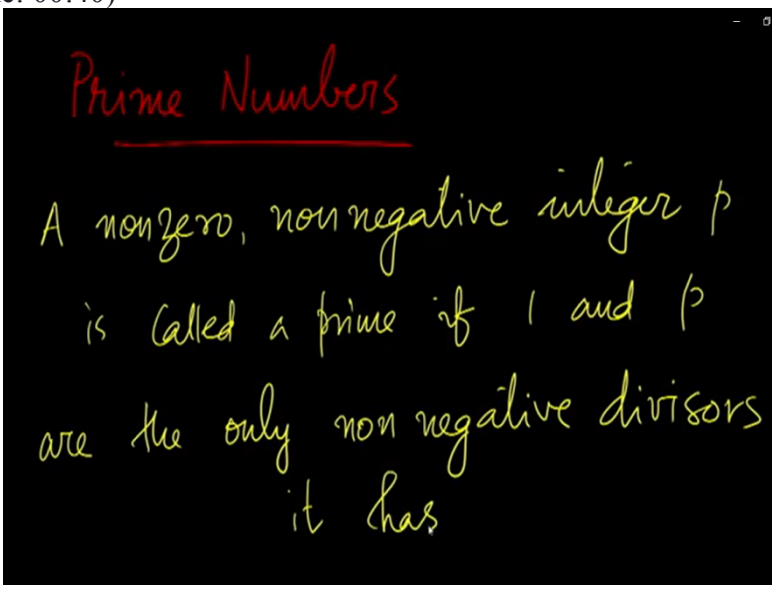
Discrete Mathematics
Professor Sajith Gopalan
Professor Benny George
Department of Computer Science & Engineering
Indian Institute of Technology Guwahati
Lecture 25 - Prime numbers

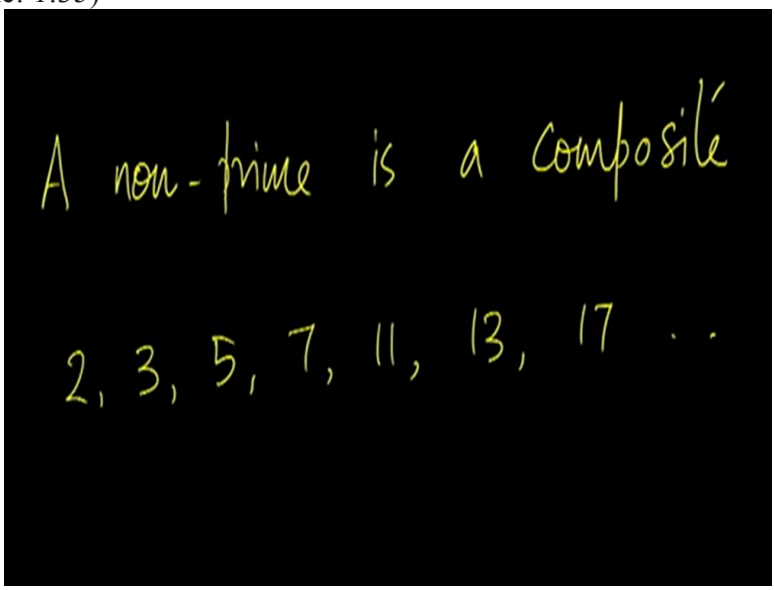
Welcome to the NPTEL MOOC on Discrete Mathematics. This is the third lecture on number theory. Today, we study prime numbers.

(Refer Slide Time: 00:40)



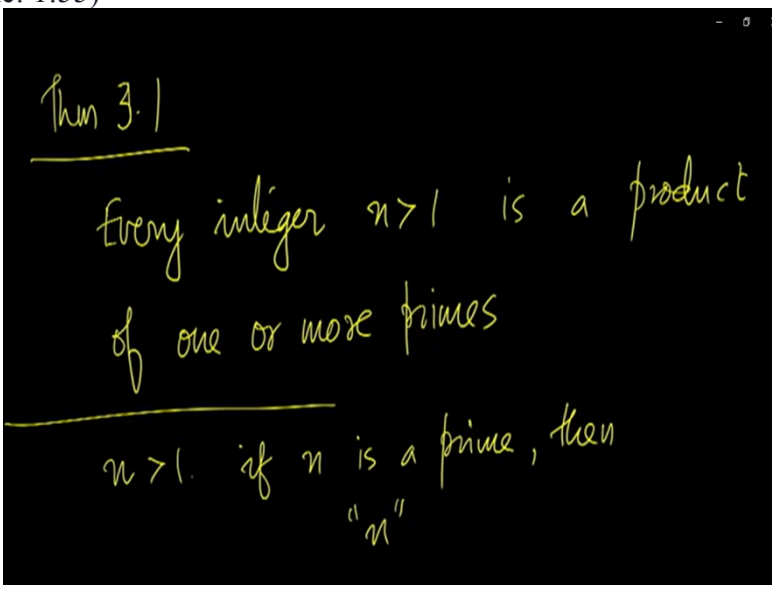
A non-zero integer, a non-zero, non-negative integer P is called a prime if 1 and P are only the non-negative divisors it has.

(Refer Slide Time: 1:35)



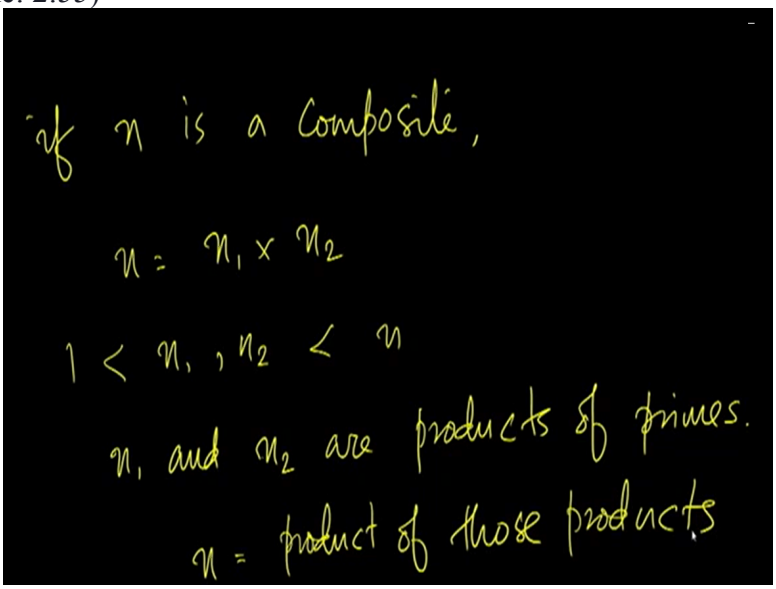
A non-prime is called a composite number. So the prime numbers are 2, 3, 5, 7, 11, 13, 17, and so on.

(Refer Slide Time: 1:55)



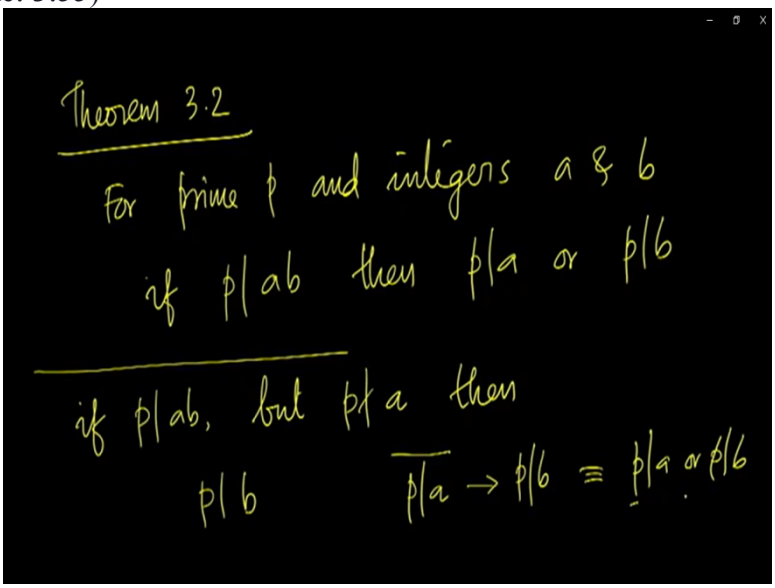
So, let us see theorem that we call theorem 3 1. The theorem says that every integer n greater than 1 is a product of one or more primes. The proof is easy. Consider the number n greater than 1. If n is a prime then n alone forms the product that we look for. The theorem states that n can be written as a product of one or more primes. So in those case, n is a prime, so n is a product on its own.

(Refer Slide Time: 2:55)



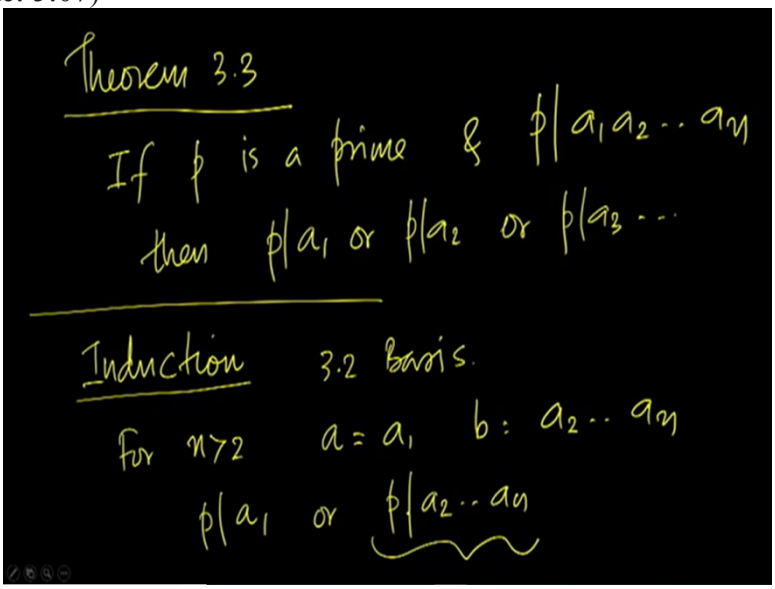
So, if n is a composite then by definition n is n 1 into n 2 where n 1 and n 2 are both less than n and greater than 1. Now, let us inductively assume that n 1 and n 2 are products of primes, then n is a product of those products, therefore, n is also representable as a product of primes. So, either way, every positive integer can be expressed as a product of multiple primes.

(Refer Slide Time: 3:55)



Another theorem which we call theorem 3 2. For prime p and integers a and b, if p divides the product ab then either p divides a or p divides b. The proof is easy again. If p divides ab but p does not divide a then by a theorem we found in the last class p divides b. Therefore, we have that p divides a negated implies p divides b which is equivalent to saying that either p divides a or p divides b. Hence the theorem.

(Refer Slide Time: 5:07)

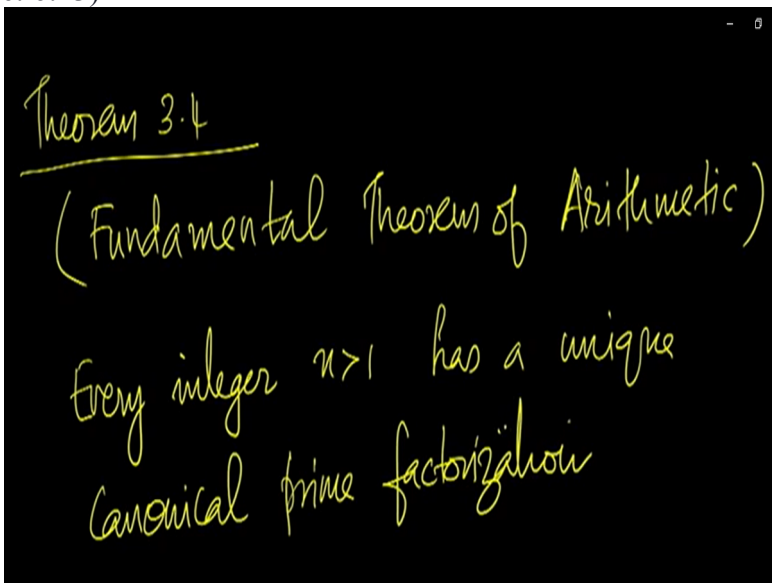


Extending this we can say if p is a prime and p divides the product a 1, a 2 to a n where a 1, a 2 to a n are all integers then p divides a 1 or p divides a 2 or p divides a 3 and so on. We should divide one of those integers.

We can prove this using induction from the previous theorem. The previous theorem will form the basis, that is theorem 3 2 will form the basis. For n greater than 2, let a equal to a 1 and b equal to a 2 to a n in the theorem. Then we have that either p divides a 1 or p divides b which is a 2 to a n.

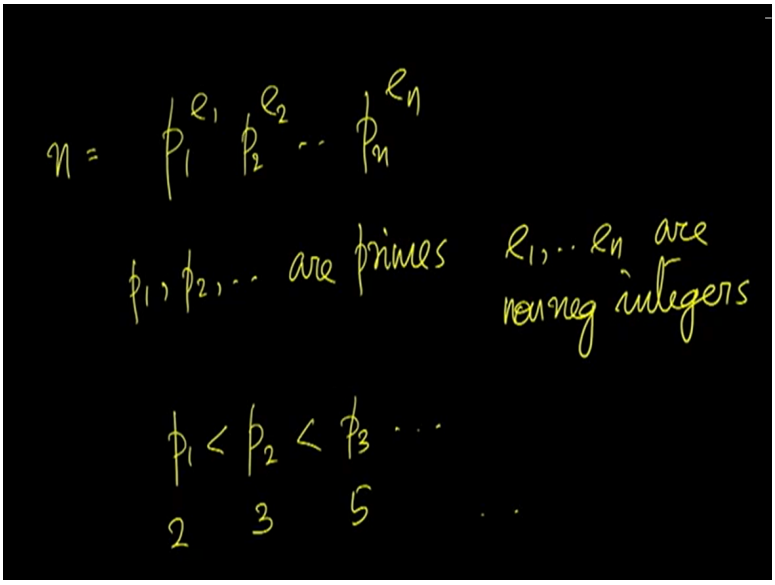
Now, by induction hypothesis, if p divides a 2 to a n, since it is a product of smaller number of integers we can say in this case p divides a 2, p divides a 3 and so on. Therefore, putting together, we have either p divides a 1 or p divides a 2 and so on and the theorem follows.

(Refer Slide Time: 6:23)



The next theorem is a famous one. This is called the fundamental theorem of the arithmetic. What it says is that every integer n greater than 1 has a unique prime factorization, unique canonical prime factorization. But what is a canonical prime factorization?

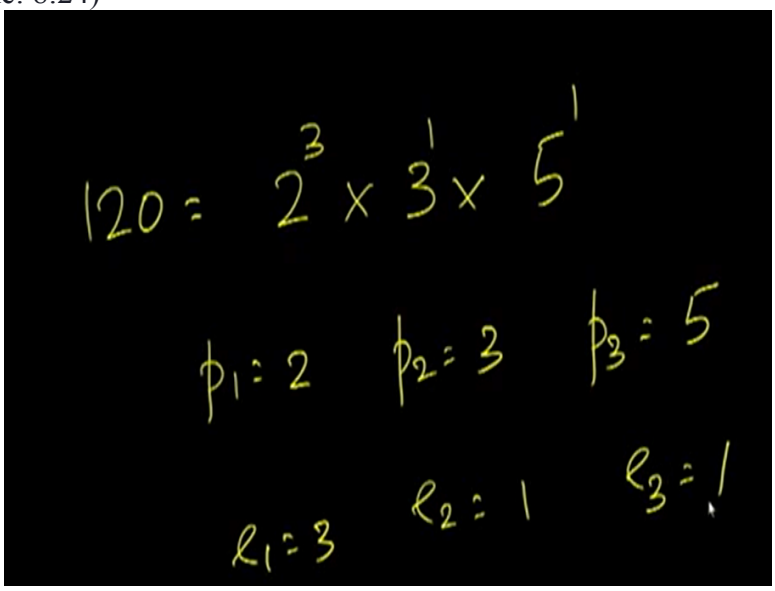
(Refer Slide Time: 7:19)



If n is expressed as a product of this form, p 1 power e 1 into p 2 power e 2 et cetera up to some prime p n power e n where p 1, p 2, et cetera are all primes, e 1, e 2, et cetera are non-negative integers and p 1 is the smallest prime, p 2 is the next prime, p 3 is the next prime and so on. So p 1 is 2, p 2 is 3, p 3 is 5 and so on.

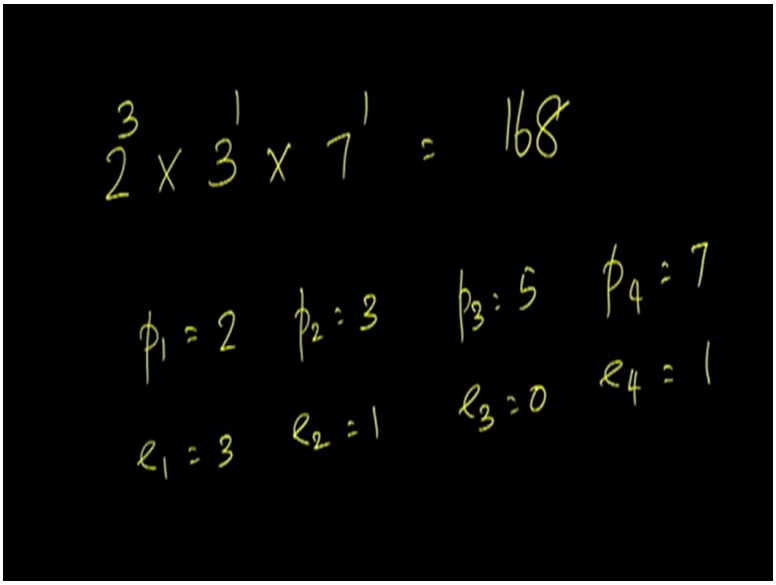
So, when n is expressed as such a product we say that this is a canonical prime factorization of n. The primes in this product appear in increasing order.

(Refer Slide Time: 8:24)



For example, 120 is 2 power 3 into 3 into 5. So the primes here are p 1 equal to 2, p 2 equal to 3 and p 3 equal to 5, e 1 is 3 we have 2 power 3, e 2 equal to 1 and e 3 equal to 1.

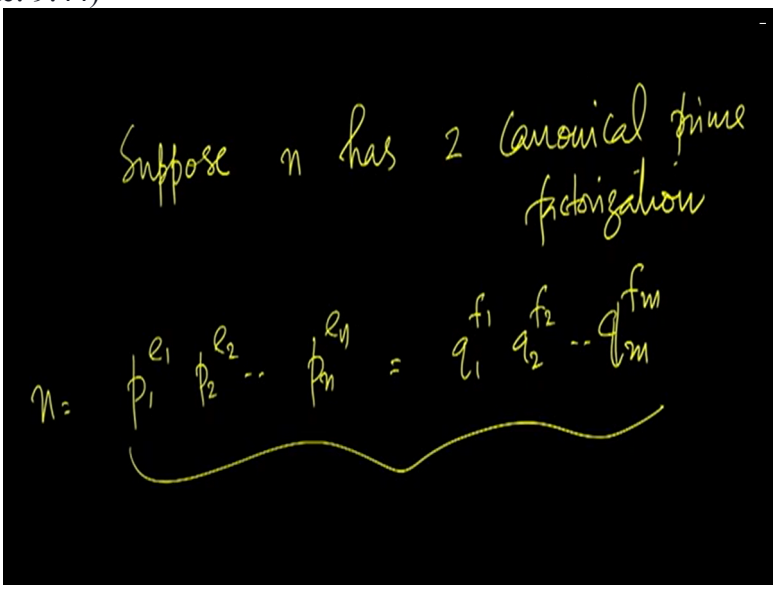
(Refer Slide Time: 8:46)



Consider 2 power 3 into 3 power 1 into 7 power 1 is equal to 168. So in this prime factorization or in this canonical prime factorization we have p 1 equal to 2, p 2 equal to 3, p 3 equal to 5 and p 4 equal to 7, e 1 is 3, e 2 is 1, e 3 in this case is 0 because 5 has an exponent of 0 in this case and e 4 equal to 1.

We do not consider primes which are greater than 7 because the exponents of all of them are 0. So such a representation of numbers is called a canonical prime factorization. So what the fundamental theorem of arithmetic says is that every non-negative integer has a unique canonical prime factorization. So, we will prove this in this manner:

(Refer Slide Time: 9:44)

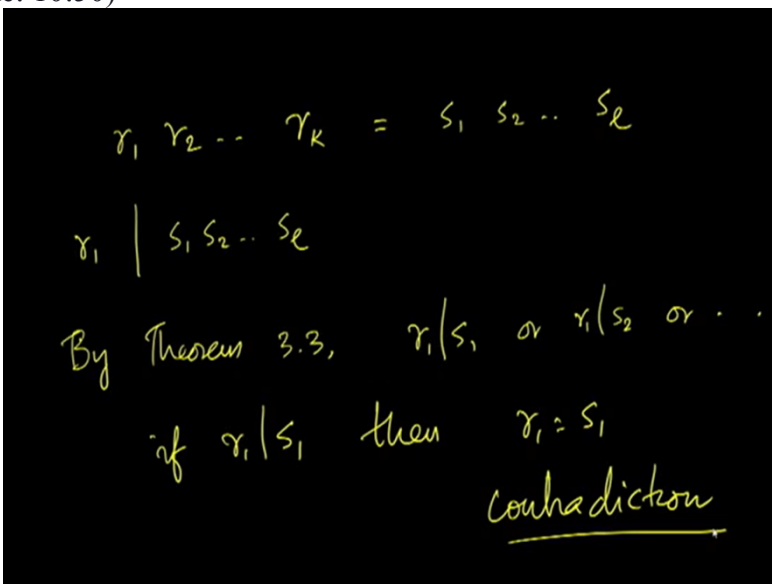


Suppose, a positive integer n has 2 canonical prime factorizations, then n is p 1 power e 1, p 2 power e 2, et cetera up to p n power e n which is also q 1 power f 1, q 2 power f 2 and so on

up to q m power f m. So, n has two distinct canonical prime factorizations. But, then let us consider this equation.

In this equation on either side of the equality we have a product, so let us cancel the common factors from both sides. Since these two prime factorizations are distinct everything will not cancel out.

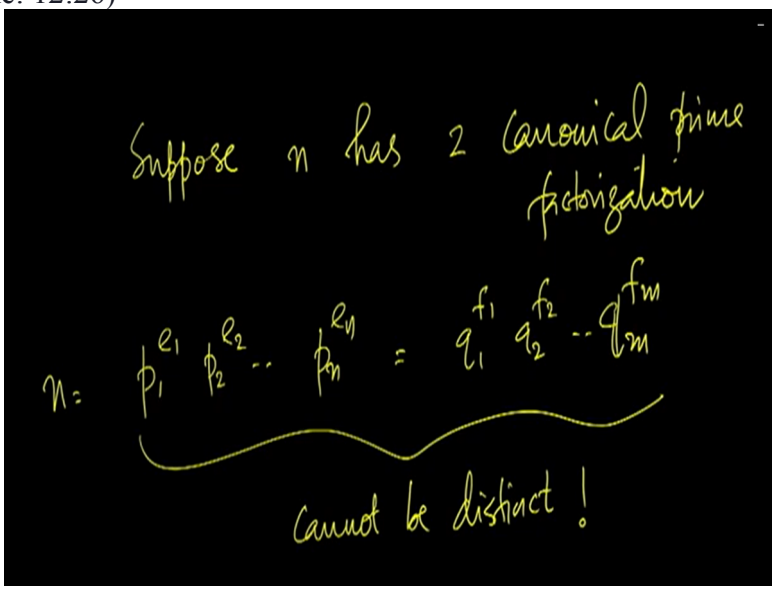
(Refer Slide Time: 10:50)



So finally we will be left with some k primes on the left side and some l primes on the right side. So there will be now no common prime on the left side and the right side. Every prime on the left side will be distinct from the primes on the right side. Now, in particular, consider are 1 and the right-hand side s 1 to s l. We know that r 1 divides s 1 through s l that is because r 1 multiplied by r 2 through r k is s 1 through s l. So, there is an integer so that r 1 into that integer is right hand side. So r 1 divides the right-hand side. But then by theorem 3 3, r 1 divides s 1 or r 1 divides s 2 and so on. It should divide one of the primes, at least one of the primes on the right hand side.

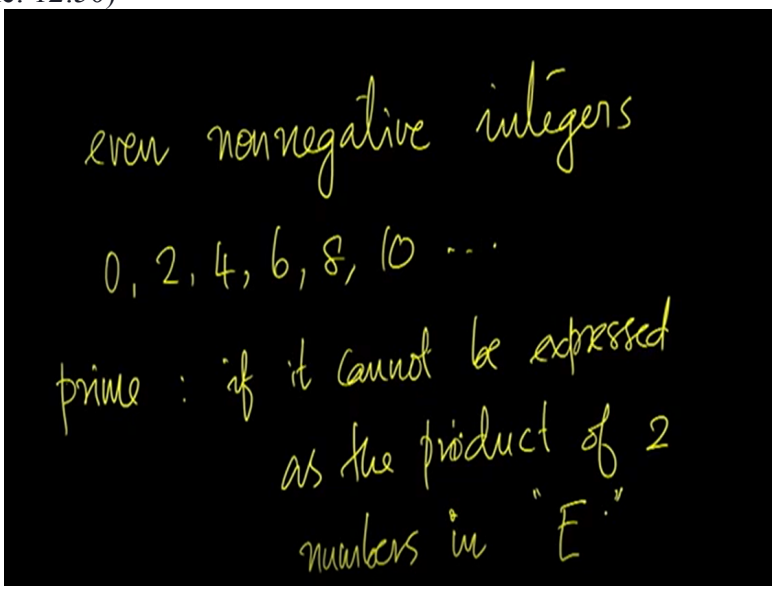
Now, r 1 is a prime and if r 1 divides s 1 which is also a prime, s 1 is also a prime then r 1 is equal to s 1. So, r 1 must equal one of the primes on the right hand side which is a contradiction that is because we have already canceled all primes that appear on both sides. So, here we get a contradiction.

(Refer Slide Time: 12:26)



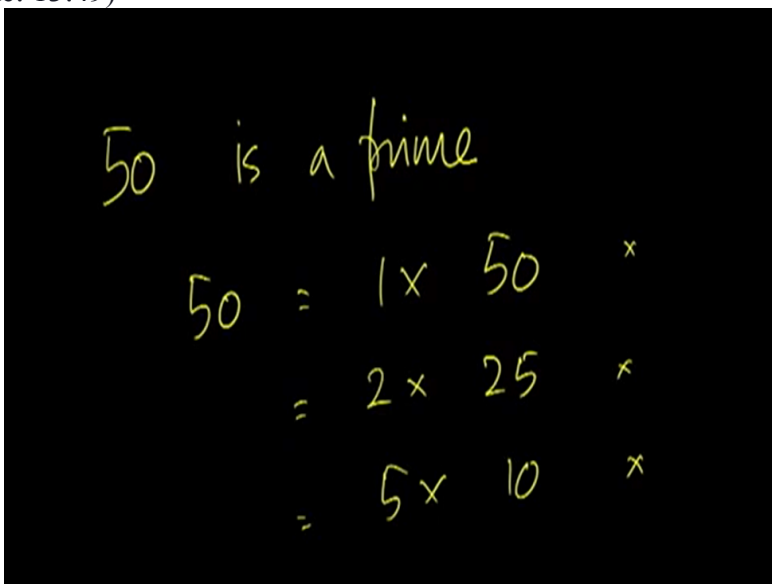
Therefore, the two prime factorizations that we began with cannot be distinct. In other words, every number n has a unique canonical prime factorization. Now, this is the case with integers but in every system this need not be the case.

(Refer Slide Time: 12:50)



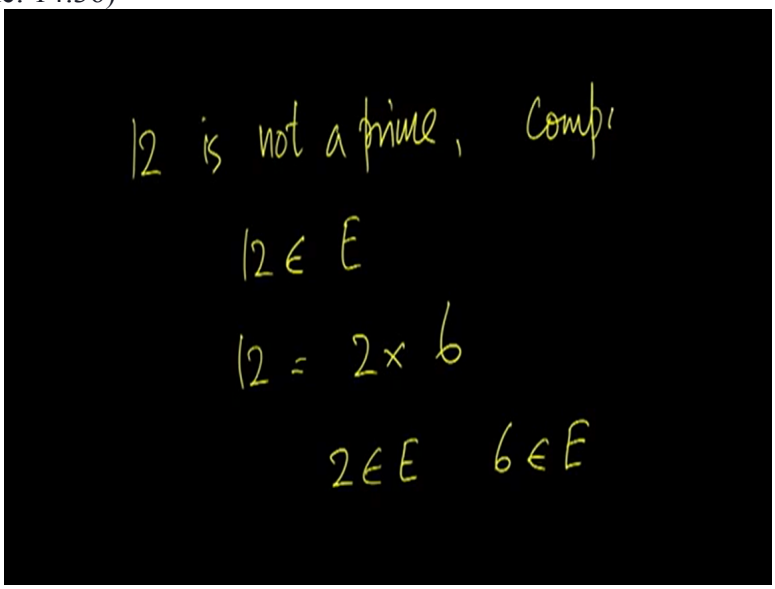
In particular, let us consider the system of even non-negative integers. So we consider these numbers. In this, we say that a number is prime if it cannot be expressed as the product of two numbers in the system. So let us call this system E. So, this is a system of even non-negative integers. So, a number in the system will be considered a prime if it cannot be expressed as the product of two numbers in E.

(Refer Slide Time: 13:49)



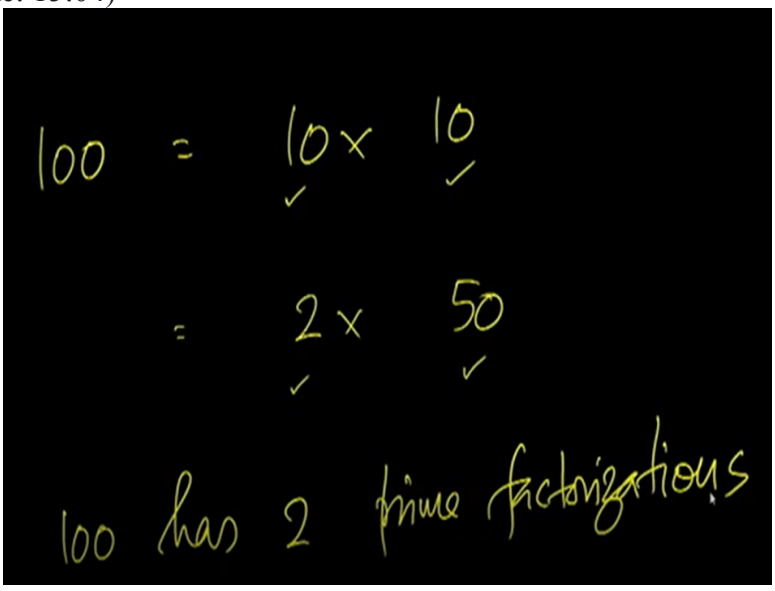
For example 50. We will say that 50 is a prime number in the system because 50 is if you factorize 50, you have the various factorizations, 1 into 50, but 1 is an odd number, so this is not a product of two even numbers. Then we have 2 into 25, 25 is an odd number, so this also does not qualify and we have 5 into 10, 5 is an odd number so this does not qualify. The rest are all the same factorizations, we have 10 into 5, 25 into 2, and 50 into 1. So, 50 cannot be expressed as the product of two smaller even numbers. Therefore, 50 is a prime.

(Refer Slide Time: 14:36)



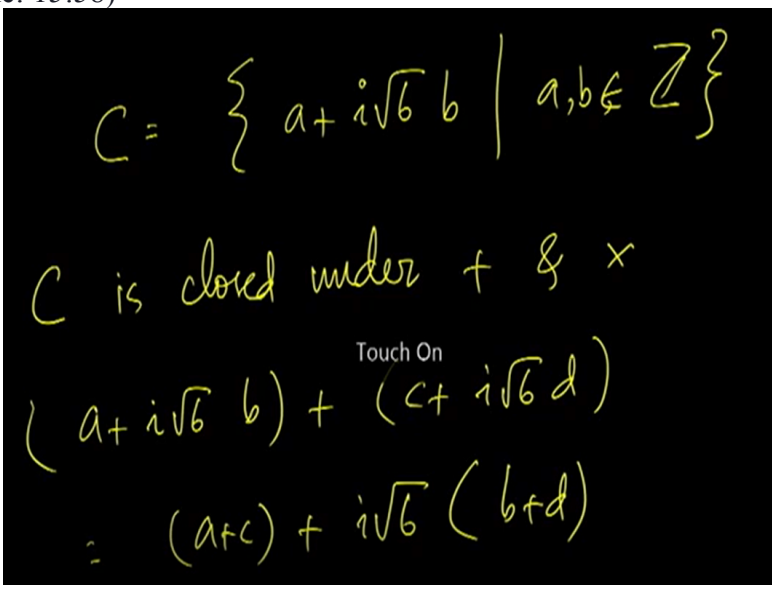
But 12 is not a prime. That is because 12 belongs to E and 12 can be expressed as 2 into 6, where 2 is an even number and 6 is also an even number, therefore 12 is not a prime, 12 is a composite within this system.

(Refer Slide Time: 15:04)



But then consider number 100. 100 can be expressed as 10 into 10. 10 belongs to E, so we are now expressing 100 as a product of two numbers both of which are even and smaller than 100, but 100 is also 2 into 50, 2 is an even number and 50 is also an even number, so 2 belongs to E and 50 belongs to E, so 100 has two prime factorizations, two canonical prime factorizations within the system, canonical because here the prime numbers are appearing in increasing order. Therefore, within this system every number need not have a unique prime factorization.

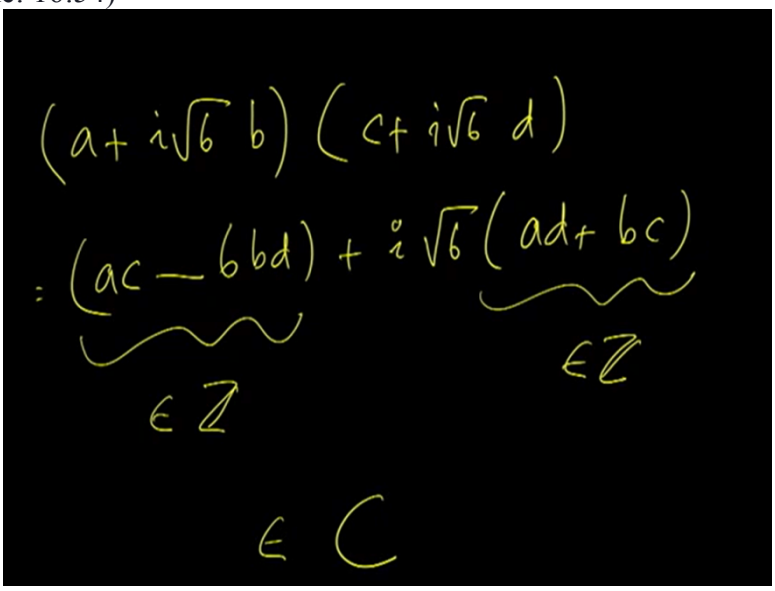
(Refer Slide Time: 15:58)



As another example consider the set of some complex numbers. We consider all complex numbers of the form a plus i root 6 b where a and b are integers. Now, C is closed under

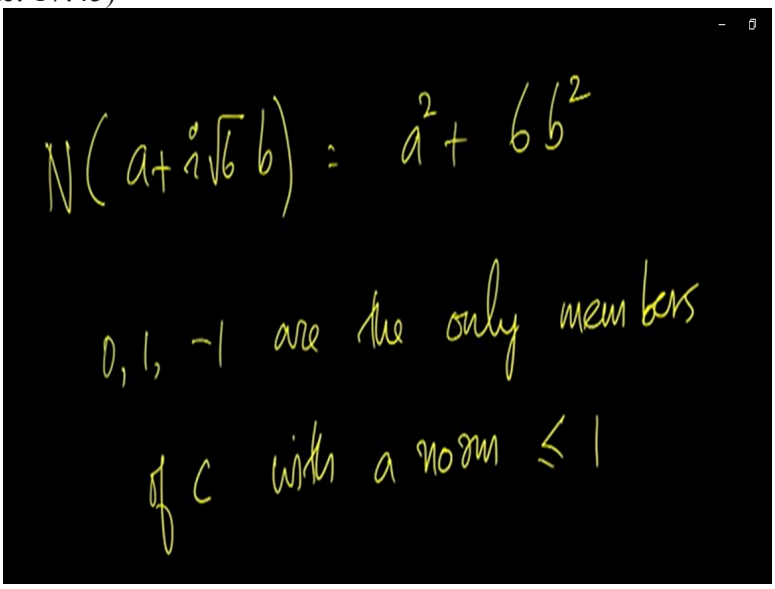
addition and multiplication. That is because a plus i root 6 b plus c plus i root 6 d is a plus c plus i root 6 into b plus d. Therefore, C is closed under addition and…

(Refer Slide Time: 16:54)



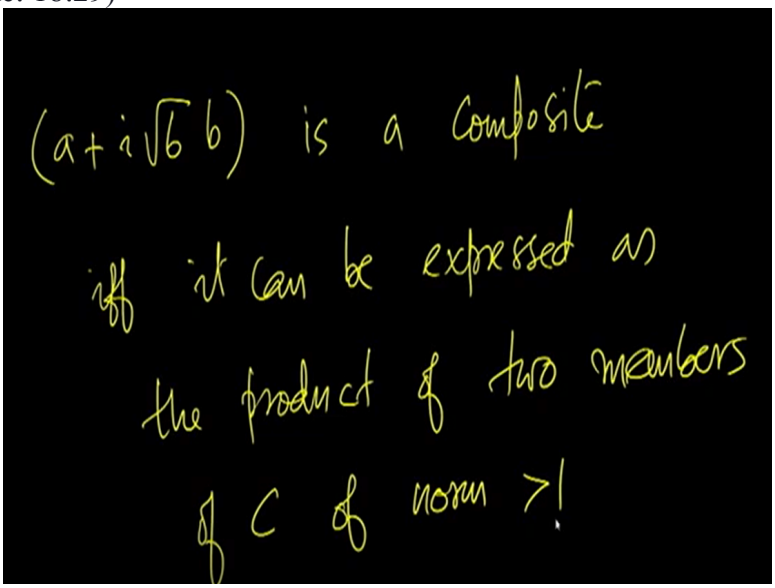
In the case of multiplication we have a plus i root 6 b into c plus i root 6 d which is ac minus 6 bd, the real part, i root 6 into ad plus bc. Since a and b are integers ac minus 6 bd is also an integer, ad plus bc is also an integer. So, here we express the product in the a plus i root 6 form again. Therefore this is also a member of C. So C is closed under multiplication as well.

(Refer Slide Time: 17:45)



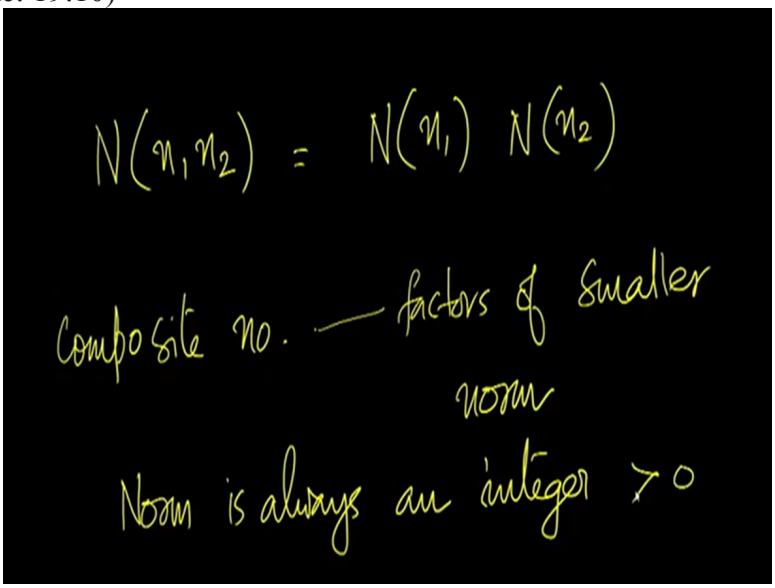
Let us define the norm of one such number as a square plus 6 b square, the square of its absolute value. 0, 1 and minus 1 are the only members of C with a norm of value less than or equal to 1.

(Refer Slide Time: 18:29)



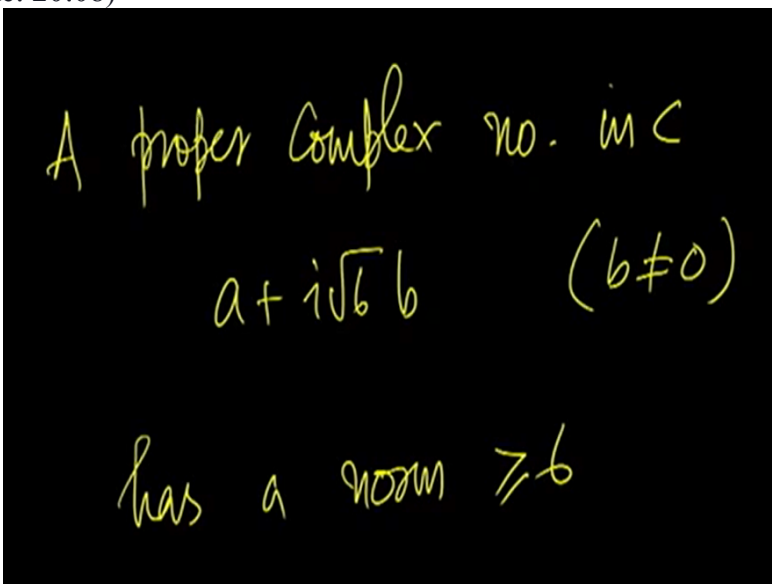
We say that in this system a number a plus i root 6 b is a composite, in other words, it is not a prime if it can be expressed as the product of two members of C of norm greater than 1.

(Refer Slide Time: 19:10)



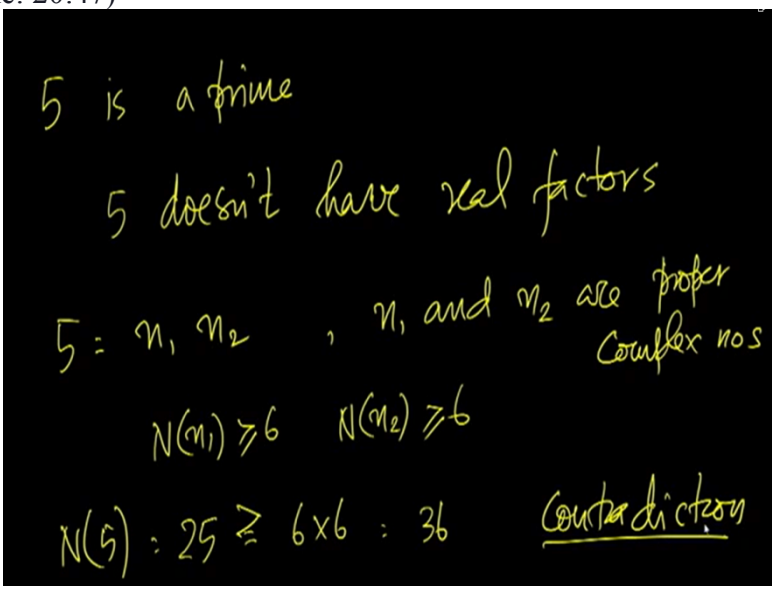
So you can verify that the norm of a product of two members of C is equal to the product of the norms. In other words, for two members n 1 and n 2 of C, the norm of n 1 into n 2 is the norm of n 1 into the norm of n 2. So if you consider a composite number it factorizes into factors of smaller norm and the norm is always an integer greater than 0.

(Refer Slide Time: 20:08)



And a proper complex number in C which means in this b is not equal to 0, has a norm greater than or equal to 6. So even if b equal to 1 the i root 6 b part will contribute 6 to the norm. So norm will be greater than or equal to 6.

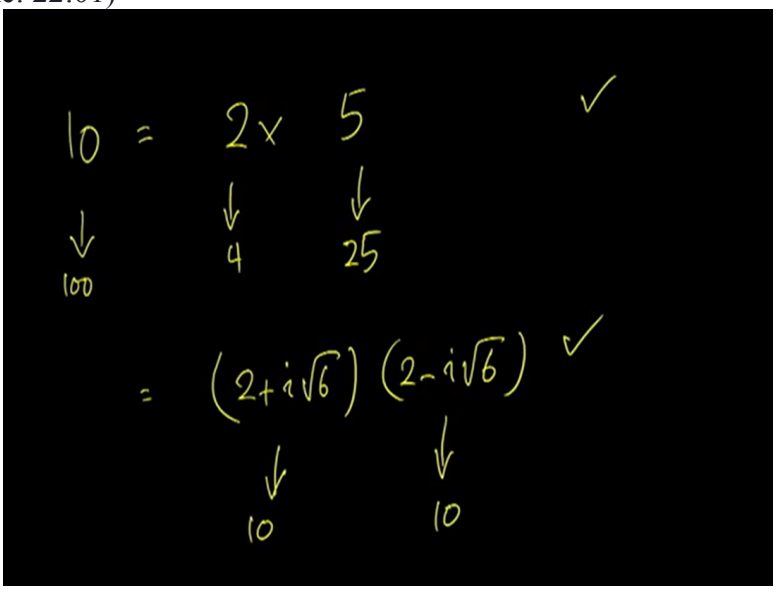
(Refer Slide Time: 20:47)



So, in this system 5 is a prime because 5 does not have real factors. So if 5 has factors n 1 and n 2 then n 1 and n 2 are complex, are proper complex numbers which means the norm of n 1 is greater than or equal to 6 and the norm of n 2 is also greater than or equal to 6 but the norm of 5 alone is 25. Therefore, we have that 25 greater than or equal to 6 into 6 which is 36 which is a contradiction.

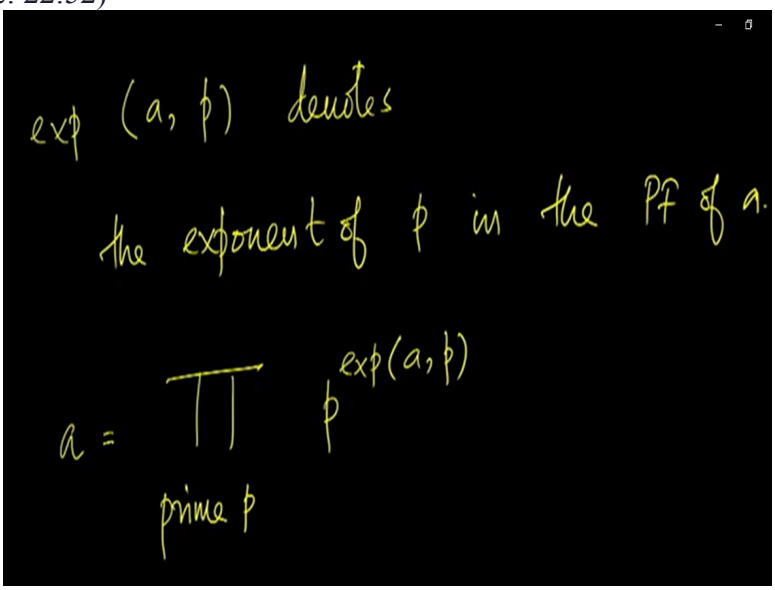
Therefore, 5 cannot be expressed as n 1 and n 2 where n 1 and n 2 are both complex numbers belonging to C. Therefore, 5 is a prime. That means there are prime numbers in the system.

(Refer Slide Time: 22:01)



Now, consider 10. 10 can be expressed as 2 into 5. Now, 2 belongs to the system and 5 also belongs to the system. So 10 has a norm of 100, 2 has a norm of 4 and 5 has a norm of 25 but 10 can also be expressed as the product of 2 plus i root 6 into 2 minus i root 6. 2 plus i root 6 has a norm of 10 and 2 minus i root 6 also has a norm of 10. So now we find that 10 has two prime factorizations. So within the system again, there are numbers with multiple canonical prime factorizations. But then what we find that within the system of integers the rest are unique prime factorizations that is what the fundamental theorem of arithmetic says.

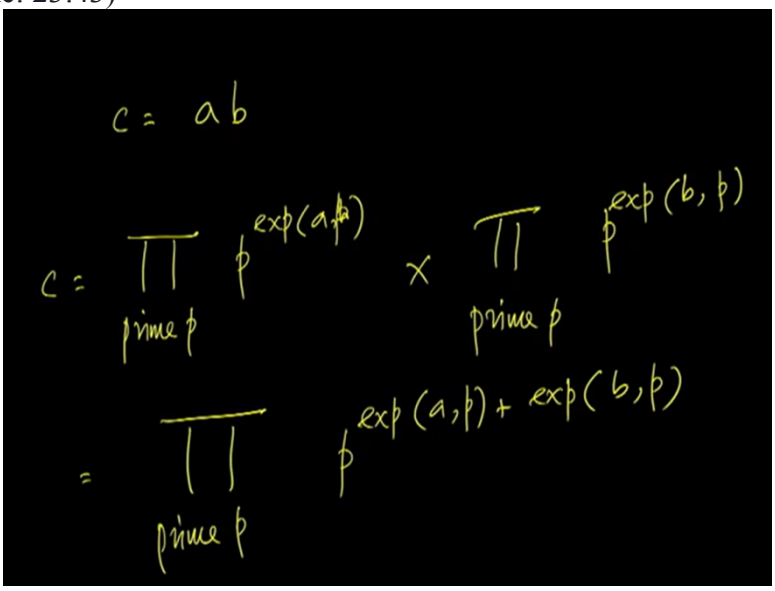
(Refer Slide time: 22:52)



Now, let exp of a, p denote the exponent of prime p in the prime factorization of a. Since the prime factorization is unique this is well defined, exponent of a, p is well defined. Therefore,

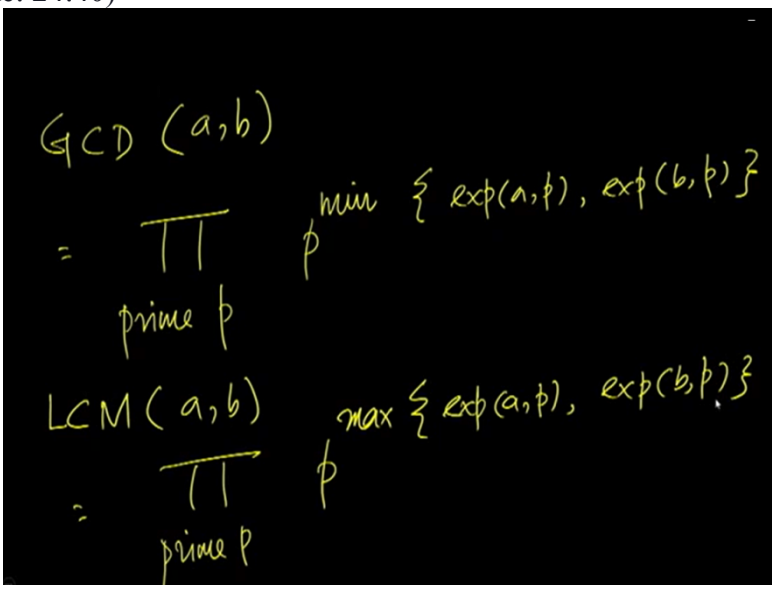
number a can be expressed as the product over all primes p of p power exp of a, p. Every integer a can be expressed as a product in this function.

(Refer Slide Time: 23:43)



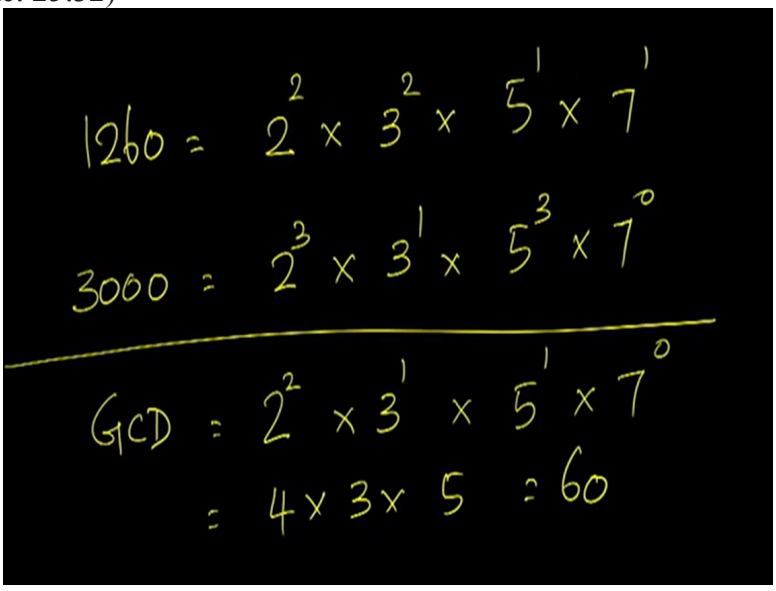
Now, let us say integer c is integer a multiplied by integer b. Then c is the prime factorization of a which is this product multiplied by the prime factorization of b which can therefore be written as…So in the prime factorization of c, the exponent of p is going to be the sum of the exponents of p in the prime factorizations of a and b respectively.

(Refer Slide Time: 24:40)



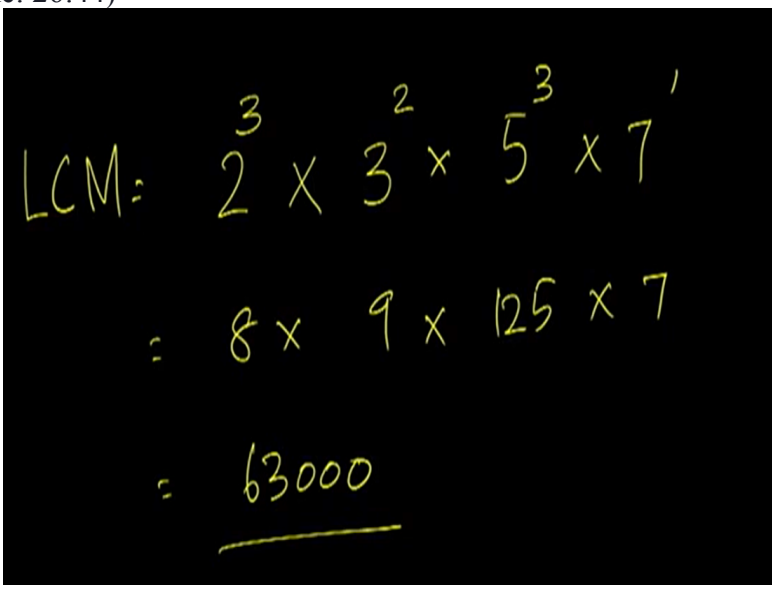
So, it is easy to say that GCD of a and b is the product over all prime p of this. Similarly, LCM of a and b is the product over all prime p of p power max of exp a, p and exp b, p.

(Refer Slide Time: 25:32)



As an example, consider 1260 which can be prime factorized into 2 power 2 multiplied by 3 power 2 multiplied by 5, multiplied by 7 and consider the number 3000 which is, for uniformity let us include 7 here. Then to find the GCD we have to take the respective minima of the exponents. So in 2160, the exponent of 2 is 2 and in 3000 exponent of 2 is 3. The minimum exponent here is 2. Therefore, in the case of GCD we have to take 2 as the exponent of 2, for 3 the exponent is the smaller of 1 and 2, for 5 it is 1 and for 7 it is 0 which is 4 into 3 into 5 that is 60. So the GCD of 1260 and 3000 is 60.

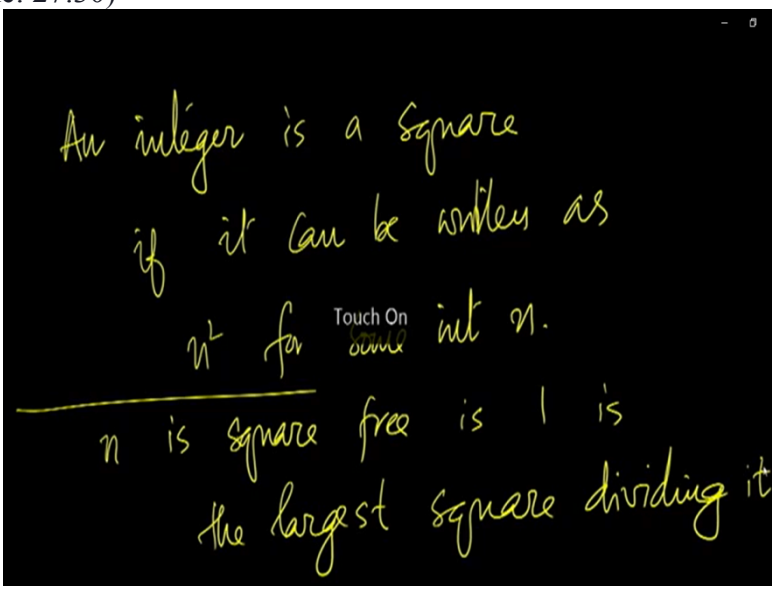
(Refer Slide Time: 26:44)



And then LCM can be obtained by taking the larger of the exponents. So the largest exponent of 2 among these two numbers is 3, the larger exponent of 3 among these two numbers is 2,

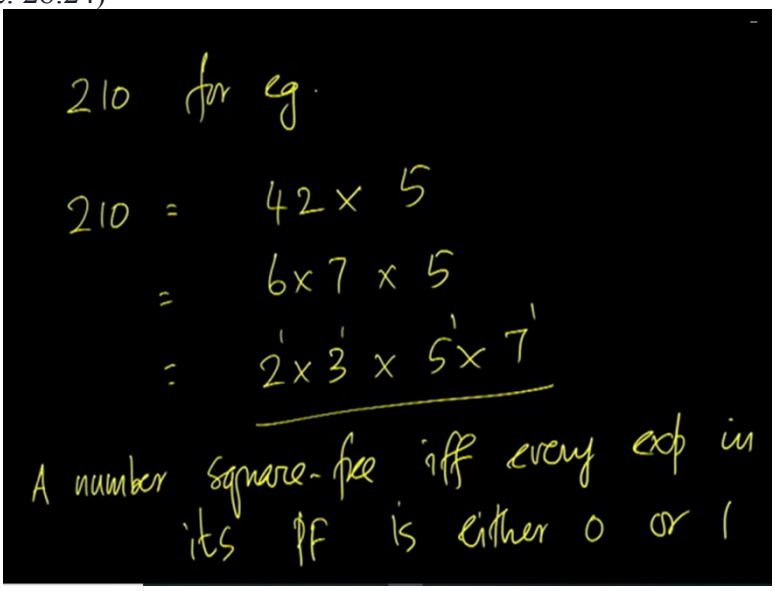
for 5 it is 3 and for 7 it is 1. So, it is 8 into 9 into 125 into 7 that is 1000 into 63, 63000. So, this is the LCM of 1260 and 3000.

(Refer Slide Time: 27:30)



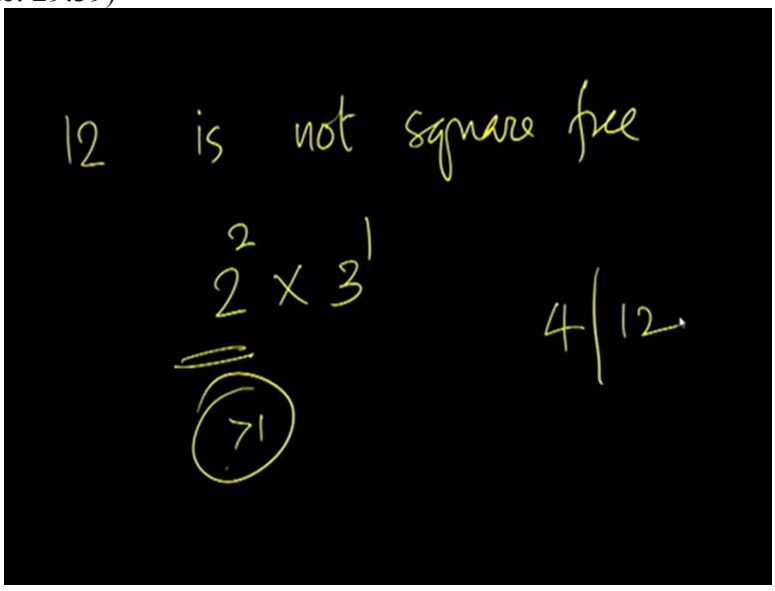
We say that an integer is a square if it can be written as n square for some integer n and we say that an integer n is square-free if 1 is the largest square dividing it.

(Refer Slide time. 28:24)



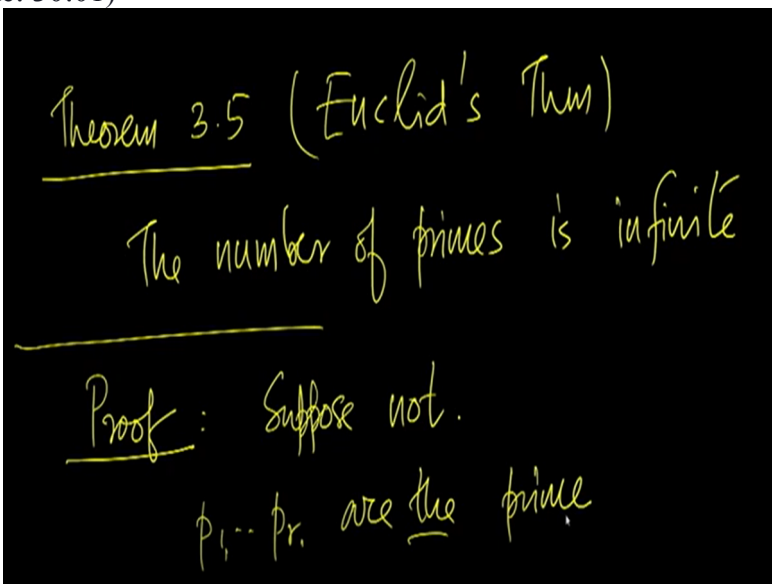
Consider 210 for example. 210 is 42 into 5 which is 6 into 7 into 5 or which can be written as 2 into 3 into 5 into 7, canonical prime factorization. The exponent is 1 everywhere. So, here we find that it does not have a square factor. So, then it is immediately clear that a number is square-free if and only if every exponent in its prime factorization is either 0 or 1. So in this case, 2, 3, 5, 7 are the prime numbers with an exponent of 1, every larger prime number has an exponent of 0.

(Refer Slide Time: 29:39)



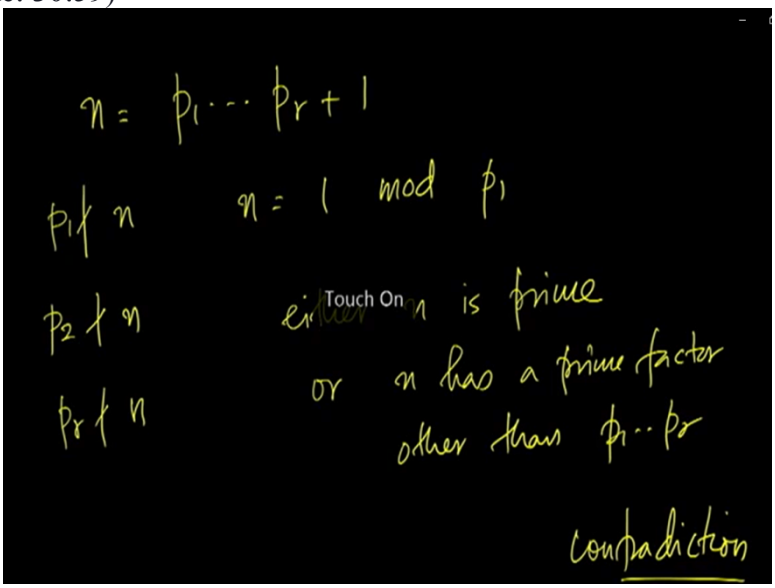
Number 12 is not square free. Its prime factorization is 2 power 2 which is 4 into 3 power 1. So, 2, in this case, has an exponent greater than 1. So, 12 is not square free. In particular, the square 4 divides 12.

(Refer Slide Time: 30:01)



The next theorem is called Euclid's theorem. What it says is that the number of primes is infinite. That is we can keep on finding ever-larger primes. The proof goes like this: Suppose the number of primes is infinite in which case let us say p 1 through p r are the primes. So there are only r primes and when they are listed in increasing order they are p 1 through p r. So p r is the largest prime let us say.

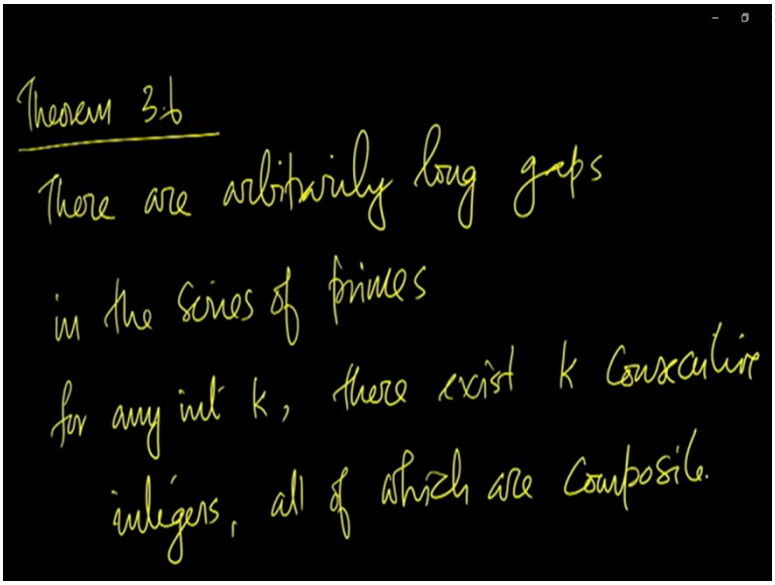
(Refer Slide Time: 30:59)

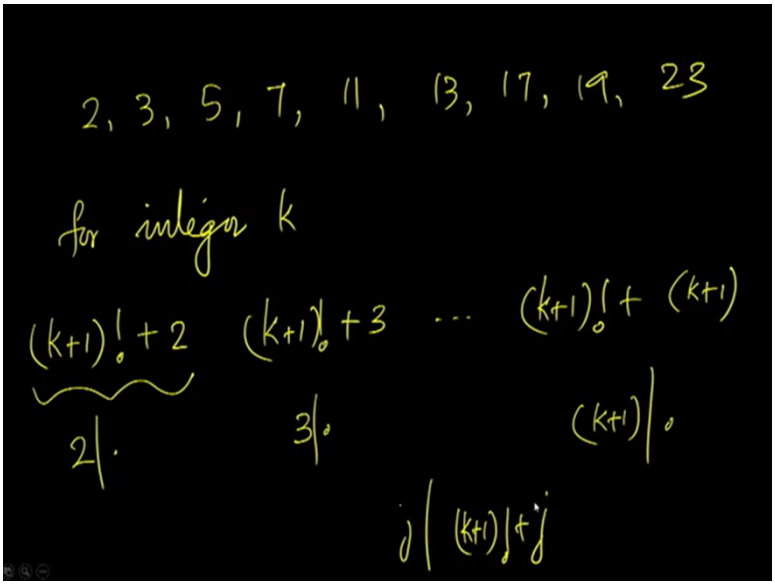


So, let us consider integer n which is the product p 1 through p r plus 1. Then we find that p 1 does not divide n because n is 1 mod p 1 that is when n is divided by p 1 we would get a remainder of 1. Similarly, p 2 also does not divide n, p 2 divides p 1through p r, therefore, n is not divisible by p 2. Similarly, none of these primes would divide n. So primes p 1 through p r do not divide n. Therefore, either n is prime which is a contradiction because we assume that p 1 through p r are the only primes.

Now n is a number which is larger than p r. Therefore, this cannot be or n has a prime factor other than p 1 through p r which again is a contradiction because we have assumed that p r is the largest prime and p 1 through p r are the only primes available. So, if n has a prime factor than it must be a prime which is larger than p r. So either way, we are finding a prime which is larger than p r which is a contradiction. So either way, we get a contradiction. Therefore, there is no largest prime. We can keep on finding larger primes. But then how dense are the primes.

(Refer Slide Time: 32:41)





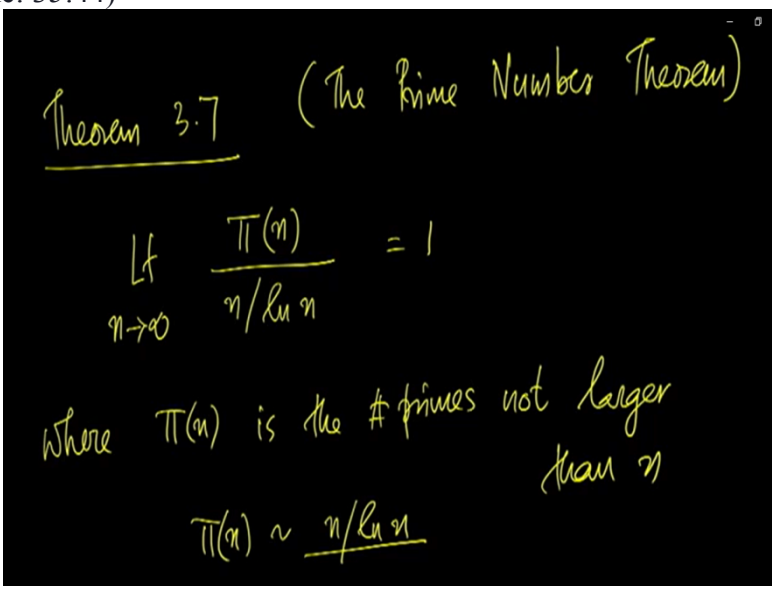
The next theorem says that there are arbitrarily long gaps in the series of primes. In other words, for any integer k there exist k consecutive integers all of which are composite. If you consider a few initial primes, you find that the gap between them is not much. So the primes are quite dense in the smaller integers. But then for integer k consider the sequence k plus 1 factorial plus 2, k plus 1 factorial plus 3 et cetera, k plus 1 factorial plus k plus 1. So that is a sequence of k integers, k consecutive integers and we can see that all of them are composite.

That is because if you consider this number k plus 1 factorial plus 2, in this number 2 divides k plus 1 factorial and 2 divides 2 too, therefore 2 divides this number. When you come to the second in the sequence 3 divides k plus 1 factorial and 3 divides 3, therefore 3 divides the

sum as well, so this number is divided by 3. When you come to the last of the sequence k plus 1 divides k plus 1 factorial and k plus 1 as well, therefore k plus 1 divides this sum. So in particular if you consider k plus 1 factorial plus j, we find that j divides k plus 1 factorial plus j for j ranging from 2 to k plus 1.

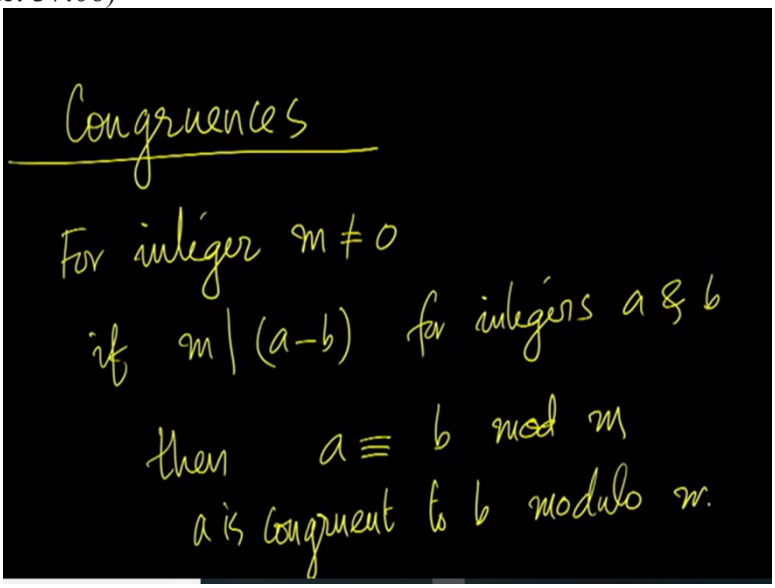
So these are k consecutive numbers all of which are composite. So you using this technique we can find arbitrarily large gaps in the series of primes.

(Refer Slide Time: 35:44)



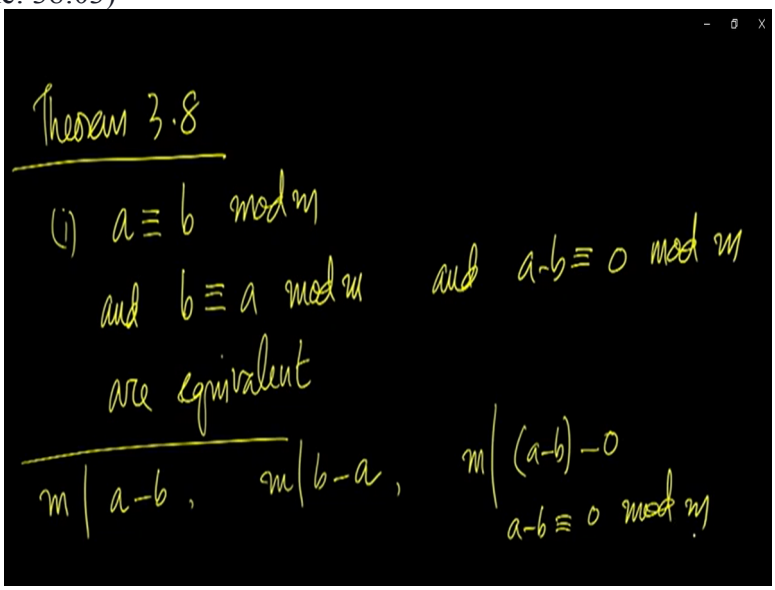
I will not prove the next theorem. This is called the prime number theorem or this theorem states is that limit of n tending to infinity pi of n divided by n by log of n equal to 1 where pi of n is the number of primes not larger than n. There is a number of primes not larger than n divided by n by the natural log of n tends to 1 as n tends to infinity. In other words, pi of n, the number of primes not larger than n is approximately n by log n. So out of the n numbers that we consider 1 to n approximately n by log n are primes.

(Refer Slide Time: 37:06)



Next, we study congruences. We say that for integer m not equal to 0 if m divides a minus b for integers a and b then we say a is b mod m or we say a is congruent to b modulo m. In short we write a is congruent to b mod m.

(Refer Slide Time: 38:03)

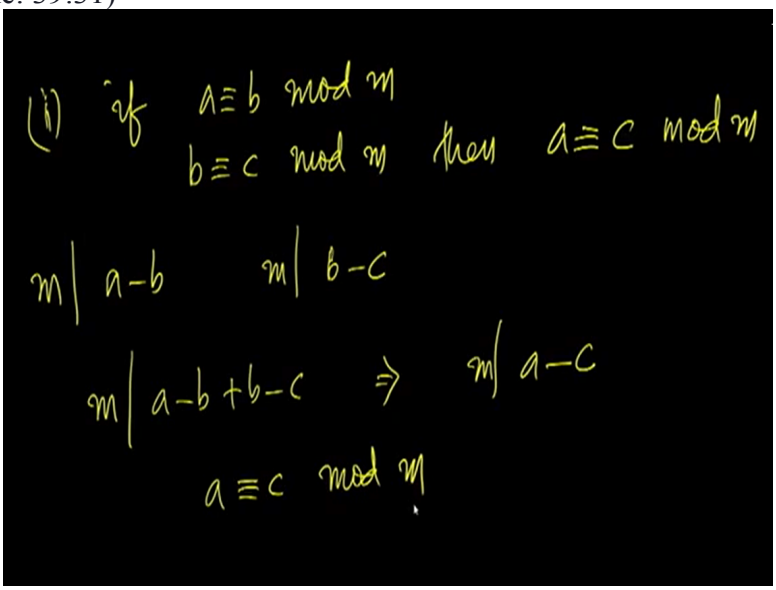


Let us see a theorem related to congruences. This theorem shows several properties of congruences. The first property says that a is congruent to b mod m and b is congruent to a mod m and a minus b congruent to 0 mod m for all equivalent statements.

You find that all these fall in the definition itself. If a is congruent to b mod m, then a minus b is divisible by m but if m divides a minus b, m divides b minus a as well which is the

negative of it. If m divides b minus a then we have b is congruent to a mod m. But then this can be written as m divides a minus b minus 0, a minus b is an integer when a and b are integers and 0 is an integer. Therefore, when we say m divides a minus b minus 0 what it means is that a minus b is congruent to 0 mod m.

(Refer Slide Time: 39:31)



The second part of the theorem says if a equal to b mod m and b equal to c mod m then a is congruent to c mod m. Once again it follows from the definition if a is congruent to b mod m then a minus b is divisible by m. From the second assumption we have m divides b minus c. If m divides a minus b and b minus c then m should divide their sum too which is a minus b plus b minus c which means m divides a minus c. If m divides a minus c where a and c both are integers we have that a is congruent to c modulo m which is the conclusion. Ok, that is it from this lecture. Hope to see you in the next. Thank you.