Math135 - October 29'th, 2015

Everything We Know About Congruences

$a \equiv r \pmod{n}$

- $\iff m \mid (a-b)$
- $a \bmod m = b \bmod m$
- Transitive:
  $[a \equiv b \pmod{m}\ ] \wedge\ [b \equiv c \pmod{m}\ ] \implies a \equiv c \pmod{m}$
- Symetric:
  $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$
- Reflective:
  $a \equiv a \pmod{m}$
- You can multiply, add, or subtract a to the left side and b to the right side so long as $a \equiv b \pmod{m}$
- You can divide both sides by n if $\gcd(n, m) = 1$ (Co-prime)

Congruent Iff Same Remainder (CISR)

Let $a, b, c \in \mathbb{N}$ where $m > 0$
$a \equiv b \pmod{m} \iff a$ and b have the same remainder when divided by m.

Linear Congruence

Let $a, c, m \in \mathbb{Z}$ where $m > 0$ A relation of the form

$$ax \equiv c \pmod{m}$$

is called a Linear Congruence in the variable x. A solution is an integer $ax_0 \equiv c \pmod{m}$

Examples:

i) $4x \equiv 5 \pmod{8}$
$4x - 5 = 8k$
$4x - 8k = 5$
$\gcd(4, -8) = 4$
$4 \nmid -8$
$\therefore$ No solution

ii) $5x \equiv 3 \pmod{7}$
$5x - 3 = 7k$
$5x - 7k = 3$
$5x + 7y = 3$ (Let $y = -k$)
$x = 2, y = 1$
$x = 2 + 7n$ (By LDET2)
$\therefore x \equiv 2 \pmod{7}$

iii) $2x \equiv 4 \pmod{6}$
$2x - 4 = 6k$
$2x - 6k = 4$
$2x + 6y = 4$
$\gcd(2, 6) = 2$
$2|4$ Thus there is a solution
By inspection, $x = -1, y = 1$
$x = -1 + 3n$ By LDET2
$x \equiv -1 \pmod{3}$
$x \equiv 3 \pmod{3}$

Generalised Linear Congruence Rules:

i) A solution does not always exist.
ii) $\gcd(a, m)|c$ means a solution exists.
iii) To find a particular solution, convert into a linear diophantine equation using:
$ax \equiv c \pmod{m} \implies (ax - c) = mk, k \in \mathbb{N}$

Generalised Linear Congruence Rules:

Example) Solve $x^2 \equiv 6 \pmod{10}$

- There is no efficient way to solve polynomial congruences.

$x \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$x^2 \pmod{10}$	0	1	4	9	6	5	6	9	4	1

- As we can see, $x \equiv 4, 6 \pmod{10}$