UNIT-V.

CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

5.1 WILSON'S THEOREM

LEMMA 1.

A positive integer a is self-invertible modulo p if and only if $a \equiv \pm 1 \pmod{p}$.

Proof : Given : a is self-invertible modulo p

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

i.e., $p \mid (a^2 - 1)$

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

$$\Rightarrow \quad p \mid a-1 \text{ (or) } p \mid a+1$$

Hence either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$

Converse part :

Given : $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$

In either case, $a^2 \equiv 1 \pmod{p}$

$\Rightarrow$ a is self-invertible modulo p.

Theorem 1.

(Wilson's theorem) If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof : Given : p is a prime.

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

Proof : For $p = 2$,

(1) $\Rightarrow$ $(2-1)! \equiv -1 \pmod 2$ $\Rightarrow 1! \equiv -1 \pmod 2$

$\Rightarrow$ $1 \equiv -1 \pmod 2$

$\therefore$ the theorem is true for $p = 2$

So, let $p > 2$,

$\therefore$ the least positive residues 1 through $p-1$ are invertible modulo p.

But two of them, 1 and $p-1$, are their own inverses by lemma 1.

So we can group the remaining $p-3$ residues, 2 through $p-2$, into $(p-3)/2$ pairs of inverses a and $b = a^{-1}$ such that

$ab \equiv 1 \pmod p$ for every pair a and b

Hence, $2.3 \ldots (p-2) \equiv 1 \pmod p$

$$(p-1)! = 1.[2.3 \ldots (p-2)].(p-1)$$

$$= 1.1.(p-1) \pmod p$$

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

Theorem 2.

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

Proof : We prove this by contradiction method

Let n is composite, say $n = ab$, where $1 < a, b < n$.

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

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

Since $1 < a < n$, a is one of the integers 2 through $n-1$, so $a \mid (n-1)!$.

Therefore, $a \mid [(n-1)! + 1 - (n-1)!]$ i.e., $a \mid 1$.

So $a = 1$, a contradiction.

Hence, n must be a prime.

Theorem 3.

If p be a prime and n any positive integer, then

$$\frac{(np)!}{n!\,p^n} \equiv (-1)^n \pmod{p}$$

Solution :

Let a be any positive integer congruent to 1 modulo p. Then, by Wilson's theorem,

$$a(a+1)\ldots[a+(p-2)] \equiv (p-1)! \equiv -1 \pmod{p}.$$

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

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

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

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

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

Example 5.1.1

Find the self-invertible least residues module each prime p

(a) 7 (b) 23

Solution :

(a) Given $p = 7$

Then $(p-1)! = 6! = 1.2.3.4.5.6$

The least residues modulo 7 that are self-invertible are 1 and 6.

(b) Given $p = 23$

Then $(p - 1) = 22!$

The least residues modulo 23 that are self-invertible are 1 and 22.

Example 5.1.2

Solve the congruence $x^2 \equiv 1 \pmod{m}$ for each modulo m.

(a) 6 (b) 8

Solution :

(a) Given : $m = 6$

$$\therefore x^2 = 1 \pmod 6$$

$x = 1 \Rightarrow 1^2 = 1 \pmod 6$

$x = 2 \Rightarrow 4 \neq 1 \pmod 6$

$x = 3 \Rightarrow 9 \neq 1 \pmod 6$

$x = 4 \Rightarrow 16 \neq 1 \pmod 6$

$x = 5 \Rightarrow 25 = 1 \pmod 6$

$\therefore x = 1, 5$

(b) Give : $m = 8$

$$\therefore x^2 = 1 \pmod 8$$

$x = 1 \Rightarrow 1 = 1 \pmod 8$

$x = 2 \Rightarrow 4 \neq 1 \pmod 8$

$x = 3 \Rightarrow 9 = 1 \pmod 8$

$x = 4 \Rightarrow 16 \neq 1 \pmod 8$

$x = 5 \Rightarrow 25 = 1 \pmod 8$

$x = 6 \Rightarrow 36 \neq 1 \pmod 8$

$x = 7 \Rightarrow 49 = 1 \pmod 8$

$\therefore x = 1, 3, 5, 7$

Example 5.1.3

Prove or disprove : If the congruence $x^2 \equiv 1 \pmod{m}$ has exactly two solutions, then m is a prime.

Solution :

The congruence $x^2 \equiv 1 \pmod{6}$ has exactly two solutions, but $m = 6$ is not a prime.

Hence, the given statement is not true.

Example 5.1.4

If $x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$, does it follow that $x^2 \equiv 1 \pmod{pq}$, where p and q are distinct primes?

Solution :

Yes. Since $x^2 \equiv 1 \pmod{p}$ and $x^2 \equiv 1 \pmod{q}$,

$x^2 \equiv 1 \pmod{[p, q]}$ i.e., $x^2 \equiv 1 \pmod{pq}$

Example 5.1.5

Let a be a solution of the congruence $x^2 \equiv 1 \pmod{m}$. Show that $m - a$ is also a solution.

Solution :

Let $a^2 \equiv 1 \pmod{m}$

$$(m - a)^2 = m^2 - 2am + a^2 \equiv 1 \pmod{m}$$

So $m - a$ is also a solution.

Example 5.1.6

Without using Wilson's theorem, verify that $(p-1)! \equiv -1 \pmod{p}$ for each p.

(a) 5 (b) 7

Solution :

(a) Here $p = 5$

$$(p-1)! = (5-1)! = 4! = 24 \equiv -1 \pmod{5}$$

Hence, verified.

(b) Here $p = 7$

$$(p-1)! = (7-1)! = 6! = 720 \equiv -1 \pmod{7}$$

Hence, verified.

Example 5.1.7

If p is a prime and p be odd, then $2(p-3)! \equiv -1 \pmod{p}$

Solution :

By Wilson's theorem, $(p-1)! \equiv -1 \pmod{p}$

i.e., $(p-3)!(p-2)(p-1) \equiv (p-3)!(-2)(-1)$

$$\equiv 2(p-3)! \equiv -1 \pmod{p}$$

Example 5.1.8

Prove that $(p-1)(p-2)\ldots(p-k) \equiv (-1)^k k! \pmod{p}$, where $1 \leq k < p$

Solution :

$$(p-1)(p-2)\ldots(p-k) \equiv (-1)(-2)\ldots(-k) \equiv (-1)^k k! \pmod{p}$$

$[\because p-1 \equiv -1 \pmod{p}, p-2 \equiv -2 \pmod{p} \ldots (p-k) \equiv -k \pmod{p}]$

Example 5.1.9

Let p be odd. Then $1^2 . 3^2 \ldots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$

Solution :

We know that $i \equiv -(p-i) \pmod{p}$ ... (1)

$\therefore 1^2 . 3^2 \ldots (p-2)^2 \equiv [1 . 3 \ldots (p-2)] [1 . 3 \ldots (p-2)] \pmod{p}$

$\equiv [1.3 \ldots (p-2)] [[-(p-1)] [-(p-3) \ldots [-(p-(p-2))]] \pmod{p}$ by (1)

$\equiv [1 . 3 \ldots (p-2)] [(p-1)(p-3) \ldots 2)] (-1)^{(p-1)/2} \pmod{p}$

$\equiv (p-1)! (-1)^{(p-1)/2} \pmod{p}$

$\equiv (-1)(-1)^{(p-2)/2} \pmod{p}$, by Wilson's theorem.

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

Example 5.1.10

A positive integer $n \geq 2$ is a prime if and only if $(n-2)! \equiv 1 \pmod{n}$

Solution :

Let $n \geq 2$ be a prime.

Then, by Wilson's theorem, $(n-1)! \equiv -1 \pmod{n}$;

i.e., $(n-2)!(n-1) \equiv (-1)(n-2)! \equiv -1 \pmod{n}$,

so $(n-2)! \equiv 1 \pmod{n}$

Conversely, let $(n-2)! \equiv 1 \pmod{n}$.

Then $(n-1)! = (n-2)!(n-1) \equiv 1 . (-1) \equiv -1 \pmod{n}$, so by the converse of Wilson's theorem, n is a prime.

Example 5.1.11

Let r be a positive integer $< p$ such that $r! \equiv (-1)^r \pmod p$. Then $(p-r-1)! \equiv -1 \pmod p$

Solution :

By Wilson's theorem,

$$-1 \equiv (p-1)! = (p-r-1)!\,[(p-r)\ldots(p-1)!\,(-1)^r]$$
$$\equiv (p-r-1)!\,(-1)^r\, r! \equiv (p-r-1)!\,(-1)^r \equiv (p-r-1)! \pmod p.$$

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

Example 5.1.12

$$\frac{1.3.5\ldots(p-2)}{2.4.6\ldots(p-1)} \equiv (-1)^{(p-1)/2} \pmod p, \text{ where } p > 2$$

Solution :

$$\frac{1.3.5\ldots(p-2)}{2.4.6\ldots(p-1)} = \frac{[1.3.5\ldots(p-2)]\,[1.3.5\ldots(p-2)]}{[2.4.6\ldots(p-1)]\,[1.3.5\ldots(p-2)]}$$

$$= \frac{1^2.3^2.5^2\ldots(p-2)^2}{(p-1)!} \quad \ldots (1)$$

$$\text{Nr} = [1.3.5\ldots(p-2)]\,[1.3.5\ldots(p-2)] \pmod p$$

$$= [1.3.5\ldots(p-2)]\,\big[[-(p-1)]\big]\,[-(p-3)]\ldots[-(p-(p-2)] \pmod p$$

$$\because\ i \equiv -(p-i) \pmod p$$

$$= [1.3.5\ldots(p-2)]\,[(p-1)(p-3)\ldots 2]\,(-1)^{(p-1)/2} \pmod p$$

$$= (p-1)!\,(-1)^{(p-1)/2} \pmod p$$

$$\therefore (1) \Rightarrow \quad = \frac{(-1)^{(p-1)/2}(p-1)! \pmod p}{(p-1)!}$$

$$= (-1)^{(p-1)/2} \pmod p$$

Example 5.1.13

Prove that $\prod_{n=1}^{p-1}(1+p/n) \equiv 1 \pmod{p}$

Solution :

Let $N = \prod_{n=1}^{p-1}(1+p/n) = \left(1+\frac{p}{1}\right)\left(1+\frac{p}{2}\right)\left(1+\frac{p}{3}\right)\ldots\left(1+\frac{p}{p-1}\right)$

$$= (1+p)\left(\frac{2+p}{2}\right)\left(\frac{3+p}{3}\right)\ldots\left(\frac{p-1+p}{p-1}\right)$$

$$= \frac{(p+1)(p+2)\ldots(2p-1)}{(p-1)!} = \binom{2p-1}{p-1}$$

is an integer. Then

$$(p-1)!\binom{2p-1}{p-1} = (p+1)\ldots(2p-1)$$

$$\equiv 1.2\ldots(p-1) \pmod{p}$$

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

Since $\left((p-1)!, p\right) = 1$, it follows that $N \equiv 1 \pmod{p}$

EXERCISE 5.1

1. Find the self-invertible least residues modulo each prime p.

   (a) 13 (b) 19

2. Solve the congruence $x^2 \equiv 1 \pmod{m}$ for each modulus m.

   (a) 12 (b) 15

3. Without using Wilson's theorem, verify that $(p-1)! \equiv -1 \pmod{p}$ for each p.

   (a) 3 (b) 13

Prove each, where p is a prime.

4. Let p be odd. Then $2(p-3)! \equiv -1 \pmod{p}$

5. Let p be odd. Then $2^2 . 4^2 \ldots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$

6. Let $0 \le r \le p-1$. Then $r!\,(p-1-r)! + (-1)^r \equiv 0 \pmod{p}$

7. $\binom{np}{p} \equiv n \pmod{p}$

5.2 Fermat's Little theorem

Lemma 1.

Let p be a prime and a any integer such that $p \nmid a$. Then the least residues of the integers $a, 2a, 3a, \ldots, (p-1)a$ modulo p are a permutation of the integers $1, 2, 3, \ldots, (p-1)$

Proof :

I-Part

To show that, $ia \not\equiv 0 \pmod{p}$, $1 \le i \le p-1$

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

$$\Rightarrow p \mid ia$$

But $(p, a) = 1$

So $p \mid i$, which is impossible since $i < p$

$$\therefore ia \not\equiv 0 \pmod{p}$$

II-Part

To show that if $ia \equiv ja \pmod{p}$, $1 \le i, j \le p-1$ then $i = j$

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

Since $(p, a) = 1$

$$\Rightarrow i \equiv j \pmod{p}$$

But both i and j are least residues modulo p.

So, $i = j$

Hence, if $ia \equiv ja \pmod{p}$, $1 \le i, j \le p-1$ then $i = j$

In other words, no two least residues of $a, 2a, 3a, \ldots, (p-1)a$ are congruent modulo p.

Theorem 1.

(Fermat's Little 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 lemma 1, the least residues of the integers $a, 2a, 3a, \ldots (p-1)a$ modulo p are the same as the integers

1, 2, 3, ..., $(p-1)$ in same order.

$\therefore$ their products are congruent modulo p.

i.e., $a \cdot 2a \cdot 3a \ \ldots \ (p-1)a \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}$

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

But $\left((p-1)!, p\right) = 1$

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

Since we know that,

If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$ then $a \equiv b \pmod{m}$

Example 5.2.1

Find the primes p for which $\dfrac{2^{p-1} - 1}{p}$ is a square.

Solution :

Let $\dfrac{2^{p-1} - 1}{p} = n^2$ for some positive integer n

$\Rightarrow 2^{p-1} - 1 = pn^2$.

Clearly, both p and n must be odd.

Let $p = 2k + 1$ ... (1) for some positive integer k.

Then $2^{2k} - 1 = pn^2 \Rightarrow (2^k)^2 - 1^2 = pn^2 \Rightarrow (2^k)^2 = (r^2 + 1)^2$

$\Rightarrow 2^{2k} = (r^2 + 1)^2$

$\Rightarrow (2^k - 1)(2^k + 1) = pn^2$.

Since $2^k - 1$ and $2^k + 1$ are consecutive odd integers, they are relatively prime.

Consequently, either $2^k - 1$ or $2^k + 1$ must be a perfect square.

Suppose $2^k - 1$ is perfect square r^2

$$2^k - 1 = r^2$$

$$\Rightarrow \quad 2^k = r^2 + 1$$

$$\Rightarrow \quad (2^k)^2 = (r^2 + 1)^2$$

$$\Rightarrow \quad 2^{2k} = (r^2 + 1)^2$$

$$\text{i.e.,} \quad 2^{p-1} = (r^2 + 1)^2 \quad \text{by (1)}$$

Since $r \geq 1$ and is odd, $r = 2i + 1$ for some integer ≥ 0

Then $2^k = (2i + 1)^2 = 2(2i^2 + 2i + 1)$; this is possible if and only if $i = 0$.

Then $r = 1$, so $2^{p-1} = (1^2 + 1)^2 = 4$ and hence $p = 3$.

Suppose 2^{k+1} is a perfect square s^2

$$2^k + 1 = s^2$$

$$2^k = s^2 - 1$$

$$\Rightarrow \quad (2^k)^2 = (s^2 - 1)^2 \Rightarrow 2^{2k} = \left[(s-1)(s+1)\right]^2$$

$$\Rightarrow \quad 2^{p-1} = (s-1)^2 (s+1)^2$$

Since $s \geq 3$ and is odd, $s = 2i + 1$ for some $i \geq 1$.

Then $2^k = (2i+1)^2 - 1 = 4i(i+1)$, that is $2^{k-2} = i(i+1)$.

This is possible if and only if $i = 1$.

Then $s = 3$ and hence $2^{p-1} = 2^2 . 4^2 = 2^6$

So $p = 7$.

Hence, p must be 3 or 7.

Example 5.2.2

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

Solution :

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

$$\Rightarrow 24^{1947} = 7^{1947} \pmod{17} \qquad \ldots (1)$$

Fermat's little theorem is $a^{p-1} \equiv 1 \pmod{p}$, p prime, any integer $p \nmid a$

Here, $p = 17$, $p - 1 = 16$, $a = 7$, $17 \nmid 7$

$16 \overline{)1947}$

$1936 - 11$

$$\therefore \quad 7^{16} \equiv 1 \pmod{17} \qquad \ldots (2)$$

$$7^{1947} \equiv 7^{(16)(121)+11} = (7^{16})^{121} 7^{11}$$

$$\therefore \quad 7^{1947} \equiv 1^{121} 7^{11} \pmod{17}$$

$$7^{1947} \equiv 7^{11} \pmod{17} \qquad \ldots (3)$$

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

$$7^{11} \equiv (7^2)^5\, 7 \pmod{17}$$
$$\equiv (-2)^5\, 7 \pmod{17}$$
$$\equiv (-32)\,(7) \pmod{17}$$
$$\equiv (2)\,(7) \text{ mod } 17$$
$$\equiv 14 \text{ mod } 17 \quad \ldots (4)$$

$\Rightarrow 24^{1947} \equiv 14 \text{ mod } (17)$ by (2), (3) & (4)

So, the remainder is 14

Example 5.2.3

Find the remainder when 30^{2020} is divided by 19.

Solution :

$$30 \equiv (-8) \pmod{19}$$
$$30^{2020} \equiv (-8)^{2020} \pmod{19}$$
$$\equiv 8^{2020} \pmod{19} \quad \ldots (1)$$

Fermat's little theorem is $a^{p-1} \equiv 1 \pmod{p}$, p prime, any integer $p \nmid a$

$$8^{18} \equiv 1 \pmod{19}$$
$$8^{2020} \equiv (8^{18})^{112}\, 8^4 \pmod{19}$$
$$\equiv (1)\, 8^4 \pmod{19}$$
$$\equiv 11 \pmod{19} \quad \ldots (2)$$
$$30^{2020} \equiv 11 \pmod{19}$$

$18 \mid 2020$

$112 - 4$

$8^4 = 4096$

$19 \mid 4096$

$215 - 11$

Example 5.2.24

Find the ones digit in the base-seven expansion of each decimal number

(a) 5^{101} (b) 37^{3434}

Solution :

$$5 \equiv -2 \pmod 7$$

$$5^{101} \equiv (-2)^{101} \pmod 7 \qquad \ldots (1)$$

Fermat's little theorem is $a^{p-1} \equiv 1 \pmod p$, p prime, any integer $p \nmid a$

$$6 \mid 101$$
$$16-5$$

$$\therefore (-2)^6 \equiv 1 \pmod 7$$

$$(-2)^{101} \equiv (-2)^{(6)(16)+5} \pmod 7$$

$$\equiv (-2)^{6(16)} (-2)^5 \pmod 7$$

$$7 \mid 32$$
$$4-4$$

$$\equiv (1) (-2)^5 \pmod 7$$

$$\equiv -4 \pmod 7$$

$$5^{101} \equiv 3 \pmod 7$$

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

$$(37)^{3434} = 2^{3434} \pmod 7$$

Fermat's little theorem is $a^{p-1} \equiv 1 \pmod p$, p prime, any integer $p \nmid a$

$$6 \mid 3434$$
$$572-2$$

$$2^6 \equiv 1 \pmod 7$$

$$2^{3434} \equiv (2^6)^{572} 2^2 \pmod 7$$

$$\equiv (1)^{572} 2^2 \pmod 7$$

$$\equiv 4 \pmod 7$$

Theorem 2.

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 Fermta's little theorem, $a^{p-1} \equiv 1 \pmod{p}$. That is, $a \cdot a^{p-2} \equiv 1 \pmod{p}$, so a^{p-2} is an inverse of a modulo p

Theorem 3.

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 $p \nmid a \Rightarrow$ the congruence $ax \equiv b \pmod{p}$ has a unique solution.

Since, a^{p-2} is an inverse of a modulo p, multiplying both sides of the congruence by a^{p-2}, we have

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

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

$$x \equiv a^{p-2} b \pmod{p}, \text{ by Fermat's little theorem.}$$

Theorem 4.

Let p be a prime and a any positive integer. Then $a^p \equiv a \pmod{p}$

Proof :

Case 1 : Suppose $p \nmid a$. Then, by Fermat's little theorem, $a^{p-1} \equiv 1 \pmod{p}$, so $a^p \equiv a \pmod{p}$

Case 2 : Suppose $p \mid a$. Then $p \equiv a \equiv 0 \pmod{p}$, so $a^p \equiv 0 \pmod{p}$

$$\therefore\ a^p \equiv a \pmod{p}$$

Hence, in both cases, $a^p \equiv a \pmod{p}$

Theorem 5.

Let $p_1, p_2, ..., p_k$ be any distinct primes, a any positive integer, and $l = [p_1 - 1, p_2 - 1, ..., p_k - 1]$. Then $a^{l+1} \equiv a \pmod{p_1 p_2 ..., p_k}$

Proof :

By Fermat's little theorem, $a^{p_i - 1} \equiv 1 \pmod{p_i}$, where $1 \le i \le k$.

Since $p_i - 1/l$

$$\Rightarrow (a^{p_i} - 1)^{l/(p_i - 1)} \equiv 1 \pmod{p_i}.$$

i.e., $a^l \equiv 1 \pmod{p_i}$. Thus, $a^{l+1} \equiv a \pmod{p_i}$.

Consequently, $a^{l+1} \equiv a \pmod{[p_1, p_2, ..., p_k]}$

i.e., $a^{l+1} \equiv a \pmod{p_1 p_2 \cdots p_k}$.

Corollary 1.

Let a be any integer and p and prime > 3. Then $a^p \equiv a \pmod{6p}$.

Example 5.2.5

Solve each linear congruence.

(a) $12x \equiv 6 \pmod{7}$

(b) $24x \equiv 11 \pmod{17}$

(c) $43x \equiv 17 \pmod{23}$

Solution :

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

$$12x \equiv 6 \pmod{7}$$

$$\Rightarrow \quad x \equiv (12)^{7-2} 6 \pmod{7}$$

$$\equiv (12)^5 \, 6 \pmod{7}$$

$$\equiv (3)(6) \pmod{7}$$

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

$$7 \overline{)\,248832}$$
$$35547 - 3$$

$$[\because \quad 12 \equiv -2 \pmod{7}$$

$$12^5 \equiv (-2)^5 \pmod{7}$$

$$\equiv -(2)^2 2^3 \pmod{7}$$

$$\equiv (-4)(1) \pmod{7}$$

$$\equiv -4 \pmod{7}$$

$$\equiv 3 \pmod{7}]$$

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

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

$$x = (24)^{17-2} \, 11 \pmod{17}$$

$$= (24)^{15} \, 11 \pmod{17} \qquad \ldots (1)$$

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

$$24^3 \equiv 3 \pmod{17}$$

$$(1) \Rightarrow x \equiv (24^3)^5\, 11 \pmod{17}$$

$$\equiv (3)^5\, 11 \pmod{17}$$

$$\equiv 2673 \pmod{17}$$

$$= 4 \pmod{17}$$

$24^3 = 13824$
17 | 13824
813–3
17 | 2673
157–4

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

$$43x \equiv 17 \pmod{23}$$

$$x \equiv (43)^{23-2}\, 17 \pmod{23}$$

$$\equiv (43)^{21}\, 17 \pmod{23} \quad \ldots (1)$$

$$43 \equiv 20 \pmod{23}$$

$$(43)^3 \equiv 19 \pmod{23}$$

$43^3 = 79507$
23 | 79507
3456–19

$$(1) \Rightarrow \quad x \equiv (43^3)^7\, 17 \pmod{23}$$

$$x \equiv (19)^7\, 17 \pmod{23} \quad \ldots (2)$$

$$19^3 \equiv 5 \pmod{23}$$

$$(2) \Rightarrow \quad x = (19^3)^2\, (19)\, (17) \pmod{23}$$

$$\equiv (5)^2\, (323) \pmod{23}$$

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

Example 5.2.6

Compute the least residue of each

(a) $2^{340} \pmod{341}$ (b) $11^{16} + 17^{10} \pmod{187}$

Solution :

(a) $2^{340} \pmod{381}$

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

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

$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}$

$2^{340} = (2^{30})^{11} 2^{10} \equiv (1)(1) \equiv 1 \pmod{31}$

$\Rightarrow 2^{340} \equiv 1 \pmod{[11, 31]}$

$\equiv 1 \bmod (341)$

(b) $11^{16} \equiv 1 \pmod{17}$

$17^{10} \equiv 1 \pmod{11}$

$\Rightarrow 11^{16} + 17^{10} \equiv 1 + 0 \equiv 1 \pmod{17}$

$\Rightarrow 11^{16} + 17^{10} \equiv 0 + 1 \equiv 1 \pmod{11}$

$\Rightarrow 11^{16} + 17^{10} \equiv 1 \pmod{[17, 11]}$

$11^{16} + 17^{10} \equiv 1 \pmod{[187]}$

Example 5.2.7

Verify $(12 + 15)^{17} \equiv 12^{17} + 15^{17} \pmod{17}$

Solution :

$(12 + 15)^{17} = (27)^{17} = 27 \pmod{17}$ by theorem 4.

$\equiv (12 + 15) \pmod{17}$

$\equiv 12^{17} + 15^{17} \pmod{17}$ by theorem 4.

Example 5.2.8

If p be any odd prime and a any non-negative integer then $1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod{p}$.

Solution :

We know that, $k^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem

where $0 < k < p$

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

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

$\equiv -1 \pmod{p}$

EXERCISE 5.2

1. Find the remainder when the first integer is divided by the secor

   (a) 7^{1001}, 17 (b) 15^{1976}, 23 (c) 43^{5555}, 31

2. Find the ones digit in the base-seven expansion of each decimal number.

   (a) 12^{1111} (b) 29^{2076}

3. Solve each linear congruence.

   (a) $8x \equiv 3 \pmod{11}$

   (b) $26x \equiv 12 \pmod{17}$

   (c) $15x \equiv 7 \pmod{13}$

4. $(16 \div 21)^{23} \equiv 16^{23} + 21^{23} \pmod{23}$

5. Find the primes p such that $(2^{p-1} - 1)/p$ is a perfect cube.

6. Let p and q be distinct primes, and a, b, and n arbitrary positive integers. Prove each

   (a) If $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$

   (b) If $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$

   (c) $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

   (d) $p^q + q^p \equiv p + q \pmod{pq}$

7. Using Fermat's little theorem, prove that

   $(a + b)^p \equiv a^p + b^p \pmod{p}$

5.3 Euler's theorem - Euler's Phi function

Definition : Euler's Phi function

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

Theorem 1

A positive integer p is a prime if and only if $\phi(p) = p - 1$

Proof :

Let p be a prime.

Then there are $p - 1$ positive integers $\leq p$ and relatively prime to p, so $\phi(p) = p - 1$

Conversely, let p be a positive integer such that $\phi(p) = p - 1$.

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

Since there are exactly $p - 1$ positive integers $< p$,

d is one of them, and $(d, p) \neq 1$

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

Hence, p must be a prime.

Theorem 2.

Let m be a positive integer and a very 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 $ar_1, ar_2, \ldots, a r_{\phi(m)}$ modulo m are a permutation of the integers $r_1, r_2, \ldots, a_{\phi(m)}$

Theorem 3.

(Euler's Theorem) (or) Generalised Fermat'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 :

Given m is a positive integer a any integer such that $(a, m) = 1$

Let $r_1, r_2, \ldots, r_{\phi(m)}$ be the least residues modulo m that are relatively prime to m.

To prove that $(ar_i, m) = 1$ for every i

Let $(ar_i, m) > 1$

Let p be a prime factor of (ar_i, m)

$\Rightarrow p \mid ar_i$ and $p \mid m$ $\quad [\because p \mid ar_i, p \mid a$ or $p \mid r_i]$

If $p \mid r_i$, then $p \mid r_i$ and $p \mid m$,

So, $(r_i, m) \neq 1$, a contradiction.

So $p \mid a$

This coupled with $p \mid m \Rightarrow p \mid (a, m)$, $\Rightarrow (a, m) \neq 1$ again a contradiction.

Hence, $(ar_i, m) = 1$

i.e., the integers $ar_1, ar_2, \ldots, a r_{\phi(m)}$ are relatively prime to m.

So the integers $ar_1, ar_2, \ldots, ar_{\phi(m)}$ are congruent modulo m to $r_1, r_2, \ldots, r_{\phi(m)}$ in same order.

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

Since each r_i is relatively prime to m

$$\Rightarrow (r_1 r_2 \ldots r_{\phi(m)}, m) = 1$$

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

Hence the proof.

Definition : Multiplicative Function

A number theoretic function f is **multiplicative** if $f(mn) = f(m) f(n)$ whenever m and n are relatively prime.

Theorem 4.

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 : We prove this by induction on the number of distinct primes in n

If $k = 1$, that is, if $n = p_1^{e_1}$, then $f(n) = f(p_1^{e_1})$, so the theorem is trivally true.

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

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

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

$$n = p_1^{e_1} p_2^{e_2} \ldots p_{k+1}^{e_{k+1}}.$$

Since $(p_1^{e_1} \ldots p_k^{e_k}, p_{k+1}^{e_{k+1}}) = 1$ and f is multiplicative

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

$$= f(p_1^{e_1}) \ldots f(p_k^{e_k}) f(p_{k+1}^{e_{k+1}}),$$

by the inductive hypothesis.

Therefore, by induction, the result is true for any positive integer n.

Theorem 5.

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

Proof :

$\phi(p^e)$ = number of positive integers $\leq p^e$ and relatively prime to it

$$= \begin{pmatrix}\text{number of positive}\\ \text{integers} \leq p^e\end{pmatrix} - \begin{pmatrix}\text{number of positive integers} \leq p^e\\ \text{and not relatively prime to it}\end{pmatrix}$$

The positive integers $\leq p^e$ and not relatively prime to it are the various multiples of p, they are $p, 2p, 3p, \ldots, (p^{e-1})p$, and p^{e-1} in number.

Hence $\phi(p^e) = p^e - p^{e-1}$

Note : $\phi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right)$

Theorem 6.

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

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

Proof :

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

$$\phi(n) = \phi\left(p_1^{e_1}\right)\phi\left(p_2^{e_2}\right) \ldots \phi\left(p_k^{e_k}\right) \qquad [\because \phi \text{ is multiplicative}]$$

$$= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_2^{e_2}\left(1 - \frac{1}{p_2}\right) \ldots p_k^{e_k}\left(1 - \frac{1}{p_k}\right), \text{ by Theorem 5.}$$

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

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

Theorem 7.

The Euler function ϕ is multiplicative.

Proof :

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

To show that $\phi(mn) = \phi(m)\,\phi(n)$

Arrange the integers 1 through mn in m rows of n each

1	$m+1$	$2m+1$	...	$(n-1)m+1$	
2	$m+2$	$2m+2$	...	$(n-1)m+2$	
3	$m+3$	$2m+3$	...	$(n-1)m+3$	
			:		
r	$m+r$	$2m+r$	...	$(n-1)m+r$	$\leftarrow r^{\text{th}}$ row
			:		
m	$2m$	$3m$	...	nm	

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

To show that no element of the r^{th} row in the array relatively prime to mn.

Let $d = (r, m)$.

Then $d \mid r$ and $d \mid m$, so $d \mid km + r$ for any integer k.

i.e., d is a factor of every element in the r^{th} row.

Hence, no element in the r^{th} row is relatively prime to m and hence to mn if $(r, m) > 1$.

By definition, there are $\phi(m)$ such integers r and hence $\phi(m)$ such rows.

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

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

Their least residues modulo n are a permutation of 0, 1, 2, ..., $(n-1)$ of which $\phi(n)$ are relatively prime to n.

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

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

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

$$\text{i.e., } \phi(mn) = 0\ \phi(m)\,\phi(n)$$

$\Rightarrow \phi$ is multiplicative.

Example 5.3.1

Find $\phi(11)$

Solution :

11 is a prime.

Every positive integer < 11 is relatively prime to 11

$$\therefore \phi(11) = 10$$

Example 5.3.2

Find $\phi(18)$

Solution :

$$\begin{array}{c|c} 2 & 18 \\ \hline 3 & 9 \\ \hline & 3 \end{array}$$

$$18 = (2)(3^2)$$

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

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

$$= (1)(9)\left(\frac{2}{3}\right) \qquad [\because \phi(2) = 2 - 1 \text{ by Theorem 1}]$$

$$= 6 \qquad \left[\phi(p^e) = p^e\left(1 - \frac{1}{p}\right) \text{ Theorem 5}\right]$$

Example 5.3.3

Find $\phi(28)$

2	28
2	14
	7

Solution :

$$28 = (2^2)(7)$$

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

$$= 2^2\left(1-\frac{1}{2}\right)(6) \qquad [\because \phi(7) = 7-1 \text{ by Theorem 1}]$$

$$= (4)\left(\frac{1}{2}\right)(6) \qquad \phi(p^e) = p^e\left(1-\frac{1}{p}\right) \text{ Theorem 5}]$$

$$= 12$$

Example 5.3.4

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

Solution :

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

$$245^{1040} \equiv 11^{1040} \pmod{18} \qquad \ldots (1)$$

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

$$= \phi(3^2)\,\phi(2)$$

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

$$= (9)\left(\frac{2}{3}\right)(1)$$

$$= 6$$

$$11^{\phi(18)} \equiv 11^6 \equiv 1 \pmod{18} \text{ by Euler.}$$

$$(1) \Rightarrow 11^{1040} = (11^6)^{173} \cdot 11^2 \equiv 1^{173}(121) \bmod 18$$

$$\equiv 13 \bmod 18$$

$$6 \mid 1040$$

$$173 - 2$$

Hence, the remainder is 13

Example 5.3.5

Find the remainder when 199^{2020} is divided by 28.

Solution :

$$199 \equiv 3 \pmod{28}$$

$$199^{2020} \equiv 3^{2020} \pmod{28} \quad \ldots (1)$$

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

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

$$= (4)\left(\frac{1}{2}\right)(6) = 12$$

$$2 \mid 28$$

$$2 \mid 14$$

$$7$$

$$3^{\phi(28)} \equiv 3^{12} \equiv 1 \pmod{28}$$

$$(1) \Rightarrow 199^{2020} = 3^{2020} \pmod{28}$$

$$\equiv (3^{12})^{168}\, 3^4 \pmod{28}$$

$$= 1^{168}(81) \pmod{28}$$

$$= 25 \pmod{28}$$

$$12 \mid 2020$$

$$168 - 4$$

Hence, the remainder is 25.

Example 5.3.6

Using Euler's theorem, find the ones digit in the decimal value of 23^{7777}

Solution :

$$23 \equiv 3 \pmod{10}$$

$$23^{7777} = 3^{7777} \pmod{10} \quad \ldots (1)$$

$$\phi(10) = \phi(2)\,\phi(5)$$

$$= (1)\,(4) = 4$$

$$3^{\phi(10)} \equiv 3^4 \equiv 1 \pmod{10} \text{ by Euler.}$$

$$(1) \Rightarrow 23^{7777} = 3^{7777} \pmod{10}$$

$$\equiv (3^4)^{1944}\, 3 \pmod{10}$$

$$\equiv 1^{1944}\, 3 \pmod{10}$$

$$\equiv 3 \pmod{10}$$

$4 \mid 7777$

$1944 - 1$

So the ones digit is 3.

Theorem 8.

Let m be a positive integer and a any integer with $(a, m) = 1$.

Then $a^{\phi(m)-1}$ is an inverse of a modulo m.

Theorem 9.

Let m be a positive integer and a any integer with $(a, m) = 1$.

Then the solution of the linear congruence $ax \equiv b \pmod{m}$ is given by $x \equiv a^{\phi(m)-1} \pmod{m}$.

Example 5.3.7

Solve the linear congruence $25x \equiv 13 \pmod{18}$

Solution :

$$25x \equiv 13 \pmod{18}$$

$$\Rightarrow \quad 7x \equiv 13 \pmod{18} \quad \ldots (1)$$

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

$$= (2-1)\,3^2\left[1-\frac{1}{3}\right]$$

$$= (1)(9)\left(\frac{2}{3}\right)$$

$$= 6$$

$$(1) \Rightarrow \quad x \equiv 7^{\phi(18)-1}\ 13 \pmod{18}$$

$$x \equiv 7^{6-1}\ 13 \pmod{18}$$

$$\equiv 7^5\ (13) \pmod{18} \qquad \ldots (2)$$

$$7^5 \equiv 13 \pmod{18}$$

$$\therefore (2) \Rightarrow \quad x \equiv (13)(13) \pmod{18}$$

$$\equiv 7 \pmod{18}$$

Theorem 10.

Let $m_1, m_2, \ldots, m_k$ be any positive integers and a any integer such that $(a, m_i) = 1$ for $1 \le i \le k$. then

$$a^{[\phi(m_1), \phi(m_2), \ldots \phi(m_k)]} \equiv 1 \pmod{[m_1, m_2, \ldots m_k]}$$

Corollary : Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime integers and a any integer such that $(a, m_i) = 1$ for $1 \le i \le k$. Then

$$a^{[\phi(m_1), \phi(m_2), \ldots \phi(m_k)]} \equiv 1 \pmod{m_1 m_2 \ldots m_k}$$

Theorem 11.

Let n be a positive integer. Then $\sum_{d|n} \phi(d) = n$

Example 5.3.8

Compute $\sum_{d|n} \phi(d)$ for $n = 7$

Solution :

$$\sum_{d|7} \phi(d) = \phi(1) + \phi(7)$$

$$= 1 + 6$$

$$= 7$$

Example 5.3.9

Prove that m be a positive integer and a any integer with $(a, m) = 1$. Then $a^{\phi(m)-1}$ is an inverse of a modulo m.

Proof :

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

i.e., $a \cdot a^{\phi(m)-1} \equiv 1 \pmod{m}$.

$\therefore a^{\phi(m)-1}$ is an inverse of a modulo m.

Example 5.3.10

If $n = 2^k$, then $\phi(n) = \frac{n}{2}$

Solution :

Given : $n = 2^k$ ... (1)

$$\phi(n) = \phi(2^k)$$

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

$$= \frac{1}{2}(2^k)$$

$$= \frac{n}{2} \text{ by (1)}$$

Example 5.3.11

Compute $\phi(p!)$ for the prime 7.

Solution :

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

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

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

$$= (8)(6)(4)(6)$$

$$= 1152$$

Example 5.3.12

Derive a formula for $\phi(pq)$, where p and q are twin primes.

Solution :

$$\phi(p\,q) = \phi(p)\,\phi(q)$$

$$= (p-1)(q-1)$$

$$= (p-1)(p+1)$$

$$= p^2 - 1$$

Example 5.3.13

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

Solution :

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

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

$$= 2^{2k}$$

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

$\therefore \phi(2^{2k+1})$ is a square.

Example 5.3.14

If a and b are relatively prime, then $a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{ab}$.

Solution :

By Euler's theorem $a^{\phi(b)} \equiv 1 \pmod{b}$ and $b^{\phi(a)} \equiv 1 \pmod{a}$.

$\therefore \quad a^{\phi(b)} + b^{\phi(a)} \equiv 1 + 0 \equiv 1 \pmod{b}$

and $\quad a^{\phi(b)} + b^{\phi(a)} \equiv 0 + 1 \equiv 1 \pmod{a}$.

Hence $\quad a^{\phi(b)} + b^{\phi(a)} \equiv 1 \pmod{[a,b]} \equiv 1 \pmod{ab}$

EXERCISE 5.3

1. Compute $\phi(m)$ for each integer m

   (a) 8 (b) 15

2. List the positive integers $\leq m$ and relatively prime to it.

3. Verify that $a^6 \equiv 1 \pmod{18}$ for $a = 1, 5, 7, 11, 13$ and 17.

4. Using the values of $\phi(m)$ for $m \leq 15$, make a conjecture on the evenness of $\phi(m)$

5. Find the remainder when the first integer is divided by the second.

   (a) 7^{1020}, 15 (b) 79^{1776}, 24 (c) 25^{2550}, 18

6. Using Euler's theorem, find the ones digit in the decimal value of 17^{6666}

7. Using Euler's theorem, find the ones digit in the hexadecimal value of each.

   (a) 7^{1030} (b) 13^{4444}

8. Solve each linear congruence

   (a) $7x \equiv 8 \pmod{10}$ (b) $143x \equiv 47 \pmod{20}$

   (c) $23x \equiv 17 \pmod{12}$ (d) $17x \equiv 20 \pmod{24}$

   (e) $79x \equiv 17 \pmod{25}$

9. If m and n are relatively prime, then $\phi(mn) = \phi(m) \cdot \phi(n)$. Using this fact, compute each.

   (a) $\phi(15)$ (b) $\phi(105)$ (c) $\phi(35)$

10. Compute $\sum_{d|n} \phi(d)$ for each n.

    (a) 12 (b) 17

5.4 Tau and Sigma functions

Definition : The Tau function

Let n be a positive integer. Then $\tau(n)$ denotes the number of positive factors of n,

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

Definition : The Sigma function

Let n be a positive integer. Then $\sigma(n)$ denotes the sum of the positive factors of n,

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

Definition : Let f be a multiplicative function.

Then F is defined by

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

Theorem 1.

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

Proof :

Let m and n be relatively prime positive integers.

To prove : $F(mn) = F(m)\,F(n)$

By definition,

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

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

$$\therefore F(mn) = \sum_{\substack{d_1 | m \\ d_2 | m}} f(d_1 d_2)$$

$f(d_1 d_2) = f(d_1) f(d_2)$. $\therefore f$ is multiplicative.

$$\text{So } F(mn) = \sum_{\substack{d_1 | m \\ d_2 | m}} f(d_1 d_2)$$

$$= \sum_{d_2 | n} F(m) f(d_2), \text{ by the definition of } F$$

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

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

Thus, F is multiplicative.

Corollary 1.

The tau and sigma functions are multiplicative.

Proof :

We know that the constant function $f(n) = 1$ and the identity function $g(n) = n$ are multiplicative.

$$\therefore \sum_{d | n} f(d) = \sum_{d | n} 1 = r(n) \text{ and } \sum_{d | n} g(d) = \sum_{d | n} d = \sigma(n)$$

are multiplicative, i.e., if $(m, n) = 1$, then $\tau(mn) = \tau(m) \tau(n)$ and $\sigma(mn) = \sigma(m) \sigma(n)$

Theorem 2.

Let p be any prime and e 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 of the form p^i, where $0 \le i \le e$; there are $e + 1$ of them, so $\tau(p^e) = e + 1$

$$\Rightarrow \sigma(p^e) = \sum_{i=0}^{e} p^i = \frac{p^{e+1} - 1}{p - 1}$$

Theorem 3.

Let n be a positive integer with canonical decomposition $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$. Then $\tau(n) = (e_1 + 1)(e_2 + 1) \ldots (e_k + 1)$ and

$$\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1}$$

Proof :

Since τ is multiplicative,

$$\Rightarrow \tau(n) = \tau(p_1^{e_1}) \cdot \tau(p_2^{e_2}) \ldots \tau(p_k^{e_k})$$

$$= (e_1 + 1)(e_2 + 1) \ldots (e_k + 1)$$

Since σ is multiplicative,

$$\sigma(n) = \sigma(p_1^{e_1}) \cdot \sigma(p_2^{e_2}) \ldots \sigma(p_k^{e_k})$$

$$= \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1}$$

Example 5.4.1

Compute $\tau(n)$ for each n

(a) 18 (b) 23 (c) 1560 (d) 2187

(e) 36 (f) 6120

Solution :

2	18
3	9
	3

(a) $18 = (2^1)(3^2)$

$\tau(18) = \tau(2^1)\,\tau(3^2)$

$= (1+1)(2+1) \qquad [\because \tau = (p^e) = e+1]$

$= (2)(3) = 6$

Note : The number of positive divisors of 18 are 1, 2, 3, 6, 9 and 18

(b) 23, being a prime

23 has exactly two positive divisors

so $\tau(23) = 2$

Note : The number of positive divisors of 23 are 1, 23

2	1560
2	780
2	390
3	195
5	65
	13

(c) $1560 = (2^3)(3)(5)(13)$

$\tau(1560) = \tau(2^3)\,\tau(3^1)\,\tau(5^1)\,\tau(13^1)$

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

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

$= 32$

(d) $2187 = 3^7$

$\tau(2187) = \tau(3^7)$

$= (7 + 1)$

$= 8$

3	2187
3	729
3	243
3	81
3	27
3	9
	3

(e) $36 = (2^2)(3^2)$

$\tau(36) = \tau(2^2)\,\tau(3^2)$

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

$= (3)(3) = 9$

2	36
2	18
3	9
	3

(f) $6120 = (2^3)(5)(3^2)(17)$

$\tau(6120) = \tau(2^3)\,\tau(5^1)\,\tau(3^2)\,\tau(17)$

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

$= (4)(2)(3)(2) = 48$

2	6120
2	3060
2	1530
5	765
3	153
3	51
	17

Example 5.4.2

Compute $\sigma(n)$ for each n

(a) $\sigma(12)$ (b) $\sigma(28)$ (c) $\sigma(36)$ (d) $\sigma(6120)$ (e) $\sigma(2187)$

Solution :

Let p be any prime and e any prime, then

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

(a) $12 = (2^2)(3)$

$\sigma(12) = \sigma(2^2) \cdot \sigma(3^1)$

$= \left[\frac{2^{2+1} - 1}{2 - 1}\right]\left[\frac{3^{1+1} - 1}{3 - 1}\right]$

2	12
2	6
	3

$$= \left[\frac{8-1}{1}\right]\left[\frac{9-1}{2}\right]$$

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

$$= 28$$

(b) $28 = (2^2)\ (7)$

$$\sigma(28) = \sigma(2^2)\,\sigma(7')$$

$$= \left[\frac{2^{2+1}-1}{2-1}\right]\left[\frac{7^{1+1}-1}{7-1}\right]$$

$$= \left[\frac{8-1}{1}\right]\left[\frac{49-1}{6}\right]$$

$$= [7]\ [8]$$

$$= 56$$

2	28
2	14
	7

(c) $36 = (2^2)\ (3^2)$

$$\sigma(36) = \sigma(2^2)\,\sigma(3^2)$$

$$= \left[\frac{2^{2+1}-1}{2-1}\right]\left[\frac{3^{2+1}-1}{3-1}\right]$$

$$= \left[\frac{8-1}{1}\right]\left[\frac{27-1}{2}\right]$$

$$= (7)\ (13)$$

$$= 91$$

2	36
2	18
3	9
	3

(d) $6120 = (2^3)\ (3^2)\ (5)\ (17)$

$$\sigma(6120) = \sigma(2^3)\,\sigma(3^2)\,\sigma(5)\,\sigma(17)$$

$$= \left[\frac{2^{3+1}-1}{2-1}\right]\left[\frac{3^{2+1}-1}{3-1}\right]\left[\frac{5^{1+1}-1}{5-1}\right]\left[\frac{17^{1+1}-1}{17-1}\right]$$

$$= \left[\frac{15}{1}\right]\left[\frac{26}{2}\right]\left[\frac{24}{4}\right]\left[\frac{288}{16}\right]$$

$$= (15)(13)(6)(18)$$

$$= 21060$$

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

(c) $2187 = 3^7$

$$\sigma(2187) = \sigma(3^7)$$

$$= \frac{3^{7+1} - 1}{3 - 1}$$

$$= \frac{6560}{2}$$

$$= 3280$$

3	2187
3	729
3	243
3	81
3	27
3	9
	3

Example 5.4.3

List the positive factors of each, where p and q are distinct primes

(a) pq^2 (b) p^2q^3

Solution :

(a) $1, p, q, pq, q^2$ and pq^2

(b) $1, p, q, pq, p^2, q^2, q^3, p^2q, pq^2, pq^3, p^2q^2$ and p^2q^3

Example 5.4.4

Find the sum of the positive divisors of each number

(a) pq (b) p^2q

Solution :

(a) $\sigma(pq) = 1 + p + q + pq$

(b) $\sigma(p^2q) = (1 + p + p^2)(1 + q)$

Example 5.4.5

Let p and q be distinct primes find the sum of the positive factors of $p^i q^j$

Solution :

$$\sigma(p^i q^j) = \sigma(p^i)\,\sigma(q^j)$$

$$= \frac{p^{i+1}-1}{p-1} \cdot \frac{q^{j+1}-1}{q-1}$$

Example 5.4.6

Let $n = p_1 p_2 \ldots p_k$ be a product of k distinct primes. Find $\tau(n)$ and $\sigma(n)$

Solution :

Given : $n = p_1 p_2 \ldots p_k$

Each p_i is a prime.

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

τ and σ are multiplicative functions

$\therefore$ $\tau(n) = \tau(p_1)\,\tau(p_2) \ldots \tau(p_k)$

$= (2)\ (2) \ldots (2)$

$= 2^k$

$\sigma(n) = \sigma(p_1)\,\sigma(p_2) \ldots \sigma(p_k)$

$= (p_1 + 1)\,(p_2 + 1) \ldots (p_k + 1)$

Example 5.4.7

If $n = 2^{2^e}$, find $\tau(x)$ and $\sigma(n)$.

Solution :

Given : $n = 2^{2^e}$

$$\tau(n) = \tau(2^{2^e}) = 2^e + 1$$

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

Example 5.4.8

Show that $\sigma(p^e) - p^e = \dfrac{p^e - 1}{p - 1}$

Solution :

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

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

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

$$= \frac{p^e - p}{p - 1}$$

Example 5.4.8

Let $n = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are primes, find $\tau(n)$ and $\sigma(n)$

Solution :

Given : $n = 2^{p-1}(2^p - 1)$ ... (1)

τ and σ are multiplicative functions

Let $q = 2^p - 1$

(1) $\Rightarrow$ $n = 2^{p-1} q$

$$\tau(n) = \tau(2^{p-1})\, \tau(q^1)$$

$$= (p - 1 + 1)(1 + 1)$$

$$= p(2)$$

$$= 2p$$

$$\sigma(n) = \sigma(2^{p-1})\, \sigma(q)$$

$$= \frac{2^{p-1+1} - 1}{2 - 1} \; \frac{q^{1+1} - 1}{q - 1}$$

$$= (2^p)\left(\frac{q^2 - 1}{q - 1}\right)$$

$$= (2^p - 1)\, 2^p$$

$$= \frac{2}{2}(2^p - 1)\, 2^p$$

$$= 2(2^p - 1)\, 2^{p-1}$$

$$= 2n$$

Example 5.4.9

Let n be the product of a pair of twin primes, p being the smaller of the two

(a) Find $\tau(n)$

(b) Prove that $\sigma(p + 2) = \sigma(p) + 2$

(c) Find p for which $\sigma(p)$ is odd.

(d) Prove that $\sigma(n) = (p+1)(p+3)$

Solution :

(a) Let $n = p(p+2)$ is the product of two primes

$$\tau(n) = \tau(p)\ \tau(p+2)$$

$$= (2)\ (2) = 4$$

(b) $\sigma(p+2) = 1 + (p+2)$ [$\because p+2$ is a prime]

$$= (1+p) + 2$$

$$= \sigma(p) + 2$$

(c) $\sigma(p) = 1 + p$ to be odd $\Rightarrow$ p must be even p is a prime and p must be even

$\Rightarrow p = 2$ [$\because$ the only even prime is 2]

(d) $\sigma(n) = \sigma(p(p+2))$

$$= \sigma(p)\,\sigma(p+2)$$

$$= (p+1)(p+3)$$

Example 5.4.10

Prove that if n is a power of 2, then $\sigma(n)$ is odd.

Proof :

Let $n = 2^i$

$$\sigma(n) = \sigma(2^i)$$

$$= \frac{2^{i+1} - 1}{2 - 1} = 2^{i+1} - 1 \text{ is always odd.}$$

$\therefore \sigma(n)$ is odd.

Example 5.4.11

Prove that $\sigma_k(n)$ is multiplicative.

Proof : We know that, $F(n) = \sum_{d|n} f(d)$ is multiplicative

Let $f(n) = n^k$

$\Rightarrow \sigma_k = F(n) = \sum_{d|n} d^k$ is multliplicative.

[$\because f$ is multiplicative]

EXERCISE 5.4

1. Compute $\tau(n)$ for each n and $\sigma(n)$ for each n

   (a) 43 (b) 2187 (c) 44982

2. List the positive factors of each, where p and q are distinct primes.

   (a) pq (b) p^2q

3. Find the product of the positive divisors of p^e.

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

5. Prove that if n is a square, then $\sigma(n)$ is odd.

6. Prove that $\frac{\sigma(p^e)}{p^e} < \frac{p}{p-1}$