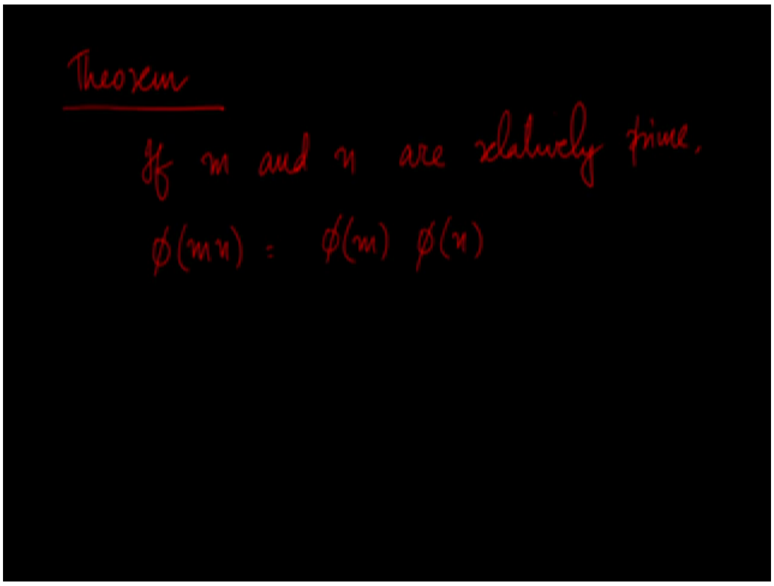
Discreet Mathematics

Professor. Sajith Gopalan
Department of Computer Science and Engineering,
Indian Institute of Technology, Guwahati.

Lecture 36
Totient; Congruence, Floor and Ceiling Functions

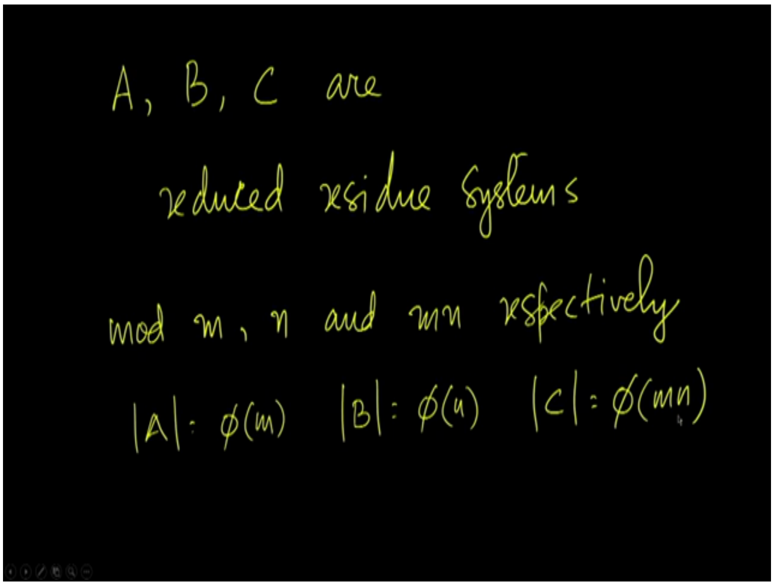
Welcome to the NPTEL mock on discreet mathematics this is the 7 th lecture on number theory.

(Refer Slide Time: 00:36)



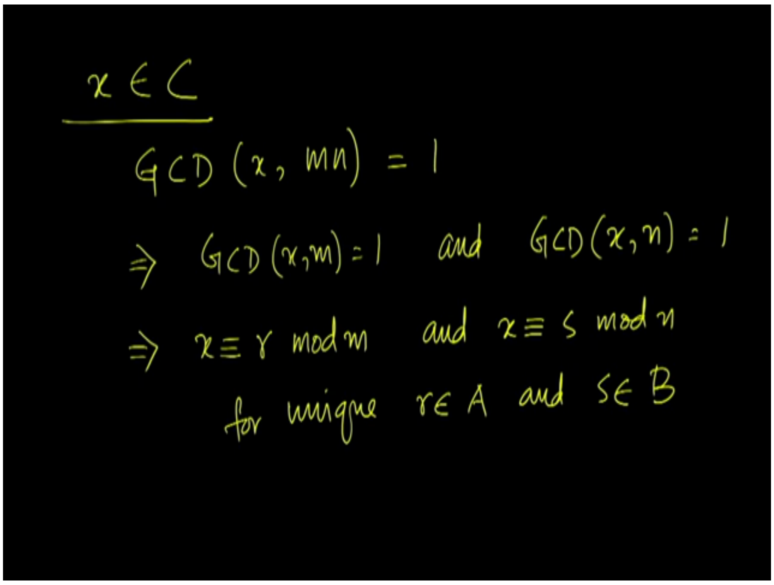
First we will consider a theorem regarding (())(0:43) five functions, if m and n are relatively prime then phi of mn is equal to phi of m into phi of n, for any 2 positive integers m and n that are relatively prime to each other phi of m into phi of n.

(Refer Slide Time: 1:23)



So let us prove this, let us say A, B, C are three set they are 3 reduced residue systems, modulo m and n, mn respectively. Then the size of A is phi of m, size of B is phi of n and size of C is phi of m into n.

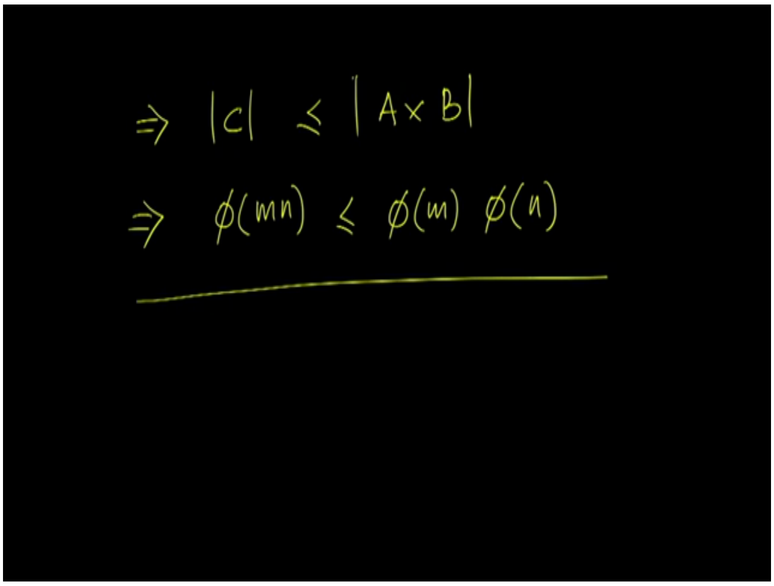
(Refer Slide Time: 02:04)



Let us say x is some member of C, the reduced residue systems modulo mn, then GCD of x and mn is 1 by definition. So x does not divide m and n there is no common factor between x and mn, therefore GCD of x and m should be 1 and the GCD of x and n should be 1 to which means x is r mod m and x is s mod n for unique r and s.

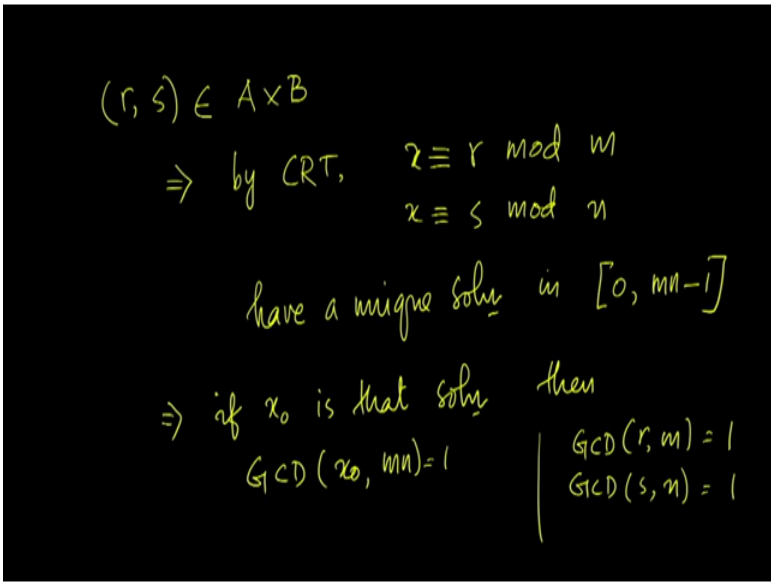
Where r belongs to A and S belongs to B. If x is relatively prime to m and x is relatively prime to n then x belongs to the reduced residue systems modulo m and x also belongs to the reduced residue systems modulo n. Which means in this residue systems A and B that we consider there are some elements unique elements r and s so that x is congruent to r mod m and x is congruent to s mod n.

(Refer Slide Time: 03:23)



Which means the size of C is less than or equal to the size of A cross B, because we take an arbitrary element x belonging to C and correspondingly we find an ordered pair or s belonging to A cross B. Therefore, the size of C must be less than or equal to the size of A cross B, but what is the size of C? That is phi of mn this is less than or equal to phi of m into phi of n. so that is what we have established that is one way.

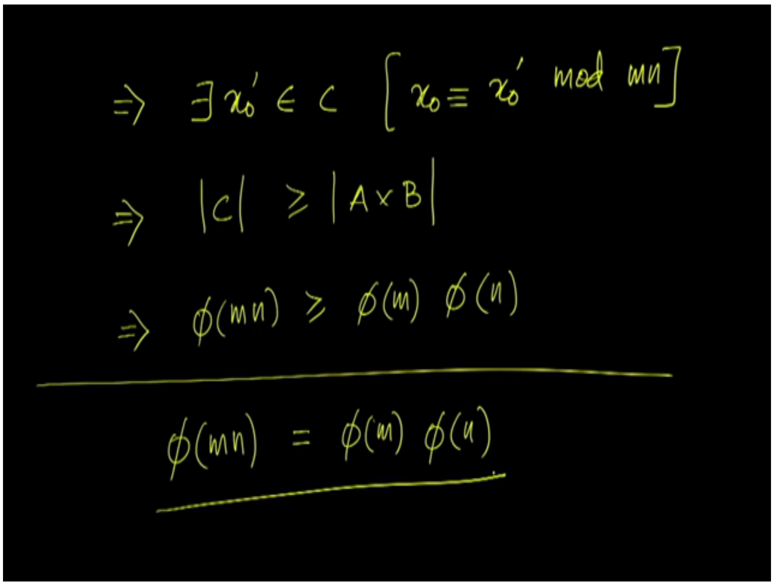
(Refer Slide Time: 04:00)



Now let us take an ordered pair r, s belonging to A cross B, then by Chinese Remainder Theorem x is r mod m and x is s mod n these two congruences have a unique solution in 0 to mn minus 1. So if x naught is that solution then GCD of x naught mn is 1 because GCD of r, m equal to 1, r belongs to A and GCD of s belongs to n. GCD of s, n is 1 because s belongs to

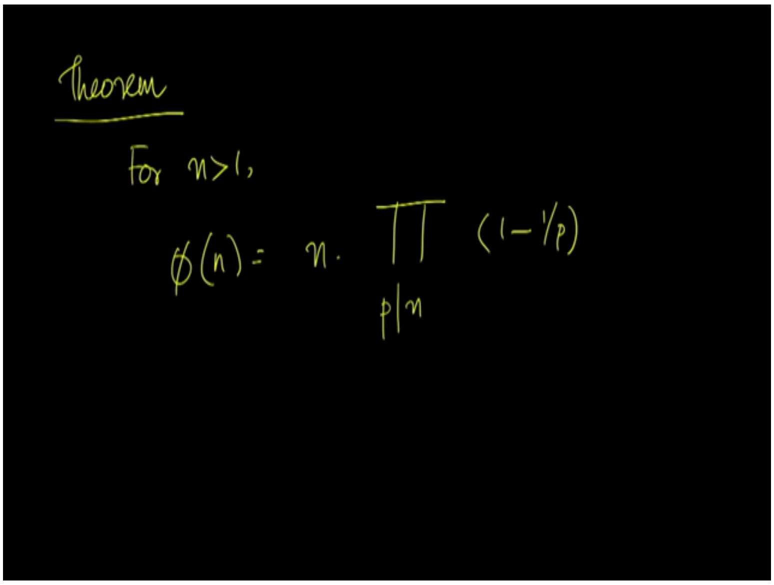
B which is a reduced residue systems modulo n. Therefore, x naught is relatively prime to mn.

(Refer Slide Time: 05:25)



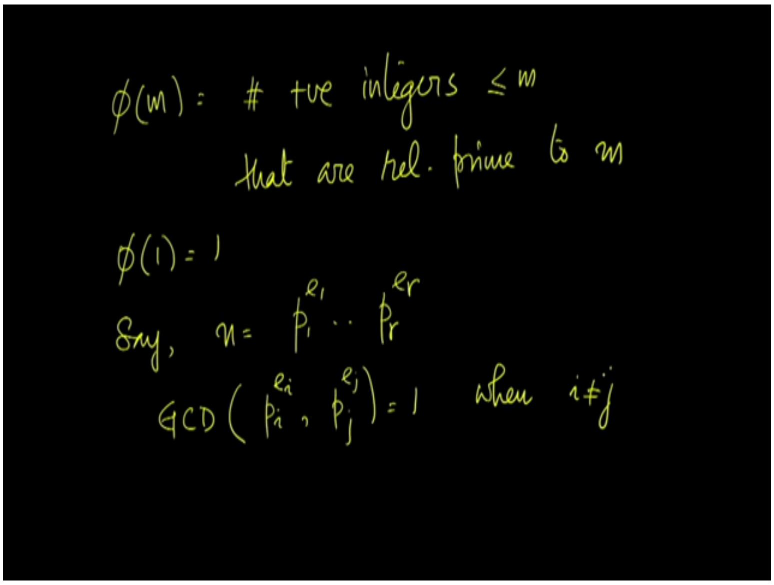
Which means there exists an x not prime belonging to C, such that x naught is congruent to x naught prime modulo mn, C is reduced residue systems modulo mn therefore there should be an x naught prime which is congruent to x naught in that. This establishes that the size of C is greater than or equal to the size of A cross B, that is for each ordered pair or s belonging to A cross B. We have been able to find an element x naught prime in other words phi of mn is greater than or equal to phi of m into phi of n. So combining both we have the theorem when m and n are relatively prime then phi of mn is equal to phi of m into phi of n.

(Refer Slide Time: 06:30)



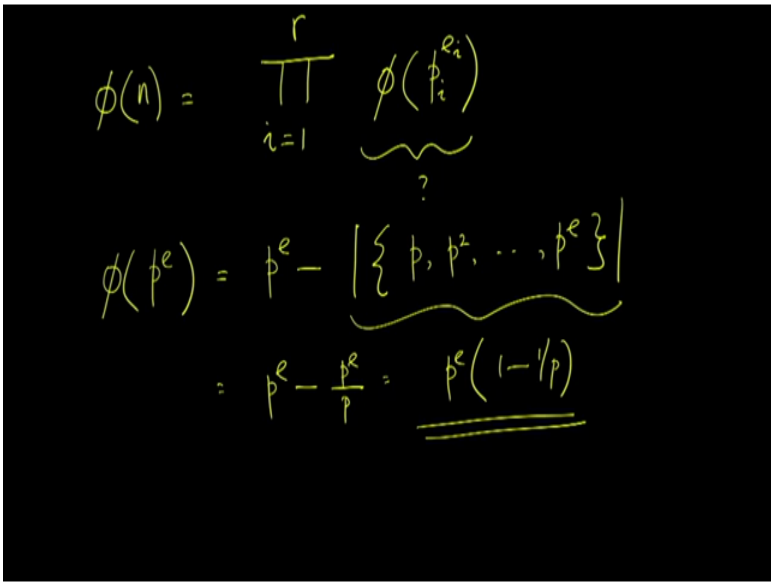
Another interesting theorem which allows us to calculate phi easily, for n greater than 1 phi of n is equal to n times the product over all p which divides n of 1 minus 1 by p. So this makes it easy to calculate the phi function for you unfairly large numbers.

(Refer Slide Time: 07:04)



From the definition we know that phi m is the number of positive integers greater than or equal to 1, less than or equal to m that are relatively prime to m, we know phi of 1 equal to 1. Say the given number n is prime factorized in this fashion p1 power e1 etc upto pr power er where pi is the ith prime number. So this is the prime factorization therefore pi and pj are not the same when i not equal to j, which means the GCD of pi power ei and pj power ej is 1 when i not equal to j.

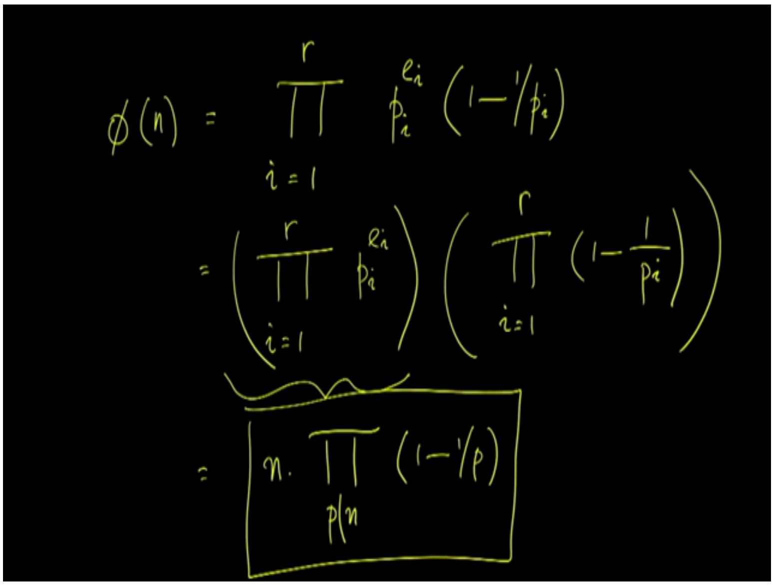
(Refer Slide Time: 08:09)



So by default the previous theorem we can express phi of n as the product over i varying from 1 to r of phi of p i power ei but what is this quantity? Let us compute this first phi of p power e so here we consider all integers less than or equal to p power e all positive integers less than or equal to p power e and from this we remove all numbers that are devices of p power e.

The size of the resultant that is phi of p power e, that is we consider the reduced residue systems, then the reduced is residue system will have these many elements, p power e minus the size of all devices of p power e but what are the devices of p power e. there p, p square, etc upto p power e, but what is this quantity? That is p power e divided by p, so this can be written as p power e into 1 minus 1 by p, so that is the phi value of p power e.

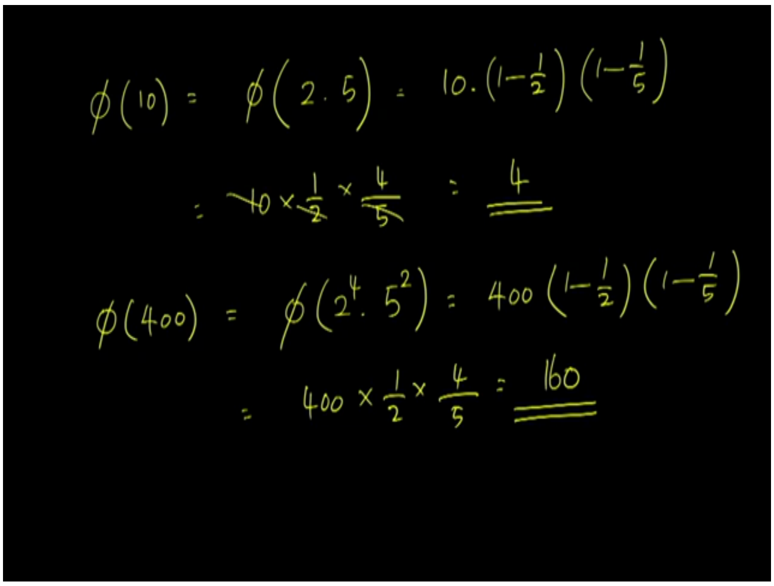
(Refers Slide Time: 09:35)



Therefore, coming back to this equation we can write phi of n as product of i varying from 1 to r of p i power ei into 1 minus 1 by using this form, but this is pie varying from 1 to r of pi power ei and again pie varying from 1 to r of 1 minus 1 by pi but the quantity within the first bracket is nothing but n, so this is n multiplied by the product over phi varying from 1 to r of 1 minus 1 by pi.

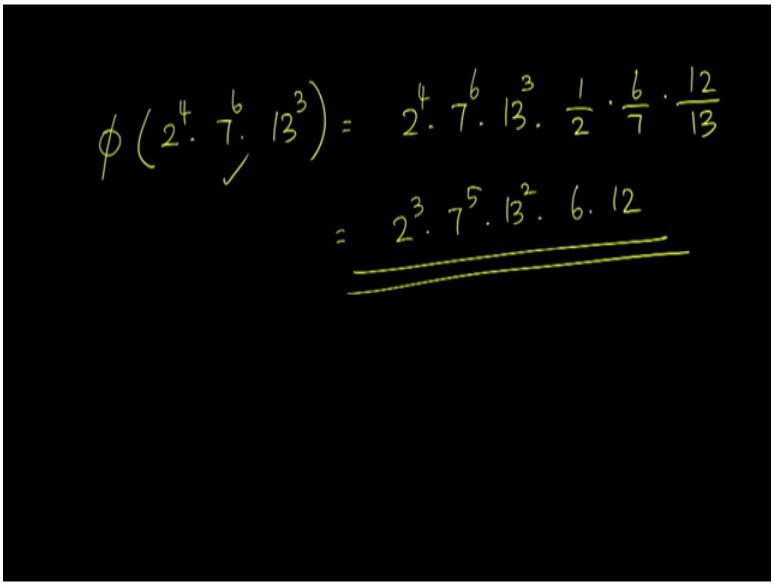
Which means we are considering all prime numbers that divide n, so this product is actually over all prime numbers that divide n, for each such prime number 1 minus 1 by p has to be multiplied together, so this product is what phi of n is.

(Refer Slide Time: 10:46)



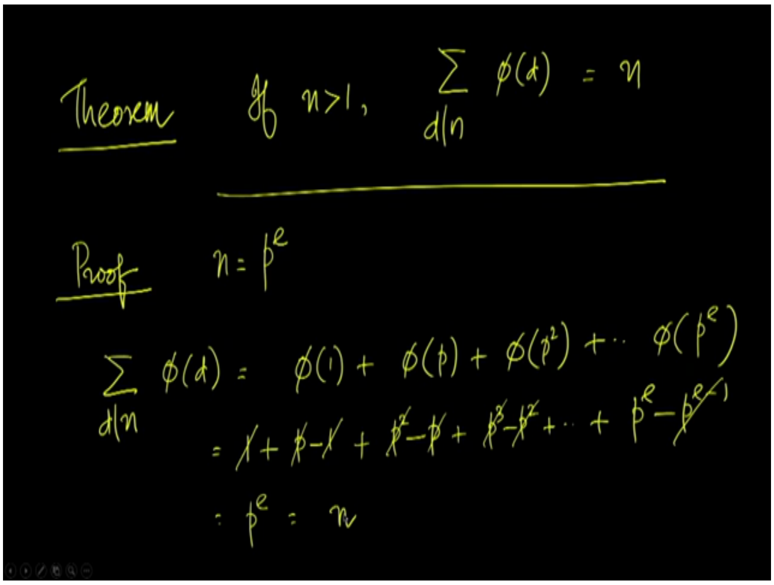
For example, let us calculate phi of 10 which is taking the prime factorization of 10 this is phi of 2 into 5 then that would be 10 multiplied by 1 minus 1 by 2, 2 is a prime which divides 10 and 5 is a prime which divides 10 therefore this is 10 into half into 4 by 5, so 5 of 10 is 4. Let us now compute phi of 400, phi of 400 is phi of 2 power 4 into 5 power 2 so there are two primes here 2 and 5 again, so this will be n into 1 minus 1 by 2 into 1 minus 1 by 5, this is 400 into half into 4 by 5, 200 into 0.8 which is 160. So phi of 400 is 160 which we have used in an example earlier in one of the earlier lectures.

(Refer Slide Time: 12:03)



Phi of 2 power 4 multiplied by 7 power 6 multiplied by 13 power 3 is this number 2 power 4 into 7 power 6 into 13 power 3 multiplied by 1 minus 1 by 2 which is 1 by 2, 1 minus 1 by 7 which is 6 by 7 and 1 minus 1 by 13 which is 12 by 13, that would be 2 power 3, 7 power 5, 13 power 2, multiplied by 6 and 12. So this is phi value of this number.

(Refer Slide Time: 12:51)

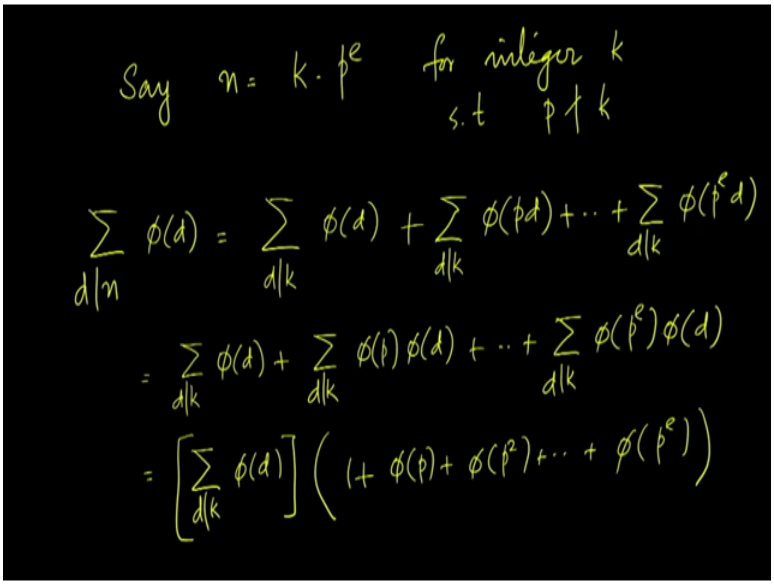


Now from this we can prove another interesting result, if n is a positive integer sum of phi of d over all devices d of n is n, the proves goes this way first consider numbers of the form p power e so n is p power e let us say, then we are summing over all devices of n of phi of d.

So this would be phi of 1 plus phi of p plus phi of p square etc, all the way upto phi of p power e, these are the devices of n when n is of the form p power e, 1p, p square etc are the devices of n. but phi of 1 is 1, phi of p is p minus 1 as we have seen before phi of p power e is p power into 1 minus 1 by p.

So, phi of p square would be p square into 1 minus 1 by p which is p square minus p then we have p cube minus p squared eliminating with p power e minus p power e minus 1, so we find that the sum telescopes 1 and 1 cancel, p and minus p cancel, p squared and minus p squared cancel, p cube cancels, p power e minus 1 cancels what remains is p power e which is nothing but n. So the theorem holds when n is of the form p power e.

(Refer Slide Time: 14:44)

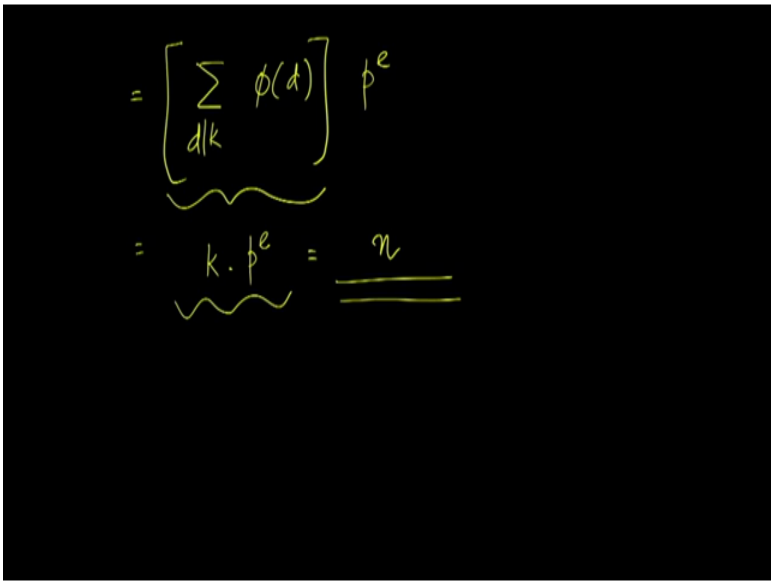


Now, suppose n is of the form k times p power e for integer k such that p does not divide k, so k and p power e are relatively prime to each other, then our required sum, sum over all devices of n of phi of d can be written like this. First consider all devices of k, so this is the part of the sum but then that is not the whole of it.

We also consider all devices of pd that have not been considered before that is for every device a d of k we consider pd, continuing like this if you sum in this fashion we would exhaust all devices of n, so all these sums are over devices k, but then since d and p are relatively prime to each other this can be written this fashion the first term does not change the second term can be written like this phi of p into phi of d.

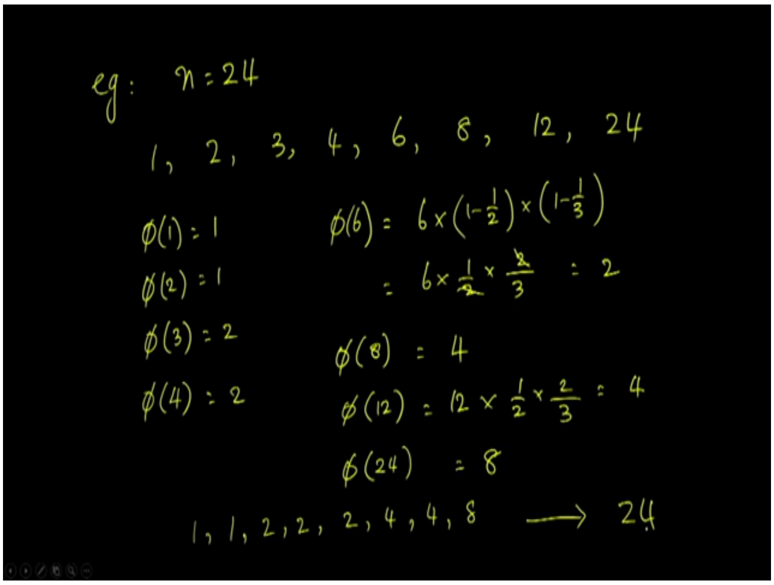
Here it is phi of p power e into phi of d, then this is a common factor this is taken outside we have 1 plus phi of p plus phi of p square plus etc all the way up to phi of p power e, but this is the sum that we have just seen since 1 is the same as phi of 1 it is identical to this sum which we know evaluates to p power e.

(Refer Slide Time: 17:00)



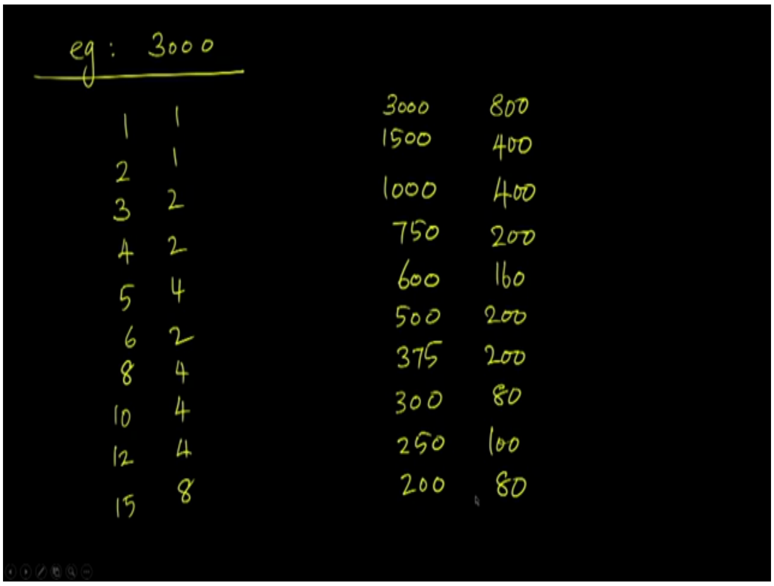
Therefore, this is the quantity within the square brackets which is sigma d that divides k of phi of d into p power e, but this quantity inductively we assume is k then we have the sum reducing to k into p power e which is nothing but n, and that is what we seek to prove so the case for p power e is the basis and inductively here we apply the hypothesis that this sum evaluates to k, therefore the induction holds so inductively we prove the statement.

(Refer Slide Time: 17:51)



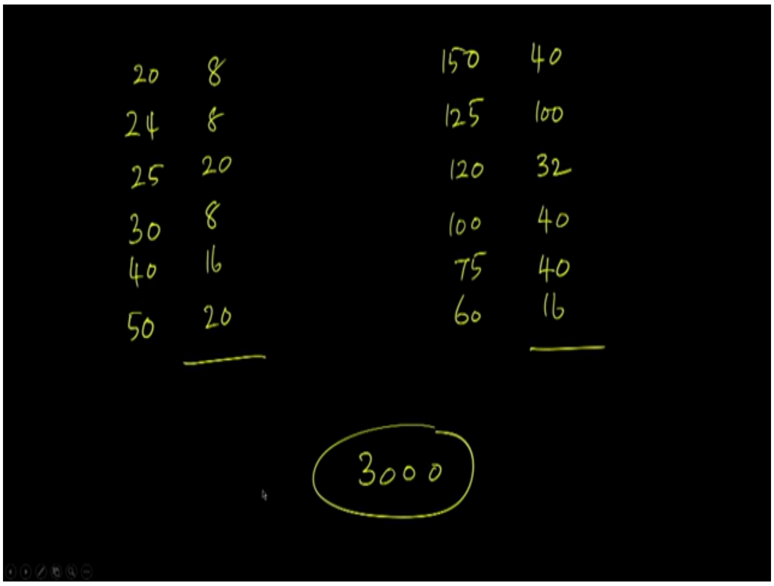
For example, let us say n equals to 24 and the devices 1, 2, 3, 4, 6, 8, 12 and 24. Phi of 1 is 1, phi of 2 is 1, phi of 3 is 2, phi of 4 is 2 that is 1 and 3 now phi of 6 using the formula would be 6 multiplied by 1 minus 1 by p for every primes, so 2 and 3 are the primes which coexist and 6 so have 1 minus 1 by 2 into 1 minus 1 by 3 which is 6 into half into 2 by 3 which is 2, So phi of 6 is 2. Phi of 8 similarly is 4, phi of 12 is 12 into half into 2 by 3 which is 4, phi of 24 is 8 so summing all these values 1, 1, 2, 2, 2, 4, 4 and 8 you find that the sum comes to 24.

(Refer Slide Time: 19:19)



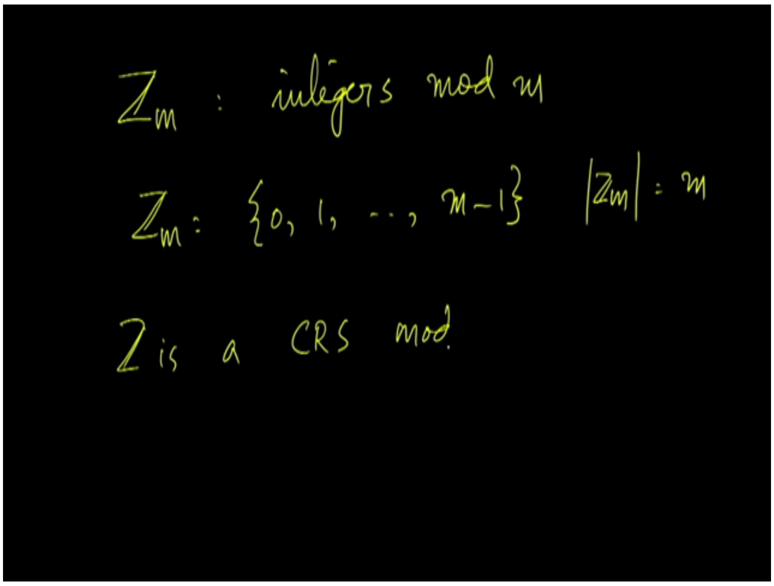
Taking the larger example, consider n equals 3000 then the factors would be 1 3000, 2 1500, 3 1000, 4 750, 5 600, 6 500, 8 375, 10 300, 12 250, 15 200. So these are sum of the factors if you compute the corresponding phi values you find these are 3000 you can see that the phi value is 800, 1500 it is 400 for 1000 again it is 400, for 750 it is 200, 600 is 160, 500 is 200, 375 is 200, 300 is 80, 250 is 100, 200 is 80.

(Refer Slide Time: 20:59)



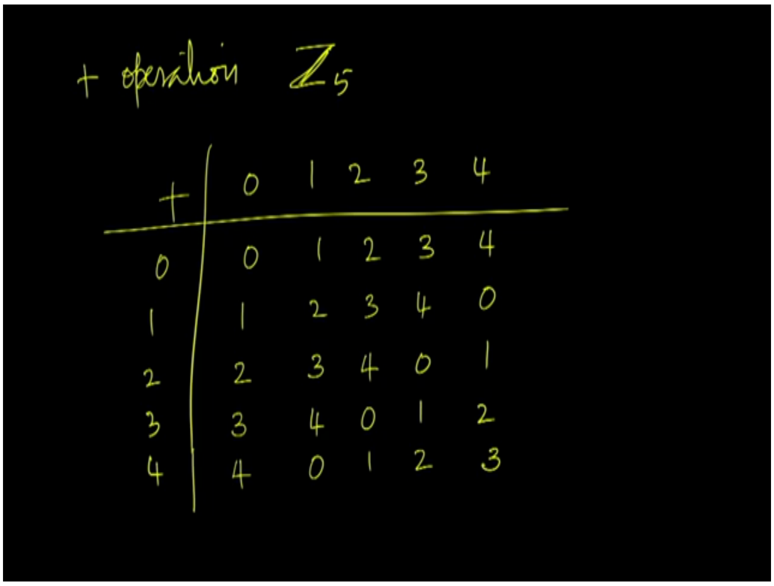
The remaining factors would be 20, 24, 25, 30, 40, 50, 50 into 60 is 3000, 40 into 75, 30 into 100, 25 into 120, 24 into 125, 20 into 150 so the corresponding phi values would be 8, 8, 20, 8, 16, 20 for 150 it is 40, for 125 it is 100, for 120 it is 32, for 100 it is 40, 75 it is 40 again, for 60 it is 16. So these are the phi values if you add up all the phi values together you find that the sum comes to 3000 again, this is what n is.

(Refer Slide Time: 22:16)



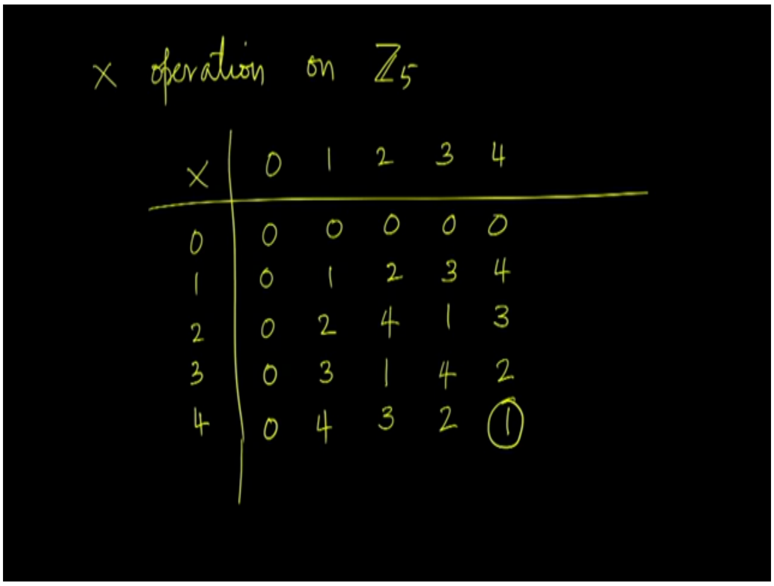
By Zm we denote integers modulo m, there is Zm is 0 to m minus 1 the cordiality of Zm would be m, so as you can see Zm is a complete a residue system module m.

(Refer Slide Time: 22:48)



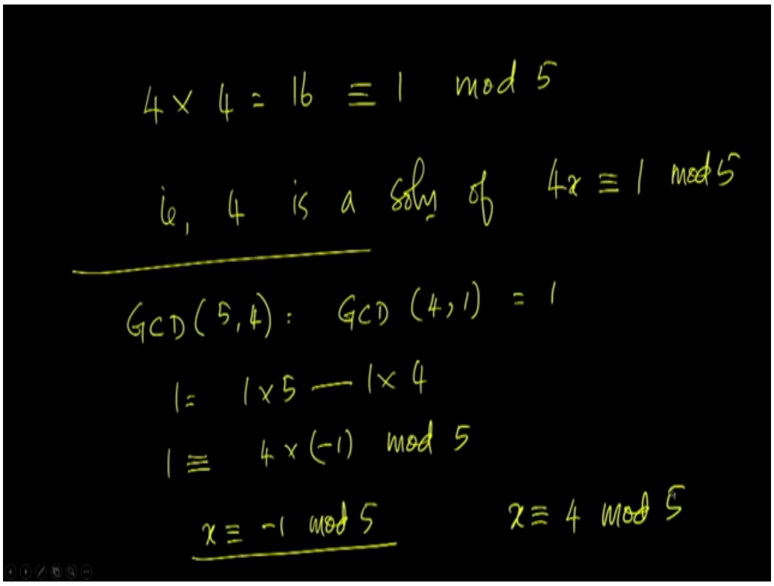
We can define the addition operation on Zm plus you can draw up a table so here let us consider the table of Z5, so 0 plus X is X, 1 plus 4 is 5 which is 0 modulo 5, 2 plus 4 is 6 which is 1 modulo 5, 3 plus 4 is 7 which is 2 modulo 5, 4 plus 4 is 8 which is 3 modulo 5. So this is the addition table for Z5.

(Refer Slide Time: 24:00)



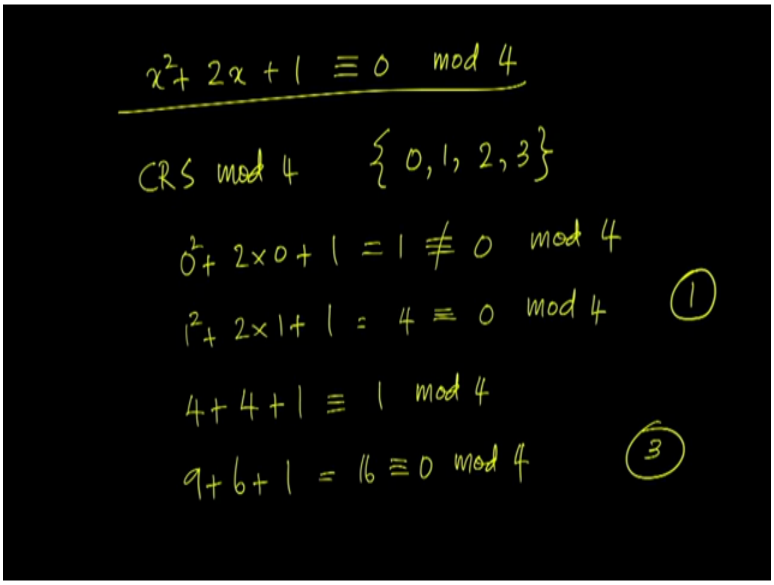
When we come to the multiplication operation on Z5 0 into X is 0. So the top row is all 0 similarly the left most column is also all 0, 1 into X is X so here we have values in this fashion, now 2 into 2 is 4, 4 is 4 mod 5, 2 into 3 is 6 so we have 1 mod 5 here 2 into 4 is 8 which is 3 mod 5, 3 into 2 is 6 which is 1 mod 5, 3 into 3 is 9 which is 4 mod 5, 3 into 4 7 which is 2 mod 5, 4 into is 8 which is 3 mod 5, 4 into 3 is 7 which is 2 mod 5, 4 into 4 is 16 which is 1 mod 5. So this is the multiplication table on Z5, so from the table you find that 4 into 4 is 16 which is 1 mod 5.

(Refer Slide Time: 25:23)



For example, that is 4 is the solution of 4x equals 1 mod 5. Recalled we solved such equations using Euclids algorithm, GCD of 5, 4 is the same as GCD of 4, 1 which is 1 therefore 1 is 1 into 5 minus 1 into 4 if you take mod 5 on both sides you have 1 congruent to 4 into minus 1 mod 5. So minus 1 is a solution for this equation. So x congruent to minus 1 mod 5 is a solution but then minus 1 is congruent to 4 so this is the same as x congruent 4 mod 5.

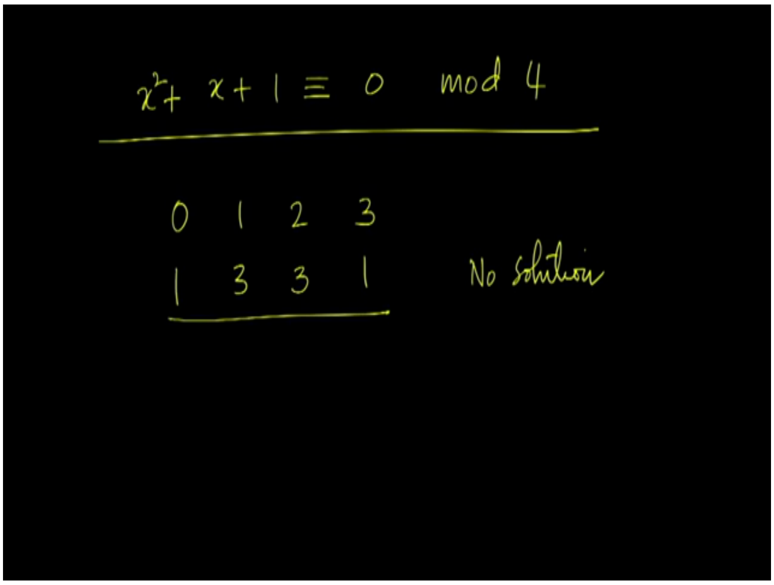
(Refer Slide Time: 26:37)



Let us now consider some quadratic congruencies, x squared plus 2 x plus 1 is congruent to 0 mod 4, the complete residue system mod 4 has 4 members this is one complete residue system, so we can try its members. So when x equals to 0 we have 0 squared plus 2 into 0 plus 1 which is 1 this is not congruent to 0 mod 4, so 0 is not a solution so if you put 1 here we have 1 squared plus 2 into 1 plus 1 which is 1 plus 2 plus 1 which is 4 that is 0 mod 4.

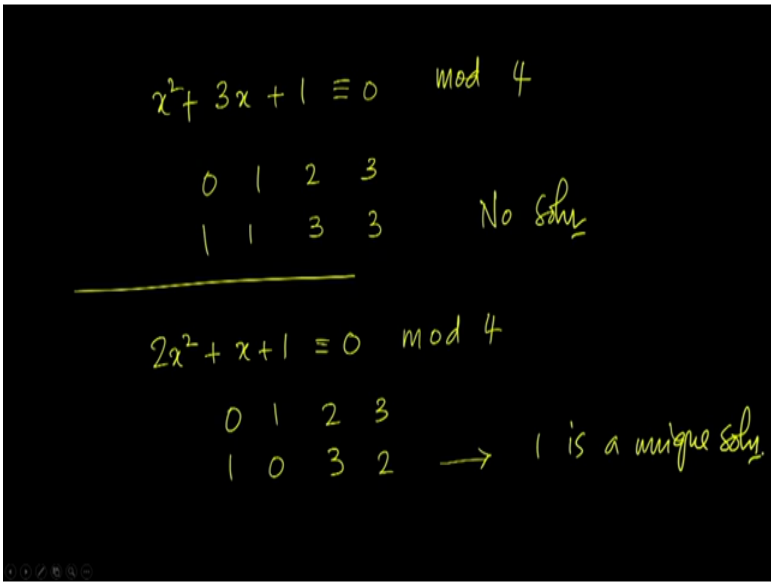
Which means 1 is a solution, if you put 2 in we have 2 squared which is 4 plus 2 into 2 which is 4 plus 1 so that is 8 plus 1 9 which is 1 mod 4 so this is not a solution when you have 3 into 3 9, 2 into 3 6 plus 1 which is 16 which is 0 mod 4. So this is a solution 2, so 1 and 3 or two solutions for this quadratic congruence and modulo 4 this are the only solutions, modulo 4 there could be 4 solutions we have tried all of them and we found that only 1 and 3 are solutions. By what we have seen earlier if for in any complete residue system modulo 4 there will be exactly 2 members that are solutions for this quadratic congruent those two solutions would be congruent to 1 and 3 respectively modulo 4.

(Refer Slide Time: 28:35)



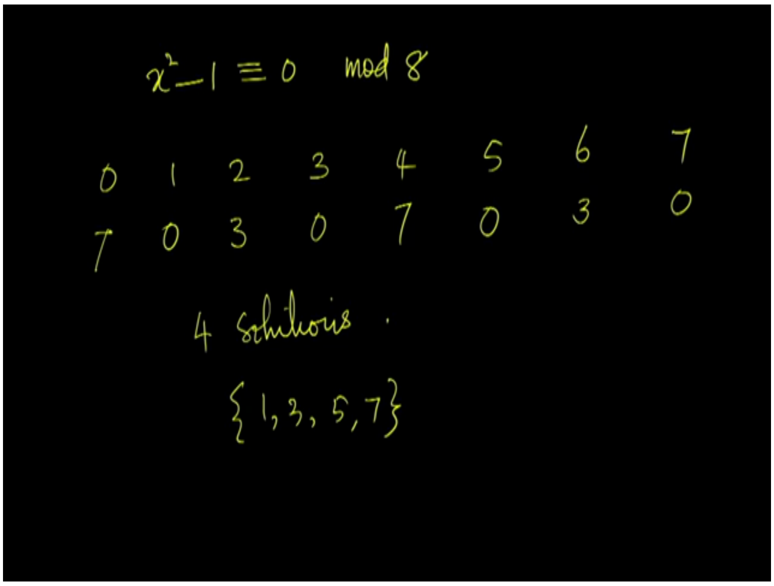
Consider another quadratic congruence, again we are considering CRS modulo 4 so we can consider the members of CRS 0, 1, 2, 3 or members of Z4 then when you plug in these values for x from 0 you get 1, from 1 you get 1 plus 1 plus 1 which is 3, from 2 you have 4 plus 2 6 plus 1 7, 7 mod 4 is 3 and then from 3 you find 9 plus 3 12 plus 1 13 which is 1 mod 4. So we find that none of them will provide a solution, so this quadratic congruent is without a solution so it is possible for congruence to have no solution.

(Refer Slide Time: 29:32)



Consider another one x squared plus 3x plus 1 is 0 mod 4 this is what we want to solve again when you consider 0, 1, 2, 3 you find that the values are 1 1 3 3 again there is no solution. If you consider 2x squared plus x plus 1 equals congruent to 0 mod 4, if this is the case then for 0, 1, 2, 3 you find that the values are 1 0 3 and 2, so there is a unique solution here, 1 is a unique solution.

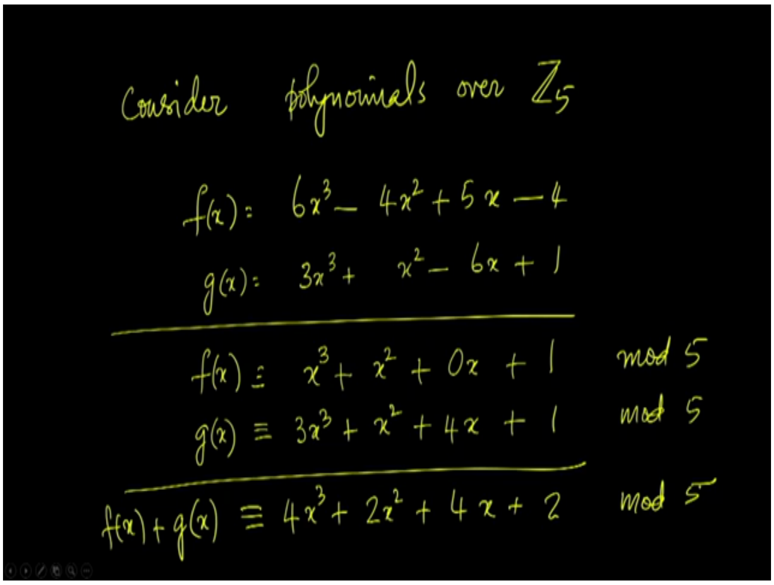
(Refer Slide Time: 30:22)



Consider x squared minus 1 congruent to 0 mod 8, so here the members of Z8 would be 0, 1, 2, 3, 4, 5, 6 and 7. So if you evaluate here for 0 x squared minus 1 is minus 1 which is 7 mod 8, for 1 it is 1 minus 1 0, for 2 it is 4 minus 1 3, for 3 it is 9 minus 1 8 which is 0, for 4 it is 16 minus 1 15 which is 7 again.

For 5 25 minus 1 24, for 6 35 which is 3, for 7 it is 49 minus 1 48 which is 0 mod 8 so you find that there are 4 solutions, so the solution as it 1, 3, 5, 7. If you find that the number of solutions could be larger than the degree of the polynomial, so here we have a quadratic polynomial for the number of solutions is 4.

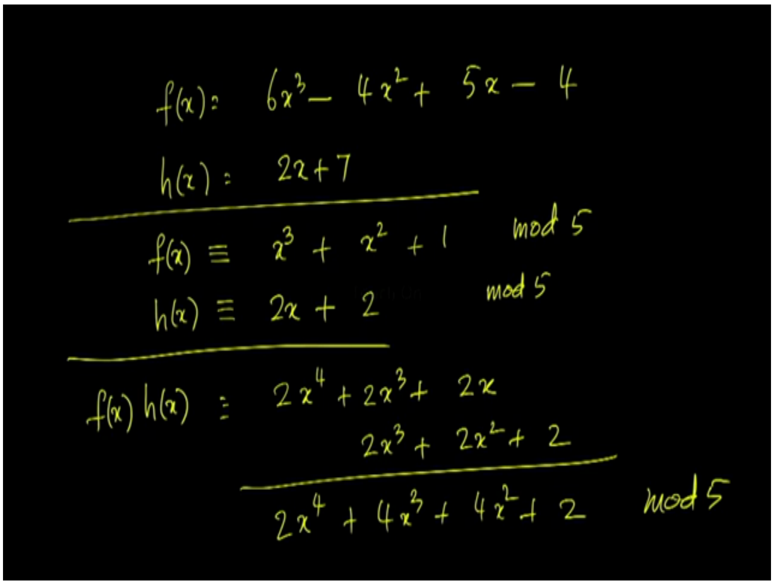
(Refer Slide Time: 31:38)



Regarding polynomial addition, multiplication consider these 2 polynomials over Z5, let us say f of x is 6x cube minus 4x squared plus 5x minus 4, g of x is 3x cube plus x squared minus 6x plus 1. These can be simplified in this fashion, f of x is the sum of the first term of 6x cube but since 5x cube for any integer x is divisible by 5 this can be written as x cube minus 4 is congruent to 1 modulo 5.

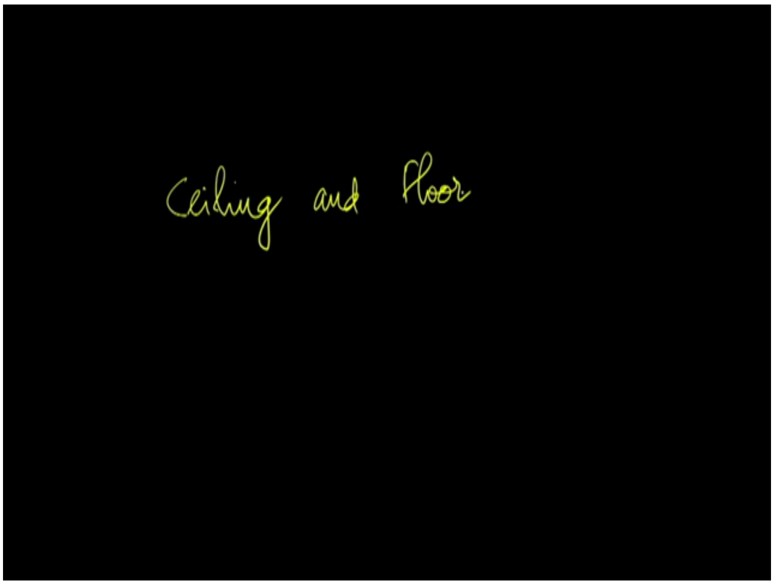
So this can be written as x squared, 5x is divisible by 5 so we have 0x and then minus 4 is congruent to plus 1 again so we have plus 1, so f of x can be written in this simplified form module 5. So we say f of x is congruent to this polynomial modulo 5, similarly g of x is congruent to 3x cube plus x squared minus 6x is the same as minus x which is the same plus 4x and plus 1. If you were to add these polynomials the sum would be 4x cube plus 2x squared plus 4x plus 2 mod 5.

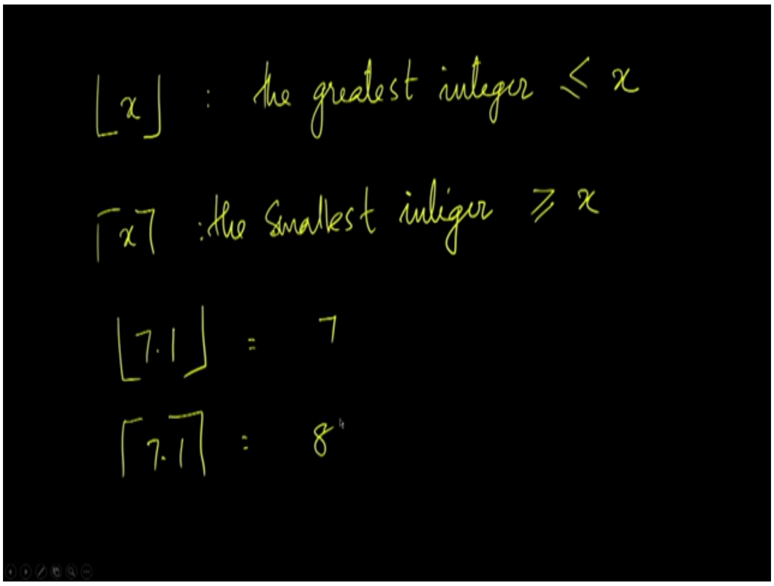
(Refer Slide Time: 33:44)



Once again if f of x is 6x cube minus 4x squared plus 5x minus 4 and h of x is 2x plus 7 then as before we can simply the f of x is congruent to x cube plus x squared plus 1 h of x is congruent to this is of course mod 5, f of x is congruent to 2x plus 2 mod 5 again then if you take the product f of x into h of x to get 2x power 4 plus 2 x cube plus 2x, 2x cube plus 2x square plus 2 which is 2 x power 4 plus 4 x cube plus 4 x squared plus 2. So that is how you add and multiply polynomials in modular arithmetic.

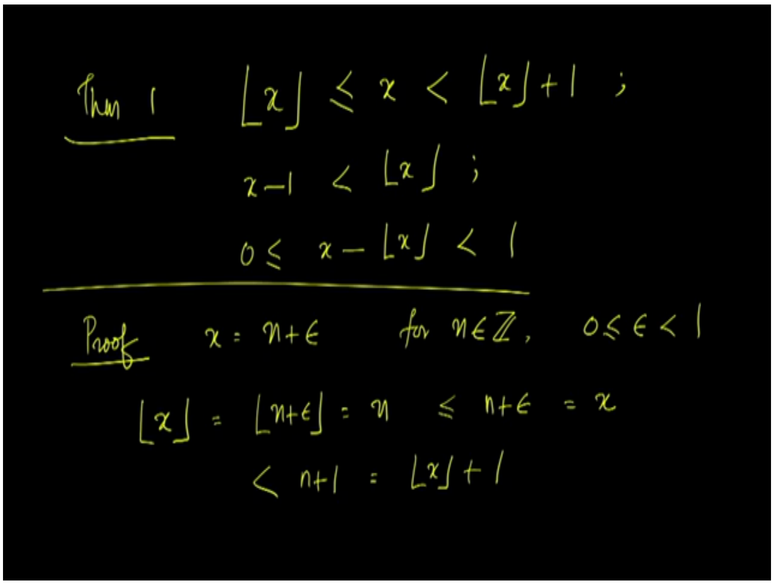
(Refer Slide Time: 35:05)





Now, let us study the Ceiling and Floor functions. The floor of x is defined as the greatest integer less than or equal to x and the ceiling effects is defined as the smallest integer greater than or equal to x, for example floor of 7.1 is 7 ceiling of 7.1 is 8.

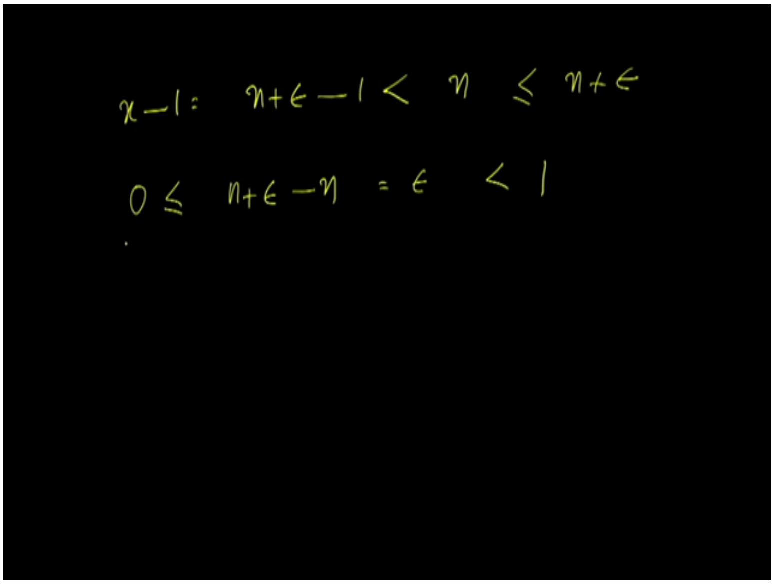
(Refer Slide Time: 35:53)



So, let us see a few results regarding the ceiling and floor functions, the first theorem says that floor of x is less than or equal to x. which is less than floor of x plus 1 and x minus 1 is less than floor of x and 0 is less than or equal to x minus floor of x which is less than 1, so to prove this suppose x is n plus epsilon for an integer n and a epsilon which is between 0 and 1.

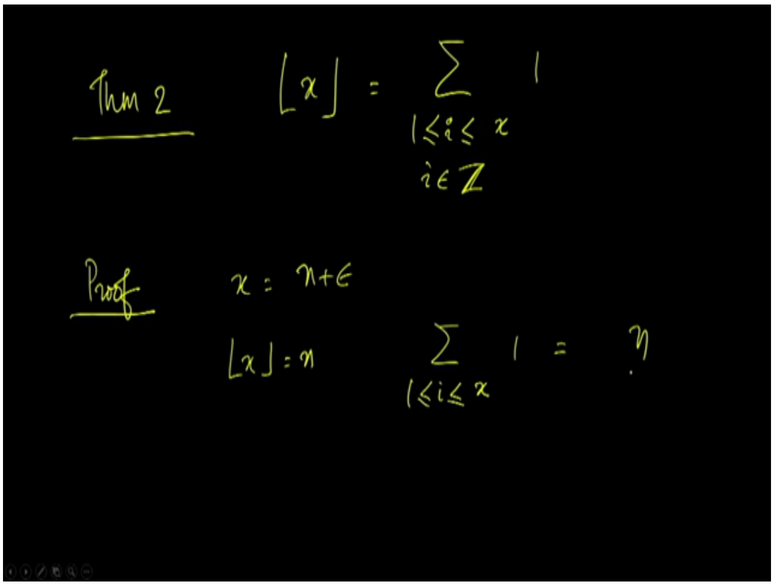
Epsilon could be 0 but epsilon is less than 1, then the floor of x is the floor of n plus epsilon which is n this is less than or equal to n plus epsilon naturally because epsilon is between 0 and 1but this is what x is. So we have that the floor of x is less than or equal to x but x is n plus epsilon which is less than n plus 1 because epsilon is less than 1 this is as we have seen n is floor of x so this is floor of x plus 1, so which proves the first line here.

(Refer Slide Time: 37:30)



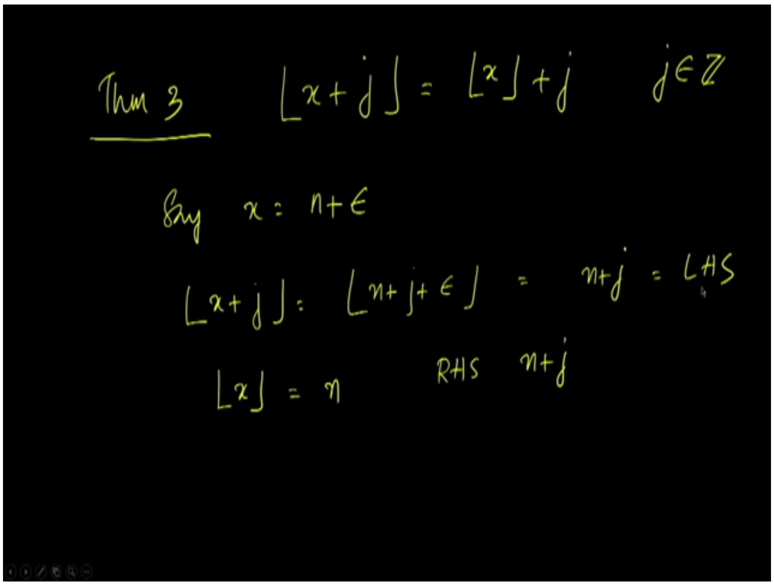
x minus 1 is n plus epsilon minus 1 which is less than n which is less than or equal to n plus epsilon which proves the second line, 0 is less than or equal to n plus epsilon minus n because epsilon is greater than or equal to 0 this is of course epsilon which is less than 1 which proves the third line.

(Refer Slide Time: 37:57)



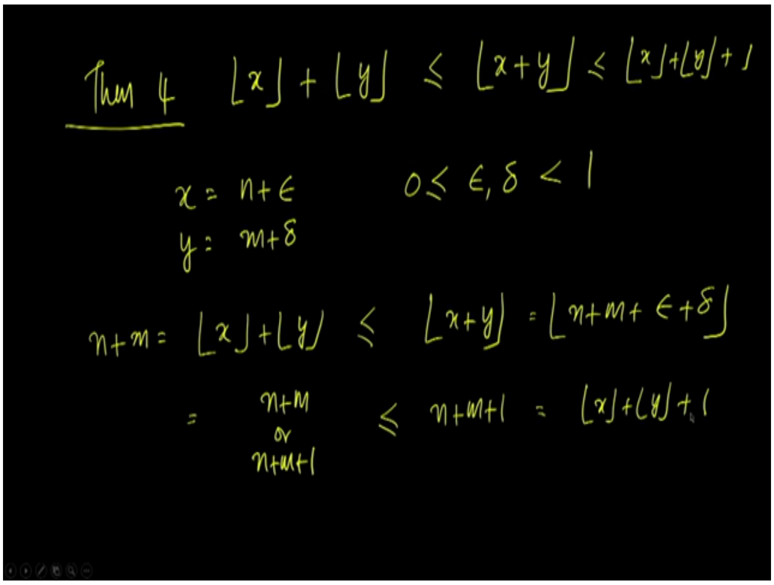
Floor of x is also equal to the sum over 1 less than or equal to i less than or equal to x. Where i is an integer of 1 thus the prove consider x is n plus epsilon where epsilon is as before then floor of x is n that is what the left hand side then sigma 1 less than or equal to i less than or equal to x for integer i would be less than n.

(Refer Slide Time: 38:38)



Thirdly the floor of x plus j is the floor of x plus j for any integer j belonging to Z any j belonging to Z, say x is n plus epsilon where epsilon is as before then floor of x plus j would be the floor of n plus j plus epsilon, n is an integer j is also an integer so n plus j is an integer, so this would be n plus j. Floor of x is n so the right hand side is n plus j which is the same as the left hand side.

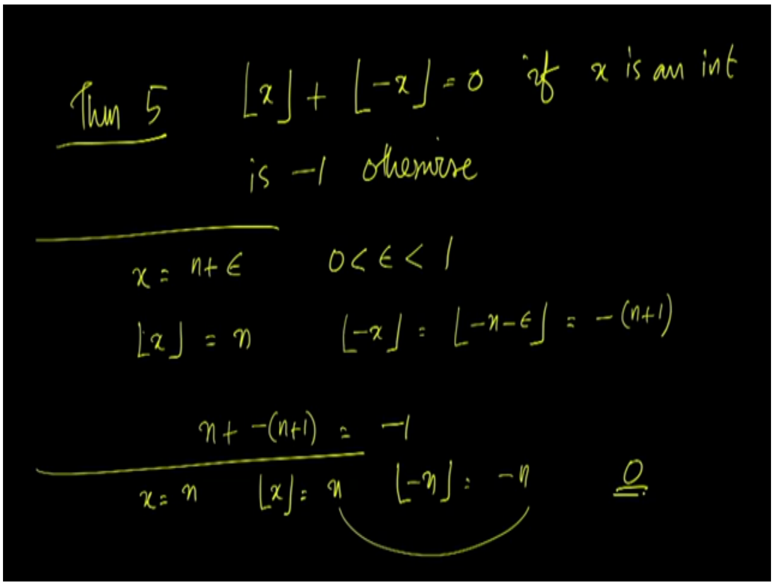
(Refer Slide Time: 39:30)



The next theorem says that floor of x plus floor of y is less than or equal to floor of x plus y, which is less than or equal to floor of x plus floor of y plus 1. Let us ay x is n plus epsilon and y is m plus delta where 0 less than or equal to epsilon and delta which are less than 1. Then n plus m this is what floor of x plus floor of y is this is less than or equal to floor of x plus y which is n plus m plus epsilon plus delta.

So depending on epsilon and delta this is either n plus m or n plus m plus 1, so indeed the first inequality holds n plus m is less than or equal to this and this is less than or equal to n plus m plus 1 which is what floor of x plus floor of y plus 1 is therefore the second inequality 2.

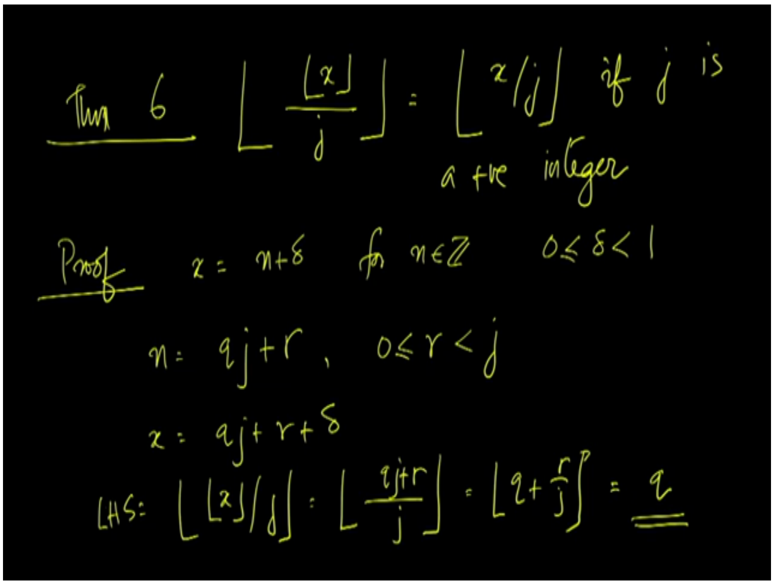
(Refer Slide Time: 40:53)



Floor of x plus floor of minus x equal to 0 if x is an integer is minus 1 otherwise, so let us consider a non-integer first, suppose x is n plus epsilon where epsilon is neither 0 nor 1. It is strictly between 0 and 1 in which case floor of x is n floor of minus x is floor of minus n minus epsilon, so we are looking at the integer which is smaller than this but as the greatest there will be minus of n plus 1.

Therefore, when you take the sum you have n plus minus of n plus 1 which is minus 1, now if x is an integer floor of x is the same as n minus of x is minus n the floor of minus n is minus n therefore the sum would be 0 as a theorem claims.

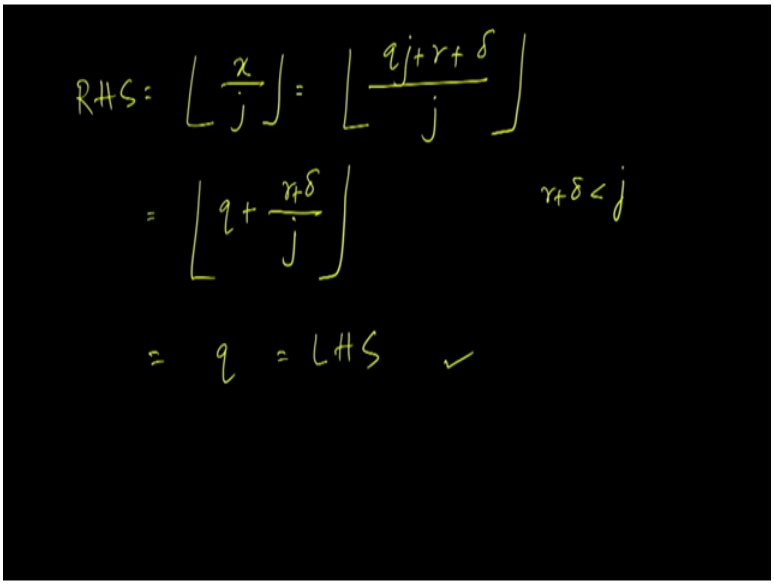
(Refer Slide Time: 42:21)



The floor of floor of x by j is floor of x by j if j is a positive integer, to prove this let us assume that x is n plus delta for an integer n and 0 less than or equal to delta less than 1, suppose n is qj plus r for any n and any j we can write n as qj plus r where r is greater than or equal to 0 but less than j.

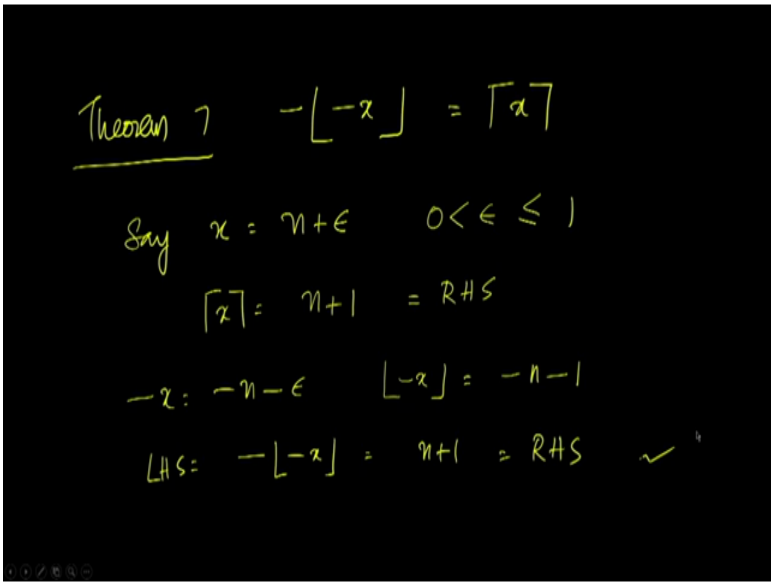
Then x is qj plus r plus delta now let us consider the left hand side the ceiling the floor of x is qj plus r so we have the floor of qj plus r by j which is the floor of q plus r by j, since r is less than j this fraction r by j is strictly less than 1, therefore this would be q, so the left hand side is q.

(Refer Slide Time: 43:50)



Now the right hand side is floor of x by j which is floor of qj plus r plus delta divided by j which is q plus r plus delta by j floor but r plus delta is less than j, r is less than j so r can be at most j minus 1 and delta is strictly less than 1, so r plus delta is less than j therefore the fraction r plus delta by j is less than 1 so this would be q, which is same as the left hand side. So theorem is then proved.

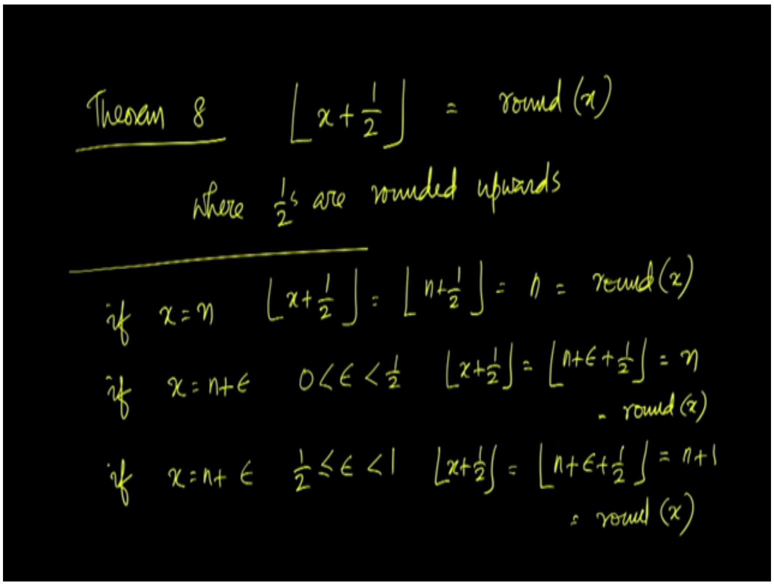
(Refer Slide Time: 44:37)



The seventh result would be this, the negative of the floor of minus x is same as ceiling affects say x is n plus epsilon for 0 less than epsilon less than or equal to 1, note here I have taken epsilon as strictly greater than 0 where n is an integer. Then ceiling of x is n plus 1 this is what right hand side is.

Minus of x is minus n minus epsilon, the floor of minus x therefore is minus n minus 1 then negative of that this is what the left hand side is that will be n plus 1 this is the right hand side, hence the result holds.

(Refer Slide Time: 45:40)

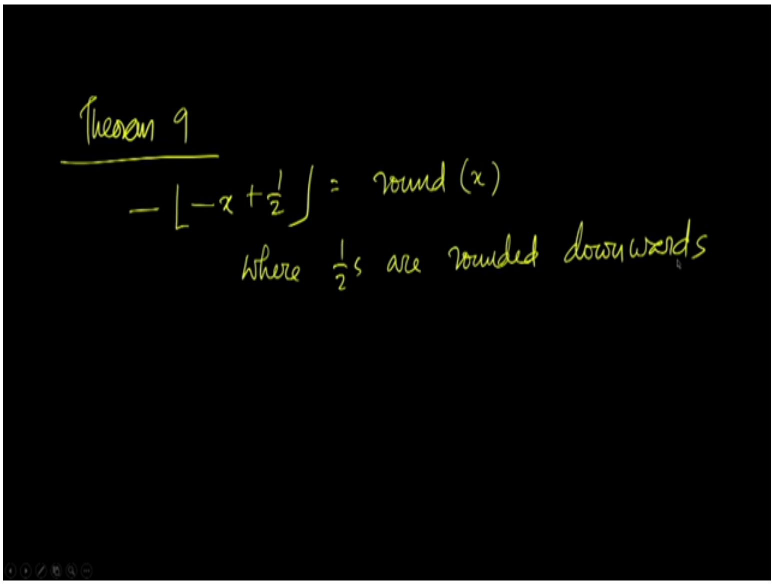


The floor of x plus half is round of x where halves are rounded upwards, for example round of 7.5 is 8 because a half is rounded upwards to prove this first consider x is equal to n there is no fractional part then floor of x plus half is the floor of n plus half which is n but this is the same as round of x.

Since x is an integer round of x is the same as round of n if x is n plus epsilon where epsilon is greater than 0 but less than half then floor of x plus half is the floor of n plus epsilon plus half which is n. epsilon is less than half so epsilon plus half together will not make up one so the floor here is 1, floor here is n.

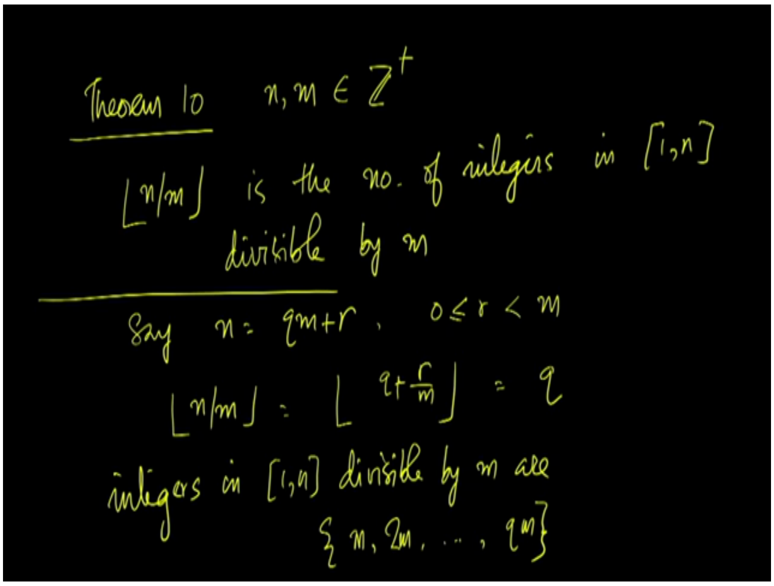
Which is the same as round of x, since epsilon is not large enough the round function will not round upwards if x is n plus epsilon for epsilon there is greater than or equal to half but less than 1 floor of x plus half would be floor of n plus epsilon plus half which is n plus 1 which is the same as round of x, so in this case epsilon could be half in which case x would be rounded upwards.

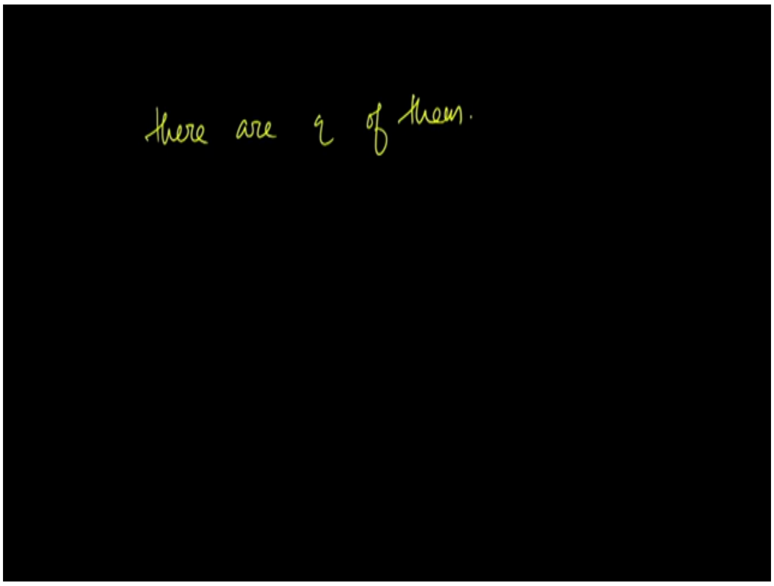
(Refer Slide Time: 47:58)



Analogously, negative of the floor of negative x plus half is round of x where halves are rounded downwards, the prove is a develop a previous one so I leave it as an exercise.

(Refer Slide Time: 48:21)

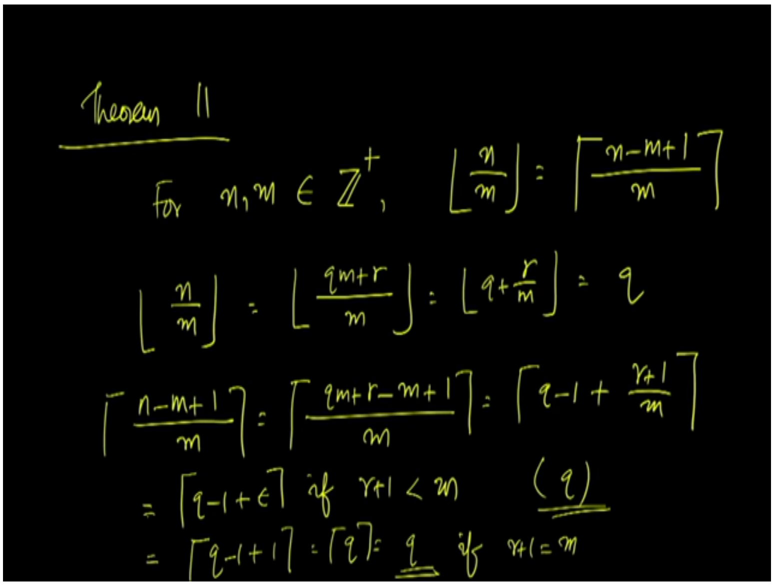




Another result about ceiling and floor is this for n and m belonging to Z plus set of positive integers floor of n by m is the number of integers in the range 1 to n divisible by m, say n is qm plus r for any 2 positive integers n and m we can write n as qm plus r for r that is greater than or equal to 0 but less than m.

Then, floor of n by m is the floor of q plus r by m which is q because r by m is less than 1, so integers n 1 to n divisible by m are will formed the set m, 2m, 3m, etc upto qm, n is qm plus r therefore n is greater than or equal to qm. So there are q of them hence the theorem.

(Refer Slide Time: 50:00)



For n, m which are in Z plus floor of n by m is the same as the ceiling of n minus m plus 1 divided by m, so again assume that n can be expressed as qm plus r as before so floor of n by m is the floor of q m plus r by m which is floor of q plus r by m which is q as we have seen before.

Then the ceiling of n minus m plus 1 by m would be the ceiling of qm plus r minus plus 1 divided by m, which is the ceiling of q minus 1 plus r plus 1 by m, this is q minus 1 plus a fraction epsilon r plus 1 by m is less than 1 when r plus 1 is less than m and therefore this quantity will be q, this would be ceiling of q minus 1 plus 1 which is a ceiling of q which is again q if r plus 1 equal to m.

Since our range is from 0 to r minus 1 both inclusive r plus 1 is either less than 1 or is equal to m either less than m or is equal to m so this are the only 2 possibilities in both the cases we find that the right hand side evaluates to q hence the theorem. So that is it from the this lecture this is the last lecture of the module and number theory hope to see you in the other modules thank you.