Discrete Math

Lecture 34

Solving Congruence Equations

Main Idea

$$\underbrace{\cancel{a^{-1}}\,\cancel{a}}x = a^{-1}b$$

$$1 \cdot x = a^{-1}b$$

$$x = a^{-1} \cdot b = \frac{b}{a}$$

$$ax \equiv b \mod n$$

we need an a^{-1} to use!

- in mod n not all integers have an inverse!

gcd (a, n) saves us here!

- $\gcd(a,n) \mid b \longrightarrow$ there are solutions!

$\gcd(a,n) = 1 \longrightarrow$ we can find $a^{-1} \mod n$ *

$\gcd(a,n) > 1 \longrightarrow$ we replace the original eqn w/ a new one where there are inverses

we use Bezout's Id. (E. Algrthm backwards) to find an inverse ex) $4x \equiv 12 \mod 7$

1) $\gcd(4,7) = 1$ $\quad 1 \mid 12 \longrightarrow$ there are solutions

Euclid's Algorithm

$7 = \underline{1} \cdot 4 + \underline{\boxed{3}}$ gcd

$4 = \underline{1} \cdot 3 + \underline{1}$

$3 = \underline{3} \cdot 1 + \underline{\boxed{0}}$

2) 4 & 7 are rel. prime $\longrightarrow$ 4 has an inverse mod 7

Run Euclid's Algorithm Backwards

$(1 = \_\_4 + \_\_7)$

$1 = 4 - 1 \cdot \boxed{3} = 4 - 1 \cdot (7 - 1 \cdot 4)$

$1 = 4 - 7 + 4 = 2 \cdot 4 + (-1) \cdot 7$

3) rewrite Bezout's Id. mod n = mod 7

$1 \equiv (2) \cdot 4 + (-1) \cdot 7 \mod 7$

$r = 0$ when div by 7

$$1 \equiv (2)\cdot 4 \mod 7$$

this tells us what a^{-1} is

$$4^{-1} \equiv 2 \mod 7$$

check: $2 \cdot 4 = 8 \equiv 1 \mod 7$

4) multiply both sides by a^{-1} to find one solution.

$$4x \equiv 12 \mod 7$$

$$\underbrace{2 \cdot 4}\, x \equiv 2 \cdot 12 \mod 7$$

$$1 \cdot x \equiv 24 \mod 7$$

$\boxed{\text{one solution is } x = 24}$

5) the solution set is: $\{ \ldots \boxed{3}, 10, 17, 24, 31, 38 \ldots \}$

$$\to \{ 24 + n \cdot 7 : n \in \mathbb{Z} \}$$

only one solution in $\{0, 1, 2, \boxed{3}, 4, 5, 6\}$

<u>Note</u> $ax \equiv b \bmod n$

$\gcd(a, n) = 1 \longrightarrow$ solutions

exactly one solution in $\{0, 1, \ldots, n-1\}$

<u>ex</u> $26x \equiv 180 \bmod 13$

$\gcd(26, 13) = 13$ but $13 \nmid 180$

therefore there are no solutions!

<u>ex</u> $3x \equiv 24 \bmod 9$

$\gcd(3, 9) = 3$ + $3 \mid 24 \longrightarrow$ are solutions

since $\gcd(3, 9) > 1$, we first replace this eqn with a new one by dividing by $\gcd(3, 9) = 3$

$$x \equiv 8 \bmod 3$$

new eqn has $\gcd(a', n') = 1$

we can now find an inverse!

$x = 8$ is one solution

check : $3 \cdot 8 = 24 \equiv 24 \mod 9$ ✓

(there are other solutions

$$8 + \frac{n}{\gcd(a,n)} = 8 + 3 = 11$$
)

$$\{0, 1, \boxed{2}, 3, 4, \boxed{5}, 6, 7, \boxed{8}\}$$

$8 + 3 = 11 \equiv 2 \mod 9$

$2 + 3 = 5 \equiv 5 \mod 9$

ex) $6x \equiv 24 \mod 9$

$\gcd(6, 9) = 3 \quad 3 \mid 24 \longrightarrow$ solutions ✓

$$2x \equiv 8 \mod 3$$

$\gcd(2,3) = 1 \longrightarrow 2$ has an inverse mod 3

$$3 = \underline{1} \cdot 2 + \underline{1}$$

$$\boxed{1 = 3 - 1 \cdot 2}$$

$$2 = \underline{2} \cdot 1 + \boxed{0}$$

$$1 \equiv (-1) \cdot 2 \mod 3$$

$$\left(\begin{array}{l} 1 = 2 \cdot 2 + (-1) \cdot 3 \\ 1 \equiv 2 \cdot 2 \mod 3 \end{array} \right)$$

$$2x \equiv 8 \mod 3$$

$$\underbrace{(-1) \cdot 2}_{1} x \equiv (-1) \cdot 8 \mod 3$$

$$x \equiv -8 \mod 3 \longrightarrow \boxed{\text{one soln } x = -8}$$

orig. eqn. $6x \equiv 24 \mod 9$

$$-8 + 1 \cdot 9 = \boxed{1}$$

$$\{ 0, \boxed{1,} \, 2, 3, \boxed{4,} \, 5, 6, \boxed{7,} \, 8 \}$$

$$x_0 \qquad x_0 + \frac{n}{\gcd} \qquad x_0 + \frac{2n}{\gcd}$$