MATH3360 Lecture 2/16

Benjamin Thompson
Spring 2023, Cornell

Congurences (cont.)

Last time: abbreviation of "if and only if"

Def $a \equiv b \pmod{n} \Leftrightarrow a$ & b have the have the same remainder after division by n.

Prop $a \equiv b \pmod{n}$ iff $n \mid a-b$.

Prop $a \equiv c \pmod{n}$, $b \equiv d \pmod{n}$

$\Rightarrow$ (1) $a \pm b \equiv c \pm d \pmod{n}$

(2) $ab \equiv cd \pmod{n}$.

Prop If $n>1$, $ax \equiv 1 \pmod{n}$ has a solution iff $\gcd(a,n)=1$.

Today:

$ax \equiv b \pmod{n}$; congurence classes.

Prop 1 $ax \equiv b \pmod{n}$ has a solution iff it has a solution when $0 \le x < n$.

Pf ($\Leftarrow$): obvious.

($\Rightarrow$): Let $z \in \mathbb{Z}$ satisfy $az \equiv b \pmod{n}$. Apply the division algorithm to z: $z = qn + r$, $0 \le r < n$.

Then $z \equiv r \pmod{n}$, so

$$az \equiv ar \pmod{n}.$$

Hence $ar \equiv az \equiv b \pmod{n}$. $\square$

From now on, we will only consider solutions to $ax \equiv b \pmod{n}$ satisfying $0 \leq x < n$.

<u>Exercise</u> How many distinct solutions do the following eqns. have?

$2x \equiv 1 \pmod{3}$

$2x \equiv 0 \pmod{4}$

$3x \equiv 2 \pmod{5}$

$2x \equiv 6 \pmod{102}$

$2^{300}x \equiv 2^{350} \pmod{2^{400}}$.

<u>Theorem 2</u>: Let $a, b, n \in \mathbb{Z}$, $n > 1$. The equation $ax \equiv b \pmod{n}$:

(1) has a solution iff $\gcd(a, n) \mid b$.

(2) Let $d = \gcd(a, b)$. If $d \mid b$, the equation has d solutions, and they are congruent mod n/d.

Pf (1) $az \equiv b \pmod n$

$\iff n \mid az - b$ means "there exists"

$\iff \exists k$ s.t $az - nk = b$

$\iff \gcd(a,n) \mid b$. Exercise! $\square$

(2) Let y and z be solutions to $ax \equiv b \pmod n$. Then

$$n \mid a(y-z), \text{ so}$$

$$n \mid \gcd(a,n)(y-z) \text{ or } n \mid d(y-z).$$

hence $\frac{n}{d} \mid \frac{d}{d}(y-z)$ or $n/d \mid y-z$

$$\iff$$

$$y \equiv z \pmod{n/d}$$

It is easy to show that if

$y \equiv z \pmod{n/d}$ and $ay \equiv b \pmod n$,

then $az \equiv b \pmod n$ too. $\blacksquare$

Eg $2x \equiv 6 \bmod 102$ has a soln. at $x = 3$. Since $\gcd(2, 102) = 2$, there is one more solution, and since $102/2 = 51$, this solution is $3 + 51 = 54$.

Idea: Can we define $+$ and $\times$ on remainders?

Def Let $a \in \mathbb{Z}$. The congruence class of $a \bmod n$ is defined as:

$$[a]_n := \{z \in \mathbb{Z} : a \equiv z \pmod n\}$$

Def: Let $A, B \subseteq \mathbb{Z}$ be subsets of the integers.

means "is defined to be"

Then $A \tilde{+} B := \{a+b : a \in A, b \in B\}$

$$A \tilde{\times} B := \{ab : a \in A, B \in B\}.$$

Exercise What are the following?

$[1]_2 \tilde{+} [1]_2$

$[0]_2 \tilde{\times} [1]_2$

Prop: (1): $[a]_n \tilde{+} [b]_n = [a+b]_n$

(2): $[a]_n \tilde{\times} [b]_n \subset [ab]_n$.

Pf: (1) Let $\tilde{a} \in [a]_n$, $\tilde{b} \in [b]_n$.

So $\tilde{a} \equiv a \pmod n$, $\tilde{b} \equiv b \pmod n$.

Then $\tilde{a} + \tilde{b} \equiv a + b \pmod n$, so

$\tilde{a} + \tilde{b} \in [a+b]_n$.

Hence $[a]_n \tilde{+} [b]_n \subset [a+b]_n$.

Now let $z \equiv a+b \pmod n$.

Then $z - a \equiv b \pmod n$, and

$z = a + (z-b)$, so $z \in [a]_n \tilde{+} [b]_n$.

Hence $[a+b]_n \subset [a]_n + [b]_n$. $\boxtimes$

(2): Exercise. $\blacksquare$

Note $[2]_5 \tilde{\times} [3]_5 \neq [6]_5$!

<u>Idea:</u> Define $+, -$ on congruence classes by representatives.

<u>Prop:</u> $[a]_n + [b]_n := [a+b]_n$,
$[a]_n [b]_n := [ab]_n$
is well-defined.

<u>Pf:</u> Let $[a]_n = [x]_n$,
$[b]_n = [y]_n$.

We want to show that
$[a+b]_n = [x+y]_n$, and
$[ab]_n = [xy]_n$.

This amounts to showing that
$a+b \equiv x+y \pmod n$, and
$ab \equiv xy \pmod n$. $\blacksquare$

Eg The equation $x^2+y^2=3$ has no rational solutions.

Step 1 A rational solution gives an integer solution to $x^2+y^2=3z^2$ with $\gcd(x,y,z)=1$.

Step 2 If $x^2+y^2=3z^2$ with $\gcd(x,y,z)=1$, at least one of x, y is odd.

Step 3 $x^2 + y^2 = 3z^2$ has no solutions if one of x, y are odd.