M 328K: Lecture 5

Katherine Ho

September 10, 2024

1 Modular Congruences

Recall: We often use arguments like "n is of the form $4k, 4k+1, 4k+2, \text{or } 4k+3\ldots$"

Definition 1.1 (Precise)**.** *Let $a, b, n \in \mathbb{Z}$ and $n > 0$. We say that a is congruent to b mod n if $n|(a-b)$. We write*

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

Definition 1.2 (Informal)**.** *$a \equiv b$ mod n if a and b give the same remainder after division by n.*
Examples:

- $7 \equiv 2 \pmod{5}$
- $-31 \equiv 11 \pmod{7}$
- $10^{2024} + 1 \equiv 1 \pmod{1}0$
- $a \equiv b \pmod{2}$ *iff a and b are both even or both odd*
- *a can be written in the form*
$$a = nk + r$$
iff $a \equiv r \pmod{n}$

Proposition 1.1. *Every integer is congruent modulo n to exactly one of* $0, 1, 2, \ldots, n-1$

Proof. Let $a \in \mathbb{Z}$. By the division algorithm, we can write

$$a = nq + r,\ 0 \leq r < n$$

Then $a - r = nq$, so $n|a-r$, ie.

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

Uniqueness follows from uniqueness of division algorithm remainder. □

Theorem 1.1. *Let $a, b, c \in \mathbb{Z}, n > 0$. Then*

1. $a \equiv a \pmod{n}$
2. *if* $a \equiv b \pmod{n}$ *then* $b \equiv a \pmod{n}$
3. *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$

Proof (3). By definition, $n|a-b$ and $n|b-c$. Recall that if $n|r, n|s$, then $n|(rx+sy)$ for any $x, y \in \mathbb{Z}$. In particular,

$$n|((a-b)+(b-c)) \Leftrightarrow n|(a-c)$$

So $a \equiv c \pmod{n}$. □

Theorem 1.2. *Let $a, b, c, d \in \mathbb{Z}$ and assume* $a \equiv b \pmod{n}$.

1. *if* $c \equiv d \pmod{n}$*, then* $a + c \equiv b + d \pmod{n}$*.*

2. *if* $c \equiv d \pmod{n}$*, then* $ac \equiv bd \pmod{n}$*.*

3. $a^k \equiv b^k \pmod{n}\ \forall k \in \mathbb{Z}$*.*

Proof (1). Suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. By definition, $n|a-b$ and $n|c-d$.
But, $(a+c)-(b+d) = (a-b)+(c-d)$ which is divisible by n, so $a+c \equiv b+d \pmod{n}$. □

Proof (3) by Induction. Base case: $k = 1$. Tautology
Inductive step: Assume for some $k > 1$ that $a^k \equiv b^k \pmod{n}$ (WTS: $a^{k+1} \equiv b^{k+1}$)
Note by (2) we have

$$\begin{aligned} a^k &\equiv b^k \pmod{n} && [IH] \\ a^k \cdot a &\equiv b^k \cdot b \pmod{n} && [2] \\ a^{k+1} &\equiv b^{k+1} \pmod{n} \end{aligned}$$

□

WARNING: In general, if $ac \equiv bc \pmod{n}$, it is not true that $a \equiv b \pmod{n}$. Ex: $2 \cdot 3 \equiv 2 \cdot 0 \pmod{6}$

Example 1.2.1. *Show* $41|(2^{20}-1) \Leftrightarrow$ *Show* $2^{20} \equiv 1 \pmod{41}$.
First,

$$\begin{aligned} 2^5 &\equiv 32 \pmod{41} \\ (2^5)^2 &\equiv (-9)^2 \\ 2^{10} &\equiv 81 \pmod{41} \\ 2^{10} &\equiv -1 \pmod{41} \\ 2^{20} &\equiv (-1) \equiv 1 \pmod{41} \end{aligned}$$

Proposition 1.2. *A decimal integer is divisible by 3 iff the sum of its digits is divisible by 3.*

Proof. Let n be an integer whose decimal representation is

$$(a_n a_{n-1} \dots a_1 a_0)_{10}$$

Then

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 100 + \cdots + a_n \cdot 10^n$$

Then

$$a = a_0 + a_1 \cdot 10 + \cdots + a_n \cdot 10^n \pmod{n}$$

Since $10 \mod 3 \equiv 1$, we have

$$a \equiv a_0 + a_1 + \cdots + a_n \pmod{3}$$

□

2 Congruences with Unknowns

Example 2.0.1. *Solve*

$$\begin{aligned} x + 12 &\equiv 5 \pmod{8} \\ x &\equiv -7 \pmod{8} \end{aligned}$$

We also have

- $x \equiv 1 \pmod{8}$ *is also a solution*

- $x \equiv 9$
- $x \equiv 17$

But we consider these to be the "same" since they are congruent.

Example 2.0.2. *Solve*

$$\begin{aligned} 4x &\equiv 3 \pmod{19} \\ 20x &\equiv 15 \pmod{19} \\ x &\equiv 15 \pmod{19} \\ \textit{Since } 20 &\equiv 1 \pmod{19} \end{aligned}$$

Example 2.0.3. *Solve*

$$6x \equiv 15 \pmod{514}$$

This has no solutions.
Why?! $6x - 15$ *is always odd.*
In particular, $514 \nmid (6x - 15)$.
In general, we want to understand when $ax \equiv b$ *has solutions and how to find them.*

Example 2.0.4. $18x \equiv 8 \pmod{22}$ *has incongruent solutions*
$x \equiv 20 \pmod{22}$ *and* $x \equiv a \pmod{22}$