Congruences

Two numbers a and b are said to be congruent with respect to modulo m if they leave the same remainder when divided by m. It is denoted by $a \equiv b \pmod m$

Example

(i) $35 \equiv 0 \pmod 7$

(ii) $36 \equiv 1 \pmod 7$

(iii) $37 \equiv 2 \pmod 7$

Note: If $a \equiv b \pmod m$ Then $(a-b)$ is divisible by m.

Properties of Congruence

(1) If $a \equiv b \pmod m$ and $a' \equiv b' \pmod m$ then $a \pm a' \equiv b \pm b' \pmod m$

(2) If $a \equiv b \pmod m$ and $a' = b' \pmod m$ then $aa' \equiv bb' \pmod m$

(3) $ax \equiv bx \pmod m$

(4) $\frac{a}{x} \equiv \frac{b}{x} \pmod m$

where x is a common divisor of a and b and prime to m.

Proof:

Property (1) If $a \equiv b \pmod m$ then $a = b + km$

and $a' \equiv b' \pmod m$ then $a' = b' + k'm$

Now

$$a + a' = b + km + b' + k'm$$

$$a + a' = (b + b') + (k + k')m$$

$$\Rightarrow a + a' \equiv b + b' \pmod m \longrightarrow (1)$$

Similarly $a - a' \equiv b - b' \pmod m \longrightarrow (2)$

From (1) & (2) $a \pm a' \equiv b \pm b' \pmod m$

Property (2) If $a \equiv b \pmod m$ and $a' \equiv b' \pmod m$

then $aa' = bb' \pmod m$

Proof

If $a \equiv b \pmod m$ then $a = b + km$

and $a' \equiv b' \pmod m$ then $a' = b' + k'm$

Now $aa' = (b+km)(b'+k'm)$

$= bb' + bk'm + b'km + kk'm^2$

$= bb' + m(bk' + b'k + kk'm)$

$$\boxed{aa' = bb' \pmod m}$$

Property (3) $ax = bx \pmod m$

Proof let $a \equiv b \pmod m$ then $a = b + km$

Now $ax = (b+km)x$

$= bx + kmx$

$$\boxed{ax = bx \pmod m}$$

Property (4) $\frac{a}{x} \equiv \frac{b}{x} \pmod m$

where x is a Common divisor of a and b and prime to m

Proof: let $a \equiv a' \pmod m$ then $a = a' + km$

and $b \equiv b' \pmod m$ then $b = b' + km$

Given that x is a Common divisor of a and b

$\therefore$ $\frac{a}{x} = \alpha$ (say)

$\frac{b}{x} = \beta$ (say)

then $a = \alpha x$ and $b = \beta x$

$a - b = (\alpha - \beta)x$

Since x is a prime to m

$\therefore \frac{a-b}{x} = \alpha - \beta$

$\frac{a}{x} - \frac{b}{x} = \alpha - \beta$

$\frac{a}{x} - \frac{b}{x}$ is divisible by m

$\therefore \frac{a}{x} \equiv \frac{b}{x} \pmod m$ {$\because$ by note

<u>Problem</u> Find the number of divisors and the sum of divisors of the number 480.

<u>Solution</u>

Prime factorization of 480 is

2	480
2	240
2	120
2	60
2	30
3	15
5	5
	1

$480 = 2\times2\times2\times2\times2 \times 3\times5$

$= 2^5 \times 3^1 \times 5^1$

(i) $\therefore$ The number of divisors of 480 is

$= (5+1)(1+1)(1+1)$

$= 6\times2\times2$

$$\boxed{\text{Number of divisors of } 480 = 24}$$

(ii) Sum of the divisors of 480 $= \left(\frac{2^6-1}{2-1}\right)\left(\frac{3^2-1}{3-1}\right)\left(\frac{5^2-1}{5-1}\right)$

$= \left(\frac{64-1}{1}\right)\left(\frac{9-1}{2}\right)\left(\frac{25-1}{4}\right)$

$= 63 \times 4 \times 6$

$$\boxed{\text{Sum of the divisors of } 480 = 1412}$$

Problem verify that 220 and 284 are amicable numbers

Solution

Prime factorization of 220 and 284 are

$$220 = 2^2 \times 5 \times 11$$

$$284 = 2^2 \times 71$$

Sum of the divisors of 220 $= \left(\frac{2^3-1}{2-1}\right) \times \left(\frac{5^2-1}{5-1}\right) \times \left(\frac{11^2-1}{11-1}\right)$

$$= \left(\frac{8-1}{1}\right) \times \left(\frac{25-1}{4}\right) \times \left(\frac{121-1}{10}\right)$$

$$= 7 \times \frac{24}{4} \times \frac{120}{10}$$

$$= 7 \times 6 \times 12$$

Sum of the divisors of 220 $= 504$

Sum of the divisors of 220, excluding 220 is $= 504 - 220$

$= 284 \longrightarrow (1)$

Sum of the divisors of 284 $= \left(\frac{2^3-1}{2-1}\right) \times \left(\frac{71^2-1}{71-1}\right)$

$$= \left(\frac{8-1}{1}\right) \times \left(\frac{5041-1}{70}\right)$$

$$= 7 \times \frac{5040}{70}$$

$$= 7 \times 72$$

Sum of the divisors of 284 $= 504$

Sum of the divisors of 284, excluding 284 $= 504 - 284$

$= 220 \longrightarrow (2)$

From (1) & (2),

220 and 284 are amicable numbers

Problem Find the number of divisors of 24

Solution

Let N be any positive integer and its prime factors be $2^a, 3^b, 5^c, 7^d \dots$

then $N = 2^a \cdot 3^b \cdot 5^c \, 7^d \dots$

Number of divisors of $N = (a+1)(b+1)(c+1)(d+1)\dots$

$$24 = 2^3 \times 3^1$$

$$\begin{array}{r|l} 2 & 24 \\ \hline 2 & 12 \\ \hline 2 & 6 \\ \hline 3 & 3 \\ \hline & 1 \end{array}$$

No. of divisors of $24 = (3+1)(1+1)$

$= 4 \times 2$

No. of divisors of $24 = 8$

Problem Find the smallest number with 24 divisors.

Solution:

Let the number with 24 divisors be N

then $N = 2^a \times 3^b \times 5^c \times 7^d \dots \longrightarrow (1)$

Number of divisors of $N = (a+1)(b+1)(c+1)(d+1)\dots$

But $24 = 2 \times 2 \times 2 \times 3$

$24 = (1+1) \times (1+1) \times (1+1) \times (2+1)$

From (1) $N = 2^2 \times 3^1 \times 5^1 \times 7^1$

$= 4 \times 3 \times 5 \times 7$

$N = 420$

Problem Find the number of integers which are less than 500 and prime to it.

Solution

$$500 = 2\times 2\times 5\times 5\times 5$$

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

$$\phi(500) = 500\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{5}\right)$$

$$= 500\left(\tfrac{1}{2}\right)\left(\tfrac{4}{5}\right)$$

$$= 500 \times \frac{2}{5}$$

$$= 100 \times 2$$

$$\boxed{\phi(500) = 200}$$

$$\begin{array}{r|l} 2 & 500 \\ 2 & 250 \\ 5 & 125 \\ 5 & 25 \\ 5 & 5 \\ & 1 \end{array}$$

Problem Find the sum of all integers which are less than 500 and prime to it.

Solution

we have $\phi(500) = 200$

Sum of all integers which are less than 500 and prime to it $= \frac{N}{2}\phi(N)$

$$= \frac{500}{2}(200)$$

$$= 500 \times 100$$

$$= 50{,}000$$

Problem Find the highest power of 3 in $\lfloor 1000$

Solution:

$$\left\lfloor\frac{1000}{3}\right\rfloor + \left\lfloor\frac{1000}{3^2}\right\rfloor + \left\lfloor\frac{1000}{3^3}\right\rfloor + \left\lfloor\frac{1000}{3^4}\right\rfloor + \left\lfloor\frac{1000}{3^5}\right\rfloor + \left\lfloor\frac{1000}{3^6}\right\rfloor + \left\lfloor\frac{1000}{3^7}\right\rfloor + \cdots$$

$$= 333 + 111 + 37 + 12 + 4 + 1 + 0 + 0 \ldots$$

$$= 498$$

Problem Find the higher power of 2 in $\lfloor 1000$

Solution

$$\left\lfloor \frac{1000}{2} \right\rfloor + \left\lfloor \frac{1000}{2^2} \right\rfloor + \left\lfloor \frac{1000}{2^3} \right\rfloor + \left\lfloor \frac{1000}{2^4} \right\rfloor + \left\lfloor \frac{1000}{2^5} \right\rfloor + \left\lfloor \frac{1000}{2^6} \right\rfloor + \left\lfloor \frac{1000}{2^7} \right\rfloor +$$

$$\left\lfloor \frac{1000}{2^8} \right\rfloor + \left\lfloor \frac{1000}{2^9} \right\rfloor + \left[\frac{1000}{2^{10}} \right] + \left\lfloor \frac{1000}{2^{11}} \right\rfloor + \dots$$

$$= 500 + 250 + 125 + 62 + 31 + 15 + 7 +$$
$$3 + 1 + 0 + 0 + \dots$$

$$= 994$$

Problem with how many zeros does $\lfloor 75$ end ?

Solution

Any number ends with zero is a multiple of 10

$\therefore$ The prime factor of $10 = 2 \times 5$

first let us find the highest power of 2 and 5 in $\lfloor 75$.

$$\left\lfloor \frac{75}{2} \right\rfloor + \left\lfloor \frac{75}{2^2} \right\rfloor + \left\lfloor \frac{75}{2^3} \right\rfloor + \left\lfloor \frac{75}{2^4} \right\rfloor + \left\lfloor \frac{75}{2^5} \right\rfloor + \left\lfloor \frac{75}{2^6} \right\rfloor + \left\lfloor \frac{75}{2^7} \right\rfloor + \dots$$

$$= 37 + 18 + 9 + 4 + 2 + 1 + 0 + \dots$$

$$= 71$$

$\therefore$ The higher Power of 2 in $\lfloor 75$ is 71

and $\left\lfloor \frac{75}{5} \right\rfloor + \left\lfloor \frac{75}{5^2} \right\rfloor + \left\lfloor \frac{75}{5^3} \right\rfloor + \left\lfloor \frac{75}{5^4} \right\rfloor + \left\lfloor \frac{75}{5^5} \right\rfloor + \dots$

$$= 15 + 3 + 0 + 0 + \dots$$

$$= 18$$

$\therefore$ The highest Power of 5 in $\lfloor 75$ ~~is~~ is 18

∴ The highest power of 10 in $\lfloor 75$ = minimum of 71, 18

= 18

∴ 75 ends with 18 zeroes.

Problem: Find the number of zeroes with which $\lfloor 61$ ends.

Ans: 14

Fermats little theorem

Statement If 'p' is a prime number and 'a' is a positive integer not divisible by 'p', then

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

For Example:

$$a = 13 \quad , \quad p = 17$$

By Fermat's little theorem

$$13^{17-1} \equiv 1 \pmod{17}$$

$$13^{16} \equiv 1 \pmod{17}$$

Problem ①

Find the remainder when 11^7 is divided by 13

Solution

First we starts with the power of 11 is 1,

$11^1 = 11 \pmod{13} = 11$ (or) -2

$11^2 = 11 \times 11 = -2 \times -2 = 4 \pmod{13} = 4$

$11^4 = 11^2 \times 11^2 = 4 \times 4 = 16 \pmod{13} = 3$

$11^7 = 11^4 \times 11^3 = 11^4 \times 11^2 \times 11 = 3 \times 4 \times -2$

$= -24 \pmod{13}$

$= -11 \pmod{13}$

$= 2$

$$13 \overline{)\,24\,} \; 1, \quad 24 - 13 = 11$$

$\therefore$ 11^7 is divided by 13 the remainder is 2

Problem

Find the remainder when 7^{256} is divided by 13

Solution

$7 \bmod 13 = 7$ (or) -6

$7^2 = 7 \times 7 = -6 \times -6 = 36 \pmod{13}$

$= 10 \pmod{13}$

$= 10$ or -3

$= -3$ (choose -3)

$$13 \overline{)\,36\,} \; 2, \quad 36 - 26 = 10$$

$7^4 = 7^2 \times 7^2 = -3 \times -3 = 9 \pmod{13}$

$= 9$ or -4 (choose -4)

$= -4$

$7^8 = 7^4 \times 7^4 = -4 \times -4 = 16 \pmod{13}$

$= 3 \pmod{13}$

$= 3$ or -10 (choose 3)

$= 3$

$7^{16} = 7^8 \times 7^8 = 3 \times 3 = 9 \pmod{13}$

$= 9$ or -4 (choose -4)

$= -4$

$7^{32} = 7^{16} \times 7^{16} = -4 \times -4$

$= 16 \pmod{13}$

$= 3 \pmod{13}$

$= 3$ or -10 (Choose 3)

$= 3$

$7^{64} = 7^{32} \times 7^{32} = 3 \times 3$

$= 9 \pmod{13}$

$= 9$ or -4 (Choose -4)

$= -4$

$7^{128} = 7^{64} \times 7^{64} = -4 \times -4$

$= 16 \pmod{13}$

$= 3 \pmod{13}$

$= 3$ or -10 (Choose 3)

$= 3$

$7^{256} = 7^{128} \times 7^{128} = 3 \times 3$

$= 9 \pmod{13}$

$= 9$ or -4

$= 9$ (at the final stage we choose only positive number)

$\therefore$ 7^{256} is divided by 13 the remainder is 9

Problem Find the remainder when $(129)^{8941}$ is divisible by 29 using Fermat's theorem.

Solution

Since 29 is a prime number, and 129 is not divisible by 29.

Let $a = 129$ and $p = 29$

By Fermat's theorem.

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

$$\therefore 129^{29-1} \equiv 1 \pmod{29}$$

$$129^{28} \equiv 1 \pmod{29} \longrightarrow (1)$$

By division algorithm,

$$\begin{array}{r|l} & 319 \\ 28 & 8941 \\ & 84 \\ \hline & 54 \\ & 28 \\ \hline & 261 \\ & 252 \\ \hline & 9 \end{array}$$

$$8941 = 28 \times 319 + 9$$

$$(129)^{8941} = (129)^{28 \times 319 + 9}$$

$$= \left[(129)^{28}\right]^{319} \cdot (129)^9$$

$$= (1)^{319} \cdot (129)^9 \quad \{\because \text{from } (1)$$

$$= (129)^9$$

$$\begin{array}{r|l} & 4 \\ 29 & 129 \\ & 116 \\ \hline & 13 \end{array}$$

$$= (29 \times 4 + 13)^9 \pmod{29}$$

$$= (0 + 13)^9$$

$$= (13)^9$$

$$= (13^2)^4 \times 13$$

$$= (169)^4 \times 13$$

$$= (29 \times 5 + 24) \times 13 \pmod{29}$$

$$= 24 \times 13$$

$$= 312 \pmod{29}$$

29

$$\begin{array}{r} 24\times \\ \hline 72 \\ 24 \\ \hline 31 \end{array}$$

$= 29 \times 10 + 22 \pmod{29}$

$= 0 + 22 \pmod{29}$

$$\begin{array}{r|l} & 10 \\ 29 & 312 \\ & 290 \\ \hline & 22 \end{array}$$

$(129)^{8941} = 22 \pmod{29}$

Hence, $(129)^{8941}$ is divisible by 29 the remainder is 22

Problem

Show that

$$4^{2n+1} + 3^{n+2} \equiv 0 \pmod{13}$$

Solution

$$4^{2n+1} + 3^{n+2} = 4^{2n} \cdot 4 + 3^{n} \cdot 3^{2}$$

$$= (4^2)^n \, 4 + 3^n \cdot 3^2$$

$$= 16^n \cdot 4 + 3^n \cdot 9$$

$$= (13+3)^n \, 4 + 3^n \cdot 9 \pmod{13}$$

$$= 3^n \cdot 4 + 3^n \, 9$$

$$= 3^n (4+9)$$

$$= 3^n \cdot 13 \pmod{13}$$

$3^n \cdot 13$ is a multiple of 13

$\therefore$ It is completely divisible by 13

$$4^{2n+1} + 3^{n+2} \equiv 0 \pmod{13}$$

Wilson's Theorem

If p is a prime number then $\lfloor p-1 + 1$ is divisible by p.

Problem Prove that $\lfloor 18 + 1$ is divisible by 437.

Solution

$437 = 19 \times 23$ where 19 and 23 are primes.

By Wilson's Theorem,

$\cancel{\lfloor 18 + 1}$ $\lfloor 19-1 + 1$ is divisible by 437

$\Rightarrow \lfloor 18 + 1$ is divisible by 437

and $\lfloor 22 + 1 \equiv 0 \pmod{23}$

$22 \times 21 \times 20 \times 19 \times \lfloor 18 + 1 \equiv 0 \pmod{23}$

$(23-1) \times (23-2) \times (23-3) \times (23-4) \times \lfloor 18 + 1 \equiv 0 \pmod{23}$

$-1 \times -2 \times -3 \times -4 \times \lfloor 18 + 1 \equiv 0 \pmod{23}$

$24 \times \lfloor 18 + 1 \equiv 0 \pmod{23}$

$(23+1) \times \lfloor 18 + 1 \equiv 0 \pmod{23}$

$\lfloor 18 + 1 \equiv 0 \pmod{23}$

$\therefore \lfloor 18 + 1 = 0 \mod (19, 23)$