 11 last revised: 2003-04-14

We will prove this by induction on n. It is obviously true for $n \le 3$.

For the induction step let $N \ge 4$ and assume that the assertion is true for all integers $n < N$.

First case: N even. Obviously $F(N) = F(N-1)$. For $F(N-1)$ we can use the induction hypothesis and obtain $F(N) = F(N-1) < 4^{N-1} < 4^N$.

Second case: N odd. We write N as $N = 2n+1$. Consider the binomial coefficient

$$\binom{2n+1}{n} = \frac{(2n+1)\cdot 2n\cdot(2n-1)\cdot\ldots\cdot(n+2)}{1\cdot 2\cdot 3\cdot\ldots\cdot n}.$$

Clearly, for every prime p with $n+2 \le p \le 2n+1$ one has

$$p \,\Big|\, \binom{2n+1}{n},$$

hence

$$\prod_{n+1<p\leqslant 2(n+1)} p \;\le\; \binom{2n+1}{n}.$$

Now $\binom{2n+1}{n} = \binom{2n+1}{n+1}$ are the two central terms in the binomial expansion of $(1+1)^{2n+1}$, therefore

$$\binom{2n+1}{n} < \tfrac{1}{2}(1+1)^{2n+1} = 4^n.$$

By induction hypothesis $\prod\limits_{p\leqslant n+1} p < 4^{n+1}$, hence

$$F(2n+1) = \prod_{p\leqslant 2n+1} p \;<\; 4^{n+1}\binom{2n+1}{n} < 4^{n+1}4^n = 4^{2n+1}, \qquad \text{q.e.d.}$$

11.4. Lemma (Abel summation II). *Let n_0 be an integer, $(a_n)_{n\geqslant n_0}$ a sequence of complex numbers and $A : [n_0,\infty[\, \to \mathbb{C}$ the function defined by*

$$A(x) := \sum_{n_0\leqslant n\leqslant x} a_n.$$

Further let $f : [n_0,\infty[\, \to \mathbb{C}$ be a continuously differentiable function. Then for all real $x \ge n_0$ the following formula holds

$$\sum_{n_0\leqslant k\leqslant x} a_k f(k) = A(x)f(x) - \int_{n_0}^{x} A(t)f'(t)dt.$$

Proof. We consider first the case when $x = n$ is an integer and prove the formula by induction on n. For $n = n_0$ both sides are equal to $a_{n_0}f(n_0)$.

Induction step $n \to n+1$. Denoting by $L(x)$ the left hand side and by $R(x)$ the right hand side of the asserted formula we have

$$L(n+1) - L(n) = a_{n+1} f(n+1)$$

and

$$\begin{aligned} R(n+1) - R(n) &= A(n+1)f(n+1) - A(n)f(n) - \int_n^{n+1} A(n)f'(t)dt \\ &= A(n+1)f(n+1) - A(n)f(n) - A(n)(f(n+1) - f(n)) \\ &= A(n+1)f(n+1) - A(n)f(n+1) \\ &= a_{n+1}f(n+1) = L(n+1) - L(n). \end{aligned}$$

This proves the induction step.

In the general case when x is not necessarily an integer, set $n := \lfloor x \rfloor$. Then

$$L(x) - L(n) = 0$$

and

$$\begin{aligned} R(x) - R(n) &= A(x)f(x) - A(n)f(n) - \int_n^x A(n)f'(t)dt \\ &= A(n)f(x) - A(n)f(n) - A(n)(f(x) - f(n)) = 0, \quad \text{q.e.d.} \end{aligned}$$

11.5. Theorem. *The following relations hold between the prime number function and the Chebyshev theta function:*

a) $$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t\,\log^2 t}\,dt = \frac{\vartheta(x)}{\log x} + O\Big(\frac{x}{\log^2 x}\Big),$$

b) $$\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\,dt = \pi(x)\log x + O\Big(\frac{x}{\log x}\Big).$$

Proof. a) Let $(a_n)_{n\geqslant 2}$ be the sequence defined by

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

$b_n := a_n \log n$, and $f(x) = 1/\log x$. Then

$$\pi(x) = \sum_{2\leqslant n\leqslant x} a_n = \sum_{2\leqslant n\leqslant x} b_n f(n).$$

Since $\sum_{n\leqslant x} b_n = \vartheta(x)$ and $f'(x) = -1/(x\log^2 x)$, Abel summation (lemma 11.4) yields

$$\pi(x) = \vartheta(x)f(x) - \int_2^x \vartheta(t)f'(t)dt = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t\log^2 t}\,dt.$$

To estimate the integral, we use the result of theorem 11.3 that $|\vartheta(t)/t| \le \log 4$. Hence it remains to show that

$$\int_2^x \frac{dt}{\log^2 t} = O\Big(\frac{x}{\log^2 x}\Big).$$

This can be seen as follows (we may assume $x > 4$):

$$\begin{aligned}\int_2^x \frac{dt}{\log^2 t} &= \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \\ &\le \frac{\sqrt{x}}{(\log 2)^2} + \frac{x}{(\log\sqrt{x})^2} = O(\sqrt{x}) + \frac{4x}{\log^2 x} = O\Big(\frac{x}{\log^2 x}\Big).\end{aligned}$$

b) With a_n as defined in a) we have $\vartheta(x) = \sum\limits_{2\leqslant n\leqslant x} a_n \log(n)$. Abel summation yields

$$\vartheta(x) = \pi(x)\log(x) - \int_2^x \frac{\pi(t)}{t}\,dt.$$

From $\vartheta(x) = O(x)$ and a) it follows that $\pi(x) = O(x/\log x)$, hence

$$\int_2^x \frac{\pi(t)}{t}\,dt = O\Big(\int_2^x \frac{dt}{\log t}\Big).$$

The last integral is estimated by the same trick as used in a)

$$\begin{aligned}\int_2^x \frac{dt}{\log t} &= \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \\ &\le \frac{\sqrt{x}}{\log 2} + \frac{x}{\log\sqrt{x}} = O\Big(\frac{x}{\log x}\Big).\end{aligned}$$

11.6. Corollary. *The asymptotic relation*

$$\pi(x) \sim \frac{x}{\log x} \quad \text{for } x \to \infty \quad \text{(prime number theorem)}$$

is equivalent to the asymptotic relation

$$\vartheta(x) \sim x \quad \text{for } x \to \infty.$$

11.7. Definition (Mangoldt function). The arithmetical function $\Lambda : \mathbb{N}_1 \to \mathbb{Z}$ is defined by

$$\Lambda(n) := \begin{cases} \log p, & \text{if } n = p^k \text{ is a prime power } (k \ge 1), \\ 0 & \text{otherwise.} \end{cases}$$

11.8. Theorem. *The Dirichlet series associated to the Mangoldt arithmetical function satisfies for all $s \in \mathbb{C}$ with* $\mathrm{Re}(s) > 1$

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

Proof. By theorem 4.7 one has for $\mathrm{Re}(s) > 1$

$$\log \zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k} \sum_{p \in \mathbb{P}} \frac{1}{p^{ks}}.$$

This can be written as

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

with

$$a_n := \begin{cases} 1/k, & \text{if } n = p^k \text{ is a prime power } (k \geq 1) \\ 0 & \text{otherwise} \end{cases}$$

Since

$$\frac{d}{ds} \frac{1}{n^s} = \frac{d}{ds} e^{-s \log n} = -\log n \; e^{-s \log n} = -\frac{\log n}{n^s}$$

and $a_n \log n = \Lambda(n)$, we get

$$\frac{\zeta'(s)}{\zeta(s)} = \frac{d}{ds} \log \zeta(s) = -\sum_{n=1}^{\infty} \frac{a_n \log n}{n^s} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}, \quad \text{q.e.d.}$$

11.9. Definition (Chebyshev psi function). This function is defined by

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n).$$

11.10. Theorem. *The Chebyshev psi function and the Chebyshev theta function are related in the following way.*

a) $\psi(x) = \sum_{k \geqslant 1} \vartheta(x^{1/k}) = \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + \ldots = \vartheta(x) + O(x^{1/2} \log x)$,

b) $\vartheta(x) = \sum_{k \geqslant 1} \mu(k) \psi(x^{1/k}) = \psi(x) - \psi(x^{1/2}) - \psi(x^{1/3}) - \psi(x^{1/5}) + \psi(x^{1/6}) - + \ldots$.

Proof. a) By the definition of the Mangoldt function one has

$$\psi(x) = \sum_{k \geqslant 1} \sum_{p^k \leqslant n} \log p = \sum_{k \geqslant 1} \sum_{p \leqslant x^{1/k}} \log p = \sum_{k \geqslant 1} \vartheta(x^{1/k}).$$

Since $\vartheta(t) = 0$ for $t < 2$, we have $\vartheta(x^{1/k}) = 0$ for $k > \log x/\log 2$, hence

$$\sum_{k\geqslant 2} \vartheta(x^{1/k}) \leq \Big\lfloor \frac{\log x}{\log 2} \Big\rfloor \vartheta(x^{1/2}) = O(x^{1/2}\log x).$$

b) This is just another form of the Möbius inversion theorem

$$\begin{aligned}\sum_{k\geqslant 1} \mu(k)\psi(x^{1/k}) &= \sum_{k\geqslant 1} \mu(k) \sum_{\ell\geqslant 1} \vartheta(x^{1/k\ell}) \\ &= \sum_{n\geqslant 1} \sum_{k|n} \mu(k)\vartheta(x^{1/n}) = \sum_{n\geqslant 1} \delta_{1,n}\, \vartheta(x^{1/n}) = \vartheta(x).\end{aligned}$$

11.11. Corollary. *The asymptotic relation*

$$\pi(x) \sim \frac{x}{\log x} \quad \text{for } x \to \infty \quad \text{(prime number theorem)}$$

is equivalent to the asymptotic relation

$$\psi(x) \sim x \quad \text{for } x \to \infty.$$

Proof. Since by the preceding theorem $\vartheta(x) \sim x$ is equivalent to $\psi(x) \sim x$, this follows from corollary 11.6.

Remark. We will indeed use this equivalence when we prove the prime number theorem in chapter 13.

11.12. Lemma. *The prime decomposition of $n!$ is*

$$n! = \prod_p p^{\alpha_p}, \qquad \text{where} \quad \alpha_p = \sum_{k\geqslant 1} \Big\lfloor \frac{n}{p^k} \Big\rfloor.$$

Proof. . . .

11.13. Theorem (Bertrand's postulate). *For every positive integer n there is at least one prime p with $n < p \leq 2n$.*

Proof. . . .

11.14. Theorem.

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

Proof. . . .

11.15. Theorem. *There exists a real constant B such that*

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

Proof. . . .

12. Laplace and Mellin Transform

12.1. Laplace Transform. Let $f : \mathbb{R}_+ \to \mathbb{C}$ be a measurable function such that $|f(x)|e^{-\sigma_0 x}$ is bounded on $\mathbb{R}_+$ for some $\sigma_0 \in \mathbb{R}$. Then the integral

$$F(s) = \int_0^\infty f(x)e^{-sx}dx$$

exists for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \sigma_0$ and represents a holomorphic function in the halfplane

$$H(\sigma_0) = \{s \in \mathbb{C} : \mathrm{Re}(s) > \sigma_0\}$$

F is called the Laplace transform of f.

Remark. Measurable here means Lebesgue measurable. In our applications, f will always be at least piecewise continuous. Hence the reader who does not feel confortable with Lebesgue integration theory may assume f piecewise continuous.

The existence of the integral follows from the estimate

$$|f(x)e^{sx}| \le Ke^{-(\sigma-\sigma_0)x}, \quad \sigma := \mathrm{Re}(s) > \sigma_0,$$

where K is an upper bound for $|f(x)|e^{\sigma_0 x}$ on $\mathbb{R}$.

Example. Let $f(x) = 1$ for all $x \in \mathbb{R}_+$. The Laplace transform of this function is

$$F(s) = \int_0^\infty e^{-sx}dx = \lim_{R\to\infty}\Big[-\frac{e^{-sx}}{s}\Big]_{x=0}^{x=R} = \lim_{R\to\infty}(1 - e^{-sR}) = \frac{1}{s} \quad \text{for } \mathrm{Re}(s) > 0.$$

12.2. *Relation between Laplace and Fourier transform.*
We set $s = \sigma + it$, $\sigma, t \in \mathbb{R}$. Then the formula for the Laplace transform becomes

$$F(\sigma + it) = \int_0^\infty f(x)e^{-\sigma x}e^{-itx}dx = \int_{-\infty}^\infty g(x)e^{-itx}dx,$$

where

$$g(x) = \begin{cases} f(x)e^{-\sigma x} & \text{for } x \ge 0, \\ 0 & \text{for } x < 0. \end{cases}$$

Therefore the function $t \mapsto F(\sigma + it)$ can be regarded (up to a normalization constant) as the Fourier transform of the function g.

12.3. Mellin Transform. The Mellin transform is obtained from the Laplace transform by a change of variables. With the substitution

$$x = \log t, \quad dx = \frac{dt}{t},$$

Chap. 12 last revised: 2003-04-14

the formula for the Laplace transform becomes

$$F(s) = \int_1^\infty f(\log t)\, t^{-s}\, \frac{dt}{t}.$$

This can be viewed as a transformation of the function $g(t) := f(\log t)$, $t \geq 1$, and leads to the following definition.

Definition. Let $g : [1,\infty[\to \mathbb{R}$ a measurable function such that $g(x)x^{-\sigma_0}$ is bounded on $[1,\infty[$ for some $\sigma_0 \in \mathbb{R}$. Then the integral

$$G(s) = \int_1^\infty g(x) x^{-s}\, \frac{dx}{x}$$

exists for all $s \in \mathbb{C}$ with $\mathrm{Re}(s) > \sigma_0$. The function G is holomorphic in the halfplane $H(\sigma_0)$ and is called the Mellin transform of g.

Remark. There exists a generalization of the Mellin transform where the integral is extended from 0 to ∞. An example is the Euler integral for the Gamma function

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

This generalized Mellin transform corresponds to the "two-sided" Laplace transform

$$F(s) = \int_{-\infty}^\infty f(x) e^{-sx} dx$$

12.4. Theorem. *The Mellin transform of the Chebyshev ψ-function is*

$$\int_1^\infty \psi(x)\, x^{-s}\, \frac{dx}{x} = -\frac{\zeta'(s)}{s\zeta(s)} \quad \text{for } \mathrm{Re}(s) > 1.$$

Proof. It follows from theorems 11.3 and 11.10 that $\psi(x)/x$ is bounded, hence the Mellin transform of ψ exists for $\mathrm{Re}(s) > 1$. We apply the Abel summation theorem 11.4 to the sum $\sum\limits_{n \leqslant x} \dfrac{\Lambda(n)}{n^s}$. Since

$$\frac{d}{dx}\frac{1}{x^s} = -s\, \frac{1}{x^{s+1}},$$

we obtain

$$\sum_{n \leqslant x} \frac{\Lambda(n)}{n^s} = \frac{\psi(x)}{x^s} + s \int_1^x \frac{\psi(t)}{t^{s+1}}\, dt.$$

Letting $x \to \infty$, we get $\psi(x)/x^s \to 0$ for $\mathrm{Re}(s) > 1$, and using theorem 11.8

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = s \int_1^\infty \frac{\psi(t)}{t^{s+1}}\,dt, \quad \text{q.e.d.}$$

12.5. Theorem (Tauberian theorem of Ingham and Newman). *Let $f : \mathbb{R}_+ \to \mathbb{C}$ be a measurable bounded function and*

$$F(s) = \int_0^\infty f(x)e^{-sx}dx, \quad \mathrm{Re}(s) > 0,$$

its Laplace transform. Suppose that F, which is holomorphic in

$$H(0) = \{s \in \mathbb{C} : \mathrm{Re}(s) > 0\},$$

admits a holomorphic continuation to some open neighborhood U of $\overline{H(0)}$. Then the improper integral

$$\int_0^\infty f(x)dx = \lim_{R\to\infty} \int_0^R f(x)dx$$

exists and one has

$$F(0) = \int_0^\infty f(x)dx,$$

where $F(0)$ denotes the value at 0 of the continued function.

Proof. For a real parameter $R > 0$ define the function

$$F_R(s) := \int_0^R f(x)e^{-sx}dx.$$

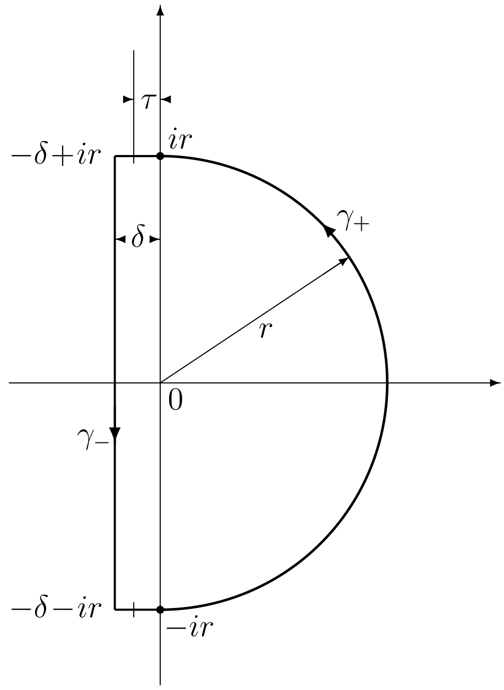
Since the integration interval $[0, R]$ is compact, F_R is holomorphic in the whole plane $\mathbb{C}$. The assertion of the theorem is equivalent to

$$\lim_{R\to\infty} (F(0) - F_R(0)) = 0.$$

The function $F - F_R$ is holomorphic in $U \supset \overline{H(0)}$, therefore its value at the point 0 can be calculated by the Cauchy formula.

$$F(0) - F_R(0) = \frac{1}{2\pi i} \int_\gamma (F(s) - F_R(s)) \frac{1}{s}\,ds.$$

Here the curve $\gamma = \gamma_+ + \gamma_-$ is chosen as indicated in the following figure. γ_+ is a semi-circle of radius $r > 0$ with center 0 in the right halfplane from $-ir$ to ir, and γ_- consists of three straight lines from ir to $-\delta + ir$, from $-\delta + ir$ to $-\delta - ir$ and from $-\delta - ir$ to $-ir$. The constant $\delta > 0$ has to be chosen (depending on r) sufficiently small, such that γ and its interior are completely contained in U.



The function $s \mapsto (F(s) - F_R(s))\, e^{Rs}$ is holomorphic in U and for $s = 0$ its value is $F(0) - F_R(0)$. Therefore we have also

$$F(0) - F_R(0) = \frac{1}{2\pi i} \int_\gamma (F(s) - F_R(s))\, e^{Rs}\, \frac{1}{s}\, ds.$$

We still use another trick and write

$$F(0) - F_R(0) = \frac{1}{2\pi i} \int_\gamma (F(s) - F_R(s))\, e^{Rs} \left(\frac{1}{s} + \frac{s}{r^2}\right) ds. \tag{$*$}$$

This is true since the added function

$$s \mapsto (F(s) - F_R(s))\, e^{Rs}\, \frac{s}{r^2}$$

is holomorphic in U, hence its integral over γ vanishes.

Note that for $|s| = r$ one has

$$\left(\frac{1}{s} + \frac{s}{r^2}\right) = \frac{\bar{s}}{s\bar{s}} + \frac{s}{r^2} = \frac{s + \bar{s}}{r^2} = \frac{2\sigma}{r^2}, \quad \text{where } \sigma = \mathrm{Re}(s).$$

For the proof of our theorem, we have to estimate the integral $(*)$.

Let $\varepsilon > 0$ be given. We choose $r := 3/\varepsilon$ and a suitable $\delta > 0$. We estimate the integral in three steps.

1) Estimation of the integral over the curve γ_+.

Since by hypothesis $f : \mathbb{R} \to \mathbb{C}$ is bounded, we may suppose $|f(x)| \le 1$ for all $x \ge 0$. Then for $\sigma = \mathrm{Re}(s) > 0$

$$|F(s) - F_R(s)| = \Big|\int_R^\infty f(x)e^{-sx}dx\Big| \le \int_R^\infty e^{-\sigma x}dx = \frac{e^{-R\sigma}}{\sigma}.$$

With the abbreviation

$$G_1(s) := (F(s) - F_R(s))\, e^{Rs}\left(\frac{1}{s} + \frac{s}{r^2}\right)$$

we get therefore on γ_+

$$|G_1(s)| \le \frac{e^{-R\sigma}}{\sigma}\, e^{R\sigma}\, \frac{2\sigma}{r^2} = \frac{2}{r^2},$$

hence

$$\Big|\frac{1}{2\pi i}\int_{\gamma_+} G_1(s)ds\Big| \le \frac{1}{2\pi}\int_{\gamma_+} \frac{2}{r^2}\,|ds| = \frac{1}{2\pi}\cdot\frac{2}{r^2}\cdot\pi r = \frac{1}{r} = \frac{\varepsilon}{3}.$$

2) Estimation of the integral $\displaystyle\int_{\gamma_-} F_R(s)e^{Rs}\Big(\frac{1}{s} + \frac{s}{r^2}\Big)ds.$

Since F_R is holomorphic in the whole plane, we may replace the integration curve γ_- by a semicircle α of radius r in the halfplane $\mathrm{Re}(s) \le 0$ from ir to $-ir$. For $\sigma = \mathrm{Re}(s) < 0$ we have

$$|F_R(s)| \le \int_0^R e^{-x\sigma}dx = \frac{1}{\sigma}(1 - e^{-R\sigma}) \le \frac{e^{-R\sigma}}{|\sigma|},$$

Therefore the integrand

$$G_2(s) := F_R(s)e^{Rs}\Big(\frac{1}{s} + \frac{s}{r^2}\Big)$$

satisfies the following estimate on the curve α

$$|G_2(s)| \le \big|F_R(s)e^{Rs}\big|\,\frac{2|\sigma|}{r^2} \le \frac{2}{r^2},$$

hence

$$\Big|\frac{1}{2\pi i}\int_\alpha G_2(s)ds\Big| \le \frac{1}{2\pi}\int_\alpha \frac{2}{r^2}|ds| = \frac{1}{\pi r^2}\int_\alpha |ds| = \frac{1}{r} = \frac{\varepsilon}{3}.$$

3) Estimation of the integral $\displaystyle\int_{\gamma_-} F(s)e^{Rs}\Big(\frac{1}{s} + \frac{s}{r^2}\Big)ds.$

The function $s \mapsto F(s)\Big(\dfrac{1}{s}+\dfrac{s}{r^2}\Big)$ is holomorphic in a neighborhood of the integration path γ_-. Therefore there exists a constant $K>0$ such that

$$\Big|F(s)\Big(\frac{1}{s}+\frac{s}{r^2}\Big)\Big| \le K \quad \text{for all } s \text{ on the curve } \gamma_-.$$

Hence the integrand

$$G_3(s) := F(s)e^{Rs}\Big(\frac{1}{s}+\frac{s}{r^2}\Big)$$

satisfies the following estimate on γ_-

$$|G_3(s)| \le Ke^{R\sigma}, \quad \text{where } \sigma = \mathrm{Re}(s).$$

Let τ be some constant with

$$0<\tau<\delta,$$

whose value will be fixed later. We split the integration curve γ_- into two parts

$$\begin{aligned}\gamma'_- &:= \gamma_- \cap \{\mathrm{Re}(s) \ge -\tau\},\\ \gamma''_- &:= \gamma_- \cap \{\mathrm{Re}(s) \le -\tau\}.\end{aligned}$$

γ'_- consists of two line segments of length τ each. Let L be the length of γ_-. Then

$$\begin{aligned}\Big|\frac{1}{2\pi i}\int_{\gamma_-} G_3(s)ds\Big| &\le \frac{1}{2\pi}\Big\{\int_{\gamma'_-} Ke^{R\sigma}|ds| + \int_{\gamma''_-} Ke^{R\sigma}|ds|\Big\}\\ &\le \frac{K}{2\pi}\Big\{\int_{\gamma'_-}|ds| + \int_{\gamma''_-} e^{-R\tau}|ds|\Big\}\\ &\le \frac{K}{2\pi}\left(2\tau + Le^{-R\tau}\right).\end{aligned}$$

We now fix a value of $\tau>0$ such that

$$\frac{K}{2\pi}\cdot 2\tau < \frac{\varepsilon}{6}$$

and choose an $R_0>0$ such that

$$\frac{K}{2\pi}\cdot Le^{-R_0\tau} < \frac{\varepsilon}{6}$$

Then we have

$$\Big|\frac{1}{2\pi i}\int_{\gamma_-} G_3(s)ds\Big| < \frac{\varepsilon}{3} \quad \text{for all } R \ge R_0.$$

Putting the estimates of 1), 2) and 3) together we finally get

$$|F(0)-F_R(0)| = \Big|\frac{1}{2\pi i}\int_\gamma (F(s)-F_R(s))\,e^{Rs}\left(\frac{1}{s}+\frac{s}{r^2}\right)ds\Big| < \varepsilon$$

for all $R \ge R_0$, q.e.d.

13. Proof of the Prime Number Theorem

13.1. In this chapter we will prove the prime number theorem

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

As we have seen in corollary 11.11, this is equivalent to the asymptotic relation

$$\psi(x) \sim x \quad \text{for } x \to \infty.$$

To prove this, we use the Mellin transform of ψ, calculated in theorem 12.4

$$\int_1^\infty \psi(x)\, x^{-s}\, \frac{dx}{x} = -\frac{\zeta'(s)}{s\zeta(s)} \quad \text{for } \mathrm{Re}(s) > 1.$$

A first step is

13.2. Proposition. *The following improper integral exists:*

$$\int_1^\infty \Big(\frac{\psi(x)}{x} - 1\Big)\, \frac{dx}{x} = \lim_{R\to\infty} \int_1^R \Big(\frac{\psi(x)}{x} - 1\Big)\, \frac{dx}{x}.$$

Proof. We write the Mellin transform of ψ as a Laplace transform

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

Since

$$\int_0^\infty e^{-(s-1)x} dx = \frac{1}{s-1} \quad \text{for } \mathrm{Re}(s) > 1,$$

we get for $\mathrm{Re}(s) > 1$

$$\int_0^\infty \Big(\frac{\psi(e^x)}{e^x} - 1\Big) e^{-(s-1)x} dx = -\frac{\zeta'(s)}{s\zeta(s)} - \frac{1}{s-1} =: F(s).$$

The zeta function has a pole of order 1 at $s = 1$, hence $\zeta'(s)/(s\zeta(s))$ has a pole of order 1 with residue -1 at $s = 1$. It follows that F is holomorphic at $s = 1$. We now use the fact that the zeta function has no zeroes on the line $\mathrm{Re}(s) = 1$ and get that the function F can be continued holomorphically to some neighborhood of the closed halfplane $\mathrm{Re}(s) \geq 1$. The Tauberian theorem 12.5 of Ingham/Newman can be applied to the above Laplace transform (after a coordinate change $\tilde{s} = s - 1$), yielding the existence of the improper integral

$$\int_0^\infty \Big(\frac{\psi(e^x)}{e^x} - 1\Big)\, dx.$$

Chap. 13 last revised: 2002-02-10

By the substitution $\tilde{x} = e^x$ this is nothing else than the improper integral

$$\int_1^\infty \Big(\frac{\psi(x)}{x} - 1\Big)\frac{dx}{x},$$

which proves the proposition.

13.3. Lemma. *Let $g : [1,\infty[\; \to \mathbb{R}$ be a monotonically increasing function such that the improper integral*

$$\int_1^\infty \Big(\frac{g(x)}{x} - 1\Big)\frac{dx}{x}$$

exists. Then

$$\lim_{x\to\infty} \frac{g(x)}{x} = 1.$$

Remark. In general, the existence of an improper integral $\int_1^\infty f(x)\frac{dx}{x}$ does not imply $\lim\limits_{x\to\infty} f(x) = 0$, as can be seen by the example

$$\int_1^\infty \sin x \,\frac{dx}{x} = \lim_{R\to\infty}\int_1^R \frac{\sin x}{x}\,dx.$$

That this improper integral converges follows from the Leibniz criterion for the convergence of alternating series.

Proof. $\lim\limits_{x\to\infty} g(x)/x = 1$ is equivalent to the following two assertions

$$(1)\qquad \limsup_{x\to\infty}\frac{g(x)}{x} \le 1,$$

$$(2)\qquad \liminf_{x\to\infty}\frac{g(x)}{x} \ge 1.$$

Proof of (1). If this is not true, there exists an $\varepsilon > 0$ and a sequence (x_ν) with $x_\nu \to \infty$ such that

$$g(x_\nu) \ge (1+\varepsilon)x_\nu \quad \text{for all } \nu.$$

Since g is monotonically increasing, it follows that

$$\int\limits_{x_\nu}^{(1+\varepsilon)x_\nu} \Big(\frac{g(x)}{x} - 1\Big)\frac{dx}{x} \ge \int\limits_{x_\nu}^{(1+\varepsilon)x_\nu} \Big(\frac{(1+\varepsilon)x_\nu}{x} - 1\Big)\frac{dx}{x} = [\text{Subst. } t = \tfrac{x}{x_\nu}]$$

$$= \int\limits_1^{1+\varepsilon} \Big(\frac{1+\varepsilon}{t} - 1\Big)\frac{dt}{t} = \alpha(\varepsilon) > 0,$$

where $\alpha(\varepsilon)$ is a positive constant independent of ν (the function $\frac{1+\varepsilon}{t} - 1$ is continuous and positive on the interval $[1, 1+\varepsilon[$). But this contradicts the Cauchy criterion for the existence of the improper integral $\int_1^\infty (\frac{g(x)}{x} - 1)\,\frac{dx}{x}$.

Remark. The Cauchy criterion for the existence of the improper integral $\int_a^\infty f(x)dx$ can be formulated as follows: For every $\varepsilon > 0$ there exists an $R_0 \geq a$ such that

$$\Big|\int_R^{R'} f(x)dx\Big| < \varepsilon \quad \text{for all } R, R' \text{ with } R' \geq R \geq R_0.$$

Proof of (2). If this is not true, there exists an $\varepsilon > 0$ and a sequence (x_ν) with $x_\nu \to \infty$ such that

$$g(x_\nu) \leq (1-\varepsilon)x_\nu \quad \text{for all } \nu.$$

Since g is monotonically increasing, it follows that

$$\int\limits_{(1-\varepsilon)x_\nu}^{x_\nu} \Big(\frac{g(x)}{x} - 1\Big)\frac{dx}{x} \leq \int\limits_{(1-\varepsilon)x_\nu}^{x_\nu} \Big(\frac{(1-\varepsilon)x_\nu}{x} - 1\Big)\frac{dx}{x} = \ [\text{Subst. } t = \tfrac{x}{x_\nu}]$$

$$= \int\limits_{1-\varepsilon}^{1} \Big(\frac{1-\varepsilon}{t} - 1\Big)\frac{dt}{t} = -\beta(\varepsilon) < 0,$$

where $\beta(\varepsilon)$ is a positive constant independent of ν (the function $\frac{1-\varepsilon}{t} - 1$ is continuous and negative on $]1-\varepsilon, 1]$). This contradicts the Cauchy criterion for the existence of the improper integral $\int_1^\infty (\frac{g(x)}{x} - 1)\,\frac{dx}{x}$. Therefore (2) must be true, which completes the proof of the lemma.

13.4. Theorem (Prime number theorem). *The prime number function*

$$\pi(x) := \#\{p \in \mathbb{N}_1 : p \text{ prime and } p \leq x\}$$

satisfies the asymptotic relation

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

Proof. Lemma 13.3 applied to proposition 13.2 yields $\psi(x) \sim x$, which is by corollary 11.11 equivalent to $\pi(x) \sim x/\log x$, q.e.d.

The following corollary is a generalization of Bertrand's postulate (theorem 11.13).

13.5. Corollary. *For every $\varepsilon > 0$ there exists an $x_0 \geq 1$ such that for all $x \geq x_0$ there is at least one prime p with*

$$x < p \leq (1+\varepsilon)x.$$

Proof. By the prime number theorem

$$\lim_{x\to\infty} \frac{\pi((1+\varepsilon)x)}{\pi(x)} = \lim_{x\to\infty} \frac{(1+\varepsilon)x}{\log(1+\varepsilon)+\log x} \cdot \frac{\log x}{x} = 1+\varepsilon.$$

Therefore there exists an x_0 such that $\pi((1+\varepsilon)x) > \pi(x)$ for all $x \geq x_0$, hence there must be a prime p with $x < p \leq (1+\varepsilon)x$, q.e.d.

13.6. Corollary. *Let p_n denote the n-th prime (in the natural order by size). Then we have the asymptotic relation*

$$p_n \sim n \log n \quad \text{for } n \to \infty.$$

Proof. By the prime number theorem, we have the following asymptotic relation for $n \to \infty$

$$\pi(n\log n) \sim \frac{n\log n}{\log(n\log n)} = \frac{n\log n}{\log n + \log\log n} = \frac{n}{1+\frac{\log\log n}{\log n}} \sim n.$$

Since $\pi(p_n) = n$ by definition, the assertion follows immediately from the next lemma.

13.7. Lemma. *Let $f, g : \mathbb{N}_1 \to \mathbb{R}_+$ be two functions with $\lim\limits_{n\to\infty} f(n) = \lim\limits_{n\to\infty} g(n) = \infty$ and*

$$\pi(f(n)) \sim \pi(g(n)) \quad \text{for } n \to \infty.$$

Then we have also

$$f(n) \sim g(n) \quad \text{for } n \to \infty.$$

Proof. We have to show

$$(1) \quad \limsup_{n\to\infty} \frac{f(n)}{g(n)} \leq 1 \qquad \text{and} \qquad (2) \quad \limsup_{n\to\infty} \frac{g(n)}{f(n)} \leq 1.$$

To prove (1), assume this is false. Then there exists an $\varepsilon > 0$ and a sequence (n_ν) with $n_\nu \to \infty$ such that

$$f(n_\nu) \geq (1+\varepsilon)g(n_\nu) \quad \text{for all } \nu.$$

Since

$$\lim_{\nu\to\infty} \frac{\pi((1+\varepsilon)g(n_\nu))}{\pi(g(n_\nu))} = 1+\varepsilon,$$

cf. the proof of corollary 13.5, this implies

$$\limsup_{\nu\to\infty} \frac{\pi(f(n_\nu))}{\pi(g(n_\nu)} \geq 1+\varepsilon,$$

contradicting the hypothesis $\pi(f(n)) \sim \pi(g(n))$. Therefore (1) must be true. Assertion (2) follows from (1) by interchanging the roles of f and g.