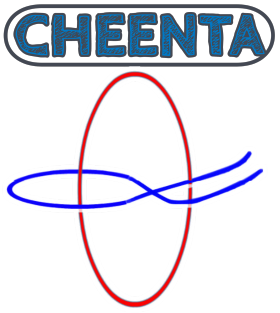

Cheenta

IOQM Concepts Revisited

Created By :
J V Raghunath

Topic : Linear Congruences - CRT, FLT

Overview

We will learn about,

1. Linear Congruences
2. System of Linear Congruences and CRT
3. Fermat's Little Theorem - FLT

1 Linear Congruences

A Linear Congruence equation is of the form,
$ax \equiv b \pmod{n}$, for $a, b, x \in \mathbb{Z}$ and $n \in \mathbb{N}$, where x is the variable.
x_0 is a solution $\iff ax_0 \equiv b \pmod{n}$. We say that two solutions are "equal" if both are congruent (mod n). For example, $3x \equiv 9 \pmod{12}$, has solutions, $x = \ldots, -5, -1, 3, 7, 11, 15, 19, \ldots$. But many of which are "equal" (mod 12), i.e., $-5 \equiv 7 \equiv 19 \pmod{12}$. So we say that the number of solutions to be the cardinality of set of all mutually incongruent solutions (mod 12), that is, $3x \equiv 9 \pmod{12}$, has 3 mutually incongruent solutions $\{3, 7, 11\} \pmod{12}$.

Theorem 1.1. *The Linear Congruence* $ax \equiv b \pmod{n}$ *has a solution* $\iff d \mid b$, *where* $d = \text{GCD}(a, n)$. *If* $d \mid b$, *then it has "d" mutually incongruent solutions* (mod n).

Proof. If $ax \equiv b \pmod{n} \implies n \mid ax - b \implies b = ax - nk$, for some $k \in \mathbb{Z}$. Since $\text{GCD}(a, n)$ divides both $a, n \implies \text{GCD}(a, n) \mid ax - nk \implies d \mid b$.

Conversely suppose if, $d \mid b \implies b = sd$, for some $s \in \mathbb{Z}$. From the *Bezout's Lemma* we know that, there exist $w, y \in \mathbb{Z}$, such that, $d = \text{GCD}(a, n) = aw + ny \implies sd = a(sw) + n(sy) \implies n \mid b - a(w_0)$, for some $w_0 \in \mathbb{Z}$. So $aw_0 \equiv b \pmod{n}$, and hence there is a solution for the linear congruence.

Now, suppose $d \mid b$, then $b = ax_0 - nk_0$, for some $x_0, k_0 \in \mathbb{Z}$ by the preceding argument. Let us say that there is another solution x_1, so, $b = ax_1 - nk_1$, for some $x_1, k_1 \in \mathbb{Z}$. So, $ax_0 - nk_0 = ax_1 - nk_1 \implies a(x_0 - x_1) = n(k_0 - k_1)$. If $a = da_0, n = dn_0$, then $a_0(x_0 - x_1) = n_0(k_0 - k_1) \implies n_0 \mid a_0(x_0 - x_1)$. By the *Euclid's Lemma*, since $\text{GCD}(\frac{a}{d}, \frac{n}{d}) = 1 \implies n_0 \mid (x_0 - x_1) \implies x_0 \equiv x_1 \pmod{n_0}$. Also note that conversely, any $x \equiv x_0 \pmod{n_0}$, is a solution of the congruence because $n_0 \mid (x - x_0) \implies n \mid ax - ax_0 \implies ax \equiv ax_0 \equiv b \pmod{n}$. Hence, the set of solutions of the linear congruence $ax \equiv b \pmod{n}$ is the set $\{x \mid x \equiv x_0 \pmod{n_0}\}$. But to determine the number of solutions, we need the number of incongruent

solutions (mod n). We know that,

$$x = \ldots,\ x_0,\ x_0 + \left(\frac{n}{d}\right),\ x_0 + 2\left(\frac{n}{d}\right),\ x_0 + 3\left(\frac{n}{d}\right), \cdots,\ x_0 + (d-2)\left(\frac{n}{d}\right),\ x_0 + (d-1)\left(\frac{n}{d}\right),$$
$$x_0 + n,\ x_0 + (d+1)\left(\frac{n}{d}\right), \ldots,\ \text{since } n_0 = \frac{n}{d}$$

So observe that, there are exactly "d" solutions that are mutually incongruent (mod n), completing the proof. □

Question 1.1. *Find the solutions and the number of solutions of the linear congruence,* $18x \equiv 30 \pmod{42}$
Sol. Note that $d = \text{GCD}(18, 42) = 6$; $a = 18$; $b = 30 \implies d \mid b$, so there is solution and the number of solutions $= d = 6$.
$18x \equiv 30 \pmod{42} \implies 3x \equiv 5 \pmod{7} \implies 3x \equiv 12 \pmod{7} \implies x \equiv 4 \pmod{7}$, is the set of solutions.

Question 1.2. *Find the solutions and the number of solutions of the linear congruence,* $9x \equiv 21 \pmod{30}$
Sol. Note that $d = \text{GCD}(9, 30) = 3$; $a = 9$; $b = 21 \implies d \mid b$, so there is solution and the number of solutions $= d = 3$.
$9x \equiv 21 \pmod{30} \implies 3x \equiv 7 \pmod{10} \implies 3x \equiv -3 \pmod{10} \implies x \equiv 9 \pmod{10}$, is the set of solutions.

2 System of Linear Congruences and CRT

Instead of one congruence equation, suppose you are given with multiple, say r simultaneous system of congruence equations and we are interested to find the solutions and the number of solutions for it. Suppose the congruence equations are,

$$\begin{aligned} b_1 x &\equiv c_1 \pmod{m_1} \\ b_2 x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ b_r x &\equiv c_r \pmod{m_r} \end{aligned}$$

where $m_1, m_2, \ldots, m_r$ are mutually coprime. Obviously, each of the congruence must hold true, otherwise there is no solution, and by the Theorem 1.1, we have $\text{GCD}(b_i, m_i) \mid c_i$, for each $i \in \{1, 2, \ldots, r\}$. If this is true, then we have solutions for

each congruence written as below,

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

where $n_i = \frac{m_i}{\text{GCD}(b_i, m_i)}$, which are also mutually co-prime $\forall i \in \{1, \ldots, r\}$ since m_i's are mutually coprime. Now we use the following *Chinese Remainder Theorem*, to understand more about this,

Theorem 2.1 (Chinese Remainder Theorem)**.** *Let $n_1, n_2, \ldots, n_r \in \mathbb{Z}$ such that* $\text{GCD}\,(n_i, n_j) = 1$ *for $i \neq j$. Then the system of linear congruences,*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Proof. We start by forming the product $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \ldots, r$, let

$$N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$$

In words, N_k is the product of all the integers n_i with the factor n_k omitted. By hypothesis, the n_i are relatively prime in pairs, so that $\gcd\,(N_k, n_k) = 1$. According to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 \pmod{n_k}$; call the unique solution x_k. Our aim is to prove that the integer

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

is a simultaneous solution of the given system. First, observe that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, because $n_k \mid N_i$ in this case. The result is

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 \pmod{n_k}$, which forces

$$\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}$$

This shows that a solution to the given system of congruences exists. As for the uniqueness assertion, suppose that x' is any other integer that satisfies these congruences. Then

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

and so $n_k \mid \bar{x} - x'$ for each value of k. Because $\gcd(n_i, n_j) = 1$,
$\implies n_1 n_2 \cdots n_r \mid \bar{x} - x'$; hence $\bar{x} \equiv x' \pmod{n_k}$, completing the proof. □

Question 2.1. *Solve the linear congruence* $17x \equiv 9 \pmod{276}$
Sol. $276 = 2^2 \times 3 \times 23$. So,
$276 \mid 17x - 9 \iff 2^2 \mid 17x - 9$ and $3 \mid 17x - 9$ and $23 \mid 17x - 9$, since these factors are relatively coprime. Hence, we just need to solve the simultaneous system of congruences,

$$17x \equiv 9 \pmod{4}$$
$$17x \equiv 9 \pmod{3}$$
$$17x \equiv 9 \pmod{23}$$

Firstly, let us solve each of the congruences and after some calculations we get,

$$x \equiv 1 \pmod{4}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 10 \pmod{23}$$

Now, we know by the *Chinese Remainder Theorem* that there is a unique solution $\pmod{276 = 4 \times 3 \times 23}$. We just need to find this unique solution and we are done. For this, list down the numbers that are congruent to $10 \pmod{23}$ and < 276, that is, $10, 33, 56, 79, \ldots$. Out these numbers, exactly one satisfy the system of congruences which is 33. Hence $x \equiv 33 \pmod{276}$ is the set of solutions.

Question 2.2. *Solve the following system of linear congruences,*

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

It is easily observed that $x \equiv 23 \pmod{105}$ is the solution. A rigorous solution would be to find the solution using the proof of the *Chinese Remainder Theorem.*

Remark. Think about the simultaneous system of congruences when the n_i's are not mutually coprime. Under what conditions do they have solution(s) and how many solution(s)?

3 Fermat's Little Theorem - FLT

Theorem 3.1 (Fermat's Little Theorem)**.** *Let $a \in \mathbb{Z}$ and p be any prime number, then*

$$a^p \equiv a \pmod p$$

Proof. We can use induction to prove it, i.e., $1^p \equiv 1 \pmod p$. Suppose, $a^p \equiv a \pmod p$, then $(a+1)^p = a^p + pk_1 + 1^p$, for some $k_1 \in \mathbb{Z}$, by the *Binomial Theorem.* Then, $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod p$, by the induction hypothesis. Hence, $a^p \equiv a \pmod p, \forall a \in \mathbb{Z}$ by the *First principle of Finite Induction.*

There is as well another elegant method, which states that if $\text{GCD}(a,p) \neq 1 \implies p \mid a \implies a^p \equiv 0 \equiv a \pmod p$. If $\text{GCD}(a,p) = 1$, then we can divide by a on both sides to get, $a^{p-1} \equiv 1 \pmod p$. Consider the set $\{a, 2\cdot a, 3\cdot a, \ldots, (p-1)\cdot a\}$, which is special because none of them is divisible by p and no two of them are congruent $\pmod p$, because if $n_1 \cdot a \equiv n_2 \cdot a \pmod p \implies p \mid (n_1 - n_2)$, since $\text{GCD}(a,p) = 1$, but this not possible unless $n_1 = n_2$, because $n_i < p$. So, we can observe that the remainder set of $\{a, 2\cdot a, 3\cdot a, \ldots, (p-1)\cdot a\}$ must be $\{1, 2, 3, \ldots, p-1\}$, in some order. Hence, $(a)\cdot(2a)\cdot(3a)\cdots((p-1)a) \equiv 1\cdot 2\cdot 3\cdots(p-1) \pmod p \implies (p-1)!\cdot a^{p-1} \equiv (p-1)! \pmod p \implies a^{p-1} \equiv 1 \pmod p$. □

Question 3.1. *Prove that* 17 *divides* $11^{104}+1$
Sol. $11^{17} \equiv 11 \pmod{17}$, by the *Fermat's Little Theorem*. So, $(11^{17})^5 \equiv 11^5 \pmod{17} \implies 11^{105} \equiv 11^5 \pmod{17} \implies 11^{104} \equiv 11^4 \equiv (-6)^4 \equiv 36^2 \equiv 4^2 \equiv -1 \pmod{17}$. Hence $17 \mid 11^{104}+1$

One can also use the *Fermat's Little Theorem* to prove that a number is not a prime. For example, Let us prove that 117 is not a prime,

$$2^{117} = 2^{7\cdot 16+5} = \left(2^7\right)^{16} 2^5$$

and $2^7 = 128 \equiv 11 \pmod{117}$, we have

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}$$

But $2^{21} = (2^7)^3$, which leads to

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}$$

Combining these congruences, we finally obtain

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}$$

So, 117 doesnot follow the *Fermat's Little Theorem* and hence it cannot be a prime. Actually, $117 = 3^2 \times 13$.