Discrete mathematics

Bernadett Aradi, Ágnes Baran

2023 Fall

Table of contents

Introduction: sets

- Set, element of a set (notation: $\in$, negation: $\notin$): basic concepts.
- Defining a set: by enumeration, e.g., $\{1, 2, 3\}$,
  or with the help of a defining property T concerning the elements of a given set S in the way $\{x \in S \mid T(x)\}$, e.g.,

$$\{x \in \mathbb{N} \mid 1 \leq x \leq 5\}.$$

- Emptyset: the unique set, that doesn't have any element.
  Notation: $\emptyset$.
- Notation of the subset relation: $\subset$.
- Two sets are equal or coincide if their elements are the same.
  Equivalently, if they are each others' subsets:

$$A = B \iff A \subset B \text{ and } B \subset A.$$

Cardinality of sets, power set

Definition

The power set of a given set S is the set of all subsets of S. Notation: $\mathcal{P}(S)$ or 2^S.

E.g., in the case of $S = \{0, 1, 2, 3\}$:

$$\mathcal{P}(S) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{0,1,2\}, \{0,1,3\}, \{0,2,3\}, \{1,2,3\}, S\}$$

Definition

If a set has a finite number of elements, then this number is called the cardinality of the set. Notation for a given set S: $\#S$.
In this case we say that S is a finite set.

Theorem

If S has cardinality of n, then the power set of S has cardinality of 2^n, that is

$$\#(\mathcal{P}(S)) = 2^{\#S}.$$

Fundamental operations on sets

- The complement of a set A: $\overline{A}$.
- The union of two sets: $A \cup B$.
- The intersection of two sets: $A \cap B$.
- The (set-theoretic) difference of two sets: $A \setminus B$.
- The symmetric difference of two sets, notation: $\triangle$.

$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$$

  E.g., if $A = \{0, 1, 2, 3, 4\}$, $B = \{2, 4, 6, 8, 10\}$ what is $A \triangle B =$?

- The Cartesian product of two sets, notation: $\times$.

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

  E.g., if $A = \{0, 1, 2\}$, $B = \{1, 2\}$ what is $A \times B =$?

Theorem – De Morgan's laws

If A and B are arbitrary sets, then

$$\overline{(A \cup B)} = \overline{A} \cap \overline{B} \quad \text{and} \quad \overline{(A \cap B)} = \overline{A} \cup \overline{B}.$$

Furthermore, these identities hold for arbitrary number of sets.

Notation

Special sets of numbers:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$: the set of natural numbers (to be defined later)
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$: the set of integers
- $\mathbb{Q}$: the set of rational numbers
- $\mathbb{R}$: the set of real numbers
- $\mathbb{C}$: the set of complex numbers (to be defined later)

Quantifiers:

- $\exists$: 'there exists' (existential quantifier)
- $\forall$: 'for all' (universal quantifier)

E.g., $\exists n \in \mathbb{N} : 2n = 6$, but $\nexists n \in \mathbb{N} : 2n = 7$

$\forall m \in \mathbb{N} : m \in \mathbb{Z}$, but $\not\forall m \in \mathbb{Z} : m \in \mathbb{N}$

Introduction: functions

Function: an association rule, assignment or correspondence $x \mapsto f(x)$

If the function f accomplishes a correspondence between the set D (the domain of the function) and the set R (the range of the function), then we can view the function as pairs $(x, f(x))$, where $x \in D$ and $f(x) \in R$.

$$f\colon D \to R,\ x \mapsto f(x)$$

That is, the function is a subset of the Cartesian product $D \times R$, such that if

$$f\colon x \mapsto y_1 \ \text{ and } \ f\colon x \mapsto y_2,$$

then necessarily $y_1 = y_2$.

Examples of functions

- $x \in \mathbb{R}$, $x \mapsto f(x) := x^2$
- $x \in \mathbb{R}^+$, $x \mapsto f(x) := \{$a number with square $x\}$

  Not a function!
- $n \in \mathbb{N}$, $n \mapsto f(n) := \{$an odd number such that it's a divisor of $n\}$

  Not a function!
- $n \in \mathbb{N}$, $n \mapsto f(n) := \{$the greatest positive divisor of $n\}$

  Function!

Notation

The meaning of $:=$ is: definition, prescribing a value, 'let it be equal with'

Notation

The meaning of different arrows: $\to$, $\mapsto$, $\Rightarrow$, $\Leftrightarrow$

Basic functions

- constant: $f(x) = c$
- first order (linear): $f(x) = mx + b$
- second order: $f(x) = ax^2 + bx + c \quad (a \neq 0)$
  factored form: $f(x) = a \cdot \left(x - \frac{-b+\sqrt{b^2-4ac}}{2a}\right) \cdot \left(x - \frac{-b-\sqrt{b^2-4ac}}{2a}\right)$
- polynomial
- exponential: $f(x) = a^x \quad (a > 0,\ a \neq 1)$
- logarithmic: $f(x) = \log_a x \quad (a > 0,\ a \neq 1)$
- trigonometric functions
- absolute value function
- sign function or signum function

Properties of functions

Let us consider an arbitrary function

$$f\colon D \to R,\; x \mapsto f(x).$$

Definition

The function f is injective if $f(a) = f(b)$ implies $a = b$.

That is, in this case the function f assigns a *different* value to each element.

Definition

The function f is surjective if for every element y in R there exists an element $x \in D$ such that $f(x) = y$.

That is, f is surjective if all elements of R become an image of an element.

Definition

The function f is bijective if it is injective and surjective.

Reasoning with mathematical induction

Let us assume that we want to prove a proposition (for example, the relation below) for *all natural numbers*:

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \quad \forall n \in \mathbb{N}.$$

Then we can use the following reasoning:

(1) **We prove** the proposition for $n = 1$. (By trial and error.)

(2a) **We assume** that the proposition is true for an arbitrary natural number k,

(2b) then **we prove** it for the natural number $k + 1$.

(2a): inductive hypothesis

The set of natural numbers

For the axiomatic introduction of this set we use the so-called Peano axioms.

Definition – Peano axioms

- (P1) 1 is a natural number.
- (P2) For every natural number n there exists uniquely a successor natural number.
- (P3) There is no natural number whose successor is 1.
- (P4) If two natural numbers have the same successors, then the two natural numbers coincide.
- (P5) Axiom of induction: if A is a set such that
  - it contains the natural number 1,
  - for every element of A its successor is also in A,

  then A contains all the natural numbers.

The conditions (P1)–(P5) uniquely determine a set, which is called the set of natural numbers. Notation: $\mathbb{N}$.

Remarks on the Peano axioms

(P2) For every natural number n it is possible to provide a 'greater by 1' natural number, which is called the successor of n.
$\rightsquigarrow$ $n+1$, $S(n)$ (S: successor function)

(P4) If two natural numbers have the same successors, then the two natural numbers coincide.
In other words: the successor function is injective.

(P5) Axiom of induction: if A is a set such that

- it contains the natural number 1,
- for every element of A its successor is also in A,

then A contains all the natural numbers.
In other words: A is an inductive set. $\Rightarrow$ $\mathbb{N}$ is the smallest inductive set.
Another example for inductive sets: the set of positive numbers ($\mathbb{R}^+$).

The Peano axioms with mathematical formalism

Definition – Peano axioms

Let $\mathbb{N}$ be a set satisfying the following conditions:

- P1 $1 \in \mathbb{N}$
- P2 $\forall n \in \mathbb{N} : \exists S(n) \in \mathbb{N},\ S(n) =: n + 1$
  or: $\exists S : \mathbb{N} \to \mathbb{N}$ so-called successor function
- P3 $\nexists n \in \mathbb{N} : S(n) = 1$
- P4 $n, m \in \mathbb{N} : S(n) = S(m) \Rightarrow n = m$
- P5

$$\left.\begin{array}{l} 1 \in A \\ n \in A \Rightarrow S(n) \in A \end{array}\right\} \Longrightarrow \mathbb{N} \subset A$$

Then $\mathbb{N}$ is uniquely determined, and it is called the set of natural numbers.

Proof by induction

Based on the definition the elements of $\mathbb{N}$ are:

$$1,\ S(1),\ S(S(1)),\ S(S(S(1))), \dots, S(S(\dots(S(1))\dots)), \dots$$
$$S(1) = 1 + 1 =: 2$$
$$S(S(1)) = S(1) + 1 =: 3$$

The axiom of induction expresses that all the natural numbers can be given with the help of the special natural number 1 and the successor function S. Thus, if we want to prove a proposition (for example, a relation below) for *all natural numbers*, then we can apply the reasoning of mathematical induction:

(1) **We prove** the proposition for $n = 1$. (By trial and error.)

(2a) **We assume** that the proposition is true for an arbitrary natural number k,

(2b) then **we prove** it for the natural number $k + 1$.

(2a): inductive hypothesis

Examples for proof by induction

1. The sum of the first n natural numbers is $\frac{n(n+1)}{2}$. We can apply induction here. ✓
2. $x + \frac{1}{x} \geq 2, \forall x > 0$. We cannot apply induction for this!
3. Prove that
$$1 + 3 + 5 + \cdots + (2n-1) = n^2, \quad \forall n \in \mathbb{N}.$$
4. Prove that
$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}, \quad n \in \mathbb{N}.$$

Notation

$$\sum_{i=1}^{n} \text{sum}, \qquad \prod_{i=1}^{n} \text{product}$$

Prove that

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2, \quad \forall n \in \mathbb{N}.$$

(1) **We prove** the proposition for $n = 1$:
left-hand side: 1 right-hand side: $1^2 = 1$.
$\implies$ the proposition is true for $n = 1$

(2a) **We assume** that the proposition is true for an arbitrary natural number k:

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2$$

(2b) then **we prove** it for the natural number $k + 1$:
The proposition:

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2$$

The proof:

$$\underbrace{1 + 3 + 5 + \cdots + (2k - 1)}_{k^2} + (2k + 1) = k^2 + 2k + 1 = (k + 1)^2$$

Prove that

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}, \quad n \in \mathbb{N}.$$

(1) **We prove** the proposition for $n = 1$:
left-hand side: $1^2 = 1$ right-hand side: $\frac{1\cdot(1+1)(2\cdot 1+1)}{6} = 1.$
$\Longrightarrow$ the proposition is true for $n = 1$

(2a) **We assume** that the proposition is true for an arbitrary natural number k:

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}, \quad n \in \mathbb{N}.$$

(2a) **We assume** that the proposition is true for an arbitrary natural number k:

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}, \quad n \in \mathbb{N}.$$

(2b) then **we prove** it for the natural number $k+1$:
The proposition:

$$1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

The proof:

$$\underbrace{1^2 + 2^2 + 3^2 + \cdots + k^2}_{\frac{k(k+1)(2k+1)}{6}} + (k+1)^2 = \frac{(k+1)[6(k+1) + k(2k+1)]}{6} =$$

$$\frac{(k+1)[6k + 6 + 2k^2 + k]}{6} = \frac{(k+1)(k+2)(2k+3)}{6}$$

The set of integers

The set of integers can be introduced with the help of the already defined set of natural numbers.

The set of integers ($\mathbb{Z}$) is the smallest set which contains the natural numbers and is closed under subtraction.

Divisors, divisibility

Let $a, b \in \mathbb{Z}$.

Definition

We say that b is a divisor of a, or a is a multiple of b, or a is divisible by b if there exists $c \in \mathbb{Z}$ such that $a = b \cdot c$. Notation: $b|a$

Theorem – the properties of divisibility

1. $\forall a \neq 0, a \in \mathbb{Z} : a|0,\ 1|a,\ a|a$
2. If $a|b$ and $c \in \mathbb{Z}$, then $a|bc$. $(a|b \wedge c \in \mathbb{Z} \Rightarrow a|bc)$
3. If $a|b_1$ and $a|b_2$, then $a|(b_1 + b_2)$.
4. If $a|b$ and $b|c$, then $a|c$.
5. If $a|b$ and $b|a$, then $a = \pm b$.

2 and 3 $\Rightarrow$ If $a|b_i$, $i = 1, 2, \ldots, n$ and $c_1, c_2, \ldots, c_n \in \mathbb{Z}$, then

$$a|(b_1c_1 + b_2c_2 + \cdots + b_nc_n).$$

Divisibility rules

$A \in \mathbb{N} \Rightarrow$

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0,$$

$$a_i \in \{0, 1, \ldots, 9\},\ a_n \neq 0.$$

- Divisibility by 2

$$A = (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1) \cdot 10 + a_0$$

$2|10$, thus if $2|a_0$, then $2|A$

- Divisibility by 5: $A =$as above
  $5|10$, thus if $5|a_0$, then $5|A$

Divisibility rules

$A \in \mathbb{N} \Rightarrow$

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0,$$

$$a_i \in \{0, 1, \ldots, 9\},\ a_n \neq 0.$$

- Divisibility by 4: $4 \not| 10$, but $4|100$

$$A = (a_n \cdot 10^{n-2} + a_{n-1} \cdot 10^{n-3} + \cdots + a_2) \cdot 100 + a_1 \cdot 10 + a_0$$

$4|100$, so if $4|(a_1 \cdot 10 + a_0)$, then $4|A$

- Divisibility by 25: analogously to 4, since $25|100$.

Divisibility rules

- Divisibility by 8: $8 \not| 100$, however $8 | 1000 \Rightarrow$

$$8 | A \iff 8 | (100a_2 + 10a_1 + a_0)$$

  $100a_2 + 10a_1 + a_0$ is the remainder when dividing A by 1000.

- Divisibility by 3 and 9: $10^k - 1 = 99\ldots9 \Rightarrow 3|(10^k - 1)$, $9|(10^k - 1)$

$$\begin{aligned} A &= a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = \\ &= a_n(10^n - 1) + a_{n-1}(10^{n-1} - 1) + \cdots + a_1(10 - 1) + \\ &\quad + a_n + a_{n-1} + \cdots + a_1 + a_0 \end{aligned}$$

  $\Rightarrow A$ is divisible by 3 or 9 if the sum of its digits is divisible by 3 or 9

- Divisibility by 11: $10^1+1=11$, $10^2-1=99$, $10^3+1=1001$, $10^4-1=9999$, ... We can prove that

$$11|(10^k+1) \text{ if } k \text{ is odd and } 11|(10^k-1) \text{ if } k \text{ is even.}$$

$$\begin{aligned} A &= a_0 + a_1(10^1+1) - a_1 + a_2(10^2-1) + a_2 + \dots = \\ &= (a_1(10^1+1) + a_2(10^2-1) + \dots) + (a_0 - a_1 + a_2 - a_3 + \dots) \end{aligned}$$

$\Rightarrow$ A is divisible by 11 if the alternating sum of its digits is divisible by 11

Definition

We say that $d \in \mathbb{N}$ is the greatest common divisor of the integers a and b

- $d|a$ and $d|b$,
- for all $\bar{d} \in \mathbb{N}$ such that $\bar{d}|a$ and $\bar{d}|b$, the relation $\bar{d}|d$ also holds.

Notation: $d = \gcd(a, b)$.

Furthermore $d \in \mathbb{N}$ is the greatest common divisor of $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ if

- $d|a_i$, $i \in \{1, \ldots, n\}$,
- for every $\bar{d} \in \mathbb{N}$ such that $\bar{d}|a_i$ $(i \in \{1, \ldots, n\})$, the relation $\bar{d}|d$ also holds.

Definition

The integers a and b are called relatively prime or coprime numbers if $\gcd(a, b) = 1$.

Definition

We say that $k \in \mathbb{N}$ is the least common multiple of $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ if

- $a_i|k$, $i \in \{1, \ldots, n\}$,
- for all $\bar{k} \in \mathbb{N}$ such that $a_i|\bar{k}$ $(i \in \{1, \ldots, n\})$, the property $k|\bar{k}$ also holds.

Notation: $k = \operatorname{lcm}(a_1, a_2, \ldots, a_n)$.

The Euclidean algorithm

Theorem – Euclidean division

Given arbitrary $a, b \in \mathbb{Z}$, $b \neq 0$ numbers there uniquely exist integers $q, r \in \mathbb{Z}$ such that
$$a = b \cdot q + r, \quad 0 \leq r < |b|.$$

The Euclidean algorithm (or Euclid's algorithm)

$a, b \in \mathbb{Z}$, $b \neq 0$, theorem above $\Rightarrow q, r \in \mathbb{Z}$, let us denote them by q_0, r_0 this time:
$$a = b \cdot q_0 + r_0$$
Let us repeat the Euclidean division with b and $r_0 \Rightarrow q_1, r_1 \in \mathbb{Z}$, then with r_0 and r_1 ($\Rightarrow q_2, r_2 \in \mathbb{Z}$):

$$b = r_0 \cdot q_1 + r_1$$
$$r_0 = r_1 \cdot q_2 + r_2.$$

By continuing the procedure in this manner (each time with the obtained remainders) we finish in finite steps, since
$$|b| > r_0 > r_1 > r_2 > \cdots > r_i > \cdots \geq 0.$$

Theorem

When applying the Euclidean algorithm for the integers a and $b \neq 0$, the last non-zero remainder is the greatest common divisor of a and b. Furthermore, if $d := \gcd(a, b)$, then the equation

$$ax + by = d$$

can be solved among integers. That is, there exist $x, y \in \mathbb{Z}$ solutions.

Example: $\gcd(1227, 216) = ?$, $\gcd(-1227, -216) = ?$

$$1227 = 216 \cdot 5 + 147$$
$$216 = 147 \cdot 1 + 69$$
$$147 = 69 \cdot 2 + 9$$
$$69 = 9 \cdot 7 + 6$$
$$9 = 6 \cdot 1 + \boxed{3}$$
$$6 = 3 \cdot 2 + 0$$

$\gcd(1227, 216) = 3$

Definition

Equations of the form $ax + by = c$ (where $a, b, c \in \mathbb{Z}$ are known, $x, y \in \mathbb{Z}$ are unknown) are called linear Diophantine equations.

Theorem

The linear Diophantine equation $ax + by = c$ is solvable if, and only if, $\gcd(a, b) | c$.

Theorem

If the Diophantine equation $ax + by = c$ is solvable, then it has infinitely many solutions, which can be written in the form

$$x = x_0 + t\frac{b}{\gcd(a, b)}, \quad y = y_0 - t\frac{a}{\gcd(a, b)}, \quad t \in \mathbb{Z},$$

where (x_0, y_0) is a particular solution.

Examples

. Solve the following Diophantine equations.

1. $168x - 45y = 12$, where $x, y \in \mathbb{Z}$
2. $700x + 539y = 21$, where $x, y \in \mathbb{Z}$
3. $300x - 147y = 14$, where $x, y \in \mathbb{Z}$

Prime numbers

Every $n > 1$, $n \in \mathbb{N}$ has two positive divisors: 1 and n, these are called the trivial divisors of n. All the other divisors are called non-trivial divisors.

Definition

Natural numbers which are greater than 1 and has only trivial divisors are called prime numbers or primes. Natural numbers with also non-trivial divisors are called composite numbers. 1 is a unit.

Theorem

An integer $p > 1$ is prime if, and only if, $p|ab$ implies $p|a$ or $p|b$.

Theorem – the fundamental theorem of arithmetic (also called unique-prime-factorization theorem)

Every natural number greater than 1 is either a prime itself or is the product of prime numbers. Furthermore, this product is unique up to the order of the factors. The obtained unique product is called the canonical representation or the standard form of n, which is $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where $p_1, p_2, \dots, p_r$ are pairwise different primes, $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N}$.

Number of divisors

Theorem

The number of positive divisors of a natural number $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ is

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1).$$

Example: $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$ and $14850 = 2 \cdot 3^3 \cdot 5^2 \cdot 11$

gcd and lcm from the canonical representation

Example

Determine $\gcd(1260, 14850)$ and $\operatorname{lcm}(1260, 14850)$.

$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$ and $14850 = 2 \cdot 3^3 \cdot 5^2 \cdot 11$

gcd: take the common prime factors to the smaller power
$1260 = 2^2 \cdot 3^2 \cdot 5^1 \cdot 7$ and $14850 = 2^1 \cdot 3^3 \cdot 5^2 \cdot 11$

$\gcd(1260, 14850) = 2 \cdot 3^2 \cdot 5 = 90$

lcm: take all the prime factors to the greater power
$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^1$ and $14850 = 2 \cdot 3^3 \cdot 5^2 \cdot 11^1$

$\operatorname{lcm}(1260, 14850) = 2^2 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 = 207900$

Theorem

There are infinitely many prime numbers.

Proof: Suppose that there are only finitely many prime numbers, let them be $p_1, p_2, \ldots, p_k$. Consider the number $b = p_1 \cdot p_2 \cdot \cdots \cdot p_k + 1$. Then $b \neq 1$ and b is a composite number, thus for some index $i \in \{1, 2, \ldots, k\}$ we have $p_i | b$. But $p_i | \prod p_j$ as well, thus $p_i | 1$, which is a contradiction.

Remark

The integers a and b are coprime numbers if there are no common prime factors in their canonical representation.

Congruence

Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$.

Definition

We say that a and b are congruent modulo m if $m|(a-b)$.
Notation: $a \equiv b \pmod{m}$, m: is the modulus of the congruence.

Example: for $m = 4$ we have $3 \equiv 11 \pmod{4}$

The integers $a, b \in \mathbb{Z}$ are congruent modulo m if they provide the same remainder when divided by m.

Theorem

The congruence modulo m is a so-called equivalence relation: reflexive, symmetric, transitive.

Definition

Let us consider the class of integers which are congruent with each other modulo m. The obtained classes are called the congruence classes or residue classes modulo m. The residue classes are represented by the integers $0, 1, \ldots, m-1$. Thus, there are m residue classes modulo m.

The properties of congruence

Proposition – the properties of congruence

Let $m \in \mathbb{N}$ $(m \geq 2)$ and $a, b, c, d \in \mathbb{Z}$.

1. If $a \equiv b$ and $c \equiv d \pmod{m}$, then
$$a \pm c \equiv b \pm d \pmod{m} \quad \text{and} \quad a \cdot c \equiv b \cdot d \pmod{m}.$$
2. If $a \cdot c \equiv b \cdot c \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b$.

Example: $15 \equiv 63 \pmod{8}$

Definition

Any set of m integers, no two of which are congruent modulo m, is called a complete residue system modulo m. The set of integers $\{0, 1, 2, \ldots, m-1\}$ is called the least residue system modulo m.

Example: for $m = 5$ the set $\{5, 6, 12, 28, 9\}$ is a complete residue system, while $\{0, 1, 2, 3, 4\}$ is the least residue system.

Proposition

If $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

Reduced residue system

Definition

A residue class is a member of the reduced residue system if its members are coprime to the modulus. Notation: the number of elements of a reduced residue system modulo m is denoted by $\varphi(m)$. That is

$$\varphi(m) = \#\{a \in \{1, \dots, m\} \mid \gcd(a, m) = 1\}.$$

The name of the function φ: Euler's φ function or Euler's totient function.

By definition, $\varphi(1) = 1$.

m	complete	reduced	$\varphi(m)$
$m=2$	0,1	1	$\varphi(2)=1$
$m=3$	0,1,2	1,2	$\varphi(3)=2$
$m=4$	0,1,2,3	1,3	$\varphi(4)=2$
$m=5$	0,1,2,3,4	1,2,3,4	$\varphi(5)=4$
$m=6$	0,1,2,3,4,5	1,5	$\varphi(6)=2$
$m=7$	0,1,2,3,4,5,6	1,2,3,4,5,6	$\varphi(7)=6$

Euler's φ function

Proposition

If p is a prime, then $\varphi(p) = p - 1$.

Theorem

The value of Euler's φ function can be calculated by the formula

$$\varphi(m) = m \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right),$$

where m has canonical representation $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$.

Example: $m = 24$, $\varphi(24) = ?$

Theroem – Euler's theorem

If $\gcd(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Corollary – Fermat's little theorem

If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Example: what is the remainder when dividing 2^{2019} by 15?

Congruence equations

Theorem

The (linear) congruence equation $ax \equiv b \pmod{m}$ is solvable among integers if, and only if, $\gcd(a, m) | b$.

Proof: we can derive a Diophantine equation from the congruence equation:

$$ax \equiv b \pmod{m} \;\Leftrightarrow\; m|(ax - b) \;\Leftrightarrow$$
$$\Leftrightarrow\; \exists y \in \mathbb{Z}:\; my = ax - b \;\Leftrightarrow\; ax - my = b$$

Remark: if $c \in \mathbb{Z}$ is a solution, then so is $c + km$.

Example: $12x \equiv 8 \pmod{16}$
$\gcd(12, 16)|8 \quad \Longrightarrow$ the equation is solvable

Example

Solve the linear congruence equation $12x \equiv 8 \pmod{16}$.

$\gcd(12, 16) = 4|8 \quad \Longrightarrow$ the equation is solvable

Solution 1:
Solve the linear Diophantine equation $12x - 16y = 8$ (i.e. $3x - 4y = 2$)

Solution 2:
Consider the equation $\frac{12}{\gcd(12,16)} x \equiv \frac{8}{\gcd(12,16)} \pmod{\frac{16}{\gcd(12,16)}}$
Then

$$\begin{aligned} 3x &\equiv 2 \pmod{4} \\ 3x &\equiv 2 + 4 = 6 \pmod{4} \\ x &\equiv 2 \pmod{4} \qquad (\text{because } \gcd(3,4) = 1) \end{aligned}$$

The solutions:

$$x = \ldots, -10, -6, -2, 2, 6, 10, \ldots$$