Analytic Number Theory
Lecture 1

Mariusz Mirek
Rutgers University

Padova, March 11, 2025.

Supported by the NSF grant DMS-2154712,
and the CAREER grant DMS-2236493.

Number systems

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ – non-negative integers.
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$ – the set of integers.
- $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$ – positive integers.
- $\mathbb{Q} = \{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{Z} \setminus \{0\}\}$ – the set of rationals.
- $\mathbb{R}$ – the set of real numbers.
- $\mathbb{R}_+ := (0, \infty)$ – the set of positive real numbers.
- $\mathbb{C}$ – the set of complex numbers.

For $N \in \mathbb{R}_+$ and any $A \subseteq [0, \infty)$ we will use the following useful notation

$$A_{\leq N} := [0, N] \cap A, \qquad A_{<N} := [0, N) \cap A,$$
$$A_{\geq N} := [N, \infty) \cap A, \qquad A_{>N} := (N, \infty) \cap A.$$

Basic functions

- The Eulers' function will be denoted by

$$e(t) := e^{2\pi i t} = \cos(2\pi t) + i \sin(2\pi t) \quad \text{for} \quad t \in \mathbb{R},$$

  where $i := \sqrt{-1}$ is the imaginary unit.
- For any $x \in \mathbb{R}$ we will use the floor and fractional part functions

$$\lfloor x \rfloor := \max\{n \in \mathbb{Z} : n \leq x\} \quad \text{and} \quad \{x\} := x - \lfloor x \rfloor.$$

- For $x \in \mathbb{R}$ the sign function will be denoted by

$$\operatorname{sgn}(x) := \begin{cases} -1 & \text{if } x < 0 \\ 0 & \text{if } x = 0 \\ 1 & \text{if } x > 0 \end{cases}.$$

  It is not difficult to see that $\operatorname{sgn}(x) = \frac{x}{|x|}$ whenever $x \neq 0$.

Three important principles

Well-Ordering Principle (WOP)

If A is a nonempty subset of nonnegative integers $\mathbb{N}$, then A contains the smallest number.

Principle of Induction (PI)

If A is a set of nonnegative integers $\mathbb{N}$ satisfying the following two properties:

- (Basic step): $0 \in A$,
- (Induction step): Whenever A contains a number n, it also contains the number $n + 1$.

Then $A = \mathbb{N}$. In other words, one can write

$$\forall_{A \subseteq \mathbb{N}} \ (0 \in A \ \text{ and } \ \forall_{k \in \mathbb{N}} \ (k \in A \Longrightarrow k + 1 \in A) \text{ then } A = \mathbb{N}) \,.$$

Maximum Principle (MP)

A nonempty subset of $\mathbb{N}$, which is bounded from above contains the greatest number.

All these three principles are equivalent

Theorem

One has the following

$$(\text{WOP}) \iff (\text{PI}) \iff (\text{MP}).$$

We will show the following:

$$(\text{WOP}) \implies (\text{PI}) \implies (\text{WOP}) \implies (\text{MP}) \implies (\text{WOP}).$$

Proof (WOP) $\implies$ (PI).

If A is a set of non-negative integers such that

(i) $0 \in A$.

(ii) Whenever A contains a number n, it also contains $n+1$.

We want to establish $A = \mathbb{N}$. Suppose for contradiction that $\mathbb{N} \setminus A \neq \emptyset$. By the well-ordering principle (WOP) there is the smallest element m of $\mathbb{N} \setminus A$. Since $0 \in A$, we have $m \neq 0$. Observe that $m-1 \in A$. Otherwise $m-1 \in \mathbb{N} \setminus A$, which contradicts the fact that m is the smallest element of $\mathbb{N} \setminus A$. But if $m-1 \in A$, then by (ii) we have $m \in A$, which is impossible. The implication (WOP) $\implies$ (PI) follows. □

All these three principles are equivalent

Proof (PI) $\Longrightarrow$ (WOP).

Let $\emptyset \neq A \subseteq \mathbb{N}$. Suppose that A does not have a minimal element.

(a) It is easy to see that $0 \notin A$, because otherwise it would be a minimal element of A (as 0 is the minimal element of $\mathbb{N}$).

(b) We also see $1 \notin A$, otherwise it is a minimal element of A.

(c) We continue and assume that $1, 2, \ldots, n \notin A$. Then $n + 1 \notin A$, otherwise $n + 1$ is the smallest element of A.

Now we can use the principle of induction (PI) and conclude that $A = \emptyset$, which is impossible. Hence the implication (PI) $\Longrightarrow$ (WOP) follows. □

Proof (WOP) $\Longrightarrow$ (MP).

Suppose that $A \neq \emptyset$ is bounded, which means that there exists $M \in \mathbb{N}$ such that $a \leq M$ for all $a \in A$. Equivalently, $M - a \geq 0$ for all $a \in A$. Let us consider the set $B = \{M - a \colon a \in A\} \neq \emptyset$. By the well-ordering principle (WOP) there is $b \in A$ such that $M - b$ is the smallest element of B. Thus $M - b \leq M - a$ for all $a \in A$, equivalently $a \leq b$ for all $a \in A$. The implication (WOP) $\Longrightarrow$ (MP) now follows. □

All these three principles are equivalent

(MP) $\Longrightarrow$ (WOP).

Let $\emptyset \neq A \subseteq \mathbb{N}$ and we show that A has a minimal element. Let

$$B = \{n \in \mathbb{N} \colon n \leq a \text{ for every } a \in A\}.$$

The set B is bounded and $0 \in B$ since $0 \leq a$ for any $a \in \mathbb{N}$. Thus, by the maximum principle (MP) we find $b_0 \in B$ such that b_0 is maximal in B. We see that $b \leq b_0 \leq a$ for all $a \in A$ and $b \in B$. The proof will be completed if we show $b_0 \in A$. Assume for contradiction $b_0 \neq a$ and $b_0 \leq a$ for all $a \in A$. Thus $b_0 < a$ for all $a \in A$. Hence, $b_0 + 1 \leq a$ for any $a \in A$. Then $b_0 + 1 \in B$, but b_0 is the maximal element of B, which gives contradiction. Hence the implication (MP) $\Longrightarrow$ (WOP) follows and the proof of Theorem 1 is finished. $\square$

Divisibility

Divisibility is a fundamental concept in number theory. Let $a, d \in \mathbb{Z}$ and we say that d is a divisor of a, and that a is a multiple of d, if there exists an integer $q \in \mathbb{Z}$ such that

$$a = dq.$$

If d divides a, we write $d \mid a$, and a/d is called the divisor conjugate to d.

Theorem (Divisibility)

Let $a, b, d, n, m \in \mathbb{Z}$. Divisibility has the following properties:

1. $d \mid n$ *and* $n \mid m$ *implies* $d \mid m$.
2. $d \mid n$ *and* $d \mid m$ *implies* $d \mid (an + bm)$.
3. $d \mid n$ *implies* $ad \mid an$.
4. $ad \mid an$ *and* $a \neq 0$ *implies* $d \mid n$.
5. $1 \mid n$ *and* $n \mid 0$.
6. $0 \mid n$ *implies* $n = 0$.
7. $d \mid n$ *and* $n \neq 0$ *implies* $|d| < |n|$.
8. $d \mid n$ *and* n/d *implies* $|d| = |n|$.
9. $d \mid n$ *and* $d \neq 0$ *implies* $(n/d) \mid n$.

The division algorithm

Theorem (The division algorithm)

Let $a, d \in \mathbb{Z}$ and $d \neq 0$. There exist unique integers q and r such that

$$a = dq + r, \quad \textit{where} \quad 0 \leq r < |d|. \tag{1}$$

Proof.

Let $S := \{a - dq : q \in \mathbb{Z}\} \cap \mathbb{N}$ and note that $S \neq \emptyset$, indeed if $a \geq 0$, then $a = a - d \cdot 0 \in S$. If $a < 0$, then $a - d(d|d|^{-1}a) = (-a)(|d| - 1) \in S$.

- **Existence**: By the minimum principle, S contains a smallest element $r \in \mathbb{N}$, and $a = dq + r$ for some $q \in \mathbb{Z}$. If $r \geq |d|$, then

$$0 \leq r - |d| = a - d(q + d|d|^{-1}) < r,$$

  and $r - |d| \in S$, which contradicts the minimality of r implying (1).

- **Uniqueness**: Let $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ be integers such that $a = dq_1 + r_1 = dq_2 + r_2$ and $0 \leq r_1, r_2 < |d|$. If $q_1 \neq q_2$, then

$$|d| \leq |d||q_1 - q_2| = |r_2 - r_1| < |d|.$$

  which is impossible. Therefore, $q_1 = q_2$ and $r_1 = r_2$ as desired.

Finally note that $d \mid a$ if and only if $r = 0$. $\square$

Some remarks

Remarks on the division algorithm

- The integers q and r in the equation $a = dq + r$ of the division algorithm are called the quotient and the remainder, respectively, in the division of a by d.
- Although the division algorithm theorem is an existence theorem, its proof actually gives us a method for computing the quotient q and the remainder r. We subtract from a (or add to a) enough multiples of d until it is clear that we have obtained the smallest nonnegative number of the form $a - bq$.
- In the previous theorem we can take

$$q := \begin{cases} \lfloor a/d \rfloor & \text{if } d > 0, \\ -\lfloor a/|d| \rfloor & \text{if } d < 0, \end{cases}$$

where $\lfloor x \rfloor := \max\{n \in \mathbb{Z} : n \leq x\}$ denotes the integer part of $x \in \mathbb{R}$.

Groups

Definition of groups

A group $\mathbb{G} := (\mathbb{G}, \cdot)$ is a nonempty set $\mathbb{G}$ with a binary operation $\mathbb{G} \times \mathbb{G} \ni (x, y) \mapsto x \cdot y \in \mathbb{G}$ that satisfies the following three axioms:

(i) **Associativity:** $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in \mathbb{G}$.

(ii) **Identity element:** There exists a neutral element $e \in \mathbb{G}$ such that for all

$$e \cdot x = x \cdot e = x \quad \text{for all} \quad x \in \mathbb{G}.$$

The element e is called the identity of the group.

(iii) **Inverses:** For every $x \in \mathbb{G}$, there exists an element $y \in \mathbb{G}$ such that

$$x \cdot y = y \cdot x = e.$$

The element y is called the inverse of x.

Abelian groups

A group $\mathbb{G} = (\mathbb{G}, \cdot)$ is called abelian or commutative if the binary operation satisfies (i)–(iii) and also satisfies the axiom

(iv) **Commutativity:** $x \cdot y = y \cdot x$ for all $x, y \in \mathbb{G}$.

Examples

- The set $\mathrm{GL}_2(\mathbb{C})$ of 2×2 matrices with complex coefficients and nonzero determinant, is a nonabelian group with the usual matrix multiplication as the binary operation.
- Examples of abelian groups are the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$, with the usual operation of addition. The nonzero rational, real, and complex numbers, denoted by $\mathbb{Q}^\times$, $\mathbb{R}^\times$, and $\mathbb{C}^\times$, respectively, are also abelian groups, with the usual multiplication as the binary operation.
- For every $m \in \mathbb{Z}_+$, the set of complex numbers

  $$\Gamma_m := \{e(k/m) : k \in \mathbb{N}_{<m}\}$$

  is a multiplicative group. The elements of Γ_m are called mth roots of unity, since $\omega^m = 1$ for all $\omega \in \Gamma_m$.
- If $\mathbb{G}$ is an abelian group can use additive notation and denote the image of the ordered pair $(x, y) \in \mathbb{G} \times \mathbb{G}$ by $x + y$. We call $x + y$ the sum of x and y. In an additive group, the identity is usually written 0, the inverse of x is written $-x$, and we define $x - y = x + (-y)$.
- If $\mathbb{G}$ is nonabelian we can also use multiplicative notation and denote the image of the ordered pair $(x, y) \in \mathbb{G} \times \mathbb{G}$ by xy. We call xy the product of x and y. In a multiplicative group, the identity is usually written e or 1 and the inverse of x is written x^{-1}.

Subgroups

- A nonempty subset $\mathbb{H}$ of a group $\mathbb{G}$ is a subgroup of $\mathbb{G}$ if it is also a group under the same binary operation as $\mathbb{G}$. If $\mathbb{H}$ is a subgroup of $\mathbb{G}$, then $\mathbb{H}$ is closed under the binary operation in $\mathbb{G}$, it contains the identity element of $\mathbb{G}$, and the inverse of every element of $\mathbb{H}$ belongs to $\mathbb{H}$.
- A nonempty subset $\mathbb{H}$ of an additive abelian group $\mathbb{G}$ is a subgroup if and only if $x - y \in \mathbb{H}$ for all $x, y \in \mathbb{H}$
- For every $d \in \mathbb{Z}$, the set of all multiples of d is a subgroup of $\mathbb{Z}$. We denote this subgroup by $d\mathbb{Z}$. If $a_1, \ldots, a_k \in \mathbb{Z}$, then the set $\{a_1x_1 + \cdots + a_kx_k : x_1, \ldots, x_k \in \mathbb{Z}\}$ is also a subgroup of $\mathbb{Z}$.
- The set $\mathbb{Q}$ of rational numbers is a subgroup of the additive group $\mathbb{R}$. The set $\mathbb{R}_+$ is a subgroup of the multiplicative group $\mathbb{R}^\times$. The unit circle in the complex plane $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$ is a subgroup of the multiplicative group $\mathbb{C}^\times$, and Γ_m is a subgroup of $\mathbb{T}$.
- If $\mathbb{G}$ is a group, written multiplicatively, and $g \in \mathbb{G}$, then $g^n \in \mathbb{G}$ for all $n \in \mathbb{Z}$, and $\{g^n : n \in \mathbb{Z}\}$ is a subgroup of $\mathbb{G}$.
- The intersection of a family of subgroups of a group $\mathbb{G}$ is a subgroup of $\mathbb{G}$. Let S be a subset of a group $\mathbb{G}$. The subgroup of $\mathbb{G}$ generated by S is the smallest subgroup of $\mathbb{G}$ that contains S. In fact, this is simply the intersection of all subgroups of $\mathbb{G}$ that contain S.
- For example, the subgroup of $\mathbb{Z}$ generated by the set $\{d\}$ is $d\mathbb{Z}$.

Structure of the subgroups of $\mathbb{Z}$

Theorem

Let $\mathbb{H}$ be a subgroup of the integers under addition. There exists a unique nonnegative integer $d \in \mathbb{N}$ such that $\mathbb{H} = \{0, \pm d, \pm 2d, \ldots\} = d\mathbb{Z}$.

Proof of the existence.

- We have $0 \in \mathbb{H}$ for every subgroup $\mathbb{H}$. We can assume that $\mathbb{H} \neq \{0\}$, otherwise we choose (uniquely) $d = 0$ and $\mathbb{H} = 0\mathbb{Z}$.
- Since $\mathbb{H} \neq \{0\}$, then there exists $0 \neq a \in \mathbb{H}$. Since $-a$ also belongs to $\mathbb{H}$, it follows that $\mathbb{H}$ contains positive integers. By the well-ordering principle, $\mathbb{H}$ contains a least positive integer $d \in \mathbb{Z}_+$. Hence, $dq \in \mathbb{H}$ for every $q \in \mathbb{Z}$, and so $d\mathbb{Z} \subseteq \mathbb{H}$.
- Now we show that $\mathbb{H} \subseteq d\mathbb{Z}$. Let $a \in \mathbb{H}$. By the division algorithm, we can write $a = dq + r$, where q and r are integers and $0 \leq r < d$. Since $dq \in \mathbb{H}$ and $\mathbb{H}$ is closed under subtraction, it follows that

$$r = a - dq \in \mathbb{H}.$$

  Since $0 \leq r < d$ and d is the smallest positive integer in $\mathbb{H}$, we must have $r = 0$, that is, $a = dq \in d\mathbb{Z}$ and $\mathbb{H} \subseteq d\mathbb{Z}$. It follows that $\mathbb{H} = d\mathbb{Z}$.

□

Subgroups of $\mathbb{Z}$ and the greatest common divisors

Proof of the uniqueness.

We have proved that $\mathbb{H} = d\mathbb{Z}$ for some $d \in \mathbb{N}$. If $\{0\} \neq \mathbb{H} = d\mathbb{Z} = d'\mathbb{Z}$, where $d, d' \in \mathbb{Z}_+$, then $d' \in d\mathbb{Z}$ implies that $d' = dq$ for some $q \in \mathbb{Z}$, and $d \in d'\mathbb{Z}$ implies that $d = d'q'$ for some integer $q' \in \mathbb{Z}$. Therefore,

$$d = d'q' = dqq',$$

and so $qq' = 1$, hence $q = q' = \pm 1$ and $d = \pm d'$. Since $d, d' \in \mathbb{Z}_+$, we have $d = d'$, and consequently d is unique as claimed. $\square$

Definition of the greatest common divisor

Let $\emptyset \neq A \subseteq \mathbb{Z}$ be a set of integers, not all zero.

- If the integer d divides a for all $a \in A$, then d is called a common divisor of A.
- For example, 1 is a common divisor of every nonempty set of integers.
- The positive integer d is called the greatest common divisor of the set A, denoted by $d = \gcd(A)$, if d is a common divisor of A and every common divisor of A divides d.

Greatest common divisors

Theorem

Let $\emptyset \neq A \subseteq \mathbb{Z}$ be a set of integers, not all zero. Then A has a unique greatest common divisor, and there exist integers $a_1, \ldots, a_k \in A$ and $x_1, \ldots, x_k \in \mathbb{Z}$ such that

$$\gcd(A) = a_1 x_1 + \cdots + a_k x_k.$$

Proof.

Let $\mathbb{H} := \{a_1 x_1 + \cdots + a_k x_k : a_1, \ldots, a_k \in A,\ x_1, \ldots, x_k \in \mathbb{Z} \text{ for } k \in [\#A]\}$.

- Then $\mathbb{H}$ is a subgroup of $\mathbb{Z}$ and $A \subseteq \mathbb{H}$. By the previous theorem there exists a unique $d \in \mathbb{Z}_+$ such that $\mathbb{H} = d\mathbb{Z}$.
- In particular, every integer $a \in A$ is a multiple of d, and so d is a common divisor of A. Since $d \in \mathbb{H}$, there exist integers $a_1, \ldots, a_k \in A$ and $x_1, \ldots, x_k \in \mathbb{Z}$ for some $k \in [\#A]$ such that

$$d = a_1 x_1 + \cdots + a_k x_k.$$

- From this formula it follows that every common divisor of A must divide d, hence d is a greatest common divisor of A.
- If the positive integers d and d' are both greatest common divisors, then $d \mid d'$ and $d' \mid d$, and so $d = d'$. It follows that $\gcd(A)$ is unique.

□

Greatest common divisors and Euclid's lemma

If $A = \{a_1, \ldots, a_k\}$ is a nonempty, finite set of integers, not all zero, we write $\gcd(A) = (a_1, \ldots, a_k)$. Then the previous theorem readily implies.

Theorem (GCD theorem)

Let $a_1, \ldots, a_k \in \mathbb{Z}$ be integers, not all zero. Then $(a_1, \ldots, a_k) = 1$ if and only if there exist integers $x_1, \ldots, x_k \in \mathbb{Z}$ such that

$$a_1 x_1 + \cdots + a_k x_k = 1.$$

Definition

- The integers $a_1, \ldots, a_k \in \mathbb{Z}$ are called relatively prime or coprime if their greatest common divisor is 1, that is, $(a_1, \ldots, a_k) = 1$.
- The integers $a_1, \ldots, a_k \in \mathbb{Z}$ are called pairwise relatively prime if $(a_i, a_j) = 1$ for $i \neq j$.

Lemma (Euclid's lemma)

Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Proof.

Since $(a, b) = 1$, by the previous theorem, we can write $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Therefore, multiplying by c gives us $c = acx + bc$. Since $a \mid acx$ and $a \mid bc$, it follows that $a \mid c$ as desired. □

Consequences of Euclid's lemma

Theorem (GCD theorem for products)

Let $k \geq 2$, and let $a, b_1, b_2, \ldots, b_k \in \mathbb{Z}$. If $(a, b_i) = 1$ for all $i \in [k]$, then

$$(a, b_1 b_2 \cdots b_k) = 1.$$

Proof.

Assume that $k = 2$ and $d = (a, b_1 b_2)$ and show that $d = 1$.

- Since $d \mid a$ and $(a, b_1) = 1$, it follows that $(d, b_1) = 1$.
- Since $d \mid b_1 b_2$, Euclid's lemma implies that d divides b_2.
- Therefore, d is a common divisor of a and b_2, but $(a, b_2) = 1$, so $d = 1$.
- Let $k \geq 3$ and we will proceed by induction on k. Assume that the result holds for $k - 1$. Let $a, b_1, \ldots, b_k$ be integers such that $(a, b_i) = 1$ for $i \in [k]$. The induction assumption implies that $(a, b_1 \cdots b_{k-1}) = 1$.
- Since we also have $(a, b_k) = 1$, it follows from the case $k = 2$ that $(a, b_1 \cdots b_{k-1} b_k) = 1$.

□

Exercise

Let $k \in \mathbb{Z}_+$, and let $a, b_1, \ldots, b_k \in \mathbb{Z}$. If $b_1, \ldots, b_k$ are pairwise relatively prime and all divide a, then $b_1 b_2 \cdots b_k \mid a$.

Euclid's algorithm

Theorem (The Euclidean algorithm)

Let $r_0 := a \in \mathbb{Z}_+, r_1 := b \in \mathbb{Z}_+$ *with* $b < a$ *be given. Apply the division algorithm repeatedly to obtain a set of remainders* $r_2, \ldots, r_{n+1}$ *defined by*

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2, && \textit{where} \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3, && \textit{where} \quad 0 < r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, && \textit{where} \quad 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n + r_{n+1}, && \textit{where} \quad r_{n+1} = 0.
\end{aligned}
$$

Then $r_n = \gcd(a, b)$.

Proof.

- There is $n \in \mathbb{Z}_+$ such that $r_{n+1} = 0$ because the r_i are decreasing and nonnegative. The last relation, $r_{n-1} = r_n q_n$, shows that $r_n \mid r_{n-1}$. The next to last shows that $r_{n-1} \mid r_{n-2}$. By induction, we see that r_n divides each r_i. In particular, $r_n \mid r_1 = b$ and $r_n \mid r_0 = a$.
- Now let d be any common divisor of a and b. The definition of r_2 shows that $d \mid r_2$. The next relation shows that $d \mid r_3$. By induction, d divides each r_i, so $d \mid r_n$. Hence, $r_n = \gcd(a, b)$. $\square$

Prime numbers

Definition (Prime and composite numbers)

- An integer $n \in \mathbb{Z}$ is called prime if $n > 1$ and if the only positive divisors of n are 1 and n.
- If $n > 1$ and if n is not prime, then n is called composite.
- The set of all prime numbers will be denoted by $\mathbb{P}$.

If $p \in \mathbb{P}$, $a \in \mathbb{Z}$ and $(p, a) > 1$, then the definition readily implies that $p \mid a$.

Example

The prime numbers less than 100 are:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.$$

Theorem

If $p \in \mathbb{P}$ and p divides a product of integers, then p divides one of the factors.

Proof.

Let $b_1, \ldots, b_k \in \mathbb{Z}$ be integers such that $p \mid b_1 \cdots b_k$. By the theorem on GCD with product of coprime factors we have $(p, b_i) > 1$ for some $i \in [k]$. Since $p \in \mathbb{P}$ is prime, it follows that p divides b_i as desired. $\square$

Factorization of integers into primes

Theorem (Factorization theorem)

Every integer $n > 1$ is either a prime number or a product of prime numbers.

Proof.

The theorem is clearly true for $n = 2$. Proceeding by induction on $n > 1$ we can assume that it is also true for every integer less than n. Then, if n is not prime, it has a positive divisor d such that $1 < d < n$. Hence, $n = cd$, where $1 < c < n$. By induction each of c and d is a product of prime numbers by induction. Therefore, n is also a product of prime numbers. □

Theorem (Euclid)

There are infinitely many prime number.

Proof after Hermite.

For each integer $n > 1$, let $p_n \in \mathbb{P}$ denote the smallest prime divisor of $n! + 1$, which exists by the factorization theorem. We readily see that $p_n > n$ and consequently the set of prime numbers $\mathbb{P}$ must be infinite. □

Remark

Euclid originally argued by contradiction, assuming that $\mathbb{P} = \{p_1, \ldots, p_n\}$ is finite for some $n \in \mathbb{Z}_+$. Then, considering $N = p_1 \cdots p_n + 1$ and applying the factorization theorem, we reach a contradiction.

Fundamental theorem of arithmetic

Theorem (Fundamental theorem of arithmetic)

Every integer $n > 1$ can be represented as a product of prime factors in only one way, apart from the order of the factors.

Proof.

- The theorem is obviously true for $n = 2$. Proceeding by induction on $n > 1$ we can assume that it is also true for every integer greater than 1 and less than n. If n is prime, there is nothing more to prove.
- Assume, that n is composite and has two factorizations, say

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t.$$

- We show that $s = t$ and that each p_i equals some q_j. Since $p_1 \mid q_1 \cdots q_t$, it must divide at least one factor. Relabel $q_1, \ldots, q_t$ so that $p_1 \mid q_1$. Then $p_1 = q_1$ since both $p_1, q_1 \in \mathbb{P}$. Dividing by p_1 on both sides we obtain

$$\frac{n}{p_1} = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t.$$

- If $s > 1$ or $t > 1$, then $1 < \frac{n}{p_1} < n$. By induction the two factorizations of $\frac{n}{p_1}$ must be identical, apart from the order of the factors. Therefore, $s = t$ and the conclusion follows. □

The standard prime power factorization

- For any $n \in \mathbb{N}$ and a prime number $p \in \mathbb{P}$, we define $v_p(n)$ as the greatest integer $r \in \mathbb{N}$ such that $p^r \mid n$. Then $v_p(n) \in \mathbb{N}$ and
$$v_p(n) \geq 1 \iff p \mid n.$$
- If $v_p(n) = r$ then we say that the prime power p^r exactly divides n, and write $p^r \parallel n$. The standard factorization of n is given by:
$$n = \prod_{p \mid n} p^{v_p(n)}.$$
- Since every positive integer is divisible by only a finite number of primes, we can also write:
$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)},$$
where the product is an infinite product over the set of all prime numbers and $v_p(n) = 0$ and $p^{v_p(n)} = 1$ for all but finitely many primes p.
- The function $v_p(n)$ is called the p-adic value of n. It is completely additive in the sense that $v_p(mn) = v_p(m) + v_p(n)$ for all positive integers m and n. For instance, $v_p(n!) = \sum_{k \in [n]} v_p(k)$.
- If $m \mid n$, then $v_p(m) \leq v_p(n)$ for all $p \in \mathbb{P}$.

Least common multiple

Definition of the least common multiple

Let $a_1, \ldots, a_k \in \mathbb{N}$ be nonzero integers.

- An integer $m \in \mathbb{Z}$ is called a common multiple of $a_1, \ldots, a_k$ if it is a multiple of a_i for all $i \in [k]$, that is, every integer $a_i \mid m$.
- The least common multiple of $a_1, \ldots, a_k$ is a positive integer $m \in \mathbb{Z}_+$ such that m is a common multiple of $a_1, \ldots, a_k$, and m divides every common multiple of $a_1, \ldots, a_k$.
- We denote by $\operatorname{lcm}(a_1, \ldots, a_k)$ the least common multiple of $a_1, \ldots, a_k$.

Theorem (Exercise, prove it!)

Let $a_1, \ldots, a_k \in \mathbb{Z}_+$ be positive integers. Then

$$\gcd(a_1, \ldots, a_k) = \prod_{p \in \mathbb{P}} p^{\min\{v_p(a_1), \ldots, v_p(a_k)\}},$$

and

$$\operatorname{lcm}(a_1, \ldots, a_k) = \prod_{p \in \mathbb{P}} p^{\max\{v_p(a_1), \ldots, v_p(a_k)\}}.$$

In particular, for $k = 2$, we have $a_1 a_2 = \gcd(a_1, a_2)\operatorname{lcm}(a_1, a_2)$.

Prime power factorization of $n!$. For instance, $10! = 2^8 3^4 5^2 7$

Theorem

For every positive integer $n \in \mathbb{Z}_+$ and a prime number $p \in \mathbb{P}$, we have

$$v_p(n!) = \sum_{r=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^r} \right\rfloor .$$

Proof.

Let $1 \leq m \leq n$. If p^r divides m, then $p^r \leq m \leq n$ and $r \leq \frac{\log n}{\log p}$. Since r is an integer, we have $r \leq \left\lfloor \frac{\log n}{\log p} \right\rfloor$, and thus,

$$v_p(m) = \sum_{\substack{r=1 \\ p^r \| m}}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} 1.$$

The number of positive integers not exceeding n that are divisible by p^r is exactly $\left\lfloor \frac{n}{p^r} \right\rfloor$, and so

$$v_p(n!) = \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{\substack{r=1 \\ p^r \| m}}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} 1 = \sum_{r=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \sum_{\substack{m=1 \\ p^r \| m}}^{n} 1 = \sum_{r=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^r} \right\rfloor . \qquad \square$$

Euler's theorem

Theorem (Euler's theorem)

One has that

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty.$$

In particular, this implies that $\mathbb{P}$ *is infinite.*

Proof.

For every positive integer $n \in \mathbb{Z}_+$, we have

$$\sum_{k=1}^{n} \frac{1}{k} \leq \prod_{p \leqslant n} \left(1 - \frac{1}{p}\right)^{-1}.$$

- Indeed, take $m \in \mathbb{Z}_+$ so that $2^m > n$ and observe that

$$\left(1 - \frac{1}{p}\right)^{-1} = \sum_{k=0}^{\infty} \frac{1}{p^k} \geq \sum_{k=0}^{m} \frac{1}{p^k}.$$

  In the first equality, we used the expansion into a geometric series.

Euler's theorem: proof

- Let $\mathbb{P}_{\leq n} := \{p \in \mathbb{P} : p \leq n\} := \{p_1, \ldots, p_l\}$. By the last inequality

$$\prod_{p \leq n} \left(1 - \frac{1}{p}\right)^{-1} \geq \prod_{p \leqslant n} \sum_{k=0}^{m} \frac{1}{p^k} = \prod_{j=1}^{l} \sum_{k=0}^{m} \frac{1}{p_j^k} = \sum_{k_1=0}^{m} \cdots \sum_{k_l=0}^{m} \frac{1}{p_1^{k_1} \cdots p_l^{k_l}} \geq \sum_{k=1}^{n} \frac{1}{k},$$

  since every integer $1 < k \leq n$ can be written as $k = \prod_{p \in \mathbb{P}_{\leq n}} p^{v_p(k)}$, where $v_p(k) \leq m$ due to our choice of $m \in \mathbb{Z}_+$ satisfying $2^m > n$.
- Now using

$$\sum_{k \leqslant n} \frac{1}{k} > \int_1^n \frac{\mathrm{d}t}{t} = \log n,$$

  we obtain that

$$\log \log n < \log \prod_{p \leqslant n} \left(1 - \frac{1}{p}\right)^{-1} = -\sum_{p \leqslant n} \log \left(1 - \frac{1}{p}\right).$$

  By the Taylor expansion for $0 \leqslant x < 1$, we may write

$$-\log(1-x) = \sum_{k=1}^{\infty} \frac{x^k}{k} < x + \frac{1}{2} \sum_{k=2}^{\infty} x^k \leq x + \frac{x^2}{2(1-x)}.$$

Euler's theorem: proof

- Combining this Taylor expansion for $x = 1/p$ with the last inequality, we have

$$\begin{aligned}
\log\log n < \log \prod_{p \leqslant n} \left(1 - \frac{1}{p}\right)^{-1} &= -\sum_{p \leqslant n} \log\left(1 - \frac{1}{p}\right) \\
&\leqslant \sum_{p \leqslant n} \frac{1}{p} + \frac{1}{2} \sum_{p \leqslant n} \frac{1}{p(p-1)} \\
&\leqslant \sum_{p \leqslant n} \frac{1}{p} + \frac{1}{2} \sum_{k=2}^{\infty} \frac{1}{k(k-1)} = \sum_{p \leqslant n} \frac{1}{p} + \frac{1}{2}
\end{aligned}$$

  so that

$$\sum_{p \leqslant n} \frac{1}{p} > \log\log n - \frac{1}{2}.$$

- Hence we deduce that the series $\sum_{p \in \mathbb{P}} 1/p$ is divergent, which implies that there are infinitely many primes. □

Sieve of Eratosthenes

The sieve is based on a simple observation.

Observation

If an $n \in \mathbb{Z}_+$ is composite, then n can be written in the form $n = d_1 \cdot d_2$, where $1 < d_1 \leq d_2 < n$. If $d_1 > \sqrt{n}$, then we obtain a contradiction, since

$$n = d_1 \cdot d_2 > \sqrt{n} \cdot \sqrt{n} = n.$$

- Therefore, if $n \in \mathbb{Z}_+$ is composite, then n has a divisor d such that $1 < d \leq \sqrt{n}$. In particular, every composite number $n \leq x$ is divisible by a prime $p \leq \sqrt{x}$.

Eratosthenes algorithm

To find all the primes up to x, we write down the integers between 1 and x, and eliminate numbers from the list according to the following rule:

1. Cross out 1. The first number in the list that is not eliminated is 2; cross out all multiples of 2 that are greater than 2.
2. The iterative procedure is as follows: Let d be the smallest number on the list whose multiples have not already been eliminated. If $d \leq \sqrt{x}$, then cross out all multiples of d that are greater than d. If $d > \sqrt{x}$, stop.

This algorithm must terminate after at most x steps. The prime numbers up to x are the numbers that have not been crossed out.

Sieve of Eratosthenes for $n = 40$

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40

- In the first step we remove 1 and all multiples of 2 grater than 2:

	2	3		5		7		9	
11		13		15		17		19	
21		23		25		27		29	
31		33		35		37		39	

- In the second step we remove all multiples of 3 grater than 3:

	2	3		5		7			
11		13				17		19	
		23		25				29	
31						37			

- In the third step we remove all multiples of 5 grater than 5:

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			

- In the fourth step the algorithm stops, since $7 > \sqrt{40}$.

A first glance at sieve theory

The prime counting function

For $x \in \mathbb{R}_+$ the set of all prime numbers not exceeding x will be denoted by $\mathbb{P}_{\leq x} := \mathbb{P} \cap [0, x]$. The counting function for $\mathbb{P}_{\leq x}$ will be denoted by

$$\pi(x) := \#\mathbb{P}_{\leq x} := \{p \in \mathbb{P} : p \leq x\}.$$

- Let $n \geqslant 2$ be a fixed integer. As a consequence of Eratosthenes sieve, an integer $m \in (\sqrt{n}, n]$ is a prime number if and only if

$$\Big(m, \prod_{p \in \mathbb{P}_{\leq \sqrt{n}}} p\Big) = 1.$$

- If S_n is the set of positive integers $m \leqslant n$ which are not divisible by all prime numbers $\leqslant \sqrt{n}$, then by Eratosthenes sieve we have

$$\mathbb{P}_{\leq n} \subseteq S_n \cup \{1, \ldots, \sqrt{n}\},$$

  and $S_n = \pi(n) - \pi(\sqrt{n}) + 1$, which implies

$$\pi(n) \leq \#S_n + \lfloor \sqrt{n} \rfloor.$$

Counting primes using sieve

- More generally, let $r \geqslant 2$ be an integer. We define $\pi(n, r)$ to be the number of positive integers $m \leqslant n$ which are not divisible by prime numbers $\leqslant r$ (hence $\#S_n = \pi(n, [\sqrt{n}])$). Similarly as above, we have

$$\pi(n) \leqslant \pi(n, r) + r.$$

Exclusion–inclusion principle

Consider N objects and r properties denoted by $p_1, \ldots, p_r$. Suppose that $A = \{p_{i_1}, \ldots, p_{i_m}\}$ for some $m \in [r]$ and let N_A be the number of objects that satisfy properties $p_{i_1}, \ldots, p_{i_m}$. Then, the number S of objects that satisfy none of those properties is equal to

$$S = \sum_{k=0}^{r} (-1)^k \sum_{\substack{A \subseteq r \\ \#A = k}} N_A.$$

Applying the exclusion–inclusion principle to $\pi(n, r)$, we obtain

$$\pi(n, r) = n - \sum_{p \leq r} \left\lfloor \frac{n}{p} \right\rfloor + \sum_{p_1 < p_2 \leq r} \left\lfloor \frac{n}{p_1 p_2} \right\rfloor - \sum_{p_1 < p_2 < p_3 \leq r} \left\lfloor \frac{n}{p_1 p_2 p_3} \right\rfloor + \cdots + (-1)^r \left\lfloor \frac{n}{p_1 \cdots p_r} \right\rfloor.$$

Counting primes using sieve

- Since $x-1 < \lfloor x \rfloor \leqslant x$, we obtain

$$\begin{aligned}\pi(n,r) &< n - \sum_{p\leqslant r}\frac{n}{p} + \sum_{p_1<p_2\leqslant r}\frac{n}{p_1p_2} + \cdots + (-1)^r\frac{n}{p_1\cdots p_r} + \sum_{k=1}^{k}\sum_{p_1<\ldots<p_k\leqslant r} 1 \\ &= n - \sum_{p\leqslant r}\frac{n}{p} + \sum_{p_1<p_2\leqslant r}\frac{n}{p_1p_2} + \cdots + (-1)^r\frac{n}{p_1\cdots p_r} + \sum_{k=1}^{r}\binom{\pi(r)}{k} \\ &= n\prod_{p\leqslant r}\left(1-\frac{1}{p}\right) + 2^{\pi(r)} - 1.\end{aligned}$$

- Now inserting this bound to $\pi(n) \leqslant \pi(n,r) + r$, implies that

$$\pi(n) < n\prod_{p\leqslant r}\left(1-\frac{1}{p}\right) + 2^{\pi(r)} + r - 1.$$

- In the proof of Euler's theorem we showed that

$$\sum_{p\leqslant n}\frac{1}{p} > \log\log n - \frac{1}{2}.$$

Counting primes using sieve

- Using $\log(1-x) \leqslant -x$ and the last bound, we obtain

$$\prod_{p \leqslant r} \left(1 - \frac{1}{p}\right) \leqslant \exp\left(-\sum_{p \leqslant r} \frac{1}{p}\right) < \frac{e^{1/2}}{\log r}.$$

- This implies

$$\pi(n) < \frac{ne^{1/2}}{\log r} + 2^r + r - 1.$$

- Choosing $r = 1 + \lfloor \log n \rfloor$ with $n \geqslant 10$ implies that

$$\pi(n) < \frac{3n}{\log \log n}.$$

- This shows that $\pi(n) = o(n)$ as $n \to \infty$, which says that the set of prime numbers has zero upper density.
- The upper density for $A \subseteq \mathbb{N}$ is defined by

$$\limsup_{N \to \infty} \frac{\#(A \cap [1, N])}{N} \geq 0.$$