Unit-5

Classical Theorems And Multiplicative Functions

WILSON'S THEOREM:

If p is prime, then $(p-1)! \equiv -1 \pmod{p}$

PROOF:

To prove: $(p-1)! \equiv -1 \pmod{p}$

When $p=2$, $(p-1)! = (2-1)!$

$= 1$

$\equiv -1 \pmod{2}$

So, the theorem is true when $p = 2$

Now, let $p > 2$ and

let a be a positive Integer such that $1 \leq a \leq p-1$.

Since p is a prime and $a < p$, $(a, p) = 1$

Then, congruence $ax \equiv 1 \pmod{p}$ has a solution a'

Congruence modulo p.

$aa' \equiv 1 \pmod{p}$ where $1 \leq a' \leq p-1$

a, a' are inverses of each other

modulo p.

If $a' = a$, then $a \cdot a \equiv 1 \pmod{p}$

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

$p \mid a^2 - 1 \Rightarrow p \mid (a-1)(a+1) \Rightarrow p \mid a-1$ or $p \mid a+1$

Since $a < p$, if $p \mid a+1$, then $a = p-1$

If $p \mid a-1$, then $a-1 = 0$

$$a = 1$$

$a = 1$ or $p-1$ if $a = a'$

1 and $p-1$ are their own inverses.

ie) If $a' \neq a$, excluding 1 and $p-1$, the remaining $p-3$ resides 2, 3, 4, ... $(p-3)$, $(p-2)$ can be grouped into $\frac{p-3}{2}$ pairs of the type a, a' such that

$$aa' \equiv 1 \pmod{p}$$

Multiplying all these pairs together, we get

$$2 \cdot 3 \cdot 4 \cdots (p-3)(p-2) \equiv 1 \pmod{p}$$

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-2)(p-1) \equiv p-1 \pmod{p}$$

$$(p-1)! \equiv -1 \pmod{p}$$

Hence the theorem.

This can be rewritten as $(p-1)! + 1 \equiv 0 \pmod{p}$

$$p \mid (p-1)! + 1$$

which is the result suggested by Wilson

Examples:

1) Show that $18! + 1$ is divisible by 437.

Wilson theorem is $(p-1)! + 1$ is divisible by a prime p

437 is not a prime and $437 = 19 \cdot 23$,

where 19 & 23 are primes

since 19 is a prime

$(19-1)! + 1 = 18! + 1$ is div by 19

$18! + 1 \equiv 0 \pmod{19}$

since 23 is a prime

$(23-1)! + 1 = 22! + 1$ is div by 23

$22! + 1 \equiv 0 \pmod{23}$

$22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! + 1 \equiv 0 \pmod{23}$

$22 \equiv -1 \pmod{23}$

$21 \equiv -2 \pmod{23}$

$20 \equiv -3 \pmod{23}$

$19 \equiv -4 \pmod{23}$

$22 \cdot 21 \cdot 20 \cdot 19 \equiv (-1)(-2)(-3)(-4) \pmod{23}$

$\equiv 24 \pmod{23}$

$\equiv 1 \pmod{23}$

x by $18!$ we get

$22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! = 18! \pmod{23}$

$22 \cdot 21 \cdot 20 \cdot 19 \cdot 18! + 1 = 18! + 1 \pmod{23}$

LHS is $22! + 1 \equiv 0 \pmod{23}$

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

$\therefore$ $18! + 1$ is div by 19 & 23

$18! + 1$ is div by lcm $[19, 23] = 19 \cdot 23$

$= 437$.

2) If p is a prime number of the form $4m+1$, where m is a positive integer, prove that

$$(2m!)^2 + 1 \equiv 0 \pmod{p}$$

Soln:

Gn, the prime number p is of the form $4m+1$, where m is a positive integer.

To prove: $(2m!)^2 + 1 \equiv 0 \pmod{p}$

Since $p = 4m+1$ is a prime, by Wilson theorem

$$(p-1)! \equiv -1 \pmod{p}$$

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

$$(4m+1-1)! + 1 \equiv 0 \pmod{p}$$

$$4m! + 1 \equiv 0 \pmod{p}$$

$\Rightarrow$ $4m(4m-1)(4m-2)\ldots(4m-(2m-1)) \cdot 2m! + 1 \equiv 0 \pmod{p}$

$4m+1 = p$

$$4m = p-1 \equiv -1 \pmod p$$

$$4m-1 = p-2 \equiv (-2) \pmod p$$

$$4m-2 = p-3 \equiv (-3) \pmod p$$

$$4m-(2m-1) = p-2m \equiv -2m \pmod p$$

x together we get

$$4m\,(4m-1)(4m-2)\ldots(4m-(2m-1))$$

$$\equiv (-1)(-2)(-3)\ldots(-2m) \pmod p$$

$$\equiv 2m! \pmod p$$

x by $(2m)!$ on both sides

$$4m(4m-1)(4m-2)\ldots(4m-(2m-1))(2m)!$$

$$\equiv (2m!)(2m!) \pmod p$$

$$4m! \equiv (2m!)^2 \pmod p$$

$$4m! + 1 \equiv (2m!)^2 + 1 \pmod p$$

$$0 \equiv (2m!)^2 + 1 \pmod p$$

$$\therefore \quad (2m!)^2 + 1 \equiv 0 \pmod p$$

3) If n is a positive integer such that $(n-1)! \equiv -1 \pmod n$, then prove that n is a prime.

Gn: n is positive integer such that

$$(n-1)\,1 \equiv -1 \pmod{n}$$

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

To Prove n is a prime

Suppose n is not a prime, then n is a composite number.

$\therefore n = ab$, where a, b are Integers b/w 1 and n

ie $1 < a, b < n$

Since $a \mid ab$, $a \mid n$ by (1)

$$n \mid [(n-1)! + 1]$$

$$a \mid [(n-1)! + 1]$$

But $1 < a < n$, so a is one of the Integers $2, 3, 4 \cdots (n-1)$

$\therefore a$ divides the product $2 \cdot 3 \cdot 4 \cdots (n-1) = (n-1)!$

$$a \mid [(n-1)! + 1] \text{ and } a \mid (n-1)!$$

$$a \mid [(n-1)! + 1 - (n-1)!] \Rightarrow a \mid 1$$

which is a contradiction, since $1 < a$.

Our assumption n is composite is wrong.

Hence n is prime.

4) Prove that $63! \equiv -1 \pmod{71}$.

Hence $p=71$ is a prime.

by Wilson's theorem $(p-1)! + 1 \equiv 0 \pmod{71}$

$(71-1)! \equiv -1 \pmod{71}$

$70! \equiv -1 \pmod{71}$

$70! = 70 \cdot 69 \cdot 68 \cdot 67 \cdot 66 \cdot 65 \cdot 64 \cdot 63!$

Now $70 \equiv -1 \pmod{71}$

$69 \equiv -2 \pmod{71}$

$68 \equiv -3 \pmod{71}$

$67 \equiv -4 \pmod{71}$

$66 \equiv -5 \pmod{71}$

$65 \equiv -6 \pmod{71}$

$64 \equiv -7 \pmod{71}$

$\therefore 70 \cdot 69 \cdot 68 \cdot 67 \cdot 66 \cdot 65 \cdot 64 \equiv (-1)(-2)(-3)(-4)(-5)(-6)(-7) \pmod{71}$

$\equiv -5040 \pmod{71}$

$\equiv -(-1) \pmod{71}$

$\equiv 1 \pmod{71}$

$\times 63!$ on both sides

$70 \cdot 69 \cdot 68 \cdot 67 \cdot 66 \cdot 65 \cdot 64 \cdot 63! \equiv 63! \pmod{71}$

$70! \equiv 63! \pmod{71}$

$-1 \equiv 63! \pmod{71}$

$$63! \equiv -1 \pmod 7$$

5) If p is a prime, prove that

$$(p-1)(p-2)(p-3)\cdots(p-k) \equiv (-1)^k k! \pmod p$$

where $1 \le k < p$.

Gin: p is prime

$$p-1 \equiv -1 \pmod p$$
$$p-2 \equiv -2 \pmod p$$
$$\vdots$$
$$p-k \equiv -k \pmod p$$

* together, we get

$$(p-1)(p-2)\cdots(p-k) \equiv (-1)(-2)\cdots(-k) \pmod p$$
$$= (-1)^k\, 1.2.3\cdots k \pmod p$$
$$= (-1)^k\, k! \pmod p$$

6) If $n = 1.3.5\cdots(p-2)$, where p is an odd prime, show that $n^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$.

Given: $n = 1.3.5\cdots(p-2)$, where p is an odd prime.

Since p is prime, by Wilson's theorem.

$$(p-1)! \equiv -1 \pmod p$$

$$1.2.3.4.5.\cdots(p-2)(p-1) \equiv -1 \pmod{p}$$

$$(1.3.5\cdots(p-2))\,(2.4.6\cdots(p-1)) \equiv -1 \pmod{p}$$

$$2(2.4.6\cdots(p-1)) \equiv -1 \pmod{p}$$

$$2^{n}\left[p-(p-2)\right]\left[p-(p-4)\right]\cdots(p-1) \equiv -1 \pmod{p}$$

$$2^4 \equiv -1 \pmod{17}$$

$$(2^4)^2 \equiv (-1)^2 \pmod{17}$$

$$2^8 \equiv 1 \pmod{17}$$

$$2^{1000} = 2^{992+8} = 2^{992} \cdot 2^8$$

$$2^{1000} \equiv 1 \cdot 1 \pmod{17}$$

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

The remainder is 1 when 2^{1000} is divided by 17.

7) Find remainder when 193^{183} is devided by 19.

19 is a prime and $19 \nmid 193$.

By Feermats Little theorem..

$$193^{19-1} \equiv 1 \pmod{19}$$

$$193^{18} \equiv 1 \pmod{19}$$

$$(193^{18})^{10} \equiv 1^{10} \pmod{19}$$

$$\begin{array}{r} 10 \\ 18\overline{)183} \\ 180 \\ \hline 3 \end{array}$$

$$\begin{array}{r} 10 \\ 19\overline{)193} \\ 190 \\ \hline 3 \end{array}$$

$193^{180} \equiv 1 \pmod{19}$

$193^{183} = 193^{180+2+1}$

$= 193^{180} \cdot 193^2 \cdot 193$

$193 \equiv 3 \pmod{19}$

$193^2 \equiv 3^2 \pmod{19} \Rightarrow 193^2 \equiv 9 \pmod{19}$

$193^{183} \equiv 1.9.3 \pmod{19}$

$\equiv 27 \pmod{19}$

$\equiv 8 \pmod{19}$

$\therefore$ The remainder is 8, when 193^{183} is divided by 19

2) Find the remainder when 24^{947} is divided by 17.

Here $a = 24$, $p = 17$

WKT 17 is a prime and $17 \nmid 24$

$\therefore$ By Fermat's theorem, $24^{17-1} \equiv 1 \pmod{17}$

$p - (p-2) \equiv -(p-2) \pmod{p}$

$p - (p-4) \equiv -(p-4) \pmod{p}$

$\vdots$

$p - 3 \equiv -3 \pmod{p}$

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

The number of equations is $\frac{p-1}{2}$

Multiplying together, we get

$$[p-(p-2)][p-(p-4)]\cdots(p-3)(p-1)$$

$$\equiv (-1)^{\frac{p-1}{2}} \cdot (p-2)(p-4)\cdots 3.1 \pmod p$$

$$\equiv (-1)^{\frac{p+1}{2}} \cdot x \pmod p$$

Sub in (1), we get

$$x \cdot x(-1)^{\frac{p+1}{2}} \equiv -1 \pmod p$$

$$x^2 \equiv (-1)^{\frac{p+1}{2}+1} \pmod p$$

$$x^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p$$

FERMAT'S LITTLE THEOREM

Statement:

If p is a prime and a is any integer not divisible by p, then $a^{p-1} \equiv 1 \pmod p$

Proof:

Gin p is a prime and a is any integer not div by p

i.e) $p \nmid a$

When an integer is divided by p, the set of possible remainders are $0, 1, 2, 3, \ldots p-1$.

Consider the set of integers,

$$1.a,\ 2.a,\ 3.a,\ \ldots\ (p-1)a \quad \rightarrow (1)$$

Suppose $pa \equiv 0 \pmod p$, then $p \mid ia$.

But $p \mid a$ $\therefore$ $p \mid i$, which is impossible, since $i < p$

$$pa \not\equiv 0 \pmod p \quad \text{for } (i = 1, 2, \ldots p-1)$$

So, no term of (1) is zero

Next, we prove they are all distinct

Suppose $pa \equiv ja \pmod p$, where $1 \le i, j \le p-1$.

Then $(i-j)a \equiv 0 \pmod p$

$\Rightarrow p \mid (i-j)a$

Since $p \mid a$, $p \mid i-j$ and $i, j < p \Rightarrow |i-j| < p$

$$i - j = 0 \Rightarrow i \equiv j \pmod p$$

$$i \neq j \Rightarrow ia \neq ja.$$

This means, no of two of integers in (1) are congruent modulo p.

$\therefore$ The least residues of the integers $a, 2a, 3a, \ldots$

$(p-1)a$ modulo p are the same as the integers

$1, 2, 3, \ldots p-1$ in some order.

So, their product are congruent modulo p.

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

$$1 \cdot 2 \cdot 3 \cdots (p-1)\, a^{p-1} \equiv (p-1)! \pmod{p}$$

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$$

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

The result $a^{p-1} \equiv 1 \pmod{p}$ is equivalent to $a^p \equiv a \pmod{p}$

Using this theorem, and properties of congruences, we can find remainders of certain number of the for a^m when divided by p.

1) Find the remainder when 2^{1000} is divided by 17

WKT: 17 is prime

By Fermats theorem

$$2^{17-1} \equiv 1 \pmod{17}$$

$$2^{16} \equiv 1 \pmod{17}$$

$$(2^{16})^{62} \equiv 1^{62} \pmod{17}$$

$$2^{992} \equiv 1 \pmod{17}$$

$$2^4 \equiv 16 \equiv -1 \pmod{17}$$

$$2^{4^{16}} \equiv 1 \pmod{17}$$

$$\begin{array}{r|l} & 62 \\ \hline 16 & 1000 \\ & 96 \\ \hline & 40 \\ & 32 \\ \hline & 8 \end{array}$$

$(24^{16})^{121} \equiv 1^{121} \pmod{17}$

$24^{1936} \equiv 1 \pmod{17}$

$24^{1947} = 24^{1936+11} = 24^{1936} \cdot 24^{11}$

$24^2 = 576 \equiv -2 \pmod{17}$

$(24^2)^2 \equiv (-2)^2 \pmod{17}$

$24^4 \equiv 4 \pmod{17}$

$(24^4)^2 \equiv 4^2 \pmod{17}$

$24^8 \equiv 16 \pmod{17}$

$\equiv -1 \pmod{17}$

$24^{11} = 24^8 \cdot 24^2 \cdot 24 \equiv (-1)(-2) \cdot 7 \pmod{17}$

$= 14 \pmod{17}$

$24^{1947} = 1 \cdot 14 \pmod{17}$

$= 14 \pmod{17}$

The remainder is 14 when 24^{1947} is divided by 17

2) Find the remainder when 15^{1976} is divided by 23

WKT 23 is a prime & $23 \nmid 15$

By Fermat's little theorem

$$15^{23-1} \equiv 1 \pmod{23}$$

$$15^{22} \equiv 1 \pmod{23}$$

$$(15^{22})^{89} \equiv 1^{89} \pmod{23}$$

$$15^{1958} \equiv 1 \pmod{23}$$

$$15^{1976} \equiv 15^{1958+18}$$

$$= 15^{1958} \cdot 15^{16} \cdot 15^{2}$$

$$15^2 = 225 \equiv 18 \pmod{23}$$

$$\equiv -5 \pmod{23}$$

$$(15^2)^2 \equiv (-5)^2 \pmod{23}$$

$$15^4 \equiv 25 \pmod{23}$$

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

$$(15^4)^4 \equiv 2^4 \pmod{23}$$

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

$$15^{16} \equiv -7 \pmod{23}$$

$$15^{1976} \equiv 1 \cdot (-7)(-5) \pmod{23}$$

$$\equiv 35 \pmod{23}$$

$$\equiv 12 \pmod{23}$$

$$\begin{array}{r|l} 22 & 1976 \\ & 176 \\ \hline & 216 \\ & 198 \\ \hline & 18 \end{array} \quad 89$$

$$\begin{array}{r|l} 23 & 225 \\ & 207 \\ \hline & 18 \end{array} \quad 9$$

3) Find remainder when 2^{341} is divided by 341.

W.K.T $341 = 11.31$, where 11 & 31 are primes

Here $a=2$, 11 and 31 do not divide 2

So, by Fermat's Theorem

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

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

$$2^{31-1} \equiv 1 \pmod{31}$$

$$2^{30} \equiv 1 \pmod{31}$$

$$(2^{30})^{10} \equiv 1^{10} \pmod{31}$$

$$2^{300} \equiv 1 \pmod{31}$$

$$(2^{10})^4 = 1^4 \pmod{11}$$

$$2^{40} \equiv 1 \pmod{11}$$

$$2^{341} = 2^{300+40+1}$$

$$= 2^{300} \cdot 2^{40} \cdot 2$$

$$= 1.1.2 \bmod (\text{lcm}(31, 11))$$

$$= 2 \pmod{341}$$

The remainder is 2 when 2^{341} is divided by 341.

4) Find the remainder when 5^{2003} is divided by 11.

Here $p=11$, $a=5$ & $p \nmid a$

By Fermat's theorem,

$$5^{11-1} \equiv 1 \pmod{11}$$

$$5^{10} \equiv 1 \pmod{11}$$

$$(5^{10})^{200} \equiv 1^{200} \pmod{11}$$

$$5^{2000} \equiv 1 \pmod{11}$$

$$5^2 = 25 \equiv 3 \pmod{11}$$

$$5^3 \equiv 15 \pmod{11}$$

$$\equiv 4 \pmod{11}$$

$$5^{2003} = 5^{2000} \cdot 5^3 \equiv 1.4 \pmod{11}$$

$$\equiv 4 \pmod{11}$$

Remainder = 4

$$11 \overline{)25} \quad 2$$
$$22$$
$$3$$

5) Compute the remainder when 7^{1001} is divided by 17.

$$7^2 = 49 \equiv -2 \pmod{17}$$

$$(7^2)^2 \equiv (-2)^2 \pmod{17}$$

$$7^4 \equiv 4 \pmod{17}$$

$$(7^4)^2 \equiv 4^2 \equiv 16 \pmod{17}$$

$$7^8 \equiv -1 \pmod{17}$$

$$(7^8)^2 \equiv (-1)^2 \pmod{17}$$

$7^{16} \equiv 1 \pmod{17}$

$(7^{16})^{62} \equiv 1^{62} \pmod{17}$

$7^{992} \equiv 1 \pmod{17}$

$7^{1001} = 7^{992+8+1}$

$= 7^{992} \cdot 7^{8} \cdot 7$

$\equiv 1 (-1) \cdot 7 \pmod{17}$

$\equiv -7 \pmod{17}$

$\equiv 10 \pmod{17}$

Remainder = 10

6) Find the remainder when $13^{18} + 19^{12}$ is divided by 247.

$247 = 13 \cdot 19$

Both 13, 19 are primes.

By Fermant's little theorem,

$13^{19-1} \equiv 1 \pmod{19}$

$13^{18} \equiv 1 \pmod{19}$

$19 \equiv 0 \pmod{19}$, $19^{12} \equiv 0 \pmod{19}$

$13^{18} + 19^{12} \equiv 1 + 0 \pmod{19}$

$\equiv 1 \pmod{19}$

$13 \equiv 0 \pmod{13}$

$\Rightarrow 13^{18} \equiv 0 \pmod{13}$

By Fermat's Little theorem

$$19^{13-1} \equiv 1 \pmod{13}$$

$$19^{2} \equiv 1 \pmod{13}$$

$$13^{18} + 19^{12} \equiv 0 + 1 \pmod{13}$$

$$\equiv 1 \pmod{13}$$

Since $13^{18} + 19^{12}$ gives same remainder 1 when divided by 13, 19

$$13^{18} + 19^{12} \equiv 1 \pmod{[13, 19]}$$

$$\equiv 1 \pmod{13 \cdot 19}$$

$$\equiv 1 \pmod{247}$$

Remainder is 1

7) Prove that $1^{p-1} + 2^{p-1} + 3^{p-1} + \dots + (p-1)^{p-1} \equiv -1 \pmod{p}$ WKT

By Fermat's Theorem,

$$a^{p-1} \equiv 1 \pmod{p}, \text{ if } (p, a) = 1$$

$\therefore$ It is true for $a = 1, 2, 3, \dots p-1$

$$1^{p-1} \equiv 1 \pmod{p}, \; 2^{p-1} \equiv 1 \pmod{p}, \; 3^{p-1} \equiv 1 \pmod{p}$$

$$(p-1)^{p-1} \equiv 1 \bmod p$$

Adding all these congurences, we get

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \dots + (p-1)^{p-1} \equiv (1 + 1 + \dots + 1) \pmod{p}$$

$$\equiv (p-1) \pmod p$$

$$p-1 \equiv -1 \pmod p$$

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod p$$

Theorem:

Let p be a prime and a any integer such that $p \nmid a$, then the solution of the linear congruence $ax \equiv b \pmod p$ is given by $x \equiv a^{p-2} b \pmod p$

Gin:

p is a prime and a is an integer not divisible by p.

$$(a, p) = 1$$

the congruence, $ax \equiv b \pmod p \rightarrow (1)$ has unique solution

By Fermat's Theorem

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

$$a \cdot a^{p-2} \equiv 1 \pmod p$$

So, a^{p-2} is the inverse of $a \bmod p$.

$\times (1)$, by a^{p-2}, we get,

$$a^{p-2}(ax) \equiv a^{p-2} b \pmod p$$

$$a^{p-1} x \equiv a^{p-2} b \pmod p$$

$$1x \equiv a^{p-2} b \pmod p$$

$$x \equiv a^{p-2} b \pmod p$$

Hence the theorem.

EULER'S THEOREM:

Arithmetical Function or Number Theoretic Function

A real (or complex) valued function defined on the set of positive Integers N:

ϕ - Euler's phi function or Euler totient function

Def:

Let $\phi: N \to N$ be a fn defined by $\phi(1)=1$ and for $n>1$.

$\phi(n)$ = the no. of positive integers $\leq n$ and relatively prime to n.

This fn is called as Euler's function.

Theorem:

EULERS THEOREM

let m be a positive integer and a be any integer such that $(a,m)=1$, then $a^{\phi(m)} \equiv 1 \pmod m$

Proof:

Gin m is a positive Integer and a is any Integer such that $(a,m)=1$

Let $x_1, x_2, \ldots x_{\phi(m)}$ be all the positive integers $\leq m$ and relatively prime to m.

since $x_p - x_j < m$, clearly $x_p \not\equiv x_j \pmod m$ if $i \neq j$

Consider the products $ar_1, ar_2, \cdots, ar_{\phi(m)}$

Since $(a,m)=1$,

$$ar_i \not\equiv ar_j \pmod{m} \text{ if } i \neq j$$

$ar_1, ar_2, \cdots ar_{\phi(m)}$ mod m are distinct

We now prove $(ar_i, m)=1$

Suppose $(ar_i, m) > 1$, then let p be a prime factor of $(ar_i, m)=d$.

$$p \mid ar_i \text{ and } p \mid m$$

$$p \mid a \text{ or } p \mid r_i \text{ and } p \mid m$$

If $p \mid a$ and $p \mid m$, then $p \mid (a,m) \Rightarrow (a,m) \neq 1$

which is again a contradiction.

$$(ar_i, m)=1, \quad i=1,2,3,\cdots \phi(m)$$

$\therefore$ the $\phi(m)$ least residues $ar_1, ar_2, \cdots ar_{\phi(m)}$ modulo m are distinct and relatively prime to m. So, they are the same as integers $r_1, r_2 \cdots r_{\phi(m)}$ in some order modulo m.

$\therefore$ their product $ar_1, ar_2, \cdots ar_{\phi(m)} \equiv r_1, r_2, \cdots r_{\phi(m)} \pmod{m}$

Since each r_i is relatively prime to m,

$(a_1 a_2 \cdots a_{\phi(m)}, m) = 1$

we get $a^{\phi(m)} \equiv 1 \pmod{m}$

Hence the proof.

Theorem:

Multiplicative Function.

A number theoretic function f is multiplicative if f is not identically zero and if $f(mn) = f(m) f(n)$ whenever $(m,n) = 1$.

A multiplicative function is called completely multiplicative if we also have,

$$f(mn) = f(m) f(n) \quad \text{for all } m, n \in N$$

Theorem:

Let f be a multiplicative function and n be a positive integer with canonical decomposition

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Then $f(n) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdots f(p_k^{\alpha_k})$.

Proof: We prove by induction on the no. of distinct primes k.

If $k=1$, then $n=p_1^{a_1}$ and $f(n)=f(p_1^{a_1})$, which is trivially true.

Assume, it is true for any integer with canonical decomposition consisting of k distinct primes.

$$f(n)=f(p_1^{a_1}).f(p_2^{a_2})\dots f(p_k^{a_k})$$

Let n be any integer with $k+1$ distinct primes in its canonical decomposition, say.

$$n=p_1^{a_1}.p_2^{a_2}\dots p_k^{a_3}\,p_{k+1}^{a_{k+1}}.$$

Since $(p_1^{a_1}.p_2^{a_2}\dots.p_k^{a_k}.p_{k+1}^{a_{k+1}})=1$. and f is multiplicative

$$f(p_1^{a_1}\,p_2^{a_2}\dots p_k^{a_k}\,p_{k+1}^{a_{k+1}})=f(p_1^{a_1}\,p_2^{a_2}\dots p_k^{a_k})\cdot f(p_{k+1}^{a_{k+1}})$$

$$=f(p_1^{a_1})f(p_2^{a_2})\dots f(p_k^{a_k})\dots f(p_{k+1}^{a_{k+1}})$$

Using induction hypothesis,

The assumption for k distinct primes is true.

$\Rightarrow$ it is true for $k+1$ distinct primes

Hence by mathematical induction, it is true for any positive integer n.

Theorem:

Euler function ϕ is multiplicative.

Proof: Let m and n be positive integers such that $(m,n)=1$

To prove: $\phi(mn) = \phi(m)\phi(n)$

Arrange the mn integers $1, 2, 3, \ldots mn$ in m rows of n numbers each.

	1	$m+1$	$2m+1$	$3m+1$	$\cdots$ $(n-1)m+1$
	2	$m+2$	$2m+2$	$3m+2$	$\cdots$ $(n-1)m+2$
	3	$m+3$	$2m+3$	$3m+3$	$\cdots$ $(n-1)m+3$
	$\vdots$	$\vdots$			
r^{th} row	r	$m+r$	$2m+r$	$3m+r$	$\cdots$ $(n-1)m+r$
	$\vdots$	$\vdots$			
	m	$2m$	$3m$	$4m$	$\cdots$ nm

Let r be a positive integer $\leq m$ such that $(r,m) > 1$.

We will now show that no element of the r^{th} row in the array is relatively prime to mn.

Let $d = (r, m)$. Then $d \mid r$ and $d \mid m \Rightarrow d \mid km+r$ for any integer k.

This means d is a factor of every element in r^{th} row. Thus, no element in the r^{th} row is relatively prime to m and hence to mn if $(r, m) > 1$.

In other words, the elements in the array relatively prime to mn come from r^{th} row only if $(r, m) = 1$

Since $r < m$ and relatively prime to m, we find there are $\phi(m)$ such integers r and have $\phi(m)$ each rows

Now, let us consider the r^{th} row where $(r, m) = 1$

The elements in the r^{th} row are

$$r, m + r, 2m + r, \ldots (n-1)m + r$$

Then they are divided by n, the remainders are $0, 1, 2 \ldots n-1$ in some order of which $\phi(n)$ are relatively prime to n.

$\therefore$ exactly $\phi(n)$ elements in r^{th} row are relatively prime to n and hence to mn.

Thus there are $\phi(m)$ rows containing positive integers relatively prime to mn and each row contains (m, n) elements relatively prime to it.

Hence the array contains $\phi(m)\,\phi(n)$ positive integers $\leq mn$ and relatively prime to mn.

That is $\phi(mn) = \phi(m)\,\phi(n)$.

Theorem:

Let p be a prime and α is a positive integer.

then $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left[1-\frac{1}{p}\right]$

Proof:

$\phi(p^\alpha)$ = no. of positive integers $\leq p^\alpha$ and relatively prime to it.

= no of positive integers $\leq p^\alpha$ -

number of positive integers $\leq p^\alpha$ and not relatively prime to it.

The number of positive integers $\leq p^\alpha$ is p^α (because they are $1, 2, 3, \cdots p^\alpha$)

The number of positive integers $\leq p^\alpha$ and not prime to it are various multiples of p.

They are $1p, 2p, 3p, \cdots p^{\alpha-1}p$.

The number of such numbers $= p^{\alpha-1}$

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right)$$

Theorem:

Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the canonical decomposition of the positive integer n.

Then $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$.

Given the canonical decomposition of positive integer

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

Since ϕ is multiplicative,

$$\phi(n) = \phi(p_1^{\alpha_1})\ \phi(p_2^{\alpha_2}) \dots \phi(p_k^{\alpha_k})$$

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right) p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right) \dots p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right).$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}\left[1-\frac{1}{p_1}\right]\left[1-\frac{1}{p_2}\right] \dots \left[1-\frac{1}{p_k}\right]$$

$$= n\left[1-\frac{1}{p_1}\right]\left[1-\frac{1}{p_2}\right] \dots \left[1-\frac{1}{p_k}\right]$$

1). Find $\phi(1105)$ and $\phi(71)$.

We have $1105 = 5 \cdot 13 \cdot 17$

5 | 1105
13 | 221
17

$$\phi(1105) = \phi(5) \cdot \phi(13) \cdot \phi(17)$$

$$= 4 \cdot 12 \cdot 6$$

$$= 768$$

$$7! = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$$

2 | 5040
2 | 2520
2 | 1260
2 | 630
5 | 315
7 | 63
9 = 3^2

$$\phi(7!) = \phi(2^4) \cdot \phi(3^2) \cdot \phi(5) \cdot \phi(7)$$

$$= 2^4\left(1-\frac{1}{2}\right) 3^2\left(1-\frac{1}{3}\right) \cdot 4 \cdot 6$$

$$= 2^3 \cdot 3 \cdot 2 \cdot 4 \cdot 6$$

$$= 1152$$

2) Compute $\phi(6860)$

$6860 = 2^2 \cdot 5 \cdot 7^3$

$\phi(6860) = \phi(2^2) \cdot \phi(5) \cdot \phi(7^3)$

$= 2^2\left(1-\frac{1}{2}\right) \cdot 4 \cdot 7^3\left(1-\frac{1}{7}\right)$

$= 2 \cdot 4 \cdot 7^2 \cdot 6$

$= 2352$

2	6860
2	3430
5	1715
7	343
7	49
	7

3) Find the positive integers n such that $\phi(n)=6$

$\phi(n)=6$

Find n by trial & error

$\phi(6) = \phi(2 \cdot 3) = \phi(2) \cdot \phi(3) = 1 \cdot 2 = 2 \neq 6$

$\phi(7) = 7-1 = 6 \quad \therefore n=7$

$\phi(8) = \phi(2^3) = 2^3\left(1-\frac{1}{2}\right) = 4 \neq 6$

$\phi(9) = \phi(3^2) = 3^2\left(1-\frac{1}{3}\right) = 6 \quad \therefore n=9$

$\phi(10) = \phi(2 \cdot 5) = \phi(2) \cdot \phi(15) = 1 \cdot 4 \neq 6$

$\phi(11) = 10 \neq 6$

$\phi(12) = \phi(2^2 \cdot 3) = \phi(2^2) \cdot \phi(3) = 2^2\left(1-\frac{1}{2}\right) \cdot 2$

$= 4 \neq 6$

$\phi(13) = 12 \neq 6$

$\phi(14) = \phi(2 \cdot 7) = \phi(2) \cdot \phi(7) = 1 \cdot 6 = 6 \quad \therefore n=14$

$\phi(15) = \phi(3.5) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8 \neq 6$

$\phi(16) = \phi(2^4) = 2^4 \left[1 - \frac{1}{2}\right] = 8 \neq 6$

$\phi(17) = 16$

$\phi(18) = \phi(3^2 \cdot 2) = \phi(3^2) \cdot \phi(2)$

$= 3^2 \left(1 - \frac{1}{3}\right) \cdot 1$

$= 3 \cdot 2$

$= 6 \qquad \therefore n = 18$

The only possible values of n are 7, 9, 14, 18

4) Show that $\phi(n) = \frac{n}{2}$ if $n = 2^k$.

$n = 2^k$

$$\phi(n) = \phi(2^k) = 2^k \left(1 - \frac{1}{2}\right)$$

$$= 2^k \cdot \frac{1}{2}$$

$$= \frac{n}{2}$$

5) Prove that $\phi(2^{2k+1})$ is a square

$$\phi(2^{2k+1}) = 2^{2k+1} \left(1 - \frac{1}{2}\right)$$

$$= 2^{2k+1} \cdot \frac{1}{2}$$

$$= 2^{2k}$$

$$= (2^k)^2$$

6) Prove that $16^{99} \equiv 1 \pmod{437}$ using Euler's theorem.

$437 = 19 \cdot 23$ where 19 & 23 are primes

$$\phi(437) = \phi(19) \cdot \phi(23)$$
$$= 18 \cdot 22$$
$$= 396$$

Since $(2, 437) = 1$, by Euler's Theorem

$$2^{\phi(437)} \equiv 1 \pmod{437}$$
$$2^{396} \equiv 1 \pmod{437}$$
$$(2^4)^{99} \equiv 1 \pmod{437}$$
$$16^{99} \equiv 1 \pmod{437}$$

7) Using Euler's theorem, find remainder when 245^{1040} is divided by 18.

Here $a = 245 = 5 \cdot 7^2$ and $m = 18 = 3^2 \cdot 2$

$$(a, m) = 1$$

By Euler's Theorem

$$a^{\phi(m)} \equiv 1 \pmod{m}$$
$$245^{\phi(18)} \equiv 1 \pmod{18}$$
$$\phi(18) = \phi(3^2 \cdot 2) = \phi(3^2) \cdot \phi(2)$$
$$= 3^2\left(1 - \frac{1}{3}\right) \cdot 1 = 6$$
$$245^6 \equiv 1 \pmod{18}$$
$$(245^6)^{173} \equiv 1^{173} \pmod{18}$$

$$\begin{array}{r|l} & 173 \\ \hline 6 & 1040 \\ & 6 \\ \hline & 44 \\ & 42 \\ \hline & 20 \\ & 18 \\ \hline & 2 \end{array}$$

$245^{1038} \equiv 1 \pmod{18}$

$245^{1040} = 245^{1038+2} = 245^{1038} \cdot 245^2$

$245 \equiv 11 \pmod{18}$

$245^2 = 11^2 \pmod{18}$

$\equiv 121 \pmod{18}$

$\equiv 13 \pmod{18}$

$245^{1049} \equiv 1 \cdot 13 \pmod{18}$

$\equiv 13 \pmod{18}$

Remainder = 13

Theorem:

If n is a positive integer, then $\sum_{d/n} \phi(d) = n$

Proof:

Given n is a positive Integer

Let $S = \{1, 2, 3, \ldots n\}$. We partition S into disjoint sets as below.

Let d be a divisor of n and let C_d denote the set of those positive integers $m \leq n$ such that $d = (m, n)$

$m \in C_d$ if $(m, n) = d \Rightarrow \left(\frac{m}{d}, \frac{n}{d}\right) = 1$

The no. of elements in the set C_d = number of positive integer $\leq \frac{n}{d}$ and relatively prime to it

$= \phi(n/d)$

Since there is a set of corresponding to every divisor d of n and every integer m belongs to exactly one such set C_d, these sets partition S.

The sum of elements in various sets = the total number of elements in S

$$\sum_{d|n} \phi(n/d) = n$$

But d runs over the set of divisors of n, so does n/d

$$\sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$$

$$\sum_{d|n} \phi(d) = n.$$

1) verify the theorem $\sum_{d|n} \phi(d) = n$ for $n = 28$

$n = 28$

the positive divisors of 28 are 1, 2, 4, 7, 14, 28

$$\sum_{d|n} \phi(d) = \phi(1) + \phi(2) + \phi(4) + \phi(7) + \phi(14) + \phi(28)$$

$\phi(1) = 1$, $\phi(2) = 1$,

$\phi(4) = \phi(2)^2 = 2^2\left(1 - \frac{1}{2}\right) = 2$

$\phi(7) = 7 - 1 = 6$

$\phi(14) = \phi(2 \cdot 7) = \phi(2) \cdot \phi(7) = 1 \cdot 6 = 6$

$\phi(28) = \phi(2^2 \cdot 7) = \phi(2^2) \cdot \phi(7)$

$$= 2^2\left(1-\frac{1}{2}\right).6$$

$$= 2.6$$

$$= 12$$

$$\sum_{d|n} \phi(d) = 1+1+2+6+6+12$$

$$= 28$$

2) For $n = 11^3.5$ verify that $\sum_{d|n} \phi(d) = n$

The divisors of n are $1, 5, 11, 5.11, 11^2, 5.11^2, 11^3, 5.11^3$

There are 8 divisors.

$$\sum_{d|n} \phi(d) = \phi(1)+\phi(5)+\phi(11)+\phi(5.11)+\phi(11^2)+\phi(5.11^2)+\phi(11^3)+\phi(5.11^3)$$

$\phi(1) = 1$ $\phi(5) = 5-1 = 4$

$\phi(11) = 11-1 = 10$

$\phi(5.11) = \phi(5).\phi(11) = 4.10 = 40$

$\phi(11^2) = 11^2\left(1-\frac{1}{11}\right) = 11.10 = 110$

$\phi(5.11^2) = \phi(5).\phi(11^2) = 4.110 = 440$

$\phi(11^3) = 11^3\left(1-\frac{1}{11}\right) = 11^2.10 = 1210$

$\phi(5.11^3) = \phi(5).\phi(11^3) = 4.1210 = 4840$

$$\sum_{d|n} \phi(d) = 1+4+10+40+110+440+1210+4840$$

$$= 6655$$

$$= n$$

Tau and Sigma Functions

τ function:

For a positive integer n, $\tau(n)$ denotes the number of positive divisors of n

$$\tau(n) = \sum_{d|n} d^0 = \sum_{d|n} 1$$

σ function:

For a positive integer n, $\sigma(n)$ denotes the sum of the positive divisors of n

$$\sigma(n) = \sum_{d|n} d$$

Examples:

1) Find $\tau(12)$ and $\tau(19)$

The positive divisors of 12 are 1, 2, 3, 4, 6, 12

So, there are 6 divisors-

$\tau(12)$ = no. of positive devisors of 12

$= 6$

The positive divisors of 19 are 1, 19

$\tau(19)$ = the no. of positive divisors of 19

$= 2$

Since for any prime p, the positive divisors are 1 & p

$\tau(p) = 2$ for any prime p.

2) Find $\sigma(12)$ & $\sigma(19)$

Positive divisors of 12 are 1, 2, 3, 4, 6, 12

$$\sigma(12) = 28$$

The positive divisors of 19 are 1 & 19

$$\sigma(19) = 1+19 = 20$$

[$\sigma(p) = 1+p$, For any prime p]

3) Compute value of σ for $n=28$

Positive divisors of 28 are 1, 2, 4, 7, 14, 28

$$\sigma(28) = 1+2+4+7+14+28$$
$$= 56$$

Theorem:

If f is a number theoretic function which is multiplicative and for any positive integer n the function F given by $F(n) = \sum_{d|n} f(d)$ is also multiplicative.

Given: f is multiplicative function

∴ for any two positive integers m and n, which are relatively prime,

$$f(m.n) = f(m).n$$

$$F(n) = \sum_{d|n} f(d)$$

$$F(mn) = \sum_{d \mid mn} f(d)$$

Since $(m,n)=1$, every positive divisor of mn is the product of a unique pair of positive divisors d_1 of m and d_2 of n, where $(d_1,d_2)=1$

$$F(mn) = \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2)$$

$$= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2)$$

$$= \sum_{d_2 \mid n} \left[\sum_{d_1 \mid m} f(d_1) \right] f(d_2)$$

$$= \sum_{d_2 \mid n} [F(m)] f(d_2)$$

$$= F(m) \sum_{d_2 \mid n} f(d_2)$$

$$F(mn) = F(m) \cdot F(n)$$

Hence F is multiplicative.

Theorem:

Prove that τ and σ are multiplicative functions

Proof:

By Theorem

$$F(n) = \sum_{d|n} f(d)$$ is multiplicative if f is multiplicative

1. If $f(d) = d^0 = 1$, is the constant for each $d|n$

If d_1, d_2 are two divisors $(d_1, d_2) = 1$

$$f(d_1 d_2) = 1,$$

$$f(d_1) = 1$$

$$f(d_2) = 1$$

$$\therefore \quad f(d_1 d_2) = f(d_1) f(d_2)$$

So, constant function is multiplicative.

Then $$F(n) = \sum_{d|n} 1 = \tau(n)$$

If $(m,n) = 1$, then $F(mn) = F(m) F(n)$

$$\tau(mn) = \tau(m) \tau(n)$$

So, τ is multiplication.

2) To prove: σ is multiplicative.

Take $f(d) = d$, identity function.

If d_1 and d_2 are two divisors and $(d_1, d_2) = 1$

Then, $f(d_1 d_2) = d_1 d_2$

$= f(d_1) f(d_2)$

f is multiplicative

Hence $F(n) = \sum_{d|n} d = \sigma(n)$

For $(m,n)=1$,

$F(mn) = F(m)\, F(n)$

$\sigma(mn) = \sigma(m)\, \sigma(n)$

σ is multiplicative.

Theorem:

If $n = p^\alpha$, where p is a prime and α is a positive integer, then $\tau(p^\alpha) = \alpha + 1$, $\sigma(p^\alpha) = \dfrac{p^{\alpha+1} - 1}{p-1}$

Proof:

Given $n = p^\alpha$

$\therefore$ the factors of p^α are $1, p, p^2, p^3, \ldots p^{\alpha-1}, p^\alpha$

So, there are $\alpha+1$ factors

Hence, $\tau(p^\alpha) =$ number of factors of p^α

$= \alpha + 1$

$\sigma(p^\alpha) =$ sum of all the factors of p^α

$= 1 + p + p^2 + \ldots + p^\alpha$

$$\sigma(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}$$

Theorem:

If n is a positive integer with canonical decomposition $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then $\tau(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}-1}{p_2-1} \cdots \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

Proof:

Given, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

where $p_1, p_2, \ldots p_k$ are distinct primes and $a_1, a_2 \cdots \alpha_k$ are positive integers. Since τ and σ are multiplicative functions.

$$\tau(n) = \tau(p_1^{\alpha_1}) \cdot \tau(p_2^{\alpha_2}) \cdots \tau(p_k^{\alpha_k})$$

$$= (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1)$$

$$\sigma(n) = \sigma(p_1^{\alpha_1}) \cdot \sigma(p_2^{\alpha_2}) \cdots \sigma(p_k^{\alpha_k})$$

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \frac{p_2^{\alpha_2+1}}{p_2-1} \cdots \frac{p_k^{\alpha_k+1}-1}{p_k-1}$$

Examples

1) If $n = p_1 . p_2 \cdots p_k$ be a product of k primes, then find $\tau(n)$ and $\sigma(n)$.

Given:

$n = p_1 , p_2 , \cdots p_k$ where each p_i is a prime.

$\therefore$ Each p_i has 2 factors 1 and p_i.

But τ and σ are multiplicative functions.

$(p_i , p_j) = 1$ for all $i \neq j$

$\tau(n) = \tau(p_1) . \tau(p_2) \cdots \tau(p_k)$

$= 2 . 2 \cdots 2$

$\tau(n) = 2^k$

$\sigma(n) = \sigma(p_1)\sigma(p_2) \cdots \sigma(p_k)$

$= (p_1+1)(p_2+1) \cdots (p_k+1)$

2) If $n = 2187$, find $\tau(n)$ and $\sigma(n)$.

$n = 2187 = 3^7$

So, the positive factors are $1, 3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7$.

$\tau(n)$ = number of factors = 8

$\sigma(n)$ = sum of factors.

$= 1 + 3 + 3^2 + 3^3 + 3^4 + 3^5 + 3^6 + 3^7$

$= \frac{3^8 - 1}{3 - 1} = 3,280$

3) For any prime p, prove that

i) $\sigma(p+2) = \sigma(p)+2$ ii) $\sigma(p)$ is odd.

Soln:

Since p is a prime $p+2$ is also a prime.

So the factors of $p+2$ are 1 and $p+2$

i) $\therefore \sigma(p+2)$ = sum of factors

$= p+2+1$

$= (p+1)+2$

$= \sigma(p)+2.$

ii) $\sigma(p)$ = sum of factors of p

$= p+1$, which is odd.

4) Compute $\tau(28)$ and $\sigma(28)$.

$28 = 4 \cdot 7$

$(4,7) = 1$

$\tau(28) = \tau(4) \cdot \tau(7)$ & $\sigma(28) = \sigma(4) \cdot \sigma(7)$

But the positive divisors of 4 are 1, 2, 4 and positive divisors of 7 are 1, 7

$\tau(28) = 3 \cdot 2 = 6$

$\sigma(28) = 7 \cdot 8 = 56$

5) If $n = 6120$, compute $\tau(n), \sigma(n)$.

Given:

$n = 6120 = 2^3 \cdot 3^2 \cdot 5 \cdot 17$

2	6120
2	3060
2	1530
3	765
3	255
5	85
	17

By theorem,

$$\tau(n) = \tau(2^3) \cdot \tau(3^2) \cdot \tau(5) \cdot \tau(17)$$

$$= (3+1)(2+1)\cdot(1+1)\cdot(1+1)$$

$$= 4 \cdot 3 \cdot 2 \cdot 2$$

$$= 48$$

$$\sigma(n) = \sigma(2^3) \cdot \sigma(3^2) \cdot \sigma(5) \cdot \sigma(17)$$

$$= \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} \cdot \frac{17^2-1}{17-1}$$

$$= 15 \cdot 13 \cdot 6 \cdot 18$$

$$= 21,060$$

6) Prove that the cubes of an integer has one of the forms $9m$, $9m+1$, $9m+8$.

Soln:

When an integer a is divided by 9, then the remainder is one of $0, 1, 2, 3, 4, 5, 6, 7, 8$.

$\therefore$ the number a is of the form.

$a = 9q$ or $9q+1$, $9q+2$ .... or $9q+8$

When $a = 9q$ then $a^3 = q^3q^3 = q(q^2q^3) = 9m$ form

$a = 9q+1$, then $a^3 = q^3q^3 + 3 \cdot q^2q^2 + 3 \cdot 9q + 1$

$= q(q^2q^3 + 27q^2 + 3q) + 1$

$= 9m+1$ form

$a = 9q+2$, then $a^3 \equiv 9m+8$

$a = 9q+3 = 3(3q+1)$, then $a^3 = 27(3q+1)^3 = 9m$ form

When $a = 9q+4$ then $a^3 = (9q+4)^3$

$= q^3q^3 + 3q^2q^2 \cdot 4 + 3 \cdot 9q \cdot 4^2 + 4^3$

$= q^3 \cdot q^3 + 3 \cdot q^2 \cdot q^2 \cdot 4 + 3 \cdot 9 \cdot q \cdot 4^2 + 64$

$= q(q^2q^3 + 3 \cdot 9 \cdot q^2 \cdot 4 + 3 \cdot q \cdot 4^2 + 7) + 1$

$= 9m+1$ form

When $a = 9q+5$ then $a^3 = (9q+5)^3$

$= q^3q^3 + 3 \cdot q^2 \cdot q^2 \cdot 5 + 3 \cdot 9q \cdot 5^2 + 5^3$

$= q^3q^3 + 3 \cdot q^2 \cdot q^2 \cdot 5 + 3 \cdot 9 \cdot q \cdot 5^2 + 125$

$= q^3q^3 + 3q^2q^2 \cdot 5 + 3 \cdot 9 \cdot q \cdot 5^2 + 117 + 8$

$= q(q^2q^3 + 3 \cdot 9q^2 \cdot 5 + 3 \cdot q \cdot 5^2 + 13) + 8$

$= 9m+8$ form

Similarly, $a = 9q+6$, $a = 9q+7$, $9q+8$, then a^3

will be of the form $9m, 9m+1, 9m+8$.

$\therefore$ the cube of an integer is one of the forms.

$9m, 9m+1, 9m+8$.

7) Prove that $3^{2n+1} + 2^{n+2} \equiv 0 \pmod 7$ for all positive Integers n.

$3^2 = 9 \equiv 2 \pmod 7$

$3^{2n} \equiv 2^n \pmod 7$

$3^{2n+1} \equiv 3 \cdot 2^n \pmod 7$ $\rightarrow$ (1)

$2 \equiv 2 \pmod 7$

$2^{n+2} \equiv 2^{n+2} \pmod 7$

$\equiv 4 \cdot 2^n \pmod 7$ $\rightarrow$ (2)

(1) + (2) $\Rightarrow$ $3^{2n+1} + 2^{n+2} \equiv 3 \cdot 2^n + 4 \cdot 2^n \pmod 7$

$\equiv 7 \cdot 2^n \pmod 7$

$\equiv 0 \pmod 7$

8) If p is a prime and a and b are integers,

P.T $(a+b)^p \equiv a^p + b^p \pmod p$

Soln: p is prime, a and b are integers.

$\therefore$ p is a positive Integer.

Using binomial expansion for positive integer index, we have.

$$(a+b)^p = a^p + {}^pC_1\, a^{p-1}.b + {}^pC_2\, a^{p-2}.b^2 + \ldots + {}^pC_r\, a^{p-r} b^r + \ldots + {}^pC_{p-1}\, a.b^{p-1} + b^p$$

$${}^pC_r = \frac{p(p-1)\ldots 1\,(p-r+1)}{r!},$$

$p \mid {}^pC_r$ for $r = 1, 2, \ldots, n-1$

$${}^pC_r \equiv 0 \pmod p$$

$$(a+b)^p \equiv a^p + 0 + 0 + \ldots + 0 + b^p \pmod p$$

$$\equiv a^p + b^p \pmod p$$

q) show that $7^{2n+1} + 1 \equiv 0 \pmod 8$.

$$7^{2n} = (7^2)^n$$

$$= 49^n$$

$$= (1+48)^n$$

$$(p-1)! \equiv -1 \pmod p$$

Hence the theorem.

This can be rewritten as $(p-1)! + 1 \equiv 0 \pmod p$

$p \mid (p-1)! + 1$, which is the result suggested by wilson.

1. Show that $18! + 1$ is divisible by 437.

Soln:

10) Show that for any integer n, $n^5 - n$ is divisible by 30.

We have to prove, $n^5 - n \equiv 0 \pmod{30}$

$$n^5 \equiv n \pmod{30}$$

$$30 = 2 \cdot 3 \cdot 5$$

$$\phi(30) = \phi(2) \cdot \phi(3) \cdot \phi(5)$$

$$= 1 \cdot 2 \cdot 4$$

$$= 8$$

$$n^8 \equiv 1 \pmod{30}$$

$$n^8 - 1 \equiv 0 \pmod{30}$$

$$(n^4 - 1)(n^4 + 1) \equiv 0 \pmod{30}$$

$$n^4 - 1 \equiv 0 \pmod{30}$$

$$n^4 \equiv 1 \pmod{30}$$

$$n^5 \equiv n \pmod{30} \Rightarrow n^5 - n \equiv 0 \pmod{5}$$

$n^5 - n$ is divisible by 30.

Part-A

1) compute the remainder when 3^{302} is divided by 5.

$3^4 = 81 \equiv 1 \pmod 5$

$(3^4)^{75} \equiv 1^{75} \pmod 5$

$3^{300} \equiv 1 \pmod 5$

$3^{302} = 3^{300+2} = 3^{300} \cdot 3^2$

$3^2 = 9 \equiv 4 \pmod 5$

$3^{302} \equiv 1 \cdot 4 \pmod 5$

$\equiv 4 \pmod 5$

Remainder is 4

2) Find the remainder when 100! is divided by 101

WKT 101 is prime

By wilsons theorem,

$(101-1)! \equiv -1 \pmod{101}$

$100! \equiv 100 \pmod{101}$

$\therefore$ the remainder is 100

3) Find the remainder when 18! is divided by 19

19 is prime

WKT.

By Wilson's Theorem

$$(19-1)! \equiv -1 \pmod{19}$$

$$18! \equiv -1 \pmod{19}$$

$$\equiv 18 \pmod{19}$$

Remainder is 18.

4. Define a multiplicative function with an example.

A number theoretic function f is multiplicative if f is not identically zero and if $f(mn) = f(m).f(n)$ whenever $(m,n)=1$

Eg: number theoretic constant function $f(n)=1$ is multiplicative.

If $(m,n)=1$, then $f(m)=1$, $f(n)=1$ & $f(m,n)=1$

$$f(mn) = f(m)\, f(n)$$

5) Compute the value of sigma function if $n=28$.

$$n = 28 = 4.7$$

$$(4,7)=1$$

Factors of 4 are 1, 2, 4 $\quad \therefore \sigma(4) = 1+2+4=7$

Factors of 7 are 1, 7 $\quad \therefore \sigma(7) = 1+7=8$

$$\sigma(n) = \sigma(4 \cdot 7) = \sigma(4) \cdot \sigma(7)$$
$$= 7 \times 8$$
$$= 56$$

6) Verify Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$ if $p=7$

$p = 7$

$(p-1)! = 6! = 720$

$720 \equiv -1 \pmod{7}$

$(p-1)! \equiv -1 \pmod{p}$ when $p=7$

$$\begin{array}{r} 103 \\ 7 \overline{)\,720} \\ \underline{7} \\ 20 \\ \underline{21} \\ -1 \end{array}$$

7) Compute the value of sigma function for $n=36$.

$n = 36 = 4 \cdot 9$

$(4, 9) = 1$

$\sigma(36) = \sigma(4) \cdot \sigma(9)$

$\sigma(4) = 1 + 2 + 4 = 7$

$\sigma(9) = 1 + 3 + 9 = 13$

$\sigma(36) = 7 \cdot 13 = 91$

8) When $n = 2^k$, prove that $\phi(n) = n/2$

$$\phi(n) = \phi(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^k \cdot \frac{1}{2}$$
$$= \frac{n}{2}$$

9) If p is a prime and a is any integer such that p|a. Then prove that a^{p-2} is an inverse of a mod p.

Since p is a prime and p|a,

By Fermats Theorem,

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

$$a \cdot a^{p-2} \equiv 1 \pmod{p}$$

a^{p-2} is an inverse of a mod p.

10) If p and q are different primes then find the remainder when $p^{q-1} + q^{p-1}$ is divided by pq.

Gn p and q are different primes, then $(p,q) = 1$

By Fermats Theorem,

$$p^{q-1} \equiv 1 \pmod{q} \quad \text{and} \quad q^{p-1} \equiv 1 \pmod{p}$$

$$p \equiv 0 \pmod{p}$$

$$p^{q-1} \equiv 0 \pmod{p} \quad \text{and} \quad q \equiv 0 \pmod{q}$$

$$q^{p-1} \equiv 0 \pmod{q}$$

$$p^{q-1} + q^{p-1} \equiv 1 + 0 \pmod{q}$$

$$\equiv 1 \pmod{q}$$

$$p^{q-1} + q^{p-1} \equiv 0 + 1 \pmod{p}$$

$$\equiv 0 + 1 \pmod{p}$$

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$$

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{(\text{Lcm}(p,q))}$$

$$\equiv 1 \pmod{pq}$$

11) Given two different numbers m and n for which $\tau(m) = \tau(n)$

$\tau(m)$ = the number of different factors

WKT For any prime number there are only 2 factors

If $m = 13$, $n = 17$

then $\tau(13) = 2$, $\tau(17) = 2$

$$\tau(13) = \tau(17)$$

12) If p is a prime such that $\sigma(p)$ is odd, then find p.

since p is a prime, its only factors are 1 & p

$$\sigma(p) = 1 + p.$$

For $1+p$ to be odd, p must be even.

$$p = 2$$

13) Prove that for a prime p, $\phi(p) + \sigma(p)$ is always even.

Since p is a prime, $\phi(p) = p - 1$

$\sigma(p) = p+1$

$\phi(p) + \sigma(p) = p-1+p+1$

$= 2p$, which is always even.

14) If n is a power of 2, then prove that $\sigma(n)$ is always odd.

Let $n = 2^k$, k is a positive integer.

$\sigma(n) = \sigma(2^k) = 2^{k+1} - 1$

Since 2^{k+1} is always even, $2^{k+1} - 1$ is always odd

$\sigma(2^k)$ is always odd.

15) Let p be a positive integer such that $\phi(p) = p-1$, prove that p is a prime.

Given p is a positive integer.

Suppose p is not a prime, then p is composite number and it has a factor.

Let $d \mid p$, where $1 < d < p$

Given there are exactly $p-1$ positive integers $\leq$ and relatively prime to p, d is not relatively prime to p.

$\phi(p) < p-1$, a contradiction.

$\therefore p$ is a prime.

16) Find self invertible least residue modulo 7.

Let x be self invertible mod 7.

$$x\,x \equiv 1 \pmod 7$$

$$x^2 \equiv 1 \pmod 7$$

$$x^2 - 1 \equiv 0 \pmod 7$$

$$7 \mid x^2 - 1 \Rightarrow 7 \mid (x-1)(x+1)$$

$$7 \mid x-1 \quad \text{or} \quad 7 \mid x+1$$

$$x - 1 \equiv 0 \quad \text{or} \quad x + 1 \equiv 0 \pmod 7$$

$$x \equiv 1 \text{ or } -1 \pmod 7$$

$$x \equiv 1 \text{ or } 6 \pmod 7 \text{ , since } -1 \equiv 6 \pmod 7$$

So, the self invertible numbers are $1, 6 \pmod 7$

17) If P is odd prime and $(a, P) = 1$, show that $a^{\frac{1}{2}(P-1)} \pm 1$ is divisible by P.

Gn: P is an odd prime $(P \neq 2)$ and $P \mid a$

$\therefore$ By Fermats Theorem $a^{P-1} \equiv 1 \pmod P$

$$a^{P-1} - 1 \equiv 0 \pmod P$$

Since p is odd, $P-1$ is even

$\frac{P-1}{2}$ is an Integer

$$\therefore a^{P-1} - 1 = a^{\left(\frac{P-1}{2}\right)^2} - 1$$

$$= \left(a^{\frac{P-1}{2}} - 1\right)\left(a^{\frac{P-1}{2}} + 1\right)$$

since $P \mid a^{P-1} - 1$, we get $P \mid a^{\frac{P-1}{2}} - 1$ or $a^{\frac{P-1}{2}} + 1$

$$\Rightarrow a^{\frac{1}{2}(P-1)} \pm 1 \text{ is divisible by } P.$$

16) Prove that $\phi(n)$ is even if $n \geq 3$.

$\phi(n)$ is the number of numbers $\leq n$ and relatively prime to n.

Let a be an integer less than n and relatively prime to n.

Then $n - a < n$ and $n - a$ is prime to n.

Hence all the numbers $< n$ can be grouped into pairs as $a, n-a$ whose sum is n.

Hence $\phi(n)$ is even.

19) Show that $n^2 + n \equiv 0 \pmod 2$ for any positive integer n.

For any integer n, $n^2 + n = n(n+1)$ is a product of two consecutive integers and hence it is even.

$\therefore n(n+1)$ is divisible by 2.

20) Find the Incongruent solution of $12x \equiv 8 \pmod{14}$

$12x \equiv 8 \pmod{14}$

$a = 12 \quad b = 8 \quad m = 14$

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

$d = 2$ and $d \mid b$

So, the equation has 2 incongruent solutions

$12 \cdot 3 = 36 \equiv 8 \pmod{14}$, $x_0 = 3$

So, the incongruent solutions are

$x = x_0 + \frac{14}{2} t$, $0 \leq t < 2$

$= 3 + 7t$, $t = 0$ or 1

$x = 3, \; 3 + 7 = 10$

3, 10 are the two incongruent solutions (mod 14).

P. Bamade

prepared by

Sub Expert Signature

verified by

Approved by