M 328K: Lecture 6

Katherine Ho

September 12, 2024

1 From Last Time

Solve $ax \equiv b \pmod{n}$.
It's possible for there to be no solutions OR a single solution OR multiple incongruent solutions.

Theorem 1.1. *1.* $a \equiv a \pmod{n}$

2. if $a \equiv b \pmod{n}$ *then* $b \equiv a \pmod{n}$

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

Example 1.1.1. $20 \equiv 1 \pmod{19}$

$$\begin{aligned} 20 &\equiv 1 \pmod{19} && \\ 20x &\equiv x \pmod{19} && \\ 20x &\equiv 15 \pmod{19} && \textit{We also have this} \\ x &\equiv 20x \pmod{19} && \textit{By (2)} \\ x &\equiv 15 \pmod{19} && \textit{By (3)} \end{aligned}$$

2 Solving stuff

WARNING: If $ac \equiv bc \pmod{n}$, we can't conclude $a \equiv b \pmod{n}$.

Theorem 2.1. *If* $\gcd(c, n) = 1$, *then* $ac \equiv bc \pmod{n}$ *implies* $a \equiv b \pmod{n}$.

Proof. By definition, we have

$$n \mid (a - b)c$$

By Euclid's Lemma, since $\gcd(n, c) = 1$, we have $n \mid (a - b)$, hence $a \equiv b \pmod{n}$. □

Proposition 2.1. *Let* $d = \gcd(a, b)$ *for some* $a, b \in \mathbb{Z}$. *Then* $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof. By Bezout, there exist integers x and y such that $ax + by = d$. Then,

$$(\frac{a}{d}x + \frac{b}{d}y) = 1$$

So $\frac{a}{d}, \frac{b}{d}$ are relatively prime. □

Theorem 2.2. *Consider* $ac \equiv bc \pmod{n}$ *and let* $d = \gcd(c, n)$. *Then* $a \equiv b \pmod{\frac{n}{d}}$.
Note: If $d = 1$, *this is the same statement as before.*

Proof. $n \mid (a-b)c$ as before. So there exists $k \in \mathbb{Z}$ such that $(a-b)c = nk$. Then,

$$(a-b)\frac{c}{d} = \frac{n}{d}k$$

So,

$$\frac{n}{d} \mid (a-b)\frac{c}{d}$$

By Proposition 2.1, $\gcd(\frac{n}{d}, \frac{c}{d}) = 1$, so Euclid's Lemma says

$$\frac{n}{d} \mid (a-b), \text{ ie. } a \equiv b \pmod{\frac{n}{d}}$$

□

Example 2.2.1.

$$2 \cdot 3 \equiv 2 \cdot 0 \pmod 6 \qquad \gcd(2,6) = 2$$
$$3 \equiv 0 \pmod 3$$

Theorem 2.3 (Build-a-theorem)**.** *Let $a, b, n \in \mathbb{Z}$ with $n > 1$, let $d = \gcd(a, n)$. Then the linear congruence $ax \equiv b \pmod n$.*

- *has no solution if $d \nmid b$*
- *has exactly d incongruent solutions $\pmod n$ if $d \mid b$*

In particular, if x_0 is a solution, then

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$$

is a complete set of solutions $\pmod n$, ie. if x is a solution, then x is congruent modulo n to exactly one of

$$x_0 + t(\frac{n}{d}) \text{ for } 0 \leq t \leq d-1$$

Study $ax \equiv b \pmod n$. If this has a solution x, then $n \mid (ax - b)$. Then there exists $y \in \mathbb{Z}$ such that

$$ax - b = ny$$

So,

$$ax - ny = b$$

This linear diophantine equation has a solution exactly when $\gcd(a, n) = d \mid b$.

Recall: $6x \equiv 15 \pmod{512}$. $\gcd(6, 512) = (1, 2, 3, \text{or } 6)$. Note $3 \nmid 512$ since $3 + (5 + 1 + 2)$.
But $2 \nmid 15$, so there are no solutions.

Example 2.3.1. *Solve*

$$9x \equiv 21 \pmod{30}$$

$d = \gcd(9, 30) = 3 \mid 21$ *Either write down*

$$9x - 30y = 21$$

dividing,

$$3x - 10y = 7$$

OR apply Theorem 2.2 to yield

$$3x \equiv 7 \pmod{10}$$

leading to

$$3x - 10y = 7$$

Extended Euclidean algorithm

$$\begin{aligned} 10 &= 3 \cdot 3 + 1 \\ 10 - 3 \cdot 3 &= 1 \\ 10 \cdot 7 - 3 \cdot 21 &= 7 \\ -10(-7) + 3(-21) &= 7 \end{aligned}$$

$\boxed{x\text{=-}21, y\text{=-}7}$

But $x \equiv (-21) + 30 \pmod{30}$. $x \equiv 9 \pmod{30}$. *So we have found one solution (up to congruence).*
*Note: * $x = 9$ *is a solution to* $3x \equiv 7 \pmod{10}$. *So,* $x = 19$ *and* $x = 29$ *are also soolutions to* $3x \equiv 7 \pmod{10}$ *that are distrinct* $\pmod{30}$.

Example 2.3.2. *Solve*

$$18x \equiv 8 \pmod{22}$$

$d = \gcd(18, 22) = 2$. *First find a solution to*

$$9x \equiv 4 \pmod{11}$$

Solve

$$9x - 11y = 4$$

this has a solution $x = -2$, $y = -22$.
Choose $x = -2 + 11 = 9$ *is one solution.*
The other distinct solution $\pmod{22}$ *is*

$$x = 9 + 11 = 20$$

$x = 9, 20$ *is a complete set of solutions up to congruence* $\pmod{22}$.