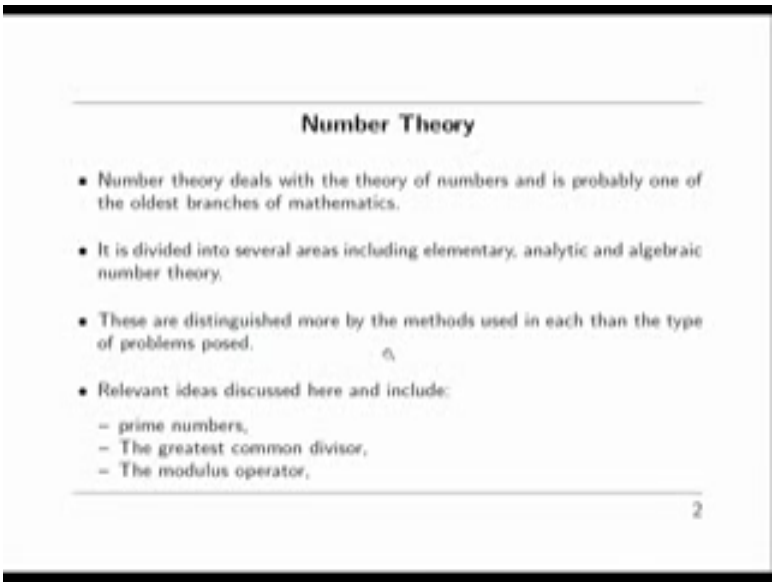
**Internetwork Security**
**Prof. Sourav Mukhopadhyay**
**Department of Mathematics**
**Indian Institute of Technology, Kharagpur**

**Lecture - 14**
**Number Theory**

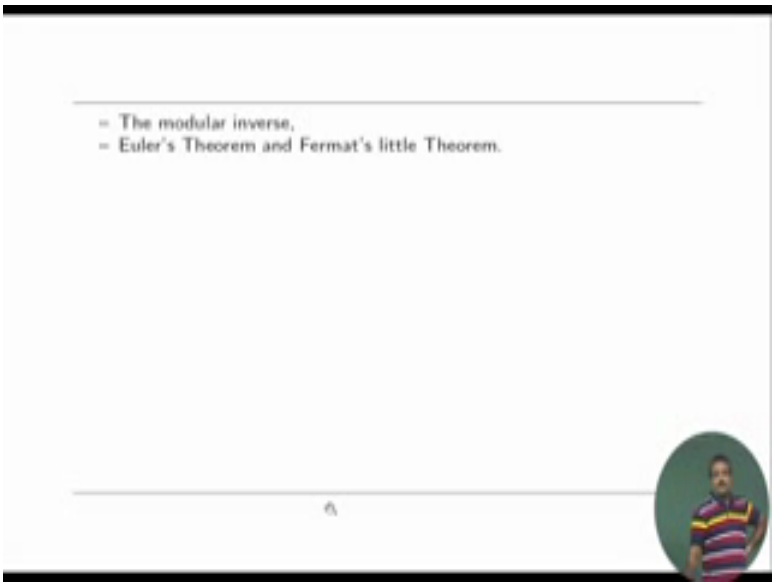
We will talk about number theory which is the very essential field in mathematics which is the very oldest field in mathematics and which is required for our cryptographic protocol; cryptographic primitives. So, let us start with the number theory. So, slide please.

(Refer Slide Time: 00:45)



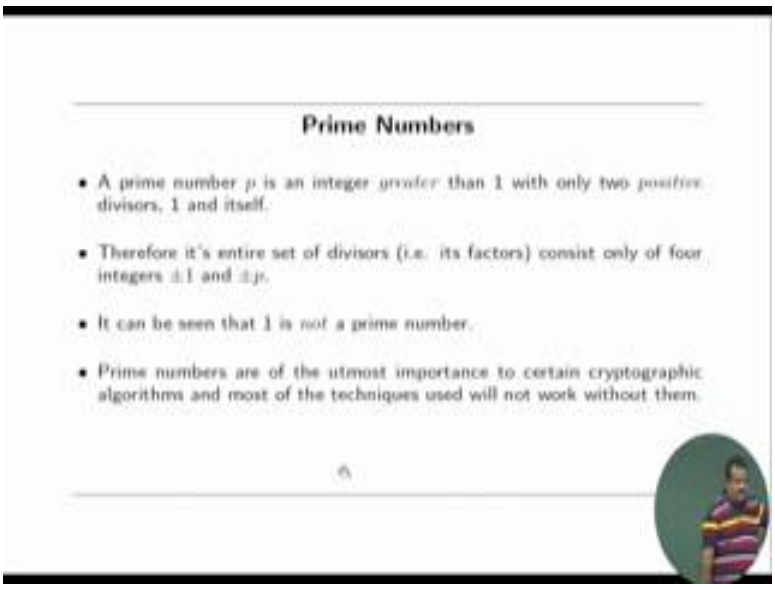

The number theory deals with the theory of numbers and it is probably one of the oldest branches of mathematics, it is a divided into several areas including elementary number theory, analytic number theory, algebraic number theory. So, depending on the method we will use to prove some theorem. These are the areas it is defined and here we will be talking about mostly on prime numbers, what are the prime numbers, what is a prime numbers because these prime numbers is required for many cryptographic scheme like RSA. So, we need to have primes. So, what is a prime numbers then we talk about the GCD, which is greatest common divisor between 2 numbers, 2 integers a b and then we talk about modulus operation, which is congruent operation basically.

(Refer Slide Time: 01:40)




And then we talk about modular inverse which is required in RSA and some other cryptographic primitives. And then we talk about some numbers theory result like Fermat's little theorem and Euler's theorem we will. So, discuss about Euler 5 function which is used in RSA and many other cryptosystem.

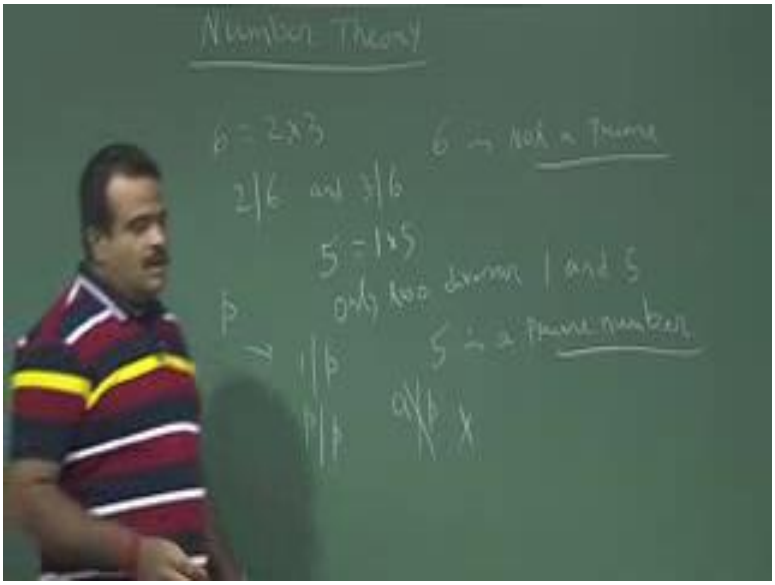
(Refer Slide Time: 02:07)




Let us start with the prime number. So, what is a prime number? Basically it is an integer greater than 1 and which has basically no divisor I mean which has basically only 2

divisor positive divisor 1 and itself. So, a number, an integer is called prime if it has no divisor other than divisor means it should divides that number like.

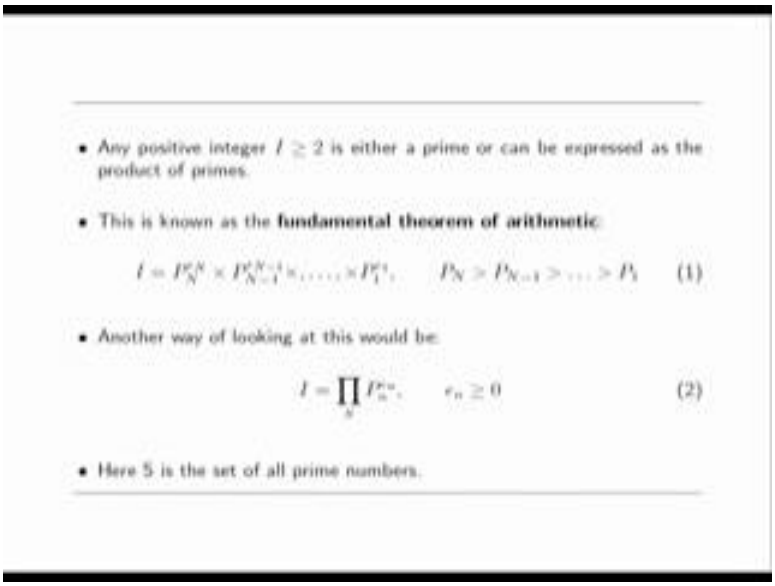
(Refer Slide Time: 02:38)




If we have a 6, 6 has 2 divisor 3 and 2. So, that means, 2 divide 6 and 3 divide 6 so; that means, since it has a divisor other than 6 other then itself an 1 so; that means, 6 is not a prime, but if we take 5, 5 is basically 1 into 5 so; that means, it has only 2 divisor only 2 positive divisor 1 and 5 itself then it is called a prime. So, 5 is a prime number is a prime number so and positive integer is called a prime if it is has 2 divisor only. So, P if P is called a prime, it has if it has 2 divisor only 1 and P itself no other no other integer a should exist so that it divides p. So, this should not be, we should not find a such that this exist. So, this is this number is P is then called prime number.

It can be seen that 1 is not a prime, 1 is consider not a prime. So, prime numbers are they have heavy important role in cryptographic algorithm. So, we will see those slowly.

(Refer Slide Time: 04:23)



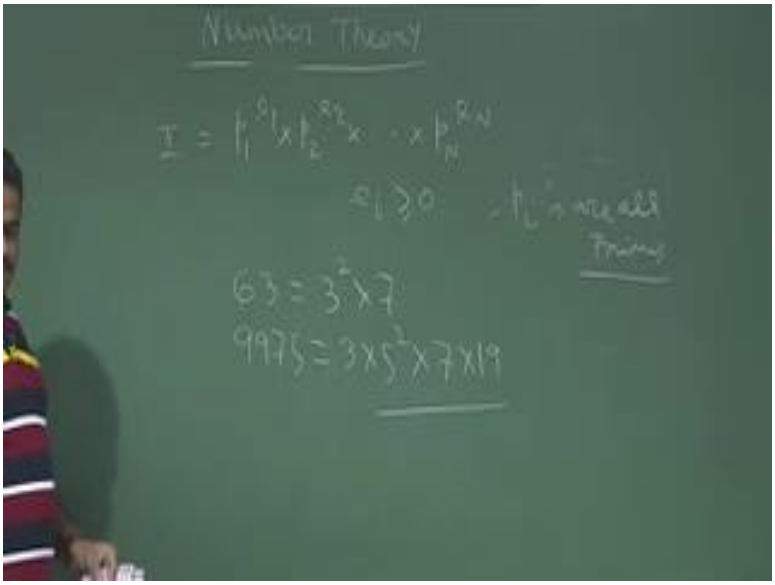

Now for any positive integer I, this is the fundamental theorem of arithmetic. So, any positive integer I, it is either a prime or it can be written as a product of prime. So, like if you have so any positive integer say 3, 3 itself is a prime, 7; 7 itself is a prime, suppose we have 21, 21 is not a prime, but it can be written as product of primes.

(Refer Slide Time: 04:50)


Now if you have 63, 63 can be written as in this form now for example, if we have this 9975. Any integer I is either a prime or it can be written as any positive integer it can be

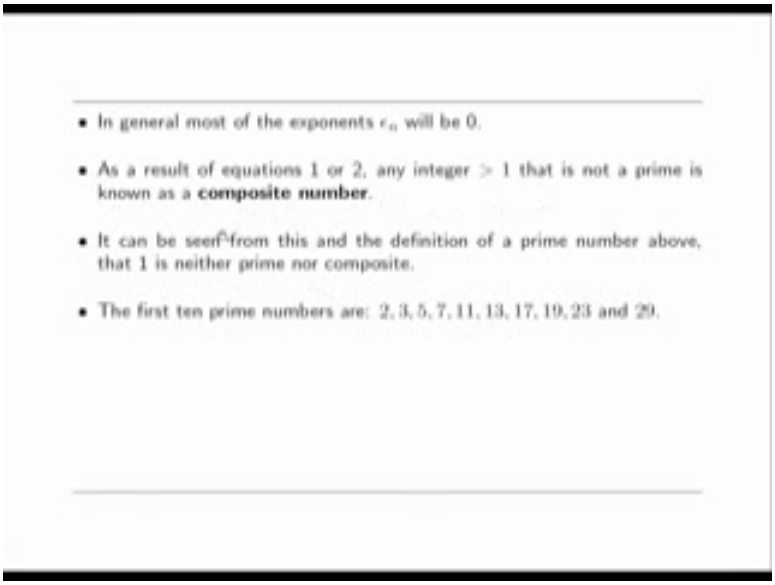
written as product of prime. So, this can be written as we can easily verify 5 square into 7 into 19.

(Refer Slide Time: 05:40)




That means, any integer I is either a prime or it can be written as a prime factor dot, dot, dot, say there are say n, p N e to the power N where e I are greater than equal to 0, this is a positive integer and p i is our all prime. So, this is the fundamental theorem of arithmetic. So, any integer i is either a prime or it can be written as product of prime factor like this.

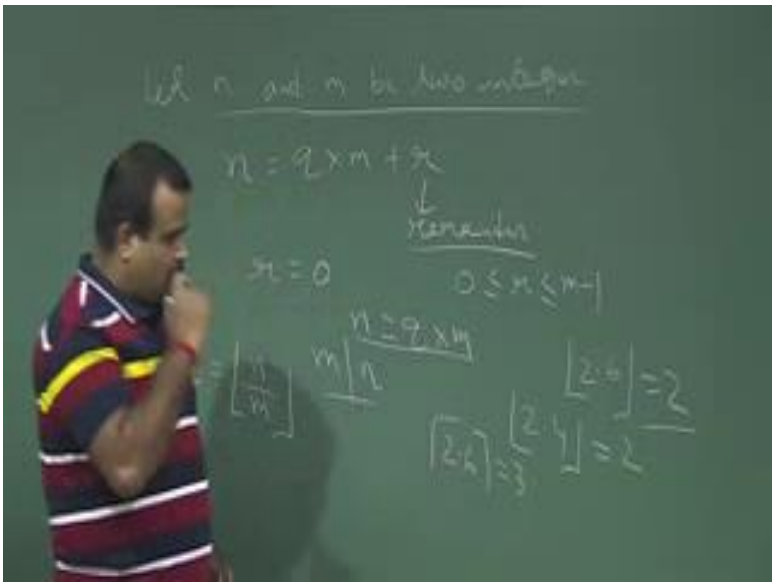
(Refer Slide Time: 06:31)



If integer is not a prime then it is called a composite number and then this is the first 10 primes 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, so these are all prime numbers. So, these are first 10 primes, we can easily verify all these number are basically prime numbers, it is not having any common any divisor other than 1 an itself. So, if a number is not a prime number, it is called composite number.

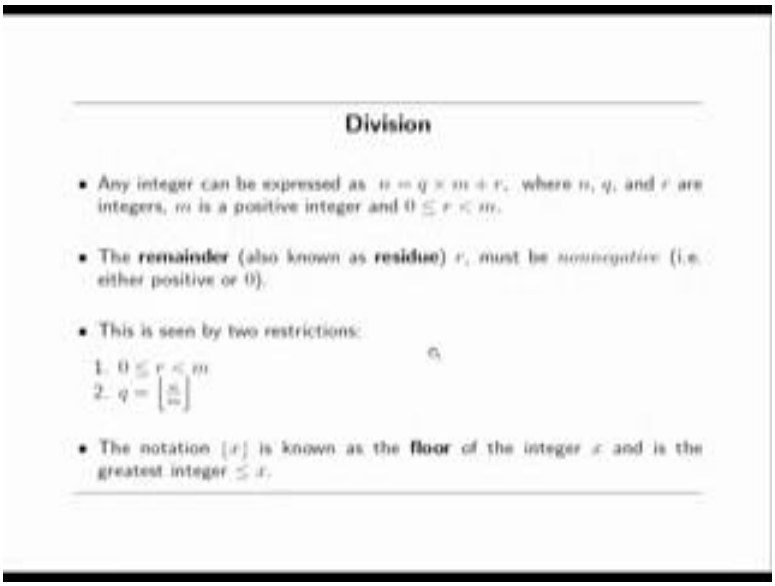
Now we will talk about division, what you mean by division of 2 numbers.

(Refer Slide Time: 07:24)



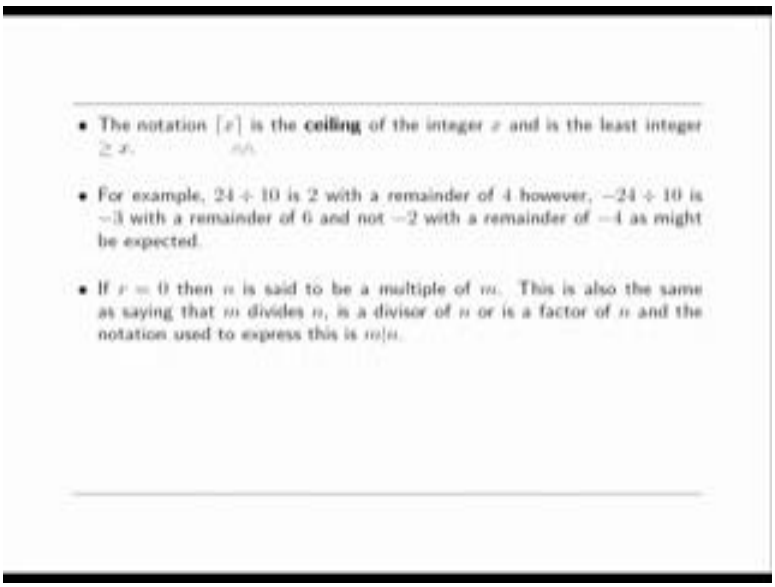

Suppose you have 2 integer, let n and m be 2 integer then if we try to divide n by m, so that means, n can be detain as q into m plus r and this r is basically called reminder and this r is always lies between 0 less than r less than equal to m minus 1 because r if r is greater than n then q will be q plus 1, we will divide once more like this and if r is 0, 0 then basically n is equal to q into m. That means, we say m divides n, we say this implies m divides n so; that means, m is a factor of n if r is equal to 0, this is the division rule and what is q? Q is basically n by m this is called lower ceiling lower ceiling means it is the least integer which is less than this. So, this is the flooring lower floor we have the upper floor.

(Refer Slide Time: 09:11)



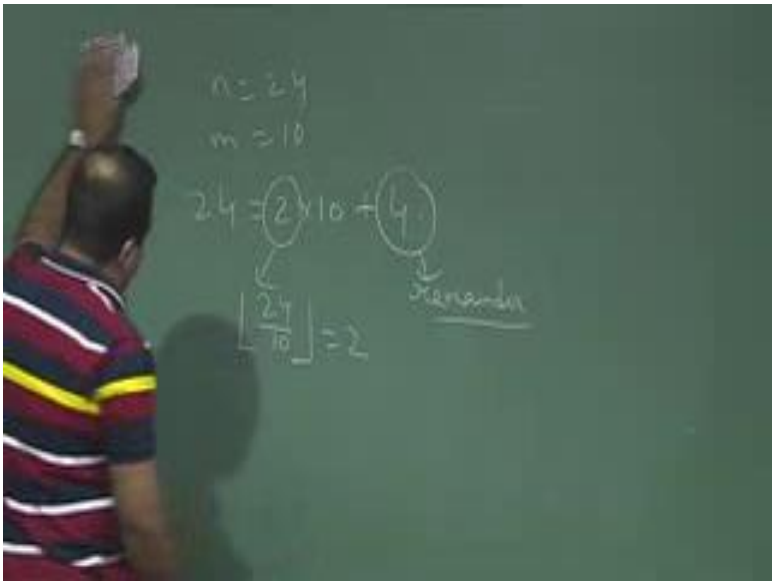

Here is the division, division if we want to divide n by m. So, n is basically q into this where all these are basically integer and r is the remainder or it is sometimes called residue and r must be nonnegative that is the either positive or 0, if it is 0 then we say m divides n and q (Refer Time: 09:37) is basically n by n by m in the floor this is basically the floor of integer a floor, this be integer part integer part of this, but it is less than x. That means, if it is say 2.6 floor means 2, 2.4 floor means also 2, but for 2.6, if you have upper ceiling then it is basically 3. So, if it is aspersion, this is the notation basically.

(Refer Slide Time: 10:18)



It is x bar is upper ceiling. So, like this. Now, suppose we want to divide 20, 24 by 10. Suppose n is equal to 24 m is equal to 10.

(Refer Slide Time: 10:33)

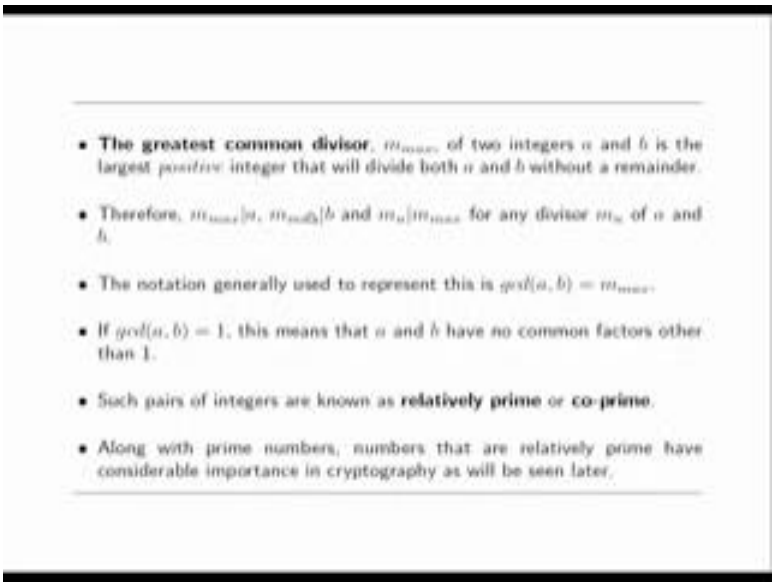



So, we want to divide 24 by 10. So, 24 basically can be written as 2 into 10 plus 4. So, this is basically r, this is the reminder which is less than 10 which is greater than, equal to 0 and this 2 is basically our q which is basically lower ceiling of 24 by 10. So, this is basically 2. So, any you have any 2 integer, we can always have this thing. So, now, suppose when you say a divides b suppose you have 2 integers a b.

(Refer Slide Time: 11:40)

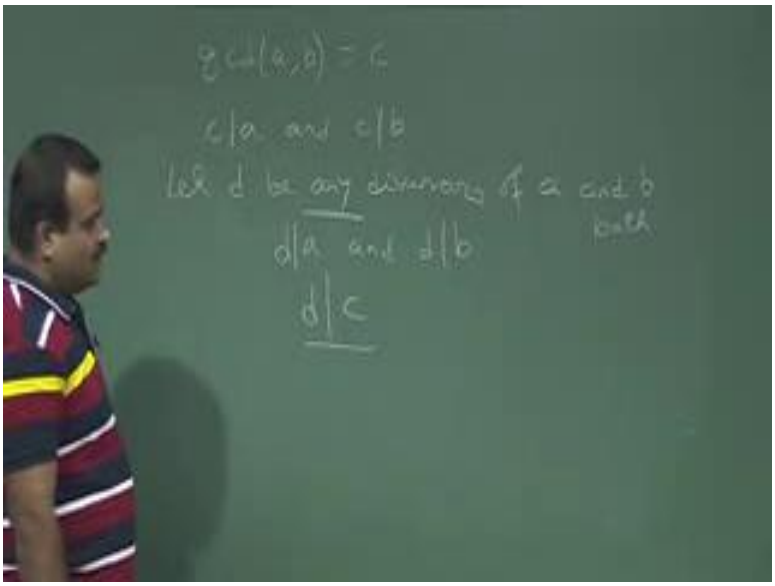
If you have 2 integer let a and b, be 2 integer and we say a divides b if an only if b is basically some q into a so; that means, the reminder is 0 then we say a divides b so; that means, a is a factor of b. So, this is the division and now we denote this by this form now we will talk about greatest common divisor.

(Refer Slide Time: 12:24)




Greatest common divisor between a and b is denoted by m max which is basically which is a divisor both a and b, it is common divisor. So, it must divides both a and b and any other divisor of a b suppose m n is the other divisor of a b then it must divides then m n must divides this greatest common divisor then will denote this by n max which is basically greatest common divisor.

(Refer Slide Time: 13:00)




Basically we denote this by gcd or the greatest common divisor gcd of a b if it is a c; that means, c divides it is a common divisor. So, c divides a and c divides b and if any other divisor d let d be any divisor this or this true, this is true for all divisor of a b divisor of a and b both, so that means, d divides a and d divides b then d must divides c and this must true for any other divisor d. So, this basically then c is a greatest common divisor of a b. Now suppose we want to find the greatest common divisor of say 24 32.

(Refer Slide Time: 14:31)

Suppose a is 24, so suppose we want to find 24 and 32, these how much we want to find this. So, a is 24 b is equal to 32, now what is the divisor of a? So, the divisor set, set a all divisor set of 24 is basically plus minus 1 plus minus 2, these are all divisor of 24 plus minus 3 plus minus 4 and then plus minus 4 then plus minus 6 then plus minus 8 plus minus 12 plus minus 24. So, these are all divisor of 24, now this the divisor set of 24, now let us check the divisor set of 32. So, this is basically plus minus 1 plus minus 2 plus minus 4 6 is not a divisor of 32, so, plus minus 8 then plus minus 16 and then plus minus 32.

These are the divisor of 32, now the common divisor means the intersection between these 2 set. So, the common divisor of divisor of 24 and 32 is basically the common integers the intersection between these 2 sets. So, this is basically plus minus 1, this is common plus minus 2 is common then plus minus 4 is common and plus minus 8 is common. So, plus minus 2 plus minus 4 plus minus 8, so, these are the common divisor of this a b, now among this which is the greatest common divisor. So, 8 is the gcd of this so, 8 is the gcd of 24 32. So, we can check that if you take any other divisor of any other common divisor of 24 and 32 like for example, 4 then 4 divides 8. So, that is the gcd of the 2 number a b, it is a common divisor and it is the greatest common divisor so; that means, if you take any other divisor, common divisor of a b then that must divides this greatest common divisor, so 2 also divides 8.

Now, we will talk about some result based on the greatest common divisor and then we will talk about how to find the greatest common divisor of 2 integers a b that is called Euclid algorithm or Euclidean algorithm.

(Refer Slide Time: 18:05)

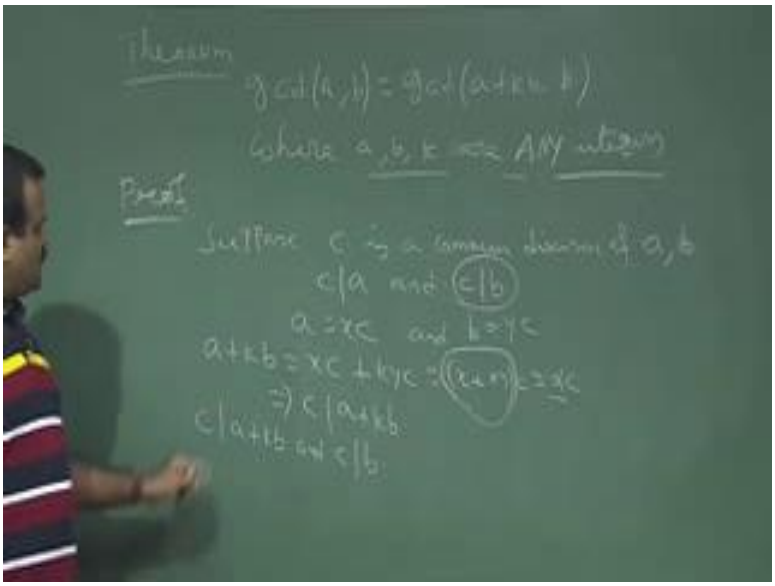

Some result will discuss here. So, this is result we can have a theorem form. So, gcd of a b is basically same as gcd of b a this is quite of here I mean we are just changing the base thing. So, this is quite obvious no need to go for the proof now another theorem may be. So, we can mark the number gcd of a b same as gcd of a because a b could be negative also, but for divisor we are taking the greatest common devices. So, this mod is. So, if c is a divisor then minus is also divisor if c divides a then minus c also divides minus a. So, this is also quit straight forward you are not going to prove this now theorem number 3 is basically gcd of a 0 is basically a.

And now we are going to proof the theorem which will give us the Euclid algorithm to find the greatest common divisor of 2 numbers a b.

(Refer Slide Time: 19:53)


This theorem is telling the statement of this theorem is may be this is 4. So, 1 2 3 4 anyway, this is theorem is telling gcd of a b is basically gcd of a plus k b coma b where a b k are any integer this is gcd of base, now how to prove this? Now this is the proof of this theorem, now gcd of a b is same as these, now to proof this if you can show that set of common divisor of a b is same as set of common divisor of these 2 then you are done. So, basically if we can so that set of common divisor of a b is equal to set of same they are same set basically set of common divisor of common divisor of a plus k b comma b if we can prove that then we have done because then we can take the maximum of that set I mean the gcd. So, we are going to prove this, the set of common divisor of a b is same as set of common divisor of a plus a b comma b so; that means, to prove this, what we need to show? We take a common divisor of a b so that will show is a common divisor of a plus k b. So, let us take that.

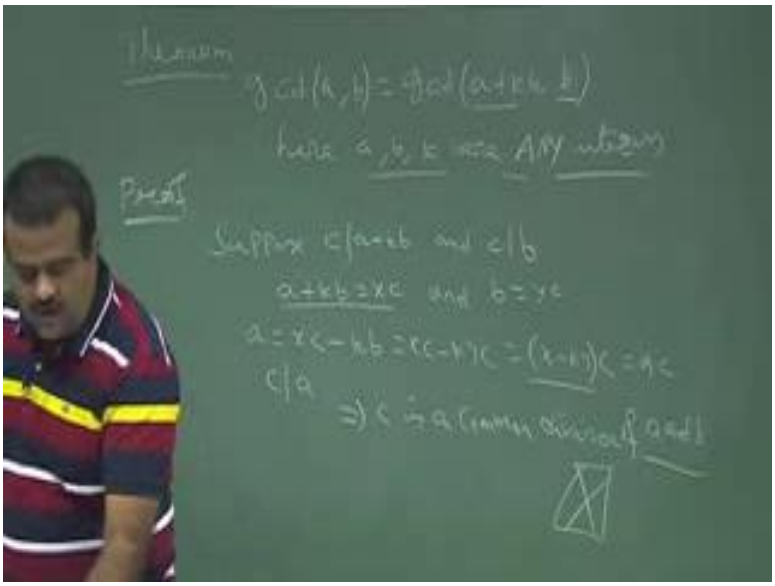
(Refer Slide Time: 22:14)




Suppose c is a common divisor of a coma a and b, that means, c divides a and c divides b. So, c divides a means a should be written as x c and c divides b means b should be written as some y c x y are 2 integer, now we will proof that c will divides both c already divides b now we have to show that c divides a plus k b. So, how to show this? So, a plus k b is basically what a plus k b is basically a e is basically x c plus k b b is y c. So, k y c, so, this is basically a plus k y c. So, this is an integer a plus k y is an integer. So, this is sum alpha c where alpha is an integer. So, this implies c divides a plus k b now we already know c divides b, so that means, this implies c divides a plus k b and c divides b so; that means, c is a common divisor of this and this.

So, one part is done now the reverse. Now you assume suppose c is a common divisor of this and this and then we need to show c is also a common divisor of a b so; that means, c divides a. So, this is one part is completed.

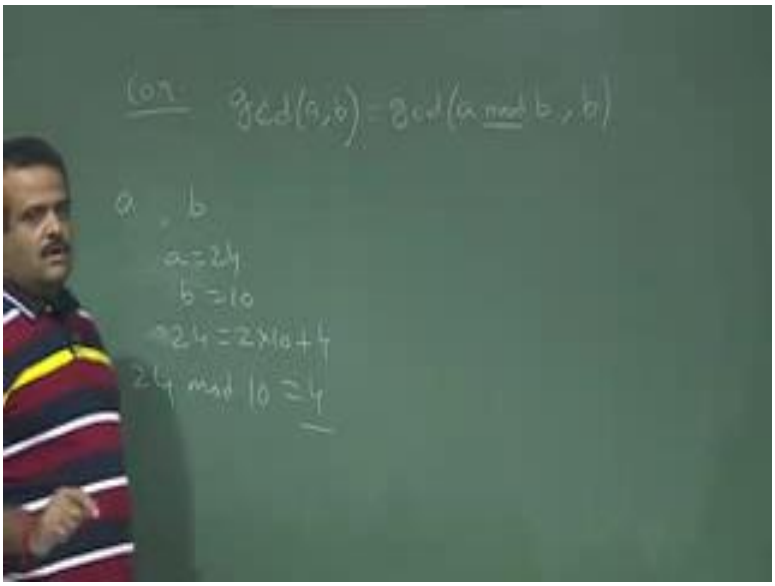
(Refer Slide Time: 24:15)




Now, the second part, suppose c divides, see suppose c is a common divisor of this and this, so that means, suppose c divides a plus k b and c divides b then we need to show c is also common divisor of a b so; that means, we need to show that c divides a also. So, this means what this means a plus k b is must written as some x into c some other integer x and c divides b means b must be written as some integer y into c now from here a is basically x c minus k b now k is basically y c, so, x c minus k y c, so, if u take c common x minus x y c. So, this is some integer alpha c some integer alpha. So, this means c divides a done so; that means, c is a common divisor of this implied c is a common divisor of a and b so; that means, set common divisor of a b is same as set of common divisor of a plus k b coma b, so that set is same so; that means, the greatest common divisor must be same. So, this is the proof of this theorem.

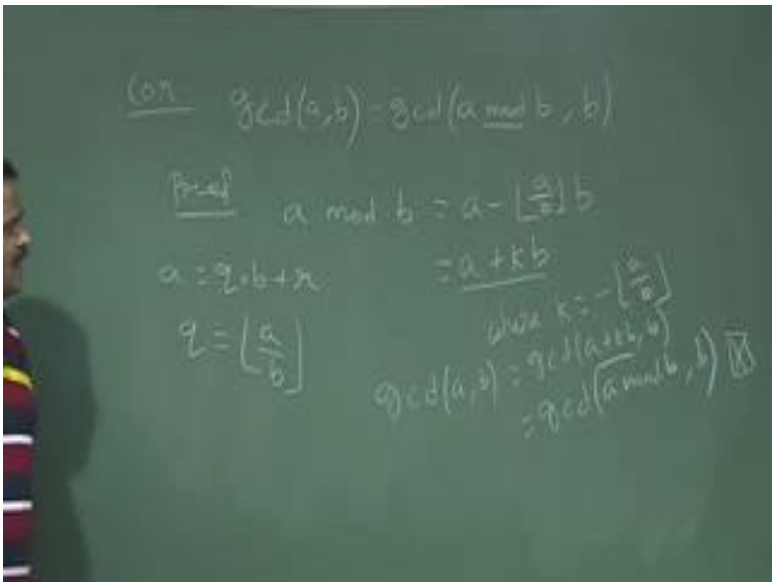
From this theorem, we can have algorithm which is called extended which is the sorry Euclid algorithm which is method to find the greatest common divisor of a b. So, this is coming from this, what is called, this colorable of this theorem.

(Refer Slide Time: 26:35)




So, gcd of a b is basically gcd of a mod b comma b, see this mod operation is basically what? So, a is an integer b is an integer. So, if you divides a by b then a mod b basically the remainder. So, like 24 can be written as if we if a is 24 and b is 10 say than 24 can be written as 2 into 10 plus 4, so that means, 24 mod 10 is basically this remainder 4; that means, if you divides 24 by 10 then whatever is the remainder is 4 is the basically a mod b. So, that is that sense a mod b a mod b is basically a is an integer b is an integer. So, if you divides a by b the remainder will be the denoted by a mod b we do have a modular operation modular arithmetic we will discuss in the let next lecture maybe, so now the mod.

(Refer Slide Time: 28:08)




So now, how to proof this? We will just use the previous theorem we have discussed, so, basically a mod b is basically r. So, a is basically written as q into b plus r where q is basically a by b. So, this is basically r, this is basically a minus a by b into b. So, this is of the form a plus k b where k is equal to k is equal to basically minus a by b it is integer. So now, this gcd also this is we have seen. So, gcd of we know this result from the previous theorem gcd of a b is basically gcd of a plus k b comma b. So, a plus k b is basically a mod b. So, gcd of a mod b coma b, so this is the proof of this result and this results gives us the what is called Euclid algorithm to find the gcd of 2 numbers which we discuss in the next class.

Thank you.