UNIT - V

CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

Wilson's Theorem:

Definition:

When p is a prime we know that,

$$Z_p^* = \{[1], [2], \ldots, [p-1]\}$$

is a group under Multiplication Modulo p.
Hereafter we write $1, 2, \ldots, p-1$ instead of $[1][2], \ldots, [p-1]$.
Note that only 1 and $p-1$ are self invertible.
i.e., $1.1 \equiv 1 \pmod p$ and $(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \pmod p$.

Lemma:

A positive integer 'a' is self - invertible iff $a \equiv 1 \pmod p$.

Proof: Assume that 'a' is self-invertible.

Then $a \cdot a \equiv 1 \pmod p$

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

$\Rightarrow (a+1)(a-1) \equiv 0 \pmod p$

$\Rightarrow p \mid (a+1)(a-1) \Rightarrow p \mid (a+1)$ (or) $p \mid (a-1)$. Since p is a prime.

$\Rightarrow a \equiv -1 \pmod p$ (or) $a \equiv 1 \pmod p$

$\Rightarrow a \equiv \pm 1 \pmod p$

Conversely, assume that $a \equiv \pm 1 \pmod p$

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

if $p \mid (a+1)$, then $p \mid (a+1)(a-1) \Rightarrow p \mid (a^2 - 1)$

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

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

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

$\Rightarrow a$ is self-invertible.

Example:

Let $p=11$, Then $(p-1)! = 10! = 1.2.3....9.10$, 1 and 10 are only self-invertible.

Solution:

Given $p=11$ and $(p-1)! = 10! = 1.2.3.....9.10.$

Since $1^2 = 1 \equiv 1 \pmod{11}$ and $10^2 = 100 \equiv 1 \pmod{11}$.

Remaining integers are $2, 3, ..., 9$ and they are $8 = (p-3)$ numbers.

2 and 6 are inverse of one another since $2 \times 6 = 12 \equiv 1 \pmod{11}$

3 and 4 are inverse of one another

5 and 9 are inverse of one another

7 and 8 are inverse of one another.

There are $4 = \frac{p-3}{2}$ pairs such that in each pair one is the inverse of the other.

$$10! = 1.2.3.4.5.6.7.8.9.10.$$
$$= 1.(2.6)(3.4)(5.9)(7.8).10.$$
$$\equiv 1.1.1.1.1.10 \equiv -1 \pmod{11}$$

$\Rightarrow 10! \equiv -1 \pmod{11}$

$\Rightarrow (p-1)! \equiv -1 \pmod{p} \Rightarrow [(p-1)!+1]$ is divisible by p.

Wilson Theorem:

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

Proof: when $p = 2$, $(p-1)! = 1 \equiv -1 \pmod p$.

so, assume that $p > 2$.

we know that the least positive residues $1, 2, 3, \ldots, (p-1)$ are all invertible modulo p. 1 and $(p-1)$ are self-invertible, since $1^2 = 1 \equiv 1 \pmod p$ and $(p-1)^2 = p^2 - 2p + 1 \equiv 1 \pmod p$.

Now, consider the remaining $(p-3)$ residues $2, 3, \ldots (p-2)$. Group these $(p-3)$ residues into $\frac{p-3}{2}$ pairs such that in each pair (a, b) one is the inverse of the other.

ie, $ab \equiv 1 \pmod p$. Hence $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \pmod p$ $\rightarrow$ (1)

Hence,
$$(p-1)! = 1 \cdot [2 \cdot 3 \cdot 4 \cdots (p-2)](p-1)$$
$$\equiv 1 \cdot 1 \cdot (p-1) \pmod p \quad (\text{by } (1))$$
$$\equiv (p-1) \pmod p$$
$$(p-1)! \equiv -1 \pmod p.$$

Converse of Wilson's Theorem:

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

proof: Assume the contrary that n is composite. Then there exist integers a, b such that $1 < a, b < n$ and $n = ab$

$n = ab \Rightarrow a | n$ and by hypothesis $n | [(n-1)! + 1]$

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

$1 < a < n$ and n is an integer.

$\Rightarrow$ a is one of the integers $2, 3, \ldots, (n-1)$

$\Rightarrow a \mid [2 \cdot 3 \cdot 4 \cdot \ldots (n-1)]$

$\Rightarrow a \mid (n-1)!$ $\rightarrow$ ②

From ① and ②, $a \mid \{[(n-1)!+1] - (n-1)!\}$

$\Rightarrow a \mid 1$, a contradiction, since $a > 1$

$\therefore$ n is not composite, i.e., n is prime.

An application of wilson's Theorem:

Let p be any prime an 'n' any positive integer. Then prove that $\dfrac{(np)!}{n!\,p^n} \equiv (-1) \pmod{p}$.

Proof:

Let $n!\,p^n = (1 \cdot 2 \cdot 3 \cdot \ldots n)\, p^n$

$= (p)(2p)(3p) \ldots np.$

$$\frac{(np)!}{n!\,p^n} = \frac{(np)!}{p \cdot 2p \cdot 3p \ldots np}$$

$$= \prod_{r=1}^{n} [(r-1)p+1] \ldots [(r-1)p+(p-1)]$$

$$= \prod_{r=1}^{n} (p-1)! \pmod{p}$$

$$= \prod_{r=1}^{n} (-1) \pmod{p}$$

$$\equiv (-1)^n \pmod{p}.$$

Example:

Let $p = 7$ and $a = 12$. Then $p \nmid a$.

Solution:

Given: $p = 7$ and $a = 12$

$1.a = 1.12 \equiv 5 \pmod p$

$2.a = 2.12 \equiv 3 \pmod p$

$3.a = 3.12 \equiv 1 \pmod p$

$4.a = 4.12 \equiv 6 \pmod p$

$5.a = 5.12 \equiv 4 \pmod p$

$6.a = 6.12 \equiv 2 \pmod p$.

Thus the least residues of $1.a, 2.a, 3.a, 4.a, 5.a, 6.a$ are the same as the integers $1, 2, 3, 4, 5$ and 6 in some order.

Lemma:

Let $p \nmid a$. Then the remainders when $1.a, 2.a, 3.a \ldots, (p-1)a$ are divided by p are the integers $1, 2, 3, \ldots, (p-1)$ in some order.

Proof:

First we prove that, for any i with $1 \le i \le p-1$, ia does not leave remainder 0 when divided by p.

Suppose $ia \equiv 0 \pmod p$, for some i with $1 \le i \le p-1$.

Then $p | ia$ with $p \nmid a$.

Hence, $p | i$, since p is a prime.

This is impossible, since $i < p$.

$\therefore$ $ia \not\equiv 0 \pmod p$ for any i with $1 \le i \le p-1$.

Next, we prove that $ia \equiv ja \pmod{p}$, where $1 \le i, j \le p-1$ $\Rightarrow i = j$

Suppose $ia \equiv ja \pmod{p}$, where $1 \le i, j \le p-1$.

Since $(p, a) = 1$, by a known theorem $i \equiv j \pmod{p}$

Both i and j are least residues Modulo p.

$\therefore \quad i = j$.

Hence, when $1.a, 2.a, 3.a, \ldots, (p-1)a$ are divided by p, we get the remainders $1, 2, 3, \ldots, (p-1)$ in some order.

Fermat's Little Theorem (or) Fermat's Theorem:

Let p be a prime and 'a' any integer such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: By the above lemma, $1.a, 2.a, 3.a, \ldots, (p-1)a$ when divided by p leave the remainder $1, 2, 3, \ldots p-1$ in some order.

Hence, $(1.a)(2.a)(3.a)\ldots[(p-1)a] \equiv [1.2.3.\ldots p-1] \pmod{p}$

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

$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$, since $((p-1)!, p) = 1$.

Problems:

1. Find the remainder when 24^{1947} is divided by 17.

Solution:

Given: 24^{1947} is divided by 17.

$$24 \equiv 7 \pmod{17}$$

$$\Rightarrow 24^{1947} \equiv 7^{1947} \pmod{17} \rightarrow (1)$$

Take $p = 17$ and $a = 7$. Then $p \nmid a$.

$\therefore$ By Fermat's Theorem,

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

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

$$\begin{array}{r|l} & 121 \\ \hline 16 & 1947 \\ & 16 \\ \hline & 34 \\ & 32 \\ \hline & 27 \\ & 16 \\ \hline & 11 \end{array}$$

$$\therefore \quad 7^{1947} = 7^{16 \times 121 + 11}$$

$$= (7^{16})^{121} \cdot 7^{11}$$

$$\equiv 1^{121} \cdot 7^{11} \pmod{17}$$

$$\equiv 7^{11} \pmod{17} \rightarrow (2)$$

$$7^2 \equiv -2 \pmod{17} \Rightarrow 7^{11} = (7^2)^5 \cdot 7 \equiv (-2)^5 \, 7 \pmod{17}.$$

$$\Rightarrow 7^{11} \equiv -32 \times 7 \pmod{17}$$

$$\equiv 2 \times 7 \pmod{17}$$

$$\equiv 14 \pmod{17} \rightarrow (3)$$

using (3) in (2), $7^{1947} \equiv 14 \pmod{17}$

using (4) in (1), $24^{1947} \equiv 14 \pmod{17}$

Hence the remainder is 14.

Theorem:

Let p be a prime and 'a' any integer such that $p \nmid a$. Then a^{p-2} is an inverse of a modulo p.

proof: By Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$

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

$\Rightarrow a^{p-2}$ is an inverse of a modulo 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 $x \equiv a^{p-2} b \pmod{p}$.

proof: Since $p \nmid a$, by a known theorem $ax \equiv b \pmod{p}$ has a unique solution.

By the above theorem a^{p-2} is an inverse of a modulo p.

$\therefore \quad ax \equiv b \pmod{p} \Rightarrow a^{p-2} ax \equiv a^{p-2} b \pmod{p}$

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

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

Example:

Solve the linear congruence $12x \equiv 6 \pmod{7}$.

Solution:

Here $p = 7$, $a = 12$ and $b = 6$

$\therefore$ p is prime and $p \nmid a$.

Hence by the above theorem,

The required Solution is,

$$x \equiv a^{p-2} \pmod p$$
$$\equiv 12^{7-2}\, 6 \pmod 7$$
$$\equiv 5^5 \cdot 6 \pmod 7$$
$$\equiv 25 \cdot 25 \cdot 5 \cdot 6 \pmod 7$$
$$\equiv 4 \cdot 4 \cdot 5 \cdot 6 \pmod 7$$
$$\equiv 16 \cdot 30 \pmod 7$$
$$\equiv 2 \cdot 2 \pmod 7$$
$$x \equiv 4 \pmod 7$$

Euler's phi-function:

Let 'm' be a positive integer. Then the Euler's function $\phi(m)$ is defined as the number of positive integers $\leq m$ and relatively prime to m.

Ex: Let $m=5$. Then the positive integers ≤ 5 and relatively prime to 5 are 1, 5, 7, 11.

$$\Rightarrow \phi(12) = 4.$$

Lemma:

A positive integer p is a prime iff $\phi(p) = p-1$.

Proof: Assume that p is a prime.

Then there are $p-1$ integers, namely $1, 2, 3, \ldots, p-1$. which are $\leq p$ and relatively prime to p.

$\therefore \phi(p) = p-1$.

Conversely, assume that $\phi(p) = p-1$, for a positive integer p.

Let $1 < d < p$ and $d | p$. (i.e., let p be not a prime)

Then $d < p$ and $(d, p) \neq 1$.

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

$\therefore$ p is a prime.

Example:

Solve the congruence relation $24x \equiv 11 \pmod{17}$.

Solution:

Given: $24x \equiv 11 \pmod{17}$

Here $p = 17$, $a = 24$ and $b = 11$

$\therefore$ p is prime and $p \nmid a$.

Hence the solution is given by,

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

$\equiv 24^{15} \cdot 11 \pmod{17}$

$\equiv 7^{15} \cdot 11 \pmod{17}$

$\equiv 7^{14}\ 77 \pmod{17}$

$\equiv 8 \cdot 9 \pmod{17}$

$\equiv 4 \pmod{17}$.

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

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

$\Rightarrow 7^8 \equiv 16 \pmod{17}$

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

$7^6 \equiv -8 \pmod{17}$

$\Rightarrow 7^{14} \equiv 8 \pmod{17}$]

Euler's Theorem:

Fermat's theorem states that when p is a prime and 'a' is any integer such that $p \nmid a$.

$$a^{p-1} \equiv 1 \ (\text{mod } p) \Rightarrow a^{f(p)} \equiv 1 \ (\text{mod } p).$$

where $f(p) = p-1$.

Lemma:

Let m be a positive integer and 'a' any integer with $(a,m) = 1$. Let $r_1, r_2, \ldots, r_{\phi(m)}$ be the positive integers $\leq m$ and relatively prime to m. Then the least residues of the integers $ar_1, ar_2, \ldots, ar_{\phi(m)}$ modulo m are the integers $r_1, r_2, \ldots, r_{\phi(m)}$ in some order.

Proof: First we prove that each ar_i is relatively prime m.

i.e., $(ar_i, m) = 1$ for every $i = 1, 2, \ldots, \phi(m)$.

To prove this assume the contrary that, for some i,

$(ar_i, m) > 1$. Let p be a prime factor of ar_i and m.

Then $p \mid ar_i$ and $p \mid m$.

$p \mid ar_i$ and p is prime $\Rightarrow p \mid a$ or $p \mid r_i$.

Let $p \mid r_i$. Then $p \mid m \Rightarrow (r_i, m) \geq p > 1$, a contradiction.

Let $p \mid a$. Then $p \mid m \Rightarrow (a,m) \geq p > 1$. a contradiction.

Hence $(ar_i, m) = 1$ for every $i = 1, 2, \ldots, \phi(m)$.

Next we prove that $ar_i \not\equiv ar_j$ for any two i, j such that $1 \leq i < j \leq \phi(m)$.

To prove this assume the contrary that

$$ar_i \equiv ar_j \pmod m \rightarrow (1)$$

for some i, j with $1 \le i < j \le \phi(m)$.

Since $(a, m) = 1$ $((1)) \Rightarrow r_i \equiv r_j \pmod m$.

But r_i and r_j are least residues mod m.

$\therefore$ $r_i = r_j$, a contradiction.

Hence $ar_i \not\equiv ar_j \pmod m$.

Thus the least residues of $ar_1, ar_2, \ldots, ar_{\phi(m)}$ modulo m are distinct and are $\phi(m)$ in number.

So they are $r_1, r_2, \ldots, r_{\phi(m)}$ in some order.

Euler's Theorem:

Let m be a positive integer and 'a' any integer with $(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod m$.

Proof: Let $r_1, r_2, \ldots r_{\phi(m)}$ be integers $\le m$ and relatively prime to m. Then by the above lemma $ar_1, ar_2, \ldots, ar_{\phi(m)}$ are integers congruent modulo m to $r_1, r_2, \ldots, r_{\phi(m)}$ in some order.

$$\therefore \quad ar_1 ar_2 \ldots ar_{\phi(m)} \equiv r_1 r_2 \ldots r_{\phi(m)} \pmod m$$

$$\Rightarrow a^{\phi(m)} (r_1 r_2 \ldots r_{\phi(m)}) \equiv (r_1 r_2 \ldots r_{\phi(m)}) \pmod m$$

$$\Rightarrow a^{\phi(m)} \equiv 1 \pmod m, \text{ since } (r_1 r_2 \ldots r_{\phi(m)}, m) = 1.$$

Note: Let $ab \equiv ac \pmod m$ and $(a, m) = 1$. Then $ab - ac$ is divisible by m. $\Rightarrow m \mid (b - c) \Rightarrow b \equiv c \pmod m$.

Fermat's Little Theorem:

Let p be a prime number and 'a' any integer such that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

proof:

Given: p is prime and $p \nmid a \Rightarrow (p, a) = 1$

Further p is prime $\Rightarrow \phi(p) = p-1$. (by the above lemma)

$\therefore$ By Euler's theorem, $a^{\phi(p)} \equiv 1 \pmod{p}$

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

Example:

Find the remainder when 245^{1040} is divisible by 18.

Solution:

Given: 245^{1040} is divisible by 18.

$$245 \equiv 11 \pmod{18}$$

$$\Rightarrow 245^{1040} \equiv 11^{1040} \pmod{18} \longrightarrow (1)$$

Take $m = 18$ and $a = 11$. Then $(m, a) = 1$ and $\phi(m) = 6$.

(since: 1, 5, 7, 11, 13, 17 are ≤ 18 are relatively prime to 18).

$\therefore$ By Euler's theorem,

$$11^{\phi(m)} \equiv 1 \pmod{18}$$

$$\Rightarrow 11^6 \equiv 1 \pmod{18}$$

$$\Rightarrow 11^{1040} = (11^6)^{173} (11^2)$$

$$\equiv 1 \cdot 121 \pmod{18}$$

$$\equiv 13 \pmod{18} \longrightarrow (2)$$

using (2) in (1) $(245)^{1040} \equiv 13 \pmod{18}$. $\therefore$ The remainder is 13.

Multiplicative functions:

A number – theoretic function f is multiplicative if $f(mn) = f(m) f(n)$ whenever $(m, n) = 1$.

Example: The constant function $f(n) = 1$ and when k is an integer, function $g(n) = n^k$ are Multiplicative.

proof: Let $(m, n) = 1$. Then $f(mn) = 1 = 1.1 = f(m) f(n)$

$\Rightarrow f$ is multiplicative.

Also, $g(mn) = (mn)^k = m^k n^k = g(m) g(n)$

$\Rightarrow g$ is multiplicative.

Fundamental Theorem for multiplicative functions:

Let f be a Multiplicative function and n a positive integer with Canonical decomposition

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

Then $f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \ldots f(p_k^{e_k})$.

proof: By induction on the number of primes in n.

If $k=1$, then $f(n) = f(p_1^{e_1})$. So the theorem is trivially true. Assume that the theorem is true when an integer contains k prime numbers in its Canonical decomposition.

i.e., if $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ then

$$f(n) = f(p_1^{e_1}) f(p_2^{e_2}) \ldots f(p_k^{e_k}) \longrightarrow (1)$$

Let n be an integer containing $(k+1)$ primes in its canonical decomposition. That is, let $n = p_1^{e_1} p_2^{e_2} \dots p_{k+1}^{e_{k+1}}$

Then $f(n) = f([p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}] \cdot p_{k+1}^{e_{k+1}})$

$= f(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}) f(p_{k+1}^{e_{k+1}})$

since f is multiplicative and $(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}, p_{k+1}^{e_{k+1}}) = 1$

$\Rightarrow = f(p_1^{e_1}) f(p_2^{e_2}) \dots f(p_k^{e_k}) f(p_{k+1}^{e_{k+1}})$ by (1)

Thus the result is true when an integer contains $k+1$ primes in its canonical decomposition.

$\therefore$ by induction the result is true for any positive integer.

Theorem:-

Let p be a prime and e be any positive integer. Then $\phi(p^e) = p^e - p^{e-1}$.

Proof: By the definition of ϕ.

$\phi(p^e)$ = The number of integers $\le p^e$ and relatively prime to p^e

= The number of integers $\le p^e$ − {The number of integers $\le p^e$ and not relatively prime to p^e}

= p^e − the number of elements in the set $\{p, 2p, 3p, \dots p^e\}$

= p^e − the number of elements in the set $\{p, 2p, 3p \dots p^{e-1}, p\}$

$= [p^e - p^{e-1}]$.

Example: 1

Compute $\phi(8)$, $\phi(81)$ and $\phi(15625)$

Solution: $\phi(8) = \phi(2^3) = 2^3 - 2^{3-1}$, since $p=2$, $e=3$

$$= 8 - 4 = 4$$

$$\phi(81) = \phi(3^4) = 3^4 - 3^{4-1} = 81 - 27 = 54$$

$$\phi(15625) = \phi(5^6) = 5^6 - 5^5 = 15625 - 3125 = 12500.$$

Theorem:

The function ϕ is multiplicative.

Proof:

Let m, n be positive integers such that $(m,n)=1$.

Claim: (1) The integers in $S = \{s, m+s, 2m+s, \ldots, (n-1)m+s\}$ are congruent modulo n to $0, 1, 2, \ldots, n-1$ in some order for any integer s.

To prove this claim first note that any integer leaves one of the remainders $0, 1, 2, \ldots, n-1$.

When the integer is divided by n; and assume that integers $km+s$ and $lm+s$ in S leave the same remainder for $k \neq l$.

Then $km+s \equiv lm+s \pmod{n}$

$\Rightarrow km \equiv lm \pmod{n} \rightarrow (1)$

$\Rightarrow k \equiv l \pmod{n}$

Since $(m,n)=1$. As k and l are least remainders it follows that $k=l$, a contradiction

Therefore, no two integers in S leave the same remainder.
Since S contains n integers, integers in S are congruent Modulo n to $0, 1, 2, \ldots, n-1$ in some order. This proves claim ①.

Now arrange the integers from 1 to mn in m rows and n columns as follows:

$$\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots\cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots\cdots & (n-1)m+2 \\
\vdots & \vdots & \vdots & & \vdots \\
r & m+r & 2m+r & \cdots\cdots & (n-1)m+r \\
\vdots & \vdots & \vdots & & \vdots \\
s & m+s & 2m+s & \cdots\cdots & (n-1)m+s \\
\vdots & \vdots & \vdots & & \vdots \\
m & m+m & 2m+m & \cdots\cdots & (n-1)m+m = nm
\end{array}$$

Claim : (2)

If r and m are not relatively prime then no integer in the r^{th} row is relatively prime to m.

To prove this claim let $d = (r, m) > 1$. Then d/r and d/m
Then for any integer q, $d|(qm+r)$.

$\Rightarrow$ d is a factor of every integer in the r^{th} row with $d > 1$.

$\Rightarrow$ no integer in the r^{th} row is relatively prime to m. and hence to mn.

This proves claim ②.

Scanned by CamScanner

Therefore, positive integers $\le mn$ and relatively prime to mn must come from the remaining $\phi(m)$ rows.

Let s^{th} row be one such row, where $(s, m) = 1$.

$(s, m) = 1 \Rightarrow as + bm = 1$, for some integers a, b

$\Rightarrow a(km+s) + (b-ak)m = 1$

$\Rightarrow (km+s, m) = 1$ for $0 \le k \le n-1$

$\Rightarrow$ every integer in the s^{th} row is relatively prime to m $\rightarrow$ ②

By claim ①, the integers in the s^{th} row are congruent modulo n to $0, 1, 2, \ldots, n-1$ in some order.

Exactly $\phi(n)$ integers among $0, 1, 2, \ldots, n-1$ are relatively prime to n. Hence exactly $\phi(n)$ integers in the s^{th} row are relatively prime to n.

(since: Let $(k, n) = 1$ and let $lm + s \in S$ such that $lm + s \equiv k \pmod n$.

Then $(k, n) = 1 \Leftrightarrow (lm+s, k) = 1$

Therefore, by ② there are exactly $\phi(n)$ integers in the s^{th} row that are $\le mn$ and relatively prime to mn.

Since there are $\phi(m)$ such rows, the number of integers $\le mn$ and relatively prime to mn is $= \phi(m)\phi(n)$.

$\Rightarrow \phi(mn) = \phi(m)\phi(n)$ with $(m, n) = 1$

$\Rightarrow \phi$ is multiplicative.

Example:

Verify $\phi(3.4) = \phi(3)\,\phi(4)$

Solution:

Let $m=3$ and $n=4$. Then $(m,n)=1$.

Arrange the $mn=12$ integers 1 to 12 in $m=3$ rows and $n=4$ columns as follows:

1	4	7	10
2	5	8	11
3	6	9	12

only the first integer in the third row is not relatively prime to $m=3$.

Further, no integer in third row is relatively prime to $m=3$ and $mn=12$.

consequently, the positive integers ≤ 12 and relatively prime to 12 must come from the remaining $\phi(3)=2$ rows

1	4	7	10
2	5	8	11

Note that each integer in these 2 rows is relatively prime to $m=3$.

each of these 2 rows contains $\phi(4)=2$ integers relatively prime to $n=4$.

1	7
5	11

Hence, only these 4 integers are ≤ 12 and relatively prime to $mn=12$.

ie, $\phi(mn) = \phi(12) = 4 = 2\times 2 = \phi(3)\phi(4) = \phi(m)\,\phi(n)$.

Theorem:

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the Canonical decomposition of a positive integer n. Then

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

Proof: Since ϕ is multiplicative,

$$\phi(n) = \phi(p_1^{e_1})\,\phi(p_2^{e_2})\cdots\phi(p_k^{e_k})$$

$$= \left[p_1^{e_1} - p_1^{e_1-1}\right]\left[p_2^{e_2} - p_2^{e_2-1}\right]\cdots\left[p_k^{e_k} - p_k^{e_k-1}\right]$$

$$= p_1^{e_1}\left[1 - p_1^{-1}\right] p_2^{e_2}\left[1-p_2^{-1}\right]\cdots p_k^{e_k}\left[1-p_k^{-1}\right]$$

$$= p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\left(1-\frac{1}{p_k}\right)$$

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

Example:

Compute $\phi(666)$ and $\phi(1976)$.

Solution:

$$666 = 2^1 \cdot 3^2 \cdot 37^1$$

$\Rightarrow p_1 = 2 \quad p_2 = 3 \quad p_3 = 37$

$\Rightarrow e_1 = 1 \quad e_2 = 2 \quad e_3 = 1$

$$\phi(666) = 666\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{3}\right)\left(1-\tfrac{1}{37}\right)$$

$$= 666\left(\tfrac{1}{2}\right)\left(\tfrac{2}{3}\right)\left(\tfrac{36}{37}\right) = 216$$

$$\phi(1976) = 1976\left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{13}\right)\left(1-\tfrac{1}{19}\right)$$

$$= 1976\left(\tfrac{1}{2}\right)\left(\tfrac{12}{13}\right)\left(\tfrac{18}{19}\right) = 48 \times 18$$

$$= 864$$

Tau and Sigma functions

The Tau function:

Let 'n' be a positive integer. Then $\tau(n)$ is defined as the number of positive factors of n.

i.e., $\tau(n) = \sum_{d|n} 1$.

Ex:

1. Let $n = 18$. Then the positive factors of 18 are: 1, 2, 3, 6, 9, 18.
   $\therefore \tau(18) = 6$.
2. Let $n = 23$. Then the positive factors of 23 are: 1, 23.
   $\therefore \tau(23) = 2$.

The Sigma function:

Let n be a positive integer. Then $\sigma(n)$ is defined as the sum of the positive factors of n.

i.e., $\sigma(n) = \sum_{d|n} d$.

Ex:

1. Let $n = 12$. Then the positive factors of 12 are 1, 2, 3, 4, 6, 12
   $\therefore \sigma(12) = 1+2+3+4+6+12$
   $\sigma(12) = 28$
2. Let $n = 17$. Then the positive factors of 17 are 1, 17.
   $\therefore \sigma(17) = 1+17 = 18$.

Multiplicative function:

A function f is multiplicative if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$

Let f be a multiplicative function. Then we define a new function F as $F(n) = \sum_{d|n} f(d)$.

It turns out that F is multiplicative if f is multiplicat

Ex: $F(12) = \sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12)$

Example:

Determine if $F(mn) = F(m)F(n)$, where $m = 4,\ n = 7$

Solution:

$$F(4.7) = F(28) = \sum_{d|28} f(d) = f(1) + f(2) + f(4) + f(7) + f(14) + f(28)$$

$$= f(1.1) + f(1.2) + f(1.4) + f(1.7) + f(2.7) + f(4.7)$$

$$= f(1)f(1) + f(1)f(2) + f(1)f(4) + f(1)f(7) + f(2)f + f(4)f(7).$$

Since f is multiplicative.

$$= [f(1) + f(2) + f(4)]f(1) + [f(1) + f(2) + f(4)]f(7$$

$$= [f(1) + f(2) + f(4)][f(1) + f(7)]$$

$$= \sum_{d|4} f(d) \sum_{d|7} f(d)$$

$$= F(4)\ F(7)$$

$\therefore F(mn) = F(m)F(n)$ if $m = 4$ and $n = 7$.

Theorem:

If f is a multiplicative function, then $F(n) = \sum_{d|n} f(d)$ is also multiplicative.

proof: Let m, n be relatively prime. Then by the definition of F, $F(mn) = \sum_{d|mn} f(d)$. $\rightarrow$ ①

Since $(m,n) = 1$, every division d of mn is the product of positive divisors d_1 of m and d_2 of n uniquely, where $(d_1, d_2) = 1$.

$\therefore$ From ① $\Rightarrow$ $F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 \cdot d_2)$

$$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) \quad \text{since } f \text{ is multiplicative}$$

$$= \sum_{d_2|n} \left\{ \sum_{d_1|m} f(d_1) \right\} f(d_2)$$

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

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

$$= F(m) F(n)$$

$\Rightarrow$ F is multiplicative.

Corolary: The tau and Sigma functions are multiplicative.

Proof: First we prove that the constant function $f(n)=1$ and the identity functions $g(n)=n$ are multiplicative.

To prove these, let $(m,n)=1$.

Then $f(mn)=1$ & $f(m)f(n)=1.1=1 \Rightarrow f(mn)=f(m)f(n)$

$g(mn)=mn=g(m)g(n)$.

$\Rightarrow$ both f and g are multiplicative.

Now, $\tau(n)=\sum_{d|n} 1=\sum_{d|n} f(n)$, where $f(n)=1, \forall n$

$\sigma(n)=\sum_{d|n} d=\sum_{d|n} g(d)$, where $g(d)=d, \forall d$

Since f and g are multiplicative, by the above theorem τ and σ are multiplicative.

Example: Compute $\tau(36)$ and $\sigma(36)$.

Solution:

$\tau(36)=\tau(4.9)$ with $(4,9)=1$

$=\tau(4)\tau(9)$, since τ is multiplicative.

$=3.3$, since $1,2,4$ are the positive factors of 4 and $1,3,9$ are the positive factors of 9.

$\tau(36)=9$

$\sigma(36)=\sigma(4)\sigma(9)$, since $(4,9)=1$ and σ is multiplicative

$=(1+2+4)(1+3+9)$

$=(7)(13)$

$\sigma(36)=91$

Theorem: Let p be any prime and e be any positive integer. Then $\tau(p^e) = e+1$ and $\sigma(p^e) = \dfrac{p^{e+1}-1}{p-1}$.

proof: The positive factors of p^e are $1, p, p^2, \ldots, p^e$.

They are totally $e+1$ in number.

Hence $\tau(p^e) = e+1$.

Further, $\sigma(p^e) = 1 + p + p^2 + \ldots + p^e$.

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

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

Theorem:

Let n be a positive integer with canonical decomposition $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$.

Then $\tau(n) = (e_1+1)(e_2+1)\ldots(e_k+1)$.

$$\sigma(n) = \left(\frac{p_1^{e+1}-1}{p_1-1}\right)\left(\frac{p_2^{e_2+1}-1}{p_2-1}\right)\ldots\left(\frac{p_k^{e_k+1}-1}{p_k-1}\right)$$

Proof: Since $p_1^{e_1}, p_2^{e_2}, \ldots p_k^{e_k}$ are relatively prime and since τ is multiplicative.

$$\tau(n) = \tau(p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k})$$
$$= \tau(p_1^{e_1})\,\tau(p_2^{e_2})\ldots\tau(p_k^{e_k})$$
$$= (e_1+1)(e_2+1)\ldots(e_k+1).$$

llly, $\sigma(n) = \sigma(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k})$

$= \sigma(p_1^{e_1})\, \sigma(p_2^{e_2}) \dots \sigma(p_k^{e_k})$.

$= \dfrac{p_1^{e_1+1}-1}{p_1-1} \cdot \dfrac{p_2^{e_2+1}-1}{p_2-1} \dots \dfrac{p_k^{e_k+1}-1}{p_k-1}$.

Example:

compute $\tau(6120)$ and $\sigma(6120)$.

Solution:

Given: $6120 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 17^1$

$\Rightarrow p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_4 = 17$

$e_1 = 3, \quad e_2 = 2, \quad e_3 = 1, \quad e_4 = 1.$

$\therefore \tau(6120) = (e_1+1)(e_2+1)(e_3+1)(e_4+1)$

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

$= (4)(3)(2)(2)$

$\tau(6120) = 48$

$\sigma(6120) = \dfrac{p_1^{e_1+1}-1}{p_1-1} \cdot \dfrac{p_2^{e_2+1}-1}{p_2-1} \cdot \dfrac{p_3^{e_3+1}-1}{p_3-1} \cdot \dfrac{p_4^{e_4+1}-1}{p_4-1}$

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

$= \dfrac{15}{1} \cdot \dfrac{26}{2} \cdot \dfrac{24}{4} \cdot \dfrac{288}{16}$

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

$\sigma(6120) = 21{,}060$.

*** END ***