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 : III	**Unit Name:** DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

MA8551 ALGEBRA AND NUMBER THEORY

UNIT-III

DIVISIBILITY THEORY AND CANONICL DECOMPOSITIONS

INTRODUCTION:

The counting numbers 1, 2, 3, …,n, … are considered to be man's first mathematical creation. These numbers are also known the natural numbers or positive integers. The theory of numbers is the branch of mathematics, which deals with the properties of natural numbers. Once upon a time number theory was considered as the purest of pure mathematics because it had no practical applications. But today modern technology has brought a new dimension to the power of number theory with many areas of applications such as art, coding theory, cryptography computer science etc.

In this chapter we study the basic concepts of elementary numbers theory such as divisibility, greatest common divisor, prime and composite numbers, division algorithm, fundamental theorem of arithmetic, least common multiple and related results

USUAL NOTATIONS

1. The set of natural numbers N={1,2,3,…..}
2. The set of integers Z={. . . -3,-2,-1,0,1,2,3,. . . }

The Well-ordering Principle

Every non empty set of positive integers has a least number.

Note

1. The well ordering principle can be extended to the set of non negative integers and also to the set of integers $\geq k$ for some integer k.
2. The well-ordering principle is logically equivalent to the principle of induction.

DIVISIBILITY THEORY AND DIVISION ALGORITHM

Definition – Divisibility

Let $a,b \in Z$, we say b divides a and write b|a if a=bc for some integer c.

We also say that b is a factor of a or b is divisor of a or a is multiple of b.

If b does not divide a, we write b ł a.

Divisibility gives a relation between two integers with the following properties.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Theorem3.1

If a,b$\in$Z, then

(i) a|a $\forall\ a \neq 0 \in Z$ (reflectivity)

(ii) a|b and b|c $\Rightarrow$a|c $\forall\ a,b \neq 0, c \neq 0 \in Z$ (transitively)

(iii) a|b $\Rightarrow$a|bc, $\forall\ a \neq 0, b \in Z$

(iv) a|b and a|c $\Rightarrow$a|xb+yc $\forall\ x, y \in Z, a \neq 0 \in Z$ (linearity)

Proof

(i) If $a \neq 0,\ a \mid a\ (a = a.1)$

(ii) $a \mid b \Rightarrow b = q_1 a$ and $b \mid c \Rightarrow c = q_2 b$

where $a \neq 0, b \neq 0$ in Z, q_1,q_2 are some integer

$\therefore c = q_2(q_1 a) = (q_2 q_1)a \Rightarrow a \mid c.$

(iii) $a \mid b \Rightarrow b = q_1 a$

$bc = (q_1 a)c = q_1(ac) = q_1(ca) = (q_1 c)a \Rightarrow a \mid bc\ \ \forall b \in Z$

(iv) $a \mid b \Rightarrow b = q_1 a$ and $a \mid c \Rightarrow c = q_2 a$ for some integers $q_1 \text{ and } q_2 \in Z$

$\therefore xb + yc = x(q_1 a) + y(q_2 a)$

$= (xq_1)a + (yq_2)a$

$= (xq_1 + yq_2)a,\ \ xq_1 + yq_2$ is an integer

$\Rightarrow$a|xb+yc

Note xb+yc is called a linear combination of b and c

If x=1,y=1 , a|b+c and if x=1,y=-1, a|b-c

Theorem 3.2 The division algorithm

Let a be any integer and b be a positive integer. Then there exist unique integer q and r such that a=qb+r, where $0 \leq r < b.$

Proof

First we prove existence and then uniqueness

Existence is usually proved by suitable construction.

Consider the set S = {a-nb|n$\in$Z, a-nb$\geq$0}

Clearly $S \subseteq W$

Given a is any integer. Then $a < 0 or a \geq 0$.

If $a \geq 0$, then a = a-0.b$\in$ S and so a$\in$ S.

Hence S is non empty.

Now let $a < 0$,

Since b is a positive integer, $b \geq 1$,

Multiplying by a, we get $ab \leq a$

$\Rightarrow -ab \geq -a$ [since a<0, in equality will reverse]

$\Rightarrow a - ab \geq a - a = 0$.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

$\therefore a - ab \in S \Rightarrow$ S is non empty.

So, we find S is non-empty if $a < 0 \text{ or } a \geq 0$

Since S is a set of non-negative integers (by construction), by well-ordering principle S contains a least integer r.

As $r \in$ S, we can find an integer q such that r=a-qb, where $r \geq 0$

We shall now prove r<b.

We prove by contradiction.

Suppose $r \geq b$, then r-b$\geq$0 and hence r-b$\in$ S.

Since $r \geq 0$ and b > 0, r-b < r.

Now r-b$\in$ S and r-b < r, which contradicts the choice of r (as the least number S)

$\therefore r < b$

Thus there exist integers q and r such that a = qb + r, $0 \leq r < b.$

We now prove the uniqueness.

Suppose we also have a = q_1b + r_1, $0 \leq r_1 < b.$

Then qb + r = q_1b + r_1

$\Rightarrow (q - q_1)b = r_1 - r$

$\Rightarrow b \mid r_1 - r$

If $r_1 - r \neq 0, then b \mid r_1 - r$ which is a contradiction $(\because |r_1 - r| < b)$

$\therefore r_1 - r = 0 \Rightarrow r_1 = r$

Hence $(q - q_1)b = 0 \Rightarrow q - q_1 = 0 \ (\because b > 0)$

$\Rightarrow q = q_1$

$\therefore$ the expression a = qb + r , $0 \leq r < b.$ is unique, which is the division algrothem.

Note

In the expression a = qb + r , $0 \leq r < b.$

q is called the quotient and r is called the remainder.

If r=0, the a=qb $\Rightarrow$ b|a

ie., if r=0, then b is a factor of a.

Pro blem-1

Find q and r when (i) 207 is divided by 15. (ii) -23 is divided by 5. (iii) 57 is divided by 75.

Solution :-

(i)

```
      13  → q
   15 | 207
        15
      ----
        57
        45
      ----
        12 → 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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

207=13(15) =12 ($a = qb + r$, $0 \le r < b.$)
$\therefore$ q=13 and r=12, $0 \le 12 < 15$

(ii)

```
      - 4 → q
   5 | -23
     |  20
     | -3  → r (but r≥0 always)
```

```
      - 5 → q
   5 | -23
     |  25
     |  2  → r (here r≥0)
```

-23= (-5)(5)+2 ($a = qb + r$, $0 \le r < b.$)
$\therefore$ q=-5 and r=2, $0 \le 2 < 5$

(iii)

```
      0 → q
  75 | 57
     |  0
     | 57 → r
```

57=0(75)+57 ($a = qb + r$, $0 \le r < b.$)
$\therefore$ q=0 and r=57, $0 \le 57 < 75$

Pigeon Hole Principle

If m pigeons are assigned to n pigeon holes, where m > n, then at least two pigeons must occupy the same pigeon hole.

The pigeon hole principle is also known as Dirichlet box principle because the German mathematician Dirichlet used it in number theory.

Problem-2

Let b be an integer ≥ 2. Suppose b+1 integer are randomly selected. Prove that the difference of two of them is divisible by b.

Solution:-

Given b is an integer ≥ 2.

W.K.T, when an integer a is divided by b, we have the division algorithm a=qb+r, where $0 \le r < b.$

Given b +1 integer are selected randomly.

When they are divided by b, we get b+1 remainder (pigeons)

But there are only b possible remainders (pigeons holes)

So, b y pigeon hole principle two of the remainders must be equal and equal to r

Let x and y be the numbers among the b+1 numbers with remainder r when x and y are divided by b.

Then $x=q_1b+r$ and $y=q_2+r$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

$\therefore$ x-y = q_1b+r –(q_2b+r) = q_1b+r-q_2b-r = (q_1-q_2)b $\Rightarrow$ b|x-y
Hence the result.

Definition-2 (For some real number x.)

1. Absolute value or modulus function.
$$|x| = \begin{cases} x & if \ \ x \geq 0 \\ -x & if \ \ x < 0 \end{cases}$$
2. Greatest integer function
$[x]$=the greatest integer $\leq$x.
In computer science the greatest integer function is called floor function and is denoted by $\lfloor x \rfloor$
3. The ceiling function $\lceil x \rceil$ is the least integer $\geq$x.

For example

1. $\lfloor -3.4 \rfloor$ = the greatest integer $\leq$ -3.4 is -4 [$\because$ (-4,-5,-6,. . .)$\leq$ -3.4]
2. $\lceil -3.4 \rceil$ = the least integer $\geq$ -3.4 is -3 [$\because$ (-3,-2,-1,0,1. . .) $\geq$ -3.4]
3. $\lfloor 3.4 \rfloor$ = the greatest integer $\leq$ 3.4 is 3 [$\because$ (3,2,1,0,-1. . .)$\leq$ 3.4]
4. $\lceil 3.4 \rceil$ = the least integer $\geq$ 3.4 is 4 [$\because$ (4,5,6,. . .) $\geq$ -3.4]

Theorem-3

Let a and b be any positive integer. Then the number of positive integer $\leq$ a and divisible by b is $\left\lfloor \frac{a}{b} \right\rfloor or \left\lceil \frac{a}{b} \right\rceil$.

For example, the number of positive integer $\leq$ 2076 and divisible by 19 is
$\left\lfloor \frac{2076}{19} \right\rfloor or \left\lceil \frac{2076}{19} \right\rceil$ = $\lfloor 109.26 \rfloor$ = 109.

Corollary In the set of integers {1,2,3,4,. . . ,n} the number of integers divisible by a prime p is $\left\lfloor \frac{n}{p} \right\rfloor or \left\lceil \frac{n}{p} \right\rceil$.

Instead of floor function notation, we will be using greatest integer function notation.

If p_1,p_2 are distinct primes, the number of integers divisible by $p_1.p_2$ is $\left\lfloor \frac{n}{p_1 p_2} \right\rfloor or \left\lceil \frac{n}{p_1 p_2} \right\rceil$

Inclusion – Exclusion Principle

If S is a set, the number of elements in S denoted by $|S|$

If A,B,C are finite sets, then

1. $|A \cup B| = |A| + |B| - |A \cap B|$ = S_1-S_2
where S_1 = sum taken one at a time = $|A| + |B|$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

$S_2 = |A \cap B|$

2. $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| = S_1 - S_2 + S_3$

where S_1 = sum taken one at a time = $|A| + |B| + |C|$

S_2 = sum taken two at a time = $|A \cap B| + |A \cap C| + |B \cap C|$

$S_3 = |A \cap B \cap C|$

3. $|A \cup B \cup C \cup D| = S_1 - S_2 + S_3 - S_4$

where S_1 = sum taken one at a time = $|A| + |B| + |C| + |D|$

S_2 = sum taken two at a time = $|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D|$

S_3 = sum taken three at a time = $|A \cap B \cap C| + |A \cap B \cap D| + |B \cap C \cap D|$

$S_4 = |A \cap B \cap C \cap D|$

This can be extended for more number of sets.

Problem-3

Find the number of positive integers in the range 1976 through 3776 that are divisible by 13.

Solution:-

The number of positive integer ≤ 1976 that are divisible by 13 is = $\left\lfloor \frac{1976}{13} \right\rfloor = \lfloor 152 \rfloor = 152$.

The number of positive integer ≤ 3776 that are divisible by 13 is = $\left\lfloor \frac{3776}{13} \right\rfloor = \lfloor 290.46 \rfloor = 290$.

The number of positive integer from 1976 to 3776 that divisible by 13 is =290-152+1=139.

[$\because$ 1976 included in the list of the number is divisible by 13]

Alter: - Among the positive integer from 1976 to 3776 that are divisible by 13l, the first number is 1976

When 3776 is divided by 13, the remainder is 6. ie, 3776=290(13)+6 $\Rightarrow$ 3770=290(13).

So the last number divisible by 13 is 3770

$\because$ The list of numbers is 1976, 1989, 2002, . . . , 3770.

This is an A.P. with a=1976, C.D. d=13 and l=3770.

If n is the number of terms n= $\frac{l-a}{d} + 1 = \frac{3770 - 1976}{13} + 1 = 138 + 1 = 139$.

Home work-1

Find the number of positive integers in the range 1976 through 3776 that are divisible by 17.

[Answer is 1697]

Problem – 4

Find the number of positive integers ≤ 5557 that are not divisible by 24.

Solution:-

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

The number of integers ≤ 5557 that are divisible by 24 is $\left\lfloor \frac{5557}{24} \right\rfloor = \lfloor 231.54 \rfloor = 231.$

The number of integers ≤ 5557 that are not divisible by 24 = the total number of numbers -128
= 5557 – 231 = 5326

Problem-5

Find the number of positive integer $\leq$ 2076 and divisible by neither 4 nor 5.

Solution:-

First we find number of positive integer $\leq$ 2076 and divisible by 4 or 5.

Let A, B be the set of integer ≤ 2076 that are divisible by 4 or 5 respectively.

By inclusion – exclusion principle, we know

$|A \cup B| = |A| + |B| - |A \cap B|$ = S_1-S_2

where S_1 = sum taken one at a time = $|A| + |B|$

S_2 = $|A \cap B|$

Now $|A| = \left\lfloor \frac{2076}{4} \right\rfloor = \lfloor 519 \rfloor = 519$

$|B| = \left\lfloor \frac{2076}{5} \right\rfloor = \lfloor 415.2 \rfloor = 415$

$\therefore$ S_1 = $|A| + |B|$ =519+415=934

and S_2 = $|A \cap B| = \left\lfloor \frac{2076}{4(5)} \right\rfloor = \left\lfloor \frac{2076}{20} \right\rfloor = \lfloor 103.8 \rfloor = 103$

$|A \cup B| = |A| + |B| - |A \cap B|$ = S_1-S_2 = 934 -103 = 831

$\therefore$ the set of integers divisible by neither A nor B is $A' \cap B' = (A \cap B)'$

$\therefore$ $|A' \cap B'| = |(A \cap B)'|$ = the total number of integer - $|A \cap B|$ =2076-831 = 1245

Problem-6

Find the positive integers ≤ 3000 and divisible by 3,5 or 7.

Solution:-

Let A,B,C be the set of numbers $\leq$ 3000 that are divisible by 3,5 7 respectively.

Required $|A \cup B \cap C|$

By inclusion – exclusion principle is

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| = S_1 - S_2 + S_3$$

where S_1 = sum taken one at a time = $|A| + |B| + |C|$

S_2 = sum taken two at a time = $|A \cap B| + |A \cap C| + |B \cap C|$

S_3 = $|A \cap B \cap C|$

Now $|A| = \left\lfloor \frac{3000}{3} \right\rfloor = \lfloor 1000 \rfloor = 1000.$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

$$|B| = \left\lfloor \frac{3000}{5} \right\rfloor = \lfloor 600 \rfloor = 600.$$

$$|C| = \left\lfloor \frac{3000}{7} \right\rfloor = \lfloor 428.5 \rfloor = 428.$$

$\therefore S_1 = |A| + |B| + |C| = 1000 + 600 + 428 = 2028$

Also $$|A \cap B| = \left\lfloor \frac{3000}{3(5)} \right\rfloor = \left\lfloor \frac{3000}{15} \right\rfloor = \lfloor 200 \rfloor = 200$$

$$|A \cap C| = \left\lfloor \frac{3000}{3(7)} \right\rfloor = \left\lfloor \frac{3000}{21} \right\rfloor = \lfloor 142.85 \rfloor = 142$$

$$|B \cap C| = \left\lfloor \frac{3000}{5(7)} \right\rfloor = \left\lfloor \frac{3000}{35} \right\rfloor = \lfloor 85.71 \rfloor = 85$$

$\therefore S_2 = |A \cap B| + |A \cap C| + |B \cap C| = 200 + 142 + 85 = 427$

Also $$|A \cap B \cap C| = \left\lfloor \frac{3000}{3(5)(7)} \right\rfloor = \left\lfloor \frac{3000}{105} \right\rfloor = \lfloor 28.57 \rfloor = 28$$

$\therefore S_3 = |A \cap B \cap C| = 28$

$|A \cup B \cup C| = S_1 - S_2 + S_3 = 2028 - 427 + 28 = 1629.$

Home work - 2

Find the number of integers from 1 to 250 that are divisible by any of the integers 2,3,5,7. [Answer 193]

THE PRINCIPLE OF MATHEMATICAL INDUCTION

1. First Principle of Induction

Let p(n) be a proposition corresponding to positive integers n satisfying the following conditions:

(i) $p(n_o)$ is true for some integer n_o

(ii) If p(k) is true for an arbitrary integer $k > n_o$, then p(k+1) is also true. Then p(n) is true for all integers $n \geq n_o$

2. Second Principle of Induction or strong Principle of Induction

Let p(n) be a proposition corresponding to positive integers n satisfying the following conditions:

(i) $p(n_o)$ is true for some integer n_o

(ii) If the proposition is true for all integer upto $k (> n_o)$
ie., if $p(n_o+1), p(n_o+2), p(n_o+3), \ldots, p(k)$ all true, then p(k+1) is true.
Then p(n) is true for all integers $n \geq n_o$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Note

1. In both the principles condition (i) is called the basis for induction. n_0 may be 1 or 2 or3. . . . The verification of the truth of $p(n_o)$ is the basis step. The assumption in condition (ii) is called the induction hypothesis. Verification of p(k+1) is true is the inductive step or induction step.
2. The two principles differ only in the induction hypothesis. Theoretically, both the principles are equivalent. But in practice the second principle is stronger in the sense that there are propositions for which only the second principle is applicable. All those propositions for which first principle is applicable, we can apply the second principle also.
3. Sometimes if the proposition p(n) is true for n=0, we take n_o=0. In computer service, we use the set of whole number W = {0,1,2,3,. . . } rather than N.

Problem – 7

Prove by induction that $2n^3+3n^2+n$ are divisible by 6 for all $n \geq 0$.

Solution:-

Let $p(n) = 2n^3+3n^2+n$ is divisible by 6.

To prove p(n) is true for all $n \geq 0$.

Here n = 0

i.e., $p(0) = 2(0)^3 + 3(0)^2 + 0 = 0$ | $p(1) = 2(1)^3 + 3(1)^2 + 1 = 6$

$\therefore$ p(0) is divisible by 6. | $\therefore$ p(1) is divisible by 6

Let as assume that n=k [p(k)] is true , $k \geq 0$.

i.e., $p(k) = 2(k)^3 + 3(k)^2 + k$ is divisible by 6.

Now to prove that n = k+1.

i.e., to prove $p(k+1) = 2(k+1)^3 + 3(k+1)^2 + (k+1)$

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

$= (2k^3+3k^2+k) + 6k^2+6k+6k + 2+3+1$

$= (2k^3+3k^2+k) + 6k^2+12k+6$

$= (2k^3+3k^2+k) + 6(k^2+2k+1)$

$= p(k) + 6k^2+12k+6$

= is divisible by 6

i.e., p(0) is divisible by 6, assume p(k) is divisible by 6 and p(k+1) is also divisible by 6

$\therefore$ $2n^3+3n^2+n$ are divisible by 6 for all $n \geq 0$.

Problem – 8

Prove by induction that $2^{4n}+3n-1$ is divisible by 9 $\forall\ n \geq 0$

Solution:-

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Let $p(n) = 2^{4n}+3n-1$ is divisible by 9.
To prove p(n) is true for all $n \geq 0$.
Here n = 0
i.e., $p(0) = 2^{4(0)}+3(0) -1 = 2^0+0-1 =1-1 =0$
$\therefore$ p(0) is divisible by 9.

$p(1) = 2^{4(1)}+3(1) -1 = 2^4+3-1 =16+3-1 =18$
$\therefore$ p(1) is divisible by 9.

Let as assume that n=k [p(k)] is true , $k \geq 0$.
i.e., $p(k) = 2^{4k}+3k-1$ is divisible by 9. $\Rightarrow 2^{4k}+3k-1 = 9x \longrightarrow (1)$
Now to prove that n = k+1.
i.e., to prove $p(k+1) = 2^{4(k+1)}+3(k+1)-1$

$= 2^{4k+4}+3k +3-1$
$= 2^{4k}2^4 + 3k + 2$
$= 16(2^{4k}) + 3k + 2$
$= 16(9x-3k+1) + 3k +2$ by (1)
$= 144x - 48k + 16 +3k +2$
$= 144x - 45k + 18$
$= 9(16x - 5k +2)$ = is divisible by 9.

ie., p(0) is divisible by 9, assume p(k) is divisible by 9 and p(k+1) is also divisible by 9.
$\therefore$ $2^{4n}+3n-1$ is divisible by 9 $\forall\ n \geq 0$.

Problem – 9

If sum of the cubes of three consecutive integers is cube k^3 prove that 3|k
Solution:-
Let n, n+1, n+2 be three consecutive integers.
Given $n^3+(n+1)^3+(n+2)^3 = k^3$
$\Rightarrow n^3 + (n^3+3n^2+3n+1) + (n^3+12n^2+6n+8) = k^3$
$\Rightarrow 3n^3+15n^2+9n+9 = k^3$
$\Rightarrow 3(n^3+5n^2+3n+3) = k^3 \Rightarrow 3|k^3 \Rightarrow 3|k.k.k \Rightarrow 3|k$ ($\because$ 3 is prime)

Problem – 10

Show that $n^3+(n+1)^3+(n+2)^3 = (n+3)^3$ has unique solution.
Solution:-
Given $n^3+(n+1)^3+(n+2)^3 = (n+3)^3 \longrightarrow (1)$
Since LHS is sum of the cubes of three consecutive integers by problem-9, 3|n+3
Since 3|n+3 and 3|3, we get $3|n+3-3 \Rightarrow 3|n \Rightarrow n=3m$
$\therefore (1) \Rightarrow (3m)^3+(3m+1)^3+(3m+2)^3=(3m+3)^3$
$\Rightarrow 27m^3+[27m^3+3(3m)^2(1)+3(3m)(1)^2+(1)^3] + [27m^3+3(3m)^2(2)+3(3m)(2)^2+(2)^3]$
$= [27m^3+3(3m)^2(3)+3(3m)(3)^2+(3)^3]$
$\Rightarrow 27m^3+27m^3+27m^2+9m+1 + 27m^3+54m^2+36m+8 = 27m^3+81m^2+81m+27$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Simplify we get $54m^3-36m-18=0$
$\Rightarrow 18(3m^2-2m-1)=0 \Rightarrow 3m^2-2m-1=0$
$\Rightarrow (m-1)(3m^2+3m+1)=0 \Rightarrow m-1=0$ ($\because 3m^2+3m+1 \neq 0$)
Because $3m^2+3m+1=0$ has no real roots
$\therefore$ $m=1 \Rightarrow n=1$
So the solution of equation (1) is unique.

BASE –b – REPERSENTATIONS

We are familiar with the use of decimal notation, base 10, to express any integer or real number. We use it every day.
For example $352 = 3(10^2) + 5(10^1) + 2(10^0)$
$= 3(10^2) + 5(10^1) + 2(1)$
This is called the decimal expansion of 352.
And $35.23 = 3(10^1) + 5(10^0) + 2(10^{-1}) + 3(10^{-2})$.
But computers usually use binary notation, ***base 2***, when carrying out arithmetic operation. Very long binary numbers are often handled by using octal (***base 8***) or hexadecimal (***base 16***) notations. Similarly these bases are used the expressing characters such as letters or digits.

In fact, any integer ≥ 2 can be used as a valid base for representing integers.
We now state a fundamental result without proof.

Theorem – 3-3
Let b be an integer ≥ 2. If n is a positive integer, then it can be uniquely expressed in the form $n = a_k b^k + a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_1 b + a_0$, where $a_0, a_1, \ldots, a_{k-1}, a_k$ are non negative integers less than b and $a_k \neq 0$ and $k \geq 0$.

Definition
If n is a positive integer and $b \geq 2$ and
$$n = a_k b^k + a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \ldots + a_1 b + a_0 \longrightarrow (1)$$
where $a_0, a_1, \ldots, a_{k-1}, a_k$ are non negative integers then he expression (1) is called ***base 2*** expansion of the integer n.

We then write $n = (a_k a_{k-1} \ldots a_1 a_0)$
For example $(345)_{10} = 3(10^2) + 4(10^1) + 5(10^0)$
$(345)_8 = 3(8^2) + 4(8^1) + 5(8^0) = 3(64) + 4(8) + 5(1) = (229)_{10}$

Binary Expansion
When base is 2, then the expansion is called the binary expansion when b=2, each coefficient is 0 or 1. The digit 0 and 1 are called binary or bits. So, the binary expansion

of an integer is just a bit string. Binary expansions are used by computers to represent and do arithmetic with integer.

Note:-

1. The number system with base 10 is called the decimal system because the Latin word **decem** means 10. The decimal system uses the 10 digits 0, 1, 2, . . . , 9.
2. If the base b>0, we use the letters A, B, C, . . . to represent the digits 10, 11, 12, . . . respectively in decimal notation.

Hexadecimal Expansion

Another base used in computer science is 16. The base 16 expansion of an integer is called its hexadecimal expansion. Hexadecimal expansion uses the sixteen digits 0, 1, 2, . . . ,9, A, B, C, D, E and F, where A to F represent the digits 10 to 15 respectively (in decimal notation)

Problem – 11

Express $(101011111)_2$ in base 10.

Solution:-

$(101011111)_2 = 1(2^8) + 0(2^7) + 1(2^6) + 0(2^5) + 1(2^4) + 1(2^3) + 1(2^2) + 1(2^1) + 1(2^0)$

$= 256 + 64 + 16 + 8 + 4 + 2 + 1$

$= 351.$

Problem – 12

Express $(3AB0E)_{16}$ in base 10

Solution: -

We know A=10, B=11, E=14

$(3AB0E)_{16} = 3(16^4) + 10(16^3) + 11(16^2) + 0(16^1) + 14(16^0)$

$= 196608 + 40960 + 2816 + 14$

$= 240398$

Home work

Express $(3ABC)_{16}$ in base ten. [Ans. 15036]

Base Conversion Algorithm – Decimal to Base b.

The converse problem of writing a decimal integer into base b integer.

First divided n by b and obtain the quotient and remainder.

i.e., $n = q_0(b) + r_0 \quad 0 \le r_0 < b$

Now we divided q_0 by b

i.e., $q_0 = q_1(b) + r_1 \quad 0 \le r_1 < b$

Next we divided q_1 by b

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

i.e., $q_1 = q_2(b) + r_2 \quad 0 \le r_2 < b$

Proceed in this way until we get zero quotients.

Then the remainders in the reverse order give the b representation of n.

Problem -13

Express 1076 in the binary system.

Solution:-

$1076 = 538(2) + 0$ ↑
$538 = 269(2) + 0$
$269 = 134(2) + 1$
$134 = 67(2) + 0$
$67 = 33(2) + 1$
$33 = 16(2) + 1$
$16 = 8(2) + 0$
$8 = 4(2) + 0$
$4 = 2(2) + 0$
$2 = 1(2) + 0$
$1 = 0(2) + 1$

$1076 = (10000110100)_2$

Problem – 14

Express 12345 in the octal system

Solution:-

$12345 = 1543(8) + 1$ ↑
$1534 = 192(8) + 7$
$192 = 24(8) + 0$
$24 = 3(8) + 0$
$3 = 0(8) + 3$

$12345 = (30071)_8$

Home work

Express 1776 in the octal system. [Ans.:- $(3360)_8$]

Problem – 15

Represent 15036 in hexadecimal system.

Solution:-

$15036 = 939(16) + 12 \ (= C)$ ↑
$939 = 58(16) + 11 \ (= B)$
$58 = 3(16) + 10 \ (= A)$
$3 = 0(16) + 3$

$15036 = (3ABC)_{16}$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Home work

Express 177130 in the octal system. [Ans.:- $(2B3EA)_{16}$]

Base Conversion from Binary to octal

To convert a binary system number to octal system, we group the binary digits in to blocks of three bits from to right to left and adding if necessary initial zero at the left most replace each group with the corresponding octal digit.

Problem – 16

Convert the binary numbers $(1111011)_2$ in to octal digit.

Solution:-

Given 11 110 011

We group the digit in blocks of three from right to left

Here the block is 011, 110, 011 (adding 0 to left most block to get 3 digits)

Now $011 = 0(2^2) + 1(2^1) + 1(2^0) = 0 + 2 + 1 = 3.$

$110 = 1(2^2) + 1(2^1) + 0(2^0) = 4 + 2 + 0 = 6.$

$011 = 0(2^2) + 1(2^1) + 1(2^0) = 0 + 2 + 1 = 3.$

Hence $(1111011)_2 = (363)_8$

Problem – 17

Write 111010_{two} as an octal integer.

Solution:-

Given 111 010.

We group the digit in blocks of three from right to left

Here the block is 111, 010

Now $111 = 1(2^2) + 1(2^1) + 1(2^0) = 4 + 2 + 1 = 7.$

$010 = 0(2^2) + 1(2^1) + 0(2^0) = 0 + 2 + 0 = 2.$

Hence $111010_{two} = (72)_8.$

Home work

Convert $(11100101)_2$ to octal digit. [Ans.:- $(345)_8$]

Base Conversion from Binary to Hexadecimal.

To convert a binary system number to hexadecimal system, we group the binary digits in to blocks of four bits from to right to left and adding if necessary initial zero at the left most replaces each group with the corresponding hexadecimal digit.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Problem – 18

Write $(11111010111100)_2$ as a hexadecimal digit.

Solution:-

Given 11 1110 1011 1100

We write 0011, 1110, 1011, 1100

Now $0011 = 0(2^3) + 0(2^2) + 1(2^1) + 1(2^0) = 0 + 0 + 2 + 1 = 3$

$1110 = 1(2^3) + 1(2^2) + 1(2^1) + 0(2^0) = 8 + 4 + 2 + 0 = 14 = E$

$1011 = 1(2^3) + 0(2^2) + 1(2^1) + 1(2^0) = 8 + 0 + 2 + 1 = 11 = B$

$1100 = 1(2^3) + 1(2^2) + 0(2^1) + 0(2^0) = 8 + 4 + 0 + 0 = 12 = D$

$(11111010111100)_2 = (3EBD)_{16}$

Home work

Write (i) $(1110101)_2$ (ii) $(1110011)_2$ as a hexadecimal number.

[Ans.: (i) = $(75)_{16}$ (ii) = $(F3)_{16}$

Problem – 19

Rewrite 217_{16} as a binary digit.

Solution:-

Given 217_{16}

So each digit we have to rewrite as blocks of four bits.

There four we write $2 = 0(2^3) + 0(2^2) + 1(2^1) + 0(2^0) = 0010$

$1 = 0(2^3) + 0(2^2) + 0(2^1) + 1(2^0) = 0001$

$7 = 0(2^3) + 1(2^2) + 1(2^1) + 1(2^0) = 0111$

$217_{16} = (001000010111)_2$

$= (1000010111)_2$

Problem – 20

Rewrite $(3AD)_{16}$ as a binary digit.

Solution:-

Given $(3AD)_{16}$

So each digit we have to rewrite as blocks of four bits.

There four we write $3 = 0(2^3) + 0(2^2) + 1(2^1) + 1(2^0) = 0011$

$A = 10 = 1(2^3) + 0(2^2) + 1(2^1) + 0(2^0) = 1010$

$D = 13 = 1(2^3) + 1(2^2) + 0(2^1) + 1(2^0) = 1101$

$(3AD)_{16} = (001110101101)_2$

$= (1110101101)_2$

Home Work

Rewrite $(36)_{16}$ as a binary number [Ans.:- $(110110)_2$]

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Problem – 21

Rewrite $(345)_8$ as a binary number.

Solution:-

Given $(345)_8$

We write each digit as block of three bits

$\therefore$ We write $3 = 0(2^2) + 1(2^1) + 1(2^0) = 011$

$4 = 1(2^2) + 0(2^1) + 0(2^0) = 100$

$5 = 1(2^2) + 0(2^1) + 1(2^0) = 101$

$(345)_8 = (011100101)_2$

$= (11100101)_2$

Home work

Convert $(237)_8$ as a binary number. [Ans.: $(10011111)_2$)]

Problem -22

Arrange the binary number 1011, 110, 11011, 10110 and 101010 in increasing order of magnitude.

Solution:-

Given 1011, 110, 11011, 10110 and 101010

We will convert these binary numbers in to decimal numbers for comparison.

$\therefore$ We write

$1011 = 1(2^3) + 0(2^2) + 1(2^1) + 1(2^0) = 8 + 0 + 2 + 1 = 11$

$110 = 1(2^2) + 1(2^1) + 0(2^0) = 4 + 2 + 0 = 6$

$11011 = 1(2^4) + 1(2^3) + 0(2^2) + 1(2^1) + 1(2^0) = 16 + 8 + 0 + 2 + 1 = 27$

$10110 = 1(2^4) + 0(2^3) + 1(2^2) + 1(2^1) + 0(2^0) = 16 + 0 + 4 + 2 + 0 = 22$

$101010 = 1(2^5) + 0(2^4) + 1(2^3) + 0(2^2) + 1(2^1) + 0(2^0) = 32 + 0 + 8 + 0 + 2 + 0 = 42$

$\therefore$ The binary numbers in increasing order are 110, 1011, 10110, 11011, 101010.

Problem – 23

Find the number of ones in the binary representation of 2^4-1.

Solution:-

Given 2^4-1.

Now we write $2^4-1 = 16 - 1 = 15 = 7(2) + 1$

$7 = 3(2)) + 1$

$3 = 1(2) + 1$

$1 = 0(1) + 1$

$\therefore 2^4-1 = (1111)_2$

So the number of one's is 4

Note

More generally, the number of ones in the binary form $2^n - 1 = n$.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Problem – 24

Find the value of the base b if $1001_b = 9$

Solution:-

Given $1001_b = 9$

Since the digits are binary we expect b = 2.

Now $1001_b = 9$

$\Rightarrow 1(b^3) + 0(b^2) + 0(b^1) + 1(b^0) = 9$

$\Rightarrow b^3 + 0 + 0 + 1 = 9 \Rightarrow b^3 = 9-1 \Rightarrow b^3 = 8 \Rightarrow b^3 = 2^3 \Rightarrow b = 2.$

Problem – 25

If $144_b = 49$, find the base b.

Solution:-

Given $144_b = 49$

Now $1(b^2) + 4(b^1) + 4(b^0) = 49$

$\Rightarrow b^2 + 4b + 4 - 49 = 0$

$\Rightarrow b^2 + 4b - 45 = 0$

$\Rightarrow b^2 + 9b - 5b - 45 = 0$

$\Rightarrow b(b+9) - 5(b+9) = 0$

$\Rightarrow (b+9)(b-5) = 0$

$\Rightarrow b = -9$ or 5

$\therefore b = 5$ [$\because$ base > 0 always]

NUMBER PATTERNS

In drawing scientific conclusion, there are two fundamental processes of reasoning that are commonly used.

One is the process of deduction, which is the process of reasoning from general to particular.

The other process of reasoning is the process of induction, which is the process of reasoning from particular to general. The process may lead to true or false conclusion. To succeed in the art of induction reasoning one must be good at studying pattern. Observing particular cases or pattern a general statement is usually made. Such a statement is called ***a conjecture or educated guess***. A conjecture remains a conjecture until it is proved or disproved.

Inductive reasoning ends with the conjecture. Then the difficult task of proving it be gains, one of the methods of proof is by mathematical induction.

We now consider some of the famous conjectures.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

1. The great French mathematician Fermat (1601-1605) observed

   $2^{2^1} + 1 = 5$, a prime

   $2^{2^2} + 1 = 17$, a prime

   $2^{2^3} + 1 = 257$, a prime

   On the basis of this particular cases Fermat conjectured that $2^{2^n} + 1$ is a prime for any positive integer n and be challenged the mathematician of his days to disprove.
   After nearly 100 years the great Swiss mathematician Euler (1707-1783) showed that $2^{2^5} + 1 = 4294967297$ is not a prime because it is divisible by 641. Thus the conjecture is disproved.
2. The great German mathematician G.W. Leibnitz (1646 -1716) noticed that for any positive integer n.

   n^3-n is divisible by 3

   n^5-n is divisible by 5

   n^7-n is divisible by 7

   Observing this pattern, he was on the verge of conjecturing that for any odd integer r, n^r-n is divisible by r.
   But soon he noticed that 2^9-2 = 510 is not divisible by 9.
   This counter example disproved the conjecture.
3. The Prussian mathematician Christian Gold back (1690-1764) observed

   4 = 2+2

   6 = 3+3

   8 = 3+5

   10 = 3+7

   12 = 5 +7, . . .

   These even integers are expressed as a sum of two primes.

   One basis of this particular cases he conjectured that every even integer greater than 2 is a sum of two primes.
   In 2006, with help of computers it is verified for all even integers up to 2.10^7.
   But till today it continues to remain as a conjecture.

   From these examples, we find that inductive reasoning need not lead to correct conclusion.

Problem – 26

From the pattern

1.9 + 2 = 11

12.9 + 3 = 111

123.9 +5 = 1111

1234.9 + 6 = 11111

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Write down the n^{th} row and prove the validity of the number pattern.

Solution:-

From the given pattern we find the 12345…n . 9 + (n+1) = 11111….1 (n+1 ones)

LHS = 12345…n .9 + (n+1)

$= 9[1.10^{n-1}+2.10^{n-2}+3.10^{n-3}+ \ldots +(n-1)10 + n.10^0] + (n+1)$

$= (10-1)[1.10^{n-1}+2.10^{n-2}+3.10^{n-3}+ \ldots +(n-1)10 + n.10^0] + (n+1)$

$= \{10[1.10^{n-1}+2.10^{n-2}+3.10^{n-3}+ \ldots +(n-1)10 + n.10^0]$

$-1[1.10^{n-1}+2.10^{n-2}+3+.10^{n-3}+ \ldots +(n-1)10 + n.10^0]\}+ (n+1)$

$=[1.10^n+2.10^{n-1}+3.10^{n-2}+. \ldots + (n-1)10^2+n.10$

$-1.10^{n-}1-2.10^{n-2}-3.10^{n-3}- \ldots -(n-2).10^2-(n-1)10 - n.10^0] + (n+1)$

$= 1.10^n+1.10^{n-1}+1.10^{n-2}+ \ldots + 1.10^2+1.10 -n+n+1$

$= 1.10^n+1.10^{n-1}+1.10^{n-2}+ \ldots + 1.10^2+1.10 +1$

= 1111…11 (n+1 ones) = RHS.

Problem – 27

Using the number pattern

$1^2 - 0^2 = 1$

$2^2 - 1^2 = 3$

$3^2 - 2^2 = 5$

$4^2 - 3^2 = 7$

. . .

. . .

Make a conjecture about row n and prove conjecture.

Solution:-

From the given number patterns, we find the nth row is $n^2 - (n-1)^2 = 2n-1$.

$\therefore$ The conjecture is $n^2 - (n-1)^2 = 2n-1, \forall n \geq 0.$

LHS = $n^2 - (n-1)^2 = n^2 - [n^2-2n+1] = n^2-n^2+2n-1 = 2n-1$ = RHS.

Problem – 28

Given the pattern

9.9 + 7 = 88

98.9 + 6 = 888

987.9 + 5 = 8888

.

.

.

Find the formula for the nth row and prove it.

Solution:-

Observing the pattern, we find the nth row is

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

987… (10-n).9 + (8-n) = 888…8(n+1 eight), $1 \le n \le 8$

LHS = 987…(10-n).9 + (8-1)

= $9[9.10^{n-1}+8.10^{n-2}+7.10^{n-3}+ \ldots +(11-n).10+(10-n).1] + (8-n)$

= $(10-1)[9.10^{n-1}+8.10^{n-2}+7.10^{n-3}+ \ldots +(11-n).10+(10-n).1] + (8-n)$

= $10[9.10^{n-1}+8.10^{n-2}+7.10^{n-3}+ \ldots +(11-n).10+(10-n).1] -1.[9.10^{n-1}+8.10^{n-2}+7.10^{n-3}+ \ldots$
$+(11-n).10+(10-n).1] + (8-n)$

= $[9.10^{n}+8.10^{n-1}+7.10^{n-2}+ \ldots +(11-n)10^2+(10-n)10 -9.10^{n-1}-8.10^{n-2}-7.10^{n-3}- \ldots$
$-(11-n).10-(10-n).1] + (8-n)$

= $9.10^{n} -10^{n-1}-10^{n-2}- \ldots -10^2-10-(10-n)+(8-n)$

= $(10-1)10^{n}-10^{n-1}-10^{n-2}- \ldots -10^2-10-10+n+8-n$

= $10.10^{n}-10^{n}-10^{n-1}-10^{n-2}- \ldots -10^2-10-2$

= $10^{n+1}-[10^{n}+10^{n-1}+10^{n-2}+ \ldots +10^2+10+1]-1$

= $10^{n+1}-\frac{10^{n+1}-1}{10-1}-1$ $\left(Since \sum_{r=0}^{k} r^i = \frac{r^{k+1}-1}{r-1}(r \ne 1)\right)$

= $10^{n+1}-\frac{10^{n+1}-1}{9}-1 = \frac{9.10^{n+1}-10^{n+1}+1-9}{9} = \frac{8.10^{n+1}-8}{9} = \frac{8}{9}\left(10^{n+1}-1\right) \longrightarrow (1)$

Take $10^{n+1}-1$ = 999…9 (n+1 9's) $\Rightarrow \frac{10^{n+1}-1}{9} = \frac{999\ldots9}{9} = 111\ldots1$(n+1 1's)

(1) $\Rightarrow \frac{8}{9}\left(10^{n+1}-1\right)$=8(111…1) =888…8 = RHS.

PRIME AND COMPOSITE NUMBER

An important concept based on divisibility is the concept of the prime number. Prime numbers are the building blocks of integers as the fundamental theorem of arithmetic shows. It state that every integer greater than 1 can be written uniquely as the product of prime numbers. Prime numbers have become essential in modern cryptography.

Definition

A positive integer p>1 is called a prime if its only positive factors are 1 and p.

If p>1 is not a prime, then it is called a composite number (or simply composite)

It is obvious, the integer n is composite if and only if there exists an integer a such that a|n and 1<a<n

For example, 5 is a prime because its only positive factors are 1 and 5.

But 6 is composite number because it has 2 and 3 as factors.

Note that by definition the integer 1 is neither a prime not a composite number.

1 is just the multiplicative identity or unit.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Theorem

Every integer $n \geq 2$ has a prime factor.

Proof

We prove the theorem by strong principle of induction on n.

If n=2, then the statement is true. Since 2 is a prime and 2 is a factor of 2.

Assume the statement is true for all integer upto k, k>2.

To prove it a true for k+1,

If k+1 is a prime, then k+1 is prime factor of k+1.

If k+1 is not a prime, then k+1 must be a composite number.

So it must have a factor d, where $d \leq k$. Then b y the induction hypothesis, d has a prime factor of p.

Since p|d and d|k+1, we have p|k+1. So p is a factor of k+1.

Hence by second principle of induction the statement is true for every integer>1.

i.e., every integer ≥ 2 has a prime factor.

Theorem [Euclid]

There are infinitely many primes.

Proof

Assume that there are only n primes $p_1, p_2, \ldots, p_n$, where n is finite.

Now consider the integer $m=p_1.p_2. \ldots .p_n + 1$

Since m>1, m has prime factor [Every integer $n \geq 2$ has a prime factor]

But none of the primes $p_1, p_2, \ldots, p_n$ divide m

For, if $p_i|m- p_1.p_2. \ldots .p_n \Rightarrow p_i|1$, which is not true and hence contradiction.

$\therefore p_i \nmid m$

So, we have a prime p which in not in the list of n primes.

Thus we have n+1 primes $p_1, p_2, \ldots, p_n, p$.

Which is contradicts the assumption there are only n primes.

So, out assumption of finiteness is wrong.

Hence the number of primes is infinite.

A natural question now arises is that given an integer ≥ 2, can we say it is prime or not? The next theorem enables us to answer this question.

Theorem

Every composite number n has a prime factor $\leq \lfloor \sqrt{n} \rfloor$.

Proof

Given n is a composite number.

Then there exist positive integers a and b such that n=ab, where 1<a<n. 1<b<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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

We will now prove $a \le \sqrt{n}$ and $b \le \sqrt{n}$
Suppose $a > \sqrt{n}$ and $b > \sqrt{n}$
Then $a > \sqrt{n}$ =n $\Rightarrow n > n$ which is impossible.
$\therefore$ either $a \le \sqrt{n}$ or $b \le \sqrt{n}$
$\Rightarrow a \le \lfloor \sqrt{n} \rfloor$ or $b \le \lfloor \sqrt{n} \rfloor$ [$\therefore$ a and b are integers]
We know the every integer $n \ge 2$ has a prime factor.
Any such factor of a or b is also a factor of a x b = n.
So, n must have a prime factor $\le \lfloor \sqrt{n} \rfloor$.

Note From this theorem if follows that if n has no prime factor $\le \lfloor \sqrt{n} \rfloor$, then n is a prime

Problem
Show that 101 is a prime
Solution:-
Given number is 101.
First we find all primes $\le \lfloor \sqrt{101} \rfloor$= 10. The primes are 2,3,5,7.
Since none of these is a factor of 101, we get 101 is prime.

Problem
Determine whether 1601 is a prime.
Solution:-
Given the number is 1601
First we find all prime $\le \lfloor \sqrt{1601} \rfloor = \le [\ ] = 40$.
The primes are 2,3,5,7,11,13,17,19,23,29,31 and 37
Since none of these is a factor of 1601.
Hence 1601 is a prime.

Home work
Determine 1001 is a prime.

Problem
Find the smallest prime factor of 119.
Solution:-
Given number are 119
We have to find the smallest prime factor of 119.
First we find all the primes $\le \lfloor \sqrt{119} \rfloor$= 10. The primes are 2,3,5,7.
We find 7|119

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

So, the smallest prime dividing 119 is 7.

Definition

Let x be a positive real number. Then π(x) denotes the number of primes $\leq x$.

For example π(10) = 4 (∵ 2,3,5,7 are all primes ≤10)
π(18.75) = 7 (∵ 2,3,5,7 11,13,17are all primes ≤18.75)

If n is positive integer, then by using inclusion and exclusion principle we state a formula of π(n).

Theorem

Let $p_1, p_2, \ldots, p_n$, be the primes $\leq \lfloor \sqrt{n} \rfloor$. Then the number of primes $\leq n$ is π(n) and

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \left[\frac{n}{p_i}\right] + \sum_{i<j} \left[\frac{n}{p_i p_j}\right] - \sum_{i<j<k} \left[\frac{n}{p_i p_j p_k}\right] + \ldots + (-1)^r \left[\frac{n}{p_i p_j \cdots p_r}\right]$$

Problem

Find the number of primes ≤47

Solution:-

We have to find the number of primes ≤47.

Here n=47, then $\sqrt{47}$ =6.86

The primes $\leq \lfloor \sqrt{47} \rfloor$ are 2,3 and 5.

We know $\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \left[\frac{n}{p_i}\right] + \sum_{i<j} \left[\frac{n}{p_i p_j}\right] - \sum_{i<j<k} \left[\frac{n}{p_i p_j p_k}\right]$

$$\pi(47) = 47 - 1 + \pi(\sqrt{47}) - \left(\left[\frac{47}{2}\right] + \left[\frac{47}{3}\right] + \left[\frac{47}{5}\right]\right) + \left(\left[\frac{47}{2.3}\right] + \left[\frac{47}{2.5}\right] + \left[\frac{47}{3.5}\right]\right) - \left(\left[\frac{47}{2.3.5}\right]\right)$$

$$\pi(47) = 47 - 1 + 3 - ([23.5] + [15.66] + [9.4]) + ([7.83] + [4.7] + [3.13]) - [1.56]$$

$$\pi(47) = 47 - 1 + 3 - (23 + 15 + 9) + (7 + 4 + 3) - 1 = 49 - 47 + 14 - 1 = 15$$

Home work

Find the number of primes ≤100 [Ans.:- 25]

Theorem

Prime number theorem

If x > 0, then $\lim_{n \to \infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)}$ [lnx = natural log]

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

This means as x becomes very large π(x) approaches $\frac{x}{\ln x^*}$

* is known that 2, 3 are the only consecutive integers that are primes.
Also it is known that 3,5, 7 are the only three consecutive odd integers that are prime. However, there are many consecutive integers that are composite numbers. This is given by the next theorem.

Theorem

For every positive integer n, there are n consecutive integers that are composite numbers.

Proof

Let n be a positive integer and $n \geq 1$.

To prove the existence, we have to construction suitably.

Consider the n consecutive integers,

(n+1)! +2, (n+1)! + 3, (n+1)! + 4, . . . , (n+1)! + (n+1) where $n \geq 1$.

Suppose k is an integer such that $2 \leq k \leq n+1$, then k is a factor of (n+1)!

[$\because$ (n+1)!=1.2.3....k...n.(n+1)]

Now k|(n+1)! And k|k $\Rightarrow$ k|(n+1)!+k for every k.

$\therefore$ (n+1)!+k is a composite number for k=2,3, . . . , (n+1)

Thus the n consecutive composite numbers are

(n+1)! +2, (n+1)! + 3, (n+1)! + 4, . . . , (n+1)! + (n+1).

Problem

Find five consecutive composite numbers.

Solution:-

Here n=5,

We know that, the 5 consecutive composite integer are

(n+1)! +2, (n+1)! + 3, (n+1)! + 4, (n+1)! +5, (n+1)! + 6

Put n=5

(n+1)! +2 =6! +2 = 720 + 2 =722
(n+1)! +3 =6! +3 = 720 + 3 =723
(n+1)! +4 =6! +4 = 720 + 4 =724
(n+1)! +5 =6! +5 = 720 + 5 =725
(n+1)! +6 =6! +6 = 720 + 6 =726

$\therefore$ The five consecutive composite numbers are 722, 723, 724, 725, 726.

Home Work

Obtain six consecutive integers that are composite numbers.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

[Ans.:- 5042, 5043, 5044, 5045, 5046, 5047]

Problem

Find five consecutive integers < 100 that are composite numbers.

Solution:-

Since 5! = 120 > 100

We consider 4!, 4!+1, 4!+2, 4!+3, 4!+4

$\Rightarrow$ 24, 25, 26, 27, 28 are 5 consecutive composite numbers.

GREATEST COMMON DIVISOR (GCD) AND FUNDAMENTAL THEOREM OF ARITHMETIC

Definition

The greatest common divisor (gcd) of two integers a and b, not both zero, in the largest positive integer that divides both a and b.

It is denoted by gcd(a, b) or (a, b)

For example (12, 18) =6 (-15, 20)=5 (3,6)=3 (-3,6)=3 (12,23)=1

One way to find gcd of two integers is to find all positive common division and taken common largest common divisor

For example, the common factor of 24 and 36 are 1,2,3,4,6,12 of which largest is 12.

$\therefore$ gcd (24, 36) =12

Note

Since gcd (a, -b) = gcd(-a, b) = gcd(-a, -b) = gcd(a, b), we confine our discussion of gcd to positive integer. Now we give the symbolic definition of gcd.

Definition

A positive integer d is gcd of integers a and b if

(i) d|a and d|b

(ii) if c|a and c|b, then c|d, where c is the positive integer.

Theorem

The gcd of two positive integers a and b is a linear combination of a and b..

i.e., If d=(a, b), then d=la+mb for some integer l and 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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Let $S=\{xa+yb \mid xa+yb>0, x,y \in Z\}$

Since $a>0$, then $a=1a+0b \in S$

So, S is a nonempty set of positive integers.

Hence by well ordering principle S has a least positive integer d.

$\therefore d=la+mb$ for some integer l and m.

We shall now prove d=gcd (a, b).

Since $d>0$, by division algorithm to a and d we can find integer q and r such that

$a = qd + r, \ 0 \le r < d.$

$\Rightarrow \quad r = a - qd = a - q(la+mb) = (1-ql)a + (-qm)b$

This is shows that r is a liner combination of a and b.

If $r \neq 0$, then $r>0$ and so $r \in S$. Further $r<d$.

Hence we get a contradiction to the fact d is the least element of S.

$\therefore$ r=0. So, $a=qd \Rightarrow d|a$

Similarly we can prove d|b

Thus d is a common divisor of a and b.

If c|a and c|b then $c|la+mb \Rightarrow c|d$.

Hence d is a gcd of a and b $\Rightarrow$ d=(a, b).

Definition

Two positive integers a and b are relatively prime if gcd is 1 i.e., (a, b) =1

For example the gcd (8, 25) =1 and so 8 and 25 are relatively prime.

Corollary-1

Two positive integers a and b are relatively prime if and only if there exists integers $\alpha a + \beta b = 1$.

Proof:

If a and b are relatively prime, then (a, b) =1.

Then, there exists integers α and β such that $\alpha a + \beta b = 1$.

Conversely, let $\alpha a + \beta b = 1$.

To prove (a, b)=1

If d=(a, b), then d|a and d|b

$\Rightarrow d|\alpha a + \beta b \Rightarrow d|1$

$\therefore$ d=1 (as d>0)

$\Rightarrow$(a, b)=1 $\Rightarrow$a and b are relatively prime.

Corollary-2

If a|c and b|c and (a, b)=1 then prove that ab|c

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Given a|c and b|c
$\therefore$ c=ma and c=nb for some integer m,n
Also given (a,b)=1 $\Rightarrow \alpha$ a+β b=1, for some integers α and β
$\therefore \alpha$ ac+β bc=c $\Rightarrow$ α a(nb)+β b(ma)=c $\Rightarrow$ (α n +β m)ab=c $\Rightarrow$ ab|c.

Note
a|bc does not means a|b or a|c
For example, 6|24 $\Rightarrow$ 6|3.8.
But this does not mean that 6|3 or 6|8

Corollary-3
If a and b are relatively prime and if a|bc, then a|c.
Proof
Given (a, b)=1 $\Rightarrow \alpha$ a+β b=1, for some integers α and β.
Since a|α ac and a|bc, we get a|α ac+β bc
$\Rightarrow$ a|(α a+β b)c $\Rightarrow$ a|1.c $\Rightarrow$ a|c.

Theorem [Euclid's theorem]
If p is a prime and p|ab the p|a or p|b.
Proof
Given p is a prime and p|ab.
If p|a there is nothing to prove
If p ł a, then we have to prove p|b
Since p is a prime and p ł a, then (p,a)=1
$\therefore$ α p+β a=1, for some integers α and β.
Multiply by b, then α pb+β ab=b
Since p|ab and p|pb
We have p|α pb+β ab $\Rightarrow$ p|(α p+β a)b
$\Rightarrow$ p|1.b $\Rightarrow$ p|b.

Corollary,
If p is a prime and p|$a_1.a_2.a_3. . .a_n$, where a_1, a_2, a_3, . . . a_n are positive integers, then p|a_i for some i, $1 \le i \le n.$
Proof:
We prove by principle of induction
Let p(n) denote the statement p|$a_1.a_2.a_3. . .a_n \Rightarrow$ p|a_i for some a_i
If n=1, p(1) is p|$a_1 \Rightarrow$p|a_i which is true. $\therefore$ p(1) is true.
Assume that p(k) is true for an arbitrary k>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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

i.e., p| $a_1.a_2.a_3. . .a_k \Rightarrow$ p|a_i for some i, $1 \le i \le k.$
To prove p|(k+1) is true.
i.e., to prove p| $a_1.a_2.a_3. . .a_k.a_{k+1} \Rightarrow$ p|a_i for some a_i is true.
Consider p| $(a_1.a_2.a_3 . . .a_k).a_{k+1}$
Then p| $a_1.a_2.a_3. . .a_k$ or p|a_{k+1} by Euclid's Theorem
If p| $a_1.a_2.a_3 . . .a_k$ then by induction hypothesis, p|a_i for some a_i, $1 \le i \le k.$
Then p|a_i , $1 \le i \le k$ or p|a_{k+1}.
Hence p|a_i , $1 \le i \le k+1 \Rightarrow$ p(k+1) is true.
Thus p(k) is true $\Rightarrow$ p(k+1) is true.
Hence by principle of induction p(n) is true for all $n \ge 1$.

Definition
The gcd of n positive integer $a_1, a_2, a_3 , . . . a_n$ is the largest positive integer d that divide each a_i, where $n \ge 2$.

We denote the gcd as d = $(a_1, a_2, a_3, . . . a_n)$.

We remarked earlier that the prime numbers are building blocks of integers. This means that integers are made up to prime numbers or every integer can be decomposed into prime numbers.

Theorem: Fundamental theorem of arithmetic.
Every integer n (≥ 2) is either a prime or can be written as a product of primes in only one way, except for the order of the factors.
Proof:
We prove by second principle of induction.
Let p(n) denote the poroposition n is a prime or can be expressed as a product of primes.
To prove p(n) is true or all $n \ge 2$.

Basis step: Here $n_0 = 2$
$\therefore$ p(2) = 2, which is a prime
Thus p(2) is true.

Inductive Step: Assume that the proposition is true for all integers upto k, $k > 2$.
i.e., p(3), p(4), . . . ,p(k) are true.
To prove p (k+1) is true.
i.e., to prove k+1 is either a prime or is a product of primes.
If (k+1) is a prime, then we are through.
If (K+1) is not a prime, then it is a composite number.
$\therefore$ k+1 = xy is a product of two or more primes.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

$\therefore$ P(k+1) is true.

Hence by second principle or strong principle of induction p(n) is true for all $n \geq 2$.

Thus every integer n (≥ 2) is either a prime or product of primes.

Next we prove uniqueness of the product.

Let $n = p_1.p_2.p_3. \ldots .p_r$ and $n = q_1.q_2.q_3. \ldots .q_s$ be two factorizations of n into product or primes.

We shall prove that r=s and every p_i is some q_j, $1 \leq i \leq r, 1 \leq j \leq r.$

We have $p_1.p_2.p_3. \ldots .p_r = q_1.q_2.q_3. \ldots .q_s$

Suppose r<s

Since $p_1 | p_1.p_2.p_3. \ldots .p_r$ we have $p_1 | q_1.q_2.q_3. \ldots .q_s$ and p_1 is a prime.

$\therefore$ p_1 must divide some $q_j \Rightarrow p_1 = q_j$, as they are prime.

Divide both side of p_1, we get $p_2 . p_3. \ldots . p_n = q_1q_2. \ldots . q_{j-1}.q_{j+1}. \ldots .q_s.$

Repeat this argument with $p_2, p_3, \ldots, p_r.$

Since r<s, finally we get 1=a product of q's (the excess over r)

i.e., 1 = a product of primes, which is a contradiction.

$\therefore$ Our assumption r<s is wrong $\Rightarrow r \geq s.$

Similarly if s<r (arguing with q's instead of p's)

We get the contradiction

$\therefore$ $s \geq r$ and hence r=s.

Hence the primes $p_1, p_2, p_3, \ldots .p_r$ and same as $q_1, q_2, q_3, \ldots .q_s$ in some order.

Thus the factorization is unique, except for the order.

This theorem is also known as unique factorization theorem for positive integers.

For example

$240 = 2^4.3.5$

$250 = 2.5^3$

2	250
5	125
5	25
	5

2	240
2	120
2	60
2	30
3	15
	5

These are called prime power decomposition.

Since the primes are written in increasing order, these decompositions are called canonical decomposition.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Definition

The canonical decomposition pf a positive integer n is of the form $n = p_1^{\alpha_1}.p_2^{\alpha_2}.p_3^{\alpha_3}...p_k^{\alpha_k}$, where p_1, p_2. p_3, … p_k are distinct primes with $p_1 < p_2 < p_3 < ... < p_k$ and $\alpha_1, \alpha_2, \alpha_3, ...\alpha_k$ are positive integers.

Problem

Find the canonical decomposition of (i) 999 (ii) 1024 (iii) 2520

Solution

3 | 999
3 | 333
3 | 111
37

2 | 1024
2 | 512
2 | 256
2 | 128
2 | 64
$32 = 2^5$

2 | 2520
2 | 1260
2 | 630
3 | 315
3 | 63
3 | 21
7

(i) $999 = 3.3.3.37 = 3^3.37$

(ii) $1024 = 2^{10}$

(iii) $2520 = 2^3.3^3.7$

These are canonical decompositions.

We can use canonical decomposition to find gcd of two positive integers.

Problem

Find the gcd of 414 and 662 using canonical decompositions.

Solution

We have to find gcd of 414, 662

First we find the canonical decomposition

$414 = 2.3^2.23$

$662 = 2.331$

$\therefore$ gcd (414,662) = 2

2 | 414
3 | 207
3 | 69
23

2 | 662
331

Problem

Find (175, 192) using canonical decomposition

Solution:-

We have to find (175, 192)

First we find the canonical decomposition

$175 = 5^2.7$

$192 = 2^7.3$

5 | 175
5 | 35
7

2 | 192
2 | 96
2 | 48
2 | 24
2 | 12
2 | 6
3

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

We notice that there is no common factor except 1
$\therefore$ (175, 192) = 1

Problem
Find the gcd of 120 and 500
Solution
We have to find gcd of 120 and 500
First find the canonical decomposition
$\therefore$ $120 = 2^3.3.5$
and $500 = 2^2.5^3$
$\therefore$ gcd(120, 500) = $2^2.5$ =20

2 | 120	2 | 500
2 | 60	2 | 250
2 | 30	5 | 125
3 | 15	5 | 25
5	5

Home work
Find gcd of 168 and 180 using canonical decomposition [Ans.:- 12]

Notice that we choose the common factors with smaller index.
More generally,
If $a = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ and $b = p_1^{\beta_1}.p_2^{\beta_2}....p_k^{\beta_k}$ are the canonical decompositions of a and b, then gcd (a, b) = $p_1^{\min(\alpha_1,\beta_1)}.p_2^{\min(\alpha_2,\beta_2)}...p_k^{\min(\alpha_k,\beta_k)}$

Problem
Use recursion to evaluate (12, 36, 60, 108)
Solution
We have to evaluate gcd (12, 36, 60, 108)
We isolate each term from right and find gcd of the inner group as below
$\therefore$ (12, 36, 60, 108) = ((12, 36, 60) 108) = (((12, 36), 60), 108)
Now (12, 36) = 12
((12, 36), 60) = (12, 60) =12
(((12,36), 60), 108) = (12, 108) =12
$\Rightarrow$ (12, 36, 60, 108) = 12

Problem
Use recursion to evaluate (18, 30, 60, 75, 132)
Solution
We have to evaluate gcd (18, 30, 60, 75, 132)
We isolate each term from right and find gcd of the inner group as below

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 : III	**Unit Name:** DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

$\therefore$ (18, 30, 60, 75, 132) = ((18, 30, 60, 75), 132)
= (((18, 30, 60), 75), 132)
= ((((18, 30), 60), 75), 132)

2 | 18, 30
3 | 9, 15
3 5 no common factor

Now (18, 30) = 2.3 =6

$\therefore$ (18, 30), 60) = (6, 60)= 6 (6 is a factor of 60)
(18, 30), 60), 75) = (6, 75) = 3
(18, 30), 60), 75), 132) = (3, 132) = 3 (3 is factor of 132)
$\therefore$ (18, 30, 60, 75, 132) = 3

3 | 6, 75
2, 25 no common factor

Home Work

Using recursion to evaluate (i) (12, 18, 28, 38, 44) (ii) (15, 24, 28, 45)

[Ans.:- (i) 2, (ii) 1]

Problem

Find the gcd of 92928 and 123552

Solution

We have to find gcd of 92928 and 123552

First we find the canonical decomposition

$\therefore$ $92928 = 2^8.3.11^2$

$123552 = 2^5.3^3.11.13$

$\therefore$ the gcd of 92928 and 123552 = $2^5.3.11 = 1056$

2 | 92928
2 | 46464
2 | 23232
2 | 11616
2 | 5808
2 | 2904
2 | 1452
2 | 726
3 | 363
11 | 121
11

2 | 123552
2 | 61776
2 | 30888
2 | 15444
2 | 7722
3 | 3861
3 | 1287
3 | 429
11 | 143
13

Alter:

We can find gcd as below taking both the numbers

2 | 92928, 123552
2 | 46464, 61776
2 | 23232, 30888
2 | 11616, 15444
2 | 5808, 7722
3 | 2904, 3861
11 | 968, 1287
88 117 no common factor

$\therefore$ gcd (92928, 123552) = $2^5.3.11 = 1056$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Problem

Find the gcd of $a = 2^2.3^3.5^2.7.11^2$ and $b = 2^{11}.3^9.5^3.11$

Solution

Given $a = 2^2.3^3.5^2.7.11^2$

and $b = 2^{11}.3^9.5^3.11$

$(a, b) = 2^2.3^3.5^2.11$

$=2.27.25.11$

$=29700$ (Choosing minimum of powers of common factors)

THE GCD AND THE EUCLIDEAN ALGORITHM

A powerful theoretical tool for GCD of two positive integers a and b as a linear combination of a and b. But it does not provide us with practical method of finding GCD of a and b.

Euclidean algorithm, which is repeated application of division algorithm, gives us an efficient method of finding GCD of two positive integers.

Theorem

Let a and b be two positive integers such that

$a = qb + r$, $0 \le r < b$.

Then the GCD(a, b) = the GCD (b, r).

Proof

Given a and b are positive integer such that

$a = qb + r$, $0 \le r < b$. ⟶ (1).

$\Rightarrow$ $a - qb = r$

Let $d = GCD(a, b)$ and $d^1 = GCD(b, r)$

To prove $d = d^1$

Since $d = GCD(a, b)$, $d|a$ and $d|b \Rightarrow d|a-qb \Rightarrow d|r$

Thus $d|b$ and $d|r$ and so $d|GCD(b,r) \Rightarrow d|d^1$

Since $d^1 = GCD(b, r)$, $d^1|b$ and $d^1|r$

$\therefore (1) \Rightarrow$ $d^1|a$

Thus $d^1|a$ and $d^1|b$ and so $d^1|GCD(a,b) \Rightarrow d^1|d$

Hence $d = d^1 \Rightarrow GCD(a, b) = GCD(b, r)$

The gcd(b, r) means the gcd of the divisor and remaninder.

THE EUCLIDEAN ALGORITHM

Suppose a and b are positive integer with $a \ge b$

If a = b then (a,b)=(a,a)=a

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

So assume a > b

Then by successive application of division algorithm, we get

$a = q_1 b + r_1$, $0 \le r_1 < b$.

$b = q_2 b + r_2$, $0 \le r_2 < r_1$

$r_1 = q_3 r_2 + r_3$, $0 \le r_3 < r_2$

. . . . . .

. . . . . .

$r_{n-2} = q_n r_{n-1} + r_n$, $0 \le r_n < r_{n-1}$

and $r_{n-1} = q_{n+1} r_n + 0$

Where $b > r_1 > r_2 > \ldots \ge 0$. The sequence of remainders terminates with remainder 0.

By above theorem

$\gcd(a, b)=\gcd(b,r_1)=\gcd(r_1,r_2)= \ldots =\gcd(r_{n-1},r_n)=r_n$

Thus $(a,b)=r_n$, where r_n is the last non-zero remainder in the sequence of divisions.

Problem

Find the gcd (414, 662) using Euclidean algorithm.

Solution

We have to find the gcd (414, 662). Here 662 > 414.

Applying division algorithm successively, we get

662 = 1(414) + 248

414 = 1(248) + 166

248 = 1(166) + 82

166 = 2(82) + 2

82 = 41(2) + 0

The last non-zero remainder is 2.

∴ the gcd(414, 662) = 2

Problem

Find the gcd (2076, 1776) using Euclidean algorithm.

Solution

We have to find the gcd (2076, 1776). Here 2076 > 1776.

Applying division algorithm successively, we get

2076 = 1(1776) + 300

1776 = 5(300) + 276

300 = 1(276) + 24

276 = 11(24) + 12

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

$24 = 2(12) + 0$

The last non-zero remainder is 12.

$\therefore$ the gcd(2076, 1776) = 12.

Home work

Apply Euclidean algorithm to compute (3076, 1976). [Ans:- 4]

Problem

Apply Euclidean algorithm to express the gcd of 1976 and 1776 as a linear combination of them.

Solution:-

We have to find the gcd (1976, 1776). Here 1976 > 1776.

Applying division algorithm successively, we get

$1976 = 1(1776) + 200$

$1776 = 8(200) + 176$

$200 = 1(176) + 24$

$176 = 7(24) + 8$

$24 = 3(8) + 0$

The last non-zero remainder is 8

$\therefore$ the gcd(1976, 1776) = 8.

Using the above equations in reverse order and substituting for remainder each time.

We get the linear combination of 1976 and 1776.

$$\begin{aligned}(1976, 1776) &= 8\\ &= 176 - 7(24)\\ &= 176 - 7(200-1(176))\\ &= 176-7(200) + 7(176)\\ &= 8(176) - 7(200)\\ &= 8(1776 - 8(200)) - 7(200)\\ &= 8(1776) - 64(200) - 7(200)\\ &= 8(1776) - 71(200)\\ &= 8(1776) - 71(1976 - 1(1776))\\ &= 8(1776) - 71(1976) + 71(1776)\\ &= 79(1776) - 71(1976)\\ &= 79(1776) + (-71)(1976)\end{aligned}$$

Home Work

Using the Euclidean algorithm to express the gcd of 4076 and 1024 as a linear combination of them. [Ans:- gcd(4076, 1024) =4 =51(4076) + (– 203)(1024)]

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 : III	**Unit Name:** DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Theorem

There are infinitely many primes of the form 4n+3.

Proof

We prove by contradiction method.

Suppose there are only finite number of primes of the form 4n+3.

$p_0, p_1, p_2 \ldots p_k$ where $p_0=3$ and p_k is the largest prime.

Consider the positive integer $m = 4p_1p_2\ldots p_k+3$

Clearly $m > p_k$ and is on the form 4n+3 (Here $n=p_1p_2\ldots p_k$

If m is a prime, then m is prime larger, than the largest prime p_k.

which is a contradiction.

If m is not a prime, then m is a composite numb er

Clearly m is an odd number.

So, every factor of m is of the form 4n+1 or 4n+3

Suppose every factor is on the form 4n+1, then their product will be of the form 4n+1

$\therefore$ m will be of the form 4n+1 [$\because (4l+1)(4m+1)=16im+4l+4m+1=4(4im+l+m)+1$]

Since m is of the form 4n+3, at least one of thefactors of m, say p, is of the form 4n+3

If $p=p_0=3$, then $3|m$ and $3|3 \Rightarrow 3|m-3$

$\therefore$ $3|4p_1p_2\ldots p_k \Rightarrow 3|4$ or $3|$some p_i [By Euclid's lemma]

But both are impossible and hence a contradiction.

If $p=p_i$ for some p_i, then $p|m$ and $p|p_1p_2\ldots p_k \Rightarrow p|3$, a contradiction

Therefore in both cases, we get a contradiction.

This means our assumption of finiteness is wrong.

Hence there are infinitely many primes of the form 4n+3.

Problem

For any positive integer n, prove that 8n+3 and 5n+2 are relatively prime.

Solution:-

To prove (8n+3, 5n+2) = 1

When n=1, 8n+3=11 and 5n+2=7

$\therefore$ gcd(11, 7) = 1

Hence it is true when n=1

For $n \geq 2$, we have 8n+3 > 5n+2. By division algorithm,

8n+3 = 1.(5n+2) + (3n+1), $0 \leq 3n+1 < 5n+1$

5n+2 = 1.(3n+1) + (2n+1), $0 \leq 2n+1 < 3n+1$

3n+1 = 1.(2n+1) +n , $0 \leq n < 2n+1$

2n+1 = 2(n) + 1, $0 \leq 1 < n$

n = 1.(n) +0

$\therefore$ the last nonzero remainder is 1.

$$\begin{array}{r|l} & 1 \\ 5n+2 & \overline{8n+3} \\ & \underline{5n+2} \\ & 3n+1 \end{array} \qquad \begin{array}{r|l} & 1 \\ 3n+1 & \overline{5n+2} \\ & \underline{3n+1} \\ & 2n+1 \end{array}$$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

$\therefore$ gcd(8n+3, 5n+2) = 1

So, 8n+3 and 5n+2 are relatively prime for any positive integer.

Problem

Prove that (a, a-b) = 1 if and only if (a, b) = 1.

Solution:-

Let (a, b) = 1

Then there exist integer l and m such that

$la + mb = 1$

$\Rightarrow$ $la + ma + mb - ma = 1$ [adding ma and subtracting ma]

$\Rightarrow$ $(l+m)a - m(a-b) = 1$

$\Rightarrow$ $(l+m)a + (-m)(a-b) = 1$

$\Rightarrow$ $(a, a-b) = 1$

Conversely, let (a, a-b) = 1. To prove (a, b)=1

Then there exist integers s and t such that

$sa + t(a-b) = 1$

$\Rightarrow$ $sa + ta - tb = 1$

$\Rightarrow$ $(s+t)a + (-t)b = 1$

$\Rightarrow$ $(a, b) = 1$

Note Similarly, we can prove that if (a, b) = d, then (a, a-b) = d.

Problem

If the square of an integer is odd, then prove that the integer is odd.

Solution:-

Let n be an integer such that n^2 is odd.

To prove n is odd

Suppose n is not odd, then n is even

$\therefore$ $n = 2m$ for some integer m.

$\therefore$ $n^2 = 4m^2 = 2(2m^2)$

which is even and hence a contradiction.

$\therefore$ n is odd

Similarly, we can prove that if n^2 is even, then n is even.

Problem

If (a, b)=1, then prove that $(a^2, b^2) = 1$.

Solution:-

Given (a, b) = 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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

To prove that $(a^2, b^2) = 1$

Suppose $(a^2, b^2) \neq 1$, then a^2 and b^2 have a common factor and hence have a prime factor p.

$\therefore$ $p|a^2$ and $p|b^2$

$\Rightarrow$ $p|a.a$ and $p|b.b$

$\Rightarrow$ $p|a$ and $p|b$ [$\because$ p is a prime and $p|ab \Rightarrow p|a$ or $p|b$]

$\therefore$ p|the greatest common divisor of a and b.

$\Rightarrow$ $p|(a, b) \Rightarrow p|1$

which is not possible and hence a contradiction.

$\Rightarrow$ $(a^2, b^2) = 1$

Problem

If a and b are positive integers such that b|a and b|a+2, prove that b = 1 or 2.

Solution:-

Given b|a and b |a+2

$\therefore$ b||la + m(a+2) for all integers l, m

$\Rightarrow$ b|(l+m)a + 2m for all l,m

In particular, it is true for l=-1, m=1

$\Rightarrow$ $b|0a+2 \Rightarrow b|2$

Since b is a positive integer

$b|2 \Rightarrow b = 1$ or 2

Problem

If a,b are odd positive integers, prove that $2|a^2+b^2$ but $4 \nmid a^2+b^2$.

Solution:-

Given a and b are odd positive integers.

Then a=2m+1 and b=2n+1, where m and n are integers ≥ 0

$\therefore$ $a^2+b^2 = (2m+1)^2 + (2n+1)^2$

$= 4m^2+4m+1 + 4n^2+4n+1$

$= 4m^2+ 4n^2+4m+4n+2$

$= 2(2m^2+ 2n^2+2m+2n+1)$

$\therefore$ $2| a^2+b^2$, but $4 \nmid a^2+b^2$ [$\because 2m^2+ 2n^2+2m+2n+1$ is an odd integer]

Problem

Prove that the product of any two integer of the form 4k+1 is also same form.

Solution:-

Let a = 4s+1 and b=4t+1 be two integers

To prove ab is of the form 4n+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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Then a.b = (4s+1)(4s+1)
= 16st + 4s + 4t +1
= 4(4st+s+t) + 1
= 4n+1
which is of the same form
Hence ab is of the form 4n+1.

LEAST COMMON MULTIPLE (LCM)

Definition

The least common multiple of two positive integers a and b is the smallest positive integer that is divisible by both a and b.

The lcm of a and b is denoted by [a, b] or lcm(a,b)

We can use canonical decomposition to find them.

If $a = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ and $b = p_1^{\beta_1}.p_2^{\beta_2}....p_k^{\beta_k}$ are the canonical decompositions of a and b, then [a,b] = lcm (a, b) = $p_1^{\max(\alpha_1,\beta_1)}.p_2^{\max(\alpha_2,\beta_2)}...p_k^{\max(\alpha_k,\beta_k)}$

Problem

Find the lcm of 1050 and 2574.

Solution:-

We have to find lcm of 1050 and 2574

First we find the canonical decompositions.

$\therefore$ $1050 = 2.3.5^2.7 = 2.3.5^2.7.11^0.13^0$

and $2574 = 2.3^2.11.13 = 2.3^2.5^0.7^0.11^1.13^1$

$\therefore$ the lcm(a,b) = product of factors with maximum indices.

$\Rightarrow$ $[1050, 2574] = 2.3^2.5^2.7.11.13 = 450450.$

Problem

Find the gcd and lcm of 120 and 500.

Solution:-

We have to find lcm of 120 and 500

First we find the canonical decompositions.

$\therefore$ $120 = 2^3.3.5$

and $500 = 2^2.5^3$

$\therefore$ the gcd(a,b) = product of factors with minimum indices.

$\Rightarrow$ $(120, 500) = 2^2.5 = 20.$

and the lcm(a,b) = product of factors with maximum indices.

$\Rightarrow$ $[120, 500] = 2^3.3.5^3 = 3000.$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Home work

Find the gcd and lcm of 504 and 540. {Ans.:- (504, 540) = 36 & [504, 540]=7560}

Theorem

If a and b are positive integer, then $[a,b]=\frac{a.b}{(a,b)}$. $or\left\{(a,b)=\frac{a.b}{[a,b]}\right\}$

Proof

Let $a=p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ and $b=p_1^{\beta_1}.p_2^{\beta_2}....p_k^{\beta_k}$ be the canonical decompositions of a and b.

Then (a, b) = $p_1^{\min(\alpha_1,\beta_1)}.p_2^{\min(\alpha_2,\beta_2)}...p_k^{\min(\alpha_k,\beta_k)}$

and [a, b] = $p_1^{\max(\alpha_1,\beta_1)}.p_2^{\max(\alpha_2,\beta_2)}...p_k^{\max(\alpha_k,\beta_k)}$

$\therefore$ (a, b).[a, b] = $p_1^{\min(\alpha_1,\beta_1)+\max(\alpha_1,\beta_1)}.p_2^{\min(\alpha_2,\beta_2)+\max(\alpha_2,\beta_2)}...p_k^{\min(\alpha_k,\beta_k).\max(\alpha_k,\beta_k)}$

= $p_1^{\alpha_1+\beta_1}.p_2^{\alpha_2+\beta_2}...p_k^{\alpha_k+\beta_k}$

= $p_1^{\alpha_1}.p_1^{\beta_1}.p_2^{\alpha_2}p^{\beta_2}...p_k^{\alpha_k}p_k^{\beta_k}$

= $p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}.p_1^{\beta_1}.p_2^{\beta_2}....p_k^{\beta_k}$

= a.b

$\therefore$ $[a,b]=\frac{a.b}{(a,b)}$ $or\left\{(a,b)=\frac{a.b}{[a,b]}\right\}$

Note

1. This theorem gives another method for finding lcm
2. If a and b are relatively rime, then (a, b) = 1

   $\therefore$ $[a,b]=\frac{a.b}{(a,b)} \Rightarrow [a,b]=\frac{a.b}{1} \Rightarrow$ [a, b] = a.b

   Thus lcm of relatively prime numbers is their product.

Problem

Find the lcm of 504 and 540 using their gcd

Solution:-

We have to find lcm of 504 and 540

First we find the canonical decompositions.

$\therefore$ $504 = 2^3.3^2$

and $540 = 2^2.3^3.5$

$\therefore$ the gcd(a,b) = product of factors with minimum indices.

$\Rightarrow$ $(120, 500) = 2^2.3^2 = 36$.

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

WKT $[a,b]=\frac{a.b}{(a,b)} \Rightarrow [a,b]=\frac{504.500}{36}$ = 7560

Problem
Use recursion to evaluate [24, 28, 36, 40]
Solution:-
We have to find [24, 28, 36,40]
We isolated each term from the right and the lcm of inner group as below

$\therefore$ [24, 28, 36,40] = [[24, 28, 36] 40]
= [[[24, 28], 36] 40]
But [24, 28] = 2.2.6.7 = 168

$\therefore$ [[24, 28] 36] = [168, 36]
= 2.2.3.14.3 = 540
$\therefore$ [[[24, 28] 36] 40] = [540 , 40]
= 2^2.5.63 = 2520
$\therefore$ [24, 28, 36,40]= 2520

2 | 24, 18
2 | 12, 14
6, 7 (no common factor)

2 | 168, 30
2 | 84, 18
3 | 42, 9
14, 3 (no common factor)

2 | 504, 40
2 | 252, 20
2 | 126, 10
63, 5 (no common factor)

Home work
Use recursion to find [15, 18, 24, 30] [Ans.:- 360]

Problem
Find the positive integer a if [a, a+1] = 132.
Solution:-
Given [a, a+1] = 132
Since a and a+1 are consecutive integers, they are relatively prime.
$\therefore$ (a, a+1) = 1
Hence [a, a+1] = a(a+1)
132 = a(a+1)
a(a+1) = 11.12
$\therefore$ a = 11

We now state a result concerning n!
If p is a prime and p|n!, then the highest power of p dividing n ! in its canonical decomposition is $=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$

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 : III	Unit Name: DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

It is finite sum because $\left[\frac{n}{p^m}\right] = 0 \; if \; p^m > n$

Problem

Find the canonical decomposition of 23!

Solution:-

The prime dividing 23! are 2,3,5,7,11,13,17,19,23 [$\because$ 23!=1.2.3.4.5. . . . .23]

The power of 2 dividing 23! is = $\left[\frac{23}{2}\right]+\left[\frac{23}{2^2}\right]+\left[\frac{23}{2^3}\right]+\left[\frac{23}{2^4}\right]$ [$\because 2^5$=32 > 23]

= 11+5+2+1 = 19 .

The power of 3 dividing 23! is = $\left[\frac{23}{3}\right]+\left[\frac{23}{3^2}\right]$ [$\because 3^3$ =27 > 23]

= 7+2 = 9

The power of 5 dividing 23! is = $\left[\frac{23}{5}\right]$ = 4 [$\because 5^2$ =25 > 23]

The power of 7 dividing 23! is = $\left[\frac{23}{7}\right]$ = 3 [$\because 7^2$ =49 > 23]

The power of 11 dividing 23! is = $\left[\frac{23}{11}\right]$ = 2 [$\because 11^2$ =121 > 23]

The power of 17 dividing 23! is = $\left[\frac{23}{17}\right]$ = 1

The power of 19 dividing 23! is = $\left[\frac{23}{19}\right]$ = 1

The power of 23 dividing 23! is= $\left[\frac{23}{23}\right]$ = 1

$\therefore$ the canonical decomposition of 23! =$2^{19}.3^9.5^4.7^3.11^2.13.17.19.23$

Problem

Find the largest power of 2 that divides 97!

Solution:-

We know 2|97!

$\therefore$ the largest power of 2 dividing 97! Is

= $\left[\frac{97}{2}\right]+\left[\frac{97}{2^2}\right]+\left[\frac{97}{2^3}\right]+\left[\frac{97}{2^4}\right]+\left[\frac{97}{2^5}\right]+\left[\frac{97}{2^6}\right]$ ([$\because 2^7$=128 > 97]

= 48 + 24 + 12 + 6 + 3 + 1 =94

$\therefore$ 2^{94} is the highest power of 2 dividing 97.

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 : III	**Unit Name:** DIVISIBILITY THEORY AND CANONICAL DECOMPOSITIONS	Date	14-11-2017

LECTURE NOTES

Find the number of trailing zeros in the decimal value of 260!

Solution:-

The number of zeros in which 260! Is ending with is the same as the highest power of 10 dividing 260!

Now $10 = 2.5$

$10^m = 2^m.5^m$

$\therefore$ the highest power of 10 is the same as highest power of 5.

The highest power of 5 dividing 260! is = $\left[\frac{260}{5}\right]+\left[\frac{260}{5^2}\right]+\left[\frac{260}{5^3}\right]$ ($\because 5^4=625 > 260$]

$= 52+10+2 = 64$

$\therefore$ 10^{64} is the highest power of 10 dividing 260!

$\therefore$ the number of zeros in the decimal form of 260! Is 64

In other words, 260! ends 64 zeros.

Note If we find the highest power 2 contained in 260!, then we get

$$= \left[\frac{260}{2}\right]+\left[\frac{260}{2^2}\right]+\left[\frac{260}{2^3}\right]+\ldots\left[\frac{260}{2^8}\right]=258$$

Min (258, 64) = 64

So, it is enough we find the power of 5.

Home work

Find the number of trailing zeros in 234! [Ans.:- 56]