Modular Arithmetic

Birzhan Kalmurzayev

Ac. year 2025-2026

The Division Algorithm

Theorem

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

The Division Algorithm

Theorem

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Definition

Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $gcd(a, b)$

The Division Algorithm

Theorem

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Definition

Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by $gcd(a, b)$

Definition

The integers a and b are relatively prime if their greatest common divisor is 1.

Definition

The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $lcm(a, b)$.

Definition

The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $lcm(a, b)$.

Theorem

Let a and b be positive integers. Then

$$a \cdot b = gcd(a, b) \cdot lcm(a, b).$$

The Euclidean Algorithm

Lemma

Let $a = b \cdot q + r$, where a, b, q, and r are integers. Then $gcd(a, b) = gcd(b, r)$.

The Euclidean Algorithm

Lemma

Let $a = b \cdot q + r$, where a, b, q, and r are integers. Then $gcd(a, b) = gcd(b, r)$.

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

- $r_0 = r_1 \cdot q_1 + r_2 \qquad 0 \leq r_2 < r_1,$
- $r_1 = r_2 \cdot q_1 + r_3 \qquad 0 \leq r_3 < r_2,$
- $\cdots$
- $r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1},$
- $r_{n-1} = r_n \cdot q_n.$

The Euclidean Algorithm

Lemma

Let $a = b \cdot q + r$, where a, b, q, and r are integers. Then $gcd(a, b) = gcd(b, r)$.

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

- $r_0 = r_1 \cdot q_1 + r_2 \qquad 0 \leq r_2 < r_1,$
- $r_1 = r_2 \cdot q_1 + r_3 \qquad 0 \leq r_3 < r_2,$
- $\cdots$
- $r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1},$
- $r_{n-1} = r_n \cdot q_n.$

from the Lemma we have $gcd(a, b) = r_n$

Example. Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Example. Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

- $662 = 414 \cdot 1 + 248$
- $414 = 248 \cdot 1 + 166$
- $248 = 166 \cdot 1 + 82$
- $166 = 82 \cdot 2 + 2$
- $82 = 2 \cdot 41.$

$$gcd(414, 622) = 2$$

gcds as Linear Combinations

Theorem (Bezout)

If a and b are positive integers, then there exist integers s and t such that

$$gcd(a, b) = s \cdot a + t \cdot b.$$

gcds *as Linear Combinations*

Theorem (Bezout)

If a and b are positive integers, then there exist integers s and t such that

$$gcd(a, b) = s \cdot a + t \cdot b.$$

Definition

If a and b are positive integers, then integers s and t such that

$$gcd(a, b) = s \cdot a + t \cdot b \tag{1}$$

are called Bezout coefficients of a and b. Also, the equation (1) is called Bezout's identity.

gcds *as Linear Combinations*

Theorem (Bezout)

If a and b are positive integers, then there exist integers s and t such that

$$gcd(a, b) = s \cdot a + t \cdot b.$$

Definition

If a and b are positive integers, then integers s and t such that

$$gcd(a, b) = s \cdot a + t \cdot b \tag{1}$$

are called Bezout coefficients of a and b. Also, the equation (1) is called Bezout's identity.

Question: How define Bezout's identity

Continued Fractions

Definition

A **continued fraction** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

where

$$a_0 \in \mathbb{Z}, \qquad a_1, a_2, \ldots, a_n \in \mathbb{N}.$$

Continued Fractions

Definition

A **continued fraction** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

where

$$a_0 \in \mathbb{Z}, \qquad a_1, a_2, \ldots, a_n \in \mathbb{N}.$$

We use the compact notation $[a_0; a_1, a_2, \ldots, a_n]$.

Theorem

Any ratio $\frac{a}{b}$ is equal to some continued fraction $[q_0, q_1, q_2, \ldots, q_n]$

Theorem

Any ratio $\frac{a}{b}$ is equal to some continued fraction $[q_0, q_1, q_2, \ldots, q_n]$

Proof. The fraction is defined from Euclidean Algorithm:

- $a = b \cdot q_0 + r_1$,
- $b = r_1 \cdot q_1 + r_2$,
- $r_1 = r_2 \cdot q_2 + r_3$,
- $\ldots$
- $r_{n-1} = r_n \cdot q_n$

Example

Find continued fraction for $\frac{3614}{189}$

Example

Find continued fraction for $\frac{3614}{189}$

$$\frac{3614}{189} = 19 + \cfrac{1}{8 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2}}}}} = [19, 8, 4, 1, 1, 2]$$

Convergents of a Continued Fraction

Definition

Let $[a_0; a_1, a_2, \ldots]$ be a continued fraction. The **k-th convergent** is the rational number

$$\frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k].$$

Convergents of a Continued Fraction

Definition

Let $[a_0; a_1, a_2, \dots]$ be a continued fraction. The **k-th convergent** is the rational number

$$\frac{p_k}{q_k} = [a_0; a_1, \dots, a_k].$$

Recursive formulas for finding convergents.

$$P_{-1} = 1, \quad P_0 = a_0, \quad P_k = a_k P_{k-1} + P_{k-2}$$
$$Q_{-1} = 0, \quad Q_0 = 1, \quad Q_k = a_k Q_{k-1} + Q_{k-2}$$

Example

Convergents of $\frac{3614}{189}$

Example

Convergents of $\frac{3614}{189}$

	-1	0	1	2	3	4	5
a_k		19	8	4	1	1	2
P_k	1	19	153	631	784	1415	3614
Q_k	0	1	8	33	41	74	189

Example

Convergents of $\frac{3614}{189}$

	-1	0	1	2	3	4	5
a_k		19	8	4	1	1	2
P_k	1	19	153	631	784	1415	3614
Q_k	0	1	8	33	41	74	189

Note that:

$$\begin{vmatrix} 1415 & 3614 \\ 74 & 189 \end{vmatrix} = -1; \quad \begin{vmatrix} 784 & 1415 \\ 41 & 74 \end{vmatrix} = 1, \quad \begin{vmatrix} 631 & 784 \\ 33 & 41 \end{vmatrix} = -1, \ldots$$

Properties of Convergents

For all s:

1. $Q_1 < Q_2 < Q_3 < \cdots < Q_k$;

Properties of Convergents

For all s:

1. $Q_1 < Q_2 < Q_3 < \cdots < Q_k$;
2. $P_{s-1}Q_s - P_sQ_{s-1} = (-1)^s$

Properties of Convergents

For all s:

1. $Q_1 < Q_2 < Q_3 < \cdots < Q_k$;
2. $P_{s-1}Q_s - P_sQ_{s-1} = (-1)^s$
3. $gcd(P_s, Q_s) = 1$;

Properties of Convergents

For all s:

1. $Q_1 < Q_2 < Q_3 < \cdots < Q_k$;
2. $P_{s-1}Q_s - P_sQ_{s-1} = (-1)^s$
3. $gcd(P_s, Q_s) = 1$;
4. If $\delta_k = [a_0, a_1, \ldots, a_k]$, then $|\delta_s - \delta_{s-1}| = \frac{1}{Q_{s-1}Q_s}$;

Method for solving partial solution of equation $ax + by = 1$

If $gcd(a, b) \neq 1$, then the equation does not have solution in integers. So, we assume that $gcd(a, b) = 1$.

Step 1. Find the continued fraction for $\frac{a}{b} = [q_0, q_1, \ldots, q_k]$
Step 2. Find $\delta_{k-1} = [q_0, q_1, \ldots, q_{k-1}] = \frac{P_{k-1}}{Q_{k-1}}$

Then

$$x_p := (-1)^{k-1} Q_{k-1}, \qquad y_p := (-1)^k P_{k-1}$$

Solving equation in integers

General solution of equation $ax + by = 1$ is

$$x = x_p - bt, \qquad y = y_p + at, \qquad t \in Z$$

Solving equation in integers

General solution of equation $ax + by = 1$ is

$$x = x_p - bt, \qquad y = y_p + at, \qquad t \in Z$$

Example. Solve the equation $12x + 15y = 4$ in integers.

Congruence Modulo n

Definition

Let $n \in \mathbb{N}$, $n \geq 1$. For integers $a, b \in \mathbb{Z}$ we say that

$$a \equiv b \pmod{n}$$

if n divides $a - b$, or equivalently

$$a \equiv b \pmod{n} \iff a = b + kn \text{ for some } k \in \mathbb{Z}.$$

Congruence Modulo n

Definition

Let $n \in \mathbb{N}$, $n \geq 1$. For integers $a, b \in \mathbb{Z}$ we say that

$$a \equiv b \pmod{n}$$

if n divides $a - b$, or equivalently

$$a \equiv b \pmod{n} \iff a = b + kn \text{ for some } k \in \mathbb{Z}.$$

Example.

$$17 \equiv 5 \pmod{12} \quad \text{since} \quad 12 \mid (17 - 5).$$

Residue Classes

Definition

Let $n \in \mathbb{N}$, $n \geq 1$. For $a \in \mathbb{Z}$, the **residue class of a modulo n** is

$$[a]_n = \{\, b \in \mathbb{Z} \mid b \equiv a \pmod{n} \,\}.$$

Residue Classes

Definition

Let $n \in \mathbb{N}$, $n \geq 1$. For $a \in \mathbb{Z}$, the **residue class of a modulo n** is

$$[a]_n = \{\, b \in \mathbb{Z} \mid b \equiv a \pmod{n} \,\}.$$

Example (mod 5):

- $[0]_5 = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} = \{5k : \ k \in Z\};$
- $[1]_5 = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} = \{5k+1 : \ k \in Z\};$
- $[2]_5 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} = \{5k+2 : \ k \in Z\};$
- $[3]_5 = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\} = \{5k+3 : \ k \in Z\};$
- $[4]_5 = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\} = \{5k+4 : \ k \in Z\}.$

Arithmetic Modulo m

Theorem

Let m be a positive integer. If $a = b(\textbf{mod } m)$ and $c = d(\textbf{mod } m)$, then

$$a + c = b + d(\textbf{mod } m) \text{ and } a \cdot c = b \cdot d(\textbf{mod } m).$$

Arithmetic in $\mathbb{Z}_m$

Let $m \in \mathbb{N}$, $m \geq 1$. We define algebra

$$\mathbb{Z}_m = (\{0, 1, 2, \ldots, m-1\}, +, \cdot).$$

Addition modulo m.

$$a + b = (a + b) \bmod m,$$

where the addition on the right-hand side is ordinary integer addition.

Multiplication modulo m.

$$a \cdot b = (a \cdot b) \bmod m,$$

where the multiplication on the right-hand side is ordinary integer multiplication.

Solving Linear Equations in $\mathbb{Z}_n$

Consider the linear congruence

$$ax \equiv b \pmod{n}.$$

Step 1. Compute $d = \gcd(a, n)$**.**

- If $d \nmid b$, then the equation has **no solutions**.
- If $d \mid b$, then solutions exist.

Step 2. Solve the equation in integers.

$$ax - ny = b$$

Solution is x **by modulo** n.

Examples

Solve the equation: $6x = 17(\textbf{mod } 29)$

Eulier theorem

Definition

The Euler function $\varphi(n)$ is number of positive integers less or equal n which is coprime with n, i.e.

$$\varphi(n) = n \prod_{i \geq 1} (1 - \frac{1}{p_i})$$

where $n = p_0^{\alpha_0} \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the canonic form.

Theorem (Euler)

If $gcd(a, n) = 1$*, then* $a^{\varphi(n)} = 1 (\mathbf{mod}\ n)$

Example

Compute

- $3^{78} (\textbf{mod } 11)$;
- $4^{93} (\textbf{mod } 13)$;
- $46^{921} (\textbf{mod } 21)$.

Chinese Reminder Theorem

Any system of the form

$$\begin{cases} a_1 x = b_1 (\textbf{mod } m_1) \\ a_2 x = b_2 (\textbf{mod } m_2) \\ \vdots \\ a_n x = b_n (\textbf{mod } m_n) \end{cases}$$

is reducible to the form

$$\begin{cases} x = b_1 (\textbf{mod } m_1) \\ x = b_2 (\textbf{mod } m_2) \\ \vdots \\ x = b_n (\textbf{mod } m_n) \end{cases}$$

Chinese Reminder Theorem

Theorem

Assume $m_1, m_2, \ldots, m_n$ *are pairwise coprime numbers and for* $i \leq n$ *assume* x_i *is solution of*

$$m_1 \cdot m_2 \cdots m_{i-1} \cdot x_i \cdot m_{i+1} \cdots m_n = 1(\mathbf{mod}\ m_i)$$

Then
$x = x_1 \cdot b_1 \cdot m_2 \cdot m_3 \cdots m_n + m_1 \cdot x_2 \cdot b_2 \cdot m_3 \cdots m_n + \cdots m_1 \cdot m_2 \cdots x_n \cdot b_n$
is solution of the system

$$\begin{cases} x = b_1(\mathbf{mod}\ m_1) \\ x = b_2(\mathbf{mod}\ m_2) \\ \vdots \\ x = b_n(\mathbf{mod}\ m_n) \end{cases}$$

Example

Solve the following system

$$\begin{cases} x = 2(\textbf{mod } 5) \\ x = 3(\textbf{mod } 6) \\ x = 4(\textbf{mod } 7) \end{cases}$$