4·4 - LINEAR CONGRUENCES

A Congruence of the form

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

wher $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}$, and x is the variable, is called Linear Congruence.

To Solve a linear Congruence, we need to find all integers x that satify the Congruence. For the solution of the Congruence, we will use inverse.

REASON

Why do we use ~~this meth~~ Inverse to Solve Linear Congruence :

As with typical linear equation, such as

$$2x = 4$$

one method to solve this is to eliminate 2 on the left side. This could be done by multiplying the multiplicative inverse of 2 on each side.

As multiplicative inverse of 2 is $\frac{1}{2}$, so multiplying on both sides

$$\cancel{2}\cdot\frac{1}{\cancel{2}}x = \overset{2}{\cancel{4}}\cdot\frac{1}{\cancel{2}}$$

$x = 2$ is the Solution of this Linear Eq.

Multiplicative Inverse :

$a \cdot \bar{a} = 1$

$\bar{a}$ is called mul. inverse of a

EX: $2 \cdot \frac{1}{2} = 1$

$\frac{1}{2}$ is mul.inv. of 2

Similarly, to solve the Congruence

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

We need to eliminate a, and then solve it in normal way of Congruence. We will use inverse of a mod m to eliminate a on L·H·S. Suppose $\bar{a}$ is the inverse, so multiplying $\bar{a}$ on each side, we obtain

$$\cancel{\bar{a}}\cdot\cancel{a}x \equiv b\cdot\bar{a} \pmod{m}$$

$$x \equiv b\cdot\bar{a} \pmod{m}$$

Now, you can find all x that satifies this Congruence.

Note : That Inverse exists when a and m are relative primes.

INVERSE OF a MODULO m

Brute Force Algorithm : (useful for small m)

We look a multiple of a that exceeds a multiple of m by 1 .

Example :

Find inverse of 3 mod 7

Sol:-

i =	①	②	③	④	⑤	⑥
Multiple of 3 (i) :	3	6	9	12	$\boxed{15}$	18
Multiple of 7 (i) :	7	$\boxed{14}$	21	28	35	42

We can find $3\cdot i$ for $i = 1, 2, \cdots, 6$. Stopping when we find a multiple of 3 that is one more than multiple of 7

Multiple of 3, i.e. 15 , exceeds a multiple of 7, i.e 14 by 1.

i.e

$$3\cdot(5) = 7(2) + 1$$

Here 5 is the inverse of 3 modulo 7 .

Exhaustive Search:

$3\cdot(1) = 7(1) + (-4)$

$3\cdot(2) = 7(1) + (-1)$

$3\cdot(3) = 7(1) + 2$

$3\cdot(4) = 7\cdot(1) + 5$

$3\cdot(5) = 7(2) + \boxed{1}$

$=$

STOP HERE

$\bar{a}\cdot a = 1$ mod 7

✓ $5\cdot 3 = 1$ mod 7

Note :

other inverses are : found

$$-9, -2, \boxed{5}, 12, 19$$

$5 + 7 = 12$

$12 + 7 = 19$

$\vdots$

$5 - 7 = -2$

$-2 - 7 = -9$

$\vdots$

We can speed up this approach up if we note that

$3\cdot(1) = 7(1) + (-4)$

$3\cdot(2) = 7(1) + (-1) \longrightarrow 3\cdot(-2) = 7(-1) + 1$

fullfil the remainder 1 requirment.

As $3\cdot(-2) = 7(-1) + 1$

So, -2 is also the inverse of 3 mod 7

and other inverses could be found from this as :

$-2 + 7 = 5$

$5 + 7 = 12$

$\vdots$

INVERSE OF a MODULO m : (Efficient Algorithm)

We can design a more efficient algorithm than bruteforce to find inverse of a modulo m when $\gcd(a, m) = 1$ using the steps of Euclidean algorithm.

By reversing these steps, we can find a linear combination $sa + tm = 1$, where s and t are integers.

Reducing both sides of this equation modulo m tells us that s is an inverse of a modulo m.

> If $\bar{a} \cdot a = 1 \bmod m$
>
> then Integer $\bar{a}$ is said to be inverse of a modulo m

THEOREM:

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists.

Furthermore, this inverse is unique modulo m.
(that is, there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m, and every other inverse of a modulo m is congruent to $\bar{a}$ mod m.)

Proof: Suppose we have a and m are relatively primes i.e.,

$$\gcd(a, m) = 1$$

Bezout theorem

An we Know that greatest Common divisor can be expressed as Linear Combination. So, we Can express 1 as Linear Combination as

$$sa + tm = 1 \quad \text{where } s \text{ and } t \text{ are integers.}$$

- ⊙ 1 Can be written as 1 mod m
- ⊙ $tm = 0$ (as m is mod, so any multiple of m will be Zero.)
  if $m=5$ $2 \cdot 5 = 10$ remainder 0

So, above equation becomes:

$$Sa + tm = 1 \bmod m$$
$$Sa + 0 = 1 \bmod m$$
$$S \cdot a = 1 \bmod m$$

, So S is inverse of a mod m

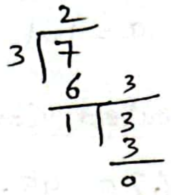
So, this theorem guarantees that an inverse of a mod m exists whenever a and m are relatively prime.

Example :-

Find an inverse of 3 modulo 7 by using efficient method.

Sol: First we use Euclidean algorithm to show that $\gcd(3,7)=1$

The steps used by Euclidean algorithm to find gcd(3,7) are :



$$7 = 2\cdot 3 + 1$$
$$3 = 3\cdot 1 + 0$$

As the last non-zero remainder is 1, so

$$\gcd(3,7)=1$$

We can now find the Bézout Coefficients for 3 and 7 by working backwords.

$1 = 7 - 2\cdot 3$ (as $7 = 2\cdot 3+1$)

or $1 = 1\cdot 7 - 2\cdot 3$ (1 and −2 are Bézout Coefficients of 3 mod 7.)

$1 \bmod 7 = 0 - 2\cdot 3$

$1 \bmod 7 = -2\cdot 3$ or $-2\cdot 3 = 1 \bmod 7$

So, −2 is an inverse of 3 mod 7.

NOTE : As −2 is an inverse of 3 mod 7, then Every integer Congruent to −2 modulo 7 is also an inverse of 3, Such as 5, −9, 12 and so on

$\bar{a}\cdot a \equiv 1 \bmod m$

$\bar{a}\cdot 3 \equiv 1 \bmod 7$

For $\bar{a}=5$

$5\cdot 3 \equiv 1 \bmod 7$

$\Rightarrow 7 \mid 5\cdot 3-1$ or $\frac{15-1}{7}$ =(true) yes it divides

For $\bar{a}=-2$

$-2\cdot 3 \equiv 1 \bmod 7$

$7 \mid -2\cdot 3 - 1$ or $7 \mid -6-1$

$\Rightarrow \frac{-7}{7}$ = (true)

Similarly for 12 etc.

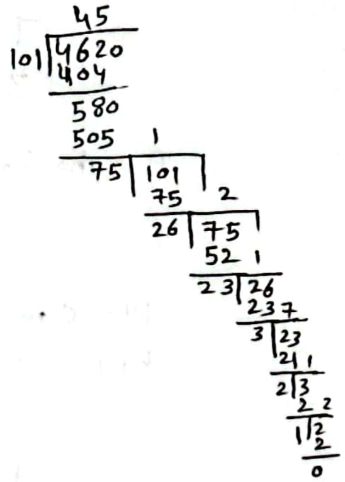
Example:-

Find an inverse of 101 modulo 4620

Sol:-

$a = 101 \qquad m = 4620$

Greatest Common Divisor:



$$4620 = 45\cdot 101 + 75$$
$$101 = 1\cdot 75 + 26$$
$$75 = 2\cdot 26 + 23$$
$$26 = 1\cdot 23 + 3$$
$$23 = 7\cdot 3 + 2$$
$$3 = 1\cdot 2 + \boxed{1}$$
$$2 = 2\cdot 1$$

So, $\gcd(4620, 101) = 1$

Bézout Coefficients:

$$1 = 3 - 1\cdot \underline{\underline{2}}$$
$$= 3 - 1\cdot(23 - 7\cdot 3) = 1\cdot 3 - 1\cdot 23 + 7\cdot 3$$
$$= -1\cdot 23 + 8\cdot \underline{\underline{3}}$$
$$= -1\cdot 23 + 8(26 - 1\cdot 23) = -1\cdot 23 + 8\cdot 26 - 8\cdot 23 = +8\cdot 26 - 9\cdot 23$$
$$= 8\cdot 26 - 9\cdot \underline{\underline{23}}$$
$$= 8\cdot 26 - 9\cdot(75 - 2\cdot 26) = 8\cdot 26 - 9\cdot 75 + 18\cdot 26$$
$$= -9\cdot 75 + 26\cdot \underline{\underline{26}}$$
$$= -9\cdot 75 + 26\cdot(101 - 1\cdot 75) = -9\cdot 75 + 26\cdot 101 - 26\cdot 75$$
$$= 26\cdot 101 - 35\cdot \underline{\underline{75}}$$
$$= 26\cdot 101 - 35\cdot(4620 - 45\cdot 101) = 26\cdot 101 - 35\cdot 4620 + 1601\cdot 101$$
$$1 = \overset{t}{-35}\cdot \overset{m}{4620} + \overset{s}{1601}\cdot \overset{a}{101}$$

-35, 1601 are Bezout Coefficients

So, 1601 is an inverse of 101 modulo 4620.

Note:-

Suppose we have

$$ax \equiv b \pmod m$$

once, we have an inverse $\bar{a}$ of a modulo m, we can solve

$$ax \equiv b \pmod m$$

by multiplying $\bar{a}$ on both sides as:

$$\cancel{\bar{a}}\cdot \cancel{a}\, x = b\cdot \bar{a} \pmod m \qquad (\text{as } \bar{a}\cdot a = 1 \bmod m)$$
$$x = b\cdot \bar{a} \pmod m$$

SOLUTION OF LINEAR CONGRUENCE :-

① Find gcd(a,m)

② Find Inverse

③ Solve Congruence

Example :

What are the solutions of linear Congurence

$$3x \equiv 4 \bmod 7$$

Sol:-

$3x \equiv 4 \bmod 7$ (here $a=3$; $m=7$)

① $\gcd(3,7) = ?$

$7 = 2 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$ $\Rightarrow \gcd(3,7) = 1$, Inverse exists

② Inverse ?

$1 = 7 - 2 \cdot 3$

$1 = 1 \cdot 7 - 2 \cdot 3$ -2 is an inverse of 3 modulo 7.

③ Solution :

$3x \equiv 4 \pmod 7$

Multiply -2 on both sides

$-2 \cdot 3x \equiv 4 \cdot -2 \pmod 7$

$x \equiv -8 \pmod 7$

(as -2 is inverse of 3, So Cancel each other or

$-2 \cdot 3 \equiv 1 \bmod 7$

$-6 \equiv 1 \bmod 7$

$\equiv$ remainder 1

$= 1$

Solutions :

Values of x: $-8, -1, \boxed{6}, 13, 20$: 6 is the smallest positive Solution

Typically, we Choose first +ve Solution to write Congruence.

$x \equiv 6 \bmod 7$: where 6 is the Solution of Linear Congruence $3x \equiv 4 \bmod 7$

Verification :

Linear Congruence

$3x \equiv 4 \bmod 7$

Check for solution $x = 6$

$3 \times 6 \equiv 4 \bmod 7$

$18 \equiv 4 \bmod 7$ (18 is Congruent 4 modulo 7)

$7 \mid 18-4$ or $7 \mid 14$:True

Similarly $x = -8$

$-24 \equiv 4 \bmod 7$ $\Rightarrow$ $7 \mid -24-4$ or $7 \mid -28$:True

Example: Find the Solutions of the Linear Congruence

$$13x = 6 \pmod{37}$$

Sol:-

① $\gcd(13, 37)$: $a = 13$, $m = 37$

$37 = 13 \cdot 2 + 11$
$13 = 11 \cdot 1 + 2$
$11 = 2 \cdot 5 + 1$
$2 = 1 \cdot 2 + 0$ $\Rightarrow \gcd(13, 37) = 1$ So, inverse exists.

②

$$1 = 11 - \underline{\underline{2}} \cdot 5 =$$
$$= 11 - 5 \cdot (13 - 1 \cdot 11) = 1 \cdot 11 - 5 \cdot 13 + 5 \cdot 11$$
$$= -5 \cdot 13 + 6 \cdot \underline{\underline{11}}$$
$$= -5 \cdot 13 + 6 \cdot (37 - 2 \cdot 13) = -5 \cdot 13 + 6 \cdot 37 - 12 \cdot 13$$

$1 = 6 \cdot 37 - 17 \cdot 13$ $\bar{a} = -17$ is inverse of 13 mod 37

③ Multiply −17 on both sides of Linear Congruence

$$13x \equiv 6 \pmod{37}$$
$$-17 \cdot 13x \equiv 6 \cdot -17 \pmod{37}$$
$$x \equiv -102 \pmod{37}$$

: (as $-17 \cdot 13 = -221$
$-221 \bmod 37 = 1 \bmod 37$)
or $-\cancel{17} \cdot \cancel{13}$ Cancel each other

other Solutions:

$-102 + 37 = -65$
$-65 + 37 = -28$
$-28 + 37 = 9$.
$9 + 37 = 46$

Values of x (Solution of ~~K~~Linear Congruence:
$-102, -65, -28, 9, 46, \ldots$

or $x \equiv -102 \pmod{37}$ Can also be written as

$x \equiv 9 \pmod{37}$ where $x = 9$ is the one Solution of Linear Congruence.

Verification:

Linear Congruence:

$$13x \equiv 6 \bmod (37)$$

$x = 9$

$$13 \cdot 9 \equiv 6 \pmod{37}$$
$$117 = 6 \pmod{37}$$
$$37 \mid 117 - 6 \text{ or } 37 \mid 111 \text{ : True as } \frac{111}{37} = 3 \in \mathbb{Z}$$

So, $x = 9$ Satisfies the Congruence.

THE CHINESE REMAINDER THEOREM

In the first century, the Chinese mathematician Sun-Tsu asked:

> There are certain things whose number is unknown.
> When divided by 3, the remainder is 2;
> When divided by 5, the remainder is 3; and
> When divided by 7, the remainder is 2.
>
> What will be the number of things?

This puzzle can be translated into the following question:
What are the solutions of the systems of congruences

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7} \; ?$$

We will solve this system of Linear Congruences using Chinese Remainder Theorem.

THEOREM: The Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdots m_n$.
(That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent ~~to~~ modulo m to this solution.)

you can find the solution of above n ~~linear~~ congruences system by the formula:

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}) \bmod M$$

APPLICATIONS:

- ⊙ systems of Linear Congruences are the basis for a method that can be used to perform arithmetic with large integers.

Example :-

Solve the following system of linear Congruences using Chinese Remainder Theorem :

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

Sol : There is unique solution x computed by the following formula only when $(m_1, m_2, m_3) = (2, 5, 7)$ are relatively primes.

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

We have :

$a_1 = 2$ $\quad$ $m_1 = 3$
$a_2 = 3$ $\quad$ and $\quad$ $m_2 = 5$
$a_3 = 2$ $\quad$ $m_3 = 7$

We have to find :

$M_1 = ?$ $\quad$ $M_1^{-1} = ?$
$M_2 = ?$ $\quad$ $M_2^{-1} = ?$ $\quad$ and $M = ?$
$M_3 = ?$ $\quad$ $M_3 = ?$

$$M = m_1 \times m_2 \times m_3$$
$$= 3 \times 5 \times 7$$
$$= 105$$

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

$\boxed{M_1^{-1} = ?}$ (Inverse of M_1 mod 3 i.e., Inverse of 35 modulo 3)

$M_1 = 35$

$35 (?) \equiv 1 \bmod 3$ $\quad$ (as $35 \cdot M_1^{-1} = 2 \bmod m_1$)

$35 (2) \equiv 1 \bmod 3$, So 2 is the inverse of M_1 modulo 3

$\Rightarrow \boxed{M_1^{-1} = 2}$

$\boxed{M_2^{-1} = ?}$

$M_2 = 21$

$21 (?) \equiv 1 \bmod 5$ $\quad$ (as $21 \cdot M_2^{-1} = 1 \bmod m_2$)

$21 (1) \equiv 1 \bmod 5$, So 1 is the inverse of M_2 modulo 5

$\Rightarrow \boxed{M_2^{-1} = 1}$

$M_3^{-1} = ?$ (Inverse of M_3 modulo 7)

$M_3 = 15$

$15 (?) \equiv 1 \bmod 7$ $\quad$ (as $M_1 \cdot M_1^{-1} = 1 \bmod m_3$)

$15 (1) \equiv 1 \bmod 7$, So 1 is the inverse of M_3 modulo 7.

$\Rightarrow \boxed{M_3^{-1} = 1}$

The Solutions to this system are those x such that

$$x \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$
$$\equiv (2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1) \bmod 105$$
$$\equiv (140 + 63 + 30) \bmod 105$$

$$\begin{array}{r|l} & 2 \\ 105 & 233 \\ & 210 \\ \hline & \boxed{23} \end{array}$$

$x \equiv 233 \bmod 105$ $\quad$ or $\quad$ $x \equiv 23 \bmod 105$ $\quad$ $(0 \leq x < M)$

$x \equiv 233 \bmod m$

$x \equiv 23 \bmod 105$ $\quad \ldots, -82, \boxed{23}, 128, 233, 338$

It follows that 23 is the smallest positive integer that is Simultaneously Solution.

We Conclude that

23 is the smallest positive integer that leaves

⊙ a remainder 2 when divided by 3

⊙ a remainder 3 when divided by 5

⊙ a remainder 2 when divided by 7

puzzle Solved.

1. $x \equiv 2 \bmod 3$
   $23 \equiv 2 \bmod 3$ (as $3|21$)
   (Verified)
2. $x \equiv 3 \bmod 5$
   $23 \equiv 3 \bmod 5$ (as $5|20$)
   (verified)
3. $x \equiv 2 \bmod 7$
   $23 \equiv 2 \bmod 7$ (as $7|21$)
   verified

Example :

Solve the following system of Congruences:

$$4x \equiv 5 \pmod 9$$
$$2x \equiv 6 \pmod{20}$$

Sol:- First we Convert ~~into~~ the following

$$ax \equiv b \bmod m$$

into

$$\bar{a}ax \equiv b \cdot \bar{a} \bmod m$$
$$x \equiv b \cdot \bar{a} \bmod m$$

Now, you Can solve it by Chinese Remainder Theorem.

$4x \equiv 5 \bmod 9$ reduces to $x \equiv 35 \pmod 9$ or $x \equiv 8 \pmod 9$

$2x \equiv 6 \pmod{20}$ reduces to $x \equiv 3 \pmod{20}$

Now you Can Solve the following System using CRT.

$$x \equiv 8 \pmod 9$$
$$x \equiv 3 \pmod{20}$$

9 and 20 are relatively primes.

(Lef~~te~~ it as an exercise)

COMPUTER ARITHMETIC WITH LARGE INTEGERS :

Suppose that

$m_1, m_2, \cdots, m_n$ are pairwise relatively primes and

Let m be their product.

By Chinese remainder theorem, we can show that

an integer a with $0 \leq a < m$, can be uniquely represented by n-tuple Consisting of its remainders upon division by m_i, $i = 1, 2, \cdots, n$.

i.e.,

We can uniquely represent a by

$(a \bmod m_1, a \bmod m_2, \cdots, a \bmod m_n)$: # equal to n-tuples

Example:

Add 123684 and 413456

Sol:-

Suppose we have a certain processor that perform arithmetic with integers less than 100 and we want to add two large integers on that processor.

We can restrict almost all our Computations to integers less than 100 if we represent integers using their remainders modulo pairwise relatively prime integers less than 100.

First, find pairwise relatively primes less than 100.

relatively prime pairwise : $\overset{m_1}{99}, \overset{m_2}{98}, \overset{m_3}{97}, \overset{m_4}{95}$

(No two have a common factor greater than 1)

By the Chinese Remainder Theorem,

Every non-negative integer less than $99 \cdot 98 \cdot 97 \cdot 95 = 89403930$ Can be represented uniquely by its remainders when divided by these four moduli.

⊛ 123684 Can be represented as :

(123684 modulo 99, 123684 modulo 98, 123684 modulo 97, 123684 modulo 95)

(123684) as (33, 8, 9, 89) —— Ⓐ

⊛ 413456 Can be represented as :

(413456 mod 99, 413456 mod 98, 413456 mod 97, 413456 mod 95)

(413456) as (32, 92, 42, 16) —— Ⓑ

To find the Sum of 123684 and 413456, we work with these 4-tuples instead of these two Large integers

We add the 4-tuple Componentwise

$$(33, 8, 9, 89) + (32, 92, 42, 16) = (65, 100, 51, 105)$$

Reduce each component with respect to the appropriate moduli.

$$= (65 \bmod 99, 100 \bmod 98, 51 \bmod 97, 105 \bmod 95)$$

$$= (65, 2, 51, 10)$$

To find the Sum, that is, the integer represented by $(65, 2, 51, 10)$, we need to solve the System of Congruences:

$$x \equiv 65 \pmod{99}$$
$$x \equiv 2 \pmod{98}$$
$$x \equiv 51 \pmod{97}$$
$$x \equiv 10 \pmod{95}$$

$$x \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + a_4 M_4 M_4^{-1}) \bmod M$$

$$M = 99 \times 98 \times 97 \times 95 = 89403930$$

$$M_1 = \frac{M}{m_1} = \frac{89403930}{99} = 903070$$

$$M_2 = \frac{M}{m_2} = \frac{89403930}{98} = 912285$$

$$M_3 = \frac{M}{m_3} = \frac{89403930}{97} = 921690$$

$$M_4 = \frac{M}{m_4} = \frac{89403930}{95} = 941094$$

Find Inverse using Euclidean Algo.

37 is inverse of M_1 modulo 99

33 " " " M_2 " " 98

24 " " " M_3 " " 97

4 " " " M_4 " " 95

$\Rightarrow M_1^{-1} = 37, M_2^{-1} = 33, M_3^{-1} = 24, M_4^{-1} = 4$

$$x \equiv (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} + a_4 M_4 M_4^{-1})$$

$$\equiv (65 * 903070 * 37 + 2 * 912285 * 33 + 51 * 921690 * 24 + 10 * 941094 * 4) \bmod 89403930$$

$$x \equiv 3,397,886,480 \pmod{89403930}$$

$$x \equiv 537140 \pmod{89403930}$$

: AS
$3,397,886,480 - (38)(89403930)$
$= 3,397,886,480 - 3,397,349,340$
$= 537140$

Solution : $x = 537140$

(verification : $123684 + 413456 = 537140$)

FERMAT'S LITTLE THEOREM

- It allows us to find a remainder when we divide huge number by a prime.
- This theorem is extremely usefull when dealing with large numbers that even a Calculator cannot compute

It states that

P divides $a^{P-1} - 1$ whenever P is prime and a is an integer not divisible by P.

In terms of Congruence, we state this theorem as:

If P is prime and a is an integer not divisible by P (i.e a and P have no common factor)

then $a^{P-1} \equiv 1 \bmod P$ or (For every integer a, we have $a^P \equiv a \bmod P$, as $\gcd(a,P)=1$)

Let's start with a small number, so you can see how it works.

Example: $a = 2$, $P = 5$

By Fermat's theorem

$$a^{P-1} \equiv 1 \bmod P$$

$$2^{5-1} \equiv 1 \bmod 5$$

$$2^4 \equiv 1 \bmod 5$$

$16 \equiv 1 \bmod 5$ YES it works

(As 5 is prime & 2 is not disible by 5. i.e. ~~As~~ $\gcd(2,5)=1$ then $2^{5-1} \equiv 1 \bmod 5$ holds)

Lets take a huge number that even our Calcutator Couldn't Compute it.

Example: Find $2^{502} \bmod 5$

As $P=5$, $a=2$

Fermat's Little theorem says:

$$a^{P-1} \equiv 1 \bmod P$$

$$2^4 \equiv 1 \bmod 5 \quad Ⓐ$$

(i.e we know that 2 remainder is 1 when ~~5|16~~ 5 divides 2^4)

We have to find $2^{502} \bmod 5$

$$2^{502} = 2^{125*4+2} = (2^4)^{125} \cdot 2^2 \equiv (1)^{125} \cdot 2^2 \bmod 5 \quad \left(\text{as } 2^4 \equiv \underset{\text{Remainder}}{\boxed{1}} \bmod 5\right) \text{ By eq Ⓐ}$$

$$\equiv \left((1)^{125} \bmod 5 \cdot 2^2 \bmod 5\right) \bmod 5$$

$$\equiv (1 \cdot 4 \bmod 5) \bmod 5 \equiv \boxed{4} \bmod 5$$

So, $2^{502} \bmod 5 = 4$

PROCEDURE:

How we can use Fermat's Little theorem to Compute $a^n \bmod P$, Wher P is prime and $P \nmid a$ i.e., $\gcd(a, P) = 1$.

This procedure shows:

To find $a^n \bmod P$, we only need to Compute $a^r \bmod P$.

{i.e this theorem allows us to find remainder when we divide huge number by a prime.}

In other words, we are going to reduce $a^n \bmod P$ to $a^r \bmod P$.

To compute $a^n \bmod P$:

We use division algorithm when n is divided by $P-1$

$$n = 2(P-1) + r \qquad (0 \leq r < P-1)$$

$$\begin{array}{r|l} & 2 \\ P-1 & \overline{n} \\ & \underline{} \\ & r \end{array}$$

So,

$$a^n = a^{2(P-1)+r} = (a^{P-1})^2 \cdot a^r \equiv (1)^2 \cdot a^r \pmod P \qquad (\text{as } a^{P-1} \equiv 1 \bmod P)$$

$$\equiv 1 \cdot a^r \pmod P$$

$$a^n \equiv a^r \pmod P$$

So, a^r is the remaind of $a^n \bmod P$

NOTE:

If you want to find the result of $a^n \bmod P$ (In case of huge a^n you can't find it). You can easily Calculate it by using $a^r \bmod P$.

Another Example:

Find $7^{222} \bmod 11$

Sol: As $P = 11$ and $a = 7$, and $\gcd(7, 11) = 1$, So

By Fermat's theorem, we have.

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

$$7^{11-1} \equiv 1 \pmod{11} \text{ --- (A)}$$

: (We will use this ~~[illegible]~~ result to find $7^{222} \bmod 11$)

So, it can be written as

$$7^{222} = 7^{22 \times 10 + 2} = (7^{10})^{22} \cdot 7^2 \equiv (1)^{22} \cdot 7^2 \bmod 11$$

$$\equiv 1 \cdot \boxed{7^2} \bmod 11 \qquad a^r$$

$$\equiv 49 \bmod 11$$

So, 49 is the remainder, when we Calculate $7^{222} \bmod 11$.

PSEUDOPRIMES

PRIMALITY TEST:

(Brute Force):

An integer n is prime when it is not divisible by any prime with $p \leq \sqrt{n}$.

This brute force algorithm is inefficient as: it requires to find all primes not exceeding $\sqrt{n}$ and to carry out trial division by each such prime.

Are there more efficient ways to determine whether an integer is prime?

Ancient chinese mathematician believed that

n was an odd prime if and only if

$$2^{n-1} \equiv 1 \bmod n$$

i.e.,

If n is odd prime, then $2^{n-1} \equiv 1 \bmod n$ (PART 1)

If $2^{n-1} \equiv 1 \bmod n$, then n is odd prime (PART 2)

If this were true, it would provide an EFFICIENT Primality test.

The ancient Chinese Mathematicians were only partially Correct.

They were Correct in thinking that

Congruence holds whenever n is prime (PART 1).

(By Fermat's little theorem, we know $2^{n-1} \equiv 1 \bmod n$ whenever n is prime)

But they were incorrect in Concluding that

n is necessarily prime if the Congruence holds (PART 2)

UNFORTUNATELY,

There are composite integers n such that $2^{n-1} \equiv 1 \pmod{n}$

Such integers are Called PSEUDOPRIMES to the base 2.

For example:

Consider $n = 341$

As $341 = 11 \cdot 31$, so it is composite.

It also satisfies the following Congruence

$$2^{n-1} \equiv 1 \bmod n$$

$$2^{340} \equiv 1 \bmod 341 \text{ :holds}$$

So, integer 341 is pseudoprime to base 2.

As $a^{p-1} \equiv 1 \bmod (p)$

or $a^{p} \equiv a \bmod p$

in case of Composite, we write

$a^{n} = a \bmod n$

$\Rightarrow n \mid a^{n} - a$

i.e $341 \mid 2^{341} - 2$

Computers can have method to make this calculation easier

$2^{341} - 2 = 44794844 \cdots\cdots$: divisible by 341

We have seen that

341 divides $2^{341} - 2$ (i.e. divides if base is 2)

~~But~~
So 341 is pseudoprime to the base 2. (Even 341 does not pass the test for base 3)

~~34~~ $3^{341} - 3 = 49928424196$ .... : not divisible by 341

Even though 341 is a psedoprime as it divides $2^{341} - 2$ (i.e $2^{341} \equiv 2 \bmod 341$)

Definition of Psuedoprime:

Let b be a positive integer. If n is a Composite positive number, and $b^{n-1} \equiv 1 \pmod{n}$, then n is called pseudoprime to the base b.

We Conclude :

If n satifies the Congruence $2^{n-1} \equiv 1 \bmod n$, then it is either prime or a pseudoprime to the base 2 (because it is a useful test that provides some evidence)

If n does not satify the Congruence $2^{n-1} \equiv 1 \bmod n$, then it is Composite.

NOTE :

Among the positive integers less than 10^{10}, there are 455,052,512 primes but only 14,884 pseodoprimes to the base 2.

(Unfortunately we cannot distinguish between primes and pseudoprimes just by choosing sufficiently many bases, because

There are Composite numbers that passes all tests with bases b such that $\gcd(b,n) = 1$. This leads to another type of number i.e Carmichael.

CARMICHAEL NUMBER

A Composite integer n that satifies the Congruence $b^{n-1} \equiv 1 \bmod n$ for all positive integers b with $\gcd(b,n) = 1$ is called Carmichael number.

Example:

Integer 561 is a Carmichael number (First Carmichael number)

Sol:

$$\begin{array}{r|l} 3 & 561 \\ \hline 11 & 187 \\ \hline & 17 \end{array}$$

561 is Composite as $561 = 3 \cdot 11 \cdot 17$

Next note that if $\gcd(b, 561) = 1$, then

$$\gcd(b, 3) = \gcd(b, 11) = \gcd(b, 17) = 1$$

Using Fermat theorem, we find that

$$b^{2} \equiv 1 \bmod 3$$

$$b^{10} \equiv 1 \bmod 11$$

$$b^{16} \equiv 1 \bmod 17$$

It follows that

$$b^{560} = \cancel{(b^{2})}\ b^{280*2+0} = (b^{2})^{280} \equiv 1 \cdot \bmod 3$$

$$b^{560} = b^{56*10+0} = (b^{10})^{56} \equiv 1 \cdot \bmod 11$$

$$b^{560} = b^{35*16+0} = (b^{16})^{35} \equiv 1 \bmod 17$$

It follows that

$b^{560} \equiv 1 \pmod{561}$ for all positive integers with $\gcd(b, 561) = 1$

Hence, 561 is a Carmichael number. (passes test for all bases)