21PC11
GINANAMBAL . M.

ALGEBRA AND NUMBER THEORY

SOLVING LINEAR CONGRUANCES.

Lemma 1: The linear congruance $ax \equiv b \pmod n$ has a solution if and only if $d = (a, n)$ divides b.

Proof: Assume that $ax \equiv b \pmod n$ has a solution say $K \in N$

Then $n \mid aK - b$ (or) $aK - b = n\alpha$ for some $\alpha \in Z$.

$$\Rightarrow b = aK - n\alpha$$

Now, $d = (a, n)$ divides the RHS and $d \mid b$.

We now assume that $d \mid b \Rightarrow b = dK$

$$d = a\alpha + n\beta \text{ for some } \alpha, \beta \in Z. \text{ (Linear combination)}$$

$$b = dK = a\alpha K + n\beta K$$

$$\Rightarrow b = a(\alpha K) \pmod n$$ Solution to the congruance.

Lemma 2: If x_0 is a solution to the linear congruance $(ax \equiv b \pmod n)$ then all the solutions are of the form $x_0 + (n/d)t$, where t varies over all integers.

Proof: In particular, there are presisely d solutions among the residue classes modulo n.

$$x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{2n}{d}, \ldots \quad x_0 + \frac{(d-1)n}{d}, \quad \frac{n}{d} \in N.$$

Assume that $a x_0 \equiv b \pmod n$, x_0 - solution.

Take $x_1 = x_0 + \frac{n}{d} t$ for some $t \in Z$.

To prove: $a x_1 \equiv b \pmod n$

$$a x_1 = a\left(x_0 + \frac{n}{d}t\right)$$

$$a x_1 = a x_0 + \frac{an}{d}t$$

$$a x_1 = a x_0 + n\frac{a}{d}t, \quad \text{since } d \mid a, \frac{a}{d} \in N$$

$$\therefore a x_1 \equiv a x_0 \pmod n$$

$$a x_1 \equiv b \pmod n$$

We now prove that any two solutions x_0, x_1 to $ax \equiv b \pmod n$ are related by $x_1 = x_0 + \frac{n}{d} t$ for some $t \in Z$.

$$a x_0 \equiv a x_1 \pmod n$$

$$\Rightarrow n \mid a x_0 - a x_1 = n \mid a(x_0 - x_1)$$

$$\Rightarrow a(x_0 - x_1) = nt.$$

$a(x_0 - x_1) = nt$

$\cancel{d} \cdot \frac{a}{d}(x_0 - x_1) = \cancel{d} \cdot \frac{n}{d} t$

$\frac{n}{d} \mid \frac{a}{d}(x_0 - x_1)$

Since $\left(\frac{n}{d}, \frac{a}{d}\right) = 1$, we get

$\frac{n}{d} \mid x_0 - x_1$ (or) $x_1 = x_0 + \frac{n}{d}s$ for some $s \in Z$.

Solve : 1) $7x \equiv 3 \pmod{12}$

Find GCD.

$d = (7, 12) = 1$.

$\Rightarrow$ There is a solution to the congruance and it is unique modulo 12.

To find solution inverse of 7 to be multiplied.

$7x \equiv 3 \pmod{12}$

$\cancel{7} \times 7x \equiv \cancel{7} \times 3 \pmod{12}$

~~$49x \equiv 21 \pmod{12}$~~ $7 \times 7 = 49 \bmod 12 = 1$.

$7 \times 3 = 21 \bmod 12 = 9$.

$\Downarrow \quad \Downarrow$

$x = 9$

$\therefore x \equiv 9 \pmod{12}$ is the unique Solution

2) Find all solutions for $10x \equiv 6 \pmod{14}$

$d = (10, 14) = 2$ and $d \mid b = 2 \mid 6$

$\Rightarrow$ We will get 2 solutions modulo 14.

It is enough to solve $5x \equiv 3 \pmod 7$

If $7 \mid 5x - 3$ then $14 \mid 10x_0 - 6$.

Here $d = (5, 7) = 1$.

We need to find a number α in Z_7 such that $5\alpha = 1$.

Here $\alpha = 3$. $\therefore$ Multiply both sides by 3.

$3 \times 5x \equiv 3 \times 3 \pmod 7$

$x = 2$.

$\therefore x_0 = 2$ is a solution to the congruance.

$\frac{n}{d} = \frac{14}{2} = 7$.

$\therefore 2 + 7 = 9$ is also a solution

Algorithm for solving linear congruance $ax \equiv b \pmod n$

→ Check if $d = (a,n)$ divides b.

→ Solve for $(a/d)x \equiv b/d \pmod{n/d}$

→ Seek whether we can reduce the coefficient of x further.

If $d \nmid b$, then there are no solutions.

Lemma 3: Let m divide each of the a, b and n, and let $a' = a/m$, $b' = b/m$ and $n' = n/m$ then $ax \equiv b \pmod n$ has a solution if and only if $a'x \equiv b' \pmod{n'}$ has a solution.

Proof: Assume that $a'x \equiv b' \pmod{n'}$ has a solution.

Let the solution be $\alpha \in \mathbb{Z}$.

Then $n' \mid a'\alpha - b'$

$$\cancel{\frac{n}{d} \mid \frac{a}{d}\alpha - \frac{b}{d}} \quad \text{i.e} \quad \frac{n}{m} \mid \frac{a}{m}\alpha - \frac{b}{m}$$

$$\Rightarrow \frac{n}{\cancel{m}} \mid \frac{1}{\cancel{m}}(a\alpha - b)$$

$$\Rightarrow n \mid a\alpha - b$$

Thus a solution to $a'x \equiv b' \pmod{n'}$ gives a solution to $ax \equiv b \pmod n$

Assume that $ax \equiv b \pmod n$ has a solution. Let the solution be $\gamma \in \mathbb{Z}$.

Then $n \mid a\gamma - b$

$$m \cdot \frac{n}{m} \mid m \cdot \left(\frac{a}{m}\gamma - \frac{b}{m}\right)$$

There is an integer m divides a, b & n.

$$\cancel{m} n' \mid \cancel{m}(a'\gamma - b')$$

$$n' \mid a'\gamma - b'$$

Thus a solution to $ax \equiv b \pmod n$ gives a solution to $a'x \equiv b' \pmod{n'}$.

Lemma 4: Let $(a,n) = 1$ (unique solution).

Let m divide a and b and let $a' = a/m$ and $b' = b/m$ then $ax \equiv b \pmod n$ has a solution if and only if $a'x \equiv b' \pmod n$ has a solution.

Proof: Assume that $a'x \equiv b' \pmod n$ has a solution say $\alpha \in \mathbb{Z}$

Then $n \mid a'\alpha - b'$ i.e

$$n \mid \frac{a}{m}\alpha - \frac{b}{m} \qquad \cancel{m\left(\frac{a}{m}\right)}.$$

$$n \mid a\alpha - b \qquad m\left(\frac{a}{m}\alpha - \frac{b}{m}\right)$$

Thus $n \mid ax - b$ or $ax \equiv b \pmod{n}$ has a solution

Thus the solution to $a'x \equiv b' \pmod{n}$ gives a solution to $ax \equiv b \pmod{n}$

Note: $(a,n) = 1$ is not yet used

Now, assume that $ax \equiv b \pmod{n}$ has a solution say $\beta \in \mathbb{Z}$.

Then, $n \mid a\beta - b \Rightarrow m \left(\frac{a}{m}\beta - \frac{b}{m} \right)$

Observe that, $m \mid a$ & $(a,n) = 1$.

$\therefore (n, m) = 1$.

Then $n \mid \frac{a}{m}\beta - \frac{b}{m}$

$\Rightarrow a'x \equiv b' \pmod{n}$ has a solution.

Thus, a solution to $ax \equiv b \pmod{n}$ gives a solution to $a'x \equiv b' \pmod{n}$

Solve: Find all solutions of $12x \equiv 18 \pmod{22}$

Step 1: $d = (12, 22) = 2$.

$2 \mid 18 \Rightarrow$ we have a solution.

Two solutions will be there since $d = 2$.

x_0 & $x_0 + 11$, modulo 22.

Step 2: Solve $6x \equiv 9 \pmod{11}$

Now, $d = (6,9) = 3$ & $(6,11) = 1$.

Step 3: Solve $2x \equiv 3 \pmod{11}$ [By lemma 4]

Multiply by 6,

$$6 \times 2x \equiv 6 \times 3 \pmod{11}$$

$$x \equiv 7 \pmod{11}$$

Thus 7 and $7 + 11 = 18$ are the solutions modulo 22.

Algorithm:

Step 1: Check if $d = (a,n)$ divides b. $\Rightarrow$ d-solutions.

Step 2: Solve for $(a/d)x \equiv b/d \pmod{n/d}$

$\left(\frac{a}{d}, \frac{n}{d}\right) = 1 \Rightarrow$ unique solution.

Step 3: Seek whether we can reduce the coefficient of x further.

$$\frac{a}{m}x \equiv \frac{b}{m}x \pmod{n} \Rightarrow ax \equiv b \pmod{n}$$

[By lemm 4]

Solve : Find all solutions of $18x \equiv 42 \pmod{50}$

Step 1: $d = (18, 50) = 2$.

$2 \mid 42 \Rightarrow$ There exists 2 solutions modulo 50.

i.e x_0, $x_0 + 25$.

Step 2: Solve $9x \equiv 21 \pmod{25}$

$d = (9, 25) = 1$

but $(9, 21) = 3$.

Step 3: Solve $3x \equiv 7 \pmod{25}$

$d = (3, 25) = 1$ and $(3, 7) = 1$.

Solve $3x \equiv 7 \pmod{25}$

$3x \equiv 32 \pmod{25}$ because $7 + 25 = 32$.

$3x \equiv 57 \pmod{25}$ $\quad 32 + 25 = 57$.

now, $d = (3, 57) = 3$.

$x \equiv 19 \pmod{25}$

Solutions : 19 and $19 + 25 = 44$.

$(a, n) = (a, b) = 1$.

Add multiples of n to b to obtain some $b' = bn + k$ such that $(a, b') > 1$