Modular Arithmetic

Def^n:- If a and b are integers and m is a positive integer, then a is ~~congruent~~ congruent to b modulo m if m divides $a-b$. It is denoted by $a \equiv b \pmod{m}$.

i.e a congruent to b modulo m.

Here $a \equiv b \pmod{m}$ is congruence and m is its modulus. i.e $\Rightarrow m \mid a-b$

If a and b are not congruent modulo m, we write

$$a \not\equiv b \pmod{m}$$

Here $a \equiv b \pmod{m}$ ⟶ represent a rel^n on the set of integers

[$a \bmod m = b$ ⟶ represents a y^n.] → after that previous huge theorem

Th^m:- Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

Ex^p:- Determine whether 17 is congruent to 5 modulo 6 and whether 24 & 14 are congruent modulo 6.

Sol^n:- ~~Check (a) (b)~~ For check $17 \equiv 5 \pmod{6}$

first we check $6 \mid 17-5 = 12 \Rightarrow 6 \mid 12$

$\Rightarrow 17 \equiv 5 \pmod{6}$

Now $6 \mid 24-14 = 10 \Rightarrow 6 \nmid 10$.

$\Rightarrow 24 \not\equiv 14 \pmod{6}$.

Primes and Composite Numbers

Def:- An integer p greater than 1 is called prime if the only positive factors of p are 1 and p.

A positive integer that is greater than 1 and is not prime called composite. Ex, 4, 6, 8, 9, 10, 12

Ex, 2, 3, 5, 7, 11, 13, 17, ——

The fundamental theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.

Ex:- Write the prime factorisation of 99, 100, 641, 1024 —

$99 = 3 \cdot 3 \cdot 11 = 3^2 \cdot 11$

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$

$641 =$ → prime 641

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Thm:- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Note: Smallest prime is 2.
odd — 3.

Ex 4 → is a composite no. it has a prime divisor 2
$\leq \sqrt{4} = 2$

~~Theorem: A prime number of the form ... it is~~

Note:- A prime number of the form $2^p - 1$, where p is prime called Mersenne primes.

& $2^n - 1$ is not prime when n is not prime.

except that $2^{11} - 1$ is is not Mersenne prime

bez $2^{11} - 1 = 2047 = 23 \cdot 89 \rightarrow$ not a prime no.

$2^2 - 1 = 4 - 1 = 3$, $2^3 - 1 = 8 - 1 = 7$

* There are infinitely many primes

Qus Show that 101 is prime.

Sol:- By using proof by contradiction let assume that $\neg p$ i.e 101 is a composite ($\neg p$ is false $\Rightarrow p$ is true)

(if a no. is not prime then it is composite).

Since 101 is a composite number then it has prime divisor less than or equal to $\sqrt{101}$. (by theorem)

Since the primes less than or equal to $\sqrt{101}$ are either 2, 3, 5 or 7 only (≤ 10)

That means 101 is divisible by either 2, 3, 5 or 7 ($\sqrt{100} = 10$)

but it is not divisible by either 2, 3, 5 or 7 ($\sqrt{101}$ something 10.1)

i.e 101 is not divisible by any prime less than or equal to $\sqrt{101}$.

$\Rightarrow$ 101 is not composite $\Rightarrow$ 101 is prime.

Pr

GCD (Greatest common divisor) :- (i.e $a, b \neq 0$)

Let a and b be integers, not both zero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b. denoted by $\gcd(a, b)$.

Ex:- ① Find $\gcd(24, 36) = 12$

② $\gcd(17, 22) = 1$

③ $\gcd(17, 17) = 1$

Def:- The integer a and b are relatively prime if (or co prime)
$\gcd(a, b) = 1$

Ex: Both are RP

Defn:- The integers $a_1, a_2, \ldots a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Ex: 10, 17, 21 → check they are pairwise RP or not

LCM (Least Common Multiple):- The LCM of the positive integers a and b is the smallest positive integer that is divisible by both a and b. denoted by $\text{lcm}(a, b)$.

Thm: Let a and b positive integers. Then
$ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

Ex: 9, 5

$9 \cdot 5 = \gcd(9, b) \cdot \text{lcm}(9, b)$

$= 1 \cdot 45 = 45$

(20, 29)

Euclidean Algorithm:- (A more efficient method of finding the gcd, called then EA).

Let $a = bq + r$, where a, b, q and r are integers.

Then $\gcd(a, b) = \gcd(b, r)$.

Ex:- Find gcd of 414 and 662 using the Euclidean algorithm.

Method:- Let we have to find $\gcd(a, b)$ let $a < b$ so if we divide a by b we have some remainder r_1 (let) $(b = ak + r_1)$ further divided a by first remainder r_1 i.e. and find second remainder. $(i.e\ a = r_1 \cdot k + r_2)$

Further, divide r_1 by r_2 and find third remainder r_3. Repeat this process till the remainder becomes zero.

So, The last non-zero remainder is the gcd (a, b) this method is called Euclidean algorithm

Sol$^{n.}_{2}$ $\gcd(414, 662)$

$a = 414,\ b = 662,\ a < b$

So, $662 = 414 \cdot 1 + 248$

$r_1 = 248$

$414 = 248 \cdot 1 + 166$

$r_2 = 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

$82 = 2 \cdot 41 + 0$

now remainder is zero

last non-zero remainder is 2

$\Rightarrow \gcd(414, 662) = 2$

Gcd as Linear Combination :-

The gcd of two integers a and b can be expressed in the form $sa + tb$ where s and t are integers.

i.e gcd (a, b) can be expressed as a linear combination with integer coefficients of a and b.

Ex:- $\gcd(6, 14) = 2$

so $2 = s \cdot a + t \cdot b = s \cdot 6 + t \cdot 14$

$$\boxed{2 = (-2) \cdot 6 + 1 \cdot 14}$$

Theorem Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$

Ex: $14 \equiv 8 \pmod{6}$

$7 \cdot 2 = 4 \cdot 2 \pmod{6}$

$14 \equiv 4 \pmod{5}$

$7 \cdot 2 = 2 \cdot 2 \pmod{5}$

$a \cdot c = b \cdot c \pmod{m}$

$\Rightarrow c = 2$

and $\gcd(2, 5) = 1$

$\Rightarrow 7 = 2 \pmod{5}$

BÉZOUT'S Theorem:- If a and b are positive integers, then $\exists$ s and t such that $\gcd(a,b) = sa+tb$

Def^n: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa+tb$ are called Bézout coefficients of a and b

and the eqn $\gcd(a,b) = sa+tb$ is called Bézout's identity → ↓ This is also called Linear combination of $\gcd(a,b) = d$ (say)

i.e $d = sa+tb$.

How to find Bézout's coefficients of positive integers using EA –

Qus: Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198

Sol^n: First find $\gcd(252, 198)$ by using EA

$a = 252, b = 198 \quad b < a$

① ~ $252 = 198 \cdot 1 + 54$, $r_1 = 54$

$198 = 54 \cdot 3 + 36$, $r_2 = 36$

$54 = 1 \cdot 36 + 18$, $r_3 = 18$

$36 = 2 \cdot 18 + 0$, $r_4 = 0$

non-zero remainder is 18 $\Rightarrow d = \gcd(252, 198) = 18$

Now find the value of each non-zero remainder

Eg.

$54 = 252 - 1 \cdot 198$ (for $252 = 198 \cdot 1 + 54$)

$36 = 198 - 3 \cdot 54 = 198 - 3(252 - 1 \cdot 198)$ (Put value

$36 = 198 - 3\cdot 252 + 3\cdot 198 = 4\cdot 198 - 3\cdot 252$

$18 = 54 - 1\cdot 36$

$= (252 - 1\cdot 198) - 1\cdot(4\cdot 198 - 3\cdot 252)$

$= 4\cdot 252 - 5\cdot 198 = 4\cdot 252 - 5\cdot 198$

i.e $s = 4,\ t = -5$

$\gcd(252, 198) = 18 = 4\cdot 252 - 5\cdot 198$

Bézout's Lemma:- If a and b are co-prime then $d = \gcd(a,b) = 1$ can be written as a LC.

$1 = \alpha\cdot a + \beta\cdot b$

Then α and a are inverse to each other under modulo b.

[Similarly β and b are inverse to each other under modulo a.]

Lemma: If a, b and c are positive integers such that $\gcd(a,b) = 1$ & $a \mid bc$, then $a \mid c$.

~~Ex: find inverse of 13 modulo 2436~~

Linear Congruence:- A congruence of the form

$$ax \equiv b \pmod m,$$

where m is a positive integer, a, b are integers and x is a variable, is called a linear congruence. This type of congruences arise throughout number theory and its applications.

* One method that we will describe uses an integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod m$, if such an integer exist. Such an integer $\bar{a}$ is said to be an inverse of a modulo m.

* If $\gcd(a,m) \neq 1$ then inverse necessarily exist.

Theorem:- If a and m are co-prime integers and $m > 1$, then an inverse of a modulo m exists and this universe is unique modulo m.

Bézout's Lemma

This theorem is about finding the inverse of a modulo m when $\gcd(a, m) = 1$ i.e Find a lc of a & m $= 1$ $1 = sa + tm$.

Ques 2 Find an inverse of 3 modulo 7. since $\gcd(3, 7) = 1 \Rightarrow$ inverse exists & unique.

By using Bézout's Lemma

if $\gcd(a, b) = 1$ then we can write as

a lc $1 = \alpha \cdot a + \beta \cdot b \rightarrow 7 = 2 \cdot 3 + 1$

$\Rightarrow 1 = \alpha \cdot 3 + \beta \cdot 7$

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

directly or $\alpha \cdot 3 \equiv 1 \pmod 7$ (where $\alpha < 7$)

i.e (-2) or 5 is inverse of 3 under modulo 7

so what is the possibility 1, 2, 3, 4, 5, 6

$1 \cdot 3 \equiv 3 \pmod 7$

$2 \cdot 3 \equiv 6 \pmod 7$

$3 \cdot 3 \equiv 2 \pmod 7$

$4 \cdot 3 \equiv 5 \pmod 7$

$5 \cdot 3 = 1 \pmod 7 \Rightarrow$ 5 is an inv of 3 mod 7.

$6 \cdot 3 = 4 \pmod 7$

and 1 is the inverse of 7 with modulo 3, i.e $7 = 1 \pmod 3$

$1 \cdot 7 \equiv 1 \pmod 3$

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

(-2) is an inverse of 3 mod 7

$-9, 12$ ——

Ex (2) 2nd way when you have big no.

Find an inverse of 101 modulo 4620, gcd = 1

Using Bézout's lemma

if $\gcd(a, b) = 1$ then $\alpha a + b\beta = 1$

where a & b are Bézout coefficients.

How to find these coefficients by using EA.

$4620 = 45 \cdot 101 + 75 \rightarrow r_1$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

$r \neq 0 = 1$

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

Now find the value of each non-zero remainder (which is 1)

$$1 = 3 - 1 \cdot 2$$
$$= 3 - 1(23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$
$$= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$
$$= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26)$$
$$= -9 \cdot 75 + 26 \cdot 26$$
$$= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75)$$
$$= 26 \cdot 101 - 35 \cdot 75$$
$$= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$$
$$1 = -35 \cdot 4620 + 1601 \cdot 101$$

$1 = a\alpha + b\beta$

Bézout coefficient $\alpha = -35$ (or 66) & $\beta = 1601$ of $4620 \& 101$

$(-35 + 101 = 66)$

and 1601 is an inverse of 101 under modulo 4620

[i.e $1601 \times 101 \equiv 1 \pmod{4620}$]

and -35 or 66 is an inverse of 4620 under modulo 101.

i.e $66 \times 4620 \equiv 1 \pmod{101}$

101
35
66

21/04/23, KOCET, Makeup class 3-5 Absent list

0, 5, 6, 7, 10, 21 → 25, 33, 34, 36, 41, 47, 51, 56, 57, 63, 67, 70, upto (71)

→ How can we solve the linear congruence $ax \equiv b \pmod{m}$, ie, find all integers x that satisfy this congruence?

One method i.e use an integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$, if such an integer exists. Such an integer $\bar{a}$ is said to be an inverse of a modulo m.

Th@:-

Qwe:- What are the solutions of the linear congruence $3x \equiv 4 \pmod{7}$?

Sol:- First what is the idea solve $ax \equiv b \pmod{m}$ (in general)

Sol:- Multiply by $\bar{a}$ both sides, where $\bar{a}$ is the inverse of a modulo m

i.e $\bar{a}ax \equiv \bar{a}b \pmod{m}$ (Since $\bar{a}$ is inverse of a so $\bar{a}a = 1$)

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

$\Rightarrow \bar{a}b$ is the sol^n and called least positive sol^n of given equ^n.

and all the value of the form $\bar{a}b + mk$ are the sol^n which satify the equ^n

Sol^n: $3x \equiv 4 \pmod{7}$

First find inverse of 3 modulo 7 which we already found that is 5.

i.e $5 \cdot 3x \equiv 5 \cdot 4 \pmod{7}$

$15x \equiv 20 \pmod{7}$ (Now divide whole equ^n by 7 & we find the sol^n under modulo 7)

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

By using the def^n of congruence modulo (if $7 \mid 13 \Rightarrow$ remainder is 6, i.e $7 \mid 20 \Rightarrow$ 6)

we have $x = 7k + 6$

Now find all the values of x which satisfy the above equ^n are the sol^n of equ^n ⊛

$7 \mid x + 6$

$\Rightarrow x - 6 = 7k$

$\Rightarrow x = 7k + 6$

Here k is an integer i.e positive, negative & 0

$k = 0$
then $x = 6$
when $k = 1$
$x = 7 \cdot 1 + 6 = 13$
$k = 2$
$x = 7 \cdot 2 + 6 = 20$
$k = 3$
$x = 7 \cdot 3 + 6 = 27$

Similarly
$k = -1$
$x = 7 \times (-1) + 6 = -1$
$k = -2$
$x = 7 \times (-2) + 6 = -8$
$k = -3$
$x = 7 \times (-3) + 6 = -15$

$\Rightarrow x = 6, 13, 20, \ldots, -1, -8, -15 \ldots$ all are soln of $3x \equiv 4 \pmod 7$.

Ques 2. Solve the linear congruence equn

$$3x \equiv 2 \pmod 4$$

[$x = 2 + 4k$ soln

(3) Show that the linear congruence equn

$2x \equiv 1 \pmod 6$ has no soln

$x = 2, 6, 10, 14$
$\ldots -2, -6, -10, \ldots$

$\gcd(2,6) = 2 = \alpha \cdot 2 + \beta \cdot 6$
$2 = (-2) \cdot 2 + 1 \cdot 6$
$\alpha = -2, \beta = 1$

$6 \mid 2x - 1$
$\Rightarrow 2x - 1 = 6 \cdot k$
$\Rightarrow 2x = 1 + 6k$
$\Rightarrow x = \frac{1}{2} + 3k$

$ax \equiv b \pmod m$ has no solutions if $GCD(a, m) \nmid b$.

$\gcd(2,6) = 2 \nmid 1$
$\Rightarrow$ it has no soln.

$b \mid a \Rightarrow a = b \cdot 1$

The Chinese Remainder Theorem:-

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers 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 soln modulo $m = m_1 m_2 \cdots m_n$.

and the soln is given by

$$x \equiv (a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n) \pmod{m}$$

where $M_k = \frac{m}{m_k}$ and $y_k M_k \equiv 1 \pmod{m_k}$.

Ex:- Solve $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$

Since 3, 5, 7 are pairwise relatively prime then these system has a unique soln.

$$m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$$

and the soln is $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

where $M_1 = \frac{m}{m_1} = \frac{105}{3} = 35$

$$M_2 = \frac{m}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{m}{m_3} = \frac{105}{7} = 15.$$

and $y_1 M_1 \equiv 1 \pmod{m_1} \Rightarrow y_1 \cdot 35 \equiv 1 \pmod 3$

$\Rightarrow y_1$ is inverse of 35 modulo 3

$\Rightarrow y_1 = 2$ bcz $2 \cdot 35 \equiv 1 \pmod 3$.

$y_2 \cdot M_2 \equiv 1 \pmod 5$

$y_2 \cdot 21 \equiv 1 \pmod 5$

$1 \cdot 21 \equiv 1 \pmod 5$

$y_2 = 1$

$y_3 \cdot M_3 \equiv 1 \pmod 7$

$y_3 \cdot 15 \equiv 1 \pmod 7$

$1 \cdot 15 \equiv 1 \pmod 7$

$y_3 = 1$

$\Rightarrow x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod m$

$\equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod m$

$x \equiv 233 \pmod{105}$

$\boxed{x \equiv 23 \pmod{105}}$

105 | 233 (2
210
23

Sol 2

Theorem:- Fermat's Little Theorem:-

If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod p$.

Furthermore, for every integer a we have

$a^p \equiv a \pmod p$

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

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

$a^p \equiv 1 \pmod p$

Ques 2. Find the value of $5^{2003} \pmod 7$

Since $5 \nmid 7$ (7 ∤ 5)

2003 is a prime number

$\Rightarrow 5^{2003} \equiv 5 \pmod 7$ (by Fermat's Little theorem)

$\Rightarrow 5 \equiv$ remainder

$q = 2, p = 7$

$2^7 \equiv 2 \pmod 7$

11/9/18

Ex: Find all solutions x, if they exist, to the system of equivalences:

$$2x \equiv 6 \pmod{14}$$
$$3x \equiv 9 \pmod{15}$$
$$5x \equiv 20 \pmod{60}$$

$x \equiv r_1 \pmod{m_1}$
$x \equiv r_2 \pmod{m_2}$
$x \equiv r_3 \pmod{m_3}$

Theorem: Let m be a positive integer, and let a, b are integers. The congruence $ax \equiv b \pmod{m}$ has a solution for x iff $\gcd(a, m) \mid b$. ✓

$x \equiv 11 \pmod{36}$
$x \equiv 7 \pmod{45}$
$x \equiv 32 \pmod{75}$

Soln: By using the above theorem

$$2x \equiv 6 \pmod{14} \quad \text{—①}$$

Since $\gcd(2, 14) = 2$, so we can cancel 2 from all term. in equ^n ① and we have,

$$x \equiv 3 \pmod{7}$$

$x \equiv 11 \pmod{2^2}$, $x \equiv 11 \pmod{3^2}$
$x \equiv 7 \pmod{2^3}$, $x \equiv 7 \pmod{5}$
$x \equiv 32 \pmod{3}$, $x \equiv 32 \pmod{5^2}$

Similarly, $3x \equiv 9 \pmod{15}$ $\left(\gcd(3, 15) = 3\right)$

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

$p=3$ $(p=5)$ $p=2$

$x \equiv 7 \pmod{2^3} = 8$
$x \equiv 11 \pmod{3^2} = 9$
$x \equiv 32 \pmod{5^2} = 25$

and $\gcd(5, 60) = 5$

$\therefore 5x \equiv 20 \pmod{60} \Rightarrow x \equiv 4 \pmod{12}$

Now, we have equ^n

$$\left.\begin{aligned} x &\equiv 3 \pmod{7} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{12} \end{aligned}\right\}$$

and $(7, 5, 12)$ are pairwise relatively prime

therefore we can apply Chinese remainder theorem, we have

a unique solution

and find solution the same way as we did for chinese remainder case

Ques 2 ① Find gcd (1529, 14039).

② gcd (12345, 54321)

③ Solve $x \equiv$

$y_1 \cdot 60 \equiv 1 \pmod 7$

7) 20 (17

7

50

One more Security Method is

(1) $f(p) = (ap+b) \bmod 26$

where a & b are integers.

Qu's What letter replaces the letter K when the $f(p) = (7p+3) \bmod 26$ is used for encryption?

Sol": p is that term which we want to replace

$p \rightarrow K = 10$ ↘ according to alphabet

$f(10) = (7 \cdot 10 + 3) \bmod 26$

$f(10) = (73) \bmod 26$

$f(10) = 21 \pmod{26}$

$21 = V$

$\Rightarrow$ K is replaced by V in the encrypted message.

(3) What is the secret message produce from the message "MEET YOU IN THE PARK" using the ceaser cipher

Sol": M EET YOU IN THE PARK

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

using ceaser shift shift the letter

$f(p) = (p+3) \pmod{26}$

15 7 7 22 27 17 23 11 16 22 10 7 18 3 20 13

∴ encrypted message is

"PH HW BRX OLQ WKH SDUN"

Cryptography: It is a technique which is used to encrypted a message i.e for decode to code or code to decode. (App - study of encryption secret message) decryption

- There are two method here we used for encryption & decryption

① Ceaser Cipher.

insert the alphabet as number 0 to 25

$f(p) = (p+3) \pmod{26}$ → encryption

and $f^{-1}(p) = (p-3) \pmod{26}$ → decryption

② Shift or affine transformation

$f(p) = (p+k) \pmod{26}$ → encryption

k can be any value which is the another way to decode a secret message

$f^{-1}(p) = (p-k) \pmod{26}$ → decryption

Example:- Decrypt these messages using the Ceaser cipher

① EOXH MHDQV

4 14 23 7 12 7 3 16 21

by using ceaser cipher

$f^{-1}(p) = (p-3) \pmod{26}$

$(4-1) = 3$

3 11 20 4 9 4 0 13 18

⇒ BLUE JEANS

② HDW GLP VXP

③ WHVW WRGDB

RSA Decryption :-

The plain text may be recovered by RSA decryption key d which is the inverse of e modulo $(p-1)(q-1)$.

By chinese Remainder theorem if

$$C^d \equiv M \pmod{p} \text{ and } C^d \equiv M \pmod{q}$$

Then $C^d \equiv M \pmod{pq}$.

Ex:- If a person received the encrypted message 09810462 then find the decrypted message if it is encrypted by RSA cryptosystem with $p=43$, $q=59$, $n=pq$ and $e=13$.

Soln:- Let d is the inverse of e mod $(p-1)(q-1)$ that is d is inverse of 13 mod $42 \cdot 58 = 2436$ then $d = 937$ which is same as encryption key.

Since received message is 09810462 = 0981 0462

Therefore, we have two value of C that is for $C = 0981$ and $C = 0462$.

Now

No need

Cryptography :- (It was by Julius Caesar)

Application of Cryptography is study of secret message.

Process:-

First replace each letter by an integer from 0 to 25, based on its position in the alphabet

i.e. A replace by 0
K " " 10.
Z " " 25.

origin to code encryption

code to origin decryption.

Caesar cipher

$f(p) = (p+3) \bmod 26$. $0 \le p \le 25$, $p \in \mathbb{Z}^+$

- This process is called Encryption.

Q:- What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar Cipher?

Sol:- MEET YOU I N THE PARK.
12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

Now, replace each of these numbers p by $f(p) = (p+3) \bmod 26$.

24+3 = 27 which is > than 26. So, $26\overline{)27}$ (1, remainder 1)

15 7 7 22 1 17 23 11 16 22 10 7 18 3 2013

encrypted message

"PHHW BRX LQ WKH SDUN".

→ To recover the original message from a secret message encrypted by the Caesar Cipher.

$f^{-1}(p) = (p-3) \bmod 26$

- The process of determining the original message from the encrypted message is called Decryption.

A - 0
B - 1
C - 2
D - 3
E - 4
F - 5
G - 6
H - 7
I - 8
J - 9
K - 10
L - 11
M - 12
N - 13
O - 14
P - 15
Q - 16
R - 17
S - 18
T - 19
U - 20
V - 21
W - 22
X - 23
Y - 24
Z - 25

One More method is

shift each letter by K, so that

$f(p) = (p+K) \bmod 26$, K can be any value we can

Such a Cipher is called a **Shift Cipher**

decryption is

$f^{-1}(p) = (p-b) \bmod 26$.

Cipher
a method of writing secret pattern of particular set of letters or symbols

* One more security Method is (Affine transformation)

$f(p) = (ap+b) \bmod 26$

where a & b are integers.

Note: f is Affine transformation if f is bijective function.

Q: What letter replaces the letter K when the func^n $f(p) = (7p+3) \bmod 26$ is used for encryption?

Sol: p is that term which we want to replace.

K = 10 K value is to acc. to alphabet.

$f(10) = (7 \cdot 10 + 3) \bmod 26$

$= (73) \bmod 26$

$= 21$ (remainder is 21)

$21 = V$

∴ K is replaced by V in the encrypted message.

Q1. What are the quotient & remainder when

(a) 19 is divided by 7? Ans :- $q = 2$, $r = 5$

(b) -111 " " by 11? Ans :- $q = -11$, $r = 10$

(c) -1 " " " 3? Ans :- $q = -1$, $r = 2$

(d) 789 " " " 23? Ans :- $q = 34$, $r = 7$

(e) 0 " " " 19? Ans :- $q = 0$, $r = 0$

(f) -1001 " " " 13? Ans :- $q = 77$, $r = 0$

$-111 = (11)(-10) + 1$

valuate these quantities.

(a) 13 mod 3
(b) -97 mod 11
(c) 155 mod 19
(d) -221 mod 23

Q2 (a) $r = a \bmod b$ i.e. $a \equiv r \pmod b$ || (c) 155 mod 19.

$r = 13 \bmod 3$

$\boxed{r = 1}$

$3\overline{)13}$ 4, 12, 1

(b) $-97 \bmod 11$

$r = -97 \bmod 11$

$\boxed{r = 2}$

$11\overline{)-97}$ -9, -99, 2

$r = 155 \bmod 19$

$\boxed{r = 3}$

$19\overline{)155}$ 8, 152, 3

(d) $r = -221 \bmod 23$

$\boxed{r = 9}$

$23\overline{)-221}$ 10, -230, +, 9.

Q3 Decide whether each of these integers is congruent to 5 modulo 17.

(a) 80 (b) 103 (c) -29 (d) -122

Soln: $x \equiv 5 \pmod{17}$

(a) If $x = 80$

$17|_{80-5} = 17|_{75} =$ (No)

(b) If $x = 103$

$17|_{103-5} = 17|_{98} =$ (No)

(c) If $x = -29$

$17|_{-29-5} = 17|_{-34} =$ (Yes)

(d) If $x = -122$

$17|_{-122-5} = 17|_{-127} =$ (No)

Q4. Encrypt the message "DO NOT PASS GO" by translat the letters into numbers, applying the encryption func given, and then translating the new back int

(b) $f(p) = (p+3) \bmod 26$

mod