# Mathematical And Statistical Foundation (MSF)

## UNIT - 1

## Number Theory

- **Greatest Common Devisior (GCD)**

The largest ~~comm~~ positive integer that devides both "a" and "b" is called GCD of "a" and "b".

It is denoted by $(a, b)$.

$$GCD(a, b) = GCD(b,\ a \bmod b),\quad a > b.$$

Stop this process till it becomes zero.

---

① Find [GCD of (10, 150)] GCD (10, 150)

Sol:

~~Let a=150, b=15010~~

$$GCD(150, 10) = GCD(10,\ 150 \,\%\, 10)$$
$$= GCD(10, 0)$$

$10)150(15$
$-10$
$50$
$-50$
$0$

$\therefore GCD(10,150) = 10.$

---

② Find GCD (36, 54)

$36)54(1$
$36$
$18$

$a > b$, $GCD(a, b) = GCD(b,\ a \bmod b)$

$$GCD(54, 36) = GCD(36,\ 54 \,\%\, 36)$$
$$= GCD(36, 18)$$

$18)36(2$
$36$
$0$

$$GCD(36, 18) = GCD(18,\ 36 \,\%\, 18)$$
$$= GCD(18, 0)$$

$\therefore GCD(36, 54) = 18.$

3. GCD (12, 18)
4. GCD (8, 12)
5. GCD (15, 36)
6. GCD (15, 15)
7. GCD (24, 56)

③ GCD (18, 12) = GCD (~~18~~ 12, 18 % 12)

= GCD (12, 6)

GCD (12, 6) = GCD (6, 12 % 6)

= GCD (6, 0)

= 6

∴ GCD (18, 12) = 6.

④ GCD (8, 12) = GCD (12, 8)

= GCD (8, 12 % 8)

= GCD (8, 4)

GCD (8, 4) = GCD (4, 8 % 4)

= GCD (4, 0)

= 4

GCD (8, 12) = 4.

⑤ GCD (15, 36) = GCD (36, 15)

= GCD (15, 36 % 15)

= GCD (15, 6)

GCD (15, 6) = GCD (6, 15 % 6)

= GCD (6, 3)

GCD (6, 3) = GCD (3, 6 % 3)

= GCD (3, 0)

= 3

GCD (15, 36) = 3.

⑥ GCD (15, 15)

∵ a > b is not possible,

$3 \underline{| 15}$ $\quad$ $3 \underline{| 15}$

$\;\;\; 5$ $\qquad\quad\;\; 5$

{3, 5} = 15

GCD (15, 15) = 15.

⑦ GCD (24, 36) = GCD (56, 24)

= GCD (24, 56 % 24)

= GCD (24, 8)

GCD (24, 8) = 8

= GCD (8, 24 % 8)

= GCD (8, 0)

= 8

GCD (24, 56) = 8.

⑧ Find GCD (1025, 35)

GCD (1024, 35) = GCD (35, 1025 % 35)

= GCD (35, 10)

GCD (35, 10) = GCD (10, 35 % 10)

= GCD (10, 5)

GCD (10, 5) = GCD (5, 10 % 5)

= GCD (5, 0)

= 5

GCD (1025, 35) = 5

- **Euclidean Algorithm :**

Euclidean Algorithm is an Algorithm used to find GCD between two integers.

Suppose, "a", "b" be two +ve integers $(a > b)$ then,

$$a = bq + r, \quad 0 \le r < b$$
$$b = rq_1 + r_1, \quad 0 \le r_1 < r$$
$$r = r_1 q_2 + r_2, \quad 0 \le r_2 < r_1$$
$$r_1 = r_2 q_3 + r_3, \quad 0 \le r_3 < r_2$$
$$\vdots \qquad \vdots \qquad \vdots$$
$$r_{i-2} = r_{i-1} q_i + r_i, \quad 0 \le r_{i-2} < r_{i-1}$$
$$r_{i-1} = r_i q_{i+1} + 0.$$

$$\begin{array}{l} b\,)\,a\,(q \\ \overline{r}\,)\,b\,(q_1 \\ \quad \overline{r_1}\,)\,r\,(q_2 \\ \qquad \overline{r_2}\,)\,r_1\,(q_3 \\ \qquad\quad \overline{r_3} \\ \qquad \vdots \\ r_{i-1}\,)\,r_{i-2}\,(q_i \\ \quad \overline{r_i}\,)\,r_{i-1}\,(q_{i+1} \\ \qquad \overline{0} \end{array}$$

The least non zero reminder is the GCD $(r_i)$

---

Q: Find GCD using Euclidean Algorithm.

1. GCD $(25, 60)$

1. sol: GCD $(a, b)$ Since, $a > b$

GCD $(60, 25)$. let $a = 60$, $b = 25$

$$\begin{array}{l} 25\,)\,60\,(2 \\ \quad\ \ 50 \\ \quad \overline{10}\,)\,25\,(2 \\ \qquad\quad 20 \\ \qquad \overline{5}\,)\,10\,(2 \\ \qquad\qquad 10 \\ \qquad\qquad \overline{0} \end{array}$$

Euclidean Algorithm for 60, 25 :

$$60 = 25 \times 2 + 10$$
$$25 = 10 \times 2 + 5 \quad \text{least non-zero reminder.}$$
$$10 = 5 \times 2 + 0$$

least non-zero reminder is GCD$(60, 25)$

$$\text{GCD}(25, 60) = 5$$

H.W 5. GCD (4076, 1024)

2. GCD (5293, 4321) = 1

3. GCD (42823, 6409) = 17

4. GCD (45, 75)

4. Sol: GCD (45, 75) :

GCD (a, b)

GCD (75, 45)

By Euclidean Algorithm,

$75 = 45 \times 1 + 30$

$45 = 30 \times 1 + 15$

~~15 = 3~~

$30 = 15 \times 2 + 0$

least non zero reminder is GCD

GCD (45, 75) = 15

45 ) 75 ( 1
45
30 ) 45 ( 1
30
15 ) 30 ( 2
30
0

---

3. Sol: GCD (5293, 4321) :

By Euclidean Algorithm :

$5293 = 4321 \times 1 + 972$

$4321 = 972 \times 4 + 433$

$972 = 433 \times 2 + 106$

$433 = 106 \times 4 + 9$

$106 = 9 \times 11 + 7$

$9 = 7 \times 1 + 2$

$7 = 2 \times 3 + 1$

$2 = 1 \times 2 + 0$

GCD (5293, 4321) = 1.

4321 ) 5293 ( 1
4321
972 ) 4321 ( 4
3888
433 ) 972 ( 2
866
106 ) 433 ( 4
424
9 ) 106 ( 11
99
7 ) 9 ( 1
7
2 ) 7 ( 3
6
1 ) 2 ( 2
2
0

---

2. Sol: GCD (42823, 6409)

By Euclidean Algorithm :

$42823 = 6409 \times 6 + 4369$

$6409 = 4369 \times 1 + 2040$

$4369 = 2040 \times 2 + 289$

$2040 = 289 \times 7 + 17$

$289 = 17 \times 17 + 0$.

least non zero reminder is GCD

GCD (42823, 6409) = 17.

6409 ) 42823 ( 6
38454
4369 ) 6409 ( 1
4369
2040 ) 4369 ( 2
4080
289 ) 2040 ( 7
2023
17 ) 289 ( 17

29/09/23



## GCD By Prime Factorization:

Find the HCF / GCD and LCM of 850, 680 using the Prime Factorization Method,

$850 = 2 \times 5 \times 5 \times 17.$

$680 = 2 \times 2 \times 2 \times 5 \times 17.$

$\Rightarrow 850 = 2 \times 5^2 \times 17$

$\Rightarrow 680 = 2^3 \times 5 \times 17$

* HCF / ~~LCM~~ GCD is the product of the smallest power of each common prime factor. i.e,

$HCF / GCD\ (850, 680) = 2^{\min(1,3)} \times 5^{\min(2,1)} \times 17^{\min(1,1)}$

$= 2 \times 5 \times 17$

$GCD = 170$

* LCM is the product of the greatest power of each common prime factor i.e,

$LCM = 2^{\max(1,3)} \times 5^{\max(2,1)} \times 17^{\max(1,1)}$

$= 2^3 \times 5^2 \times 17$

$LCM = 3400$

---

Find GCD 120, 360 by Primefactorization method

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

$360 = 2^3 \times 3^2 \times 5$

$GCD\ (120, 360) = 120. = (2^3 \times 3 \times 5)$

---

H.W GCD(119, 544)
GCD(4410, 15450) } By Prime factoriezation Method.

## Fermat Numbers:

A number $F_n$ is of the form

$$F_n = 2^{2^n} + 1 \quad ; \quad n \geq 0$$

is called a Fermat number.

## Fermat Prime:

A Fermat number which is also a prime number is called Fermat Prime.

Examples:-

$$F_0 = 2^{2^0} + 1 = 3$$

$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$$

Note: $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$ is a composit number.

---

Prove that $F_5$ (Fermat numbers) $= 2^{2^5} + 1$ is divisible by 641.

$$F_5 = 2^{2^5} + 1$$

$$= 2^{32} + 1$$

$$= 2^4 (2^{28}) + 1$$

$$= (16)\, 2^{28} + 1$$

$$= (641 - 625)\, 2^{28} + 1$$

$$= 641 (2^{28}) - 5^4 (2^7)^4 + 1$$

$$= 641 (2^{28}) - (5 \cdot 2^7)^4 + 1$$

$$= 641 (2^{28}) - (640)^4 + 1$$

$2^9 (2^{23})$

$512 (2^{23})$

$(641 - 129) (2^{23}) + 1$

$641 (2^{23}) - 129 (2^{23})$

$(128 + 1) 2^{23}$

$= 641(2^{28}) - (641-1)^4 + 1$

$\because (a-b)^4 = a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4$

$$F_5 = 641\left[2^{28}\right] - \{(641)^4 + 4(641)^3(1) - 6(641)^2(1)^2 + 4(641)(1)^3 + \cancel{1} - \cancel{1}$$

$$F_5 = 641\left[2^{28} \cancel{+} 641^3 + 4(641)^2 - 6(641) + 4\right]$$

$$\Rightarrow \frac{641}{F_5} = 2^{28} - 641^3 + 4(641)^2 - 6(641) + 4$$

Hence, $F_5$ is divisible by 641.

---

## Fermat's Method of Factorization:

Suppose, a number is composite number

$n = ab$

where, "a", "b" are unknown quantities.

Then, we can use:

$$n = ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

If "n" is odd then "a, b" are also odd.

$n = ab = t^2 - s^2 \qquad \because t = \frac{a+b}{2},\ s = \frac{a-b}{2}.$

These are non-negitive integers.

$n = ab = (t+s)(t-s)$

$\Rightarrow n = t^2 - s^2$

$s^2 = t^2 - n$ Let $t = \sqrt{n} + 1$

where $t$ is greatest integer

If $t^2 - n$ is perfect square, It is done.

If $t^2 - n$ is not perfect square, $t = \sqrt{n} + 2$

continue until we get perfect square.

Factorise 809009 using format method of Factorization.

Given $n = 809009$.

find $\sqrt{n} = 899.45$

i) Let $t = \sqrt{n}+1$

$= 899+1$

$t = 900$

$\therefore \Rightarrow s^2 = t^2 - n$

$s = \sqrt{991} = 31.48$

s is not a perfect square.

ii) Let $t = \sqrt{n}+2$

$\Rightarrow t = 901$

$s^2 = t^2 - n$

$s = 52.83$

iii) Let $t = \sqrt{n}+3$

$= 899+3$

$= 902.$

$\Rightarrow s^2 = t^2 - n$

$s = 2\sqrt{698} = \cancel{52.8}.$

$= 67.78$

vi) Let $t = \sqrt{n}+4$

$= 899+4$

$= 904$

$s^2 = t^2 - n$

$s^2 = 903^2 - 3$

$s = \sqrt{903^2-3} = 80.$

$\therefore t = 904,\ s = 80$

$\therefore$ ~~903, 80 are factors of 809009.~~

$n = t^2 - s^2$

$= (t+s)(t-s)$

$= \cancel{903}(903+80)(903-80)$

$n = (983)(823)$

$a = 983$

$b = 823$

$\therefore$ 983, 823 are the factors of 809009.

Using Fermat factorization to find $n = 119123$

Given $n = 119123$

$\sqrt{n} = 345.14$

$t = \sqrt{n} + 1$
$s^2 = t^2 - n$

i) Let $t = \sqrt{n} + 1$

$t = 346$

$s = \sqrt{346^2 - 119123}$

$= \sqrt{593}$ 578

ii) Let $\sqrt{n} + 2 = t$

$t = 347$

$s = \sqrt{347^2 - 119123}$

$= 35.86$ 35.58

iii) Let $t = \sqrt{n} + 3$

$= 348$

$s = \sqrt{348^2 - 119123}$

$= 44.5$

44.28

iv) Let $t = \sqrt{n} + 4$

$t = 349$

$s = \sqrt{349^2 - 119123}$

51.55

$s = 51.7$

Let $t = \sqrt{n} + 5$

$t = 350$

$s = 58.1$

57.88

$t = \sqrt{n} + 6$

$t = 351$

$s = 63.8$

$\sqrt{n} + 7$
$s = 69.$

---

Using Fermat factorization to find $n = 23449$.

$n = 23449$

$s = 24$

$t = 155$

~~tos~~

$a = 179$

$b = 131$

Let $t = \sqrt{n} + 1$

$t = 154$

$s = \sqrt{261}$

Let $t = \sqrt{n} + 2$

$t = 155$

$s = 24$

$n = (t+s)(t-s)$
$= ab$

$\Rightarrow a = 179,\ b = 131.$

## Chinese Reminder Theorem:

Let $n_1, n_2, \ldots, n_r$ be pair wise relativly prime +ve integers. Then, the system of congruences:

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots \qquad \vdots$$
$$x \equiv a_r \pmod{n_r}$$

has unique solution, modlo $N = n_1, n_2, n_3, \ldots, n_r$.

Proof (later)

---

30/9/23

## Congruence:

Let "n" be a fixed positive integer. Two integers "a", "b" are said to ~~to~~ be congruent modulo 'n'.

Symbolized by $a \equiv b \pmod{n}$

If n divides the difference i.e., $(a-b) = kn$ for some $k \in \mathbb{Z}$.

Example:

i) $3 \equiv 24 \pmod{7}$ $\quad \cancel{7}\ \frac{7}{3-24} = \frac{7}{-21} = \frac{1}{-3}$

ii) $-31 \equiv 11 \pmod{7}$ $\quad \frac{7}{-31-11} = \frac{7}{-42}$

iii) $12 \equiv 2 \pmod{7}$ $\quad \frac{7}{12-2} = \frac{7}{10}$ ×

## Linear Congruence:

An equation of the form $ax \equiv b \pmod{n}$ is called a linear congruence.

Solve systems of congruences $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$ using Chinese reminder Theorem. 6

Here, $a_1 = 2$, $a_2 = 3$, $a_3 = 2$

$n_1 = 3$, $n_2 = 5$, $n_3 = 7$.

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

$$N_1 = \frac{n}{n_1} = \frac{105}{3} = 35$$

$$N_2 = \frac{n}{n_2} = \frac{105}{5} = 21$$

$$N_3 = \frac{n}{n_3} = \frac{105}{7} = \cancel{150}\ 15$$

$(N_k, n_k) = 1$, $N_k x \equiv 1 \pmod{n_k}$ considaring the linear congruence:

$35x \equiv 1 \pmod 3$ — 1

$21x \equiv 1 \pmod 5$ — 2

$15x \equiv 1 \pmod 7$ — 3

1 => Let $x = 1$: $35(1) \equiv 1 \pmod 3$

$35 \equiv 1 \pmod 3$

$\frac{3}{35-1} = \frac{3}{34}$ ✗ not congruence.

Let $x = 2$: $35(2) \equiv 1 \pmod 3$

$70 \equiv 1 \pmod 3$

$\frac{3}{70-1} = \frac{3}{69}$ ✓ $\boxed{\text{Congruent}}$

$\therefore x_1 = 2$.

2 => Let $x = 1$: $21(1) \equiv 1 \pmod 5$

$\frac{5}{21-1} = \frac{5}{20}$ ✓ $\boxed{\text{Congruent}}$

$x_2 = 1$

3 => Let $x = 1$:

$15(1) \equiv 1 \pmod 7$

$\frac{7}{15-1} = \frac{7}{14}$ ✓ $\boxed{\text{Congruent}}$ $x_3 = 1$

Simultaneous Solution of the given System of congruence

$$\boxed{\bar{x} = a_1 n_1 x_1 + a_2 n_2 x_2 + a_3 n_3 x_3.}$$

$= (2)(35)(2) + (3)(21)(1) + (2)(15)(1)$

$= 233.$

$x \equiv \bar{x} \pmod{n}$

$x \equiv 233 \pmod{105}$

$\frac{233}{105} = 105 \times 2 + 23$

~~Let~~ $x$ =>

$x \equiv 23 \pmod{105}$

$233 \equiv 23 \pmod{105}$

$x = 23.$

$\therefore$ $23 \equiv 2 \pmod{3}$

$23 \equiv 3 \pmod{5}$

$23 \equiv 2 \pmod{7}$

---

Solve System of Congruences $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{4}$, $x \equiv 1 \pmod{5}$ by Chines reminder Theorem.

Comparing $x \equiv a_r \pmod{n_r}$

$a_1 = 2$ $\quad n_1 = 3$ => $N_1 = \frac{n}{n_1} = 20$

$a_2 = 3$ $\quad n_2 = 4$ $\quad N_2 = \frac{n}{n_2} = 15$

$a_3 = 1$ $\quad n_3 = 5$ $\quad N_3 = \frac{n}{n_3} = 12.$

$n = n_1 \times n_2 \times n_3$

$(n) = 60$

$(N_K, n_K) = 1$, $N_K x \equiv 1 \pmod{n_K}$ considering the linear congruence.

$$20x \equiv 1 \pmod 3 \quad \text{--- (1)}$$
$$15x \equiv 1 \pmod 4 \quad \text{--- (2)}$$
$$12x \equiv 1 \pmod 5 \quad \text{--- (3)}$$

(1) Let $x = 1$

$20(1) = 1 \pmod 3$

$\frac{3}{20-1} = \frac{3}{19}$ ✗

Let $x = 2$

$20(2) = 1 \pmod 3$

$40 = 1 \pmod 3$

$\frac{3}{40-1} = \frac{3}{39}$ ✓

congruent.

$x_1 = 2$

(2) Let $x = 1$

$15(1) = 1 \pmod 4$

$\frac{4}{15-1} = \frac{4}{14}$ ✗

Let $x = 3$

$15(3) = 1 \pmod 4$

$\frac{4}{45-1} = \frac{4}{44}$ ✓

Congruent

$x_2 = 3$

(3) Let $x = 1$

$12(1) = 1 \pmod 5$

$\frac{5}{12-1} = \frac{5}{11}$ ✗

Let $x = 3$

$12(3) = 1 \pmod 5$

$36 = 1 \pmod 5$

$\frac{5}{36-1} = \frac{5}{35}$ ✓

Congruent

$x_3 = 3$

According to Simultanues Solution of the given System of ~~Congruence~~. congruence:

$$\bar{x} = a_1 n_1 x_1 + a_2 n_2 x_2 + a_3 n_3 x_3$$

$$= 2\,\overset{(20)}{\cancel{(3)}}(2) + 3\,\overset{(15)}{\cancel{(4)}}(3) + 1\,\overset{(12)}{\cancel{(5)}}(3)$$

$\cancel{= 63}$ $= 251$

$\Rightarrow x \equiv \bar{x} \pmod n$ $\quad 251 = 60 \times 4 + 11$

$\cancel{x \equiv 63 \pmod{60}}$

$\Rightarrow x \equiv 251 \pmod{60}$

$\cancel{x \equiv 3 \pmod{60}}$

$\Rightarrow 251 \equiv 11 \pmod{60}$

$x = 11$

$\therefore$ $11 \equiv 2 \pmod 3$

$11 \equiv 3 \pmod 4$

$11 \equiv 1 \pmod 5$

H.W Q. $x \equiv 2 \pmod 3$
$x \equiv 4 \pmod 5$
$x \equiv 6 \pmod 7$

Q. $x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 7$
$x \equiv 3 \pmod{11}$

---

3/10/2023

Problems on linear Congruence

## Working Rule:

General format : $ax \equiv b \pmod n$

i) Find GCD $(a,n)$. Let $d =$ GCD $(a,n)$.

ii) Find $b/d$. If $b/d$ is whole number, Solution exists. (iii)

iii) Find $d \pmod n = d$

iv) Divide both sides with 'd'.

v) Multiply both sides with multiplicative inverse of 'a'.

vi) Find general solution $X_k = X_0 + k\left(\frac{n}{d}\right)$. $\in k = 1,2,3,\dots$.

---

Find ~~line e~~ linear Congruence of $14x \equiv 12 \pmod{18}$.

Given: $14x \equiv 12 \pmod{18}$ — (1)

Comparing to $ax \equiv b \pmod n$

Hence, Let $a = 14$, $b = 12$, $n = 18$.

GCD$(a,n)$ = GCD$(14,18) = 2$

Let $d = 2$

$18 = 14 \times 1 + 4$
$14 = 4 \times 3 + 2$
$4 = 2 \times 2 + 0$

$\frac{b}{d} = \frac{12}{2} = 6 \Rightarrow$ Hence, Solution exists.

$d \pmod n = d \Rightarrow 2 \pmod{18} = 2$

$2 \pmod{18} = 2$

Hence, 2 Solutions exist

(1) divide both sides by 2.

$$\frac{14x}{2} = \frac{12 \pmod{(18)}}{2}$$

$$7x = 6 \pmod{(9)}$$

dividing by "a" on both sides let $\frac{1}{7} = y$

$$\frac{7x}{7} = \frac{6}{7} \pmod 9 \Rightarrow x = 6y \pmod 9 \quad - (2)$$

Let $\frac{6}{x} = y$

$1 = 7y \pmod 9 \quad - (3)$

$\cancel{1x} = 6y \pmod 9$

$$1 = 7y \pmod 9 \quad - (3)$$

Let $y = 1$

$7 \pmod 9 \neq 1$

$y = 2$

$14 \pmod 9 \neq 1$

$y = 3$

$21 \pmod 9 \neq 1$

$\boxed{y = 4}$

$28 \pmod 9 = 1$

(3) $\Rightarrow$ $1 = 7(4) \pmod 9$

(2) $\Rightarrow$ $x = 6(4) \bmod 9$

$x = 24 \pmod 9$

$x_0 = 6$

General Solution: $X_k = X_0 + k\left(\frac{n}{d}\right)$

For $k = 1 \Rightarrow$ $X_1 = X_0 + 1\left(\frac{18}{2}\right)$

$= 6 + 9$

$X_1 = 15$

$\therefore$ 2 Solutions are 6, 15.

Find linear Congruence of $3x \equiv 2 \pmod{7}$

Given $ax \equiv b \pmod{n}$ — ①

$a = 3,\ b = 2,\ n = 7.$

$GCD(a, n) = GCD(3, 7) = 1.$

$d = 1$

$\frac{b}{d} = \frac{2}{1} = 2.$ (Since, $\frac{b}{d}$ is whole number, Solution exists)

$d \pmod{n} = d$

$1 \pmod{7} = 1$

One Solution exists.

① divide by d. on both sides.

$$\frac{3x}{1} \equiv \frac{2 \pmod{7}}{1}$$

divide by 'a' on both sides:

$$\frac{3x}{3} \equiv \frac{2 \pmod{7}}{3} \Rightarrow x \equiv 2\left(\tfrac{1}{3}\right) \bmod 7$$

$$x \equiv 2y \pmod{7} \quad — ②$$

$$1 = 3y \pmod{7} \quad — ③$$

For $y = 1$, $3 \pmod{7} = 3 \neq 1$

$y = 2$, $6 \pmod{7} = 6 \neq 1$

$y = 3$, $9 \pmod{7} = 2 \neq 1$

$y = 4$, $12 \pmod{7} = 5 \neq 1$

$\boxed{y = 5}$, $15 \pmod{7} = 1$ ✓

$7)\,15\,(2$
$14$
$1$

③ $\Rightarrow$ $1 = 3(5) \pmod{7}$

② $\Rightarrow$ $x = 2(5) \pmod{7}$

$x_0 = 3$

$7)\,10\,(1$
$7$
$3$

∴ Solution exists for only $x_0 = 03$.

---

H.W $10x \equiv 2 \pmod{5}$ ~~$d=5$, $\frac{b}{n}=$~~ $9x \equiv 6 \pmod{15}$

05/10/2023 ⑨

$10x \equiv 15 \pmod{45}$ . Find its linear Congruence. — ①

Given : $ax \equiv b \pmod n$

$GCD(a, n) \cdot GCD(10, 45)$

$d = 5$

$\frac{b}{d} = \frac{15}{5} = 3$

Hence, Solutions exists.

$d \pmod n = d$

$5 \pmod{45} = 5$

Hence, 5 solutions exist.

① divide by d

$\frac{10x}{5} \equiv \frac{15 \pmod{45}}{5}$

$2x \equiv 3 \pmod 9$

divide by a

$\frac{2x}{2} \equiv \frac{3}{2} \pmod 9$

$x \equiv 3y \pmod 9$ — ②

$1 \equiv 2y \pmod 9$ — ③

for $y = 1$, $2 \pmod 9 = 2 \neq 1$
$y = 2$, $4 \pmod 9 = 4 \neq 1$
$y = 3$, $6 \pmod 9 = 6 \neq 1$
$y = 4$, $8 \pmod 9 = 8 \neq 1$
$y = 5$, $10 \pmod 9 = 1$ ✓

$y = 5$

② => $x \equiv 15 \pmod 9$

[③ => $1 \equiv 10 \pmod 9$]

② => $x_0 = 6$

General Solution: $x_k = x_0 + k\left(\frac{n}{d}\right)$

$$x_1 = x_0 + 1\left(\frac{45}{5}\right)$$

Similarly, $x_1 = 15$

$x_2 = 24$

$x_3 = 33$

$x_4 = 42$

$\therefore$ 6, 15, 24, 33, 42 are the Solutions for $10x \equiv 15 \pmod{45}$

---

H.W

$15x \equiv 25 \pmod{45}$ $\quad$ $17x \equiv 9 \pmod{276}$

$5x \equiv 2 \pmod{26}$ $\quad$ $12x \equiv 16 \pmod{20}$

---

## * System Of Linear Congruences in two Variables :

The system of linear congruences

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

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

have unique solution modlo $n$

if $\text{GCD}(ad - bc, n) = 1$

---

Solve the system of linear congruences for

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

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

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

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

$$\begin{aligned} \text{GCD}(ad - bc, n) &= \text{GCD}((7)(5) - (3)(2), 16) \\ &= \text{GCD}(29, 16) \\ &= 1 \end{aligned}$$

Given congruence: $7x + 3y \equiv 10 \pmod{16}$ — ①

$2x + 5y \equiv 9 \pmod{16}$ — ②

10

$2 \times$ ① $- \ 7 \times$ ②

$$\cancel{14x} + 6y \equiv 20 \ (\text{mod } \cancel{32}\ 16)$$
$$-\ \cancel{14x} + 35y \equiv 63 \ (\text{mod } \cancel{112}\ 16)$$

$$29y \equiv 43 \pmod{16}$$

~~Comparing: $ax \equiv b \pmod{m}$~~

$$29y \equiv 43 \pmod{16}$$

$\cancel{y \equiv 43\,xy \pmod{16}}$ — ③

$1 \equiv 29\,y \pmod{16}$ — ④

for

$y = 1$, $29 \pmod{16} = 13 \neq 1$

$y = 2 \Rightarrow 58 \pmod{16} = 10 \neq 1$

$y = 3$, $87 \pmod{16} = 7 \neq 1$

$y = 4$, $116 \pmod{16} = 4 \neq 1$

$y = 5$, $145 \pmod{16} = 1$ ✓

$$y = 43(5) \pmod{16}$$

$\cancel{y = 13}$ $y = 7.$

$5 \times$ ① and $3 \times$ ②

$$35x + \cancel{15y} \equiv 50 \pmod{16}$$
$$-\ (6x + \cancel{15y} \equiv 27 \pmod{16})$$

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

$x \equiv 23\,x \pmod{16}$ — ⑤

$1 \equiv 29\,y \pmod{16}$ — ⑥

⑥ $\Rightarrow$ for,

$y = 1$ $29 \pmod{16} = 13 \neq 1$

$y = 5$ $145 \pmod{16} = 1$ ✓

$y = 5$

⑤ $\Rightarrow$

$x \equiv 23(5) \pmod{16}$

$x = 3.$

$\therefore x = 3,\ y = 7 \pmod{16}$

(H.W) $3x + 4y \equiv 5 \pmod{13}$
$2x + 5y \equiv 7 \pmod{13}$

6/10/23

Solve by Chinese reminder Theorem $4x \equiv 5 \pmod 9$
$2x \equiv 6 \pmod{20}$

Given: $4x \equiv 5 \pmod 9$ — ①
$2x \equiv 6 \pmod{20}$ — ②

① ÷ 4 => $x \equiv 5\left(\frac{1}{4}\right) \pmod 9$

$5y \pmod 9 \equiv x$ — ③

=> $4y \pmod 9 = 1$

for, $y = 7$: $4(7) \bmod 9 = 1$

③ => $5(7) \pmod 9 \equiv x$

$35 \pmod 9 \equiv x$ — ④

$x = 3$.

615
32.1

② ÷ 2 => $x \equiv 3 \pmod{20}$

④ => $x \equiv 35 \pmod 9$

$a_1 = 35$ $n_1 = 9$
$a_2 = 3$ $n_2 = 20$

$20x \equiv 1 \pmod 9$

$\frac{9}{20-1} = \frac{9}{19}$

$x_1 = 9/19$ $\boxed{x_1 = 5}$

$N = n_1 n_2 = 9 \times 20 = 180$

$N_1 = \frac{180}{9} = 20$

$9x \equiv 1 \pmod{20}$

$N_2 = \frac{180}{20} = 9$

$x = 4/19$ $9 \equiv 1 \bmod 20$

$\frac{20}{9-1} = \frac{20}{8}$

$GCD(N_K, n_K) = 1$

$N_K x \equiv 1 \pmod{n_K}$ $K = 1, 2$.

$\boxed{x_2 = 9}$

$N_1 x \equiv 1 \pmod{n_1}$

$20x \equiv 1 \pmod 9$

$x = 593$

$N_2 x \equiv 1 \pmod{n_2}$

$x = 593 \pmod{90}$

$9x \equiv 1 \pmod{20}$

$\boxed{x = 53}$

75

(4) Solve by Chines reminder theorem $17x \equiv 3 \pmod{2\cdot3\cdot5\cdot7}$ (11)

$\left[ 17x \equiv (\bmod\ 2),\ 17x \equiv 3 (\bmod\ 3) \right.$
$\left. 17x \equiv 1 (\bmod\ 5),\ 17x \equiv 3 (\bmod\ 7). \right]$

---

Fundamental Theory of Arthametic

Every integer greater than one can be written in the form $P_1^{n_1}, P_2^{n_2}, \ldots, P_k^{n_k}$ where $n_i \geq 0$ and $P_i$ are distinct Prime numbers.

The factorization is unique except possibily for the order of factors.

Every integer greater than one is either a prime or can be expressed as product of prime numbers.

OPTIONAL (maybe)

Proof: $n = 2$, 2 is prime

Here, statement is true (for $n=2$).

If n is prime. It is proved.

If $n=18$

If n is not prime, Then n is composite number

Composite numbers have factors other than one and itself

$n = 2\times9$

If $n = ab$ ( ~~1<a<n, 1<b<n~~ $\left[ \begin{array}{l} 1<a<n \\ 1<b<n \end{array} \right]$

its factors are $1, a, b, n$

$\exists$ by

a, b can be factorized into primes.

$n = 2^1 \times 3^2$

Unique-ness Part

for proving uniqueness, we will use Euclides Lemma.

If 'a' is prime, p divides the product ~~AB~~ ab of two integers a and b. Then, p must divide atleast one of these integers "a" or "b". i.e, $p/a$ (or) $p/b$ (or) $p/ab$.

$$n = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$$
$$= q_1^{m_1} q_2^{m_2} \dots q_k^{m_k}$$

Suppose, n is the least integer, greater than one, that has two distinct primefactorization.

Now, ~~n=q~~ $p_1^{n_1} p_2^{n_2} \dots p_k^{n_k} = q_1^{m_1} q_2^{m_2} \dots q_j^{m_j}$ — ①

$$\underbrace{p_1 \dots p_1}_{n_1} \times \underbrace{p_2 \dots p_2}_{n_2} \dots \underbrace{p_k \dots p_k}_{n_k} = \underbrace{q_1 \dots q_1}_{m_1} \times \underbrace{q_2 \dots q_2}_{m_2} \dots \underbrace{q_j \dots q_j}_{m_j}.$$

Hence, $p_1 / q_1^{m_1} q_2^{m_2} \dots q_j^{m_j}$ according to Euclides Lemma,

$p_1$ divides some $q_j$.

without loss of generality, simply w.r.t let it be $q_1$

$p_1 / q_1 \Rightarrow p_1 = q_1$ (because both are primes) ? equal

Since $p_1 = q_1$, Simplifying ① we get

$p_1^{n_1 - 1} \cdot p_2^{n_2} \dots p_k^{n_k} = q_1^{m_1 - 1} q_2^{m_2} \dots q_j^{m_j}$

we have two distinct facturization of some integer which is strictly smaller than "n". which controdicks the minemality of "n".

Hence, every integer greater than one can be expressed as the product of primes.

---

7/10/23

## Chinese Reminder Theorem Proof:

Let $n_1, n_2, \dots n_r$ be pairwise relativly prime positive integers. Then the system of congruences ~~exceeds~~

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots \qquad \vdots$$
$$x \equiv a_r \pmod{n_r}$$ has unique solution.

$$n = n_1, n_2, \dots n_r$$

Proof: Given: $n_1, n_2, \dots, n_r$. are relativly prime.

i.e. $GCD(n_i, n_j) = 1, \forall\ i \neq j$

Let $n = n_1, n_2, \dots, n_r$ for each

$$k_k = 1, 2, \dots, r$$

$$N_k = \frac{n}{n_k} = n_1, n_2, \dots, n_k \dots n_r$$

$$N_1 = \frac{n}{n_1}, \quad N_2 = \frac{n}{n_2}, \quad \dots, \quad N_r = \frac{n}{n_r}$$

$$N_1 = \frac{n_1 . n_2 \dots n_r}{n_1}$$

$$GCD(N_1, n_1) = 1$$
$$GCD(N_2, n_2) = 1$$
$$\vdots$$
$$GCD(N_k, n_k) = 1, \text{ for } k = 1, 2, \dots, r.$$

$N_K x \equiv 1 \pmod{n_K}$ the solution of the linear congruence.

$N_K x \equiv 1 \pmod{n_K}$ has solution.

So, $N_K x_K \equiv 1 \pmod{n_K}$ is true.

Claim:

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \dots + a_r N_r x_r$$

of given system of linear congruence.

$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \dots + a_r N_r x_r \equiv A_K N_K x_K \pmod{n_K}$

where, $n = n_1, n_2, \dots, n_r$.

$$\bar{x} \equiv a_K \pmod{n_K}$$

Uniqueness $x_i$ is any other integer that satisfies congruences.

$$\bar{x} \equiv a_k \equiv x' \pmod{n_K}$$

where $k = 1, 2, \dots, r$

Here, $\frac{n_k}{\bar{x} - x'}$

Now, $\frac{n_1}{\bar{x} - x'}, \frac{n_2}{\bar{x} - x'}, \dots, \frac{n_r}{\bar{x} - x'}$

$GCD(n_i, n_j) = 1$

$n_1, n_2, \dots, n_r / \bar{x} - x' \Rightarrow n / \bar{x} - x'$

Hence, $\bar{x} \equiv x' \pmod{n}$

$\therefore$ Thus the given congruence has unique solution.