Unit - 1

Greatest Common Divisors and prime factorization

→ The positive integer 1 has just one positive divisor. other positive integers have atleast two positive divisors because it is divisible by 1 and itself. Integers with exactly two positive divisors are of great importance in number theory, they are called "prime numbers".

Prime numbers: A prime number is an integer greater than 1 that is divisible by no positive integer other than 1 and itself.

Ex: 2, 3, 5, 7, ---

Composite numbers: An integer greater than 1 which is divisible by more than 2 positive integers. is known as composite numbers.

Ex: 4, 6, 8, 9, ---

→ we can find the Prime numbers using "Sieve of Eratosthanese method"

Prime numbers between 1-100 using Eratosthanese method.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	~~29~~	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	~~53~~	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	~~59~~	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	~~73~~	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	~~79~~	~~80~~
~~81~~	~~82~~	~~83~~	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	~~89~~	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,
53, 59, 61, 67, 71, 73, 79, 83, 89, 97,

Standard form of a Natural number:

Any natural number N can be expressed in standard form as

$$N = P_1^{n_1} \times P_2^{n_2} \times P_3^{n_3} \times \cdots \times P_r^{n_r}$$

where $P_1, P_2, \cdots P_r$ are distinct prime numbers and $n_1, n_2, \cdots n_r$ are positive integers

NOTE:

→ If $N = P_1^{n_1} \times P_2^{n_2} \times \cdots \times P_r^{n_r}$ is in standard form then (i) number of divisors of N are $d(N) = (n_1+1)(n_2+1)\cdots(n_r+1)$

(ii) Sum of divisors of N are $\sigma(N)$

$$\sigma(N) = \left[\frac{P_1^{n_1+1}-1}{P_1-1}\right] * \left[\frac{P_2^{n_2+1}-1}{P_2-1}\right] \times \cdots \left[\frac{P_r^{n_r+1}-1}{P_r-1}\right]$$

(iii) Product of divisors of N are

$$N^{\frac{1}{2}(n_1+1)(n_2+1)\cdots(n_r+1)} \Rightarrow N^{\frac{1}{2}d(N)}$$

1. Express the number 26 in the standard form then find

(i) No. of divisors

(ii) Sum of divisors

(iii) Product of divisors of 26

Sol: Given that $N = 26$

$\Rightarrow$

2	26
13	13
	1

$26 = 2^1 \times 13^1$

Here $P_1 = 2$, $P_2 = 13$

$n_1 = 1$, $n_2 = 1$

$\therefore$ (i) No. of divisors $d(N) = (n_1+1)(n_2+1)\cdots(n_r+1)$

$d(26) = (1+1)(1+1)$

$d(26) = (2)(2)$

$\therefore d(26) = 4$ [1, 2, 13, 26]

(ii) Sum of divisors $\sigma(26) = \left[\frac{2^2-1}{2-1}\right]\left[\frac{13^2-1}{13-1}\right]$

$= \left[\frac{3}{1}\right]\left[\frac{168}{12}\right]$ 42

$= 42$

(iii) Product of divisors $= (26)^{\frac{1}{2}(4)}$

$= (26)^2$

$= 676$

2. Express the following numbers in standard form. Hence find

(i) No. of divisors

(ii) Sum of divisors

(iii) Product of divisors of that numbers

(i) 54 (ii) 144 (iii) 1296

Sol: (i) Given that $N = 54$

$2 \mid 54$

$3 \mid 27$

$3 \mid 9$

$3 \mid 3$

1

$\Rightarrow 54 = 2^1 \times 3^3$

$P_1 = 2 \quad P_2 = 3$

$n_1 = 1 \quad n_2 = 3$

(i) No. of divisors $d(54) = (1+1)(3+1)$

$= (2)(4)$

$= 8$

(ii) Sum of divisors $\sigma(54) = \left(\frac{2^2-1}{2-1}\right)\left(\frac{3^4-1}{3-1}\right) = \left(\frac{3}{1}\right)\left(\frac{80}{2}\right)^{40}$

$= 120$

(iii) Product of divisors $= (54)^{\frac{1}{2}(8)}$ $= (54)^4$

$= 8503056$

(iii) Given that $N = 1296$

$$
\begin{array}{r|l}
2 & 1296 \\
2 & 648 \\
2 & 324 \\
2 & 162 \\
3 & 81 \\
3 & 27 \\
3 & 9 \\
3 & 3 \\
 & 1
\end{array}
$$

$1296 = 2^4 \times 3^4$

$\therefore P_1 = 2 \quad P_2 = 3$

$n_1 = 4 \quad n_2 = 4$

(i) No. of divisors $d(1296) = (4+1)(4+1)$

$= (5)(5)$

$= 25$

(ii) sum of divisors $\sigma(1296) = \left(\frac{2^5-1}{2-1}\right)\left(\frac{3^5-1}{3-1}\right)$

$= \left(\frac{31}{1}\right)\left(\frac{242}{2}\right)^{121}$

$= 31 \times 121$

$= 3751$

(iii) Product of divisors $= (1296)^{1/2(25)}$

12.5

$= 1296$

Greatest Common Divisor: If a,b are any two integers where atleast one is non zero then an integer d is said to be greatest common divisor of a,b if

(i) $d|a, d|b$ [d is common divisor]

(ii) If $c|a, c|b$ such that $c \leq d \; \forall \; c \in z^+$

Ex: It is represented as $(a,b) = d$

Ex: GCD of (15, 18) is

$\times$ [3 | 15 , 5 | 5 , 1] [2 | 18 , 3 | 9 , 3 | 3 , 1]

$15 = 3 \times 5$ $18 = 2 \times 3 \times 3$] $\times$

(i) We know that divisors of

$15 = 1, 3, 5, 15$

$18 = 1, 2, 3, 6, 9, 18$

Common divisors $= 1, 3$

$\therefore$ GCD $= 3$

(ii)
$$\begin{array}{r} 15 \overline{)18} (1 \\ 15 \\ \hline 3 \overline{)15} (5 \\ 15 \\ \hline 0 \end{array}$$

$\therefore$ GCD $= 3$

$(15, 18) = 3$

* GCD of numbers using prime factorization method

→ In this method we prime factorize the given numbers then we take the common prime factors then by multiplying them we get GCD of given numbers.

1. Find the GCD of 48, 52 using Prime factorization method.

2 | 48
2 | 24
2 | 12
2 | 6
3 | 3
1

2 | 52
2 | 26
13 | 13
1

$48 = 2^4 \times 3$ $\quad 52 = 2^2 \times 13$

$\therefore GCD = 4$

2. Find the GCD of 850, 680 by using Prime factorization method.

2 | 850
5 | 425
5 | 85
17 | 17
1

2 | 680
2 | 340
2 | 170
5 | 85
17 | 17
1

$850 = 2 \times 5 \times 5 \times 17$ $\quad 680 = 2 \times 2 \times 2 \times 5 \times 17$

$GCD = 2 \times 5 \times 17 = 170$

Division Algorithm: If a, b are any two integers and $a > b$ such that $a = bq + r$ where $0 \leq r < b$, $\forall r, q \in z$

Theorem: Prove that the GCD of two numbers is unique.

Proof: Let a, b are any 2 integers if possible assume d_1, d_2 are 2 GCDs of a, b

case-(i): Let d_1 is the GCD of a, b & d_2 is the common divisor

$\Rightarrow d_2 | d_1$ & $d_2 \leq d_1 \longrightarrow (1)$

case-(ii): Let d_2 is the GCD of a, b & d_1 is the common divisor

$\Rightarrow d_1 | d_2$ & $d_1 \leq d_2 \longrightarrow (2)$

From (1) & (2)

$d_1 = d_2$

i.e., The GCD of any 2 integers is unique.

NOTE:

→ If a, b, c are any 3 integers such that $c|a$ & $c|b$ then $c|a+b$, $c|a-b$

→ If a, b are any 2 integers and d is the GCD of a, b then it can be expressed as a linear combination of a, b

i.e., $d = ax + by$ $\forall x, y \in z$

1. Find the GCD of -12, 30. Hence express GCD as a linear combination -12, 30

$$-12)30(-2$$
$$\underline{24}$$
$$6)-12(-2$$
$$\underline{-12}$$
$$0$$

GCD = 6

$[6 = -12x + 30y]$ ×

$30 = -12(-2) + 6$

$-12 = 6(-2) + 0$

$30 = -12(-2) + 6$

$6 = 30 + 12(-2)$

$6 = 30x + 12y$ which is required linear combination.

$\therefore x, y = (1, -2)$

2. Find the GCD of 7200, 3132 Hence, express GCD as linear combination 7200, 3132

$$3132)7200(2$$
$$\underline{6264}$$
$$936)3132(3$$
$$\underline{2808}$$
$$324)936(2$$
$$\underline{648}$$
$$288)324(1$$
$$\underline{288}$$
$$36)288(8$$
$$\underline{288}$$
$$0$$

$7200 = 3132(2) + 936$

$3132 = 936(3) + 324$

$936 = 324(2) + 288$

$324 = 288(1) + 36$

$288 = 36(8) + 0$

$36 = 324 - 288$

$36 = 324 - [936 - 324(2)]$

$36 = 324 - 936 + 324(2)$

$36 = 324(3) - 936$

$36 = 3[3132 - 936(3)] - 936$

$36 = 3132(3) - 936(9) - 936$

$36 = 3132(3) + 936(-10)$

$36 = -10[7200 - 3132(2)] + 3132(3)$

$36 = 7200(-10) + 3132(23)$ which is required linear combination

$x = -10 \quad y = 23$

25/03/2022

3. Find the GCD of 24, 138 and express GCD as a linear combination of that numbers.

$$
\begin{array}{r|l}
24 & 138 \\
\hline
120 & 5 \\
\hline
18 & 24 \\
\hline
18 & 1 \\
\hline
6 & 18 \\
\hline
18 & 3 \\
\hline
0 &
\end{array}
$$

GCD = 6

$138 = 24(5) + 18 \Rightarrow 18 = 138 - 24(5)$

$24 = 18(1) + 6$

$18 = 6(3) + 0$

$6 = 24 - 18(1)$

$6 = 24 - 1\cancel{8}[138 - 24(5)]$

$6 = 24 - 138 + 24(5)$

$6 = 24(6) + 138(-1)$

$6 = 24x + 138y$ is the required linear combination

$(x, y) = (6, -1)$

4. Find the GCD of 198, 288, 512 then Express GCD as a linear combination of that numbers.

We know that $(198, 288, 512) = ((198, 288), 512)$

$\rightarrow (198, 288)$

$$
\begin{array}{r|l}
198 & 288 \ (1 \\
198 & \\
\hline
90 & 198 \ (2 \\
180 & \\
\hline
18 & 90 \ (5 \\
90 & \\
\hline
0 &
\end{array}
$$

$288 = 198(1) + 90$

$198 = 90(2) + 18$

$90 = 18(5) + 0$

$18 = 198 - 90(2)$

$18 = 198 - (2)[288 - 198(1)]$

$18 = 198 - 288(2) + 198(2)$

$18 = 198(3) - 288(2)$

$18 = 198(3) + 288(-2) \rightarrow (1)$

$(18, 512) \Rightarrow$

$$
\begin{array}{r|l}
18 & 512 \ (28 \\
504 & \\
\hline
8 & 18 \ (2 \\
16 & \\
\hline
2 & 8 \ (4 \\
8 & \\
\hline
0 &
\end{array}
$$

$512 = 18(28) + 8$

$18 = 8(2) + 2$

$8 = 2(4) + 0$

$$2 = 18 - 8(2)$$

$$2 = 18 - (2)[512 - 18(28)]$$

$$2 = 18 - 512(2) + 18(56)$$

$$2 = 18(57) + 512(-2) \rightarrow (2)$$

Sub (1) in (2)

$$2 = 57(198(3) + 288(-2)) + 512(-2)$$

$$2 = 198(171) + 288(-114) + 512(-2)$$

$2 = 198x + 288y + 512z$ which is required linear combination

where $x = 171$

$y = -114$

$z = -2$

5. Find the GCD of following numbers and express GCD as a linear combination of that numbers

(i) (426, 275)

(ii) (858, 325)

(iii) (3587, 1819)

(iv) (828, 342, 420)

Sol (iv) We know that $(228, 342, 420) = ((228, 342), 420)$

$(228, 342) \Rightarrow$

$$228\overline{)342}\,(1$$
$$\underline{228}$$
$$114\overline{)228}\,(2$$
$$\underline{228}$$
$$0$$

$$342 = 228(1) + 114$$

$$228 = 114(2) + 0$$

$$114 = 342 - 228(1) \rightarrow (1)$$

$$114 = 342x + 228(y)$$

$$\therefore (x, y) = (1, -1)$$

$(114, 420) \Rightarrow$

$$114\overline{)420}\,(3$$
$$\underline{342}$$
$$78\overline{)114}\,(1$$
$$\underline{78}$$
$$36\overline{)78}\,(2$$
$$\underline{72}$$
$$6\overline{)36}\,(6$$
$$\underline{36}$$
$$0$$

$$420 = 114(3) + 78$$

$$114 = 78(1) + 36$$

$$78 = 36(2) + 6$$

$$36 = 6(6) + 0$$

$6 = 78 - 36(2)$

$6 = 78 - (2)[114 - 78(1)]$

$6 = 78 - 114(2) + 78(2)$

$6 = 78(3) - 114(2)$

$6 \neq 48$

$6 = 3[420 - 114(3)] - 114(2)$

$6 = 420(3) - 114(9) - 114(2)$

$6 = 420(3) - 114(11)$

$6 = 420(3) + 114(-11) \rightarrow (2)$

Sub (1) in (2)

$6 = 420(3) + (-11)[342 - 228(1)]$

$6 = 420(3) + 342(-11) - 228(-11)$

$6 = 228(11) + 342(-11) + 420(3)$

$6 = 228x + 342y + 420z$ which is required linear combination

where $x = 11$, $y = -11$, $z = 3$

Euclidean Algorithm: Euclidean Algorithm is used to find the GCD of any 2 integers.

If a, b are any 2 integers and $a > b$ we have $a = bq + r$ where $0 \leq r < b$ [since by division algorithm] By Successively applying we get

$b = rq_1 + r_1$ where $0 \leq r_1 < r$

$r = r_1 q_2 + r_2$ where $0 \leq r_2 < r_1$

$r_1 = r_2 q_3 + r_3$ where $0 \leq r_3 < r_2$.

⋮

$r_{i-2} = r_{i-1} q_i + r_i \quad 0 \leq r_i < r_{i-1}$

$r_{i-1} = r_i \cdot q_{i+1} + 0$

After getting remainder zero the least non zero remainder is considered as GCD

$\Rightarrow (a, b) = r_i$

18/03/2022

State and prove Euclidean Algorithm

Statement: Euclidean Algorithm is used to find the GCD of any two integers.

If a, b are any two integers, $a > b$ then $a = bq + r$ where $0 \leq r < b$ [∵ by division algorithm] by Successively applying we get $b = rq_1 + r_1$ where $0 \leq r_1 < r$

$r = r_1 q_2 + r_2 \quad 0 \le r_2 < r_1$

$\vdots$

$r_{i-2} = r_{i-1} q_i + r_i \quad 0 \le r_i < r_{i-1}$

$r_{i-1} = r_i q_{i+1} + 0 \rightarrow$ (stop)

$\therefore \text{Gcd}(a,b) = r_i$ (least non zero remainder)

To prove this result we have to prove that if a, b are any two integers under $a = bq + r$ then $(a,b) = (b,r)$

Given that $a = bq + r \rightarrow (1)$

If possible let $(a,b) = d_1$ & $(b,r) = d_2$

Take $(a,b) = d_1$

$\Rightarrow d_1 | a \,,\, d_1 | b$

$\Rightarrow d_1 | a - bq$ (linear combination of a, b)

$\Rightarrow d_1 | r$ [$\because a - bq = r$ from (1)]

$\Rightarrow d_1 | b \,,\, d_1 | r$

$\Rightarrow d_1 | (b,r) \Rightarrow d_1 | d_2$

$\Rightarrow d_1 \le d_2 \rightarrow (2)$

Take $(b,r) = d_2$

$\Rightarrow d_2 | r \,,\, d_2 | b$

$\Rightarrow d_2 | bq + r$ [$\because$ linear combination of b, r]

$\Rightarrow d_2 | a$ ($\because bq + r = a$ from (1))

$\Rightarrow d_2 | a \,,\, d_2 | b$

$\Rightarrow d_2 | (a, b)$

$\Rightarrow d_2 | d_1$

$\Rightarrow d_2 \leq d_1 \rightarrow (3)$

from (2) & (3)

we have $d_1 = d_2$

i.e., If $a = bq + r$ then $(a, b) = (b, r)$

Find the GCD of 4321, 5295 using Euclidean Algorithm

$$
\begin{array}{r}
1 \\
4321 \overline{)5295} \\
\underline{4321} \\
974 \overline{)4321} \\
\underline{3896} \\
425 \overline{)974} \\
\underline{850} \\
124 \overline{)425} \\
\underline{372} \\
53 \overline{)124} \\
\underline{106} \\
18 \overline{)53} \\
\underline{36} \\
17 \overline{)18} \\
\underline{17} \\
1 \overline{)17} \\
\underline{17} \\
0
\end{array}
\quad
\begin{array}{l}
(1 \\
(4 \\
(2 \\
(3 \\
(2 \\
(2 \\
(1
\end{array}
$$

Here $5295 = 4321(1) + 974$

$4321 = 974(4) + 425$

$974 = 425(2) + 124$

$425 = 124(3) + 53$

$124 = 53(2) + 18$

$53 = 18(2) + 17$

$18 = 17(1) + 1$

$17 = 1(17) + 0$ (stop)

$\Rightarrow (4321, 5295) = 1$ which is least non-zero remainder.

Find the GCD of following integers using Euclidean Algorithm

(i) (45, 75)

(ii) (12, 33)

(iii) (25, 150)

(iv) (750, 900)

Sol: (iv) (750, 900)

$$\begin{array}{r} 750)900(1 \\ \underline{750} \\ 150)750(5 \\ \underline{750} \\ 0 \end{array}$$

$900 = 750(1) + 150$

$750 = 150(5) + 0$

$\therefore (750, 900) = 150$ which is least non-zero remainder.

29/03/2022

State and prove fundamental theorem of Arithmetic. (or) unique factorisation theorem

Statement: Every positive integer which is greater than 1 can be uniquely expressed as a product of prime factors (written in increasing order)

Proof: Let n be any positive integer which is greater than 1.

We know that n has atleast one Prime factor (P_1)

$\Rightarrow n = P_1 \cdot n_1 \longrightarrow (1)$ where $n > n_1$

if $n_1 = 1 \Rightarrow n = P_1$

The result is proved.

if $n_1 > 1$

We know that n_1 has atleast one Prime factor (P_2)

$\Rightarrow n_1 = P_2 \cdot n_2$

$n = P_1 \cdot P_2 \cdot n_2 \longrightarrow (2)$ where $n > n_1 > n_2$

if $n_2 = 1$

$\Rightarrow n = P_1 \cdot P_2$

Hence the result is proved

If $n_3 > 1$ [We know that n_2 has atleast one prime factor] (P_3)

$n_2 = P_3 n_3$

$n = P_1 P_2 P_3 n_3 \rightarrow (3)$ where $n > n_1 > n_2 > n_3$

If $n_3 = 1 \Rightarrow n = P_1 P_2 P_3$

Hence the result is proved

By successively repeating above steps we get $n = P_1 P_2 P_3 \cdots P_k n_k$ where

$n_k = 1$

$\Rightarrow n = P_1 P_2 P_3 \cdots P_k \rightarrow (4)$

i.e., n is expressed as a product of Prime factors.

Uniqueness

If possible let there exists one more set of prime factors $q_1, q_2, q_3, \cdots q_r$ such that

$n = q_1 q_2 q_3 \cdots q_r \rightarrow (5)$

we have to prove that $k = r$ and $P_i = q_j \; \forall \; i, j$

from (4) & (5)

$P_1 P_2 P_3 \cdots P_k = q_1 q_2 q_3 \cdots q_r$

$\Rightarrow \frac{P_1}{q_1 q_2 q_3 \cdots q_r}$

$\Rightarrow p_1$ divides any q_j

without loss of generality Let

p_1 divides q_1

$\Rightarrow p_1/q_1 \Rightarrow p_1 = 1$ (or) $p_1 = q_1$

we know that $p_1 \neq 1 \Rightarrow p_1 = q_1$

similarly

we can prove that $p_1 = q_1$, $p_2 = q_2$, $p_3 = q_3$, ---

if possible Let us assume $k < r$

$\Rightarrow p_1 p_2 p_3 \cdots p_k = q_1 q_2 q_3 \cdots q_k q_{k+1} \cdots q_r$

$1 = q_{k+1} q_{k+2} \cdots q_r$

which is not possible

$\Rightarrow k \not< r$

similarly, we can prove that $k \not> r$

$\Rightarrow k = r$ & $p_i = q_j \ \forall i, j$

i.e., every positive integer which is greater than 1 can be uniquely expressed as a product of prime factors.

1- Using fundamental theorem of Arithmetic (or) unique factorization theorem express the following numbers as a product of prime numbers

(i) 5544

(ii) 2520

(iii) 240

(iv) 1001

(v) 5040

(vi) 289

(vii) 9999

(viii) 4249845

Sol: (i) 5544

2	5544
2	2772
2	1386
3	693
3	231
7	77
11	11
	1

i.e., $5544 = 2 \times 2 \times 2 \times 3 \times 3 \times 7 \times 11$

$= 2^3 \times 3^2 \times 7^1 \times 11^1$

(viii) 4849845

3	4849845
5	1616615
7	323323
11	46189
13	4199
17	323
19	19
	1

$4849845 = 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19$

(vii) 9999

3	9999
3	3333
11	1111
101	101
	1

$9999 = 3 \times 3 \times 11 \times 101$

$= 3^2 \times 11 \times 101$

(ii) 2520

2	2520
2	1260
2	630
3	315
3	105
5	35
7	7
	1

$2520 = 2^3 \times 3^2 \times 5 \times 7$

Fermat Numbers: An integer which is defined as $2^{2^n}+1 \ \forall n \geq 0$ is known as fermat number. It is represented by

$f_n = 2^{2^n}+1 \ \forall n \geq 0$

$f_1 = 3, f_2 = 5, f_3 = 17, f_4 = 257$ are few fermat numbers.

NOTE:

All fermat numbers are prime numbers.

factorization of an integer by fermat method

(or)

fermat factorization method

Step-1: If 'n' is any integer

$n = x^2 - y^2$

Step-2: ~~$x^2 - n \neq y^2$~~ express above result as

$x^2 - n = y^2$

Step-3: Find the least value of k such that $k^2 - n = y^2$

Step-4: Find the values of $(k+1)^2 - n, (k+2)^2 - n$. ... till getting a perfect square $(m^2 - n)$

Step-5: i.e., $m^2 - n = y^2$

$\Rightarrow n = m^2 - y^2$

$\Rightarrow n = (m+y)(m-y)$ which is required factorization

NOTE:

Any number is said to be a Perfect square if the last two digits of that number is 00, 01, 04, 09, 16, 21, 24, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96

1. Use Fermat factorization method to factorize $n = 119143$

We know that $(345)^2 < 119143 < (346)^2$

$\Rightarrow (346)^2 - 119143 = 573$ ×

$\Rightarrow (347)^2 - 119143 = 1266$ ×

$\Rightarrow (348)^2 - 119143 = 1961$ ×

$\Rightarrow (349)^2 - 119143 = 2658$ ×

$\Rightarrow (350)^2 - 119143 = 3357$ ×

$\Rightarrow (351)^2 - 119143 = 4058$ ×

$\Rightarrow (352)^2 - 119143 = 4761 = 69^2$

$(352)^2 - 119143 = (69)^2$

$119143 = (352)^2 - (69)^2$

$119143 = (352+69)(352-69)$

$119143 = (421)(283)$

which is required factorization

2. Use Fermat factorization method to factorize $n = 23449$

We know that $(153)^2 < 23449 < (154)^2$

$(154)^2 - 23449 = 267$

$(155)^2 - 23449 = 576 = (24)^2$

$(155)^2 - 23449 = (24)^2$

$23449 = (155)^2 - (24)^2$

$23449 = (155+24)(155-24)$

$23449 = (179)(131)$

which is required factorization

30/03/2022

Congruences: The word congruence was introduced by Karl.f.Gauss. It is represented by $\equiv$

If n is a positive integer then two numbers a,b are said to be congruence modulo n if n divides $a-b$ (or) $a-b=nk \ \forall \ k \in z$, it is represented by $a \equiv b \pmod n$

Ex: 1) $3 \equiv 24 \pmod 7$ [$\because 7$ divides -21]

2) $-31 \equiv 11 \pmod 7$ [$\because 7 \mid -42$]

3) $-15 \equiv -64 \pmod 7$ [$\because 7 \mid 49$]

4) $6 \not\equiv 1 \pmod 3$ [$\because 3 \nmid 5$]

Note:

→ Any two numbers are always congruent to 1

→ Any two numbers are said to be congruent to 2 if both are either even (or) odd

→ If 'a' is any integer greater than 0 by division algorithm we have

$a = nq + r$ where $0 \leq r < n$

$\Rightarrow a - r = nq$

$\Rightarrow a \equiv r \pmod{n}$ where $r = 0, 1, 2, \cdots n-1$

Linear congruence:

If 'n' is a positive integer then the congruence $ax \equiv b \pmod{n}$ is known as a linear congruence in one variable.

NOTE:

→ The linear congruence $ax \equiv b \pmod{n}$ is said to have a solution if

(i) $(a,n) \mid b$

(ii) $(a,n) \nmid b$ then the congruence $ax \equiv b \pmod{n}$ do not have a solution

(iii) $(a,n) = d$ and $d \mid b$ then the linear congruence $ax \equiv b \pmod{n}$ will have d incongruent solution.

(iv) The solution set is obtained by

$x = x_0 + \left(\frac{n}{d}\right)t$ where x_0 is initial solution

$t = 0, 1, 2, \ldots d-1$

Linear diphantine equation:

If $ax \equiv b \pmod n$ is a linear congruence, it can be expressed as $ax = b + ny$

$\Rightarrow ax - ny = b$ which is known as linear diphantine equation.

01/04/22

Find all possible solutions of the linear congruence $9x \equiv 12 \pmod{15}$

Method I

Given that $9x \equiv 12 \pmod{15} \rightarrow (1)$

compare (1) with $ax \equiv b \pmod n$

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

we know that GCD $(9, 15) = 3$

$\therefore (9, 15) = 3$ which divides 12

$9) 15 (1$
$\quad 9$
$6) 9 (1$
$\quad 6$
$3) 6 (2$
$\quad 6$
$\quad 0$

$\therefore$ Given congruence $9x \equiv 12 \pmod{15}$ will have 3 solutions

$\Rightarrow$ Solution set $x = x_0 + \left(\frac{n}{d}\right)t \quad \forall \; t = 0, 1, 2$

we know that linear diphantine equation of given congruence is $9x - 15y = 12 \rightarrow (2)$

By Euclidean Algorithm, we have

$15 = 9(1) + 6$

$9 = 6(1) + 3$

$6 = 3(2) + 0 \rightarrow$ (stop)

have $3 = 9 - 6$

$3 = 9 - [15 - 9]$

$3 = 9(2) - 15$

$\Rightarrow 9(2\times4) - 15(1\times4) = 3\times4$

$9(8) - 15(4) = 12 \longrightarrow (3)$

from (2) & (3) we have $x_0 = 8, y_0 = 4$

∴ solution set $x = 8 + \left(\frac{15}{3}\right)t \quad \forall\ t = 0, 1, 2$

$x = 8 + 5(t)$

$x = 8,\ x = 13,\ x = 18$

$\Rightarrow x \equiv 8 \pmod{15}$,

$x \equiv 13 \pmod{15}$

$x \equiv 18 \pmod{15} = 3 \pmod{15}$ are three possible solutions [∵ 18 > 15]

Method - II

Given that $9x \equiv 12 \pmod{15} \longrightarrow (1)$

Compare (1) with $ax \equiv b \pmod{n}$

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

Now GCD(9, 15) = 9) 15 (1
9
6) 9 (1
6
3) 6 (2
6
0

$\Rightarrow (9, 15) = 3$ which divides 12.

. Given congruence $9x \equiv 12 \pmod{15}$ will have 3 solutions.

$\Rightarrow$ Solution set $x = x_0 + \left(\frac{n}{d}\right)t \quad \forall\, t = 0,1,2$

w.k.t $9x \equiv 12 \pmod{15}$

if $x = 1 \Rightarrow 9 - 12 = -3$

15 does not divide -3

if $x = 2 \Rightarrow 15 \nmid 6$ ✗

if $x = 3 \Rightarrow 15 \mid 15$ ✓

$\Rightarrow$ let $x_0 = 3$ is the initial solution of given congruence

$\Rightarrow x = 3 + \left(\frac{15}{3}\right)t \quad \forall\, t = 0,1,2$

$x = 3 + 5t$

$\Rightarrow x = 3,\ x = 13,\ x = 8$

$\Rightarrow x = 3 \pmod{15}$

$x = 8 \pmod{15}$

$x = 13 \pmod{15}$ are three possible solutions

2. find all possible solutions of the linear congruence $7x \equiv 1 \pmod{31}$

Method - I

Given that $7x \equiv 1 \pmod{31} \longrightarrow (1)$

Compare (1) with $ax \equiv b \pmod{n}$

$\Rightarrow a = 7,\ b = 1,\ n = 31$

WKT $GCD(7,31) =$

$7)31(4$
28
$3)7(2$
6
$1)3(3$
3
0

$\Rightarrow (7,31) = 1$ which divides 1

∴ Given congruence $7x \equiv 1 \pmod{31}$ will have 1 solution.

⇒ solution set $x = x_0 + \left(\frac{b}{d}\right)t \quad \forall\ t = 0$

Next linear diphantine eqn of given congruence is $7x - 31y = 1 \longrightarrow (2)$

By euclidean Algorithm, we have

$$31 = 7(4) + 3$$
$$7 = 3(2) + 1$$
$$3 = 1(3) + 0 \longrightarrow \text{Stop}$$

here

$$1 = 7 - 3(2)$$
$$1 = 7 - (2)[31 - 7(4)]$$
$$1 = 7(9) - 31(2) \longrightarrow (3)$$

Comparing (2) & (3), we get

$x_0 = 9$ and $y_0 = 2$

∴ solution set $x = 9 + \left(\frac{31}{1}\right)t \quad \forall\ t = 0$

$$x = 9 + 31(0)$$
$$x = 9$$

⇒ $x \equiv 9 \pmod{31}$ is the possible solution.

Method - II

W.K.t $7x \equiv 1 \pmod{31}$

if $x = 1 \Rightarrow 7 - 1 = 6$

31 doesn't divide 6

if $x = 2 \Rightarrow 13 | 31$ ×

if $x = 3 \Rightarrow$ ×

if $x = 4 \Rightarrow$ ×

if $x=5 \Rightarrow 31 \mid 34$

if $x=6 \Rightarrow 42-1=41 \quad 31 \mid 41$ ×

if $x=7 \Rightarrow 49-1=48 \quad 31 \mid 48$ ×

if $x=8 \Rightarrow 56-1=55 \quad 31 \mid 55$ ×

if $x=9 \Rightarrow 63-1=62 \quad 31 \mid 60$ ✓

$\Rightarrow$ let $x_0=9$ is the initial solution of given congruence

$$x = 9 + \left(\frac{31}{1}\right)t \quad \forall\ t=0$$

$$x = 9 + 31(0)$$

$$x = 9$$

$\Rightarrow x \equiv 9 \pmod{31}$ is the possible solution

06/04/2022

Find all possible solutions of $14x \equiv 12 \pmod{18}$

Given that $14x \equiv 12 \pmod{18} \rightarrow (1)$

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

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

we know that $(14, 18)$

$$\begin{array}{r} 14 \overline{)18} (1 \\ 14 \\ \hline 4 \overline{)14} (3 \\ 12 \\ \hline 2 \overline{)4} (2 \\ 4 \\ \hline 0 \end{array}$$

$(14, 18) = 2 \mid 12$

∴ The given congruence will have 2 incongruent

solutions

∴ solution set $x = x_0 + \left(\frac{n}{d}\right)t \quad \forall \quad t = 0, 1$

we know that linear diphantine eqn of ①

$$14x - 18y = 12 \longrightarrow ②$$

By euclidean algorithm we have

$$18 = 14(1) + 4$$
$$14 = 4(3) + 2$$
$$4 = 2(2) + 0 \longrightarrow \text{stop}$$

$$2 = 14(4) - 18(3)$$

$$14(24) - 18(18) = 12 \longrightarrow ③$$

but $x_0 = 24$ is the initial solution

∴ solution set $x = 24 + \left(\frac{18}{2}\right)t \quad \forall \quad t = 0, 1$

$\Rightarrow x = 24, 33$

i.e, $x \equiv 24 \pmod{18} \Rightarrow x \equiv 6 \pmod{18}$

$x \equiv 33 \pmod{18} \Rightarrow x \equiv 15 \pmod{18}$

are the possible solutions of given congruen

4. check whether the following linear congruences will have a solution or not then find all possible solutions of

(i) $9x \equiv 6 \pmod{15}$

(ii) $10x \equiv 15 \pmod{45}$

(iii) $183x \equiv 15 \pmod{31}$

(i) $9x \equiv 6 \pmod{15}$

Given that $9x \equiv 6 \pmod{15} \rightarrow (1)$

$ax \equiv b \pmod{n}$

$a = 9,\ b = 6,\ n = 15$

we know that $(9, 15)$

$$
\begin{array}{r}
9 \overline{)15} (1 \\
\underline{9} \\
6 \overline{)9} (1 \\
\underline{6} \\
3 \overline{)6} (2 \\
\underline{6} \\
0
\end{array}
$$

$(9, 15) = 3 \mid 6 = 2$

$9x - 15y = 6 \rightarrow (2)$

By Euclidean algorithm

$15 = 9(1) + 6$

$9 = 6(1) + 3$

$6 = 3(2) + 0 \rightarrow$ Stop

$9 = 6(1) + 3$

$3 = 9 - 6(1)$

$3 = 9 - (15 - 9(1))(1)$

$3 = 9(2) - 15(1)$

By (2)

$9(4) - 15(2) = 6 \rightarrow (3)$

from (2) & (3)

$x_0 = 4$ be the initial solution

solution of diphantine equation

$$x = x_0 + \left(\frac{b}{d}\right)t \quad \forall\ t = 0, 1, 2$$

$$x = 4 + \left(\frac{15}{2}\right)t$$

$$x = 4, 9, 14$$

$x \equiv 4 \pmod{15} \Rightarrow x \equiv 3 \pmod{15}$

$x \equiv 9 \pmod{15} \Rightarrow x \equiv 6 \pmod{15}$

$x \equiv 14 \pmod{15} \Rightarrow x \equiv 1 \pmod{15}$

are the possible solutions of given congruence.

8/4/22

System of linear congruences:

A linear congruence which is in the form $ax + by \equiv r \pmod{n}$

$cx + dy = s \pmod{n}$ is known as a system of linear congruence in 2 variable where n is positive integer and $a, b, c, d, r, s \in z$

Note: The necessary and sufficient condition for the system of linear congruences $ax + by \equiv r \pmod{n}$ & $cx + dy \equiv s \pmod{n}$ to have an unique solution is $(ad - bc, n) = 1$

1. Find the solutions of the system of linear congruences $3x+4y \equiv 5 \pmod{13}$
$2x+5y \equiv 7 \pmod{13}$

Sol. Given $3x+4y \equiv 5 \pmod{13} \longrightarrow (1)$
$2x+5y \equiv 7 \pmod{13} \longrightarrow (2)$

compare above congruences with
$ax+by \equiv r \pmod{n}$ &
$cx+dy \equiv s \pmod{n}$

$a=3 \quad b=4 \quad r=5 \quad n=13$
$c=2 \quad d=5 \quad s=7$

$(ad-bc, n) = (7, 13)$

$7)13(1$
$\underline{7}$
$6)7(1$
$\underline{6}$
$1)6(6$
$\underline{6}$
0

$(ad-bc, n) = 1$
∴ Given system of linear congruences have unique solution

From (1) & (2)
we have
$15x+20y \equiv 25 \pmod{13}$
$8x+20y \equiv 28 \pmod{13}$
$\overline{7x \equiv -3 \pmod{13}} \longrightarrow (3)$

we know that $(7, 13) = 1$

$\Rightarrow$ ③ will have unique solution

WKT linear diphantine eqn of ③ is

$$7x - 13y = -3 \rightarrow ④$$

By euclidean algorithm we have

$$13 = 7(1) + 6$$
$$7 = 6(1) + 1$$
$$6 = 1(6) + 0 \text{ (stop)}$$

$$1 = 7 - 6$$
$$1 = 7 - (13 - 7)$$
$$1 = 7(2) - 13(1)$$

mul with (-3)

$$7(-6) - 13(-3) = -3 \rightarrow ⑤$$

from ④ & ⑤

$$x_0 = -6, \quad y_0 = -3$$

∴ The solution set $x = -6 + \left(\frac{13}{1}\right)t \; \forall \; t = 0$

$$x = -6 \Rightarrow x \equiv 6 \pmod{13}$$

(or)

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

from ① & ② we have

$$6x + 8y \equiv 10 \pmod{13}$$
$$6x + 15y \equiv 21 \pmod{13}$$

$$-7y \equiv -11 \pmod{13}$$

$7y = 11 \pmod{13} \rightarrow (6)$

$(7, 13) = 1$

(6) will have unique solution

Now linear diophantine eqn of (6) is

$7y - 13x = 11 \rightarrow (7)$

By Euclidean algorithm we have

$7(2) - 13(1) = 1$

Mul with 11

$7(22) - 13(11) = 11 \rightarrow (8)$

from (7) & (8)

$y_0 = 22 \quad x_0 = 11$

The solution set $y = 22 + \left(\frac{13}{1}\right)t \quad \forall\, t = 0$

$y = 22 \Rightarrow y \equiv 22 \pmod{13}$

(or)

$y \equiv 9 \pmod{13}$.

$x \equiv 7 \pmod{13}$ & $y \equiv 9 \pmod{13}$ is unique solution.

2. check wheather the following system of linear congruences have a solution or not. If so then find solution of

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

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

Sol: Given $7x+3y \equiv 10 \pmod{16} \rightarrow (1)$

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

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

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

$(ad-bc, n) = (29, 16)$

$16)29(1$
$\underline{16}$
$13)16(1$
$\underline{13}$
$3)13(4$
$\underline{12}$
$1)3(3$
$\underline{3}$
0

$(ad-bc, n) = 1$

unique solution

From (1) & (2)

$35x+15y \equiv 50 \pmod{16}$

$-6x+15y \equiv 27 \pmod{16}$

$29x \equiv 23 \pmod{16} \rightarrow (3)$

WKT $(29, 16) = 1$

unique solution

linear diphantine eq (3) is

$29x - 16y = 23 \rightarrow (4)$

By Euclidean algorithm

$29 = 16(1) + 13$

$16 = 13(1) + 3$

$13 = 3(4) + 1$

$8 = 1(3) + 0$

$1 = 13 - 3(4)$

$1 = 13 - (16 - 13(1))(4)$

$1 = 13(5) - 16(4)$

$1 = (29 - 16(1))(5) - 16(4)$

$1 = 29(5) - 16(5) - 16(4)$

$1 = 29(5) - 16(9)$

$29(115) - 16(207) = 23 \rightarrow (5)$

From (4) & (5)

$x_0 = 115 \quad y_0 = 207$

∴ solution Set $x = 115 + \left(\frac{16}{1}\right)t \quad \forall t = 0$

$x = 115 \Rightarrow x \equiv 115 \pmod{16}$

(or)

$x \equiv 3 \pmod{16}$

From (1) & (2)

$14x + 86y \equiv 20 \pmod{16}$

$14x + 35y \equiv 63 \pmod{16}$

$+29y = +43 \pmod{16} \rightarrow (6)$

$(29, 16) = 1$

unique solution

linear diphantine of eq (6) is

$29y - 16x = 43 \rightarrow (7)$

$1 = 29(5) - 16(9)$ ×43

$29(215) - 16(387) = 43 \rightarrow (2)$

$y_0 = 215 \quad x_0 = 387$

solution set $y = 215 + \left(\frac{16}{1}\right)t \quad \forall\ t = 0$

$y \equiv 215 \pmod{16}$

(or)

$y \equiv 7 \pmod{16}$

16 | 215 | 13
208
7
1

9/4/22

Chinese Remainder Theorem:

If $n_1, n_2, n_3 \ldots n_r$ is pair wise relatively Prime +ve integers then set of linear congruences $x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$ ... $x = a_r \pmod{n_r}$ will have an unique simultaneous solution mod $n_1 \cdot n_2 \cdot n_3 \ldots n_r$

Proof:

Given that $n_1, n_2, \ldots n_r$ are relatively Prime positive integers

$\Rightarrow (n_i, n_j) = 1 \quad \forall\ i \neq j$

let $n = n_1 n_2 n_3 \ldots n_r$

Define $N_K = \frac{n}{n_K} \quad \forall\ K = 1, 2, 3 \ldots r$.

$N_1 = \frac{n}{n_1} \Rightarrow \frac{n_1 n_2 n_3 \ldots n_r}{n_1} \Rightarrow (N_1, n_1) = 1$

$N_2 = \frac{n}{n_2} \Rightarrow \frac{n_1 n_2 n_3 \ldots n_r}{n_2} \Rightarrow (N_2, n_2) = 1$

$(N_k, n_k) = 1$

∴ Above system of linear congruences will have a solution

$\Rightarrow N_k x_k \equiv 1 \pmod{n_k} \quad \forall\ k = 1, 2, 3, \ldots r$

Let $x = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$ be the simultaneous solution of above all congruences

Uniqueness

If possible let their exist an integer x' which satisfies above all congruences

$\Rightarrow x \equiv x' \pmod{n_k} \quad \forall\ k = 1, 2, \ldots r$

$\Rightarrow n_k \mid x - x'$

$n_1 \mid x - x',\ n_2 \mid x - x' \ldots n_r \mid x - x'$

i.e., $n_1 n_2 n_3 \ldots n_r \mid x - x'$

$\Rightarrow n \mid x - x'$

$\Rightarrow x \equiv x' \pmod{n}$ which is unique solution.

1. Using Chinese remainder theorem Solve the system of linear congruences

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Sol: Given that

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Compare above congruences with

$x_1 = a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $x \equiv a_3 \pmod{n_3}$

$a_1 = 2 \quad a_2 = 3 \quad a_3 = 2$

$n_1 = 3 \quad n_2 = 5 \quad n_3 = 7$

we know that n_1, n_2, n_3 are pairwise relatively prime integers.

By chinese remainder theorem above all congruences will have unique solution.

let $x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3$ is the unique solution where

$$n = n_1 n_2 n_3 = 3 \cdot 5 \cdot 7$$
$$= 105$$

Define $N_K = \frac{n}{n_K} \quad \forall \; K = 1, 2, 3$

$$N_1 = \frac{105}{3} = 35$$

$N_2 = \frac{105}{5} = 21$

$N_3 = \frac{105}{7} = 15$

$\therefore (N_1, n_1) = (35, 3) = 1 \Rightarrow 35x_1 \equiv 1 \pmod 3 \rightarrow (1)$

have unique solution

if $x_1 = 1 \Rightarrow 3 \mid 34$

$x_1 = 2 \Rightarrow 3 \mid 69$

$\therefore x_1 = 2$

II^{ly} $(N_2, n_2) = (21, 5) = 1$

$\Rightarrow 21x_2 \equiv 1 \pmod 5$ have unique solution

if $x_2 = 1 \Rightarrow 5 \mid 20$

$\therefore x_2 = 1$

$(N_3, n_3) = (15, 7) = 1$

$\Rightarrow 15x_3 \equiv 1 \pmod 7$ have unique solution

if $x_3 = 1 \Rightarrow 7 \mid 14$

$\therefore x_3 = 1$

i.e., $x = 2(35)(2) + (3)(21)(1) + (2)(15)(1)$

$x = 140 + 63 + 30$

$x = 233$

$x \equiv 233 \pmod{105}$ is unique solution

(or)

$x \equiv 23 \pmod{105}$

Q.No 2

Solve the following system of linear congruences using chinese remainder theorem $x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 7$

$x \equiv 3 \pmod{11}$

Sol: By comparing given congruences with

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

$x \equiv a_3 \pmod{n_3}$

we have

$a_1 = 1, a_2 = 1, a_3 = 3$

$n_1 = 5, n_2 = 7, n_3 = 11$

WKT

n_1, n_2, n_3 are pairwise relatively prime integers

By chinese remainder theorem given set of linear congruences will have an unique solution

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \rightarrow (1)$$

Let $n = n_1 n_2 \cdot n_3$

$= 5 \cdot 7 \cdot 11$

$= 385$

Define $N_K = \frac{n}{n_K} \quad \forall \; K = 1, 2, 3$

$N_1 = \frac{385}{5} = 77$

$N_2 = \frac{385}{7} = 55$

$N_3 = \frac{385}{11} = 35$

$(N_1, n_1) = (77, 5) = 1$

$77x_1 \equiv 1 \pmod 5 \rightarrow$ ② will have unique solution

if $x_1 = 1 \Rightarrow 5 \nmid 76$ ×

$x_1 = 2 \Rightarrow 5 \nmid 153$ ×

$x_1 = 3 \Rightarrow 5 \mid 230$ ✓

$\therefore \boxed{x_1 = 3}$

similarly

$(N_2, n_2) = (55, 7) = 1$

$55x_2 \equiv 1 \pmod 7 \rightarrow$ ② will have unique solution

if $x_2 = 1 \Rightarrow 7 \nmid 54$ (×)

$x_2 = 2 \Rightarrow 7 \nmid 109$ (×)

$x_2 = 3 \Rightarrow 7 \nmid 164$ (×)

$x_2 = 4 \Rightarrow 7 \nmid 219$ (×)

$x_2 = 5 \Rightarrow 7 \nmid 274$ (×)

$x_2 = 6 \Rightarrow 7 \mid 329$ (✓)

$\therefore \boxed{x_2 = 6}$

$(N_3, n_3) = (35, 11) = 1$

$35x_3 \equiv 1 \pmod{11}$ will have unique solution

if $x_3 = 1 \Rightarrow 11 | 34\ (x)$

$x_3 = 2 \Rightarrow 11 | 69\ (x)$

$x_3 = 3 \Rightarrow 11 | 104\ (x)$

$x_3 = 4 \Rightarrow 11 | 139\ (x)$

$x_3 = 5 \Rightarrow 11 | 174\ (x)$

$x_3 = 6 \Rightarrow 11 | 209\ (\checkmark)$

$\therefore \boxed{x_3 = 6}$

Sub in (1)

$$x = (1)(77)(3) + (1)(55)(6) + (3)(35)(6)$$
$$= 1191$$

$x \equiv 1191 \pmod{385}$ is unique solution

(or)

$x \equiv 36 \pmod{385}$

HW

check whether the given system of linear congruences of a solution, if so solve

$x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 4$

$x \equiv 4 \pmod 5$

Solution of set of linear congruences

$x = a_1 \pmod{n_1}$

$x = a_2 \pmod{n_2}$

⋮

$x = a_r \pmod{n_r}$ where $n_1, n_2, \ldots n_r$ not necessarily relatively prime. In such case chinese remainder theorem is not applicable.

→ We get the solution of above congruences by using iterative method

→ The set of congruences

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

⋮

$x \equiv a_3 \pmod{n_r}$ will have an unique solution if GCD of $(n_i, n_j) \mid a_i - b_i \; \forall \; i \neq j$

1. Find the value of x if possible such that $x \equiv 4 \pmod{8}$

$x \equiv 6 \pmod{6}$ ∴

Let $x \equiv 4 \pmod{8} \rightarrow (1)$

$x \equiv 6 \pmod{6} \rightarrow (2)$

wkt $a_1 = 4, a_2 = 6$

$n_1 = 8, n_2 = 6$

Here $(n_1, n_2) = 2 \Rightarrow n_1, n_2$ are not relatively prime.

∴ Chinese remainder theorem is not applicable

$(1) \Rightarrow x \equiv 4 \pmod{8}$

$x = 4 + 8y$ — (3)

Sub (3) in (2)

$4 + 8y \equiv 6 \pmod 6$

$8y \equiv 2 \pmod 6$

$4y \equiv 1 \pmod 3$

if $y = 1 \Rightarrow 3 \mid 3$

$\therefore y_0 = 1$

$y = 1 + 3t$

(3) $\Rightarrow x = 4 + 8(1 + 3t)$

$x = 12 + 24t$

$x \equiv 12 \pmod{24}$ is the unique solution of given congruence.

2. Find the value of x if possible such that $x \equiv 6 \pmod 5$

$x \equiv 1 \pmod{15}$

Let $x \equiv 1 \pmod{15} \rightarrow (1)$

$x \equiv 6 \pmod 5 \rightarrow (2)$

wkt $a_1 = 1$, $a_2 = 6$

$n_1 = 15$, $n_2 = 5$

Here $(n_1, n_2) = (15, 5) = 5 \Rightarrow n_1, n_2$ are not

∴ Chinese remainder theorem is not applicable

⑦ ⇒ here $(n_1, n_2) = 5|1-6$

$= 5|-5$ (✓)

Given congruences will have unique solution

∴ By iteration method

① ⇒ $x \equiv 1 \pmod{15}$

$x = 1 + 15y \rightarrow ③$

Sub ③ in ②

$1 + 15y \equiv 6 \pmod 5$

$15y \equiv 5 \pmod 5$

$3y \equiv 1 \pmod 1$

if $y = 1 \Rightarrow 2|1$ (✓)

$\therefore y_0 = 1$

$y = 1 + 1t$

③ ⇒ $x = 1 + 15(1 + t)$

$x = 1 + 15 + 15t$

$x = 16 + 15t$

$x \equiv 16 \pmod{15}$ is the unique solution of given congruence.

(or)

$x \equiv 1 \pmod{15}$

8/04/2022

3. Find the value of x if possible such that $x \equiv 4 \pmod 6$
$x \equiv 2 \pmod 8$
$x \equiv 1 \pmod 7$

Sol: Let $x \equiv 2 \pmod 8 \rightarrow (1)$
$x \equiv 1 \pmod 7 \rightarrow (2)$
$x \equiv 4 \pmod 6 \rightarrow (3)$

Given that $n_1 = 6, n_2 = 8, n_3 = 7$

WKT $(n_1, n_2) = (6, 8) = 2$

$\therefore n_1, n_2, n_3$ are not pairwise relatively prime integers

$\rightarrow$ CRT is not applicable

By applying iterative method we have

$x \equiv 2 \pmod 8 \rightarrow (1)$
$x \equiv 1 \pmod 7 \rightarrow (2)$
$x \equiv 4 \pmod 6 \rightarrow (3)$

Here $(8, 7) \mid 2-1$ ✓

$(7, 6) \mid 1-4$

$(8, 6) \mid (2-4)$

$\therefore$ Given set of congruences will have unique solution

$(1) \Rightarrow x = 2 + 8y \rightarrow (4)$

sub (4) in (2)

$2+8y \equiv 1 \pmod 7$

$8y \equiv -1 \pmod 7$

if $y=1 \Rightarrow 7 \nmid 9(x)$

$y=2 \Rightarrow 7 \mid 17(x)$

$y=3 \Rightarrow 7 \mid 25(x)$

$y=4 \Rightarrow 7 \mid 33(x)$

$y=5 \Rightarrow 7 \mid 41(x)$

$y=6 \Rightarrow 7 \mid 49(\checkmark)$

Let $y_0 = 6$ is the initial solution

$y = 6 + 7w \rightarrow (5)$

Sub (5) in (4)

$x = 2 + 8(6+7w)$

$x = 2 + 48 + 56w$

$x = 50 + 56w \rightarrow (6)$

Sub (6) in (3)

$50 + 56w \equiv 4 \pmod 6$

$56w \equiv -46 \pmod 6$

$28w \equiv -23 \pmod 3$

if $w=1 \Rightarrow 3 \mid 51(\checkmark)$

Let $w_0 = 1$ is the initial solution

$w = 1 + 3t \rightarrow (7)$

Sub (7) in (6)

$x = 50 + 56(1+3t)$

$x = 50 + 56 + 168t$

$x = 106 + 168t$

$x \equiv 106 \pmod{168}$ is unique solution of given all congruences

4. Find the value of x if possible such that $4x \equiv 2 \pmod 6$

$3x \equiv 5 \pmod 8$

$2x \equiv 5 \pmod 7$

$3x \equiv 4 \pmod 8$

$4x \equiv 2 \pmod 6 \Rightarrow$

Given that $2x \equiv 1 \pmod 3 \Rightarrow 4x \equiv 2 \pmod 3$

$\Rightarrow x \equiv 2 \pmod 3$

$3x \equiv 5 \pmod 8 \Rightarrow 9x \equiv 15 \pmod 8$

$\Rightarrow x \equiv 7 \pmod 8$

$2x \equiv 5 \pmod 7 \Rightarrow 8x \equiv 20 \pmod 7$

$\Rightarrow x \equiv 6 \pmod 7$

$3x \equiv 4 \pmod 8 \Rightarrow 9x \equiv 12 \pmod 8$

$\Rightarrow x \equiv 4 \pmod 8$

Here $n_1 = 3, n_2 = 8, n_3 = 7, n_4 = 8$

$(n_2, n_4) = (8, 8) = 8$

$\therefore n_1, n_2, n_3, n_4$ are not pairwise relatively Prime

$\therefore$ CRT is not applicable

Here $(8,8) \nmid 7-4$ (X)

∴ solution does not exist for above set of congruences.

5. Find the value of x if possible such that $4x \equiv 2 \pmod 6$ and $3x \not\equiv 5 \pmod 8$

Sol: $4x \equiv 2 \pmod 6 \Rightarrow 2x \equiv 1 \pmod 3$

$4x \equiv 2 \pmod 3$

$x \equiv 2 \pmod 3$

$3x \equiv 5 \pmod 8 \Rightarrow 9x \equiv 15 \pmod 8$

$x \equiv 7 \pmod 8$

Here $n_1 = 3$, $n_2 = 8$, $a_1 = 2$, $a_2 = 7$

$(n_1, n_2) = (3,8) = 1$

∴ n_1, n_2 are pairwise relatively prime

∴ chinese remainder theorem is applicable

$x = a_1 N_1 x_1 + a_2 N_2 x_2$

$n = n_1 \cdot n_2 = 3 \cdot 8 = 24$

$N_k = \frac{n}{n_k}$ where $k = 1, 2$

$N_1 = \frac{24}{3} = 8$

$N_2 = \frac{24}{8} = 3$

$(N_1, n_1) = (8, 3) = 1$

$8x_1 \equiv 1 \pmod 3 \rightarrow (1)$

if $x_1 = 1 \Rightarrow 3 \mid 7$ (x)

$x_1 = 2 \Rightarrow 3 \mid 15$ (v)

$\therefore \boxed{x_1 = 2}$

$(N_2, n_2) = (3, 8) = 1$

$3x_2 \equiv 1 \pmod 8$

if $x_2 = 1 \Rightarrow 8 | 2$ (x)

$x_2 = 2 \Rightarrow 8 | 5$ (x)

$x_2 = 3 \Rightarrow 8 | 8$ (✓)

$\therefore \boxed{x_2 = 3}$

$x = (2)(2)(8) + (7)(3)(3)$

$= 32 + 63$

$= 95$

$x \equiv 95 \pmod{24}$

(or)

$x \equiv 23 \pmod{24}$ is unique solution