Lecture 8

CONGRUENCES

(đồng dư)

Definition

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say that a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, if and only if $n \mid (a - b)$.

Note

Equivalent definitions of $a \equiv b \pmod{n}$ include:

- There exists $k \in \mathbb{Z}$ such that $a = b + kn$.
- $a \mathbin{\mathbf{mod}} n = b \mathbin{\mathbf{mod}} n$.

Example

- $17 \equiv 2 \pmod{5}$; $\quad -17 \equiv 7 \pmod{8}$; $\quad 3 \not\equiv 17 \pmod{12}$.
- For all integers a, $a \equiv (a \mathbin{\mathbf{mod}} n) \pmod{n}$.

Lemma

Let $n \in \mathbb{Z}^+$. *Then:*

1. $\forall a \in \mathbb{Z}\ (a \equiv a \pmod{n})$.
2. $\forall a, b \in \mathbb{Z}\ \Big(\big(a \equiv b \pmod{n}\big) \Rightarrow \big(b \equiv a \pmod{n}\big)\Big)$.
3. $\forall a, b, c \in \mathbb{Z}$
$$\Bigg(\Big(\big(a \equiv b \pmod{n}\big) \wedge \big(b \equiv c \pmod{n}\big)\Big) \Rightarrow \big(a \equiv c \pmod{n}\big)\Bigg).$$

Proof.

Easy exercise. □

Lemma

Let $a, b, c, d, n \in \mathbb{Z}$ *with* $n > 0$. *Suppose that* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$. *Then*

$$a + c \equiv b + d \pmod{n};$$

$$a - c \equiv b - d \pmod{n};$$

$$ac \equiv bd \pmod{n}.$$

Proof.

1. $n \mid (a - b)$ and $n \mid (c - d)$.
2. Thus $n \mid (a - b) \pm (c - d) = (a \pm c) - (b \pm d)$, so that $a \pm c \equiv b \pm d \pmod{n}$.
3. Also, $n \mid (a - b)c + (c - d)b = ac - bd$, so that $ac \equiv bd \pmod{n}$.

$\square$

Generally if $ac \equiv bc \pmod{n}$, it is not necessary that $a \equiv b \pmod{n}$ even when $c \not\equiv 0 \pmod{n}$. (For example, $2 \cdot 4 = 8 \equiv 2 \pmod{6} \equiv 2 \cdot 1 \pmod{6}$, but $4 \not\equiv 1 \pmod{6}$.)

Lemma

Let $a, b, c, n \in \mathbb{Z}$ with $n > 0$. Suppose that $ac \equiv bc \pmod{n}$. Then

$$a \equiv b \pmod{\tfrac{n}{\gcd(c,n)}}.$$

Proof.

1. $n \mid (ac - bc) = (a - b)c$.
2. Let $n' = \frac{n}{\gcd(c,n)}$ and $c' = \frac{c}{\gcd(c,n)}$. Then $\gcd(n', c') = 1$. (Tut 7, Qn 6.)
3. Since $n \neq 0$, $\frac{(a-b)c}{n} \in \mathbb{Z}$.
4. $\frac{(a-b)c}{n} = \frac{(a-b)c'}{n'}$.
5. By (3) and (4), $n' \mid (a - b)c'$.
6. By (2) and (5), $n' \mid (a - b)$ (part (2) of Lemma in Slide 29 of LECT8-1.pdf).
7. Thus $a \equiv b \pmod{n'}$.

$\square$

Solving Congruence Equations

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Suppose that we want to solve $ax \equiv b \pmod{n}$, i.e. we want to find $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$.

Note

Although not strictly necessary, it is useful to replace a and b with $a \mathbin{\mathbf{mod}} n$ and $b \mathbin{\mathbf{mod}} n$ if they are not between 0 and n (and we can do so because of the last two lemmas).
For example, the congruence equation $97x \equiv -54 \pmod{13}$ can be replaced by the much less daunting $6x \equiv 11 \pmod{13}$.

Lemma

There exists $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$ if and only if $\gcd(a, n) \mid b$.

Proof.

Let $g = \gcd(a, n)$.

1. If there exists $x \in \mathbb{Z}$ such that $ax \equiv b \pmod{n}$, then:
    1. $n \mid (ax - b)$.
    2. $g \mid n$, so $g \mid (ax - b)$.
    3. $g \mid a$ and $g \mid (ax - b)$, so $g \mid a(x) - (ax - b)(1) = b$.
2. If $g \mid b$ then:
    1. There exists $y, z \in \mathbb{Z}$ such that $ay + nz = g$ by Bézout's Identity.
    2. Let $x = \frac{b}{g}y$. Then $x \in \mathbb{Z}$ and

$$ax = a\frac{b}{g}y = \frac{b}{g}(g - nz) = b - \frac{b}{g}nz \equiv b \pmod{n}.$$

$\square$

Lemma

Let $a, b, n \in \mathbb{Z}$ with $n > 0$, and assume that $\gcd(a, n) \mid b$. Then

$$\forall x \in \mathbb{Z} \left(ax \equiv b \pmod{n} \Leftrightarrow \frac{a}{\gcd(a,n)} x \equiv \frac{b}{\gcd(a,n)} \pmod{\frac{n}{\gcd(a,n)}} \right)$$

Note

$\gcd(\frac{a}{\gcd(a,n)}, \frac{n}{\gcd(a,n)}) = 1$ (Tutorial 7, Qn 6).

Proof.

1. Let $g = \gcd(a, n)$, $a_1 = \frac{a}{\gcd(a,n)}$, $b_1 = \frac{b}{\gcd(a,n)}$, and $n_1 = \frac{n}{\gcd(a,n)}$. Then $a_1, b_1, n_1 \in \mathbb{Z}$ with $n_1 > 0$, and $a = a_1 g$, $b = b_1 g$ and $n = n_1 g$.
2. If $ax \equiv b \pmod{n}$ where $x \in \mathbb{Z}$, then $a_1 g x \equiv b_1 g \pmod{n_1 g}$, so that $a_1 x \equiv b_1 \pmod{n_1}$ by Slide 5.
3. Conversely, if $a_1 x \equiv b_1 \pmod{n_1}$, then $a_1 x = b_1 + k n_1$ for some $k \in \mathbb{Z}$. Thus $ax = a_1 g x = b_1 g + k n_1 g = b + kn$, so that $ax \equiv b \pmod{n}$.

$\square$

Multiplicative Inverse Modulo n

Definition

Let $a, n \in \mathbb{Z}$ with $n > 0$. An integer x is a **multiplicative inverse of a modulo n** if and only if $ax \equiv 1 \pmod{n}$.

Example

- Both 2 and 5 are multiplicative inverses of 2 modulo 3.
- 4 has no multiplicative inverse modulo 6.

Lemma

Let $a, n \in \mathbb{Z}$ with $n > 0$. Then a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.

Proof.

This follows from Slide 6: $ax \equiv 1 \pmod{n}$ has an integer solution for x if and only if $\gcd(a, n) \mid 1$, if and only if $\gcd(a, n) = 1$. $\square$

Corollary

Let $a, n \in \mathbb{Z}$ with $n > 0$. Suppose that $\gcd(a, n) = 1$ and let a' be a multiplicative inverse of a modulo n. Then

$$\forall x \in \mathbb{Z}\ \left(ax \equiv b \pmod{n} \Leftrightarrow x \equiv a'b \pmod{n}\right).$$

Proof.

1. If $ax \equiv b \pmod{n}$, then $a'b \equiv a'(ax) \pmod{n} \equiv (a'a)x \pmod{n} \equiv (1)x \pmod{n} \equiv x \pmod{n}$.
2. Conversely, if $x \equiv a'b \pmod{n}$, then $ax \equiv a(a'b) \pmod{n} \equiv (aa')b \pmod{n} \equiv 1(b) \pmod{n} \equiv b \pmod{n}$.

$\square$

Theorem

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then

$$\left(\exists x \in \mathbb{Z} \;\; ax \equiv b \pmod{n}\right) \Leftrightarrow \gcd(a,n) \mid b,$$

in which case

$$\forall x \in \mathbb{Z} \left(ax \equiv b \pmod{n} \Leftrightarrow x \equiv a' \frac{b}{\gcd(a,n)} \pmod{\frac{n}{\gcd(a,n)}}\right),$$

where a' is a multiplicative inverse of $\frac{a}{\gcd(a,n)}$ modulo $\frac{n}{\gcd(a,n)}$.

Proof.

The necessary and sufficient condition for the existence of solution follows from Slide 6, while the set of all solutions, when the condition holds, follows from Slide 7 and last Corollary (Slide 9). □

Corollary

Let $a, n \in \mathbb{Z}$ with $n > 0$, and suppose that $\gcd(a, n) = 1$. Let a' be a multiplicative inverse of a modulo n. Then for any $x \in \mathbb{Z}$, x is a multiplicative inverse of a modulo n if and only if $x \equiv a' \pmod{n}$.

Proof.

Just apply the last theorem with $b = 1$. □

Computing Multiplicative Inverses Modulo n

- If a' is a multiplicative inverse of a modulo n, then $a' \mathbf{mod}\ n$ is also a multiplicative inverse of a modulo n by the last Corollary. But $0 \leq a' \mathbf{mod}\ n < n$, so one can go through the list $0, 1, \ldots, n-1$ to see if any of this when multiplied with a gives 1 modulo n. This is the **trial and error method** (or guess and check method), and works well for small n.
- In general, especially when it is not practical to use the trial and error method, we can rely on the Euclidean algorithm to obtain integer x and y such that $ax + ny = 1$ (since $\gcd(a, n) = 1$ for a to have a multiplicative inverse modulo n), in which case x is a multiplicative inverse of a modulo n.
- After one multiplicative inverse of a has been found, the others can be obtained by adding multiples (both positive and negative) of n to it.

Example

Compute the multiplicative inverses of a modulo n for each of the following pairs of a and n:

(a) $a = 2$, $n = 7$; (b) $a = 7$, $n = 31$.

Solution:

(a) Since $4(2) = 8 \equiv 1 \pmod 7$, we see that 4 is a multiplicative inverse of 2 modulo 7. In general, $x \in \mathbb{Z}$ is a multiplicative inverse of 2 modulo 7 if and only if $x \equiv 4 \pmod 7$.

(b) Using the Euclidean Algorithm, we get $1 = 7(9) + 31(-2)$, so that 9 is a multiplicative inverse of 7 modulo 31. In general, $x \in \mathbb{Z}$ is a multiplicative inverse of 7 modulo 31 if and only if $x \equiv 9 \pmod{31}$.

Example

Find all solutions $x \in \mathbb{Z}$ (if any) that satisfies:
(a) $21x \equiv 32 \pmod{93}$; (b) $21x \equiv 33 \pmod{93}$.

Solution:

Observe first that $\gcd(21, 93) = 3$.

(a) This has no solution since $\gcd(21, 93) \nmid 32$.

(b) $21x \equiv 33 \pmod{93} \Leftrightarrow 7x \equiv 11 \pmod{31} \Leftrightarrow x \equiv 9(11) \pmod{31} \equiv 6 \pmod{31}$. (Note that 9 is a multiplicative inverse of 7 modulo 31 from the last Example.)

Summary

We have covered:

- Definition of congruences
- Modular arithmetic
- Multiplicative inverse modulo n
- Solving congruence equation of the form $ax \equiv b \pmod{n}$