33

Extended Euclidean Algorithm

$(9, 30) = ?$

30	1	0	9	0	1] x 3
9	0	1	3	1	-3] x 3
3	1	-3	0		

$$3 = 1 \times 30 + (-3) \times 9$$

Theorem (Chinese Remainder Theorem) 34

Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

has a simultaneous solution which is unique modulo $(n_1 n_2 \ldots n_r)$.

Proof:

Let $n = n_1 \cdot n_2 \cdot \ldots n_r$

Define $N_k = \dfrac{n}{n_k}$; $k = 1, 2, \ldots r$

$$= n_1 n_2 \ldots n_{k-1} n_{k+1} \ldots n_r$$

As $(n_i, n_j) = 1$, $i \neq j$, $\therefore$ $(N_k, n_k) = 1$

Let x_k be the solution of $N_k x \equiv 1 \pmod{n_k}$

To show $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_k N_k x_k$ is a simultaneous solution of system of linear congruence equations

35

Now $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$

$\because$ $n_k \mid N_i$

$\bar{x} \equiv a_k N_k x_k \pmod{n_k}$

$\equiv a_k \pmod{n_k}$

Solution to given system of equations exists.

<u>Uniqueness:</u> Let x' be any other solution.

$\bar{x} \equiv a_k \equiv x' \pmod{n_k}$; $k = 1, 2, \ldots r$

So $n_k \mid \bar{x} - x'$ for each k

$\because$ $(n_i, n_j) = 1$

$\therefore$ $n_1 n_2 \ldots n_r \mid \bar{x} - x'$

$\Rightarrow$ $\bar{x} \equiv x' \pmod{n}$

36

Solve
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

$n = 3 \cdot 5 \cdot 7$

$n_1 = 3, \quad n_2 = 5, \quad n_3 = 7$

$N_1 = \frac{n}{n_1} = 35$

$N_2 = 21$

$N_3 = 15$

Linear Congruences

$35x \equiv 1 \pmod 3$ Solution $x_1 = 2$

$21x \equiv 1 \pmod 5$ $x_2 = 1$

$15x \equiv 1 \pmod 7$ $x_3 = 1$

$\bar{x} = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$

$\equiv 23 \pmod{105}$

37

Solve $17x \equiv 9 \pmod{276}$ using chinese remainder theorem

$17x \equiv 9 \pmod 3 \Rightarrow x \equiv 0 \pmod 3$

$17x \equiv 9 \pmod 4 \Rightarrow x \equiv 1 \pmod 4$

$17x \equiv 9 \pmod{23} \Rightarrow x \equiv 17^{-1} \cdot 9 \pmod{23}$

$\equiv 19 \cdot 9 \pmod{23}$

$\equiv 10 \pmod{23}$

$N_1 = 92$ $\quad n_1 = 3$

$N_2 = 69$ $\quad n_2 = 4$

$N_3 = 12$ $\quad n_3 = 23$

$x_1 = 2$

$x_2 = 1$

$x_3 = 1$

$\bar{x} = 0 \cdot 92 \cdot 2 + 1 \cdot 69 \cdot 1 + 10 \cdot 12 \cdot 2 \pmod{276}$

$\equiv 309 \pmod{276}$

$\equiv 33 \pmod{276}$

Solve the linear congruence equation

$$5x \equiv 1(mod\ 117)$$

Ans: 47

(5, 117)=1: unique solution

$$x = 5^{-1}(mod\ 117)$$

117	1	0	5	0	1
5	0	1	2	1	-23
2	1	-23	1	-2	47

Solution =47

Solve $3x \equiv 6(mod\ 90)$

(3, 90)=3

3 divides 6.

So the equation is solvable

$$x \equiv 2(mod\ 30)$$

$$x = 32$$

$$x = 2, 32, 62$$

Incongruent modulo 90