Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

MA8551 ALGEBRA AND NUMBER THEORY

UNIT-V

CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS

WILSON'S THEOREM

The result known as Wilson's theorem was only conjectured (or guessed) by the British mathematician Jon Wilson (1741-1793). But the first proof was given by Langrange in 1770. He observed the converse is also true.

Theorem (Wilson's theorem)

If p is prime, then (p-1)! ≡ -1(mod p)

Proof

We have to prove (p-1)! ≡-1(mod p)

We have p=2, (p-1)!=(2-1)!=1≡-1(mod 2)

So, the theorem is true when p=2

Now let p>2 and let a be a positive integer such that $1 \le a \le p-1$

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

Then the congruence ax≡1(mod p) has a solution of congruence modulo p.

$\therefore$ aa′≡1(mod p), where $1 \le a' \le p-1$

$\therefore$ a, a′ are inverse of each other modulo p

If a′=a, then a.a≡1(mod p) $\Rightarrow a^2-1 \equiv 0 \pmod p$

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

Since a<p, if p|a+1 then a=p-1

If p|a-1, then a-1=0 $\Rightarrow$ a=1

$\therefore$ a=1 or p-1 if a=a′

i.e., 1 and p-1 are their own inverses.

If a′≠a, excluding, 1 and p-1, the remaining p-3 residues 2,3,4,…(p-3),(p-2) can be grouped in to $\frac{p-3}{2}$ pairs of the type a, a′ such that

aa′≡1(mod p)

Multiplying all these pairs together we get

2.3.4. . . . .(p-3)(p-2) ≡1(mod p)

$\Rightarrow$ 1.2.3.4. . . . .(p-2)(p-1) ≡p-1(mod p)

$\Rightarrow$ (p-1)!≡ -1(mod p)

Hence the theorem.

This can be rewritten as (p-1)!+1≡ 0(mod p)

$\Rightarrow$ p|(p-1)!+1 which is the result suggested by Wilson.

Course/Branch: BE/CSE	**Year / Semester** : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	**Subject Name** :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	**Unit Name:** CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

Problem

Show that 18!+1 is divisible by 437

Solution

By Wilson's theorem is (p-1)!+1 is divisible by a prime p.

Hence 437 is not a prime and 437=19.23, where 19 and 23 are primes.

Since 19 is a prime $(19-1)!+1 = 18!+1$ is divisible by 19

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

Since 23 is a prime $(23-1)!+1 = 22!+1$ is divisible by 23

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

$\Rightarrow 22.21.20.19.81! + 1 \equiv 0 \pmod{23}$

But $22 \equiv -1 \pmod{23}$, $21 \equiv -2 \pmod{23}$, $20 \equiv -3 \pmod{23}$, $19 \equiv -4 \pmod{23}$

$22.21.20.19 \equiv (-1)(-2)(-3)(-4) \pmod{23}$

$\equiv 24 \pmod{23}$

$\equiv 1 \pmod{23}$

Multiplying by 18!, we get

$22.21.20.19.18! \equiv 18! \pmod{23}$

$22.21.20.19.18! + 1 \equiv 18! + 1 \pmod{23}$

But L.H.S is $22!+1 \equiv 0 \pmod{23}$

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

$\therefore$ $18! + 1$ is divisible by 19 and 23

$\Rightarrow$ $18! + 1$ is divisible by lcm [19, 23] = 437

$\Rightarrow 18! + 1 \equiv 0 \pmod{437}$

Problem

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

Solution

Here p = 71 is a prime

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

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

But $70! = 70.69.68.67.66.65.64.63!$

Now $70 \equiv -1 \pmod{71}$ $69 \equiv -2 \pmod{71}$

$68 \equiv -3 \pmod{71}$ $67 \equiv -4 \pmod{71}$

$66 \equiv -5 \pmod{71}$ $65 \equiv -6 \pmod{71}$

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

$\therefore$ $70.69.68.67.66.65.64 \equiv (-1)(-2)(-3)(-4)(-5)(-6)(-7) \pmod{71}$

$\equiv -5040 \pmod{71}$

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

$\equiv 1 \pmod{71}$

```
    71
71 | 5040
     497
     ---
      70
      71
```

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

Multiplying both side by 63!, we get -1

$70.69.68.67.66.65.64.63! \equiv 63! \pmod{71}$

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

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

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

Problem

If p is a prime number of the form 4m+1, where m is a positive integer, prove that $(2m!)^2 + 1 \equiv 0 \pmod{p}$

Solution

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

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

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

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

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

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

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

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

But $4m + 1 = p$

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

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

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

. . . . . .

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

Multiplying together we get

$4m(4m-1)(4m-2)\ldots(4m-(2m-1)) \equiv (-1)(-2)(-3)\ldots(-2m) \pmod{p}$

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

Multiplying both sides by (2m)! we get

$4m(4m-1)(4m-2)\ldots(4m-(2m-1))2m! \equiv 2m!.2m! \pmod{p}$

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

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

$\Rightarrow 0 \equiv (2m!)^2+1 \pmod{p}$ [using (I)]

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

Problem

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

Solution

Given n is a positive integer such that

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

Course/Branch: BE/CSE	**Year / Semester** : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	**Subject Name** :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	**Unit Name:** CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

To prove n is prime.
Suppose n is not prime, then n is a composite number.
$\therefore$ n = a.b, where a, b are integer between 1 and n.
i.e., $1<a,b<n$
Since $a|ab$ and $a|n$

$n|[(n-1)!+1]$ by (1)
$a|[(n-1)!+1]$

But $1<a<n$, so, s is one of the integer 2,3,4,. . .,(n-1)
$\therefore$ a divides the product 2.3.4. . . . .(n-1) = (n-1)!
Thus, $a|[(n-1)!+1]$ and $a|(n-1)!$
$\Rightarrow$ $a \mid [(n-1)!+1-(n-1)!] \Rightarrow a|1$
which is a contradiction, since $1<a$
$\therefore$ our assumption n is composite is wrong.
Hence n is prime.

Problem
If p is a prime, prove that
(p-1)(p-2)(p-3). . .(p-k) $\equiv$(-1)^k k! (mod p) where $1 \le k < p$.
Solution
Given p is a prime.
Now
$p-1 \equiv -1 \pmod p$
$p-2 \equiv -2 \pmod p$
$p-3 \equiv -3 \pmod p$
. . . . . .
$p-k \equiv -k \pmod p$
Multiplying together we ge
$(p-1)(p-2)(p-3)\ldots(p-k) \equiv (-1)(-2)(-3)\ldots(-k) \pmod p$
$\equiv (-1)^k (1.2.3.4.\ldots.k) \pmod p$
$\equiv (-1)^k k! \pmod p$

Problem
If x = 1.3.5. . . . .(p-1), where p is an odd prime, show that

$$x^2 \equiv (-1)^{\frac{p+1}{2}} (\mathrm{mod}\, p)$$

Solution
Given x = 1.3.5. . . . .(p-1), where p is an odd prime
Since p is a prime, by Wilson's theorem

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

$\Rightarrow$ $1.2.3.4.5.....(p-2)(p-1) \equiv -1 \pmod p$

$\Rightarrow$ $(1.3.5.....(p-2))(2.4.6.....(p-1)) \equiv -1 \pmod p$

$\Rightarrow$ $x.(2.4.6.....(p-1)) \equiv -1 \pmod p$

$\Rightarrow$ $x.[(p-(p-2)][p-(p-4)][p-(p-6)].....(p-1) \equiv -1 \pmod p$ (1)

Now $p-(p-2) \equiv -(p-2) \pmod p$

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

. . . . . .

$(p-3) \equiv -3 \pmod p$

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

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

$\therefore$ Multiplying together, we get

$[p-(p-2)][p-(p-4)][p-(p-6)].....(p-1) \equiv (-1)^{\frac{p-1}{2}}.(p-2)(p-4)...3.1 \pmod p$

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

Substituting in (1)

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

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

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

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

FERMAT'S THEOREM

Ancient Chinese mathematicians believed that n is a prime if and only if $2^{n-1} \equiv 1 \pmod n$.

To found that it is true if n is a prime

For example: if n=5, $2^4 \equiv 1 \pmod 5$

But they were incorrect in the conclusion of the converse. It was the French mathematician Fermat who conjectured if p is a prime and p ł a then $p|a^{n-1} - 1$ and communicated to Bernhard with a note that the proof will be send subsequently.

But the first proof was given by the great Swiss mathematician Euler almost a century later.

However this result is known as Fermat's theorem or Fermat's little theorem (in order to distinguish it from Fermat's theorem)

Theorem FERMAT'S LITTLE THEOREM

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

Proof

Given p is prime and a is any integer not divisible by p. i.e., p ł a.

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

Consider the set of integers

1.a, 2.a, 3.a, . . . ,(p-1).a (1)

Suppose ia ≡ 0(mod p), then p|ia

But p ł a ∴ p|i , which is impossible, since i<p

∴ ia ≢ 0(mod p) for i=1,2, . . . ,p-1

So, no term of (1) is zero.

Next we prove they are all distinct

Suppose ia ≡ ja(mod p), where $1 \le i, j \le p-1$

Then (i-j)a ≡ 0(mod p) ⇒p|(i-j)a

Since p ł a , p|(i-j) and i,j<p ⇒ $|i-j| < p$

∴ i-j=0 ⇒ i ≡ j(mod p)

∴ i ≠ j ⇒ ia ≠ ja

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

∴ The least residues (or remainders) of the integers 1.a, 2.a, 3.a, . . . ,(p-1).a is modulo p are the same as the integers 1,2,3, . . . , p-1 in some order.

So, their products are congruent modulo p.

∴ a.2a.3a . . . . .(p-1)a ≡ 1.2.3. . . . .(p-1)(mod p)

⇒ 1.2.3. . . . .(p-1) a^{p-1} ≡ (p-1)! (mod p)

⇒ (p-1)! a^{p-1} ≡ (p-1)! (mod p)

⇒ a^{p-1} ≡ 1 (mod p)

This result a^{p-1} ≡ 1 (mod p) is equivalent to a^p ≡ a (mod p)

Using Fermat's little theorem and properties of congruence we can find remainders of certain number of the form a^m when divided by p.

Problem

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

Solution

We have find the remainder when 2^{1000} is divided by 17

We know 17 is a prime and 17 ł 2

∴ by Fermat's theorem

2^{17-1} ≡ 1 (mod 17)

⇒ 2^{16} ≡ 1 (mod 17)

⇒ $(2^{16})^{62}$ ≡ 1 (mod 17)

⇒ 2^{992} ≡ 1 (mod 17)

```
      62
16 | 1000
     96
     ---
      40
      32
     ---
       4
```

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

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

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

$\Rightarrow 2^{992}.2^8 \equiv 1.1 \pmod{17}$

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

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

Problem

Find the remainder when 193^{183} is divided by 19

Solution

We have the find the remainder when 193^{183} is divided by 19.

We know 19 is prime and 19 ł 193.

$\therefore$ by Fermat's theorem

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

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

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

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

$$\begin{array}{r|l} & 10 \\ \hline 18 & 183 \\ & 180 \\ \hline & 3 \end{array}$$

But $193 \equiv 3 \pmod{19}$

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

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

$\therefore 193^{180}.193^2.193 \equiv 1.9.3 \pmod{19}$

$\Rightarrow 193^{183} \equiv 27 \pmod{19}$

$\Rightarrow 193^{183} \equiv 8 \pmod{19}$ [27=1.19+8]

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

Problem

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

Solution

We have to find the remainder when 15^{1976} is divided by 23.

We know 23 is prime and 23 ł 15.

$\therefore$ by Fermat's theorem

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

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

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

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

$\Rightarrow 15^2 = 225 \equiv 18 \pmod{23}$ [225=9.23+18]

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

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

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

$\equiv 2 \pmod{23}$

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

$\Rightarrow \quad 15^{16} \equiv 16 \pmod{23}$

$\equiv -7 \pmod{23}$

Now $15^{1958}.\ 15^{16}.15^2 = 15^{1976} \equiv 1.(-7)\ (-5) \pmod{23}$

$\Rightarrow \quad 15^{1976} \equiv 35 \pmod{23}$

$\equiv 12 \pmod{23}$

$\therefore$ The remainder is 12 when 15^{1976} is divided by 23.

Problem

Find the remainder when 2^{341} is divided by 341

Solution

We know 341 = 11.31

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

So, by Fermat's theorem

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

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

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

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

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

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

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

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

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

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

$\equiv 1.1.2 \pmod{\text{lcm}[11,31]}$

$\equiv 2 \pmod{341}$

$\therefore$ the remainder is 2 when 2^{341} is divided by 341

Problem

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

Solution

We have to find the remainder when 5^{2003} is divided by 11.

We know 11 is prime and 11 does not divide 5

$\therefore$ by Fermat's theorem

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

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

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

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

Now $\quad 5^3 = 125 \equiv 4 \pmod{11}$

$\therefore \quad 5^{2000}.5^3 \equiv 1.\ 4 \pmod{11}$

$\Rightarrow \quad 5^{2003} \equiv 4 \pmod{11}$

$\therefore$ the remainder is 4 when 5^{2003} is divided by 11.

Problem

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

Solution

We have to find the remainder when 7^{1001} is divided by 17.

We know 17 is a prime and 17 does not divide 7.

$\therefore$ by Fermat's theorem

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

i.e., $\quad 7^{16} \equiv 1 \pmod{17}$

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

i.e., $\quad 7^{992} \equiv 1 \pmod{17}$

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

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

i.e., $\quad 7^8 \equiv 16 \pmod{17}$

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

But $\quad 7 \equiv -10 \pmod{17}$

$$7^{1001} = 7^{992}.7^8.7$$

$$\equiv 1.(-1).(-10) \pmod{17}$$

$$\equiv 10 \pmod{17}$$

$\therefore$ the remainder is 10 when 7^{1001} is divided by 17

Problem

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

Solution

We have 247 = 13.19

Both 13 and 19 are a prime

By Fermat's theorem

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

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

Since $\quad 19 \equiv 0 \pmod{19}$

$\Rightarrow \quad 19^{22} \equiv 0 \pmod{19}$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

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

By Fermat's theorem

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

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

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

$13^{18} + 19^{12} \equiv 1 \pmod{247}$

$\therefore$ the remainder is 1 when $13^{18} + 19^{12}$ is divided by 247,

Problem

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

Solution

We know by Fermat's theorem,

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

$\therefore$ it is true for a = 1, 2, 3, . . . , p-1

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

Adding all these congruences we get

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv (1 + 1 + \ldots + 1) \pmod{p} \quad [p-1 \text{ times } 1]$$
$$\equiv (p - 1) \pmod{p}$$

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

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

Theorem

Let p be a prime and a any integer such the p ł 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

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

i.e., (a, p) = 1

$\therefore$ the congruence $ax \equiv b \pmod{p}$ has a unique solution (1)

By Fermat's theorem

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

So, a^{p-2} is the inverse of a mod p.

Multiplying (1) by a^{p-2}, we get

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

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

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

Hence the theorem.

EULER'S THEOREM

Fermat's theorem is $a^{p-1} \equiv 1 \pmod p$, which is of the form $a^{f(p)} \equiv 1 \pmod p$, where p is a prime. It is natural to extend to the form $a^{f(m)} \equiv 1 \pmod m$, where m is not a prime and (a, m) =1.

Definition - rithmetical Function or Number Theoretic Function

A real (or complex) valued function defined on the set of positive integers N is called an arithmetical function or number theoretic function.

We shall now define a special number theoretic function called ***Euler's Phi function*** or ***Euler Function*** ϕ , named after one of the all time ***great mathematicians Euler***.

Definition

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

$\phi(n)$ = the number of positive integers $\leq$n and relatively prime to n.

This function is called Euler's ϕ-function.

$\phi(2) = 1$, since 1 is the only integer ≤ 2 and prime to it.

$\phi(3) = 2$, since 1,2 are the only integer ≤ 3 and prime to 3.

$\phi(4) = 2$, since 1,3 are the only integer ≤ 4 and prime to 4.

$\phi(5) = 4$, since 1,2,3,4 are the only integer ≤ 5 and prime to 5.

$\phi(6) = 2$, since 1,5 are the only integer ≤ 6 and prime to 6.

$\phi(7) = 6$, since 1,2,3,4,5,6 are the only integer ≤ 7 and prime to 7.

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

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

It is true for any prime p, since 1,2,3, . . . ,p-1 are the positive integer $\leq$p an d prime to p.

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

Theorem Euler's 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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

Let $r_1, r_2, \ldots, r_{\phi(n)}$ be all the positive integer $\leq m$ and relatively prime to m.

Since $r_i - r_j < m$, clearly $r_i \neq r_j \pmod m$ if $i \neq j$

Consider the products $ar_1, ar_2, \ldots, ar_{\phi(n)}$

Since (a, m) = 1,

$$ar_i \neq ar_j \pmod m \text{ if } i \neq j$$

we find $ar_1, ar_2, \ldots, ar_{\phi(n)}$ mod m are distinct.

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

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

$\therefore$ $p|ar_i$ and $p|m$

$\Rightarrow$ $p|a$ or $p|r_i$ and $p|m$

If $p|r_i$ and $p|m$ then $(r_i, m) \neq 1$, a contradiction.

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

which is again contradiction.

$\therefore$ $(ar_i, m) =1$, i=1,2,3, . . . , $\phi(m)$

$\therefore$ the $\phi(m)$ least residues $ar_1, ar_2, \ldots, ar_{\phi(m)}$ modulo m are distinct and relatively prime to m.

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

$\therefore$ the product $ar_1.ar_2. \ldots .ar_{\phi(m)} \equiv r_1r_2. \ldots .r_{\phi(m)} \pmod m$

$\Rightarrow$ $a^{\phi(m)} r_1r_2. \ldots .r_{\phi(m)} \equiv r_1r_2. \ldots .r_{\phi(m)} \pmod m$

Since each r_i is relatively prime to m,

$(r_1r_2. \ldots .r_{\phi(m)}, m) = 1.$

We get

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

Hence the theorem.

Note

We can deduce Fermat's theorem. If p is a prime $\phi(p) = p-1$.

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

Definition - 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

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

Theorem

Let f be a multiplicative function and n be a positive integer with canonical decomposition $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$

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

Proof

We prove by induction on the number of distinct primes k.

If k=1, then $n = p_1^{\alpha_1}$ and $f(n) = f(p_1^{\alpha_1})$

Which is trivially true.

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

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

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

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}.p_{k+1}^{\alpha_{k+1}}$$

Since $(p_1^{\alpha_1}, p_2^{\alpha_2}..., p_k^{\alpha_k}, p_{k+1}^{\alpha_{k+1}}) = 1$ and f is multiplicative,

$$f(p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}.p_{k+1}^{\alpha_{k+1}}) = f(p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k})f(p_{k+1}^{\alpha_{k+1}})$$
$$= f(p_1^{\alpha_1})f(p_2^{\alpha_2})..f(p_k^{\alpha_k})f(p_{k+1}^{\alpha_{k+1}})$$

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.

We shall now prove that ϕ is multiplicative.

Theorem

Euler function ϕ is multiplicative.

Proof

Let m and n be positive integer such that (m, n)=1

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

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

1	m+1	2m+1	3m+1	...	(n-1)m+1
2	m+2	2m+2	3m+2	...	(n-1)m+2
3	m+3	2m+3	3m+3	...	(n-1)m+3
.	.				
.	.			...	
.	.				
r^{th} row $\rightarrow$ r	m+r	2m+r	3m+r	...	(n-1)m+r

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

. .
. . …
. .
n m+n 2m 3m … mn

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

This means that d is a factor of every element in the 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 element in the array relatively prime to mn come from the r^{th} row only if (r,m)=1.

Since r<m and relatively prime to m, we find there are ϕ(m) such integer r and have ϕ(m) such rows.

Now let us consider the r^{th} row is

r m+r 2m+r 3m+r … (n-1)m+r

When they are divided by n, the remainders are 0, 1, 2, . . . ,n-1 in some order of which ϕ(n) are relatively prime to n.

Therefore, exactly ϕ(n) elements in the r^{th} row are relatively prime to n and hence to mn.

Thus there are ϕ(m) rows containing positive integers relatively prime to mn and each row contain ϕ(n) element relatively prime to n.

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

That is ϕ(mn)= ϕ(m)ϕ(n)

Hence ϕ is multiplicative function.

Theorem

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

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

Proof

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

= number of positive integer $\leq p^\alpha$ - number of positive integer $\leq p^\alpha$ and not relatively prime to it

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

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

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

$\therefore$ the number of such number = $p^{\alpha-1}$

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

Theorem

Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ ***be the canonical decomposition of the positive integer n. Then*** $\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right)$.

Proof

Given the canonical decomposition of the positive integer

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

Since ϕ is multiplicative,

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

$$= p_1^{\alpha_1}\left(1-\frac{1}{p_1}\right)p_2^{\alpha_2}\left(1-\frac{1}{p_2}\right)...p_k^{\alpha_k}\left(1-\frac{1}{p_k}\right) \quad [\because \phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right)]$$

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

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

This formula is useful to find the number of primes $\le n$ and relatively prime to n for lange values of n.

Problem

Find $\phi(1105)$ ***and*** $\phi(7!)$

Solution

We have 1105 = 5.13.17

$\therefore$ $\phi(1105) = \phi(5.13.17)$

$= \phi(5).\phi(13).\phi(17)$

$= 4.12.16$ [$\because \phi(p)=p-1$, if p is prime]

$= 768$

5	1105
13	221
	17

We have 7! = 5040

$= 2^4.3^2.5.7$

$\therefore$ $\phi(7!) = \phi(2^4.3^2.5.7)$

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

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

$= 2^4\left(1-\frac{1}{2}\right)3^2\left(1-\frac{1}{3}\right).4.6$

$= 2^4\left(\frac{1}{2}\right)3^2\left(\frac{2}{3}\right).4.6 = 2^3.3.2.4.6 = 1152$

Problem

Compute $\phi(6860)$

Solution

2	6860
2	3430
5	1715
7	343
7	49
	7

We have $6860 = 2^2.5.7^3$

$\therefore \quad \phi(6860) = \phi(2^5.5.7^3)$

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

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

$= 2^2\left(\frac{1}{2}\right).4.\ 7^3\left(\frac{6}{7}\right)$

$= 2.4.7^2.6 = 2352$

Problem

Find the positive integer n such that $\phi(n) = 6$.

Solution

Given $\phi(n) = 6$.

We have to find possible n by trial and error

$\phi(6) = \phi(2.3) = \phi(2).\phi(3) = 1.2 \neq 6.$

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

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

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

$\phi(10) = \phi(2.5) = \phi(2).\phi(5) = 1.4 = 4 \neq 6$

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

$\phi(12) = \phi(2^2.3) = \phi(2^2).\phi(3) = 2^2\left(1-\frac{1}{2}\right).2 = 2^2\left(\frac{1}{2}\right).2 = 4 \neq 6$

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

$\phi(14) = \phi(2.7) = \phi(2).\phi(7) = 1.6 = 6 \quad \therefore$ n=14

$\phi(15) = \phi(3.5) = \phi(3).\phi(5) = 2.4 = 8 \neq 6$

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

$\phi(17) = 16 \neq 6$

$\phi(18) = \phi(2.3^2) = \phi(2).\phi(3^2) = 1.6 = 6 \quad \therefore$ n=18

$\therefore$ the only possible values of n are 7, 9, 14, 18.

Problem

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

Solution

Given $n=2^k$.

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

Problem

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

Solution

Given $\phi(2^{2k+1})$

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

Problem

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

Solution

We have 437 = 19.23, where 19 and 23 are a prime.

$\phi(437) = \phi(19.23) = \phi(19).\phi(23) = 18.22 = 396$

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

$2^{\phi(437)} \equiv 1 \pmod{437}$

$\Rightarrow \quad 2^{396} \equiv 1 \pmod{437}$

$\Rightarrow \quad (2^4)^{99} \equiv 1 \pmod{437}$

$\Rightarrow \quad (16)^{99} \equiv 1 \pmod{437}.$

Problem

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

Using Euler's theorem find the remainder when 245^{1040} is divided by 18

Solution

We have to find the remainder when 245^{1040} is divided by 18.

Here $a = 245 = 5.7^2$ and $m = 18 = 2.3^2$

$\therefore$ $(a, m) = (245, 18) = 1$

Hence by Euler's theorem

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

$\Rightarrow$ $245^{\phi(18)} \equiv 1 \pmod{18}$

But $\phi(18) = \phi(2.3^2) = \phi(2).\phi(3^2) = 1.3^2\left(1-\frac{1}{3}\right) = 3^2\left(\frac{2}{3}\right) = 6.$

$\therefore$ $245^6 \equiv 1 \pmod{18}$

$\Rightarrow$ $(245^6)^{173} \equiv 1^{173} \pmod{18}$

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

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

$\Rightarrow$ $(245)^2 \equiv 11^2 \pmod{18}$

$\Rightarrow$ $(245)^2 \equiv 121 \pmod{18}$ $[\because 121 = 6.18 + 13]$

$\Rightarrow$ $(245)^2 \equiv 13 \pmod{18}$

$\therefore$ $245^{1040} = 245^{1038}.245^2$

$\Rightarrow$ $245^{1040} \equiv 1.13 \pmod{18}$

$\Rightarrow$ $245^{1040} \equiv 13 \pmod{18}$

$\therefore$ the remainder is 13 when 245^{1040} is divided by 18.

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

Problem

Find the last two digits of 273^{1961}.

Solution

The last two digits are the remainder when 273^{1961} is divided by 100.

$273 \equiv 73 \pmod{100}$

$\therefore$ $273^{1961} \equiv 73^{1961} \pmod{100}$

We apply the Euler's theorem

Here $a = 73$. $M=100$ and $(a, m) = (73, 100) = 1$

$\phi(100) = \phi(2^2.5^2) = \phi(2^2).\phi(5^2) = 2^2\left(1-\frac{1}{2}\right).5^2\left(1-\frac{1}{5}\right) = 2^2\left(\frac{1}{2}\right).5^2\left(\frac{4}{5}\right) = 2.20 = 40.$

By Euler's theorem

$73^{\phi(100)} \equiv 1 \pmod{100}$

$\Rightarrow$ $73^{40} \equiv 1^{40} \pmod{100}$

$\Rightarrow$ $(73^{40})^{49} \equiv 1^{49} \pmod{100}$

$\Rightarrow$ $73^{1960} \equiv 1 \pmod{100}$

$\Rightarrow$ $73^{1960}.73 \equiv 1.73 \pmod{100}$

$$\begin{array}{r|l} & 49 \\ 40 & 1961 \\ & 16 \\ \hline & 36 \\ & 36 \\ \hline \end{array}$$

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

$\Rightarrow \quad 73^{1961} \equiv 73 \pmod{100}$ 1

$\Rightarrow \quad 273^{1961} \equiv 73 \pmod{100}$

$\therefore$ the remainder is 73 when 273^{1961} is divided by 100.

Theorem

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

Proof

Given n is a positive integer.

Let S = {1, 2, 3, … , 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 $m \le n$ such that d = (m, n).

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

The number of elements in the set C_d

= number of positive integer $\le \frac{n}{d}$ and relatively prime to it.

$= \phi\left(\frac{n}{d}\right)$

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

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

$\sum_{d|n} \phi\left(\frac{n}{d}\right) = n$

But d runs over the set of divisors of n, so does $\frac{n}{d}$

$\therefore \quad \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$

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

Problem

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

Solution

Given n =28

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

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

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

$\phi(7) = 6, \quad \phi(14) = \phi(2.7) = \phi(2)\ \phi(7) = 1.6 = 6,$

$\phi(28) = \phi(2^2.7) = \phi(2^2).\ \phi(7) = 2.6 = 12$

$\therefore \quad \sum_{d|n}\phi(d) = 1 + 1 + 2 + 6 + 6 + 12 = 28$

Problem

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

Solution

Given $n = 11^3.5 = 6655$

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

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

But $\phi(1) = 1$

$\phi(5) = 4$

$\phi(11) = 10$

$\phi(11^2) = 11^2\left(1-\frac{1}{11}\right) = 11^2\left(\frac{10}{11}\right) = 110$

$\phi(11^3) = 11^3\left(1-\frac{1}{11}\right) = 11^3\left(\frac{10}{11}\right) = 1210$

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

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

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

$\sum_{d|n}\phi(d) = 1 + 4 + 10 + 110 + 1210 + 40 + 440 + 4840 = 6655 = 5.11^3 = n$

THE TAU AND SIGMA FUNCTIONS

We have seen the number theoretic function ϕ and its properties. We will now two more number theoretic function τ (tau) and σ (sigma) which will give the number of positive division of n and the sum of divisors of n, using the canonical decomposition of n.

Definition The τ function

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

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

Definition The σ function

For a positive integer n, σ(n) denotes the sum of the positive divisors of n.

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

Problem

Find τ(12) and σ(19)

Solution

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

So, there are 6 divisors

$\therefore$ τ(12) = the number of positive divisors of 12

= 6.

The positive divisors of 19 are 1,19

$\therefore$ σ(19) = sum of the positive divisors of 19.

= 1+ 19 = 20

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

$\therefore$ τ(p) = 2 and σ(p) = 1+p

Problem

Compute the value of the sigma function for n=28

Solution

Given n=28

The number of positive divisors of 28 are 1,2,4,7,14,28

$\therefore$ σ(28) = sum of the positive divisors of 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 gives by F(n) = $\sum_{d|n} f(d)$ is also multiplicative.

Proof

Given f is a multiplicative function.

$\therefore$ for any two positive integer m and n which are relatively prime,

f(m.n) = f(m)f(n) (1)

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

$\therefore$ 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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

$= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2)$ [using (1)]

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

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

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

$= F(m)F(n)$

$\Rightarrow$ $F(mn) = F(m).F(n)$

Hence F is multiplicative

Theorem

Prove that τ and σ are multiplicative function

Proof

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

1. If $f(d) = d^0 = 1$ is the constant for each d|n
   If d_1, d_2 are two divisors $(d_1, d_2) = 1$
   Then $f(d_1.d_2) = 1.$
   $f(d_1) = 1$
   $f(d_2) = 1$
   $\therefore$ $f(d_1.d_2) = f(d_1).\ f(d_2)$
   So, the constant function is multiplicative
   Then $F(n) = \sum_{d|n} 1 = \tau(n)$
   If (m, n) = 1, then $F(mn) = F(m).F(n)$
   $\Rightarrow$ $\tau(mn) = \tau(m).\tau(n)$
   So, τ is multiplicative.
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 $f(d_1.d_2) = d_1.d_2$
   $= f(d_1).f(d_2)$
   $\therefore$ f is multiplicative

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

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

For $(m, n) = 1$ $F(m.n) = F(m).F(n)$

$\Rightarrow$ $\sigma(m.n) = \sigma(m).\ \sigma(n)$

$\therefore$ σ is multiplicative.

Theorem

If $n = p^{\alpha}$, where p is a prime and α is a positive integer,

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

Proof

Given $n = p^{\alpha}$.

$\therefore$ the factor 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}

$= \alpha+1$

and $\sigma(p^{\alpha})$ = sum of the factors of p^{α}

$= 1 + p + p^2 + p^3 + \ldots + p^{\alpha-1} + p^{\alpha}$

$= \frac{p^{\alpha+1}-1}{p-1}$ [$\because$ it is a G.P with C.R = p]

Theorem

If n is a positive integer with canonical decomposition $n = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots p_k^{\alpha_k}$, then

$$\tau(n) = (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\ldots(\alpha_k+1)$$

$$\sigma(n) = \frac{p^{\alpha_1+1}-1}{p-1}\frac{p^{\alpha_2+1}-1}{p-1}\frac{p^{\alpha_3+1}-1}{p-1}\cdots\frac{p^{\alpha_k+1}-1}{p-1}$$

Proof

Given $n = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots p_k^{\alpha_k}$

where $p_1, p_2, p_3, \ldots, p_k$ are distinct primes and $\alpha_1, \alpha_2, \alpha_3, \ldots \alpha_k$ are positive integers.

Since τ and σ are multiplicative functions,

$$\tau(n) = \tau(p_1^{\alpha_1})\tau(p_2^{\alpha_2})\tau(p_3^{\alpha_3})\ldots\tau(p_k^{\alpha_k})$$

$$= (\alpha_1+1)(\alpha_2+1)(\alpha_3+1)\ldots(\alpha_k+1)$$

and

$$\sigma(n) = \sigma(p_1^{\alpha_1})\sigma(p_2^{\alpha_2})\sigma(p_3^{\alpha_3})\ldots\sigma(p_k^{\alpha_k})$$

$$= \frac{p^{\alpha_1+1}-1}{p-1}\frac{p^{\alpha_2+1}-1}{p-1}\frac{p^{\alpha_3+1}-1}{p-1}\cdots\frac{p^{\alpha_k+1}-1}{p-1}$$

Problem

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

Course/Branch: BE/CSE	Year / Semester : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	Subject Name :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	Unit Name: CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

Solution

Given $n = p_1.p_2. \ldots .p_k$, 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.

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

$\tau(n) = \tau(p_1).\ \tau(p_2).\ \tau(p_3) \ldots . \tau(p_k)$

$= 2.2.2. \ldots .2$

$= 2^k$

$\sigma(n) = \sigma(p_1).\ \sigma(p_2).\ \sigma(p_3). \ldots . \sigma(p_k)$

$= (p_1+1).\ (p_2+1).\ (p_3+1). \ldots . (p_k+1)$

Problem

If n = 2187 find τ(n) and σ(n).

Solution

3	2187
3	729
3	243
3	81

$27 = 3^3$

Given $n = 2187 = 3^7$

W.K.T $\tau(p^\alpha) = \alpha + 1$ if p is prime

$\therefore$ $\tau(3^7) = 7+1 = 8$

W.K.T $\sigma(p^\alpha) = \dfrac{p^{\alpha+1}-1}{p-1}$ if p is prime

$= \dfrac{3^{7+1}-1}{3-1}$ $= \dfrac{3^8-1}{3-1} = 3280$

Problem

For any prime p prove that

(i) σ (p+2) = σ(p) + 2

(ii) σ(p) is odd

Solution

Since p is prime p + 2 is also a prime

So the factor of p+2 is 1 and p+2.

(i) σ (p+2) = sum of the factors

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

= σ(p) + 2

(ii) σ (p) = sum of the factors

= p+1, which is odd

Course/Branch: BE/CSE	**Year / Semester** : III/V	Format No.	NAC/TLP-07a.5
Subject Code :MA8551	**Subject Name** :ALGEBRA AND NUMBER THEORY	Rev. No.	02
Unit No : V	**Unit Name:** CLASSICAL THEOREMS AND MULTIPLICATIVE FUNCTIONS	Date	14-11-2017

LECTURE NOTES

Problem

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

Solution

Since 28 = 4.7 and (4, 7)=1

$\tau(28) = \tau(4.7) = \tau(4).\ \tau(7)$

and $\sigma(28) = \sigma(4.7) = \sigma(4).\ \sigma(7)$

But the positive divisor of 4 is 1,2,4 and positive divisor of 7 is 1,7

$\therefore$ $\tau(28) = 3.2 = 6$

$\sigma(28) = 7.8 = 56.$

Home work

If n = 6120 compute $\tau(n)$ and $\sigma(n)$ [Ans. 48 and 21660]