Number Theory

① Show that $(a+b,\ a-b)$ is either 1 or 2 if and only if $(a,b) = 1$

Ans

First let us ~~assume~~ take $(a,b) = 1$

Now we assume, $(a+b,\ a-b) = d$

Since d is the gcd of $(a+b)$ and $(a-b)$ then, d can be expressed as a linear combination of $(a+b)$ and $(a-b)$

Let,

$$x_1(a+b) + y_1(a-b) = d \quad (x_1, y_1 \in \mathbb{Z})$$

$$\Rightarrow (x_1+y_1)a + (x_1-y_1)b = d$$

$$\Rightarrow \left(\frac{x_1+y_1}{d}\right)a + \left(\frac{x_1-y_1}{d}\right)b = 1$$

Since $(a,b) = 1$, then $\frac{x_1+y_1}{d}$ and $\frac{x_1-y_1}{d}$ both must be integers.

Let us assume, $x_1 + y_1 = N_1 d$

$x_1 - y_2 = N_2 d$

$$\Rightarrow x_1 = \left(\frac{N_1+N_2}{2}\right) \times d \text{ and } y_1 = \left(\frac{N_1-N_2}{2}\right) \times d$$

Now x_1, y_1 both are integers.

Then for $d = 2$, that property is maintained.

else if $N_1 = (2m+1)N_2$ i.e an odd multiple of N_2

then also x_1, y_1 both remains as integers.

Now if $N_1 = (2m+1) N_2$ $(m \in \mathbb{Z})$

d can take any integer values.

i.e d can take value 1.

Then summing up all the situations we can conclude d can take either 1 or 2.

$\therefore$ If $(a,b) = 1$ then $(a+b, a-b)$ is either 1 or 2.

<u>Conversely,</u>

Let,
$$(a+b, a-b) = 1$$

i.e
$$x(a+b) + y(a-b) = 1 \quad (x, y \in \mathbb{Z})$$

$$\Rightarrow (x+y)a + (x-y)b = 1$$

This concludes that $(a,b) = 1$

Let,
$$(a+b, a-b) = 2$$

i.e
$$x(a+b) + y(a-b) = 2 \quad \{x, y \in \mathbb{Z}$$

$$\Rightarrow (x+y)a + (x-y)b = 2$$

② Find all integers n such that n^2+1 is divisible by $n+1$

(Ans) We have, $n^2+1 = n^2-1+2$

$$= (n+1)(n-1)+2$$

~~Here from we can see~~

~~for $n=0$, $n+1=1$ divides $(n+1)(n-1)+2$~~

~~,, $n=2$, $n+1=2$ divides $(n+1)(n-1)+2$~~

~~,, $n=-2$, $n+1=-1$,, $(n+1)(n-1)+2$~~

~~Only for $n=0, n=-2$ and $n=1$; n^2+1 is divisible by $n+1$.~~

~~26~~

~~6~~

~~③ Show that for all odd integers n, $\gcd(3n, 3n+2) = 1$~~

Now we can see $(n+1)$ will divide (n^2+1) if $(n+1)$ divides 2.

i.e $n+1$ can take values $-2, -1, 1, 2$

then, n can take values $-3, -2, 0, 1$

---

③ Show that for all odd integers n, $\gcd(3n, 3n+2) = 1$

(Ans) Let us take $(3n, 3n+2) = d$

Then we can express that —

$$x \times (3n) + y(3n+2) = d \quad (x, y \in \mathbb{Z})$$

$\Rightarrow (3x+3y)\cdot n + y\cdot 2 = d$ ... (i)

Now we have n is odd.

Then $\gcd(n, 2) = 1$

Now we can write —

$X\cdot n + Y\cdot 2 = 1 \quad (X, Y \in \mathbb{Z})$ ... (ii)

~~Equating~~

Let, $X = 3x+3y$ and $Y = y$

then $d = 1$ (from eq (i) & (ii))

Then $\gcd(3n, 3n+2) = 1$ (proved)

---

(4) Prove that sum of first n natural numbers $(n>2)$ cannot be prime.

(Ans) Let us assume there exists a $n (n>2)$ for which sum of first n natural numbers is prime.

$\boxed{\text{Case - I}}$ n is odd.

Since n is odd, $(n+1)$ is even.

Now $n+1 \geq 4$ $(\because n>2)$

$\Rightarrow \left(\frac{n+1}{2}\right) \geq 2$

Since $(n+1)$ is even, then $\left(\frac{n+1}{2}\right)$ is also even.

Now $\left(\frac{n+1}{2}\right)$ is even and greater or equal to 2.

Then $\left(\frac{n+1}{2}\right)$ is divisible by 2.

i.e $\frac{n(n+1)}{2}$ " " " 2.

i.e Sum of n natural numbers is divisible by 2

$\therefore$ It is not prime.

$\boxed{\text{Case} \Rightarrow \text{II}}$ n is even.

Now, $n \geq 4$ $(\because n > 2)$

$\Rightarrow \left(\frac{n}{2}\right) \geq 2$

By previous manner we can say —

$2 \mid \left(\frac{n}{2}\right)$

$\Rightarrow 2 \mid \frac{n}{2}(n+1)$ $(\because n \in N)$

$\Rightarrow 2 \mid$ (Sum of first n natural numbers)

$\therefore$ Considering both case I & II, our assumption is wrong.

$\therefore$ Sum of first n natural numbers can't be prime.

Scanned by CamScanner

(5) Prove that n^2+23 is divisible by 24 for infinitely many n.

(Sol) Let us assume there exists only finite number of n for which n^2+23 is divisible by 24.

Let $n = p$ be the gretest of all such integers.

Then, $24 \mid p^2+23$

$$\Rightarrow p^2+23 \equiv 0 \pmod{24}$$

$$\Rightarrow p^2-1+24 \equiv 0 \pmod{24}$$

$$\Rightarrow p^2-1 \equiv 0 \pmod{24}$$

$$\Rightarrow p^2 \equiv 1 \pmod{24}$$

$$\Rightarrow (p^2)^2 \equiv (1)^2 \pmod{24} \quad \left\{ \because a \equiv b \pmod{c} \Rightarrow a^2 \equiv b^2 \pmod{c} \right.$$

$$\Rightarrow p^4 \equiv 1 \pmod{24}$$

This shows that ~~[illegible]~~ for $n = p^2$, n^2+23 is divisible by 24.

i.e there exists anther n $(n = p^2)$ which is greter than p for which n^2+23 is divisible by 24.

So our assumption ~~that~~ ~~[illegible]~~ is wrong.

$\therefore$ There exists there is infinitely many n for which n^2+23 is divisible by 24.

⑥ Find all the primes of the form n^3-1 for integers $n>1$

Ans We can write —

$$n^3-1 = (n-1)(n^2+n+1)$$

for $n=2$, $n^3-1 = (2-1)(2^2+2+1)$

$= 7$ (prime number)

for any $n>2$, $(n-1) \geq 2$

Now, $(n-1) \mid (n-1)(n^2+n+1)$ $(\because n \in \mathbb{Z})$

$\Rightarrow (n-1) \mid n^3-1$

i.e for any $n>2$, n^3-1 can't be prime.

$\therefore$ 7 is the only prime of the form n^3-1 for $n>1$ $(n \in \mathbb{Z})$

---

⑦ Use Euclidean Algorithm to calculate gcd (a,b) and hence express it as $au+bv$ for some $u,v \in \mathbb{Z}$ for the following a,b:

(i) gcd $(12378, 3054)$

Ans Let us take, $a = 12378$; $b = 3054$

$\therefore$ $12378 = 4 \times 3054 + 162$

$$\Rightarrow \quad 3054 = 18 \times 162 + 138$$

$$\Rightarrow \quad 162 = 138 + 24$$

$$\Rightarrow \quad 138 = 5 \times 24 + 18$$

$$\Rightarrow \quad 24 = 18 + 6$$

$$\Rightarrow \quad 18 = 3 \times 6$$

$\therefore \quad \gcd(12378, 3054) = 6$

Now we can write —

$$\begin{aligned} 6 &= 24 - 18 \\ &= 24 - (138 - 5 \times 24) \\ &= 6 \times 24 - 138 \\ &= 6 \times (162 - 138) - 138 \\ &= 6 \times 162 - 7 \times 138 \\ &= 6 \times 162 - (3054 - 18 \times 162) \times 7 \\ &= (6 + 18 \times 7) 162 - 3054 \times 7 \\ &= (6 + 18 \times 7) \times (12378 - 4 \times 3054) - 7 \times 3054 \\ &\cancel{= 132 \times 12378 - 535 \times 3054} \\ &= 132 \times 12378 - 535 \times 3054 \end{aligned}$$

Here $u = 132$, $v = -535$

for which $\gcd(12378, 3054) = u \times 12378 + v \times 3054$

7b) $\gcd(272, 1479)$

Let us take $a = 1479$; $b = 272$

$\therefore$ $1479 = 5 \times 272 + 119$ ... (i)

$272 = 2 \times 119 + 34$ ... (ii)

$119 = 3 \times 34 + 17$ ... (iii)

$34 = 2 \times 17$ ... (iv)

$\therefore \gcd(272, 1479) = 17$

We have, $17 = 119 - 3 \times 34$

$= 119 - 3 \times (272 - 2 \times 119)$

$= 7 \times 119 - 3 \times 272$

$= (1479 - 5 \times 272) \times 7 - 3 \times 272$

$= 7 \times 1479 - 38 \times 272$

Here, $u = 7$, $v = -38$

$\therefore \gcd(1479, 272) = u \times 1479 + v \times 272$

7c) $\gcd(42823, 6409)$

Let us take $a = 42823$; $b = 6409$

$\therefore$ $42823 = 6 \times 6409 + 4369$ ... (i)

$6409 = 4369 + 2040$ ... (ii)

$4369 = 2 \times 2040 + 289$ ... (iii)

$2040 = 7 \times 289 + 17$ ... (iv)

$289 = 17 \times 17 \quad \cdots \quad (v)$

$\therefore \gcd(42823, 6409) = 17$

We have, $17 = 2040 - 7 \times 289$

$= 2040 - 7 \times (4369 - 2 \times 2040)$

$= 15 \times 2040 - 7 \times 4369$

$= 15 \times (6409 - 4369) - 7 \times 4369$

$= 15 \times 6409 - 22 \times 4369$

$= 15 \times 6409 - 22 \times (42823 - 6 \times 6409)$

$= -22 \times 42823 + (15 + 132) \times 6409$

$= -22 \times 42823 + 147 \times 6409$

Here, $u = -22$, $v = 147$

$\therefore \gcd(42823, 6409) = u \times 42823 + v \times 6409$

7d) $\gcd(1819, 3587)$

Let us take $a = 3587$, $b = 1819$

$\therefore$ $3587 = 1819 + 1768 \quad \cdots \quad (i)$

$1819 = 1768 + 51 \quad \cdots \quad (ii)$

$1768 = \cancel{34 \times 51} \; 34 \times 51 + 34 \quad \cdots \quad (iii)$

$51 = 34 + 17 \quad \cdots \quad (iv)$

$34 = 17 \times 2 \quad \cdots \quad (v)$

$\therefore \text{GCD}(1819, 3587) = 17$

$$\therefore\ 17 = 51 - 34$$

$$= 51 - (1768 - 34 \times 51)$$

$$= 35 \times 51 - 1768$$

$$= 35 \times (1819 - 1768) - 1768$$

$$= 35 \times 1819 - 36 \times 1768$$

$$= 35 \times 1819 - 36(3587 - 1819)$$

$$= 71 \times 1819 - 36 \times 3587$$

$$\therefore\ \gcd(1819, 3587) = 71 \times 1819 - 36 \times 3587$$

---

(8) Find integers x, y, z satisfying ~~gcd~~ $\gcd(198, 288, 512) = 198x + 288y + 512z$

Let us take $a = 512$, $b = 288$, $c = 198$

$$\therefore\ \left.\begin{aligned} 512 &= 2 \times 198 + 116 \\ 288 &= 198 + 90 \end{aligned}\right\} \rightarrow \text{(i)}$$

$$\left.\begin{aligned} 198 &= 2 \times 90 + 18 \\ 116 &= 90 + 26 \end{aligned}\right\} \rightarrow \text{(ii)}$$

$$\left.\begin{aligned} 90 &= 18 \times 5 \\ 26 &= 18 + 8 \end{aligned}\right\} \rightarrow \text{(iii)}$$

$$26 = 3 \times 8 + 2 \rightarrow \text{(iv)}$$

$$8 = 4 \times 2$$

$$\therefore\ \gcd(198, 288, 512) = 2$$

Scanned by CamScanner

$\therefore\ 2 = 26 - 3 \times 8$

$= 26 - 3 \times (26 - 18)$

$= -2 \times 26 + 3 \times 18$

$= -2 \times (116 - 90) + 3 \times (198 - 2 \times 90)$

$\cancel{= -2 \times 116 + 198}$

$= -2 \times 116 + 3 \times 198 - 4 \times 90$

$= -2(512 - 2 \times 198) + 3 \times 198 - 4 \times (288 - 198)$

$= -2 \times 512 + (4 + 3 + 4) 198 - 4 \times 288$

$\gcd(198, 288, 512) = 11 \times 198 - 4 \times 288 - 2 \times 512$

$\therefore\ x = 11\ ;\ y = -4\ ;\ z = -2$ (Ans)

---

(9) Find the general solution in integers of the equation $56x + 72y = 40$

We have to find out the gcd of 56 and 72.

$\therefore\ 72 = 56 + 16 \quad \ldots\ (i)$

$\Rightarrow\ 56 = 16 \times 3 + 8 \quad \ldots\ (ii)$

$\Rightarrow\ 16 = 8 \times 2 \quad \ldots\ (iii)$

$\therefore\ \gcd(56, 72) = 8$

$8 = 56 - 16 \times 3 = 56 - 3 \times (72 - 56)$

$= 4 \times 56 - 3 \times 72$

$\therefore\ 8 = 4 \times 56 - 3 \times 72$

$\therefore \quad 20 \times 56 - 15 \times 72 = 40$

$\therefore \quad x_0 = 20 \,;\; y_0 = -15$

$\cancel{x = x_0 + \left(\frac{-15}{8}\right) n \,;\; y = y_0 - \left(\frac{20}{8}\right) n \quad (n = 0, 1, 2 \ldots)}$

$\therefore$ The general solution is given by —

$$x = 20 + \left(\frac{-72}{8}\right) n \qquad (n \in \mathbb{Z})$$

$$y = 20 - \left(\frac{56}{8}\right) n$$

---

(10) Find the general solution in integers of the equation $24x + 138y = 18$

(Ans) We have to find out the gcd of 24 and 138.

$$138 = 5 \times 24 + 18 \quad \ldots \text{(i)}$$
$$24 = 18 + 6 \quad \ldots \text{(ii)}$$
$$18 = 3 \times 6 \quad \ldots \text{(iii)}$$

$\therefore \quad \gcd(24, 138) = 6$

$$\therefore \quad 6 = 24 - 18$$
$$= 24 - (138 - 5 \times 24)$$
$$= 6 \times 24 - 138$$

$\therefore \quad 6 \times 24 - 138 = 6$

$18 \times 24 - 3 \times 138 = 18$

$\therefore \quad x_0 = 18 \,;\; y_0 = -3$

$\therefore$ The general solution of the equation $24x + 138y = 18$ is given by –

$$\left.\begin{aligned} x &= 18 + \left(\frac{138}{6}\right)n \\ y &= -3 - \left(\frac{24}{6}\right)n \end{aligned}\right\} (n \in \mathbb{Z})$$

---

(11) Find the general solution in integers of the equation $221x + 35y = 11$

The given equation $221x + 35y = 11$ is a linear diaphantine equation.

We have to find the gcd of 221 and 35.

$\therefore$ $221 = 6 \times 35 + 11$ ... (i)

$35 = 3 \times 11 + 2$ ... (ii)

$11 = 5 \times 2 + 1$ ... (iii)

$5 = 5 \times 1$ ... (iv)

$$\therefore \gcd(221, 35) = 1 = 11 - 5 \times 2$$
$$= 11 - (35 - 3 \times 11) \times 5$$
$$= 16 \times 11 - 35 \times 5$$
$$\boxed{\cancel{= (221 - 6 \times 35) \times 16 - 35 \times 5} \\ \cancel{= 16 \times 221 - 100 \times 35}}$$
$$= 16 \times (221 - 6 \times 35) - 35 \times 5$$
$$= 16 \times 221 - 101 \times 35$$

$\therefore$ $x_0 = 16$; $y_0 = -101$

The general solution of the given equation

$221x + 35y = 11$ is given by —

$$\left.\begin{aligned} x &= 16 + \left(\frac{35}{1}\right)\times n \\ y &= -101 - \left(\frac{221}{1}\right)\times n \end{aligned}\right\} (n \in \mathbb{Z})$$

---

(12) Find $\tau(360)$, $\sigma(360)$, $\tau(1482)$, $\sigma(1225)$, $\tau(1932)$, $\sigma(7002)$

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

Then ~~the~~ number of divisor of 360 —

$$\tau(360) = (3+1)\times(2+1)\times(1+1)$$

$$= 24$$

Sum of all the divisors of 360 —

$$\sigma(360) = \left(\frac{2^{3+1}-1}{2-1}\right)\times\left(\frac{3^{2+1}-1}{3-1}\right)\times\left(\frac{5^{1+1}-1}{5-1}\right)$$

$$= 15 \times \frac{26}{2} \times \frac{24}{4}$$

$$= 1170$$

We can represent 1482 like —

$$1482 = 2\times3\times13\times19$$

$$\therefore \tau(1432) = (1+1)\times(1+1)\times(1+1)\times(1+1)$$

$$= 16$$

Now 1225 can be written as —

$$1225 = 5^2 \times 7^2$$

Then, $$\sigma(1225) = \left(\frac{5^{2+1}-1}{5-1}\right) \times \left(\frac{7^{2+1}-1}{7-1}\right)$$

$$= \frac{124}{4} \times \frac{342}{6}$$

$$= 1767.$$

Again, 1932 can be expressed as —

$$1932 = 2^2 \times 3 \times 7 \times 23$$

$$\therefore \quad \tau(1932) = (2+1) \times (1+1) \times (1+1) \times (1+1)$$

$$= 24$$

7002 can be expressed as —

$$7002 = 2 \times 3^2 \times 389$$

$$\therefore \quad \sigma(7002) = \left(\frac{2^2-1}{2-1}\right) \times \left(\frac{3^3-1}{3-1}\right) \times \left(\frac{389^2-1}{389-1}\right)$$

$$= 3 \times \frac{26}{2} \times \frac{151320}{388}$$

$$= 15210$$

To establish the statement, we have to prove that for $n = K+1$, it is also true.

Now, $2903^{K+1} - 803^{K+1} - 464^{K+1} + 261^{K+1}$

$$= (1897+803+464-261)\,2903^{K}$$
$$+ (1897-2903+464-261)\times 803^{K}$$
$$+ (1897-2903+803-261)\times 464^{K}$$
$$+ (1897-2903+803+464)\times 26$$

$$\cancel{= 2903\,(1897\times 2903^{K-1} - 803^{K} - 464^{K} -}$$

(13) Show that $2903^n - 803^n - 464^n + 261^n$ is divisible by 1897 for all natural numbers n.

(Ans) The prime factorization of 1897 —

$$1897 = 7 \times 271$$

Now we have, $2903 \equiv 5 \pmod 7$

$$\Rightarrow 2903^n \equiv 5^n \pmod 7$$

Similarly, $803^n \equiv 5^n \pmod 7$

$$464^n \equiv 2^n \pmod 7$$
$$261^n \equiv 2^n \pmod 7$$

Scanned by CamScanner

Then using linear property of congruences, we can write —

$$2903^n - 803^n - 464^n + 261^n$$
$$\equiv 5^n - 5^n - 2^n + 2^n \pmod 7$$

$$\Rightarrow (2903^n - 803^n - 464^n + 261^n) \equiv 0 \pmod 7$$

Now, $2903 \equiv 193 \pmod{271}$

$$\Rightarrow 2903^n \equiv 193^n \pmod{271}$$

Similarly, $803^n \equiv 261^n \pmod{271}$

$$464^n \equiv 193^n \pmod{271}$$
$$261^n \equiv 261^n \pmod{271}$$

Again using linear property of congruences, we get —

$$2903^n - 803^n - 464^n + 261^n \equiv 0 \pmod{271}$$

Now 7 and 271 are prime to each another.

And $\text{lcm}(7, 271) = 1897$

Then we can write —

$$2903^n - 803^n - 464^n + 261^n \equiv 0 \pmod{\text{lem}(7,271)}$$

$$\Rightarrow 2903^n - 803^n - 464^n + 261^n \equiv 0 \pmod{1897}$$

$\therefore 1897 \mid 2903^n - 803^n - 464^n + 261^n$. (proved)

(14) Find the least positive residues in $3^{36} \pmod{77}$

(Ans) The prime factorization of 77 —

$$77 = 7 \times 11$$

~~We know $3^2 = 9 \equiv 2 \pmod 7$~~

~~$\Rightarrow 3^4 \equiv 2^2 \pmod 7$~~

~~$\Rightarrow$~~

We know, $3^{7-1} \equiv 1 \pmod 7$ {Using Fermat's little theorem

$\Rightarrow 3^6 \equiv 1 \pmod 7$

$\Rightarrow 3^{36} \equiv 1 \pmod 7 \rightarrow$ (i)

Again, $3^{11-1} \equiv 1 \pmod{11}$

$\Rightarrow 3^{10} \equiv 1 \pmod{11}$

$\Rightarrow 3^{30} \equiv 1 \pmod{11} \rightarrow$ (ii)

Again we have, $3^2 \equiv -2 \pmod{11}$

$\Rightarrow 3^4 \equiv 4 \pmod{11}$

$\Rightarrow 3^6 \equiv -8 \pmod{11}$

$\Rightarrow 3^6 \equiv 3 \pmod{11} \rightarrow$ (iii)

~~Since 7 and 11 are~~

Combining (ii) & (iii) we get —

$3^{36} \equiv 3 \pmod{11} \rightarrow$ (iv)

Now 7 and 11 are prime to each other.

~~Then, we have~~

~~$3^{36} \equiv$~~

So we use Chinese Remainder Theorem here.

~~Now,~~

We put $x = 3^{36}$

Then we have to find congruent modulo 77 of x.

We got $x \equiv 1 \pmod{7}$

$x \equiv 3 \pmod{11}$

then, $11Y_1 \equiv 1 \pmod{7}$

$\Rightarrow 4Y_1 \equiv 1 \pmod{7}$

$\Rightarrow 8Y_1 \equiv 2 \pmod{7}$

$\Rightarrow Y_1 \equiv 2 \pmod{7} \longrightarrow$ (v)

Again, $7Y_2 = 3 \pmod{11}$

$\Rightarrow 14Y_2 = 6 \pmod{11}$

$\Rightarrow 3Y_2 \equiv 6 \pmod{11}$

$\Rightarrow 12Y_2 \equiv 24 \pmod{11}$

$\Rightarrow Y_2 \equiv 2 \pmod{11} \rightarrow$ (vi)

Then using Chinese Remainder theorem —

$x \equiv 1 \cdot 11 \cdot 2 + 3 \cdot 7 \cdot 2 \pmod{77}$

$\Rightarrow 3^{36} \equiv 64 \pmod{77}$

Thus the least positive residue $= 64$ (Ans)

(15) Use the theory of congruences to prove that $7 \mid 2^{5n+3} + 5^{2n+3}$ for all $n \geq 1$

Ans

$$2^3 = 8 \equiv 1 \pmod 7 \rightarrow (i)$$

$$5^3 = 125 \equiv -1 \pmod 7 \rightarrow (ii)$$

Now, $2^5 \equiv 32 \pmod 7$

$$\Rightarrow 2^5 \equiv 4 \pmod 7$$

$$\Rightarrow (2^5)^n \equiv 4^n \pmod 7 \quad \boxed{\text{using the properties of congruence}}$$

~~Again, $5^2 \equiv 25 \pmod{}$~~

$$\Rightarrow 2^{5n} \equiv 4^n \pmod 7 \rightarrow (iii)$$

Combining eq (i) & eq (iii) we get —

$$2^{5n+3} \equiv 4^n \pmod 7 \rightarrow (iv)$$

Again, $5^2 \equiv 25 \pmod 7$

$$\Rightarrow 5^2 \equiv 4 \pmod 7$$

$$\Rightarrow 5^{2n} \equiv 4^n \pmod 7 \rightarrow (v)$$

Combining eq (ii) & eq (v) we get —

$$5^{2n+3} \equiv -4^n \pmod 7 \rightarrow (vi)$$

Now using linear property of congruences and combining eq (vi) & eq (iv) we get —

$$2^{5n+3} + 5^{2n+3} \equiv 4^n - 4^n \pmod 7$$

Then $7 \mid 2^{5n+3} + 5^{2n+3}$ (proved)

---

16. Solve the linear congruences —

(a) $15x \equiv 9 \pmod{18}$; (b) $28x \equiv 63 \pmod{105}$

Ans (a) given $15x \equiv 9 \pmod{18}$

$\Rightarrow -3x \equiv 9 \pmod{18}$ [$\because 15x \equiv -3x \pmod{18}$]

$\Rightarrow 6x \equiv -18 \pmod{18}$ (multiply by -2)

$\Rightarrow 6x \equiv 0 \pmod{18}$

$\Rightarrow 18x$

Ans (a) Given $15x \equiv 9 \pmod{18}$

The linear diophantine equation becomes —

$$15x - 9 = 18k \quad (k \in \mathbb{Z})$$

$$\Rightarrow 15x - 18k = 9 \quad \ldots (i)$$

We have, $18 - 15 = 3$

$\Rightarrow 3 \times 18 - 3 \times 15 = 9$

$\Rightarrow (-3) \times 15 - (-3) \times 18 = 9 \quad \ldots (ii)$

Equating eq (i) & (ii) —

$$x_0 = -3$$

$$\therefore x = -3 + \frac{18}{3} n \quad (n \in \mathbb{Z})$$

$$= -3 + 6n$$

$$= 3 + 6n$$

Here the given congruence has multiple solutions —

$$x \equiv 3 \pmod{18}$$
$$x \equiv 9 \pmod{18}$$
$$x \equiv 15 \pmod{18}$$

Ans (b) Given $28x \equiv 63 \pmod{105}$

The linear diophantine equation becomes —

$$28x - 63 = 105k \quad (k \in \mathbb{Z})$$

$$\Rightarrow 28x - 105k = 63 \quad \ldots \text{(i)}$$

We have —

$$4 \times 28 - 105 = 7$$

$$\Rightarrow 36 \times 28 - 9 \times 105 = 63 \quad \ldots \text{(ii)}$$

Equating eq (i) & eq (ii), the general solution of x —

$$x = 36 + \frac{105}{7} \times n \quad (n \in \mathbb{Z})$$
$$= 36 + 15n$$

$\therefore$ The given congruence has solution —

~~36, 51, 66, 81, 96, 111 (mod~~

$$x \equiv 6, 21, 36, 51, 66, 81, 96 \pmod{105}$$

(7) Solve the system of linear congruences —

(a) $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

Ans) Let us choose —

$$N_1 = 3 \quad ; \quad N_2 = 5 \quad ; \quad N_3 = 7$$

$$\therefore \quad M_1 = N_2 N_3 = 35 \; ; \; M_2 = N_1 N_3 = 21$$

$$M_3 = N_1 N_2 = 15$$

Let us choose Y_1, Y_2, Y_3 such that —

$$M_1 Y_1 \equiv 1 \pmod 3$$

$$\Rightarrow 35 Y_1 \equiv 1 \pmod 3$$

$$\Rightarrow 2 Y_1 \equiv 1 \pmod 3$$

$$\Rightarrow Y_1 \equiv 2 \pmod 3 \quad \ldots \text{(i)}$$

$$M_2 Y_2 \equiv 1 \pmod 5$$

$$\Rightarrow 21 Y_2 \equiv 1 \pmod 5$$

$$\Rightarrow Y_2 \equiv 1 \pmod 5 \quad \ldots \text{(ii)}$$

And,

$$M_3 Y_3 \equiv 1 \pmod 7$$

$$\Rightarrow 15 Y_3 \equiv 1 \pmod 7$$

$$\Rightarrow Y_3 \equiv 1 \pmod 7 \quad \ldots \text{(iii)}$$

Then using chinese remainder theorem —

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \pmod{105}$$

$$\equiv 157 \pmod{105} \quad \Rightarrow \boxed{x \equiv 52 \pmod{105}}$$

(17) (b) $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 4 \pmod 7$

Ans Let us choose —

$N_1 = 3$; $N_2 = 5$; $N_3 = 7$

$\therefore M_1 = N_2 N_3 = 35$; $M_3 = N_1 N_2 = 15$

$M_2 = N_1 N_3 = 21$;

Let us choose Y_1, Y_2, Y_3 be inverses of M_1, M_2 and M_3 of congruent modulo 3, 5, 7 respectively.

$\therefore M_1 Y_1 \equiv 1 \pmod 3$

$\Rightarrow 35 Y_1 \equiv 1 \pmod 3$

$\Rightarrow Y_1 \equiv 2 \pmod 3$

Similarly, $Y_2 \equiv 1 \pmod 5$; $Y_3 \equiv 1 \pmod 7$

Then using Chinese Remainder Theorem —

$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 4 \cdot 15 \cdot 1 \pmod{105}$

$\equiv 263 \pmod{105}$

$\equiv 53 \pmod{105}$

(17c) $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$, $x \equiv 5 \pmod 8$

Let, $N_1 = 5$; $N_2 = 7$; $N_3 = 8$

$\therefore M_1 = N_2 N_3 = 56$; $M_3 = N_1 N_2 = 35$

$M_2 = N_1 N_3 = 40$;

Let Y_1, Y_2, Y_3 be the inverse of M_1, M_2, M_3 of congruent modulo 5, 7, 8 respectively.

Scanned by CamScanner

$\therefore \quad M_1 Y_1 \equiv 1 \pmod 5$

$\Rightarrow 56 Y_1 \equiv 1 \pmod 5$

$\Rightarrow Y_1 \equiv 1 \pmod 5 \rightarrow (i)$ $\left\{\because 55 Y_1 \equiv 0 \pmod 5\right\}$

Again, $M_2 Y_2 \equiv 1 \pmod 7$

$\Rightarrow 40 Y_2 \equiv 1 \pmod 7$

$\Rightarrow 5 Y_2 \equiv 1 \pmod 7$

$\Rightarrow 50 Y_2 \equiv 10 \pmod 7 \equiv 3 \pmod 7$

$\Rightarrow Y_2 \equiv 3 \pmod 7 \rightarrow (ii)$

Also, $M_3 Y_3 \equiv 1 \pmod 8$

$\Rightarrow 35 Y_3 \equiv 1 \pmod 8$

$\Rightarrow 3 Y_3 \equiv 1 \pmod 8$

$\Rightarrow Y_3 \equiv 3 \pmod 8 \rightarrow (iii)$

Then using Chinese Remainder theorem —

$$x \equiv 2 \cdot 56 \cdot 1 + 3 \cdot 40 \cdot 3 + 5 \cdot 35 \cdot 3 \pmod{280}$$

$$\equiv 187 \pmod{280}$$

(17d) $x \equiv 5 \pmod 6$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$

(Ans) Let us take —

$N_1 = 6$; $N_2 = 11$; $N_3 = 17$

$\therefore M_1 = N_2 N_3 = 187$; $M_2 = N_1 N_3 = 102$

$$M_3 = N_1 N_2 = 66$$

Let us choose Y_1, Y_2, Y_3 ~~such that~~ be inverse of M_1, M_2, M_3 congruent modulo 6, 11, 17 ~~resp~~ respectively.

$$\therefore \quad M_1 Y_1 \equiv 1 \pmod 6$$

$$\Rightarrow 187 Y_1 \equiv 1 \pmod 6$$

$$\Rightarrow Y_1 \equiv 1 \pmod 6 \rightarrow (i)$$

Again,

$$M_2 Y_2 \equiv 1 \pmod{11}$$

$$\Rightarrow 102 Y_2 \equiv 1 \pmod{11}$$

$$\Rightarrow 3 Y_2 \equiv 1 \pmod{11}$$

$$\Rightarrow Y_2 \equiv 4 \pmod{11} \rightarrow (ii)$$

Also,

$$M_3 Y_3 \equiv 1 \pmod{17}$$

$$\Rightarrow 66 Y_3 \equiv 1 \pmod{17}$$

$$\Rightarrow 15 Y_3 \equiv 1 \pmod{17}$$

$$\Rightarrow 45 Y_3 \equiv 3 \pmod{17}$$

$$\Rightarrow -6 Y_3 \equiv 3 \pmod{17}$$

$$\Rightarrow 6 Y_3 \equiv -3 \pmod{17}$$

$$\Rightarrow 18 Y_3 \equiv -9 \pmod{17}$$

$$\Rightarrow Y_3 \equiv 8 \pmod{17} \rightarrow (iii)$$

Then using Chinese Remainder Theorem —

$$\therefore x \equiv 5 \cdot 187 \cdot 1 + 4 \cdot 102 \cdot 4 + 3 \cdot 66 \cdot 8 \pmod{1122}$$

$$\equiv 785 \pmod{1122}$$

Scanned by CamScanner

(18) Find the number of integers less than n and prime to n, when $n = 256, 324, 900, 2048, 5040, 7200$.

(Ans) For, $n = 256$

$256 = 2^8$

$\therefore$ The number of integers less than 256 and prime to 256, $\phi(256) = 256\left(1-\frac{1}{2}\right)$

$= 128$

For, $n = 324 = 2^2 \times 3^4$

$\therefore \phi(324) = 324 \times \left(1-\frac{1}{2}\right) \times \left(1-\frac{1}{3}\right)$

$= 324 \times \frac{1}{\cancel{2}} \times \frac{2}{3}$

$= 108$

For $n = 900 = 2^2 \times 3^2 \times 5^2$

$\therefore \phi(900) = 900 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

$= 900 \times \frac{1}{\cancel{2}} \times \frac{2}{3} \times \frac{4}{5}$

$= 240$

For $n = 2048 = 2^{11}$

$\therefore \phi(2048) = 2048 \times \left(1-\frac{1}{2}\right) = 1024$

For $n = 5040 = 2^4 \times 3^2 \times 5 \times 7$

$\therefore \phi(5040) = 5040 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)$

$= 5040 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7}$

$= 1152$

$\therefore$ For $n = 7200$

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

$$\therefore \phi(7200) = 7200 \times \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$

$$= 7200 \times \frac{1}{\cancel{2}} \times \frac{\cancel{2}}{3} \times \frac{4}{5}$$

$$= 1920.$$

---

(19) Find the least positive residue in $2^{41} \pmod{23}$

(Ans) We know —

$$\cancel{2^4 \equiv 16 \pmod{23}}$$

$$2^{23-1} \equiv 1 \pmod{23}$$

[using Fermat's little theorem]

$$\Rightarrow 2^{22} \equiv 1 \pmod{23}$$

$$\Rightarrow 2^{44} \equiv 1 \pmod{23}$$

[$\because a \equiv b \pmod{e}$ $\Rightarrow a^k \equiv b^k \pmod{e}$]

$$\Rightarrow 2^{41} \cdot 2^3 \equiv 1 \pmod{23}$$

$$\Rightarrow 8 \times 2^{41} \equiv 1 \pmod{23}$$

$$\Rightarrow 24 \times 2^{41} \equiv 3 \pmod{23}$$

$$\Rightarrow 2^{41} \equiv 3 \pmod{23}$$

$\therefore$ The least positive residue in $2^{41} \pmod{23}$ is 3

(20) Using congruence find the remainder when $2^{73} + 14^{23}$ is divided by 11

(Ans) We know using Fermat's little theorem –

$$2^{11-1} \equiv 1 \pmod{11}$$

$$\Rightarrow 2^{10} \equiv 1 \pmod{11}$$

$$\Rightarrow 2^{70} \equiv 1 \pmod{11}$$

$$\Rightarrow 2^{73} \equiv 8 \pmod{11} \quad \cdots \text{(i)}$$

Again using Fermat's little theorem –

$$14^{10} \equiv 1 \pmod{11}$$

$$\Rightarrow 14^{20} \equiv 1 \pmod{11} \quad \cdots \text{(ii)}$$

$$\Rightarrow 14^{21} \equiv 14 \pmod{11}$$

$$\Rightarrow 14^{22} \equiv 196 \equiv 9 \pmod{11}$$

$$\Rightarrow 14^{23} \equiv 126 \pmod{11}$$

$$\Rightarrow 14^{23} \equiv 5 \pmod{11} \quad \cdots \text{(iii)}$$

Using linear property of congruences and combining eq (i) & eq (iii) we get –

$$2^{73} + 14^{23} \equiv 8 + 5 \pmod{11}$$

$$\equiv 2 \pmod{11}$$

$\therefore$ Then remainder is 2 when $2^{73} + 14^{23}$ is divided by 11.

(21) Prove that the eigth power of any integer is of the form $17K$ or $17K \pm 1$

(Ans) Case ∋ I

~~Let~~ n be an integer and 17 divides n.

Then $n \equiv 0 \pmod{17}$

$\Rightarrow n^8 \equiv 0 \pmod{17}$

i.e $17 \mid n^8$

$\Rightarrow n^8 = 17K \quad (K \in \mathbb{Z})$

Case II

n be an integer such that 17 doesn't divide n.

Since 17 is a prime.

Then n and 17 are prime to each other

Using Fermat's little theorem —

$n^{17-1} \equiv 1 \pmod{17}$

$\Rightarrow n^{16} \equiv 1 \pmod{17} \quad \ldots (i)$

Let $n^8 \equiv K \pmod{17}$

$\Rightarrow n^{16} \equiv K^2 \pmod{17} \quad \ldots (ii)$

equating eq (i) & eq (ii) —

$K^2 \equiv 1 \pmod{17} \rightarrow (iii)$

Now This is possible only for $K \equiv 1, -1 \pmod{1}$

And for any other possible solution of K, eq (iii) doesn't hold.

Then we have —

$$n^8 \equiv \pm 1 \pmod{17}$$

$$\Rightarrow \quad n^8 = 17K \pm 1 \qquad (K \in \mathbb{Z})$$

Now summing up both case I & case II, we can conclude —

the Eigth power of any integer is of the form $17K$ or $17K \pm 1$.

---

(22) Show that $a^{12} - b^{12}$ is divisible by 91 if a and b are both prime to 91.

(Ans) We can write —

$$91 = 7 \times 13$$

Since a, b are both prime to 91.

Then a, b are both prime to 7 and 13.

Then we can write —

$$a^{7-1} \equiv 1 \pmod 7 \qquad \text{[Fermat's Little theorem]}$$

$$\Rightarrow a^6 \equiv 1 \pmod 7$$

$$\Rightarrow a^{12} \equiv 1 \pmod 7$$

Similarly $b^{12} \equiv 1 \pmod 7$ — (i)

Again 13 is a prime and 13 doesn't divide a, b.

So, $a^{13-1} \equiv 1 \pmod{13}$

$\Rightarrow a^{12} \equiv 1 \pmod{13}$ $\Big\} \to$ (ii)

And, $b^{12} \equiv 1 \pmod{13}$

Combining eq (i) & eq (ii) we get —

$a^{12} \equiv 1 \pmod{7\times 13}$ $\Big[\because \text{lcm}[7,13] = 7\times 13$

$b^{12} \equiv 1 \pmod{7\times 13}$

$\therefore\ a^{12} - b^{12} \equiv 1-1 \pmod{91}$

$\Rightarrow 91 \mid a^{12} - b^{12}$ (proved)

~~(23) If n is a prime > 7 prove that $n^6 - 1$ is divisible by 504.~~

Ans. We can write —

$504 = 2^3 \times 3^2 \times 7$

~~Now,~~ $\cancel{n^{2-1} \equiv 1 \pmod{2}}$ ~~(∵ n is prime, n > 7)~~

$\cancel{\Rightarrow n \equiv 1 \pmod{2}}$

$\cancel{\Rightarrow n^6 \equiv 1 \pmod{2}}$

$\cancel{\Rightarrow 2 \mid (n^6 - 1)}$ ... (i)

(23) If n is a prime > 7 prove that n is divisible by 504.

(Ans) We can write —

$$504 = 2^3 \times 3^2 \times 7$$

Since n is a prime > 7, then any of 2, 3, 7 doesn't divide n.

$$\therefore \quad n^{2-1} \equiv 1 \pmod 2 \quad [\text{Fermat's little}]$$

$$\Rightarrow n \equiv 1 \pmod 2$$

$$\Rightarrow n \equiv 1, 3, 5, 7 \pmod 8$$

$$\Rightarrow n^2 \equiv 1, 9, 25, 49 \pmod 8$$

$$\Rightarrow n^2 \equiv 1 \pmod 8 \qquad \left[\because \begin{array}{l} 9 \equiv 1 \pmod 8 \\ 25 \equiv 1 \ (\;,,\;) \\ 49 \equiv 1 \ (\;,,\;) \end{array}\right]$$

$$\Rightarrow n^4 = 1 \pmod 8$$

$$\Rightarrow n^6 = 1 \pmod 8$$

$$\Rightarrow 8 \mid (n^6 - 1) \quad \ldots \text{(i)}$$

Again,

$$n^{3-1} \equiv 1 \pmod 3$$

$$\Rightarrow n^2 \equiv 1 \pmod 3$$

$$\Rightarrow n^2 \equiv 1, 5, 7 \pmod 9$$

$$\Rightarrow n^6 \equiv 1, 125, 343 \pmod 9$$

$$\Rightarrow n^6 \equiv 1 \pmod 9 \qquad \left[\because \begin{array}{l} 125 \equiv 1 \pmod 9 \\ 343 \equiv 1 \ (\;,,\;) \end{array}\right]$$

$$\therefore 9 \mid (n^6 - 1) \quad \ldots \text{(ii)}$$

Also, $n^{7-1} \equiv 1 \pmod 7$

$\Rightarrow n^6 \equiv 1 \pmod 7$

$\Rightarrow 7 \mid (n^6 - 1) \quad \ldots \text{(iii)}$

Since 8, 9, 7 are prime to each other, and all of the divide (n^6-1).

Then multiple of them must divide (n^6-1).

$\therefore \; 8 \times 9 \times 7 = 504$ divide (n^6-1)

(proved)

---

(24) Show that $4(29)! + 5!$ is divisible by 31

(A4) Since 31 is a prime, the by Wilson's theorem —

$(31-1)! + 1 \equiv 0 \pmod{31}$

$\Rightarrow 30! + 1 \equiv 0 \pmod{31} \quad \ldots \text{(i)}$

~~Now let K be the congruence of 4(29)!~~

Now, let $4(29)! + 5! \equiv K \pmod{31}$

$\Rightarrow (30-26)\, 29! + 5! \equiv K \pmod{31}$

$\Rightarrow 30! - 26 \times 29! + 5! \equiv K \pmod{31}$

$\Rightarrow (30! + 1) - 1 - 26 \times 29! + 5! \equiv K \pmod{31}$

$\Rightarrow 5! - 26 \times 29! - 1 \equiv K \pmod{31}$ (by eq (i))

$\Rightarrow 4(29)! - 4 \equiv K \pmod{31}$

$\Rightarrow \quad 4\{29! - 1\} \equiv K \pmod{31}$

$\Rightarrow \quad 4\{30 \times 29! - 30\} \equiv 30K \pmod{31}$

$\Rightarrow \quad 4\{30! + 1 - 31\} \equiv 30K \pmod{31}$ $\left(\because \gcd(30,31) = 1\right)$

$\Rightarrow \quad -4 \times 31 \equiv 30K \pmod{31}$ (By eq (i))

$\Rightarrow \quad 0 \equiv 30K \pmod{31}$

$\Rightarrow \quad -K \equiv 0 \pmod{31}$

$\Rightarrow \quad K \equiv 0 \pmod{31}$

$\therefore \quad 4(29!) + 5! \equiv 0 \pmod{31}$

$\therefore \quad 31 \mid \{4(29!) + 5!\}$ (proved)

---

(25) Using congruence find the remainder when 4444^{4444} is divided by 9.

(Ans) We have —

$4444 \equiv 7 \pmod 9$

$\Rightarrow$ ~~$4444 \equiv 1, 4, 7 \pmod 9$~~

$\Rightarrow$ ~~$4444^3 \equiv 1, 64, 343 \pmod 9$~~

$\Rightarrow$ ~~$4444^3 \equiv 1 \pmod 9$~~

$\Rightarrow \quad 4444^3 \equiv 343 \equiv 1 \pmod 9$

$\Rightarrow \quad 4444^{4443} \equiv 1 \pmod 9$

$\Rightarrow \quad 4444^{4444} \equiv 4444 \equiv 7 \pmod 9$

$\therefore$ 7 is the remainder. (Ans)

(26) Prove that $641 \mid (2^{32}+1)$

(Ans) We have ——

$$2 \equiv 2 \pmod{641}$$
$$2^2 \equiv 4 \pmod{641}$$
$$2^4 \equiv 16 \pmod{641}$$
$$2^8 \equiv 256 \pmod{641}$$
$$2^{12} \equiv 250 \pmod{641}$$
$$2^{16} \equiv 154 \pmod{641}$$
$$\therefore \quad 2^{32} \equiv 23716 \pmod{641}$$
$$\Rightarrow 2^{32} \equiv -1 \pmod{641}$$
$$\Rightarrow 2^{32}+1 \equiv 0 \pmod{641}$$
$$\therefore \quad 641 \mid (2^{32}+1) \quad \text{(proved)}$$

(27) Prove that $7 \mid (2222^{5555} + 5555^{2222})$

(Ans) We have ——

$$2222 \equiv 3 \pmod 7 \quad \cdots (i)$$
$$5555 \equiv 4 \pmod 7 \quad \cdots (ii)$$

From eq (i) ——

$$(2222)^3 \equiv 27 \equiv -1 \pmod 7$$
$$\Rightarrow (2222)^{3\times 1851} \equiv (-1)^{1851} \pmod 7$$

$\Rightarrow 2222^{5553} \equiv -1 \pmod 7$

$\Rightarrow 2222^{5554} \equiv -3 \pmod 7$ (By eq (i)

$\Rightarrow 2222^{5554} \equiv 4 \pmod 7$

$\Rightarrow 2222^{5555} \equiv 5 \pmod 7$ .... (iii)

From eq (ii) —

$$(5555)^3 \equiv 64 \equiv 1 \pmod 7$$

$$\Rightarrow (5555)^{2220} \equiv 1 \pmod 7$$

$$\Rightarrow (5555)^{2222} \equiv 16 \pmod 7$$

$$\Rightarrow (5555)^{2222} \equiv 2 \pmod 7 \quad \text{.. (iv)}$$

Then by eq (iii) & eq (iv) we get —

$$2222^{5555} + 5555^{2222} \equiv 7 \pmod 7$$
$$\equiv 0 \; (\;\text{"}\;)$$

$$\Rightarrow 7 \mid (2222^{5555} + 5555^{2222})$$

(proved)

(28) If p is a prime, prove that —
$$2(p-3)! + 1 \equiv 0 \pmod p$$

By Wilson's theorem we get —

$$(p-1)! + 1 \equiv 0 \pmod p \quad (\because p \text{ is prime})$$

$$\Rightarrow \cancel{p(p-1)(p-2)P! + 1 \equiv 0 \pmod p}$$

$$\Rightarrow (p-1)(p-2)(p-3)! + 1 \equiv 0 \pmod p$$

$$\Rightarrow (p^2 - 3p + 2)(p-3)! + 1 \equiv 0 \pmod p$$

$$\Rightarrow p(p-3)(p-3)! + 2(p-3)! + 1 \equiv 0 \pmod p$$

$$\Rightarrow 2(p-3)! + 1 \equiv 0 \pmod p$$

$$\left\{ \because p(p-3)(p-3)! \equiv 0 \pmod p \right.$$

$$\therefore \boxed{2(p-3)! + 1 \equiv 0 \pmod p} \text{ (proved)}$$

Scanned by CamScanner