

Modular Arithmetic

Discrete Mathematics
Evgeny Skvortsov

Congruences

- In some situations we care only about the remainder of an integer when it is divided by some specified positive number. For instance, when we ask what time it will be 50 hours from now, we care only about the remainder 50 plus the current hour is divided by 24.

- If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$.

We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m .

If a and b are not congruent modulo m , we write $a \not\equiv b \pmod{m}$

- Integers a and b are congruent modulo m if and only if they have the same remainder when divided by m .

Indeed, if $a - b = km$ and $b = qm + r$, then $a = km + b = (k + q)m + r$

Congruences (cntd)

- Examples:

$$12 \equiv 5 \pmod{7}$$

$$12 \equiv 6 \pmod{3}$$

$$12 \equiv -3 \pmod{15}$$

$$12 \equiv 0 \pmod{12}$$

- For any integers a , b , and m , $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some integer k .

By definition, $a \equiv b \pmod{m}$ if and only if $a - b = km$ for some integer k . Then $a = b + km$

Congruences and Arithmetic Operations

- Addition, subtraction, multiplication behave really with respect to congruences

- **Theorem.**

Let m be positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$, $a - c \equiv b - d \pmod{m}$, and $ac \equiv bd \pmod{m}$

- **Proof**

For multiplication. We have $a = b + km$ and $c = d + lm$ for some k and l .

$$\begin{aligned} \text{Then } ac &= (b + km)(d + lm) = bd + blm + dkm + klm \\ &= bd + (bl + dk + klm) \cdot m \end{aligned}$$

- **Example:** $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$$

Congruences and Arithmetic Operations (cntd)

- Division is not so good:

Although $8 \equiv 24 \pmod{4}$ and $4 \equiv 8 \pmod{4}$,

$$\frac{8}{4} = 2 \not\equiv 3 = \frac{24}{8} \pmod{m}$$

Congruency properties

- **Theorem:**

- For any $m > 0$ congruency modulo m relation is an equivalence relation.

- **Proof:**

- Reflexivity and symmetricity are obvious.

- Transitivity:

- If $a \equiv b$, $b \equiv c$ then we for a and c we have:

- $a - c = a - b + (b - c) = km + lm = (k + l) m$

Residues

- Let us consider the binary relation \equiv modulo m on the set of integers, that is, the relation that contains pair (a,b) such that $a \equiv b \pmod{m}$
- It is reflexive, symmetric, and transitive. This is an equivalence relation
- Each such relation defines a partition on the set of integers into equivalence classes.
- We choose a representative from each such class
- The **residue** of an integer a modulo m is such a number b that $a \equiv b \pmod{m}$ and $0 \leq b < m$
In other words the residue of a modulo m is the remainder of a when divide by m
- Let Z_n denote the set $\{0,1,2,\dots,n-1\}$. This is the set of all possible remainders of integers when divided by n
It is called the **set of residues**, and its members are called **residues**

Modular Arithmetic

- We define addition, subtraction, and multiplication of residues:

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

$a + b \pmod{n}$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a + b \pmod{n}$

$a - b \pmod{n}$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a - b \pmod{n}$

$a \cdot b \pmod{n}$ is the element $c \in \mathbb{Z}_n$ such that $c \equiv a \cdot b \pmod{n}$

- Example. Construct operation tables for \mathbb{Z}_5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Divisors of Zero

- It is not hard to see that the operation tables of addition looks similar for all m
- It is not the case for multiplication. Consider

\cdot	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

- A **proper divisor of 0** modulo m is a residue a such that there is $b \not\equiv 0 \pmod{m}$ with $a \cdot b \equiv 0 \pmod{m}$. \mathbb{Z}_4 has a proper divisor of zero. \mathbb{Z}_5 does not.

Inverse

● A residue b modulo m is called an inverse of a residue a if $a \cdot b \equiv 1 \pmod{m}$, denoted a^{-1}

● 3 is the inverse of 2 modulo 5

● 2 does not have an inverse modulo 4

● **Theorem**



Let a be residue modulo m . The following conditions are equivalent:

- (i) a has an inverse;
- (ii) a is not a proper divisor of m ;
- (iii) a is relatively prime with m .

Inverse (cntd)

Proof.

(i) \Rightarrow (ii) By contraposition.

Suppose $a \cdot b \equiv 0 \pmod{m}$ for some b .

Then $a^{-1} \cdot a \cdot b \equiv a^{-1} \cdot 0 \pmod{m}$

$$b \equiv 1 \cdot b \equiv 0 \pmod{m}$$

(ii) \Rightarrow (iii) By contraposition.

Suppose $\gcd(a, m) = d$ and $a = ld$, $m = kd$. Note that $k \not\equiv 0 \pmod{m}$

Then $ak \equiv kld \equiv lm \equiv 0 \pmod{m}$. Thus a is a proper divisor of 0.

(iii) \Rightarrow (i)

Suppose $\gcd(a, m) = 1$. Then there are u, v with $au + mv = 1$.

Thus $au \equiv 1 \pmod{m}$; a has an inverse.

Homework

Exercises from the Book:

No. 1, 5, 9, 12, 20, 23 (page 696)