

MODULE-1

Modular Arithmetic

Divisibility

The set of integers consists of all positive integers, all negative integers and zero. It is denoted by I or $Z = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

$$= \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$$

Consider 2 integers a and b where $a \neq 0$, a divides b

If there exists an integer k such that $b = ka$

Eg: 9 divides 54, there is an integer 6 such that $54 = 6 \times 9$

Division Algorithm

Given two integers a and b where $a > 0$, two unique integers q and r such that $b = qa + r$ where $0 \leq r < a$. This is known as division algorithm. q is called the quotient and r is called the remainder.

Note: In all divisions q may be positive or negative.

Greatest Common Divisor(G.C.D) or Highest Common Factor(H.C.F)

The G.C.D of two integers a and b (both of them are not zero) is a unique positive integer d such that

- 1) d is the common divisor of both a and b .

$$d/a, d/b$$

- 2) every common divisor of a and b divides d

$$x/a \text{ and } x/b \Rightarrow x/d$$

The G.C.D of 2 numbers a and b is written as (a, b)

$$\text{i.e., } d = (a, b)$$

Euclid's Algorithm method to find the G.C.D of 2 numbers a and b and to express the G.C.D as $ax + by$

A method of finding the greatest common divisor of two numbers by dividing the larger by the smaller, the smaller by the remainder, the first remainder by the second remainder and so on until exact division is obtained. Hence the greatest common divisor is the exact divisor.

Find the G.C.D of 32 and 54 and express it in the form of $32x + 54y$

$$32 \overline{) 54} (1$$

$$\underline{32}$$

$$22 = 54 - 1(32)$$

$$22$$

$$22)32(1$$

$$\begin{array}{r} 22 \\ \hline 10 \end{array}$$

$$10=32-1(22)$$

$$10)22(2$$

$$\begin{array}{r} 20 \\ \hline 2 \end{array}$$

$$2=22-2(10)$$

$$2)10(5$$

$$\begin{array}{r} 10 \\ \hline 0 \end{array}$$

$$2=22-2(10)$$

The last non zero remainder is 2.

$$2=22-2(10)$$

$$2= [54-1(32)]-2[32-1(22)]$$

$$=54-3(32) +2(22)$$

$$=54-3(32) +2[54-1(32)]$$

$$=3(54)-5(32)$$

$$=54(3) +32(-5)$$

$$2=54(x)+32(y) \text{ where } x=3 \text{ and } y=-5$$

Relatively Prime numbers:

Two numbers a and b are said to be relatively prime or coprime if and only if $(a, b) = 1$, i.e the G.C.D of a and b is 1

Example: $(8,15)=1$

8 and 15 are relatively prime

Congruence's:

Let m be a positive integer (>1). If a and b are any integers then a is said to be congruent to b modulo m if and only if $m|(a-b)$

'a is congruent to b modulo m is written as $a \equiv b(modm)$

Example:

$$1) 25 \equiv 3(mod11), 11/25-3, \text{ i.e } 11/22$$

$$2) -69 \equiv -5(mod16), 16/-69+5, \text{ i.e } 16/-64$$

$$3) \text{ Consider the congruence } 134 \equiv 108(mod13) \text{ which is true}$$

When 134 and 108 are divided by 13, the same remainder 4 is obtained. This gives the alternative definition of the congruence.

Definition of Congruence's:

If m is a positive integer (>1) and a and b are any integer the a is said to be congruent to b modulo m if and only if a and b leave the same remainder when divided by m

Note: 1) $a \equiv b(\text{mod } m) \Rightarrow m/(a - b)$

Conversely $m/(a - b)$ then $a \equiv b(\text{mod } m)$

Problems:

1) Solve $5x \equiv 4(\text{mod } 13)$

$$\Rightarrow 13/(5x - 4)$$

$$\Rightarrow 5x - 4 = 13k \text{ where } k \in \mathbb{Z}$$

$$\Rightarrow 5x = 13k + 4$$

$$\Rightarrow x = \frac{13k+4}{5}$$

By inspection, $k = 2$ gives the integral value of Z
i.e., $x=6$

$$x \equiv 6(\text{mod } 13)$$

The general solution is $x = 6 + 13t$ where $t \in \mathbb{Z}$

2) Solve $7x \equiv 9(\text{mod } 15)$

$$\Rightarrow 15/(7x - 9)$$

$$\Rightarrow 7x - 9 = 15k \text{ where } k \in \mathbb{Z}$$

$$\Rightarrow 7x = 15k + 9$$

$$\Rightarrow x = \frac{15k+9}{7}$$

By inspection, $k = 5$ gives the integral value of Z
i.e., $x=12$

$$x \equiv 12(\text{mod } 15)$$

The general solution is $x = 6 + 13t$ where $t \in \mathbb{Z}$

3) Find the least positive values of x such that $71 \equiv x(\text{mod } 8)$

$$8)71(8)$$

$$64$$

—

$$7$$

The value of x is 7

4) $78 + x \equiv 3(\text{mod } 5)$

$$78 + x - 3 \equiv 5n$$

$$75 + x \equiv 5n$$

Let $x = 5$

$$75 + 5 \equiv 80 \text{ (80 is multiple of 5)}$$

The least value of x is 5

- 5) Find the least positive remainder when 2^{301} is divided by 5

$$2^4 \equiv 16 \equiv 1 \pmod{5}$$

$$4)301(75$$

$$\begin{array}{r} 28 \\ \hline 21 \\ 20 \\ \hline 1 \end{array}$$

$$(2^4)^{75} \equiv 1 \pmod{5}$$

$$2^{300} \equiv 1 \pmod{5}$$

$$2 \equiv 2 \pmod{5}$$

$$2^{301} \equiv 2 \pmod{5}$$

Remainder is 2.

- 6) Find the unit digit in the number 7^{289}

$$7^2 \equiv 49 \equiv 9 \pmod{10}$$

$$7^4 \equiv 2401 \equiv 1 \pmod{10}$$

$$(7^4)^{72} \equiv 1 \pmod{10}$$

$$7^{288} \equiv 1 \pmod{10} \text{-----(1)}$$

$$7 \equiv 7 \pmod{10} \text{-----(2)}$$

From (1) & (2)

$$7^{289} \equiv 7 \pmod{10}$$

The unit digit in 7^{289} is 7

- 7) Find the unit digit in the number 7^{2013}

$$7^2 \equiv 49 \equiv 9 \pmod{10}$$

$$7^4 \equiv 2401 \equiv 1 \pmod{10}$$

$$(7^4)^{503} \equiv 1 \pmod{10}$$

$$7^{2012} \equiv 1 \pmod{10} \text{-----(1)}$$

$$7 \equiv 7 \pmod{10} \text{-----(2)}$$

From (1) & (2)

$$7^{2013} \equiv 7 \pmod{10}$$

The unit digit in 7^{289} is 7

- 8) Find the unit digit in the number 7^{126}

$$7^2 \equiv 49 \equiv 9 \pmod{10}$$

$$7^4 \equiv 2401 \equiv 1 \pmod{10}$$

$$(7^4)^{31} \equiv 1 \pmod{10}$$

$$7^{124} \equiv 1 \pmod{10} \text{-----(1)}$$

$$7^2 \equiv 9 \pmod{10} \text{-----(2)}$$

From (1) & (2)

$$7^{126} \equiv 9 \pmod{10}$$

The unit digit in 7^{289} is 9

- 9) Find the unit digit in the number 13^{37}

$$13 \equiv 3 \pmod{10}$$

$$13^2 \equiv 9 \pmod{10}$$

$$13^2 \equiv -1 \pmod{10}$$

$$13^4 \equiv 1 \pmod{10}$$

$$(13^4)^9 \equiv 1 \pmod{10} \text{-----(1)}$$

$$13 \equiv 3 \pmod{10} \text{-----(2)}$$

From (1) & (2)

$$13^{37} \equiv 3 \pmod{10}$$

The unit digit in 13^{37} is 3

- 10) What is the remainder in the division of 2^{50} is divided by 7

$$2^3 \equiv 8 \equiv 1 \pmod{7}$$

$$(2^3)^{16} \equiv 1 \pmod{7} \text{-----(1)}$$

$$2^2 \equiv 4 \pmod{7} \text{-----(2)}$$

From (1) & (2)

$$2^{50} \equiv 4 \pmod{7}$$

The remainder when 2^{50} is divided by 7 is 4

- 11) Find the remainder when the number 2^{1000} is divided by 13.

$$2=2, 2^2 = 4, 2^3 = 8, 2^{16} \equiv 16 \equiv 3(mod 13), 2^5 = 32, 2^6 \equiv 64 \equiv -1(mod 13)$$

$$2^{1000} = 2^{6 \times 166 + 4}$$

$$= (2^6)^{166} \cdot 2^4$$

$$= (-1)^{166} mod 13 \cdot 3 mod 13$$

$$= 1 mod 13 \cdot 3 mod 13$$

$$2^{1000} \equiv 3 mod 13$$

Remainder is 3.

12) Find the remainder when $135 \times 74 \times 48$ is divided by 7.

$$7 \overline{)135}(1$$

$$\underline{7}$$

$$135 \equiv 2(mod 7)$$

$$65$$

$$\underline{63}$$

$$2$$

$$7 \overline{)74}(10$$

$$\underline{70}$$

$$74 \equiv 4(mod 7)$$

$$4$$

$$7 \overline{)48}(6$$

$$\underline{42}$$

$$48 \equiv 6(mod 7)$$

$$6$$

$$135 \times 74 \times 48 \equiv 48(mod 7) \equiv 6(mod 7)$$

Remainder is 6.

13) Find the remainder when $175 \times 113 \times 53$ is divided by 11.

$$11 \overline{)175}(15$$

$$\underline{11}$$

$$175 \equiv 10(mod 11)$$

$$65$$

$$\underline{55}$$

$$10$$

$$11 \overline{)113}(10$$

$$\underline{110}$$

$$113 \equiv 3(mod 11)$$

$$3$$

$$11)53(4)$$

$$\frac{44}{9}$$

$$53 \equiv 9 \pmod{11}$$

$$175 \times 113 \times 53 = 10 \times 3 \times 9 \equiv 270 \pmod{11} \equiv 6 \pmod{11}$$

Remainder is 6.

Rules for finding x in linear congruence : General format : $ax \equiv b \pmod{n}$

- 1) Find GCD $(a, n) = d$ (let)
- 2) If b/d is a whole number, then solution exists otherwise no solution
- 3) Find $d \pmod{n}$ ---- these number of solutions are possible
- 4) Divide both sides by d
- 5) Multiply both sides by an inverse
 $(aa^{-1})x \equiv b \cdot a^{-1} \pmod{n}$
- 6) General solution is given by $x_k = x_0 + k\left(\frac{n}{d}\right)$ where $k = 0, 1, 2, 3, \dots$

EXAMPLES:

$$1) 14x \equiv 12 \pmod{18}$$

$$ax \equiv b \pmod{n}$$

$$a = 14, b = 12, n = 18$$

$$1) \text{GCD}(14, 18) = 2 = d$$

$$(7xc) \pmod{9} = 1$$

$$2) \frac{b}{d} = \frac{12}{2} = 6 = \text{solutions exists}$$

$$c=1, 7 \pmod{9} \neq 1$$

$$3) d \pmod{n} = 2 \pmod{18} = 2 \text{ solutions exists}$$

$$c=2, 14 \pmod{9} \neq 1$$

4)

$$\text{Divide both side by d}$$

$$c=3, 21 \pmod{9} \neq 1$$

$$\left(\frac{14x}{2}\right) \equiv \left(\frac{12}{2}\right) \pmod{18/2}$$

$$c=4, 28 \pmod{9} = 1$$

$$7x \equiv 6 \pmod{9}$$

$$5) \text{multiply both sides by } 7^{-1}$$

$$(77^{-1})x \equiv 6 \cdot 7^{-1} \pmod{9}$$

$$x \equiv 6 \cdot 7^{-1} \pmod{9}$$

$$x \equiv 6 \cdot 4 \pmod{9}$$

$$x \equiv 24 \pmod{9}$$

$$x = 6$$

$$\text{The general solution is given by } x_k = x_0 + k\left(\frac{n}{d}\right)$$

$$\text{by } x_1 = 6 + 1\left(\frac{18}{2}\right) = 15$$

$$2) 9x \equiv 12 \pmod{15}$$

$$ax \equiv b \pmod{n}$$

$$a = 9, b = 12, n = 15$$

$$1) \text{GCD } (9,15) = 3 = d$$

$$(3xc) \bmod 5 = 1$$

$$2) \frac{b}{d} = \frac{12}{3} = 4 = \text{solutions exists}$$

$$c=1, 3 \bmod 5 \neq 1$$

$$3) d \bmod n = 3 \bmod 15 = 3 \text{ solutions exists}$$

$$c=2, 6 \bmod 5 = 1$$

4)

Divide both side by d

$$\begin{aligned} (9x/3) &\equiv (12/3) \pmod{15/3} \\ 3x &\equiv 4 \pmod{5} \end{aligned}$$

5) multiply both sides by 3^{-1}

$$(33^{-1})x \equiv 4.3^{-1} \pmod{5}$$

$$x \equiv 4.3^{-1} \pmod{5}$$

$$x \equiv 3 \pmod{5}$$

$$x = 3$$

The general solution is given by $x_k = x_0 + k\left(\frac{n}{d}\right)$

$$\text{by } x_1 = 3 + 1\left(\frac{15}{3}\right) = 8$$

THE CHINESE REMAINDER THEOREM

The Chinese Remainder theorem is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below:

$$X \equiv a_1 \pmod{m_1} ,$$

$$X \equiv a_2 \pmod{m_2} ,$$

$$X \equiv a_3 \pmod{m_3} ,$$

.....

$$X \equiv a_n \pmod{m_n}$$

CRT states that the above equations have a unique solutions if the moduli are relatively prime

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + \dots + a_n M_n M_n^{-1}) \bmod M$$

EXAMPLES:

1) Solve the following equations using CRT

$$X \equiv 2 \pmod{3} ,$$

$$X \equiv 3 \pmod{5} ,$$

$$X \equiv 2 \pmod{7} ,$$

$$\text{G.C.D } (3,5,7) = 1$$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$a_1 = 2, \quad m_1 = 3, \quad M_1 = 35, \quad M_1^{-1} = 2$$

$$a_2 = 3, \quad m_2 = 5, \quad M_2 = 21, \quad M_2^{-1} = 1$$

$$a_3 = 2, \quad m_3 = 7, \quad M_3 = 15, \quad M_3^{-1} = 1$$

$$M = m_1 X m_2 X m_3 = 3X5X7 = 105$$

$$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35 \quad ; \quad M_2 = \frac{M}{m_2} = \frac{105}{5} = 21 \quad ; \quad M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$$

$$M_1 M_1^{-1} = 1(\text{mod } m_1) \quad M_2 M_2^{-1} = 1(\text{mod } m_2) \quad M_3 M_3^{-1} = 1(\text{mod } m_3)$$

$$35 M_1^{-1} = 1 \text{mod } 3 \quad 21 M_2^{-1} = 1(\text{mod } 5) \quad 15 M_3^{-1} = 1(\text{mod } 7)$$

$$35x2 = 1 \text{mod } 3 \quad 21x1 = 1(\text{mod } 5) \quad 15x1 = 1(\text{mod } 7)$$

$$M_1^{-1} = 2 \quad M_2^{-1} = 1 \quad M_3^{-1} = 1$$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \text{mod } M$$

$$X = (2.35.2 + 3.21.1 + 2.15.1) \text{mod } 105$$

$$= 233 \text{ mod } 105$$

$$= 23$$

2) Solve the following equations using CRT

$$X \equiv 5(\text{mod } 3) \quad ,$$

$$X \equiv 2(\text{mod } 5)$$

$$X \equiv 1(\text{mod } 11)$$

$$\text{G.C.D}(3,5,11) = 1$$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \text{mod } M$$

$$a_1 = 5, \quad m_1 = 3, \quad M_1 = 55, \quad M_1^{-1} = 1$$

$$a_2 = 2, \quad m_2 = 5, \quad M_2 = 33, \quad M_2^{-1} = 2$$

$$a_3 = 1, \quad m_3 = 11, \quad M_3 = 15, \quad M_3^{-1} = 3$$

$$M = m_1 X m_2 X m_3 = 3X5X11 = 165$$

$$M_1 = \frac{M}{m_1} = \frac{165}{3} = 55 \quad ; \quad M_2 = \frac{M}{m_2} = \frac{165}{5} = 33 \quad ; \quad M_3 = \frac{M}{m_3} = \frac{165}{11} = 15$$

$$M_1 M_1^{-1} = 1(\text{mod } m_1) \quad M_2 M_2^{-1} = 1(\text{mod } m_2) \quad M_3 M_3^{-1} = 1(\text{mod } m_3)$$

$$55 M_1^{-1} = 1 \text{mod } 3 \quad 33 M_2^{-1} = 1(\text{mod } 5) \quad 15 M_3^{-1} = 1(\text{mod } 11)$$

$$55x_1 = 1 \pmod{3} \qquad 33x_2 = 1 \pmod{5} \qquad 15x_3 = 1 \pmod{11}$$

$$M_1^{-1} = 1 \qquad M_2^{-1} = 2 \qquad M_3^{-1} = 3$$

$$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \pmod{M}$$

$$X = (5 \cdot 55 \cdot 1 + 2 \cdot 33 \cdot 2 + 1 \cdot 15 \cdot 3) \pmod{165}$$

$$= 452 \pmod{165}$$

$$= 122$$

Linear Diophantine Equations:

An equation of the form $ax + by + c = 0$ where $a \neq 0$, $b \neq 0$ and c is an integer is called a linear Diophantine equation in two variables x and y

Examples : $8x + 17y = 7$, $2x + 3y = 12$

Solution of Linear Diophantine Equations:

A pair (x, y) of integers is called a solution of Linear Diophantine Equations $ax + by = c$ if $ax_0 + by_0 = c$ and $\text{GCD}(a, b) = d$ iff d/c then solution exists, then general solution is given by $x_1 = x_0 + \frac{b}{d}t$; $y_1 = y_0 - \frac{a}{d}t$

EXAMPLES:

1) Find the general solutions of the equations $70x + 112y = 168$

$$G.C.D(70, 112) = 14$$

$$\text{Now } 14/168 = 12$$

Linear Diophantine Equations $70x + 112y = 168$ has a solutions

By reverse

$$14 = 42 - 28$$

$$= 42 - (70 - 42)$$

$$= 42 - 70 + 42$$

$$= 2(42) - 70$$

$$= 2(112 - 70) - 70$$

$$= 2(112) - 2(70) - 70$$

$$14 = 2(112) - 3(70)$$

Multiply by 12

$$14(12) = 2(112 \times 12) - 3(70 \times 12)$$

$$168 = 24(112) - 36(70)$$

Thus $y_0 = 24$, $x_0 = -36$ is a particular solution of the given equation

The general solution is given by

$$x_1 = x_0 + \frac{b}{d} t ; y_1 = y_0 - \frac{a}{d} t$$

$$x_1 = -36 + \left(\frac{112}{14}\right) t ; y_1 = 24 - \left(\frac{70}{14}\right) t$$

$$x_1 = -36 + 8 t ; y_1 = 24 - 5 t$$

Hence $x_1 = -36 + 8 t ; y_1 = 24 - 5 t$, t is an integer

2) Find the general solutions of the equations $39x - 56y = 11$

$$G.C.D(39,56) = 1$$

$$\text{Now } 1/11 = 11$$

Linear Diophantine Equations $70x + 112y = 168$ has a solutions

By reverse

$$1 = 5 - 2(2)$$

$$= 5 - 2(17 - 3(5))$$

$$= 5 - 2(17) + 6(5)$$

$$= 7(5) - 2(17)$$

$$= 7(39 - 2(17)) - 2(17)$$

$$= 7(39) - 14(17) - 2(17)$$

$$1 = 7(39) - 16(17)$$

$$1 = 7(39) - 16(56 - 1(39))$$

$$1 = 7(39) - 16(56) + 16(39)$$

$$1 = 23(39) - 16(56)$$

Multiply by 11

$$1(11) = 23(11)(39) - 16(11)(56)$$

$$11 = 253(39) - 176(56)$$

Thus $y_0 = 176, x_0 = 253$ is a particular solution of the given equation

The general solution is given by

$$x_1 = x_0 + \frac{b}{d} t ; y_1 = y_0 - \frac{a}{d} t$$

$$x_1 = 253 + \left(-\frac{56}{1}\right) t ; y_1 = 176 - \left(\frac{39}{1}\right) t$$

$$x_1 = 253 - 56t ; y_1 = 176 - 39t$$

Hence $x_1 = 253 - 56t ; y_1 = 176 - 39t$, t is an integer

Polynomial congruence: -

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} \dots \dots \dots + a_n = 0 \pmod{m} \quad \text{where } n \geq 1 \quad \text{and} \\ a_0, a_1, a_2, a_3 \dots \dots \dots a_n \in \mathbb{Z}$$

Root of $f(x) \pmod{m}$

$x = c$ is called root of $f(x) \pmod{m}$ if and only if $f(c) = 0 \pmod{m}$ i.e. $m \mid f(x)$

EXAMPLES:

1) Find the roots of the polynomial $x^2 + 2x - 3 \pmod{5}$

Consider $f(x) = x^2 + 2x - 3 \pmod{5}$

$$f(0) = -3 \not\equiv 0 \pmod{5}$$

$$f(1) = 0 \equiv 0 \pmod{5}$$

$$f(2) = 5 \equiv 0 \pmod{5}$$

$$f(3) = 12 \not\equiv 0 \pmod{5}$$

$$f(4) = 21 \not\equiv 0 \pmod{5}$$

$x = 1, 2$ are the roots of $f(x) \pmod{5}$

But $x = 0, 3, 4$ are not the roots of $f(x) \pmod{5}$

2) Find all the roots of the polynomial $x^2 + x + 7 \equiv 0 \pmod{15}$

Consider $f(x) = x^2 + x + 7 \pmod{15}$

The possible solutions of given integers among $\{0, \pm 1, \pm 2\}$

$$f(0) = 7 \not\equiv 0 \pmod{15}$$

$$f(1) = 9 \not\equiv 0 \pmod{15}$$

$$f(2) = 13 \not\equiv 0 \pmod{15}$$

$$f(-1) = 7 \not\equiv 0 \pmod{15}$$

$$f(-2) = 9 \not\equiv 0 \pmod{15}$$

$f(x) = 0 \pmod{15}$ has no solution.

3) Solve the congruence of $x^5 - 3x^2 + 2 \equiv 0 \pmod{7}$

The given congruence is $f(x) = x^5 - 3x^2 + 2 \equiv 0 \pmod{7}$

Its solutions lie in the set $\{0, \pm 1, \pm 2, \pm 3\}$

$$f(0) = 2 \not\equiv 0 \pmod{7}$$

$$f(1) = 0 \equiv 0 \pmod{7}$$

$$f(2) = 22 \not\equiv 0 \pmod{7}$$

$$f(3) = 218 \not\equiv 0 \pmod{7}$$

$$f(-1) = -2 \not\equiv 0 \pmod{7}$$

$$f(-2) = -42 \equiv 0 \pmod{7}$$

$$f(-3) = -268 \not\equiv 0 \pmod{7}$$

Hence $x = 1, -2 \pmod{7}$ are solutions of the given congruence

4) Find all the roots of the congruence $x^3 + 2x - 3 \equiv 0 \pmod{9}$

The given congruence is $f(x) = x^3 + 2x - 3 \equiv 0 \pmod{9}$

Its solutions lie in the set $\{0, \pm 1, \pm 2, \pm 3, \pm 4\}$

$$f(0) = -3 \not\equiv 0 \pmod{9}$$

$$f(1) = 0 \equiv 0 \pmod{9}$$

$$f(2) = 0 \equiv 0 \pmod{9}$$

$$f(3) = 30 \not\equiv 0 \pmod{9}$$

$$f(4) = 69 \not\equiv 0 \pmod{9}$$

$$f(-1) = -6 \not\equiv 0 \pmod{9}$$

$$f(-2) = -15 \not\equiv 0 \pmod{9}$$

$$f(-3) = -36 \equiv 0 \pmod{9}$$

$$f(-4) = -75 \not\equiv 0 \pmod{9}$$

Hence $x = 1, 2, 6 \pmod{9}$ are solutions of the given congruence

SYSTEM OF LINEAR CONGRUENCE IN TWO VARIABLES

Consider a system of linear congruence in 2 variables is

$$ax + by \equiv r \pmod{n},$$

$$cx + dy \equiv s \pmod{n}$$

The system has a solution if $\text{GCD}(a, b, n) \mid c$

The system has a unique solution if $\text{GCD}(ad - bc, n) = 1$

EXAMPLES:

1) Solve the system of equations

$$7x + 3y \equiv 10 \pmod{16},$$

$$ad - bc = 35 - 6 = 29$$

$$2x + 5y \equiv 9 \pmod{16}$$

$$a = 7, \quad b = 3, \quad r = 10, \quad n = 16$$

$$c = 2, \quad d = 5, \quad s = 9,$$

$$\gcd(a, b, n) = \gcd(7, 3, 16) = 1$$

$$\gcd(ad - bc, n) = 1, \quad \gcd(29, 16) = 1$$

The system has a unique solution

$$7x + 3y \equiv 10 \pmod{16} \quad \times 5$$

$$2x + 5y \equiv 9 \pmod{16} \quad \times 3$$

$$29x \equiv 23 \pmod{16}$$

$$13x \equiv 7 \pmod{16}$$

$$\Rightarrow 16/(13x - 7)$$

$$\Rightarrow 13x - 7 \equiv 16k$$

$$\Rightarrow x \equiv (16k + 7)/13$$

if $k = 2$ gives integral value of x

$$x \equiv 3 \pmod{16}$$

$$7(3) + 3y \equiv 10 \pmod{16}$$

$$21 + 3y \equiv 10 \pmod{16}$$

$$3y \equiv -11 \pmod{16}$$

$$\Rightarrow 16/(3y + 11)$$

$$\Rightarrow 3y + 11 = 16k$$

$$\Rightarrow y = (16k - 11)/3$$

$$\text{if } k = 2, \quad y = 7$$

$$y \equiv 7 \pmod{16}$$

2) Solve the system of equations

$$5x + 6y \equiv 10 \pmod{13},$$

$$6x - 7y \equiv 2 \pmod{13}$$

$$a = 5, \quad b = 6, \quad r = 10, \quad n = 13$$

$$c = 6, \quad d = -7, \quad s = 2,$$

$$\gcd(a, b, n) = \gcd(5, 6, 13) = 1$$

$$\gcd(ad - bc, n) = 1, \quad \gcd(71, 13) = 1$$

The system has a unique solution

$$5x + 6y \equiv 10 \pmod{13} \quad \times 6,$$

$$ad - bc = -35 - 36 = -71$$

$$6x - 7y \equiv 2 \pmod{13} \quad \times 5$$

$$71y \equiv 50 \pmod{13}$$

$$6y \equiv 11 \pmod{13}$$

$$\Rightarrow 13 \mid (6y - 11)$$

$$\Rightarrow 6y - 11 \equiv 13k$$

$$\Rightarrow y \equiv (13k + 11)/6$$

if $k = 1$ gives integral value of y

$$y \equiv 4 \pmod{13}$$

$$5x + 6y \equiv 10 \pmod{13}$$

$$5x + 6(4) \equiv 10 \pmod{13}$$

$$5x + 24 \equiv 10 \pmod{13}$$

$$5x \equiv -14 \pmod{13}$$

$$\Rightarrow 13 \mid (5x + 1)$$

$$\Rightarrow 5x + 1 = 13k$$

$$\Rightarrow y = (13k - 1)/5$$

$$\text{if } k = 2, \quad x = 5$$

$$x \equiv 5 \pmod{13}$$

Wilson's Theorem

If p is a prime number, then

$$(p - 1)! \equiv -1 \pmod{p}$$

$$(p - 1)! \equiv (p - 1) \pmod{p}$$

$$(p - 2)! \equiv 1 \pmod{p}$$

$$(p - 3)! \equiv \frac{(p - 1)}{2} \pmod{p}$$

EXAMPLES

1) Find the remainder when $2(26)!$ is divisible by 29

$$P=29 \quad 29-26=3$$

$$(p - 3)! \equiv \frac{(p - 1)}{2} \pmod{p}$$

$$(29 - 3)! \equiv 14 \pmod{29}$$

$$26! \equiv 14 \pmod{29}$$

$$2(26)! \equiv 28 \pmod{29}$$

Remainder is 28.

2) Find the remainder when $4(29)!$ is divisible by 31

$$P=31 \quad 31-29=2$$

$$(p - 2)! \equiv 1 \pmod{p}$$

$$(31 - 2)! \equiv 1 \pmod{31}$$

$$29! \equiv 1 \pmod{31}$$

$$4(29)! \equiv 4 \pmod{31}$$

$$4(29)! + 5! \equiv 4 + 5! \pmod{31}$$

$$4(29)! + 5! \equiv 124 \pmod{31}$$

$$4(29)! + 5! \equiv 0 \pmod{31}$$

$4(29)! + 5!$ is divisible by 31

Euler's Theorem

For every a and n that are relatively prime $\gcd(a,n)=1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \text{Where } \phi(n) \text{ is Euler's totient function.}$$

EXAMPLES

1. Solve $3^{202} \pmod{13}$ by Euler's Theorem.

$$3^{12} \equiv 1 \pmod{13}$$

$$(3^{12})^{16} \equiv 1 \pmod{13}$$

$$3^{192} \equiv 1 \pmod{13} \quad (1)$$

$$3^3 \equiv 1 \pmod{13}$$

$$(3^3)^3 \equiv 1 \pmod{13} \quad (2)$$

$$3 \equiv 3 \pmod{13} \quad (3)$$

By equations (1), (2), (3)

$$\text{We have, } 3^{202} \equiv 3 \pmod{13}$$

12) 202(16

$$\begin{array}{r} 12 \\ 82 \\ \hline 72 \\ \hline 10 \end{array}$$

2. Solve $4^{99} \pmod{35}$ by Euler's Theorem.

$$4^{35} \equiv 1 \pmod{35}$$

$$4^{24} \equiv 1 \pmod{35}$$

$$(4^{24})^4 \equiv 1 \pmod{35} \quad (1)$$

$$4^3 \equiv 29 \pmod{35} \quad (2)$$

$$4^{99} \equiv 29 \pmod{35}$$

By equations (1), (2)

We have, $4^{99} \equiv 29 \pmod{35}$

24)99(4

$$\begin{array}{r} 96 \\ \hline 3 \end{array}$$

Fermat's Little Theorem

If p is a prime number and $(a, p) = 1$ then $a^{p-1} - 1$ is divisible by p

i.e., $a^{\phi(n)} \equiv 1 \pmod{n}$

EXAMPLES

1) Show that $2^{340} \equiv 1 \pmod{31}$ by Fermat's Little Theorem

Here $p=31$ and $a=2$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$2^{31-1} \equiv 1 \pmod{31}$$

$$2^{30} \equiv 1 \pmod{31}$$

$$(2^{30})^{11} \equiv 1 \pmod{31}$$

$$2^{330} \equiv 1 \pmod{31}$$

$$2^5 \equiv 1 \pmod{31}$$

$$(2^5)^2 \equiv 1^2 \pmod{31}$$

$$2^{10} \equiv 1 \pmod{31}$$

$$2^{330} \times 2^{10} \equiv 1 \pmod{31}$$

$$2^{340} \equiv 1 \pmod{31}$$

2)

Find the remainder when 41^{75} is divided by 3.

Here $p=3$

$$41 \equiv 2 \pmod{3}$$

$$(41)^{75} \equiv 2^{75} \pmod{3}$$

$$2^{3-1} \equiv 1 \pmod{3}$$

$$2^2 \equiv 1 \pmod{3}$$

$$(2^2)^{37} \equiv 1^{37} \pmod{3}$$

$$2^{74} \equiv 1 \pmod{3}$$

$$2^{75} \equiv 2 \pmod{3}$$

$$(41)^{75} \equiv 2 \pmod{3}$$

Remainder is 2.

RSA Algorithm

It is an asymmetric cryptographic algorithm

(2 keys) public and private key

Public key: known to all users in N/W

Private Key: Kept secret, not sharable to all

If public key of user A is used for encryption, we have to use the private key of same user for decryption.

The RSA scheme is a block cipher in which the plain text and cipher text are integers between 0 and $n-1$ for some n .

Key generation

- 1) Select 2 large prime numbers 'p' and 'q', $p \neq q$
- 2) Calculate $n = p * q$
- 3) Calculate $\phi(n) = (p - 1) * (q - 1)$
- 4) Choose value of e such that $1 < e < \phi(n)$ and $\gcd(\phi(n), e) = 1$
- 5) Calculate $d = e^{-1} \pmod{\phi(n)}$
 $de = 1 \pmod{\phi(n)}$
- 6) Public key = $\{e, n\}$
- 7) Private key = $\{d, n\}$

Encryption: $C = M^e \bmod n$

Decryption: $M = C^d \bmod n$

EXAMPLES:

- 1) Using RSA algorithm find public key and private key with respect to $p = 3, q = 11$ and $M = 31$

Let $p = 3, q = 11$ and $M = 31$

$$n = p * q = 3 * 11 = 33$$

$$\phi(n) = (p - 1) * (q - 1) = 2 * 10 = 20$$

So, let $e = 7$ as $1 < 7 < 20$ $\gcd(7, 20) = 1$

$$\text{Now } d = e^{-1} \bmod \phi(n)$$

$$de = 1 \bmod \phi(n)$$

$$7d = 1 \bmod 20$$

$$d = 3$$

Since $e = 7, d = 3$

Public key = $\{e, n\} = \{7, 33\}$

Private key = $\{d, n\} = \{3, 33\}$

Encryption: $C = M^e \bmod n$

$$C = 31^7 \bmod n$$

$$31 = -2 \bmod 33$$

$$31^7 = -2^7 \bmod 33$$

$$31^7 = -128 \bmod 33$$

$$31^7 = -(-4) \bmod 33$$

$$31^7 = 4 \bmod 33$$

$$C = 04 = AE$$

$$M = 31 = DB$$

Decryption: $M = C^d \bmod n$

$$M = 4^3 \bmod 33$$

$$4^3 = 64 \bmod 33$$

$$M = 31 \bmod 33$$

$$M = 31 = DB$$

- 2) Using RSA algorithm find public key and private key with respect to $p = 7, q = 11$ and $e = 13$ then what will be the value of d ?

Let $p = 7, q = 11$ and $M = 31$

$$n = p * q = 7 * 11 = 77$$

$$\phi(n) = (p - 1) * (q - 1) = 6 * 10 = 60$$

So, let $e = 13$ as $1 < 13 < 60$ $\gcd(13, 60) = 1$

$$\text{Now } d = e^{-1} \bmod \phi(n)$$

$$de = 1 \bmod \phi(n)$$

$$13d = 1 \bmod 60$$

$$60/13d - 1$$

$$13d - 1 = 60k$$

$$d = 37$$

Since $e = 7, d = 3$

Public key = $\{e, n\} = \{13, 77\}$

Private key = $\{d, n\} = \{37, 77\}$

3) Encode 'STOP' using RSA algorithm with key (2537, 13) and $p = 43, q = 59$

$$p = 43, q = 59$$

$$n = pq = 2537$$

$$\phi(n) = (p - 1) * (q - 1) = 42 * 58 = 2436$$

$$\gcd(2436, 13) = 1$$

$$M = \text{STOP} = 18191415$$

$$\text{Let } M_1 = 1819, M_2 = 1415$$

$$\text{Encryption} :: C = M^e \bmod n$$

$$C_1 = M_1^e \bmod n \Rightarrow C_1(1819)^{13} \bmod (2537)$$

$$C_1 = 2081$$

$$C_2 = M_2^e \bmod n \Rightarrow C_2(1415)^{13} \bmod (2537)$$

$$C_2 = 2182$$

$$c = C_1 C_2 = 2081 \ 2182$$

$$C = UHBYHC$$

