System of linear congruence

Theorem 1: Let a, b, c, d, e, f and m be integers with $m > 0$ such that $\gcd(\Delta, m) = 1$, where $\Delta = ad - bc$. Then the system of congurences

$$ax + by \equiv e \pmod{m}$$
$$cx + dy \equiv f \pmod{m}$$

Has exactly one solution modulo m with $x = \overline{\Delta}(de - bf) \pmod{m}$ and $y = \overline{\Delta}(af - ce) \pmod{m}$.

Example: find the solution of the following system of linear congruence:

$$x + 2y \equiv 1 \pmod{5}$$
$$2x + y \equiv 1 \pmod{5}$$

Definition 1: Let $A = (a_{ij})$ and $B = (b_{ij})$ be n x k matrices with integer entries. Then ***A*** is called congruence to ***B*** modulo m if $a_{ij} \equiv b_{ij} \pmod{m}, \forall i, j$

and we write $A \equiv B \pmod{m}$

Example:

$$\begin{bmatrix} 15 & 3 \\ 8 & 12 \end{bmatrix} \equiv \begin{bmatrix} 4 & 14 \\ -3 & 1 \end{bmatrix} \text{(mod 11)} \equiv \begin{bmatrix} 4 & 3 \\ -3 & 1 \end{bmatrix} \pmod{11}.$$

Definition 2: let ***A*** and $\overline{A}$ be n x n matrices of integers. If $\overline{A}A \equiv A\underline{A} \equiv I \pmod{m}$, then $\overline{A}$ is called the inverse of A modulo m.

Example:

$$\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}\begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{5} \text{ and } \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{5}$$

We call that $\begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix}$ is the inverse of $\begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix}$ modulo 5.

Theorem 2: Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be matrix of integers with $\gcd(\Delta, m) = 1$, $\Delta = ad - bc$, then

$\overline{A} = \overline{\Delta}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ is the inverse of matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $\overline{\Delta}$ is the inverse of $\Delta (\bmod m)$.

Example:

$A = \begin{bmatrix} 3 & 4 \\ 2 & 5 \end{bmatrix}$, and $\Delta = ad - bc = 15 - 8 = 7$. We know that 2 is inverse of 7 modulo 13, then

$\overline{A} = \overline{\Delta}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \equiv 2\begin{bmatrix} 5 & -4 \\ -2 & 3 \end{bmatrix} \equiv \begin{bmatrix} 10 & -8 \\ -4 & 6 \end{bmatrix} \equiv \begin{bmatrix} 10 & 5 \\ 9 & 6 \end{bmatrix} (\bmod 13)$.

Note:

We can find inverse of a matrix using adjoint matrix or elementary row operation to the matrix.

Problems:

Find solution of the following system of linear congruence:

FERMAT AND WILSON THEOREMS

Theorem 1: If gcd(a, m) = 1, then the least residuals modulo m for sequence :

a, 2a, 3a, …, (m-1)a is the permutation of 1, 2, 3, …, m-1.

Example 1: Given a = 4 and m = 9 and gcd(4, 9) = 1, then the least residuals modulo 9 for sequence : 4, 2(4), 3(4), 4(4), 5(4), 6(4), 7(4), 8(4) is a permutation of 1, 2, 3, 4, 5, 6, 7, 8.

Check that 4 $\equiv$4 mod 9), 2(4) $\equiv$ 8 (mod 9), 3(4) = 12 $\equiv$3 (mod 9), 4(4) = 16 $\equiv$ 7 (mod 9), 5(4) = 20 $\equiv$2 (mod 9), 6(4) = 24 $\equiv$6 (mod 9), 7(4) = 28 $\equiv$1 (mod 9), 8(4) = 32 $\equiv$5 (mod 9).

Theorem 2: (Fermat Theorem) If p is prime integer and gcd (a, p) = 1, then $a^{p-1} \equiv 1 (\text{mod } p)$.

Example 2: take p = 5 and a = 9, then using Fermat theorem, $9^{5-1} = 9^4 \equiv 1 (\text{mod } 5)$.

Theorem 3: If p is prime integer , then $a^p \equiv a (\text{mod } p)$ for every integer a.

Example 3: Take p = 5 and a = 20, then $20^5 \equiv 20 (\text{mod } 5)$.

The converse of theorem 3 is

If $a^p \not\equiv a (\text{mod } p)$ for an integer a, then p is not prime integer.

Example 4: Is integer 117 prime?

Check: take a = 2, then $2^{117} = 2^{7.16+5}$ and $2^7 = 128 \equiv 11 (\text{mod} 117)$,
$2^{117} = 2^{7.16+5} \equiv (11)^{16} 2^5 \text{ mod}(117) \equiv 44 (\text{mod} 117) \not\equiv 2 (\text{mod} 117)$, so 117 is not prime.

Theorem 4: If p and q are difference prime integers such that $a^p \equiv a (\text{mod } q)$ and $a^q \equiv a (\text{mod } p)$, then $a^{pq} \equiv a (\text{mod } pq)$.

Example 5: Find the remainder if 2^{340} is divided by 341?

Answer: 341 = 11.31, take p = 11 and q = 31

$2^{10} = 1024 = 31.33 + 1 \equiv 1 (\text{mod } 31)$, then $2^{11} \equiv 2 (\text{mod } 31)$

$2^{10} = 1024 = 11.93 + 1 \equiv 1 (\text{mod } 11)$, then $2^{31} = 2^{10.3+1} \equiv 2 (\text{mod } 11)$.

Using Theorem 4: $2^{341} \equiv 2^{11(31)} \equiv 2 (\text{mod } 11.31) = 2 (\text{mod } 341)$

Because gcd (2, 341) = 1, then $2^{340} \equiv 1 (\text{mod } 341)$ so the remainder if 2^{340} is divided by 341 is 1.

Theorem 5: If p is prime integer, then the congruence $x^2 \equiv 1 (\bmod\ p)$ has exactly two solutions that are 1 and p-1.

Example 6: The solution of $x^2 \equiv 1 (\bmod 11)$ are 1 and 10.

Theorem 6: If p is odd prime integer and a^{-1} is solution of $ax \equiv 1 (\bmod\ p)$ with a = 1, 2, …, p-1, then

(i). If $a \not\equiv b (\bmod\ p)$, then $a^{-1} \not\equiv b^{-1} (\bmod\ p)$.

(ii). If a = 1 or a = p-1 then $a^{-1} \equiv a (\bmod\ p)$.

Example 7: Take p= 7, then using Theorem 6, $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$, $6^{-1} = 6$.

We know that (i). If $a \not\equiv b (\bmod 7)$, then $a^{-1} \not\equiv b^{-1} (\bmod 7)$.

(ii). If a = 1 or a = p-1 = 6, then $a^{-1} \equiv a (\bmod 7)$.

Theorem 7 (Wilson Theorem): If p is prime integer, then $(p-1)! \equiv -1 (\bmod\ p)$.

Example 8: $10! \equiv -1 (\bmod 11)$.

Converse of Theorem 7 is true:

If $(p-1)! \equiv -1 (\bmod\ p)$, then p is prime integer.

Theorem 8: p is prime integer if and only if $(p-1)! \equiv -1 (\bmod\ p)$**.**

Theorem 9: If p is odd prime integer, then the congruence $x^2 + 1 \equiv 0 (\bmod\ p)$ has solution if and only if $p \equiv 1 (\bmod 4)$**.**

If p is odd prime integer and the congruence $x^2 + 1 \equiv 0 (\bmod\ p)$ has solution , then the solutions is $\left(\frac{p-1}{2}\right)!$ (mod p) and $\left(p - \left(\frac{p-1}{2}\right)!\right) (\bmod\ p)$**.**

Example 9: Does the congruence $x^2 + 1 \equiv 0 (\bmod 17)$ have solution?

Answer: because $17 \equiv 1 (\bmod 4)$, then the congruence has solution and the solutions are $\left(\frac{17-1}{2}\right)! = 8!$**=** 13 (mod 17) and 17-13 = 4 (mod 17).

Discussions:

1. Find the remainder if 314^{159} is divided by 7.

2. Find the remainder if 314^{162} is divided by 163.

3. Determine the last two digits of 7^{355}.

4. If gcd(a, 35) = 1, show that $a^{12} \equiv 1 (\mathrm{mod}\, 35)$.

5. Show that $a^{21} \equiv a (\mathrm{mod}\, 15)$ for every integer a.

6. Find the remainder if 15! Is divided by 17.

7. Prove that $2(p-3)!+1 \equiv 0 (\mathrm{mod}\, p)$ for every prime integer $p \geq 5$.

8. Find the remainder if 2(26!) is divided by 29.

9. If p is odd prime, then $2p \mid (2^{2p-1} - 2)$.

10. Find the solution of $x^2 \equiv -1 (\mathrm{mod}\, 29)$.

11. If a and b are integers that are not divisible by prime p, prove that if $a^p \equiv b^p (\mathrm{mod}\, p)$, then $a \equiv b (\mathrm{mod}\, p)$.

12. Prove that if p is odd prime, then $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 (\mathrm{mod}\, p)$.

13. Using problem 12, find the remainder if $1^6 + 2^6 + 3^6 + 4^6 + 5^6 + 6^6$ is divided by 7.