MATH 407
2/28/18

* Linear Congruences (contd.)

1) $ax \equiv 0 \pmod{n}$

$(a,n) = d$, $a'd = a$, $n'd = n$

General solution: $n'\mathbb{Z} = \{n'k : k \in \mathbb{Z}\}$

2) $ax \equiv b \pmod{n}$

If x_p solution then any other $x_p + n'k$, $k \in \mathbb{Z}$
$\Rightarrow x_p + n'\mathbb{Z}$

3) $ax \equiv b \pmod{n}$

solvable iff $d \mid b$, $b = db'$

$a'x \equiv b' \pmod{n'}$

4) $ax \equiv 1 \pmod{n}$

iff $(a,n) = 1$, $(a', n') = 1$

If $a'y_0 \equiv 1 \pmod{n'}$
then $a'(b'y_0) \equiv b' \pmod{n'}$

$b'y_0 = x_p$

$a'y_0 + n'q = 1$, for some y_0, q

$\Rightarrow a'y_0 \equiv 1 \pmod{n'}$
$(\equiv 0 \pmod{a'})$

* $y_0 b', y_0 b' + n', \ldots, y_0 b' + (d-1) n'$

$\underline{d \text{ solutions}}$

* Systems of linear congruences:

$a_1 x \equiv b_1 \pmod{n_1}$
$a_2 x \equiv b_2 \pmod{n_2}$

$(a_1, n_1) = 1 = (a_2, n_2)$

$a_1 y_1 \equiv 1 \pmod{n_1}$
$a_2 y_2 \equiv 1 \pmod{n_2}$

$x \equiv b_1 \pmod{n_1}$
$x \equiv b_2 \pmod{n_2}$

$(n_1, n_2) = 1$ (relatively prime)

$\underbrace{n_1 k_1}_{u_1} + \underbrace{n_2 k_2}_{u_2} = 1$

$u_1 \equiv 1 \pmod{n_1}, \quad u_2 \equiv 0 \pmod{n_1}$
$u_1 \equiv 0 \pmod{n_2}, \quad u_2 \equiv 1 \pmod{n_2}$

Set $x = b_1 u_1 + b_2 u_2$

$x \equiv b_1 \cdot 1 + b_2 \cdot 0 \pmod{n_1}$

$x \equiv b_1 \cdot 0 + b_2 \cdot 1 \pmod{n_2}$

Example:

Solve: $x \equiv 7 \pmod 8$, $n_1 = 8$
$x \equiv 3 \pmod 5$, $n_2 = 5$

$$1 = \underbrace{2 \cdot 8}_{u_2} + \underbrace{(-3) \cdot 5}_{u_1}$$

$$2 \cdot 8 = 16 \equiv 1 \pmod 5$$
$$\equiv 0 \pmod 3$$

$$(-3) \cdot 5 = -15 \equiv 0 \pmod 5$$
$$\equiv 1 \pmod 8$$

$$\therefore x = 7u_1 + 3u_2$$
$$= 7(-15) + 3(16)$$
$$= -105 + 48$$
$$= -57$$
$$\Rightarrow x = -60 + 3$$
$$x = -64 + 7$$

* If x_1, x_2 are solutions of

$$x_1 \equiv b_1 \pmod{n_1}$$
$$x_2 \equiv b_2 \pmod{n_2}$$
$$x_1 - x_2 \equiv 0 \pmod{n_i},\ i = 1, 2$$

$$n_1 \mid (x_1 - x_2),\ n_2 \mid (x_1 - x_2)$$

$$\Rightarrow n_1 n_2 \mid (x_1 - x_2)$$

Thus, $x_2 \in x_1 + n_1 n_2 \mathbb{Z}$, solutions in $\{0, \dots, n_1 n_2 - 1\}$
n_1, n_2 possible (b_1, b_2)

(referring back to previous example)

$\therefore x = -60 + 3$

$x = -64 + 7$

$\Rightarrow x = -57 + 80 = 33$

Chinese Remainder Thm

Given $0 \leq b_1 < n_1$

$0 \leq b_2 < n_2$

$(n_1, n_2) = 1$

$\exists x : 0 \leq x < n_1 n_2$

$x \equiv b_1 \pmod{n_1}$

$x \equiv b_2 \pmod{n_2}$

Thm. Let $n_1, n_2, \ldots, n_k$ be relatively prime moduli
Let $0 \leq b_i < n_i \ \forall i$

$\exists x : 0 \leq x < n_1 n_2 \cdots n_k$

$x \equiv b_i \pmod{n_i}, \ \forall i$

* There is a u_i s.t. $u_i \equiv 1 \pmod{n_i}$

$u_i \equiv 0 \pmod{n_j}, \ j \neq i$

$x = b_1 u_1 + \ldots + b_k u_k$

$m_1 = n_2 n_3 \cdots n_k$

$(n_1, n_j) = 1 \ \forall j \neq 1$

$(\longrightarrow)$

so: $(n_1, (n_2 n_3 \cdots n_k)) = 1$ (rel. prime)

Can find: $u_1 \equiv 1 \pmod{n_1}$
$u_1 \equiv 0 \pmod{n_2 n_3 \cdots n_k}$
$\Rightarrow u_1 \equiv 0 \pmod{n_j},\ j = 2, 3, \ldots, k$

* [Sec 4]

Let $n \in \mathbb{N}$
$\equiv \pmod{n}$ is an equivalence relation

$[a]_n = \{b : a \equiv b \pmod{n}\}$

$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$

$\Rightarrow [a]_n + [b]_n = [a+b]_n$
$[a]_n [b]_n = [ab]_n$

*More next class. Exam 1 on Monday