Week 6
Congruence Relation Modulo n
Discrete Math

Marie Demlová
http://math.fel.cvut.cz/en/people/demlova

March 24, 2022

Congruence Relation Modulo n

Given two integers a, b and a natural number $n > 1$. We say that a is congruent to b modulo n and write $a \equiv b \pmod{n}$ if $a - b$ is divisible by n.

Equivalent Characterizations of Modulo n.

Let a and b be two integers. Then the following is equivalent:

- $a \equiv b \pmod{n}$,
- $a = b + k\,n$ for some integer k,
- a and b have the same remainders when divided by n.

Congruence Relation Modulo n

Proposition.

Let a, b, and c be integers. Then

- $a \equiv a \pmod{n}$ (modulo n is reflexive);
- if $a \equiv b \pmod{n}$, then also $b \equiv a \pmod{n}$ (modulo n is symmetric);
- if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$ (modulo n is transitive).

Properties of modulo n.

Assume that for integers a, b, c, and d it holds that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

$$(a + c) \equiv (b + d) \pmod{n} \quad \text{a} \quad (a \cdot c) \equiv (b \cdot d) \pmod{n}.$$

Congruence Relation Modulo n

Corollary. Given two integers a, b such that $a \equiv b \pmod{n}$. Then

- $ra \equiv rb \pmod{n}$ for every integer r;
- $a^k \equiv b^k \pmod{n}$ for every natural number k.
- Moreover, if $a_i \equiv b_i \pmod{n}$ for every $i = 0, \ldots, k$, a $r_0, \ldots, r_k$ are arbitrary integers, then

$$(r_0\, a_0 + \ldots + r_k\, a_k) \equiv (r_0\, b_0 + \ldots + r_k\, b_k) \pmod{n}.$$

Proposition. Let r, a, b be integers and n a natural number $n > 1$ such that $ra \equiv rb \pmod{n}$. Then

$$a \equiv b \left(\mathrm{mod} \frac{n}{\gcd(n, r)} \right).$$

Congruence Relation Modulo n

Solving $(a + x) \equiv b \pmod{n}$. Given integers a, b and a natural number $n > 1$. Find all integers x for which

$$(a + x) \equiv b \pmod{n}.$$

This problem has got always a solution which is any $x \in \mathbb{Z}$ for which $x \equiv (b - a) \pmod{n}$.

Solving $(a \cdot x) \equiv b \pmod{n}$. Given two integers a, b and a natural number $n > 1$. Find all integers x for which

$$a\,x \equiv b \pmod{n}.$$

The equation above has a solution iff the number b is a multiple of $\gcd(a, n)$, and all integers x are solutions of the following Diophantic equation

$$a\,x + n\,y = b.$$

Congruence Relation Modulo n

Proposition. Let $n > 1$, $m > 1$ be two relatively prime natural number. And let for some $a, b \in \mathbb{Z}$ it holds that $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$
Then also $a \equiv b \pmod{nm}$.

A stronger version holds: Assume that $a \equiv b \pmod{n}$ and $a \equiv b \pmod{m}$. Let $n_1 = \frac{n}{\gcd(n,m)}$ and $m_1 = \frac{m}{\gcd(n,m)}$. Then

$$a \equiv b \pmod{n_1 m_1}.$$

Small Fermat Theorem.

Let p be a prime and a an integer relatively prime to p. Then

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

Residue Classes Modulo n

An equivalence class of the equivalence modulo n containing a number $i \in \mathbb{Z}$ is the residue class containing i and is denoted by $[i]_n$. We have

$$[i]_n = \{j \mid j = i + kn \text{ for some } k \in \mathbb{Z}\}.$$

The Set $\mathbb{Z}_n$.

There are n distinct residue classes modulo n; indeed, they are the residue classes corresponding to the numbers (remainders) $0, 1, \ldots, n-1$. The set of all residue classes is denoted by $\mathbb{Z}_n$, so

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

Operations in $\mathbb{Z}_n$

Addition $\oplus$ and multiplication $\odot$.

For $[i]_n, [j]_n \in \mathbb{Z}_n$ we have

$$[i]_n \oplus [j]_n = [i+j]_n, \qquad [i]_n \odot [j]_n = [i \cdot j]_n.$$

Example. Let $n = 6$, then there are 6 distinct residue classes, i.e.

$$\mathbb{Z}_6 = \{[0]_6, [1]_6, \ldots, [5]_6\}.$$

Moreover,

$$[3]_6 \oplus [5]_6 = [2]_6, \quad [3]_6 \odot [4]_6 = [0]_6.$$