In this class, we continue to solve the congruent equations.

$$f(x) \equiv 0 \pmod{m}.$$

For congruent equations, we want to find all <u>incongruent solutions</u>.

Definition: Let a, b be solutions for the congruent equation:

$$f(x) \equiv 0.$$

They are

<u>congruent solutions</u> if $a \equiv b \pmod{m}$

<u>incongruent solutions</u> if $a \not\equiv b \pmod{m}$

Example: $x^2 - 4x + 3 \equiv 0 \pmod{8}$

$x = 1$ is a solution.

$x = 9$ is a solution

$x = 3$ is a solution.

congruent

incongruent

incongruent

By the observation in last class, if $f(x) \equiv 0$ has a solution, say $x = a$, then we can find

$$0 \leq r \leq m-1$$

$a \equiv r \pmod{m}$.

Then $x = r$ is also a solution for $f(x) \equiv 0$.

We prefer to use r as the solution for

$f(x) \equiv 0$.

We would write the solution as $r \pmod{m}$

Example: $x^2 - 4x + 3 \equiv 0 \pmod{8}$

Solutions: $x \equiv 1 \pmod{8}$ $\quad x \equiv 3 \pmod{8}$

Question: Do we have other (incongruent) solutions ?

Answer: Yes! $x \equiv 5 \pmod{8}$ $\quad x \equiv 7 \pmod{8}$.

Here is a way to find all (incongruent) solutions:

- List $0, 1, \cdots, m-1$
- Plug in $f(x) \equiv 0 \pmod{m}$ to check whether it is a solution.

Linear Congruent Equations:

We consider: $ax \equiv b \pmod{m}$

Observation: if x_0 is a solution, then

$$m \mid ax_0 - b$$

In other words, we can find a number l such that

$$ax_0 - b = l \cdot m$$

This becomes $ax_0 - lm = b$

This means: $\gcd(a, m) \mid b$.

Theorem: Let $ax + b \equiv 0 \pmod{m}$

Then it has no solution if $\gcd(a, m) \nmid b$.

If $\gcd(a, m) \mid b$, we can find a solution as follows:

(1) Find r, s such that

$$ra + sm = \gcd(a, m)$$

(2) Multiply the equation by $\frac{b}{\gcd(a,m)}$

$$a \cdot \frac{rb}{\gcd(a,m)} + \frac{bs}{\gcd(a,m)} \cdot m = b$$

Then $a \cdot \frac{rb}{\gcd(a,m)} \equiv b \pmod{m}$

and $x = \frac{rb}{\gcd(a,m)}$ is a solution.

(3) Find the number between 0 and $m-1$ which is congruent to $\frac{rb}{\gcd(a,m)}$ and this is the solution.

Note: this does <u>not</u> give all the incongruent solutions for a linear congruent equation.

To find all incongruent solutions for a linear congruent equation, see Theorem 8.1 in the textbook.

Example: $7x \equiv 3 \pmod{15}$

Solution: $\gcd(7,15) = 1 \mid 3 \Rightarrow$ It has a solution!

Step I: $-2 \cdot 7 + 15 = 1$

Step II: $\frac{3}{\gcd(7,15)} = \frac{3}{1} = 3$

$3(-2 \cdot 7 + 15) = 3 \cdot 1$

$$7 \cdot (-6) + 45 = 3$$

$$7 \cdot (-6) - 3 = -45$$

$$\Rightarrow \quad 7 \cdot (-6) \equiv 3 \pmod{15}$$

$\Rightarrow$ -6 is a solution

Step III: $-6 \equiv 9 \pmod{15}$

Therefore $9 \pmod{15}$ is a solution for

$$7x \equiv 3 \pmod{15}.$$

$\square$