Module-4: Modular Arithmetic
Introduction to Congruences, Linear Congruences, The Remainder theorem (statement only), Solving Polynomials, Linear Diophantine Equation, System of Linear Congruences. Euler's Theorem (statement only), Wilson's Theorem (statement only) and Fermat's little theorem (statement only). Applications of Congruences-RSA algorithm **Self-Study**: Divisibility, GCD, Properties of Prime Numbers, Fundamental theorem of Arithmetic. **Applications of ordinary differential equations**: Cryptography, encoding and decoding, RSA applications in public key encryption. (**RBT Levels: L1, L2 and L3**)

Module-4: Modular Arithmetic

T1-Self Study: Self Study: Divisibility, GCD, Properties of Prime Numbers, Fundamental theorem of Arithmetic.

Self-Study: (Page no: 1 to 4)

Division Algorithm: For any two given integers a, b with $b \geq 0$, there exist unique integers q and r such that $a = qb + r, \quad 0 \leq r < b$.

That is, q is the quotient r reminder when you divide a by b .

$$\begin{array}{r|l} b & a \\ & bq \\ \hline & r \end{array}$$

Examples:

1. $a = 37, \ b = 7,$

$37 = 5 \times 7 + 2$

$$\begin{array}{r|l} 7 & 37 \\ & 35 \\ \hline & 2 \end{array}$$

2. $a = -33, \ b = 5$

$-33 = -7 \times 5 + 2$

$$\begin{array}{r|l} 5 & -33 \\ & -35 \\ \hline & 2 \end{array}$$

Clearly if $b = 2$, either $r = 0$ or $r = 1$.

Then integer of the form $a = 2q$ is called even, and $a = 2q + 1$ is called odd.

Use the division algorithm to establish

i) Every odd integer is either of the form $4k+1$ or $4k+3$.
ii) Square of any integer is either of the form $3k$ or $3k+1$.
iii) Cube of any integer is either of the form $9k$, $9k+1$ or $9k+8$.

Proof: i) Let a be any odd integer. Then $a = 2q+1$ for some integer q.

Here q maybe even or odd.

If q is even, then $q = 2k$ for some integer k.

$\Rightarrow \quad a = 2(2k)+1 = 4k+1.$

If q is odd, then $q = 2k+1$ for some integer k.

$\Rightarrow \quad a = 2(2k+1)+1 = 4k+3.$

ii) Square of any integer is either of the form $3k$ or $3k+1$.

If the divisor $b = 3$, reminder $r = 0,1$ or 2.

Therefore any integer a can be written as $a = 3q$, $a = 3q+1$ or $a = 3q+2$.

Then, $a^2 = (3q)^2 = 3(3q^2) = 3k.$

$a^2 = (3q+1)^2 = 9q^2+6q+1 = 3(3q^2+2q)+1 = 3k+1.$

Or $a^2 = (3q+2)^2 = 9q^2+12q+4 = 3(3q^2+4q+1)+1 = 3k+1.$

Therefore square of any integer is either of the form $3k$ or $3k+1$.

iii) Cube of any integer is either of the form $9k$, $9k+1$ or $9k+8$.

If the divisor $b = 3$, reminder $r = 0,1$ or 2.

Therefore any integer a can be written as $a = 3q$, $a = 3q+1$ or $a = 3q+2$.

$\Rightarrow \quad a^3 = (3q)^3 = 9(3q^3) = 9k.$

$a^3 = (3q+1)^3 = 9(3q^3)+9(3q^2)+9q+1 = 9(3q^3+3q^2+q)+1 = 9k+1.$

Or, $a^3 = (3q+2)^3 = 9(3q^3)+9(6q^2)+9(2q)+8$

$= 9(3q^3+6q^2+2q)+8 = 9k+8.$

Therefore cube of any integer is either of the form $9k$, $9k+1$ or $9k+8$.

Corollary: If a and b be any integers with $b \neq 0$, then there exists unique integers q and r such that $a = qb + r$, $0 \leq r < |b|$.

Divisibility: An integer b is said to be divisible by $a \neq 0$, (or a is said to be divisor of b)
If $b = ka$ for some integer k, and is denoted by $a|b$.

$a|b$ means a is a divisor of b, a is a factor of b or b is a multiple of a.
$a \nmid b$ indicate b is not divisible by a.

Theorems: For any three integers a, b and c,

i) $a|0$, $1|a$ and $a|a$ for $a \neq 0$.
ii) $a|1$ iff $a = \pm 1$.

iii) If $a|b$ and $c|d$ then $ac|bd$.
iv) If $a|b$ and $b|c$ then $a|c$.
v) $a|b$ and $b|a$ iff $a = \pm b$.
vi) If $a|b$ and $b \neq 0$ then $|a| \leq |b|$.
vii) If $a|b$ and $a|c$ then $a|(bx + cy)$.

Zero is not the divisor of any integer, but any nonzero integer is divisor of zero.

Common Divisors: Let a and b are any two integers, an integer d is said to be common divisor of a and b if both $d|a$ and $d|b$.

Greatest Common Divisor: Let a and b are any two integers with at least one of them is nonzero. The greatest common divisor of a and b denoted by $\gcd(a, b)$ is the positive integer d satisfying

1) $d|a$ and $d|b$.
2) If $c|a$ and $c|b$ then $c \leq d$.

That is among the common divisors greatest one.

Theorem: For the given integers a and b with at least one of them is nonzero there exist two integers x, y such that $\gcd(a, b) = ax + by$.

Prime: An integer $p > 1$ is called prime number, if only the positive divisors of p are $1, p$.

Theorem: If p is prime and $p|ab$, then $p|a$ or $p|b$.

Relatively prime: Two integers a and b with at least one of them is nonzero are said to be relatively prime If $\gcd(a, b) = 1$.

Theorem: Two integers a and b with at least one of them is nonzero are said to be relatively prime Iff there exist integers x, y such that $1 = ax + by$.

Corollary: If $\gcd(a, b) = d$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Note: If $a|c$ and $b|c$ with $\gcd(a, b) = 1$, then $ab|c$.

Theorem (Euclid's Lemma): If $a|bc$ with $\gcd(a, b) = 1$ then $a|c$.

Theorem: Let a and b are two integers with at least one of them is nonzero, a positive integer $d = \gcd(a, b)$ if and only if, 1) $d|a$ and $d|b$ and 2) If $c|a$ and $c|b$ then $c|d$.

That is any common divisor divides the greatest common divisor.

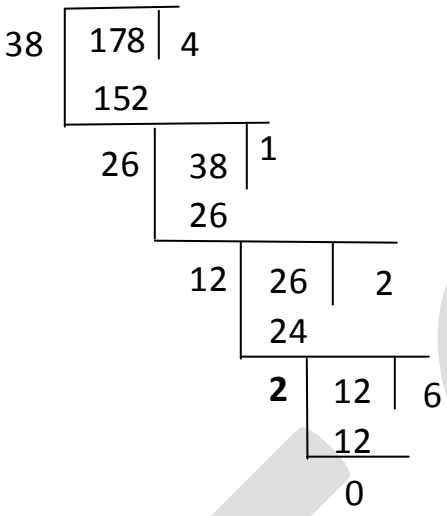
The Euclidean Algorithm:

If $a = qb + r$, with $0 < r < b$, then $\gcd(a, b) = \gcd(b, r)$
Let a and b are two integers with at least one of them is nonzero.
Since $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$, assume that $a \geq b > 0$.

By the division algorithm find q_1 and r_1 . $a = q_1 b + r_1$, where $0 \leq r_1 < b$.
If $r_1 = 0$, then $\gcd(a, b) = b$.
If $r_1 \neq 0$, then find q_2 and r_2 . $b = q_2 r_1 + r_2$, where $0 \leq r_2 < r_1$.
If $r_2 = 0$, then $\gcd(a, b) = r_1$.
If $r_2 \neq 0$, then find q_3 and r_3 . $r_1 = q_3 r_2 + r_3$, where $0 \leq r_3 < r_2$.

Continuing like this until zero remainder obtained.
Let $r_n = 0$, then $\gcd(a,\ b) = r_{n-1}$.

Example: Find the $\gcd(38, 178)$, and express as linear combination of 38 and 178.



$26 = 178 - (4)38$

$12 = 38 - (1)26$

$2 = 26 - (2)12$

Theorem: $\gcd(ka,\ kb) = k.\gcd(a,\ b)$, for any positive integer k.

Example: $\gcd(12,\ 30) = 6.\gcd(2,\ 5) = 6$.

Least common multiple: $\text{lcm}(a,\ b)$ is a positive integer m satisfying
1) $a|m$ and $b|m$.
2) If $a|c$ and $b|c$ then $m|c$.

Note:
1) $\gcd(a,\ b) \times \text{lcm}(a,\ b) = ab$.
2) $\gcd(a,\ b) = \text{lcm}(a,\ b)$ if and only if $a = b$. where a and b are nonzero integers.
3) If $\gcd(a,\ b) = 1$ and $a|c$ and $b|c$ then $ab|c$.

Fundamental Theorem of Arithmetic: Every positive integer n is a prime or a product of primes, and n can be represented uniquely in a canonical form.

That is $n = p_1^{k_1} p_2^{k_2} \cdots\cdots p_r^{k_r}$, where k_i's are positive integers, and p_i's are primes with $p_1 < p_2 < \cdots < p_r$.

Examples: $360 = 2^3 \times 3^2 \times 5$, $4725 = 3^3 \times 5^2 \times 7$.

L1- Linear Diophantine Equation Linear Congruences

Recall:

1. Define the Greatest Common Divisor (GCD) of two integers a and b.
2. If GCD(a,b)=1, what can you say about a and b?
3. What is the Euclidean Algorithm? Why does it work?
4. What is the GCD , If two integers are co-prime?

Linear Diophantine equations in two unknown: $ax + by = c$, where a, b, c are given integers with at least one of the a and b is nonzero.

Let x_0 , y_0 are integers such that $ax_0 + by_0 = c$ then $x = x_0 t$, $y = y_0 t$ is a particular solution.

Theorem: Linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = \gcd(a,b)$.

Let x_0 , y_0 is any particular solution, then all other solutions are given by

$x = x_0 + \left(\frac{b}{d}\right)t$, $y = y_0 - \left(\frac{a}{d}\right)t$ for any integer t.

Example: 1. Solve linear Diophantine equation $172x + 20y = 1000$. Find the positive solution.

First find the $\gcd(172, 20)$ by Euclidean algorithm.

$$\begin{array}{r|l|l} 20 & 172 & 8 \\ & 160 & \\ \hline 12 & 20 & 1 \\ & 12 & \\ \hline 8 & 12 & 1 \\ & 8 & \\ \hline \mathbf{4} & 8 & 2 \\ & 8 & \\ \hline & 0 & \end{array}$$

$$12 = 172 - (8)20$$
$$8 = 20 - (1)12$$
$$4 = 12 - (1)8 \qquad (1)12]$$
$$= (2)12 - (1)20$$
$$= (2)[172 - (8)20] - (1)20$$
$$= (2)172 + (-17)20$$

$\gcd(172, 20) = 4$. Since $4|1000$, solution to this equation exists.

$$4 = (2)172 + (-17)20$$

Multiplying by 250 we get, $1000 = (500)172 + (-4250)20$.

Therefore one of the solution is $x_0 = 500$, $y_0 = -4250$.

All other solutions are expressed by $x = 500 + 5t$, $y = -4250 - 43t$ for any integer .

If the required solution is positive, then $500 + 5t > 0$ and $-4250 - 43t > 0$.

$\Longrightarrow -100 < t < -98.837$. $\therefore t = -99$.

$\Longrightarrow x = 5$, $y = 7$. This is the only positive solution of the given equation.

2. A customer bought a dozen pieces of fruit, apples and oranges for 132 Rs. If an apple costs 3 Rs more than an orange and more apples than oranges were purchased, how many pieces of each kind were bought?

Solution: Let x be the number of apples, and y be the cost of an apple.

Then the number of oranges is $12-x$, and cost of each orange is $y-3$.

Given that, $xy+(12-x)(y-3)=132$.

Or, $3x+12y=168$

$\Rightarrow x+4y=56$. Which is Diophantine equation.

$\gcd(1,\ 4)=1$, and $1=(-3)1+(1)4$

$56=(-168)1+(56)4$.

Clearly one of the solution is $x_0=-168,\ \ y_0=56$. All other solutions are expressed by $x=-168+4t,\ \ y=56-t$ for any integer t .

Since number of apples is more, $6<x\leq 12$.

$\Rightarrow\ 6<-168+4t\leq 12\ \ \Rightarrow 43.5<t\leq 45.$

$\therefore\ \ t=44,\ or\ \ 45.$

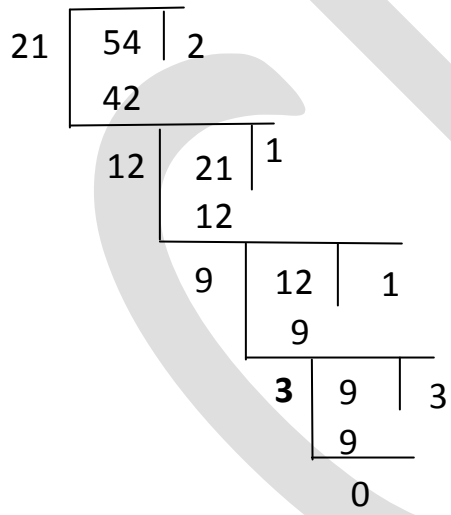
If $t=44,\ \ x=8,\ \ y=12$.

Number of apples is 8 with costs 12 Rs per piece, and 4 oranges with costs 9Rs per piece.

Or, If $t=45,\ \ x=12,\ \ y=11$.

Number of apples is 12 with costs 11 Rs per piece, and 0 oranges with costs 8Rs per piece.

3. Determine all positive solutions of $54x+21y=906$.



$12=54-(2)21$

$9=21-(1)12$

$3=12-(1)9$ $(1)12]$

$=(2)12-(1)21$

$=(2)[54-(2)21]-(1)21$

$=(2)54+(-5)21$

$\gcd(54,\ 21)=3$. Since $3|906$, solution to this equation exists.

$3=(2)54+(-5)21$

Multiplying by 302 we get, $906=(604)54+(-1510)21.$

Therefore one of the solution is $x_0=604,\ \ y_0=-1510.$

All other solutions are expressed by $x=604+7t,\ \ y=-1510-18t$ for any integer.

If the required solution is positive, then $604+7t>0$ and $-1510-18t>0$.

$\Rightarrow -86.286<t<-83.889$. $\ \ \therefore t=-85,-84.$

$\Rightarrow \{x=9,\ \ y=20\}$ and $\{x=16,\ \ y=2\}$ are the two positive solutions of the given equation.

4. Ticket charges in a movie theater is 180 Rs for adult 75 Rs for children. Total collection on a particular show is 9000 Rs, assuming that more adults than children were present, how many people attended?

Solution: Let x and y be the number of adult and children respectively.

Given that, $180x + 75y = 9000$, with $x > y > 0$.

$$
\begin{array}{r|l|l}
75 & 180 & 2 \\
 & 150 & \\
\hline
30 & 75 & 2 \\
 & 60 & \\
\hline
\mathbf{15} & 30 & 2 \\
 & 30 & \\
\hline
 & 0 &
\end{array}
$$

$$
\begin{aligned}
15 &= 75 - (2)30 \\
&= 75 - (2)[180 - (2)75] \\
&= (-2)180 + (5)75
\end{aligned}
$$

Since $15|9000$, $15 = (-2)180 + (5)75$,

Multiplying by 600, we get $9000 = (-1200)180 + (3000)75$

All the solutions are $x = -1200 + 5t$, $y = 3000 - 12t$ for any integer t.

To find the nonnegative solutions with $x > y$,

$-1200 + 5t \geq 0$,$3000 - 12t \geq 0$ and $-1200 + 5t > 3000 - 12t$.

$\Longrightarrow 247 < t \leq 250$.

$\therefore t = 248, 249, 250$.

t	x	y	Number of people attended
248	40	24	64
249	45	12	57
250	50	0	50

5. There are three idols of God on the bank of a river. An ascetic was worshiping idols. He has some flowers. He takes them and drowns them in the river. The flowers emerge doubled in number. He offers some of it to an idol. He again drowns remaining flowers in the river, the flowers again emerge doubled in number. He again offers some of it to another idol. He doubles the remaining flowers, and offers all of it to the third idol. How many flowers could he have taken at first if all the idols had to be offered the same number of flowers? How many flowers should be devoted to each idol?

Solution:

Let x be the number of flowers at first, and y be number of flowers offered to each idol.

After offering y flowers to the first idol, remaining flowers$(2x - y)$

After offering y flowers to the second idol, remaining flowers$(4x - 3y)$.

Finally he offers $8x - 6y = y$ flowers to the third idol.

Now the pattern is linear Diophantine equation, $8x + (-7)y = 0$.

Clearly $x_0 = 0$, $y_0 = 0$ is the one of the solution. Since $d = \gcd(8, 7) = 1$, other solutions are expressed by $x = x_0 + \left(\frac{b}{d}\right)t = -7t = 7k$, $y = y_0 - \left(\frac{a}{d}\right)t = -8t = 8k$. Where $k = 1, 2, 3, 4, \cdots\cdots$.

Theorem: Linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = \gcd(a, b)$.

If $a|c$ then all the solutions are, $x = \frac{c}{a} + \left(\frac{b}{d}\right)t$, $y = -\left(\frac{a}{d}\right)t$ for any integer t.

If $b|c$ then all the solutions are, $x = \left(\frac{b}{d}\right)t$, $y = \frac{c}{b} - \left(\frac{a}{d}\right)t$ for any integer t.

Example:

1. Solve linear Diophantine equation $172x + 20y = 1000$. Find the positive solution.

Solution: Since $d|c$ and $b|c$, $(4|1000\ ,\ 20|1000)$

All the solutions are $x = 5t$, $y = 50 - 43t$ for any integer t.

To find the positive solutions $5t > 0$ and $50 - 43t > 0 \Longrightarrow 0 < t < 1.16$. $\therefore t = 1$.

Hence the solution is $x = 5$, $y = 7$.

2. Determine all positive integer solutions of $30x + 17y = 300$.

Solution: Since $d|c$ and $a|c$, $(1|300\ ,\ 30|300)$

All the solutions are $x = 10 + 17t$, $y = -30t$ for any integer t.

To find the positive solutions $10 + 17t > 0$ and $-30t > 0 \Longrightarrow -0.588 < t < 0$.

Since there is no integer satisfying $-0.588 < t < 0$, there is no positive integer solution.

3. Ticket charges in a movie theater is 180 Rs for adult 75 Rs for children. Total collection on a particular show is 9000 Rs, assuming that more adults than children were present, how many people attended?

Solution: Let x and y be the number of adult and children respectively.

Given that, $180x + 75y = 9000$, with $x > y > 0$.

Solution: Since $d|c$ and $a|c$, $(15|300\ ,\ 180|9000)$

All the solutions are $x = 50 + 5t$, $y = -12t$ for any integer t.

To find the nonnegative solutions $50 + 5t \geq 0$ and $-12t \geq 0 \Longrightarrow -10 \leq t \leq 0$.

Since number of adults more $50 + 5t > -12t \Longrightarrow t > -2.941$

$\therefore t = -2, -1, 0$.

t	x	y	Number of people attended
-2	40	24	64
-1	45	12	57
0	50	0	50

Review:

1. State the general form of a Linear Diophantine Equation.
2. What are the necessary conditions for a Linear Diophantine Equation $ax + by = c$ to have integer solutions?
3. Given $15x + 21y = 42$, determine whether the equation has integer solutions. If yes, find one solution.
4. If x_0, y_0 is a particular solution of $ax + by = c$, write the general solution.
5. How can you find the smallest positive solution for x and y in $ax + by = c$?

L2- Theory of Congruences , Linear congruence

Recall:

1. Explain how the greatest common divisor (GCD) plays a role in solving Linear Diophantine Equations.
2. Describe the steps to find the particular solution of $ax + by = c$.
3. What is a Linear Diophantine Equation? Give an example.
4. Solve the equation $12x + 18y = 6$ and find all integer solutions.
5. How do you determine if a Linear Diophantine Equation has a solution?

Theory of Congruence:

If n is a positive integer, we say that the integers a and b are **congruent** modulo n, and write $a \equiv b(\mathrm{mod} n)$), if they have the same remainder on division by n .

Let n be a fixed positive integer, two integers a and b are said to be congruent modulo n

If, $n|(a-b)$ (Or $a-b=kn$)

Denoted by $a \equiv b(\mathrm{mod}\, n)$ { a is congruent to b mod n}

Theorems: Let $n>0$ be fixed integer, a, b, c, d are any arbitrary integers. Then,

1. $a \equiv a(\mathrm{mod}\, n)$.
2. If $a \equiv b(\mathrm{mod}\, n)$, then $b \equiv a(\mathrm{mod}\, n)$.
3. If $a \equiv b(\mathrm{mod}\, n)$ and $b \equiv c(\mathrm{mod}\, n)$, then $a \equiv c(\mathrm{mod}\, n)$.
4. If $a \equiv b(\mathrm{mod}\, n)$ and $c \equiv d(\mathrm{mod}\, n)$, then $ac \equiv bd(\mathrm{mod}\, n)$.
5. If $a \equiv b(\mathrm{mod}\, n)$, then $a+c \equiv b+c(\mathrm{mod}\, n)$ and $ac \equiv bc(\mathrm{mod}\, n)$.

Note: $ac \equiv bc(\mathrm{mod}\, n) \nRightarrow a \equiv b(\mathrm{mod}\, n)$.

Theorem: If $\gcd(c,\ n)=d$ and $ac \equiv bc(\mathrm{mod}\, n)$, then $a \equiv b\left(mod\ \frac{n}{d}\right)$.

Corollory1: If $\gcd(c,\ n)=1$ and $ac \equiv bc(\mathrm{mod}\, n)$, then $a \equiv b(mod\, n)$.

Corollory2: If $ca \equiv cb(\mathrm{mod}\, p)$ and $p \nmid c$, where p is a prime number, then $a \equiv b(\mathrm{mod}\, p)$.

A familiar usage of modular arithmetic is whenever we convert between 12 and 24 hour clocks. We know that 14:00 and 2:00 pm indicate the same time since $14 \equiv 2 \bmod 12$.

Congruence class of modulo n: Let a and n be integers with $n>0$.

Congruence class $[a]=\{x \in \square \mid a \equiv x(mod\, n)\}$

$\square_n$ is the set of all congruence classes modulo n.

$\therefore$ $\square_n=\{[0],[1],[2]\cdots\cdots[n-1]\}$

Or simply $\square_n=\{0,1,2\cdots\cdots,n-1\}$

Multiplicative inverse of a with respect to multiplication modulo n is an integer $b \in \square_n$ such that $ab \equiv 1(\mathrm{mod}\, n)$.

Since $2\times 3 \equiv 1(mod\ 5)$ $(2^{-1})_{\otimes_5}=3$.

Inverse of 31 with respect to multiplication modulo 17 is 11.

Inverse of 13 with respect to the addition modulo 15 is 2.

Note: $a \equiv b(\mathrm{mod}\, 1)$ for any integers a and b.

Zero divisors: $ab \equiv 0(\mathrm{mod}\, n) \nRightarrow$ Either $a \equiv 0(\mathrm{mod}\, n)$ or $b \equiv 0(\mathrm{mod}\, n)$.

Example: $3\times 4 \equiv 0(\mathrm{mod}\, 12)$ but $3 \not\equiv 0(\mathrm{mod}\, 12)$ and $4 \not\equiv 0(\mathrm{mod}\, 12)$.

$\square_6$ has three zero divisors$\{2,3,4\}$. $\because$ $2\otimes_6 3=0$, $3\otimes_6 4=0$.

Note: If $ab \equiv 0(\mathrm{mod}\, n)$ and $\gcd(a,\ n)=1$, then $b \equiv 0(\mathrm{mod}\, n)$.

Problems:

1. Solve $5x \equiv 4(\mathrm{mod}\, 13)$.

   Solution: Since the multiplicative inverse of 5 is 8, multiplying by 8 we get,

   $40x \equiv 32(\mathrm{mod}\, 13)$

   Or $x \equiv 6(\mathrm{mod}\, 13)$.

2. Find a, if $2^8 \equiv a \pmod{13}$.

Solution: Since $2^6 \equiv -1 \pmod{13}$, $2^8 \equiv -4 \pmod{13}$.

Or $2^8 \equiv 9 \pmod{13}$

$\therefore a \equiv 9 \pmod{13}$.

3. Solve $7x \equiv 9 \pmod{15}$.

Solution: Multiplying by2 we get,

$14x \equiv 3 \pmod{15}$ and $14 \equiv -1 \pmod{15}$

Or $x \equiv -3 \pmod{15}$. $\therefore x \equiv 12 \pmod{15}$.

Linear congruence: An equation of the form $ax \equiv b \pmod{n}$ is called linear congruence.

Theorem: linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d|b$.

Where $d = \gcd(a, n)$.

If $d|b$ then there are d mutually incongruent solutions modulo n.

If x_0 is any solution of $ax \equiv b \pmod{n}$ and $d = \gcd(a, n)$, then d mutually incongruent solutions are $x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d},\ x_0 + \frac{3n}{d}, \cdots\cdots,\ x_0 + \frac{(d-1)n}{d}$.

Or, simply $x_0 + \frac{n}{d}t$, where $t = 0, 1, 2, 3 \cdots\cdots (d-1)$.

1. Solve $18x \equiv 30 \pmod{42}$.

Solution: $d = \gcd(a, n) = \gcd(18, 42) = 6$.

Since $6|30$, $(d|b)$ there are 6 incongruent solutions.

$18x \equiv 30 \pmod{42} \Longrightarrow 3x \equiv 5 \pmod{7}$

[If $\gcd(c, n) = d$ and $ac \equiv bc \pmod{n}$, then $a \equiv b \left(\mod \frac{n}{d}\right)$]

$3x \equiv 5 \pmod{7} \Longrightarrow 15x \equiv 25 \pmod{7} \Longrightarrow x \equiv 4 \pmod{7}$. $\frac{n}{d} = 7$.

Therefore six solutions are $x \equiv 4 + 7t \pmod{42}$, $t = 0, 1, 2, 3, 4, 5$.

$x \equiv 4,\ 11,\ 18,\ 25,\ 32,\ 39 \pmod{42}$

2. Solve $9x \equiv 21 \pmod{30}$

Solution: Clearly $d = \gcd(9, 30) = 3$ and $3|21$. There are 3 incongruent solutions

$9x \equiv 21 \pmod{30} \Longrightarrow 3x \equiv 7 \pmod{10} \Longrightarrow 21x \equiv 49 \pmod{10} \Longrightarrow x \equiv 9 \pmod{10}$

$\frac{n}{d} = 10$, $\therefore$ $x \equiv 9 + 10t \pmod{30}$, $t = 0, 1, 2$.

Three solutions are $x \equiv 9, 19, 29 \pmod{30}$.

3. Solve $7x \equiv 15 \pmod{17}$

Solution: Clearly $d = \gcd(7, 17) = 1$ and $1|15$. There is unique incongruent solution.

$7x \equiv 15 \pmod{17} \Longrightarrow 35x \equiv 75 \pmod{17}$

$\Longrightarrow x \equiv 7 \pmod{17}$

Review:

1. How does modular arithmetic differ from standard arithmetic?
2. State the general form of a Linear Congruence.
3. Under what condition does a Linear Congruence $ax \equiv b \pmod{m}$have solutions?
4. Explain the role of the GCD in solving Linear Congruences.

5. Solve: $3x \equiv 6 (\text{mod } 9)$.

L3- The Remainder theorem

Recall:

1. How do you reduce congruence to its simplest form?
2. Describe one real-world application of Linear Congruences.
3. What does it mean for $a \equiv b (\text{mod } m)$)?
4. Solve $4x \equiv 8 (\text{mod } 20)$., and state how many solutions exist.

Chinese reminder theorem: Let $n_1, n_2, n_3, \cdots\cdots n_r$ be positive integers such that, $\gcd(n_i, n_j) = 1, \text{for } i \neq j$. Then the system of linear congruences

$x \equiv a_1 (\text{mod } n_1)$, $x \equiv a_2 (\text{mod } n_2)$, $\cdots\cdots\cdots\cdots$, $x \equiv a_r (\text{mod } n_r)$ has a simultaneous solution, which is unique modulo $n_1 n_2 n_3 \cdots\cdots n_r$.

Method to find solution: Let $n = n_1 n_2 n_3 \cdots\cdots n_r$, $N_k = \frac{n}{n_k}$ for $k = 1, 2, 3, \cdots, r$.

Since $\gcd(n_i, n_j) = 1, \text{for } i \neq j$, $\gcd(N_k, n_k) = 1$.

Solve the congruence

$N_k x \equiv 1 (\text{mod } n_k)$ and unique solution be x_k for $k = 1, 2, 3, \cdots, r$.

Then $\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 + \cdots + a_r N_r x_r$ is a simultaneous solution of the given system.

Examples:

1. Solve the system of equations $x \equiv 2 (\text{mod } 3)$, $x \equiv 3 (\text{mod } 5)$, $x \equiv 2 (\text{mod } 7)$.

Clearly 3, 5, 7 relatively primes.

$n = n_1 n_2 n_3 = 105$, $N_1 = \frac{n}{n_1} = 35$, $N_2 = \frac{n}{n_2} = 21$, $N_3 = \frac{n}{n_3} = 15$.

Solve $N_k x \equiv 1 (\text{mod } n_k)$ $k = 1, 2, 3$.

$35x \equiv 1 (\text{mod } 3) \implies 2x \equiv 1 (\text{mod } 3) \implies x \equiv 2 (\text{mod } 3) \implies x_1 = 2.$

$21x \equiv 1 (\text{mod} 5) \implies x \equiv 1 (\text{mod} 5) \implies x_2 = 1.$

$15x \equiv 1 (\text{mod } 7) \implies x \equiv 1 (\text{mod } 7) \implies \implies x_3 = 1.$

$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 233.$

$233 \equiv 23 (\text{mod} 105).$

The solution is $x \equiv 23 (\text{mod} 105)$.

2. Solve the system of equations $4x \equiv 5 (\text{mod } 9)$, $2x \equiv 6 (\text{mod } 20)$.

$4x \equiv 5 (\text{mod } 9) \implies x \equiv 35 (\text{mod } 9)$. Or $x \equiv 8 (\text{mod } 9)$

$2x \equiv 6 (\text{mod } 20) \implies x \equiv 3 (\text{mod } 10) \implies x \equiv 3, 13 (\text{mod } 20)$.

Now consider $x \equiv 8 (\text{mod } 9)$ and $x \equiv 3 (\text{mod } 20)$.

$n = n_1 n_2 = 180$, $N_1 = 20$, $N_2 = 9$. $x_1 = 5$, $x_2 = 9$.

$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 = 8 \times 20 \times 5 + 3 \times 9 \times 9 = 1043.$

$x \equiv 143 (\text{mod} 180)$

Now consider $x \equiv 8 (\text{mod } 9)$ and $x \equiv 13 (\text{mod } 20)$.

$n = n_1 n_2 = 180,\ N_1 = 20,\ \ N_2 = 9.\ \ x_1 = 5,\ \ x_2 = 9.$

$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 = 8 \times 20 \times 5 + 13 \times 9 \times 9 = 1853.$

$x \equiv 53(\text{mod}180).$

Therefore Solutions are $x \equiv 53,\ 143(\text{mod}180)$

3. Solve $17x \equiv 9(\text{mod}276)$ using reminder theorem.

Solution: $276 = 3 \times 4 \times 23.$

$\Longrightarrow 17x \equiv 9(\text{mod}\ 3)\ ,\ \ 17x \equiv 9(\text{mod}\ 4)\ ,\ \ \ 17x \equiv 9(\text{mod}\ 23).$

Or $\ x \equiv 0(\text{mod}\ 3)\ ,\ \ \ \ x \equiv 1(\text{mod}\ 4)\ ,\ \ \ \ \ x \equiv 10(\text{mod}\ 23).$

$a_1 = 0,\ \ \ \ a_2 = 1,\ \ a_3 = 10$

Clearly 3, 4, 23 are relatively primes.

$n = n_1 n_2 n_3 = 276,\ \ \ N_1 = 92,\ \ N_2 = 69,\ \ \ \ N_3 = 12\ .$

$N_k x \equiv 1(\text{mod}\ n_k)\ k = 1,\ 2,\ 3.$

$92x \equiv 1(\text{mod}\ 3)\ \ \Longrightarrow x \equiv 2(\text{mod}\ 3)\ \Longrightarrow\ x_1 = 2.$

$69x \equiv 1(\text{mod}\ 4)\ \ \Longrightarrow\ \ x \equiv 1(\text{mod}\ 4)\ \ \Longrightarrow\ \ x_2 = 1.$

$12x \equiv 1(\text{mod}\ 23)\ \Longrightarrow\ \ x \equiv 2(\text{mod}\ 23) x_3 = 2.$

$\overline{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 0 + 1 \times 69 \times 1 + 10 \times 12 \times 2 = 309.$

$309 \equiv 33(\text{mod}276).$

The solution is $x \equiv 33(\text{mod}276).$

4. Solve $17x \equiv 9(\text{mod}276).$ (Not by reminder theorem)

Solution: $276 = 3 \times 4 \times 23.$

$\Longrightarrow 17x \equiv 9(\text{mod}\ 3)\ ,\ \ 17x \equiv 9(\text{mod}\ 4)\ ,\ \ \ 17x \equiv 9(\text{mod}\ 23).$

Or $\ x \equiv 0(\text{mod}\ 3)\ ,\ \ x \equiv 1(\text{mod}\ 4)\ ,\ \ \ 17x \equiv 9(mod\ 23).$

$x \equiv 0(\text{mod}\ 3) \Longrightarrow x = 3k.$

Put $x = 3k$ in $\ \ x \equiv 1(\text{mod}\ 4) \Longrightarrow 3k \equiv 1(\text{mod}\ 4)$

$\Longrightarrow k \equiv 3(\text{mod}\ 4)\ \Longrightarrow k = 4j + 3.$

$\therefore x = 3k = 12j + 9$

Put $x = 12j + 9$ in $\ 17x \equiv 9(\text{mod}\ 23) \Longrightarrow 17(12j + 9\ ) \equiv 9(\text{mod}\ 23)$

$\Longrightarrow 204j \equiv -144(\text{mod}\ 23)\ \ \Longrightarrow -3j \equiv -6(\text{mod}\ 23)\ \Longrightarrow j \equiv 2(\text{mod}\ 23).$

$\Longrightarrow j = 23t + 2.\ \ \therefore x = 12(23t + 2) + 9 = 33 + 276t\ .$

$\Longrightarrow\ \ x \equiv 33(\text{mod}276).$

5. Using congruence solve Diophantine equation $4x + 51y = 9.$

Solution: $4x + 51y = 9 \Longrightarrow 4x - 9 = -51y \Longrightarrow\ \ 4x \equiv 9(\text{mod}\ 51)$

$4x \equiv 9(\text{mod}\ 51)\ \Longrightarrow x \equiv 15(\text{mod}\ 51)\ \ \ $ (Multiplying by 13)

$\Longrightarrow x = 15 + 51t.$

$4x + 51y = 9 \Longrightarrow 51y - 9 = -4x \Longrightarrow\ \ 51y \equiv 9(\text{mod}\ 4)$

$51y \equiv 9(\text{mod}\ 4)\ \Longrightarrow 3y \equiv 1(\text{mod}\ 4)\ \Longrightarrow y \equiv 3(\text{mod}\ 4)$

$\Longrightarrow y = 3 + 4s.$

$4x + 51y = 9 \Longrightarrow 4(15 + 51t) + 51(3 + 4s) = 9$

$\Longrightarrow t + s = -1$ Or, $s = -(t + 1) \Longrightarrow y = -1 - 4t.$

Therefore solution is $x = 15 + 51t$, $y = -1 - 4t$.

6. Using remainder theorem find the remainder when 3^{302} is divided by 5005.

Solution: $5005 = 5 \times 7 \times 11 \times 13.$

$3^4 \equiv 1(\text{mod } 5) \Longrightarrow 3^{75\times4+2} \equiv 9(\text{mod } 5) \Longrightarrow 3^{302} \equiv 4(\text{mod } 5)$

$3^6 \equiv 1(\text{mod } 7) \Longrightarrow 3^{50\times6+2} \equiv 9(\text{mod } 7) \Longrightarrow 3^{302} \equiv 2(\text{mod } 7)$

$3^5 \equiv 1(\text{mod } 11) \Longrightarrow 3^{60\times5+2} \equiv 9(\text{mod } 11) \Longrightarrow 3^{302} \equiv 9(\text{mod}11)$

$3^3 \equiv 1(\text{mod } 13) \Longrightarrow 3^{100\times3+2} \equiv 9(\text{mod}13) \Longrightarrow 3^{302} \equiv 9(\text{mod } 13).$

$a_1 = 4, \quad a_2 = 2, \quad a_3 = 9, \quad a_4 = 9$

$n = 5005, \quad N_1 = 1001, \quad N_2 = 715, \quad N_3 = 455, \; N_4 = 385$

$N_k x \equiv 1(\text{mod } n_k)$, $k = 1, \; 2, \; 3, \; 4.$

$1001x \equiv 1(\text{mod } 5) \Longrightarrow x \equiv 1(\text{mod } 5) \Longrightarrow x_1 = 1.$

$715x \equiv 1(\text{mod } 7) \Longrightarrow x \equiv 1(\text{mod } 7) \Longrightarrow x_2 = 1.$

$455x \equiv 1(\text{mod } 11) \Longrightarrow 4x \equiv 1(\text{mod}11) \Longrightarrow x \equiv 3(\text{mod}11) \Longrightarrow x_3 = 3.$

$385x \equiv 1(\text{mod } 13) \Longrightarrow 8x \equiv 1(\text{mod}13) \Longrightarrow x \equiv 5(\text{mod}13) \Longrightarrow x_4 = 5.$

$\overline{x} = a_1N_1x_1 + a_2N_2x_2 + a_3N_3x_3 + a_4N_4x_4$

$= 4 \times 1001 \times 1 + 2 \times 715 \times 1 + 9 \times 455 \times 3 + 9 \times 385 \times 5 = 35044 = 9.$

$\therefore \quad 3^{302} \equiv 9(\text{mod } 5005)$.

Review:

1. State the conditions under which the CRT can be applied to a system of congruences.
2. Why is it important that the moduli in CRT are pairwise coprime?
3. Does the CRT work if the moduli are not coprime? Justify your answer.
4. Find a general solution to $x \equiv 3 \; (\text{mod } 8), \; x \equiv 4 \; (\text{mod } 9)$

L4- Introduction to Congruences System of Linear Congruences, Solving Polynomials

Recall:

1. What is the Chinese Remainder Theorem (CRT)?
2. Describe a real-world application of the CRT.
3. Given to $x \equiv 2 \; (\text{mod } 3), \; x \equiv 3 \; (\text{mod } 4)$, solve for x.
4. Explain why the CRT guarantees a unique solution modulo the product of the moduli.

Linear congruences in two variables:

Congruence $ax + by \equiv c(\text{mod } n)$ has a solution if and only if $\gcd(a, b, n)|c$.

1. Find all solutions of $3x - 7y \equiv 11(\text{mod } 13).$

Solution: If $y \equiv 0(\text{mod } 13)$, then $3x \equiv 11(\text{mod } 13) \Longrightarrow \; x \equiv 8(\text{mod } 13)$.

If $y \equiv 1(\text{mod } 13)$, then $3x \equiv 5(\text{mod } 13) \Longrightarrow \; x \equiv 6(\text{mod } 13)$.

If $y \equiv 2(\text{mod } 13)$, then $3x \equiv 12(\text{mod } 13) \Longrightarrow \; x \equiv 4(\text{mod } 13)$.

If $y \equiv 3(\text{mod } 13)$, then $3x \equiv 6(\text{mod } 13) \Longrightarrow x \equiv 2(\text{mod } 13)$.

If $y \equiv 4(\text{mod } 13)$, then $3x \equiv 0(\text{mod } 13) \Longrightarrow x \equiv 0(\text{mod } 13)$.

If $y \equiv 5(\text{mod } 13)$, then $3x \equiv 7(\text{mod } 13) \Longrightarrow x \equiv 11(\text{mod } 13)$.

If $y \equiv 6(\text{mod } 13)$, then $3x \equiv 1(\text{mod } 13) \Longrightarrow x \equiv 9(\text{mod } 13)$.

If $y \equiv 7(\text{mod } 13)$, then $3x \equiv 8(\text{mod } 13) \Longrightarrow x \equiv 7(\text{mod } 13)$.

If $y \equiv 8(\text{mod } 13)$, then $3x \equiv 2(\text{mod } 13) \Longrightarrow x \equiv 5(\text{mod } 13)$.

If $y \equiv 9(\text{mod } 13)$, then $3x \equiv 9(\text{mod } 13) \Longrightarrow x \equiv 3(\text{mod } 13)$.

If $y \equiv 10(\text{mod } 13)$, then $3x \equiv 3(\text{mod } 13) \Longrightarrow x \equiv 1(\text{mod } 13)$.

If $y \equiv 11(\text{mod } 13)$, then $3x \equiv 10(\text{mod } 13) \Longrightarrow x \equiv 12(\text{mod } 13)$.

If $y \equiv 12(\text{mod } 13)$, then $3x \equiv 4(\text{mod } 13) \Longrightarrow x \equiv 10(\text{mod } 13)$.

Theorem:

System of linear congruences $ax + by \equiv r(\text{mod } n)$ and $cx + dy \equiv s(\text{mod } n)$ has a unique solution modulo n if $\gcd(ad - bc, n) = 1$.

Example: 1. Solve the system of congruence equations

$$7x + 3y \equiv 10(\text{mod } 16) \text{ and } 2x + 5y \equiv 9(\text{mod } 16).$$

Solution: Given that, $7x + 3y \equiv 10(\text{mod } 16)$ $\cdots\cdots\cdots(1)$

$2x + 5y \equiv 9(\text{mod } 16)$ $\cdots\cdots\cdots(2)$

$\gcd(ad - bc, n) = \gcd(29, 16) = 1$. System has unique solution.

$5(1) - 3(2) \Longrightarrow 29x \equiv 23(\text{mod } 16) \Longrightarrow 13x \equiv 7(\text{mod } 16) \Longrightarrow x \equiv 3(\text{mod } 16)$.

$2(1) - 7(2) \Longrightarrow -29y \equiv -43(\text{mod } 16) \Longrightarrow 3y \equiv 5(\text{mod } 16) \Longrightarrow y \equiv 7(\text{mod } 16)$

Solution is $x \equiv 3(\text{mod } 16)$, $y \equiv 7(\text{mod } 16)$.

2. Solve the system of congruence equations

$$2x + 6y \equiv 1(\text{mod} 7) \text{ and } 4x + 3y \equiv 2(\text{mod } 7).$$

Solution: Given that, $2x + 6y \equiv 1(\text{mod} 7)$ $\cdots\cdots\cdots(1)$

$4x + 3y \equiv 2(\text{mod } 7)$ $\cdots\cdots\cdots(2)$

$\gcd(ad - bc, n) = \gcd(18, 7) = 1$. System has unique solution.

$3(1) - 6(2) \Longrightarrow -18x \equiv -9(\text{mod } 7) \Longrightarrow 3x \equiv 5(\text{mod } 7) \Longrightarrow x \equiv 4(\text{mod } 7)$.

$2(1) - (2) \Longrightarrow 9y \equiv 0(\text{mod } 7) \Longrightarrow 2y \equiv 0(\text{mod } 7) \Longrightarrow y \equiv 0(\text{mod } 7)$

Solution is $x \equiv 4(\text{mod } 7)$, $y \equiv 0(\text{mod } 7)$.

Polynomial congruence:

Theorems:

1. Let $P(x) = \sum_{k=0}^{k=m} c_k x^k$ be a polynomial function in x with integral coefficients c_k, and if $a \equiv b(\text{mod } n)$, then $P(a) \equiv P(b)(\text{mod } n)$.
2. If $P(a) \equiv 0(\text{mod } n)$, then a is a solution (root) of the equation $P(x) \equiv 0(\text{mod } n)$.
3. If a is a solution (root) of the equation $P(x) \equiv 0(\text{mod } n)$ and $a \equiv b(\text{mod } n)$, then b is also a solution.

Examples:

1. Let $P(x) = x^2 + 2x - 3$. Then the solutions of $P(x) \equiv 0 (\text{mod } 5)$ are

$x \equiv 1,\ 2 (\text{mod } 5)$.

Because $P(1) = 0,\ P(2) = 5$, and hence $P(1) \equiv 0 (\text{mod } 5),\ P(2) \equiv 0 (\text{mod } 5)$.

2. Find all roots of $x^2 + x + 7 \equiv 0 (\text{mod } 15)$.

Solution: $15 = 3 \times 5$. $P(x) = x^2 + x + 7$.

First find the solutions of $P(x) \equiv 0 (\text{mod } 3)$

$P(0) = 7,\ P(1) = 9,\ P(2) = 13$.

Clearly $P(1) \equiv 0 (\text{mod } 3)$, but $P(1) \not\equiv 0 (\text{mod } 5)$.

Therefore equation $x^2 + x + 7 \equiv 0 (\text{mod } 15)$ has no solution.

3. Solve $x^5 - 3x^2 + 2 \equiv 0 (\text{mod } 7)$.

Solution: Let $P(x) = x^5 - 3x^2 + 2$.

Then $P(0) = 2,\ P(1) = 0,\ P(2) = 22,\ P(3) = 218,\ P(4) = 978,$

$P(5) = 3052,\ P(6) = 7670$.

Therefore solutions are $x \equiv 1,\ 5 (\text{mod } 7)$

4. Find all roots of $x^3 + 2x - 3 \equiv 0 (\text{mod } 9)$.

Let $P(x) = x^3 + 2x - 3$.

$P(0) = -3,\ P(1) = 0,\ P(2) = 9, P(3) = 30,\ P(4) = 69, P(5) = 132,$

$P(6) = 225,\ P(7) = 354,\ P(8) = 525$.

Therefore roots are $x \equiv 1,\ 2,\ 6\ (\text{mod } 9)$.

Review:

1. What is a system of linear congruences? Give an example.
2. Under what conditions does a system of linear congruences have a unique solution?
3. Solve the linear polynomial $3x + 2 \equiv 0 (\text{mod } 7)$.
4. Explain how to check if a quadratic congruence a $ax^2 + bx + c \equiv 0 (\text{mod } m)$ has a solution.

T2- Problems on Congruence

1. Find the solutions of the following linear congruence:
   a. $6x \equiv 3 (mod\ 9)$. b. $6x \equiv 15 (mod\ 21)$.
   c. $11x \equiv 4 (mod\ 15)$. d. $12x \equiv 6 (mod 21)$.

2. Find the solution of the following system of linear congruences:

   a. $5x + 3y \equiv 2 (mod\ 14)$ and $-3x + 4y \equiv 7 (mod\ 14)$

   b. $x + 2y \equiv 3 (mod\ 9)$ and $3x + y \equiv 2 (mod\ 9)$

3. Find the least positive values of *x* such that

   a) i) $71 \equiv x (mod 8)$ ii) $78 + x \equiv 3 (mod 5)$ iii) $89 \equiv (x+3) (mod 4)$

4. Solve the polynomial congruence: $x^3 + 5x + 1 \equiv 0 (\text{mod} 27)$.

L5- Fermat's little theorem.

Recall:

1. Discuss how polynomial congruences are applied in cryptography..
2. Solve the congruence $2x \equiv 8 (mod\ 6)$if possible.

3. Solve $x^2 \equiv 5(\bmod 11)$. using modular square roots.
4. Under what conditions does a system of linear congruences have a unique solution?

Fermat's little theorem: Let p be a prime and $p \nmid a$, then $a^{p-1} \equiv 1(\bmod p)$.

Corollary: If p is a prime, then $a^p \equiv a(\bmod p)$.

Lemma: If p and q are distinct primes with $a^p \equiv a(\bmod q)$ and $a^q \equiv a(\bmod p)$, then $a^{pq} \equiv a(\bmod pq)$.

Examples:

1. Show that $8^{30} - 1$ is divisible by 31. (Or Show that $8^{30} \equiv 1(\bmod 31)$)
   Since 31 is prime and $31 \nmid 8$, by Fermat's little theorem,
   $8^{30} \equiv 1(\bmod 31)$. Therefore $8^{30} - 1$ is divisible by 31.
2. Find the reminder when 72^{1001} is divided by 31.
   Since 31 is prime and $31 \nmid 72$, by Fermat's little theorem,
   $72^{30} \equiv 1(\bmod 31) \Rightarrow (72^{30})^{33} \equiv 1(\bmod 31)$
   $72 \equiv 10(\bmod 31)$, $72^2 \equiv 7(\bmod 31) \Rightarrow 72^3 \equiv 8(\bmod 31)$
   $\Rightarrow 72^6 \equiv 2(\bmod 31) \Rightarrow 72^9 \equiv 16(\bmod 31)$
   $\Rightarrow 72^{11} \equiv 19(\bmod 31)$
   $\therefore\ 72^{1001} = (72^{30})^{33} \times 72^{11} \equiv 19(\bmod 31)$.
   Reminder is 19.
3. Show that $2^{340} \equiv 1(\bmod 31)$.
   Since 31 is prime and $31 \nmid 2$, by Fermat's little theorem,
   $2^{30} \equiv 1(\bmod 31) \Rightarrow (2^{30})^{11} = 2^{330} \equiv 1(\bmod 31)$.
   $2^5 \equiv 1(\bmod 31) \Rightarrow 2^{10} \equiv 1(\bmod 31)$
   $\therefore 2^{330+10} \equiv 1(\bmod 31)$. Or, $2^{340} \equiv 1(\bmod 31)$.
4. Find the value of a if $7^{121} \equiv a(\bmod 13)$.
   Since 13 is prime and $13 \nmid 7$, by Fermat's little theorem,
   $7^{12} \equiv 1(\bmod 13) \Rightarrow (7^{12})^{10} = 7^{120} \equiv 1(\bmod 13)$.
   $\Rightarrow 7^{121} \equiv 7(\bmod 13)$.
   $\therefore\ a \equiv 7(\bmod 13)$.
5. Find the reminder when 41^{75} is divided by 3.
   Since 3 is prime and $3 \nmid 41$, by Fermat's little theorem,
   $41^2 \equiv 1(\bmod 3) \Rightarrow (41^2)^{37} \equiv 1(\bmod 3)$, $41 \equiv 2(\bmod 3)$
   $\Rightarrow 41^{75} \equiv 2(\bmod 3)$
   Required reminder is 2.
6. Find the reminder when 5^{11} is divided by 7.
   Since 7 is prime and $7 \nmid 5$, by Fermat's little theorem,
   $5^6 \equiv 1(\bmod 7) \Rightarrow 5^{12} \equiv 1(\bmod 7) \Rightarrow 5 \times 5^{11} \equiv 1(\bmod 7)$
   $\Rightarrow 15 \times 5^{11} \equiv 3(\bmod 7)$, Or $5^{11} \equiv 3(\bmod 7)$.

Required reminder is 3.

7. Show that $5^{38} \equiv 4(\bmod 11)$.

Since 11 is prime and $11 \nmid 5$, by Fermat's little theorem,

$5^{10} \equiv 1(\bmod 11) \Rightarrow 5^{40} \equiv 1(\bmod 11) \quad \Rightarrow 25 \times 5^{38} \equiv 1(\bmod 11)$

$\Rightarrow 3 \times 5^{38} \equiv 1(\bmod 11) \Rightarrow 12 \times 5^{38} \equiv 4(\bmod 11)$

$\therefore 5^{38} \equiv 4(\bmod 11)$

Review:

1. State **Fermat's Little Theorem**.
2. Use Fermat's Little Theorem to solve $x^5 \equiv 3(\bmod 11)$.?
3. What is the condition for Fermat's Little Theorem to be applicable to a number a and a modulus p?
4. Why is Fermat's Little Theorem valid only when p is a prime number?

L6- Euler's Theorem, Wilson Theorem

Recall:

1. Prove that if p is a prime number, then $a^p \equiv a(\bmod p)$ (Fermat's Little Theorem).
2. Explain the significance of Fermat's Little Theorem in modular arithmetic.
3. Compute $2^{11}(\bmod 13)$using Fermat's Little Theorem.
4. Provide a counterexample to show that Fermat's Little Theorem does not hold when p is not prime.

Euler's Phi- function (indicator or totient): For any nonnegative integer n, $\emptyset(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

For any prime p, $\emptyset(p) = p - 1$.

For any distinct primes p, q, $\emptyset(pq) = (p-1)(q-1)$.

$\emptyset(p^k) = p^k(1 - \frac{1}{p})$.

Euler's theorem: If $n \geq 0$, and $\gcd(a, n) = 1$, then $a^{\emptyset(n)} \equiv 1(\bmod n)$.

Examples:

1. Solve $3^{202} \equiv x(\bmod 13)$ by Euler's theorem.

Solution: Since $\gcd(3, 13) = 1$, then $3^{12} \equiv 1(\bmod 13)$. $\because \emptyset(13) = 12$.

$\Rightarrow (3^{12})^{17} \equiv 1(\bmod 13)$

$\Rightarrow 3^{204} \equiv 1(\bmod 13) \Rightarrow 9 \times 3^{202} \equiv 1(\bmod 13)$

$\Rightarrow 3^{202} \equiv 3(\bmod 13)$ $\because 9 \times 3 \equiv 1(\bmod 13)$.

$\therefore x \equiv 3(\bmod 13)$.

2. Prove that $4^{99} \equiv 29(\bmod 35)$.

Solution: $\emptyset(35) = \emptyset(5) \times \emptyset(7) = 4 \times 6 = 24$, $\gcd(4, 35) = 1$.

By Euler's theorem $4^{24} \equiv 1(\bmod 35)$

$\Rightarrow (4^{24})^4 \equiv 1(\bmod 35) \Rightarrow 4^{96} \equiv 1(\bmod 35)$

$\Rightarrow 4^{99} \equiv 64(\bmod 35) \Rightarrow 4^{99} \equiv 29(\bmod 35)$.

3. Find the digit in the unit's place in 3^{100}.

Solution: $\emptyset(10) = \emptyset(2) \times \emptyset(5) = 4.$

By Euler's theorem $3^4 \equiv 1(\bmod 10)$

$\Longrightarrow (3^4)^{25} \equiv 1(\bmod 10) \Longrightarrow 3^{100} \equiv 1(\bmod 10).$

Therefore digit in the unit's place is 1.

4. Find the last two digits in 13^{122}.

Solution: $\emptyset(100) = \emptyset(2^2) \times \emptyset(5^2) = 2 \times 20 = 40$

By Euler's theorem $13^{40} \equiv 1(\bmod 100)$

$\Longrightarrow (13^{40})^3 \equiv 1(\bmod 100) \Longrightarrow 3^{122} \equiv 69(\bmod 10).$

Number in the last two digits is 69.

Wilson's theorem: If p is a prime, then $(p-1)! \equiv -1(\bmod p).$

Using Wilson's theorem if p is a prime, then prove that,

i) $(p-1)! \equiv (p-1)(\bmod p).$
ii) $(p-2)! \equiv 1(\bmod p).$
iii) $(p-3)! \equiv \frac{(p-1)}{2}(\bmod p).$

i) $(p-1)! \equiv -1(\bmod p) \Longrightarrow (p-1)! \equiv (p-1)(\bmod p)$

ii) $(p-1)! \equiv (p-1)(\bmod p) \Longrightarrow (p-2)! \equiv 1(\bmod p).$

iii) $\frac{(p-1)(p-2)}{2} - 1 = \frac{p^2-3p}{2} = \frac{p(p-3)}{2} = kp$. $\because p-3$ is even.

$\therefore (p-2)\left(\frac{p-1}{2}\right) \equiv 1(\bmod p)$, but $(p-2)[(p-3)!] \equiv 1(\bmod p).$

$\Longrightarrow (p-3)! \equiv \frac{(p-1)}{2}(\bmod p).$

Examples:

1. Find the reminder when $15!$ is divided by 17.

By Wilson's theorem $(p-2)! \equiv 1(\bmod p)$ for prime p.

$\Longrightarrow 15! \equiv 1(\bmod 17).$ Therefore reminder is 1.

2. Show that $4 \times 29! + 5!$ is divisible by 31.

By Wilson's theorem $(p-2)! \equiv 1(\bmod p)$ for any prime p.

$\Longrightarrow (29)! \equiv 1(\bmod 31) \Longrightarrow 4 \times (29)! \equiv 4(\bmod 31),$

and $5! \equiv -4(\bmod 31)$

$\Longrightarrow 4 \times 29! + 5! \equiv 0(\bmod 31).$

Therefore $4 \times 29! + 5!$ is divisible by 31.

3. Find the reminder when $2 \times 26!$ is divided by 29.

By Wilson's theorem, $(28)! \equiv -1(\bmod 29) \Longrightarrow 28 \times 27 \times (26)! \equiv -1(\bmod 29)$

$\Longrightarrow (-1)(-2) \times (26)! \equiv -1(\bmod 29)$

$\Longrightarrow 2 \times (26)! \equiv -1(\bmod 29)$ Or $2 \times (26)! \equiv 28(\bmod 29)$

Therefore reminder is 28.

4. Show that $16! + 1$ is divisible by 17.

By Wilson's theorem $(p-1)! \equiv -1(\bmod p)$. for any prime p.

$\Rightarrow (16)! \equiv -1(\bmod 17)$

Or $(16)! + 1 \equiv 0(\bmod 17)$

$\therefore 16! + 1$ is divisible by 17.

5. Show that $18! \equiv -1(\bmod 437)$.

Solution: $437 = 19 \times 23$ and $\gcd(19, 23) = 1$.

$18! \equiv -1(\bmod 19) \quad \cdots\cdots\cdots(1)$

$22! \equiv -1(\bmod 23)$

$\Rightarrow 22 \times 21 \times 20 \times 19 \times 18! \equiv -1(\bmod 23)$

$\Rightarrow (-1)(-2)(-3)(-4) \times 18! \equiv -1(\bmod 23)$

$\Rightarrow 24 \times 18! \equiv -1(\bmod 23)$

Or $18! \equiv -1(\bmod 23) \quad \cdots\cdots\cdots(2)$

By (1) and (2), $18! \equiv -1(\bmod 437)$.

6. Show that $63! \equiv -1(\bmod 71)$.

Solution: By Wilson's theorem,

$70! \equiv -1(\bmod 71)$

$\Rightarrow 70 \times 69 \times 68 \times 67 \times 66 \times 65 \times 64 \times 63! \equiv -1(\bmod 71)$

$\Rightarrow (-1)(-2)(-3)(-4)(-5)(-6)(-7) \times 63! \equiv -1(\bmod 71)$

$\Rightarrow (72)(70) \times 63! \equiv 1(\bmod 71)$

$\Rightarrow (1)(-1) \times 63! \equiv 1(\bmod 71)$

Or $63! \equiv -1(\bmod 71)$.

Review:

1. Explain the difference between Fermat's Little Theorem and Euler's Theorem.
2. How does Fermat's Little Theorem relate to Wilson's Theorem?
3. State **Euler's Theorem** and **Wilson's Theorem**.
4. What is the significance of Euler's totient function $\emptyset(n)$ in the theorem?
5. Use Euler's Theorem to find the modular inverse of $3(\bmod 10)$.

L7- Applications of Congruences-RSA algorithm

Recall:

1. How does Euler's Theorem generalize Fermat's Little Theorem?.
2. Define Euler's totient function $\emptyset(n)$.
3. Compute $\emptyset(36)$.
4. Why does Euler's Theorem require $\gcd(a, n) = 1$?
5. Why is Wilson's Theorem applicable only for prime p?

RSA- Algorithm: The RSA algorithm is a public-key signature algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman.

Key Generation

1. Choose two large prime numbers (p and q)
2. Calculate $n = p \times q$ and $\emptyset(n) = (p-1)(q-1)$

3. Choose a number e where $1 < e < \emptyset(n)$ and $\gcd(e, \emptyset(n)) = 1$.
4. Calculate d such that $d \times e \equiv 1(\bmod \emptyset(n))$.
5. Private key pair is (n, d)
6. Public key pair is (n, e)

Encryption/Decryption Function

Once you generate the keys, you pass the parameters to the functions that calculate your ciphertext and plaintext using the respective key.

- If the plaintext is M, Ciphertext $\equiv M^e \pmod n$.
- If the Ciphertext is C, Plaintext $\equiv C^d \pmod n$.

Let $A:0,\ B:1,\ C:2,\ D:3,\ E:4,\ \cdots\cdots Z:25$.

Examples:

1. Using RSA algorithm find public key and private key If $p = 3,\ q = 11$ and $M = 31$.

Solution: $p = 3,\ q = 11 \Longrightarrow\ n = 33,\ \emptyset(n) = 20$.

Let $e = 7$. Since $1 < 7 < 20$ and $\gcd(7, 20) = 1$.

$d \times e \equiv 1\big(\bmod \emptyset(n)\big) \Longrightarrow d = 3$.

Public key pair is $(n, e) = \{33,\ 7\}$, and private key pair is $(n, d) = \{33,\ 3\}$.

Encryption: Ciphertext $\equiv M^e \pmod n$ i.e. $\mathrm{C} \equiv 31^7 \pmod{33}$

Since, $31 \equiv -2 \pmod{33},\ 31^2 \equiv 4 \pmod{33}$.

$31^5 \equiv -32 \pmod{33} \Longrightarrow 31^5 \equiv 1 \pmod{33} \Longrightarrow 31^7 \equiv 4 \pmod{33}$.

$\mathrm{C} \equiv 4 \pmod{33}$.

$\therefore \mathrm{C} = 04 = \mathrm{AE}$.

Decryption: Plaintext $\equiv C^d \pmod n$ i.e. $\mathrm{M} \equiv 4^3 \pmod{33}$.

Since, $4^3 \equiv 31 \pmod{33},\ \mathrm{M} \equiv 31 \pmod{33}$.

$\therefore \mathrm{M} = 31 = \mathrm{DB}$.

2. In RSA algorithm if $p = 7,\ q = 11$ and $e = 13$, then find d.

Solution: $p = 7,\ q = 11 \Longrightarrow\ n = 77,\ \emptyset(n) = 60$.

If $e = 13,\ \ d \times e \equiv 1\big(\bmod \emptyset(n)\big) \Longrightarrow 13d \equiv 1(\bmod 60)$.

Since, $13 \times 10 \equiv 10(\bmod 60)$, $13 \times 30 \equiv 30(\bmod 60)$,

and $13 \times 7 \equiv 31(\bmod 60) \Longrightarrow 13 \times 37 \equiv 1(\bmod 60)$

$\therefore d = 37$.

3. In RSA algorithm if $p = 3,\ q = 11$ and $d = 7$, then find e. Hence encrypt 19.

Solution: $p = 3,\ q = 11 \Longrightarrow\ n = 33,\ \emptyset(n) = 20$.

Given that, $d = 7$. Since $d \times e \equiv 1\big(\bmod \emptyset(n)\big)$

$\Longrightarrow 7\,e \equiv 1(\bmod 20) \qquad \therefore e = 3$.

Encryption: Ciphertext $\equiv M^e \pmod n$ i.e. $\mathrm{C} \equiv 19^3 \pmod{33}$

Since, $19^2 \equiv -2 \pmod{33},\ 19^3 \equiv -38 \pmod{33}$.

$-38 + 66 = 28 \qquad \therefore \mathrm{C} \equiv 28 \pmod{33}$.

$\therefore C = 28 = CI$.

Review:

1. In the RSA algorithm, what are the roles of the public and private keys?
2. Define the terms n, e,d and $\emptyset(n)$ in the RSA algorithm.
3. Explain the steps for generating RSA keys.
4. Why must the chosen primes p and q be large in RSA?
5. What role does Euler's totient function $\emptyset(n)$ play in RSA security?

T3- Problems on RSA algorithm

1. If $p = 3,\ q = 11$ and private key $d = 7$, Find the public key 'e' using RSA algorithm. Hence encrypt the number 19. [Take B=1 and J=9]
2. If $p = 3,\ q = 11$ and public key $e = 7$, Find the private key 'd' using RSA algorithm. Hence decrypt the cipher text 'BE'. [Take B=2 and E=5].
3. Encrypt the message STOP using RSA with key (2537, 13) using the prime numbers 43 and 59.
4. In RSA algorithm if $p = 3,\ q = 11$ and $d = 7$, then find e. Hence encrypt 19.

Course outcome

- Get acquainted and to apply modular arithmetic to computer algorithms and demonstrate using python.

PRACTICE QUESTION BANK

MODULE 4: Modular Arithmetic.

1. Solve the following linear Diophantine equation:
   a. $172x + 20y = 1000.$ b. $30x + 17y = 300.$
   c. $56x + 72y = 40$. d. $70x + 112y = 168.$
2. Find the solutions of the following linear congruence:
   a. $18x \equiv 30(mod\ 42).$ b. $21x \equiv 49(mod\ 10)$.
   c. $7x \equiv 15(mod\ 17)$. d. $12x \equiv 6(mod 21).$
3. Find the solution of the following system of linear congruences:
   a. $2x + 6y \equiv 1(mod 7)$ and $4x + 3y \equiv 2(mod\ 7)$
   b. $7x + 3y \equiv 10(mod 16)$ and $2x + 5y \equiv 9(mod\ 16)$
4. Find the least positive values of x such that
   a) i) $71 \equiv x(mod 8)$ ii) $78 + x \equiv 3(mod 5)$ iii) $89 \equiv (x+3)(mod 4)$
5. Solve the polynomial congruence: $x^3 + 5x + 1 \equiv 0(\text{mod}27)$.
6. Solve the following using Fermat's little theorem:
   a. Find the reminder when 72^{1001} is divided by 31.
   b. Show that $2^{340} \equiv 1(\ \text{mod}\ 31)$.

c. Find the value of a if $7^{121} \equiv a(\text{ mod } 13)$.

d. Find the reminder when 5^{11} is divided by 7.

7. Solve the following using Euler's theorem:
   a. Find the digit in the unit's place in 3^{100}.
   b. Find the last two digits in 13^{122}.
   c. Solve $3^{202} \equiv x(\text{ mod } 13)$.
   d. Evaluate: $2^{100000}\ (mod\ 77)$.

8. Solve the following using Wilson's theorem:
   a. Find the reminder when $14!$ is divided by 17.
   b. Show that $4 \times 29! + 5!$ is divisible by 31.
   c. Show that $63! \equiv -1(\text{ mod } 71)$.

9. Find the remainder when (349×74 ×36) is divided by 3

10. Solve the following using Chinese Remainder theorem :
    a. $x \equiv 3\ (mod\ 5)\ ;\ x \equiv 2\ (mod\ 6)\ ;\ x \equiv 4\ (mod\ 7)$.
    b. $x \equiv 2\ (mod\ 3)\ ;\ x \equiv 3\ (mod\ 5)\ ;\ x \equiv 2\ (mod\ 7)$.
    c. $x \equiv 1\ (mod\ 3)\ ;\ x \equiv 2\ (mod\ 4)\ ;\ x \equiv 3\ (mod\ 5)$.
    d. $4x \equiv 5\ (mod\ 9),\ 2x \equiv 6\ (mod\ 20)$.

11. If $p = 3,\ q = 11$ and private key $d = 7$, Find the public key 'e' using RSA algorithm. Hence encrypt the number 19. [Take B=1 and J=9]

12. If $p = 3,\ q = 11$ and public key $e = 7$, Find the private key 'd' using RSA algorithm. Hence decrypt the cipher text 'BE'. [Take B=2 and E=5].

13. Encrypt the message STOP using RSA with key (2537, 13) using the prime numbers 43 and 59.

14. In RSA algorithm if $p = 3,\ q = 11$ and $d = 7$, then find e. Hence encrypt 19.