24/11/2022

UNIT-II:

NUMBER THEORY:

→ Prime Numbers - Divisibility - Division Algorithm - Theorems.

→ GCD using Euclidean Algorithm - Examples

→ Modular Arithmetic - Theorems on congruences.

→ Finding inverse using GCD

→ Fundamental Theorem of Arithmetic - Proof

→ Fermat's Little Theorem - Proof

→ Euler's Theorem - Proof - Chinese Remainder Theorem.

* Prime Numbers:

→ A positive integer greater than 1 is called as a prime number if it is divisible by 1 & itself.

(OR)

→ An integer is a prime; if it is not divisible by any prime less than or equal to its square root.

Ex: 101 is a prime; since it is not divisible by any of the primes which are less than or equal to its square root.

* Composite Number:

A positive integer greater than 1 which is not prime is called composite number

* Division Algorithm:

If

* Divisibility:

If a and b are integers; if $a \neq b$, a divides b denoted a/b; if there exists c is an integer, a/b such that $b = ac$

$$\boxed{\exists\, c \in \mathbb{Z},\ a/b \ni b = ac}$$

→ If a doesn't divide b denoted by $a \nmid b$.

→ If a divides b; where a is a factor of b and b is multiple of b.

* Theorem-1 :

If a, b, c are integers ; then prove that

a) If a/b, a/c then a/b+c.

b) If a/b then a/bc

c) If a/b and b/c then a/c.

d) If a/b and a/c then there exists m, n∈z

∋ a/mb+nc

(i) Proof:

By divibisility

a/b ⇒ there exists ∃ p∈z ∋ b = ap —①

If a/c ⇒ ∃ q∈z ∋ c = aq —②

b+c = a(p+q) p+q = r ∈ z

a/b+c = r b+c = ar

∴ a divides b+c

(ii) Proof:

By divisibility

a/b ⇒ ∃ p∈z, ∋ b = ap —①

a/c ⇒ ∃ q∈z ∋ c = aq —②

bc = apq

bc = a(apq)

(b = ap) × c ⇒ bc = a(pc)

bc = aq

∴ a divides bc

(iii) Proof:

By divisibility

a/b ⇒ ∃ p∈z ∋ b = ap —①

b/c ⇒ ∃ q∈z ∋ c = bq —②

c = apq ∋ r∈z

c = a(r)

∴ a divides c.

(iv) Proof:

By divisibility

a/b and a/c

a/b ⇒ ∃ p∈z ⇒ ∋ b = ap

a/c ⇒ ∃ q∈z ⇒ ∋ c = aq

$mb = amp$

$nCn = anq$

$mb + nCn = a(mp+nq)$

$mb+cn = a(r)$ $\boxed{r \in Z}$

$\therefore$ a divides $bm+cn$

*Theorem-2:

If a,b,c,d are integers then P.T

(i) $a|c, b|d \Rightarrow ab|cd$

(ii) $ac|bc \Rightarrow a|b$

By divisibility:

$a|c \Rightarrow \exists\ p \in z \Rightarrow c = ap$ — ①

$b|d \Rightarrow \exists\ q \in z \Rightarrow d = bq$ — ②

① × ②

$cd = ab(pq)$

$\therefore$ ab divides cd.

$ac|bc \Rightarrow \exists\ p \in z \Rightarrow bq = a(p)$

$\Rightarrow$ a devides b.

* Division Algorithm: / Euclidean Algorithm:

If a is an integer and d is a +ve integer then there exists integers q and r with $\boxed{0 \le r < d}$; $\boxed{a = dq+r}$ is known as division algorithm

$d \overline{)\ a\ (q}$
$\underline{\quad p \quad}$
$\quad r$

a is a dividend; d is a divisor, q is a quotient; r is a remainder.

* Greatest Common divisor:

The ~~largest integer~~ non-zero integers a & b are ~~and~~ then the largest integer p such that $p|a$ & $p|b$ is called GCD of a & b.

Ex: GCD(24, 36) = 12

* Relatively Prime:

→ 2 integers a, b are said to be relatively prime if their GCD is 1.

GCD(17, 22) = 1

25/11/2022

*Prime Factorization:

It is one of the method to find gcd & LCM of 2 numbers a, b.

*To find gcd using prime factorization:

If a, b are non-zero integers; then the prime factorization is denoted by.

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$gcd(a,b) = p_1^{(\min(a_1,b_1))} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

Ex: gcd(120, 500)

$$120 = 12 \times 10 = 2 \times 2 \times 3 \times 5 \times 2 = 2^3 \times 3 \times 5$$

$$500 = 5 \times 10^2 = 5 \times 2^2 \times 5^2 = 5^3 \times 2^2$$

$$gcd(120, 500) = 2^2 \times 5 = 4 \times 5 = \underline{20}$$

*To find LCM using prime factorization

If a, b are non-zero integers then the prime factorization is denoted as

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$$

$$b = p_1^{b_1} \cdot p_2^{b_2} \cdots p_n^{b_n}$$

$$LCM(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

Ex: LCM (120, 500)

$$120 = 2^3 \times 3 \times 5$$

$$500 = 5^3 \times 2^2$$

$$LCM(120, 500) = 2^3 \times 3 \times 5^3$$

$$= 3000$$

*Modular arithmetic:

If a is an integer and m is any +ve integer then the remainder 'r' can be written as

$$\boxed{a \% m = r}$$

Ex: $6 \bmod 2 = 0$

$17 \bmod 5 = 2$

*Congruence Notation:

If a & b are integers and m is any +ve integer then a is congruent to b modulus m ($a \cong b \% m$) if m divides a − b.

$$\boxed{a \cong b \bmod m}$$

Ex: $24 \cong 14 \bmod 6$

$24 - 14 / 6$.

$\Rightarrow 24 \not\cong 14 \bmod 6$.

→ If a & b not congruent to modulo m.

$a \not\equiv b \bmod m$

★→ Theorem: 1

* If $m \in z^+$ then P.T integers a & b are congruent to b mod m iff there is an int k ∋ $a = b + km$

Proof:

Given $m \in z^+$;

we have to prove $a \cong b \bmod m$ iff

$\exists\ k \in z,\ a = b + km$,

consider $a \cong b \bmod m$

$\Leftrightarrow$ a-b is divisible by m

$m \mid a-b$

$\Leftrightarrow a - b = mk \ ;\ k \in z$ } Divisibility.

★→ Theorem: 2

If $a \cong b \bmod m$ and $c \cong d \bmod m$ then prove that

(i) $a - c \cong (b+d) \bmod m$.

(ii) $ac \cong bd \bmod m$.

where $m \in z^+$

Given $m \in z^+$, $a \cong b \bmod m$ and $c \cong d \bmod m$.

(i) to prove $a + c \cong b + d \bmod m$

Consider:

$a \cong b \bmod m$

$\Leftrightarrow$ (a-b) is divisible by m.

$\Leftrightarrow m \mid a-b$

$\boxed{a - b = mk}$ $(k \in z)$

$\boxed{a = mk + b}$ —①

Consider

$c \cong d \bmod m$

$\Leftrightarrow$ (c-d) is divisible by m.

$\Leftrightarrow m \mid (c-d)$

$c - d = ml$. $(l \in z)$

$\boxed{c = ml + d}$ —②

① + ② gives

$a + c = m(k+l) + b + d$.

$\boxed{(a+c) - (b+d) = m(k+l)}$ $\boxed{k+l = r}$ $r \in z$

$\Leftrightarrow (a+c) - (b+d) = mr$.

$\Leftrightarrow m \mid (a+c) - (b+d)$

$\Leftrightarrow (a+c) - (b+d)$ is divisible by m

$\Leftrightarrow (a+c) \cong (b+d) \bmod m$.

(ii) To prove $ac \cong bd \cdot mo$

① × ② gives

$ac = (b+mk)(d+ml)$

$ac = bd + bml + mkd + m^2lk$

$ac = bd + m(bl + kd + mlk)$.

$ac - bd = mr \quad r = bl + dk + mlk \in z$

$\Leftrightarrow m / ac - bd$

$\Leftrightarrow ac - bd$ is divisible by m.

$\Leftrightarrow ac \cong bd \bmod m$.

✱ Theorem: 3

Let m be a +ve integer ; show that $a \cong b \bmod m$ if $a \bmod m = b \bmod m$.

Proof:

Given $m \in z^+$, $a \bmod m = b \bmod m$.

We have to prove that $a \cong b \bmod m$.

Consider, $a \bmod m = b \bmod m \Rightarrow$ the remainder is same when a & b, divided by m respectively.

By division algorithm; we have.

$a \bmod m \Rightarrow a = mq_1 + r \quad -①$

$b \bmod m \Rightarrow b = mq_2 + r \quad -②$

① − ② gives

$a - b = m(q_1 - q_2)$

$a - b = mq$ $\quad q_1 - q_2 = q \in R$

$\Leftrightarrow m / (a-b)$

$\Leftrightarrow a \cong b \bmod m$

26/11

26/11/2022

Theorem: 4:

If n/m where m, n are +ve integers >1 and if $a \cong b \bmod m$ where a & b are integers: then prove that $a \cong b \bmod n$.

Proof: Given $n/m \ \forall n, m \in z^+$

(∵ By divisibility)

if $n/m \Rightarrow \exists \ k_1 \in z \Rightarrow$

$m = nk_1 \quad -①$

and also given $a \cong b \bmod m$

$\Leftrightarrow (a-b)$ is divisible by m (By congruence notation)

$\Leftrightarrow m / a - b$

$\Leftrightarrow a - b = mk_2 \ \forall k_2 \in z$

$\Leftrightarrow a = b + mk_2 \quad -②$

Substituting ① in ②

$a = b + mk_2$

$a = b + (nk_1)k_2$

$a = b + nk \qquad k = k_1 k_2 \in \mathbb{Z}$

$\Leftrightarrow a - b = nk$

$\Leftrightarrow n \mid a - b$

$\Leftrightarrow a \equiv b \bmod n$

Hence proved.

*Euclidean Algorithm:

Computing GCD using prime factorisation is time consuming and inefficient. Euclid algorithm gives efficient method to find GCD of 2 nos.

Theorem:

If $a = bq + r$ where $a, b, q, r \in \mathbb{Z}$ then prove that $(a,b) = \gcd(b,r)$

Proof: Given $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$ — ①

We have to prove $\gcd(a,b) = \gcd(b,r)$

For that it is enough to prove the common divisors of a, b are same as the common divisors of b, r.

Let 'n' be a common divisor of a, b i.e. n divides a, b.

$\Rightarrow$ n divides a and bq

$\Rightarrow$ n divides $a - bq$

$\Rightarrow$ n divides r [$\because r = a - bq$]

$\therefore$ Any common divisor of a & b is also a common divisor of b and r.

Let 'n' be a common divisor of b & r.

$\Rightarrow$ n divides b and r.

$\Rightarrow$ n divides bq and r.

$\Rightarrow$ n divides $bq + r$.

$\Rightarrow$ n divides a

$\therefore$ Any common divisor b and r is a common divisor of a and b.

Hence, the common divisors of a, b are same as common divisors of b and r.

$\therefore \boxed{\gcd(a,b) = \gcd(b,r)}$

*Working procedure to find $\gcd(a,b)$ using Euclidean algorithm.

→ Let $a > b > 0$ (otherwise interchange integers in order to divide largest by smallest).

→ Divide a/b to get remainder r & quotient q i.e. to write the division

algorithm $a = bq + r$

→ Now consider b & r and repeat step ② and continue till the remainder (r) is 0.

→ GCD (a, b) is the least non-zero divisor if remainder r is 0.

* GCD (414, 662)

$662 = 414 \times 1 + 248$

$414 = 248 \times 1 + 166$

$248 = 166 \times 1 + 82$

$166 = 82 \times 2 + 2$

$82 = \boxed{2} \times 41 + 0$

2 is the GCD

* GCD (89, 55)

* GCD (111, 201)

* GCD (1529, 4038)

89 / 55 / 34

$89 = 55 \times 1 + 34$

55 / 34 / 21

$55 = 34 \times 1 + 21$

$34 = 21 \times 1 + 13$

$21 = 13 \times 1 + 8$

$13 = 8 \times 2 + 5$

$8 = 5 \times 1 + 3$

$5 = 3 \times 1 + 2$

$\Rightarrow 3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 0$

GCD is 1

10 / 201 / 111 / 90

$201 = 111 \times 1 + 90$

$111 = 90 \times 1 + 21$

$90 = 21 \times 4 + 6$

$21 = 6 \times 3 + 3$

$6 = 3 \times 2 + 0$

GCD is 3

$4038 = 1529 \times 2 + 980$

$1529 = 980 \times 1 + 549$

$980 = 549 \times 1 + 431$

$549 = 431 \times 1 + 118$

$431 = 118 \times 3 + 77$

$118 = 77 \times 1 + 41$

$77 = 41 \times 1 + 36$

$41 = 36 \times 1 + 5$

$36 = 5 \times 7 + 1$

$5 = \boxed{1} \times 5 + 0$

GCD is 1

28/11/2022

* Linear Combination of gcd(a,b):-

- If a & b are +ve integers ∃ s,t are also integers such that $\boxed{gcd(a,b) = s*a + t*b}$

ie. gcd(a,b) is a linear combination of (s,a) & (t,b).

* Express GCD(252, 198) as a linear combination

$252 = 198 \times 1 + 54$

$198 = 54 \times 3 + 36$

$54 = 36 \times 1 + 18$

$36 = \boxed{18} \times 2 + 0$

GCD of (252, 198) = 18

$18 = 54 - 36$

$= (252 - 198) - (198 - (252 - 198) \times 3)$

$= 252 - 198 - 198 + 252 \times 3 - 198(3)$

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

$18 = 252 \times 4 - 198 \times 5$

$gcd(a,b) = s*a + t*b$

$\boxed{s = 4 \quad t = -5}$

* GCD(123, 2347)

$2347 = 123 \times 19 + 10$

$123 = 10 \times 12 + 3$

$10 = 3 \times 3 + 1$

$3 = \boxed{1} \times 3 + 0$

GCD is 1

$1 = 10 - 3 \times 3$

$= (2347 - 123 \times 19) - (123 - (2347 - 123 \times 19) \times 12) \times 3$

$1 = 2347 - 123 \times 19 - 123 + (2347 - 123 \times 19) \times 12$

$1 = 10 - 3 \times 3$

$= 10 - 3(123 - 10 \times 12)$

$= 10 - 3 \times 123 + 10 \times 36$

$= 37(2347 - 123 \times 19) - 3 \times 123$

$= 37 \times 2347 - 123(37 \times 19) - 3 \times 123$

$1 = 37 \times 2347 - 706 \times 123$

* GCD(3454, 4666)

$4666 = 3454 \times 1 + 1212$

$3454 = 1212 \times 2 + 1030$

$1212 = 1030 \times 1 + 182$

$1030 = 182 \times 5 + 920$

$182 = 120 \times 1 + 62$

$120 = 62 \times 1 + 58$

$62 = 58 \times 1 + 4$

$58 = 4 \times 14 + 2$

$4 = 2 \times 2 + 0$

GCD of $(3454, 4666) = 2$

$2 = 6 - 4 \times 1$

$= (62 - 58) - (58 - 6 \times 9)$

$= 6 - 58 + 6 \times 9$

$= 7 \times 9 - 54$

$= 10(62 - 58) - (120 - 62)$

$= 11 \times 62 - 10 \times 58 - 120$

$= 11 \times (182 - 120) - 10(120 - 62) - 120$

$= -22 \times 120 + 11 \times 182 + 10 \times 62$

$= -22 \times 120 + 10(182 - 120)$

$= -32 \times 120 + 10 \times 182$

$= -32(1030 - 182 \times 5) + 10 \times 182$

$2 = 58 - 14 \times 4$

$= 120 - 62 - 14(62 - 58)$

$= 58 - 14 \times 62 + 14 \times 58$

$= 15 \times 58 - 14 \times 62$

$= 15(120 - 62) - 14 \times 62$

$= 15 \times 120 - 29 \times 62$

$= 15 \times 120 - 29(182 - 120)$

$= 44 \times 120 - 29 \times 182$

$= 44(1030 - 182 \times 5) - 29 \times 182$

$= 44 \times 1030 - 182 \times 220 - 29 \times 182$

$= 44 \times 1030 - 249 \times 182$

$= 44 \times 1030 - 249(1212 - 1030)$

$= 44 \times 1030 + 249 \times 1030 - 249 \times 1212$

$= 293 \times 1030 - 249 \times 1212$

$= 293 \times (3454 - 1212 \times 2) - 249 \times 1212$

$= 293 \times 3454 - 1212(586 + 249)$

$= 293 \times 3454 - 1212 \times 835$

$= 293 \times 3454 - 835(4666 - 3454)$

$= -835 \times 4666 + 1128 \times 3454$

29
15
4

*Linear Congruence: The congruence of the form $ax \cong b \bmod m$ where $m \in z^+$; where a & b are integers and 'x' is a variable is known as linear congruence

*Inverse of a modulo m:

If $ax \cong b \bmod m$ is a linear congruence and if there exists $x = \bar{a} \in z$ such that ~~$a * \bar{a} \cong 1$~~ $a \cdot \bar{a} \cong 1 \bmod m$ then $\bar{a}$ is said to be inverse of a mod m

→Note: The inverse of a mod m exists whenever a and m are relatively prime.

* Find the inverse of 19 mod 141

gcd(a,m) = 1

gcd(19, 141)

141 = 19 × 7 + 8

19 = 8 × 2 + 3

8 = 3 × 2 + 2

3 = 2 × 1 + 1

2 = 1 × 2 + 0

∴ gcd(19, 141) = 1

19, 141 are relatively prime.

1 = 3 − 2 × 1

= 3 − 1(8 − 3 × 2)

= 3 − 1 × 8 + 3 × 2

= 3(19 − 8 × 2) − 1 × 8

= 19 × 3 − 8 × 6 − 8 × 1

= 19 × 5 − (141 − 19 × 7)

= 19 × 5 − 141 × 1 + 19 × 7 × 1

1 = −7 × 141 + 19 × 52

s = 52

52 is the inverse of 19 mod 141

* Find the inverse of a) 144 mod 233

b) 13 mod 2436

c) 123 mod 2347

a) 144 mod 233

233 = 144

29/11/2022

** PRIME DIVISOR PROPERTY:

If p is a prime number which divides the product of 2 natural numbers a and b then prove that p divides a (or) p divides b.

Proof:

⇒ Given p is prime which divides product of 2 natural numbers.

$\Rightarrow p \mid ab \quad -(1)$

We have to prove $p \mid a$ (or) $p \mid b$.

Let $p \nmid a$ then we have to show that $p \mid b$.

∵ $p \nmid a$ and p is prime

$$\therefore \gcd(a,p) = 1$$

∴ gcd(a, p) can be expressed as linear combination of a & p.

∴ ∃ $s, t \in \mathbb{Z}$

∃ $\gcd(a,p) = 1 = sa + tp$

Consider $sa+tp=1$ — (2)

Multiply $b \times$ (2)

$sab+tpb=b$

Let $p=ab \in \mathbb{Z}$

$sp+tpb=b$

$p(s+tb)=b$

where $k=s+tb \in \mathbb{Z}$

$p \mid b$

*FERMAT'S LITTLE THEOREM:

If p is a prime and a is an integer which is not divisible by p; then prove that $\boxed{a^{p-1} \cong 1 \bmod p}$

Furthermore,

For every integer a; we have to prove that $\boxed{a^p \cong a \bmod p}$

(or) $\left(p \mid a^p - a\right)$

If p is a prime and a is an integer which is not divisible by p, then prove that $\boxed{p \mid a^p - a}$

Proof:

Given 'p' is a prime and 'a' is an integer not divisible by p;

We have to prove that $p \mid a^p - a$.

We are proving this theorem by Mathematical Induction.

Consider

$P(a)$: "If 'p' is a prime & 'a' is an integer which is not divisible by p then $p \mid a^p - a$"

Step-1 Let the theorem is true for $a=1$ is an integer i.e. $P(a)$ is true.

$P(1)$: "p is prime and $a=1$ is an integer not divisible by p" i.e. $p \mid 1^p - 1$

$\therefore$ a is not divisible by p

Step-2: Let the theorem is true for $a=b$ i.e. $P(b)$ is true $P(b)$: If p is prime and $a=b$ is an integer which is not divisible by p i.e. $p \mid b^p - b$ is true.

Step-3: Now we have to prove the theorem is true for $a=b+1$ i.e. $P(b+1)$ is true.

P(b+1) : "P is prime and a = b+1 is an integer which is not divisible by P"

i.e. $P/(b+1)^P-(b+1)$ will be true

$(b+1)^P-(b+1)$ can be expanded using binomial theorem

$a^P-a = (b+1)^P-(b+1)$ $\quad (\because a = b+1)$

$= P_{C_0} 1 b^P + P_{C_1} 1^1 b^{P-1} + P_{C_2} 1^2 b^{P-2} + \cdots$

$\cdots + P_{C_{P-1}} 1^{P-1} b + P_{C_P} 1^P b^0 - b - 1$

$= (b^P - b) + (P_{C_1} b^{P-1} + \cdots + P_{C_{P-1}} b) = 0$ ①

By Mathematical Induction p divides b^P-b and by then "P is a prime and $0<K<p$ then p divides P_{C_K}"

we have $P/(P_{C_1} b^{P-1} + \cdots + P_{C_{P-1}} b)$

∴ p divides RHS of eqn ①

$P/(b+1)^P-(b+1)$

∴ P(b+1) is true.

Hence by the principle of finite mathematical Induction the theorem is true $\forall z^+$ values of A.

* FUNDAMENTAL THEOREM OF ARITHMETIC: (UNIQUENESS):

Every positive integer $n>1$ can be expressed uniquely as a prime number or as a product of 2 or more prime numbers.

Proof:

Let $n>1$ be a +ve integer.

Initially; we show that 'n' can be expressed as a prime (or) product of prime.

The proof is carried out by mathematical induction of n.

Let $P(n)$: "Every +ve integer $n>1$ can be expressed as prime (or) product of primes."

By Mathematical Induction.

Step-1: Let $P(n)$ be true for $n=2$

i.e. since $n=2$ is >1 and is a prime and it can be expressed as a prime.

$\therefore P(n)$ is true for $n=2$.

Step-2 Let $p(n)$ be true for $n > 2$ and $n \leq k$ i.e.

If n is a +ve integer > 2 and $\leq k$ then it can be expressed as a prime (or) product of primes is true.

Now, we have to prove the theorem is true for $n = k+1$ i.e. every +ve integer $n = k+1$ can be expressed as a prime (or) product of primes.

$\therefore p(k+1)$ is true.

Here 2 cases arise:

Case(i): When $k+1$ is a prime

Since $n = k+1$ being prime, it can be expressed as a prime itself i.e.

$p(n)$ is true for $n = k+1$.

Case(ii): When $k+1$ is a composite

Since, $k+1$ is a composite number; by def. of composite number $k+1$ can be expressed as the product of 2 integers a & b such that $\boxed{2 \leq a \leq b < k+1}$

By induction hypothesis;

Since a & b be b/w 2 & $k+1$

i.e. $2 \leq a \leq b < k+1$

a & b can be written as product of primes.

i.e. If $n = k+1$ is a composite number then it can also be expressed as product of primes

Hence, by the principle of Mathematical Induction "Every +ve integer > 1 can be expressed as prime (or) product of primes.

* **To show uniqueness:**

Let the +ve integer $n > 1$ can be written as product of primes in two different ways namely

$$n = p_1 \cdot p_2 \cdot \cdots p_i \cdots p_s \quad -(1)$$

$$n = q_1 \cdot q_2 \cdots q_j \cdots q_t \quad -(2)$$

where p_i and q_j are primes written in increasing order $i = 1$ to s and $j = 1$ to t

Now, removing the common primes from the above two factorization we have equal products of

primes as

$$p_1 p_2 \cdots\cdots p_s = q_1 \cdot q_2 \cdots q_t \quad -③$$

In the above equation no prime

$\boxed{p_i = q_j}$; since p_i is a factor of

LHS of eq ③

p_i also divides RHS

By prime divisor property:

"If p is a prime which divides product of two int a & b then either p divides a (or) p divides 'b'.

we have p_i / q_1 (or) p_i / q_2 (or) $\cdots$ p_i / q_t

By lemma: if p & q are primes & p divides q then $p = q$.

we have

$$p_1 = q_1, \; p_2 = q_2, \; p_i = q_3 \cdots\cdots p_i = q_j$$

This is a contradiction to the fact that no prime p = any prime q.

This contradiction is because of our false supposition that any +ve integer $n > 1$ can be expressed as a product of primes in 2 different ways, which is false.

Hence, every +ve integer $n > 1$ can be expressed as a prime (or) a product of primes in a unique way.

Hence proved.

This contradiction is because of our false supposition that any +ve integer $n > 1$ can be expressed as a product of primes in 2 different ways, which is false.

Hence, every +ve integer $n > 1$ can be expressed as a prime (or) a product of primes in a unique way.

Hence proved.

*Chinese Remainder Theorem: (CRT) 09/12/22

Let $m_1, m_2, \ldots, m_n$ be pairwisely relatively prime positive integers $a_1, a_2, \ldots, a_n$ be 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 $m = m_1 m_2 \ldots m_n$.

(OR)

* If $m_1, m_2, \ldots, m_k$ be positive integers such that $\gcd(m_i, m_j) = 1$ $(i \neq j)$ and

$M = m_1 \cdot m_2 \cdots m_k$ and then the system of congruences

$x_1 \equiv b_1 \pmod{m_1}$

$x_2 \equiv b_2 \pmod{m_2}$

⋮

$x_k \equiv b_k \pmod{k}$

where $b_1, b_2, \ldots, b_k$ are integers.

has exactly one solution given by

$x_0 \bmod M$

*Procedure to solve the system of congruences using CRT:

→Let us consider the given congruences

$x_1 \equiv b_1 \pmod{m_1}$
$x_2 \equiv b_2 \pmod{m_2}$
$x_3 \equiv b_3 \pmod{m_3}$ } Given. —(1)

STEP1: Here Compare: $b_1 =$ $b_2 =$ $b_3 =$ | $m_1 =$ $m_2 =$ $m_3 =$ $M = m_1 \cdot m_2 \cdot m_3$

$\gcd(m_1, m_2) = 1$
$\gcd(m_2, m_3) = 1$
$\gcd(m_3, m_1) = 1$ } all gcd values must be 1.

∴ CRT will be applicable.

STEP-2 $x_0 = \sum_{i=1}^{k=3}$

$x_0 = \sum_{i=1}^{3} \frac{M}{m_i} y_i b_i$

$x_0 \equiv \frac{M}{m_1} y_1 b_1 + \frac{M}{m_2} y_2 b_2 + \frac{M}{m_3} y_3 b_3$ —(2)

STEP-3: To find y_i

$\frac{M}{m_i} y_i \equiv 1 \bmod m_i$

→ to find y_1

$\frac{M}{m_1} y_1 \equiv 1 \bmod m_1$

→ to find y_2

$\frac{M}{m_2} y_2 \equiv 1 \bmod m_2$

→ to find y_3

$\frac{M}{m_3} y_3 \equiv 1 \bmod m_3$.

→Find the solutions of system of congruences:

$x \equiv 1 \pmod 4$
$x \equiv 2 \pmod 3$

Compare: $b_1 = 1$ $b_2 = 2$ | $m_1 = 4$ $m_2 = 3$. $M = m_1 \cdot m_2 = 12$

Step-I

$\gcd(m_1, m_2) = 1$

~~$\gcd(m_2, m_3) = 1$~~

∴ CRT will be applicable.

*Applications:
- To find the time and calendar
- No. of mondays after 100 yrs.

Step-II:

$$x_0 \cong \frac{M}{m_1} y_1 b_1 + \frac{M}{m_2} y_2 b_2 \quad -(1)$$

Step-III:

$$\frac{M}{m_i} y_i \cong 1 \bmod m_i \quad -(2)$$

$$\frac{M}{m_1} y_1 \cong 1 \bmod m_1$$

$$\frac{12}{4} y_1 \cong 1 \bmod 4$$

$$3y_1 \cong 1 \bmod 4$$

$$\therefore \boxed{y_1 = 3}$$

$$\frac{M}{m_2} y_2 \cong 1 \bmod m_2$$

$$\frac{12}{3} y_2 \cong 1 \bmod 3$$

$$4y_2 \cong 1 \bmod 3$$

$$\boxed{y_2 = 1}$$

$a \cong b \bmod m$

$\frac{a-b}{m}$

$$x_0 \cong \frac{12}{4}(3)(1) + \frac{12}{3}(2)(1)$$

$$x_0 \cong 9 + 8 \cong 17$$

∴ Unique solution is 17 mod 12

$$\boxed{x_0 = 5 \bmod 12}$$

* $x \cong 5 \pmod 4$

$x \cong 3 \pmod 7$

$x \cong 2 \pmod 9$

$b_1 = 5$, $b_2 = 3$, $b_3 = 2$

$m_1 = 4$, $m_2 = 7$, $m_3 = 9$

$M = 252$

4, 36, ×7, 252

Step-II:

$$x_0 \cong \frac{M}{m_1} y_1 b_1 + \frac{M}{m_2} y_2 b_2 + \frac{M}{m_3} y_3 b_3 \quad -(1)$$

Step-III

$$\frac{M}{m_i} y_i \cong 1 \bmod m_i$$

$$\frac{252}{4} y_1 \cong 1 \bmod 4$$

$$63 y_1 \cong 1 \bmod 4$$

$$\boxed{y_1 = 3}$$

$$\frac{252}{9} y_3 \cong 1 \bmod 9$$

$$28 y_3 \cong 1 \bmod 9$$

$$\boxed{y_3 = 1}$$

$$\frac{252}{7} y_2 \cong 1 \bmod 7$$

$$36 y_2 \cong 1 \bmod 7$$

$$\boxed{y_2 = 1}$$

63 ×2 126; 63 ×3 189; 63 ×4 252

$$x_0 = \frac{252}{4}(3)(5) + \frac{252}{7}(1)(3) + \frac{252}{9}(1)(2)$$

$$= 252\left[\frac{15}{4} + \frac{3}{7} + \frac{2}{9}\right]$$

$$= 252\left[\frac{63 \times 5 + 27 + 14}{63}\right]$$

$= \frac{252}{63}(315 + 41)$

$= \frac{252 \times 392}{63}$

$= 252\left[\frac{15}{4} + \frac{3}{7} + \frac{2}{9}\right]$

$= \frac{252}{28 \times 9}[945 + 108 + 56]$

$= 1109$

$= 1109 \mod 252$

$\Rightarrow 101 \mod 252$

* A child has some chocolates (x) in a box,

1) If the chocolates are grouped in 7s there are 5 left over. $5 \mod 7$

2) If grouped in 11's there will be 6 left over $6 \mod 11$

3) If grouped in 13's there be 8 left over $8 \mod 13$

$x \cong 5 \mod 7$ $\quad b_1 = 5$ $\quad m_1 = 7$

$x \cong 6 \mod 11$ $\quad b_2 = 6$ $\quad m_2 = 11$

$x \cong 8 \mod 13$ $\quad b_3 = 8$ $\quad m_3 = 13$

$M = m_1 \cdot m_2 \cdot m_3 = 1001$

Step-II:

$x_0 \cong \frac{M}{m_1} y_1 b_1 + \frac{M}{m_2} y_2 b_2 + \frac{M}{m_3} y_3 b_3$

Step-III:

$\frac{M}{m_i} y_i \cong 1 \mod m_i$

$\frac{M}{m_1} y_1 \cong 1 \mod m_1$

$\frac{1001}{7} y_1 \cong 1 \mod 7$

$143 y_1 \cong 1 \mod 7$

$y_1 = 5$

$91 y_2 = 1 \mod 11$

$y_2 = 4$

$77 y_3 = 1 \mod 13$

$y_3 = 12$

$x_0 = 2003 \mod 1001$

$x_0 = 1 \mod 1001$

* FERMAT'S LITTLE THEOREM:

Let p be a prime ; $p \nmid a$ (i.e. $\gcd(a,p)=1$)

$$a^{p-1} \cong 1 \bmod p$$

* $n^{6k}-1$ is divisible by 7 ; if $\gcd(n,7)=1$ where $k \in z^+$

Given that $\gcd(n,7)=1$

Here $p=7$ is a prime ; $\boxed{a=n}$

By Fermat's little theorem:

$$a^{p-1} \cong 1 \bmod p$$

$$n^{7-1} \cong 1 \bmod 7 \Rightarrow n^{6K} \cong 1^K \bmod 7$$

$$n^{6k} \cong 1 \bmod 7$$

$n^{6k}-1$ is divisible by 7.

* If $7 \nmid a$; P.T. either a^3-1 (or) a^3+1 is divisible by 7.

By the statement of Fermat's little theorem

$p=7 \quad a=a$.

is a prime

$$a^{p-1} \cong 1 \bmod p$$

$$a^6 \cong 1 \bmod 7$$

a^6-1 is divisible by 7

$(a^3-1)(a^3+1)$ are divisible by 7.

15/12/2022

* Compute $3^{1000} \bmod 5$ (or) Find the remainder ~~B~~ of 3^{1000} which is divisible by 5.

$a=3$; $p=5$

$\gcd(3,5)=1$

By Fermat's little theorem

$$a^{p-1} \cong 1 \bmod p$$

$$3^{5-1} \cong 1 \bmod 5$$

$$3^4 \cong 1 \bmod 5$$

$$(3^4)^{250} \cong 1^{250} \bmod 5$$

$$3^{1000} \cong 1 \bmod 5$$

remainder $=1$

$3^{1002} \bmod 5$

$a=3$; $p=5$

$\gcd(3,5)=1$

$$3^{5-1} \cong 1 \bmod 5$$

$$(3^4)^{250} \cdot 3^2 \cong 9 \bmod 5$$

$$3^{1002} \cong 9 \bmod 5$$

$r=4$

* Find the remainder of 11^{470} which is divisible by 37

$a = 11 ; p = 37$

$\gcd(11, 37) = 1$

By Fermat's Little Theorem

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

$$11^{36} \equiv 1 \bmod 37$$

$$((11)^{36})^{13} \cdot 11^2 \equiv (1)^{13} \cdot 1^{13} \bmod 37.$$

$$(11^{36})^{13} \cdot 11^2 \equiv 10 \bmod 37$$

remainder = 10

* $2^{105} \bmod 11 / 2^{105} \equiv 1 \bmod 11$
* $2^{20} \equiv 4 \bmod 7$ (Prove that).

* Symbolic Fraction Method : [to solve linear congruence]

If $ax \cong b \bmod m$ with $\gcd(a, m) = 1$; then

$\Rightarrow ax \cong b \bmod m$

By congruence relation

$ax - b$ is divisible by m.

$\Rightarrow m \mid ax - b$

$ax - b = mr \quad \forall r \in z$ (By divisibility Rule)

$ax = b + mr$

$$\boxed{x = \frac{b+mr}{a}}$$

* $5x \cong 2 \bmod 16$

$x \cong \frac{2}{5} \bmod 16$

$a = 5 \quad b = 2 \quad m = 16$

$$x = \frac{b+mr}{a} \equiv \frac{2+16(3)}{5} \bmod 16$$

$x \equiv 10 \bmod 16$

$\boxed{\text{remainder} = 10}$

* Criteria for solving L.C:

→ The linear congruence $ax \cong b \bmod m$

(i) a unique solution if $\gcd(a, m) = 1$

$\boxed{a \cong x + mr}$ where $r = 0, 1, 2 \ldots\ldots$

(ii) the given system has no solution if $d \nmid b$ (here $d = \gcd(a, m)$; where $d \neq 0, 1$)

(iii) incongruent solutions if $d \mid b$ $d \neq 0, 1$

→ different (or) infinite

$\boxed{x \cong x_0 + r\left(\frac{m}{d}\right) \bmod m}$ $r = 0, 1, 2, \ldots$

* Solve the linear congruence $14x \cong 21 \bmod 12$

$14x \cong 21 \bmod 12$

$ax \cong bx \bmod m$

$a = 14 ; \quad b = 21 ; \quad m = 12$

$\gcd(a, m) = \gcd(14, 12) = 2$

$\therefore$ We observe $\boxed{2 \nmid 21}$

Given linear congruence has no solution.

* $5x \cong 2 \bmod 26$

$a = 5 ; \quad b = 2 \quad m = 26$

$\gcd(a, m) = \gcd(5, 26) = 1$

Given linear congruence has a

unique solution.

$x \cong \frac{2}{5} \bmod 26$

$x = \frac{2+26(3)}{5} \bmod 26$

$\boxed{x = 16 \bmod 26}$

remainder = 16

By inspection $x = 16$ is a soln of given L.C.

* $6x \cong 15 \bmod 21$

$a = 6 \quad b = 15 \quad m = 21$

$\gcd(6, 21) = 3$

Given LC has 3 no. of incongruent solutions.

By inspection.

$x \cong \frac{15}{6} \bmod 21$

$= \frac{15 + 21(\ )}{6} \bmod 21$

$= 6 \bmod 21$

$x = 6$ is a soln of LC.

$x \cong x_0 + (\frac{m}{d}) \bmod m \quad r = 0, 1, 2$

$x \cong 6 + (\frac{21}{3}) \bmod 21$

$x \cong 6 + 7r \bmod 21 \quad r = 0, 1, 2$

$x \cong 6 \bmod 21 \quad x \cong 13 \bmod 21$

$x \cong 20 \bmod 21$

Note

$x = 6, 13, 20$

$6 \not\equiv 13 \bmod 21$

$13 \not\equiv 20 \bmod 21$

$6 \not\equiv 20 \bmod 21$

* Solve:

(i) $18x \cong 27 \bmod 16$

(ii) $4x \cong 3 \bmod 5$

(iii) $16x \cong 25 \bmod 19$

* $18x \cong 27 \bmod 16$

$a = 18; \quad b = 27 \quad m = 16$

$\gcd(a, m) = \gcd(18, 16) = 2$

Given LC has 2 incongruent solutions

By inspection

$x \cong \frac{27}{18} \bmod 16$

$x \cong \frac{27 + 16(\ )}{18}$