Modular Arithmetic

Aleksandra Gorzkowska

Modular Arithmetic

Theorem (Division Notation)

Let $a, b \in \mathbb{Z}$, $b > 0$. *Then* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *where* $0 \leq r < b$.

Modular Arithmetic

Theorem (Division Notation)

Let $a, b \in \mathbb{Z}$, $b > 0$. *Then* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *where* $0 \leq r < b$.

Example

1. $a = 11, b = 3$: $11 = 3 \cdot 3 + 2$

Modular Arithmetic

Theorem (Division Notation)

Let $a, b \in \mathbb{Z}$, $b > 0$. *Then* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *where* $0 \leq r < b$.

Example

1. $a = 11, b = 3$: $11 = 3 \cdot 3 + 2$
2. $a = -11, b = 3$: $-11 = -4 \cdot 3 + 1$

Modular Arithmetic

Theorem (Division Notation)

Let $a, b \in \mathbb{Z}$, $b > 0$. *Then* $\exists! r, q \in \mathbb{Z}$: $a = q \cdot b + r$, *where* $0 \leq r < b$.

Example

1. $a = 11, b = 3$: $11 = 3 \cdot 3 + 2$
2. $a = -11, b = 3$: $-11 = -4 \cdot 3 + 1$
3. $a = -27, b = 4$: $-27 = -7 \cdot 4 + 1$

Modular Arithmetic

Theorem (Division Notation)

Let $a, b \in \mathbb{Z},\ b > 0$. *Then* $\exists! r, q \in \mathbb{Z}\colon a = q \cdot b + r$, *where* $0 \leq r < b$.

Example

1. $a = 11, b = 3\colon 11 = 3 \cdot 3 + 2$
2. $a = -11, b = 3\colon\ -11 = -4 \cdot 3 + 1$
3. $a = -27, b = 4\colon\ -27 = -7 \cdot 4 + 1$
4. $a = 18, b = 7,\ a = -103, b = 20$

Definition (Divisibility)

Let $a, b \in \mathbb{Z},\ b > 0$. We write

$$b|a \Leftrightarrow \exists k \in \mathbb{Z}\colon\ a = k \cdot b$$

Read: "b divides a"

Definition (Divisibility)

Let $a, b \in \mathbb{Z},\ b > 0$. We write

$$b|a \Leftrightarrow \exists k \in \mathbb{Z}\colon\ a = k \cdot b$$

Read: "b divides a"

Definition (Congruence Modulo an Integer)

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}_+$. We say that a is congruent to b modulo m if

$$m|b - a$$

Notation: $m|b - a \Leftrightarrow a \equiv_m b \Leftrightarrow a = b(\mathrm{mod}\ m)$

Definition (Divisibility)

Let $a, b \in \mathbb{Z},\ b > 0$. We write

$$b|a \Leftrightarrow \exists k \in \mathbb{Z}\colon\ a = k \cdot b$$

Read: "b divides a"

Definition (Congruence Modulo an Integer)

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}_+$. We say that a is congruent to b modulo m if

$$m|b - a$$

Notation: $m|b - a \Leftrightarrow a \equiv_m b \Leftrightarrow a = b(\mathrm{mod}\ m)$

Observation: $a = b(\mathrm{mod}\ m) \Leftrightarrow a$ and b have the same remainder upon division by m

Theorem

Let $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}_+$, $n \in \mathbb{N}$.
If $a = b \pmod{m}$ *and* $c = d \pmod{m}$, *then*

1. $a + c = b + d \pmod{m}$,
2. $a \cdot c = b \cdot d \pmod{m}$,
3. $a^n = b^n \pmod{m}$.

Theorem

Let $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}_+$, $n \in \mathbb{N}$.
If $a = b \pmod m$ *and* $c = d \pmod m$, *then*

1. $a + c = b + d \pmod m$,
2. $a \cdot c = b \cdot d \pmod m$,
3. $a^n = b^n \pmod m$.

Example

$13 = 5 \pmod 8$, $2 = 18 \pmod 8$
$13 + 2 = 5 + 18 \pmod 8 = 7 \pmod 8$,
$13 \cdot 2 = 5 \cdot 18 \pmod 8 = 2 \pmod 8$

Definition

Let $a, b \in \mathbb{N}$. A number $d \in \mathbb{N}$ is called the greatest common divisor of a and b if:

1. $d|a$ and $d|b$,
2. $\forall c \in \mathbb{N}$: $[(c|a \wedge c|b) \Rightarrow c|d]$.

Notation: $\gcd(a, b)$

Definition

Let $a, b \in \mathbb{N}$. A number $d \in \mathbb{N}$ is called the greatest common divisor of a and b if:

1. $d|a$ and $d|b$,
2. $\forall c \in \mathbb{N}$: $[(c|a \wedge c|b) \Rightarrow c|d]$.

Notation: $\gcd(a, b)$

Definition

The numbers a and b are called relatively prime if $\gcd(a, b) = 1$.
Notation: $a \perp b$

Euclidean Algorithm

$a, b \in \mathbb{N}_+$, $a > b$

We recursively construct a sequence of remainders (r_k):

$r_0 = a$, $r_1 = b$, $r_{k-1} = q_k \cdot r_k + r_{k+1}$.

Euclidean Algorithm

$a, b \in \mathbb{N}_+$, $a > b$

We recursively construct a sequence of remainders (r_k):

$r_0 = a$, $r_1 = b$, $r_{k-1} = q_k \cdot r_k + r_{k+1}$.

The last nonzero remainder equals $\gcd(a, b)$.

Euclidean Algorithm

$a, b \in \mathbb{N}_+$, $a > b$

We recursively construct a sequence of remainders (r_k):

$r_0 = a$, $r_1 = b$, $r_{k-1} = q_k \cdot r_k + r_{k+1}$.

The last nonzero remainder equals $\gcd(a, b)$.

Example

$\gcd(121, 114)$:

Theorem

Let $a, b \in \mathbb{N}$, $a^2 + b^2 > 0$. *Then*

$$\gcd(a, b) = \min\{c > 0 \colon c = \alpha \cdot a + \beta \cdot b, \alpha, \beta \in \mathbb{Z}\}$$

Theorem

Let $a, b \in \mathbb{N}$, $a^2 + b^2 > 0$. *Then*

$$\gcd(a, b) = \min\{c > 0 \colon c = \alpha \cdot a + \beta \cdot b, \alpha, \beta \in \mathbb{Z}\}$$

Example

Find α, β such that $\gcd(121, 114) = \alpha \cdot 121 + \beta \cdot 114$:

The set of all possible remainders upon division by n is denoted by $\mathbb{Z}_n$, so

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

We define the operation "addition modulo n" $+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ as follows:

$$\forall a, b \in \mathbb{Z}_n \quad a +_n b = k \iff a + b \equiv_n k \wedge k \in \mathbb{Z}_n$$

Simply: addition modulo n gives the remainder upon division of $a+b$ by n.

Properties of $(\mathbb{Z}_n, +_n)$.

1. identity element: $e = 0 \in \mathbb{Z}_n$ is an element such that $\forall x \in \mathbb{Z}_n \quad x +_n e = e +_n x = x$
2. additive inverse: for a given $x \in \mathbb{Z}_n$ we are looking for $y \in \mathbb{Z}_n$ such that $x +_n y = y +_n x = e$

   for $k \neq 0$ it is $n - k \in \mathbb{Z}_n$; for $k = 0$ it is 0

We also define the operation "multiplication modulo n" $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ as follows:

$$\forall a, b \in \mathbb{Z}_n \quad a \cdot_n b = k \iff a \cdot b \equiv_n k \wedge k \in \mathbb{Z}_n$$

We also define the operation "multiplication modulo n" $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ as follows:

$$\forall a, b \in \mathbb{Z}_n \quad a \cdot_n b = k \iff a \cdot b \equiv_n k \wedge k \in \mathbb{Z}_n$$

The identity element in this case is $e = 1$, but not every element has an inverse: 0 has no inverse.

We also define the operation "multiplication modulo n" $\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ as follows:

$$\forall a, b \in \mathbb{Z}_n \quad a \cdot_n b = k \iff a \cdot b \equiv_n k \wedge k \in \mathbb{Z}_n$$

The identity element in this case is $e = 1$, but not every element has an inverse: 0 has no inverse.

Then let us consider $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$.
There is still a problem. For example, for $(\mathbb{Z}_8 \setminus \{0\}, \cdot_8)$ there problem is $2 \cdot_8 4 = 0 \notin \mathbb{Z}_8 \setminus \{0\}$, so the operation $\cdot_8$ is not closed on $\mathbb{Z}_8 \setminus \{0\}$.

Theorem

An element $a \in \mathbb{Z}_n$ has an inverse in $(\mathbb{Z}_n, \cdot_n)$ if and only if $a \perp n$.

Theorem

An element $a \in \mathbb{Z}_n$ has an inverse in $(\mathbb{Z}_n, \cdot_n)$ if and only if $a \perp n$.

Let $\mathbb{Z}_n^*$ denote the set of all elements of $\mathbb{Z}_n$ relatively prime to n

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a \perp n\}$$

Then $(\mathbb{Z}_n^*, \cdot_n)$ is a good structure.

Theorem

An element $a \in \mathbb{Z}_n$ has an inverse in $(\mathbb{Z}_n, \cdot_n)$ if and only if $a \perp n$.

Let $\mathbb{Z}_n^*$ denote the set of all elements of $\mathbb{Z}_n$ relatively prime to n

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a \perp n\}$$

Then $(\mathbb{Z}_n^*, \cdot_n)$ is a good structure.

To simplify notation, we write $+$ instead of $+_n$ and $\cdot$ instead of $\cdot_n$.
The value of n is clear from the context.

The Euclidean algorithm allows us to find the inverse of an element x in $(\mathbb{Z}_n^*, \cdot_n)$. Set $a = n$, $b = x$.

The Euclidean algorithm allows us to find the inverse of an element x in $(\mathbb{Z}_n^*, \cdot_n)$. Set $a = n$, $b = x$.

Example

Find 114^{-1} in $\mathbb{Z}_{121}^*$.

Why do we need inverses in the group $\mathbb{Z}_n^*$?
They are used to solve congruences (equations modulo an integer), which we discuss next.

Why do we need inverses in the group $\mathbb{Z}_n^*$?
They are used to solve congruences (equations modulo an integer), which we discuss next.

Remark

Cancellation law:

$$\forall a, b, c \in \mathbb{Z}\ \forall m \in \mathbb{N}_+((ac \equiv_m bc \wedge c \perp m) \Rightarrow a \equiv_m b).$$

Theorem (Chinese Remainder Theorem)

Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ *and let* $m_1, m_2, \ldots, m_n \in \mathbb{N}_+$ *be pairwise relatively prime.*
Then the system of congruences

$$\begin{cases} x &= a_1 (\mathrm{mod}\ m_1) \\ x &= a_2 (\mathrm{mod}\ m_2) \\ &\vdots \\ x &= a_n (\mathrm{mod}\ m_n) \end{cases}$$

has exactly one solution modulo $\prod_{i=1}^{n} m_i$*, and all integer solutions are congruent to it modulo* $\prod_{i=1}^{n} m_i$*.*

Example

Solve the following system of congruences.

$$\begin{cases} x &= 3 (\mathrm{mod}\ 7) \\ x &= 0 (\mathrm{mod}\ 4) \\ x &= 8 (\mathrm{mod}\ 25) \end{cases}$$

To ensure that a solution exists, check that $7, 4, 25$ are pairwise relatively prime.
$\gcd(7, 4) = 1, \gcd(7, 25) = 1, \gcd(4, 25) = 1.$
Indeed, they are pairwise relatively prime.

The congruence $x = 3 (\mathrm{mod}\ 7)$ can be written as $x = 7a + 3$ (the remainder upon division of x by 7 is 3).

Example

We reduce the number of congruences one at a time until a single congruence remains. Choose any two congruences and solve them together by equating the expressions for x:

$$3 + 7a = 0 + 4b$$

We aim to find a or b. Reduce both sides modulo the smaller of $m_1 = 7$ and $m_2 = 4$.

$$3 + 3a = 0 (\mathrm{mod}\ 4)\ / - 3$$

$$3a = -3 = 1 (\mathrm{mod}\ 4)$$

Example

Now use the cancellation law. To divide both sides by 3, multiply by 3^{-1}. Since $3 \perp 4$, the inverse 3^{-1} exists in $\mathbb{Z}_4^*$. Find it using the Euclidean algorithm.
3^{-1} in $\mathbb{Z}_4^*$:

$$4 = 1 \cdot 3 + 1$$
$$1 = 4 - 1 \cdot 3$$
$$1 = -1 \cdot 3 (\mathrm{mod}\ 4)$$
$$3^{-1} = -1 = 3 (\mathrm{mod}\ 4)$$

Example

Returning to our congruence:

$$3a = 1 (\mathrm{mod}\ 4)\ / \cdot 3^{-1}$$
$$a = 3^{-1} = 3 (\mathrm{mod}\ 4)$$

Thus $a = 3 + 4k$. Substituting, we get:

$$x = 3 + 7a = 3 + 7(3 + 4k) = 24 + 28k$$

The system of congruences now becomes:

$$\begin{cases} x &= 24 (\mathrm{mod}\ 28) \\ x &= 8 (\mathrm{mod}\ 25) \end{cases}$$

Solve it in the same way.

Example

$$x = 24 + 28k = 8 + 25c \ /(\text{mod } 25)$$
$$24 + 3k = 8(\text{mod } 25)$$
$$3k = -16 = 9(\text{mod } 25) \ / \cdot 3^{-1}$$

3^{-1} in $\mathbb{Z}_{25}^*$:

$$25 = 8 \cdot 3 + 1$$
$$1 = 25 - 8 \cdot 3$$
$$1 = -8 \cdot 3(\text{mod } 25)$$
$$3^{-1} = -8 = 17(\text{mod } 25)$$

Example

Returning to the congruence:

$$k = 9 \cdot 17 = 153 = 3 (\mathrm{mod}\ 25)$$

$$k = 3 + 25l$$

Substituting:
$x = 24 + 28(3 + 25l) = 24 + 84 + 4 \cdot 7 \cdot 25l = 108 (\mathrm{mod}\ 4 \cdot 7 \cdot 25)$.

Answer: $x = 108$.

Definition

The order of $(X, \circ)$ is the number of its elements, i.e. the cardinality of X.
Notation: $|X|$

Definition

The order of $(X, \circ)$ is the number of its elements, i.e. the cardinality of X.
Notation: $|X|$

Example

$(\mathbb{Z}_n, +_n)$: $|\mathbb{Z}_n| = n$, because $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Definition

The order of $(X, \circ)$ is the number of its elements, i.e. the cardinality of X.
Notation: $|X|$

Example

$(\mathbb{Z}_n, +_n)$: $|\mathbb{Z}_n| = n$, because $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

What is the order of $(\mathbb{Z}_n^*, \cdot_n)$?

Definition

Euler's totient function assigns to each natural number n the number of nonnegative integers less than n that are relatively prime to n.

$$\varphi\colon \mathbb{N} \ni n \mapsto \varphi(n) = \left|\{m \in \mathbb{N}\colon m < n \wedge m \perp n\}\right|$$

Thus $|\mathbb{Z}_n^*| = \varphi(n)$.

Definition

Euler's totient function assigns to each natural number n the number of nonnegative integers less than n that are relatively prime to n.

$$\varphi\colon \mathbb{N} \ni n \mapsto \varphi(n) = |\{m \in \mathbb{N}\colon m < n \wedge m \perp n\}|$$

Thus $|\mathbb{Z}_n^*| = \varphi(n)$.

Example

$\varphi(0) = 0, \varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2$
$\varphi(p) = p - 1, p \in \mathbb{P}$ (where $\mathbb{P}$ denotes the set of primes)

What if n is not prime? How do we compute $\varphi(n)$?

Theorem

If the prime factorization of n is
$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \forall i\ \alpha_i \neq 0, \forall i\ p_i \in \mathbb{P}, p_i \neq p_j$ *for* $i \neq j$, *then*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

What if n is not prime? How do we compute $\varphi(n)$?

Theorem

If the prime factorization of n is $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \forall i\ \alpha_i \neq 0, \forall i\ p_i \in \mathbb{P}, p_i \neq p_j$ for $i \neq j$, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

Consequences:

- If $n = p \in \mathbb{P}$, then $\varphi(n) = n\left(1 - \frac{1}{p}\right) = n - 1$,
- If $n = p_1 p_2$, then $\varphi(n) = p_1 p_2\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) = (p_1 - 1)(p_2 - 1)$.

Example

$|\mathbb{Z}_{450}^*| = ?$, i.e. $\varphi(450) = ?$

$450 = 2 \cdot 3^2 \cdot 5^2$

$$\varphi(450) = 450 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 2 \cdot 3^2 \cdot 5^2 \cdot \frac{1 \cdot 2 \cdot 4}{2 \cdot 3 \cdot 5} =$$

$$= 2 \cdot 3 \cdot 4 \cdot 5 = 120$$