Unit - 5

CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS.

Theorem 1 Wilson's Theorem.

U.Q 8m If p is a prime then $(p-1)! \equiv -1 \pmod p$

Proof

When $p=2$, $(2-1)! = 1 \equiv -1 \pmod 2$

When $p=3$, $(3-1)! = 2 \equiv -1 \pmod 3$

$\therefore$ The theorem is true for the primes 2 and 3.

Assume that $p>3$ be a prime number.

Let a be any one of the positive integers $1, 2, 3, \dots (p-1)$.

Then the linear congruence $ax \equiv 1 \pmod p$ has a unique solution modulo p.

($\because$ $ax \equiv b \pmod m$ has a soln if $\gcd(a,m) / b$ and it has 'd' number of incongruent solutions $d = \gcd(a,m)$)

Let a' be the unique soln of $ax \equiv 1 \pmod p$

$\Rightarrow aa' \equiv 1 \pmod p$ where $1 \leq a' \leq (p-1)$ → ①

$\therefore$ $1 \leq a, a' \leq (p-1)$

Scanned with CamScanner

Claim ① $a = a'$ iff $a = 1$ (or) $a = (p-1)$

From ①, $aa' \equiv 1 \pmod p$

$$a = a' \iff a \cdot a \equiv 1 \pmod p$$
$$\iff a^2 \equiv 1 \pmod p$$
$$\iff (a^2 - 1) \equiv 0 \pmod p$$
$$\iff (a+1)(a-1) \equiv 0 \pmod p$$
$$\iff p \,/\, (a+1)(a-1)$$
$$\iff p \,/\, (a+1) \quad \text{or} \quad p \,/\, (a-1)$$
$$\iff a = (p-1) \quad \text{or} \quad a = 1 \qquad (\because 1 \le a, a' \le p-1)$$

Hence the claim ①.

Claim ② $(p-1)! \equiv -1 \pmod p$

Omit the numbers 1 and $(p-1)$

Group the remaining integers $2, 3, \ldots (p-2)$ into different pairs a, a' where $a \neq a'$ with $aa' \equiv 1 \pmod p$.

$a \neq a' \Rightarrow a$ and a' are unequal.

Totally $\frac{(p-3)}{2}$ congruences are possible

Multiply these $\frac{(p-3)}{2}$ congruences and arrange them

$$2 \cdot 3 \cdot 4 \ldots (p-2) \equiv 1 \pmod p$$

Multiply both sides by $(p-1)$

$$2 \cdot 3 \cdot 4 \ldots (p-2)(p-1) \equiv (p-1) \pmod p \rightarrow ②$$

$$(p-1) \equiv -1 \pmod p \rightarrow ③.$$

Using Transitive property $2 \cdot 3 \cdot 4 \ldots (p-2)(p-1) \equiv -1 \pmod p$

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

H/p.

Scanned with CamScanner

Problems

① Find the remainder when $2(26!)$ is devided by 29.

Soln.

By wilson's theorem, $(p-1)! \equiv -1 \pmod p$., p is prime.

Since $p = 29$ is a prime

$(29-1)! \equiv -1 \pmod{29}$.

$(28)! \equiv -1 \pmod{29}$

$28 \times 27 \times (26!) \equiv -1 \pmod{29} \longrightarrow ①$.

We know that $28 \equiv -1 \pmod{29}$

$27 \equiv -2 \pmod{29}$

$\Rightarrow 27 \times 28 \equiv -1 \times -2 \pmod{29}$

$\Rightarrow 27 \times 28 \equiv 2 \pmod{29} \longrightarrow ②$

Sub ② in ①.

$2(26!) \equiv -1 \pmod{29}$

$2(26!) \equiv (29-1) \pmod{29}$

$\Rightarrow 2(26!) \equiv 28 \pmod{29}$.

$\therefore$ Required remainder is '28'

---

② Find the remainder when $15!$ is devided by 17.

Soln

Since 17 is a prime, $(17-1)! \equiv -1 \pmod{17}$

$16! \equiv -1 \pmod{17}$

$16 \times 15! \equiv -1 \pmod{17}$. $\rightarrow ①$

We know that $16 \equiv -1 \pmod{17}$. $\rightarrow ②$

From ① and ②, $(-1) 15! \equiv -1 \pmod{17}$.

Scanned with CamScanner

$\Rightarrow (15)! \equiv 1 \pmod{17}$

$\therefore$ Required remainder is '1'.

---

③ Prove that $4(29!)+5!$ is devisible by 31.

Soln.

Since 31 is a prime, by wilsons theorem

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

$(30)! \equiv -1 \pmod{31}$.

$30 \times 29! \equiv -1 \pmod{31} \longrightarrow$ ①.

$30 \equiv -1 \pmod{31} \longrightarrow$ ②

From ① and ②, $-1 \times 29! \equiv -1 \pmod{31}$

$\Rightarrow 29! \equiv 1 \pmod{31}$

$\Rightarrow 4(29!) \equiv 4 \pmod{31} \longrightarrow$ ③.

$5! = 120 \equiv 27 \pmod{31} \longrightarrow$ ④.

$$\begin{array}{r|l} & 3 \\ 31 & 120 \\ & 93 \\ \hline & 27 \end{array}$$

③ + ④

$\Rightarrow 4(29!)+5! \equiv 27+4 \pmod{31}$

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

$31 \equiv 0 \pmod{31}$.

Using Transitive property, $4(29!)+5! \equiv 0 \pmod{31}$.

$\Rightarrow 31 \,/\, 4(29!)+5!$

H/p.

Scanned with CamScanner

4 Show that $18! \equiv -1 \pmod{437}$

Soln.

$437 = 19 \times 23$

Since 19 and 23 are primes, by wilsons theorem

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

$(18)! \equiv -1 \pmod{19} \longrightarrow ①$

and $(23-1)! \equiv -1 \pmod{23}$

$(22)! \equiv -1 \pmod{23}$

$22 \times 21 \times 20 \times 19 \times (18!) \equiv -1 \pmod{23} \longrightarrow ②$

$$\left.\begin{array}{l} 22 \equiv -1 \pmod{23} \\ 21 \equiv -2 \pmod{23} \\ 20 \equiv -3 \pmod{23} \\ 19 \equiv -4 \pmod{23} \end{array}\right\} \Rightarrow 22 \times 21 \times 20 \times 19 \equiv (-1)\times(-2)\times(-3)\times(-4) \pmod{23}$$

$22 \times 21 \times 20 \times 19 \equiv 24 \pmod{23}$

$24 \equiv 1 \pmod{23}$

Using Transitive property

$22 \times 21 \times 20 \times 19 \equiv 1 \pmod{23} \longrightarrow ③$

From ② & ③,

$1 \times (18)! \equiv -1 \pmod{23}$

$18! \equiv -1 \pmod{23} \longrightarrow ④.$

From $(18)! \equiv -1 \pmod{19 \times 23}$

$(18!) \equiv -1 \pmod{437}$

Result

$a \equiv b \pmod{m}$

$a \equiv b \pmod{n}$

$\Rightarrow a \equiv b \pmod{m \times n}$

Scanned with CamScanner

(5) Prove that an integer $n>1$ is prime iff

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

Proof:

Let n be any integer >1.

Assume that n is prime.

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

Since n is prime, by wilsons thm $(n-1)! \equiv -1 \pmod{n}$

$\Rightarrow (n-2)!\,(n-1) \equiv -1 \pmod{n} \longrightarrow (1)$

But $(n-1) \equiv -1 \pmod{n} \longrightarrow (2)$

Sub (2) in (1)

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

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

Conversely assume that $(n-2)! \equiv 1 \pmod{n}$

To prove n is prime.

Suppose n is not a prime.

Then $n = ap$ where $1 < a, p < n$.

p is prime

Also $p \leq (n-2)$.

p/n and $n / (n-2)! - 1$ (using our assumption)

$\Rightarrow p / (n-2)! - 1$

Scanned with CamScanner

$\Rightarrow P/_0 \quad \left(\because (n-2)! \equiv 1 \pmod n \right)$

$\Rightarrow (n-2)! - 1 \equiv 0 \pmod n$.

Which is a $\Rightarrow\Leftarrow$ to P is prime.

$\therefore$ n is prime.

H/P.

Homework

① What is the remainder when $(22)!$ is divided by 23.

② What is the remainder when $(52)!$ is divided by 53.

Defn [Multiplicative Function]

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

Note

* Euler phi function (ϕ), Tau function (τ), Sigma function (σ) are multiplicative functions.

Scanned with CamScanner

Defn [Euler Phi function]

Let m be the positive integer. Then Euler phi function denotes the number of positive integers $\leq m$ and relatively prime to m. It is denoted by $\phi(m)$

Defn [Tau Function] (or) [τ function]

Let m be a positive integer Then $\tau(m)$ denote the number of positive divisors of m.

$\tau \to$ Tau

Defn [Sigma Function] (or) [σ- function].

Let m be a +ve integer. Then $\sigma(m)$ denote the sum of positive divisors of m

$$\sigma(m) = \sum_{d/m} d$$

Example.

Suppose $m = 6$.

$\gcd(1,6) = 1$

$\gcd(2,6) = 2$

$\gcd(3,6) = 3$.

$\gcd(4,6) = 2$

$\gcd(5,6) = 1$

$\gcd(6,6) = 6$.

$\therefore \phi(m) = 2$

$\tau(m) = 4$ ($\because$ 1, 2, 3, 6 are +ve divisors of 6)

$\sigma(m) = \sum_{d/m} d$

Scanned with CamScanner

$\therefore \sigma(6) = 1+2+3+6$
$= 12.$

Important Formulae.

Suppose $m = P_1^{a_1} \times P_2^{a_2} \times \dots \times P_k^{a_k}$ is canonical decomposition of m. where $P_1, P_2, \dots, P_k$ are primes.

Then

$$\boxed{\begin{aligned} \phi(m) &= m \times \left(1-\tfrac{1}{P_1}\right) \times \left(1-\tfrac{1}{P_2}\right) \times \dots \times \left(1-\tfrac{1}{P_k}\right) \\ \tau(m) &= (a_1+1) \times (a_2+1) \times \dots \times (a_k+1) \\ \sigma(m) &= \left(\frac{P_1^{a_1+1}-1}{P_1-1}\right) \times \left(\frac{P_2^{a_2+1}-1}{P_2-1}\right) \times \dots \left(\frac{P_k^{a_k+1}-1}{P_k-1}\right) \end{aligned}}$$

Problems

(1) If $n = 2^k$ then prove that Euler phi function of n is $\frac{n}{2}$.

U.Q 2m

Soln.

Given $n = 2^k$ is a canonical decomposition of n.

$\Rightarrow$ Euler phi function $\phi(n) = n \times (1-\tfrac{1}{2})$
$= n \times \tfrac{1}{2}$
$= n/2.$

---

(2) Compute the Euler phi function and Tau functions for 18 and 11.

Soln

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

$\therefore 18 = 2 \times 3^2$

$11 = 11^1.$

$\therefore \phi(18) = 18 \times (1-\tfrac{1}{2}) \times (1-\tfrac{1}{3})$
$= 18 \times \tfrac{1}{2} \times \tfrac{2}{3}$
$= 6.$

$\phi(11) = 11 \times (1-\tfrac{1}{11})$
$= 11 \times \tfrac{10}{11} = 10$

Scanned with CamScanner

$18 = 2^1 \times 3^2$

$11 = 11^1.$

$\therefore \tau(18) = (1+1) \times (2+1)$

$= 2 \times 3$

$= 6.$

$\tau(11) = (1+1)$

$= 2.$

Problem (3) A +ve integer p is prime iff $\phi(p) = p-1$.

Soln. Let p be any +ve integer.

Assume that p is prime.

Then $1, 2, 3, 4, \ldots, (p-1)$ are +ve integers which are relatively prime to p.

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

Conversely assume that $\phi(p) = p-1$.

To prove p is prime.

Suppose p is not a prime.

Then $\exists$ a divisor d with d/p where $1 < d < p$.

Since there are exactly $(p-1)$ positive integers $< p$, d is one of them.

Also $\gcd(d, p) \neq 1$.

$\Rightarrow \phi(p) < (p-1).$

Scanned with CamScanner

which is a $\Rightarrow\Leftarrow$ to $\phi(p) = p-1$.

$\therefore$ p is prime

H/p.

Problem ④ Find the σ-function for the following

(i) 18 (ii) 13.

Soln.

(i) +ve Devisors of 18 are 1, 2, 3, 6, 9, 18.

$\therefore \sigma(18) = 1+2+3+6+9+18$

$= 39.$

(ii) +ve Devisors of 13 are 1, 13.

$\therefore \sigma(13) = 1+13$

$= 14.$

Homework.

① Find $\phi(m)$, $\tau(m)$ and $\sigma(m)$ for the following

(i) $m = 17$

(ii) $m = 20$

(iii) $m = 21$.

② Compute $\tau(36)$ and $\sigma(36)$

③ Compute $\tau(6120)$, $\sigma(6120)$, $\phi(6120)$

Scanned with CamScanner

Theorem ② **Euler Theorem.**

Let m be a +ve integer and a be any integer with $\gcd(a,m)=1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$

Proof:- Given m is a +ve integer and $a \in \mathbb{Z}$ with $\gcd(a,m)=1$.

We know that there are exactly $\phi(m)$ positive integers which are relatively prime to m.

List them by $r_1, r_2, \ldots, r_{\phi(m)}$

Claim ① $\gcd(ar_i, m)=1$ for every i.

Suppose ~~gcd(ar)~~, $\gcd(ar_i, m) > 1$.

Let 'p' be a prime factor of $\gcd(ar_i, m)$.

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

Now $p \mid ar_i \Rightarrow p \mid a$ or $p \mid r_i$. $\left[p \mid ab \Rightarrow p \mid a \text{ or } p \mid b. \right]$

If $p \mid a$ then $p \mid \gcd(a,m)=1$ which is a $\Rightarrow\Leftarrow$.

If $p \mid r_i$ then $p \mid \gcd(r_i, m)=1$ which is a $\Rightarrow\Leftarrow$.

$\therefore \gcd(ar_i, m)=1$ for every i.

Hence the claim ①.

Claim ② $a^{\phi(m)} \equiv 1 \pmod{m}$.

By claim ①, $\gcd(ar_i, m)=1$ for every i.

$\Rightarrow ar_i, m$ are relatively prime for every i.

Scanned with CamScanner

$$\Rightarrow \quad ar_1 \equiv r_1 \pmod m$$

$$ar_2 \equiv r_2 \pmod m$$

$$\vdots$$

$$ar_{\phi(m)} \equiv r_{\phi(m)} \pmod m.$$

Multiplying above congruences

$$(ar_1) \times (ar_2) \times \dots \times (ar_{\phi(m)}) \equiv r_1 \times r_2 \times \dots \times r_{\phi(m)} \pmod m \longrightarrow ①$$

Since $\gcd(r_i, m) = 1$, $\gcd(r_1 \times r_2 \times \dots \times r_{\phi(m)}, m) = 1$.

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

Hence the claim ②

H/p.

Theorem ③ <u>Fermat's</u> <u>Little</u> <u>Theorem</u>.

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

<u>Proof</u>

Prove Euler Theorem.

Apply Euler Theorem with, $m = p$

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

But $\phi(p) = (p-1)$ ($\because$ p is a prime)

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

H/p.

Scanned with CamScanner

Problems

① Find the remainder when 245^{1040} is divided by 18.

U.Q

8m Soln.

We know that $245 \equiv 11 \pmod{18}$

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

Since $\gcd(11, 18) = 1$, By Euler Thm $11^{\phi(18)} \equiv 1 \pmod{18} \longrightarrow ②$

But $\phi(18) = 18 \times (1 - 1/2) \times (1 - 1/3)$

$= 18 \times 1/2 \times 2/3$

$\boxed{\phi(18) = 6}$

Sub $\phi(18) = 6$ in ②

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

$$\Rightarrow (11^6)^{173} \equiv 1^{173} \pmod{18}$$

$$\Rightarrow (11)^{1038} \equiv 1^{173} \pmod{18}$$

$$\Rightarrow (11)^{1038} \equiv 1 \pmod{18}$$

$$\begin{array}{r} 173 \\ 6 \overline{)1040} \end{array}$$

Multiply by $(11)^2$ both sides

$$\Rightarrow (11)^{1038} \cdot (11)^2 \equiv 11^2 \pmod{18}$$

$$\Rightarrow 11^{1040} \equiv 121 \pmod{18}$$

$$121 \equiv 13 \pmod{18}$$

$$\begin{array}{r} 6 \\ 18 \overline{)121} \\ 108 \\ \hline 13 \end{array}$$

∴ By Trans. prop $11^{1040} \equiv 13 \pmod{18} \longrightarrow ③$

From ① and ③, $(245)^{1040} \equiv 13 \pmod{18}$

∴ Required remainder is '13'

Scanned with CamScanner

② If $\gcd(a,35)=1$ then show that $a^{24} \equiv 1 \pmod{35}$.

Soln:

$$5 \,\underline{|\, 35}$$
$$7.$$

$\therefore 35 = 5 \times 7$.

$$\therefore \phi(35) = 35 \times \left(1-\tfrac{1}{5}\right) \times \left(1-\tfrac{1}{7}\right)$$

$$= 35 \times \tfrac{4}{5} \times \tfrac{6}{7}$$

$$= 24.$$

By Euler thm, $a^{\phi(m)} \equiv 1 \pmod m$. where $\gcd(a,m)=1$.

Appy Euler thm with $m=35$,

$$a^{24} \equiv 1 \pmod{35}.$$

---

③ Using Fermat's theorem prove that $13 \,/\, 11^{12n+6}+1$ for $n \geq 0$.

Soln:

Fermats thm $a^{p-1} \equiv 1 \pmod p$ where p is prime, $p \not/ a$.

To prove: $13 \,/\, 11^{12n+6}+1$.

It is enough to prove $11^{12n} \cdot 11^{6} \equiv -1 \pmod{13}$.

We know that

13 is a prime and $13 \not/ 11$.

$\therefore$ By Fermats thm, $11^{12} \equiv 1 \pmod{13}$

$\Rightarrow 11^{12n} \equiv 1 \pmod{13} \longrightarrow ①$; $n \geq 0$.

Scanned with CamScanner

$11^2 = 121 \equiv 4 \pmod{13}$

$$\begin{array}{r} 9 \\ 13 \overline{)121} \\ 117 \\ \hline 4 \end{array}$$

i.e) $11^2 \equiv 4 \pmod{13}$

$\therefore (11^2)^3 \equiv 4^3 \pmod{13}$

$$\begin{array}{r} 4 \\ 13 \overline{)64} \\ 52 \\ \hline 12 \end{array}$$

$4^3 \equiv 12 \pmod{13}$

By Trans. prop $(11^2)^3 \equiv 12 \pmod{13}$

i.e) $11^6 \equiv 12 \pmod{13} \longrightarrow (2)$

From (1) & (2)

$11^{12n} \cdot 11^6 \equiv 1 \cdot 12 \pmod{13}$

$11^{12n+6} \equiv 12 \pmod{13}$

$11^{12n+6} \equiv -1 \pmod{13}$

H/p.

Scanned with CamScanner

③ Find the remainder when 24^{1947} is divided by 17.

Soln:

$24 \equiv 7 \pmod{17}$

$\Rightarrow 24^{1947} \equiv 7^{1947} \pmod{17} \longrightarrow ①$

Fermats Thm: $a^{p-1} \equiv 1 \pmod{p}$ where p is prime $p \nmid a$.

Apply Fermats thm with $p=17$, $a=7$.

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

$$\begin{array}{r|l} & 121 \\ \hline 16 & 1947 \\ & 1936 \\ \hline & 11 \end{array}$$

$(7^{16})^{121} \equiv 1^{121} \pmod{17}$.

$7^{1936} \equiv 1 \pmod{17}$.

Multiply by 7^{11} both sides

$7^{1936} \cdot 7^{11} \equiv 7^{11} \pmod{17}$

$7^{1947} \equiv 7^{11} \pmod{17} \longrightarrow ②$

From ① and ②, $24^{1947} \equiv 7^{11} \pmod{17} \longrightarrow ③$

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

$\Rightarrow (7^2)^5 \equiv (-2)^5 \pmod{17}$

$\Rightarrow 7^{10} \equiv -32 \pmod{17}$.

$-32 \equiv 2 \pmod{17}$

Trans. property $\Rightarrow 7^{10} \equiv 2 \pmod{17}$

Multiply by 7 both sides

$7^{11} \equiv 2 \times 7 \pmod{17}$

$7^{11} \equiv 14 \pmod{17}. \longrightarrow ④$

From ③ and ④

$(24)^{1947} \equiv 14 \pmod{17}$. Req. remainder is 14.

Scanned with CamScanner

Problem: Compute $\tau(6120)$ and $\sigma(6120)$.

Soln

$$\begin{array}{r|l}
2 & 6120 \\ \hline
2 & 3060 \\ \hline
2 & 1530 \\ \hline
3 & 765 \\ \hline
3 & 255 \\ \hline
5 & 85 \\ \hline
 & 17.
\end{array}$$

$$\therefore \quad 6120 = 2^3 \times 3^2 \times 5^1 \times 17^1.$$

$$\tau(6120) = (3+1) \times (2+1) \times (1+1) \times (1+1)$$

$$= 4 \times 3 \times 2 \times 2$$

$$= 48$$

$$\sigma(6120) = \left(\frac{2^{3+1}-1}{2-1}\right) \times \left(\frac{3^{2+1}-1}{3-1}\right) \times \left(\frac{5^{1+1}-1}{5-1}\right) \times \left(\frac{17^{1+1}-1}{17-1}\right)$$

$$= \left(\frac{2^4-1}{2-1}\right) \times \left(\frac{3^3-1}{3-1}\right) \times \left(\frac{5^2-1}{5-1}\right) \times \left(\frac{17^2-1}{17-1}\right)$$

$$= \left(\frac{15}{1}\right) \times \left(\frac{26}{2}\right) \times \left(\frac{24}{4}\right) \times \left(\frac{288}{16}\right)$$

$$\cancel{= \frac{2765040}{128}}$$

$$= 15 \times 13 \times 6 \times 18$$

$$= 21060.$$

Scanned with CamScanner

Problem (U.Q) 16m.

Let n be a +ve integer with canonical decomposition

$$n = p_1^{a_1} \times p_2^{a_2} \times \dots p_k^{a_k}.$$

Derive the formula for Tau and Sigma functions.

Hence evaluate $\tau(n)$ and $\sigma(n)$ for $n = 1980$.

Soln:-

Let $n = p_1^{a_1} \times p_2^{a_2} \times \dots \times p_k^{a_k}$ be a canonical decomposition of n.

$$\tau(n) = \tau\left(p_1^{a_1} \times p_2^{a_2} \times \dots \times p_k^{a_k}\right)$$

$$= \tau(p_1^{a_1}) \times \tau(p_2^{a_2}) \times \dots \times \tau(p_k^{a_k}) \quad (\because \tau \text{ is multiplicative})$$

$$= (a_1+1) \times (a_2+1) \times \dots \times (a_k+1)$$

$(\because \tau(p_1^{a_1})$ = no. of +ve divisors of $p_1^{a_1}$

+ve divisors of $p_1^{a_1}$ are $1, p, p^2, \dots, p^{a_1})$.

$$\sigma(n) = \sigma\left[p_1^{a_1} \times p_2^{a_2} \times \dots p_k^{a_k}\right]$$

$$= \sigma(p_1^{a_1}) \times \sigma(p_2^{a_2}) \times \dots \times \sigma(p_k^{a_k}) \quad (\because \sigma \text{ is multiplicative}$$

$$= \left(\frac{p_1^{a_1+1}-1}{p_1-1}\right) \times \left(\frac{p_2^{a_2+1}-1}{p_2-1}\right) \times \dots \times \left(\frac{p_k^{a_k+1}-1}{p_k-1}\right)$$

$(\because \sigma(p_1^{a_1})$ = sum of +ve devisors of $p_1^{a_1}$

$$= 1 + p_1 + p_1^2 + \dots + p_1^{a_1}$$

$$= \frac{p_1^{a_1+1}-1}{p_1-1})$$

Formula : $1 + r + r^2 + \dots + r^n = \dfrac{r^{n+1}-1}{r-1}$ when $r > 1$)

Scanned with CamScanner

when $n = 1980$

$$\begin{array}{r|l} 2 & 1980 \\ \hline 2 & 990 \\ \hline 3 & 495 \\ \hline 3 & 165 \\ \hline 5 & 55 \\ \hline & 11 \end{array}$$

$$\therefore \quad 1980 = 2^2 \times 3^2 \times 5^1 \times 11^1$$

$$\tau(n) = (2+1) \times (2+1) \times (1+1) \times (1+1)$$

$$= 3 \times 3 \times 2 \times 2$$

$$\tau(1980) = 36.$$

$\cancel{\sigma(1980) =}$ $$\sigma(n) = \left(\frac{P_1^{a_1+1} - 1}{P_1 - 1}\right) \times \left(\frac{P_2^{a_2+1} - 1}{P_2 - 1}\right) \times \cdots \times \left(\frac{P_k^{a_k+1} - 1}{P_k - 1}\right)$$

$$= \left(\frac{2^{2+1} - 1}{2 - 1}\right) \times \left(\frac{3^{2+1} - 1}{3 - 1}\right) \times \left(\frac{5^{1+1} - 1}{5 - 1}\right) \times \left(\frac{11^{1+1} - 1}{11 - 1}\right)$$

$$= \left(\frac{2^3 - 1}{2 - 1}\right) \times \left(\frac{3^3 - 1}{3 - 1}\right) \times \left(\frac{5^2 - 1}{5 - 1}\right) \times \left(\frac{11^2 - 1}{11 - 1}\right)$$

$$= \frac{7}{1} \times \frac{26}{2} \times \frac{24}{4} \times \frac{120}{10}.$$

$$= 7 \times 26 \times 3 \times 12$$

$$\sigma(1980). \quad = 6552.$$

Problem Verify that $\phi(\sigma(666)) = 2\,\phi(666)$

Soln.

$$\begin{array}{r|l} 2 & 666 \\ \hline 3 & 333 \\ \hline 3 & 111 \\ \hline & 37 \end{array}$$

$\therefore\ 666 = 2^1 \times 3^2 \times 37^1$ is canonical decomposition.

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

$$= 666 \times \tfrac{1}{2} \times \tfrac{2}{3} \times \tfrac{36}{37}.$$

$$= 216. \longrightarrow (1)$$

$$\sigma(666) = \left(\frac{2^{1+1}-1}{2-1}\right) \times \left(\frac{3^{2+1}-1}{3-1}\right) \times \left(\frac{37^{1+1}-1}{37-1}\right)$$

$$= \left(\frac{2^2-1}{2-1}\right) \times \left(\frac{3^3-1}{3-1}\right) \times \left(\frac{37^2-1}{37-1}\right)$$

$$= \left(\frac{3}{1}\right) \times \left(\frac{26}{2}\right) \times \left(\frac{1368}{36}\right)$$

$$\cancel{\frac{106782}{78}} = 3 \times 13 \times 38$$

$$\sigma(666) = 1482$$

$$\therefore\ \phi(\sigma(666)) = \phi(1482)$$

$$\begin{array}{r|l} 2 & 1482 \\ \hline 3 & 741 \\ \hline 13 & 247 \\ \hline & 19 \end{array}$$

$\therefore\ 1482 = 2^1 \times 3^1 \times 13^1 \times 19^1$ is canonical decomposition of 1482.

$$\therefore\ \phi(1482) = 1482 \times \left(1-\tfrac{1}{2}\right) \times \left(1-\tfrac{1}{3}\right) \times \left(1-\tfrac{1}{13}\right) \times \left(1-\tfrac{1}{19}\right)$$

$$= 1482 \times \tfrac{1}{2} \times \tfrac{2}{3} \times \tfrac{12}{13} \times \tfrac{18}{19}$$

$$= 1482 \times \frac{4 \times 18}{13 \times 19}$$

$$\phi(\sigma(666)) = \phi(1482) \qquad = 6 \times 4 \times 18$$

$$= 432. \longrightarrow (2)$$

Scanned with CamScanner

From ① and ②

$$\phi\left(\sigma(666)\right) = 432 = 2\,\phi(666)$$

Hence the verification.

Problem: Verify that $\phi(665) = 2\,\phi(666)$.

Soln.

$$\begin{array}{r|l} 5 & 665 \\ \hline 7 & 133 \\ \hline & 19 \end{array} \qquad\qquad \begin{array}{r|l} 2 & 666 \\ \hline 3 & 333 \\ \hline 3 & 111 \\ \hline & 37. \end{array}$$

$\therefore\ 665 = 5^1 \times 7^1 \times 19^1$

$\therefore\ 666 = 2^1 \times 3^2 \times 37^1$

$$\phi(665) = 665 \times \left(1-\tfrac{1}{5}\right) \times \left(1-\tfrac{1}{7}\right) \times \left(1-\tfrac{1}{19}\right)$$

$$= 665 \times \tfrac{4}{5} \times \tfrac{6}{7} \times \tfrac{18}{19}$$

$$= 4 \times 6 \times 18$$

$$= 432. \longrightarrow ①$$

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

$$= 666 \times \tfrac{1}{2} \times \tfrac{2}{3} \times \tfrac{36}{37}.$$

$$= 216. \longrightarrow ②$$

$\phi(665) = 432$ (using ①)

$= 2(216)$

$= 2\,\phi(666)$ (using ②)

Homework

① Verify that $\sigma(668) = 2\sigma\left(\phi(668)\right)$

② Verify that $\sigma\left(\phi(667)\right) = 2\sigma(667)$.

Scanned with CamScanner