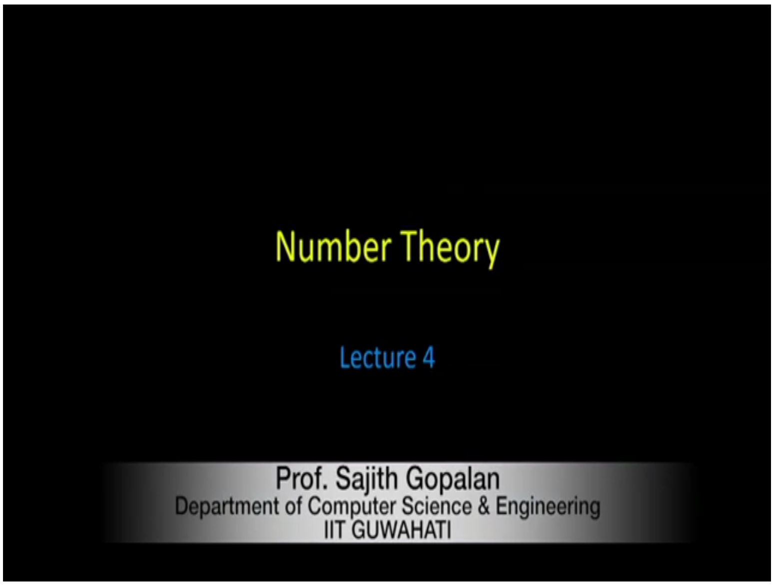
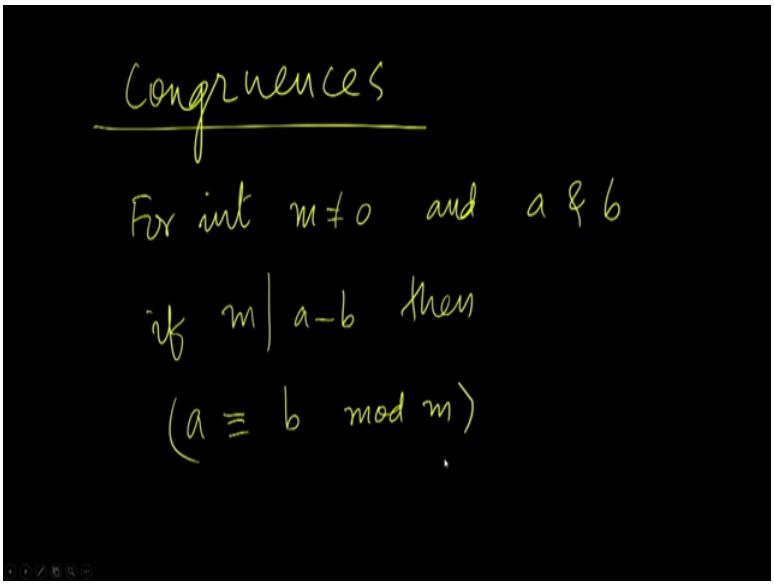
Discrete Mathematics
Professor Sajith Gopalan
Professor Benny George
Department of Computer Science and Engineering
Indian Institute of Technology, Guwahati
Lecture 4 - Number Theory

(Refer Slide Time: 00:34)



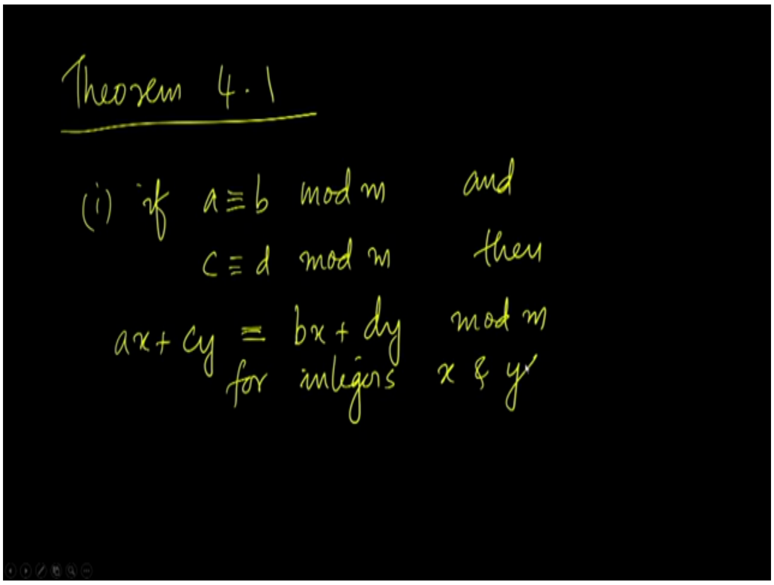
Welcome to the NPTL MOOC on Discrete Mathematics. This is the fourth lecture on Number Theory.

(Refer Slide Time: 00:40)



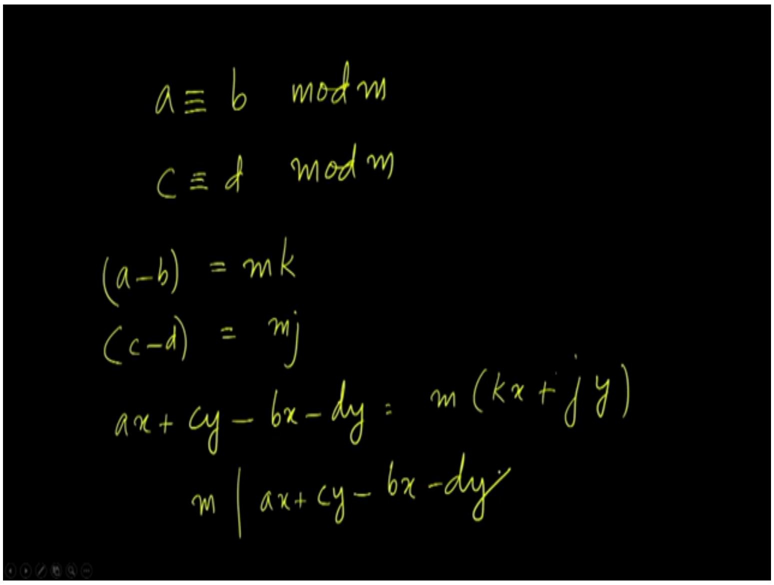
In the last class, we were discussing congruences. We say that, for integer m not equal to zero and integers a and b if m divides a minus b, then we say that a is congruent to b mod m. We were looking at some properties of congruences. So, we will see some more properties.

(Refer Slide Time: 01:18)



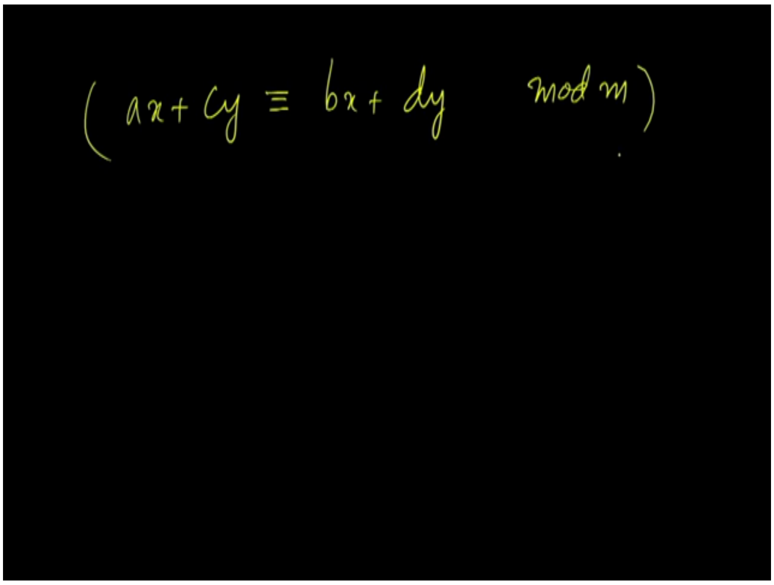
One property is that, if a is congruent to b mod m and c is congruent to d mod m, then ax plus cy is congruent to bx plus dy mod m for integers x and y.

(Refer Slide Time: 02:10)



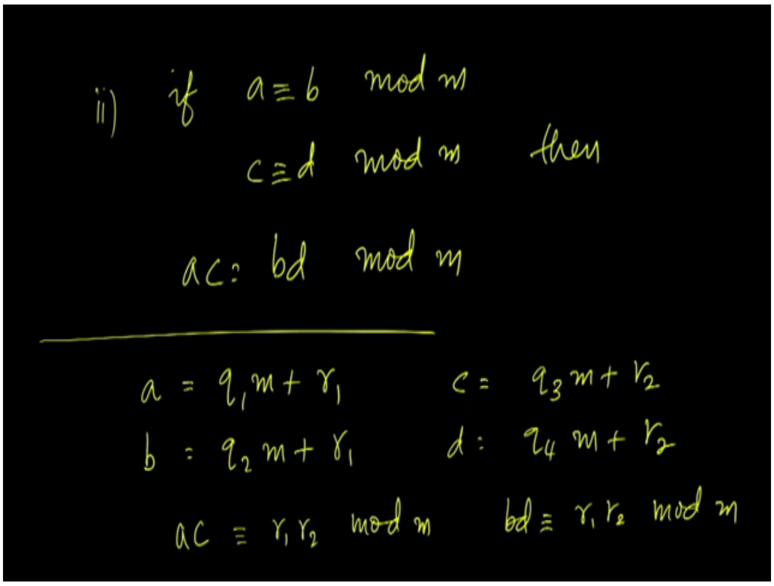
So to prove this, we start with our assumptions: a is congruent to b mod m and c is congruent to d mod m which means a minus b is mk for some integer k and c minus d is mj for some integer j. Therefore, ax plus cy minus bx minus dy would be m into kx plus jy. kx plus jy is an integer, therefore m divides ax plus cy minus bx minus dy.

(Refer Slide Time: 03:09)



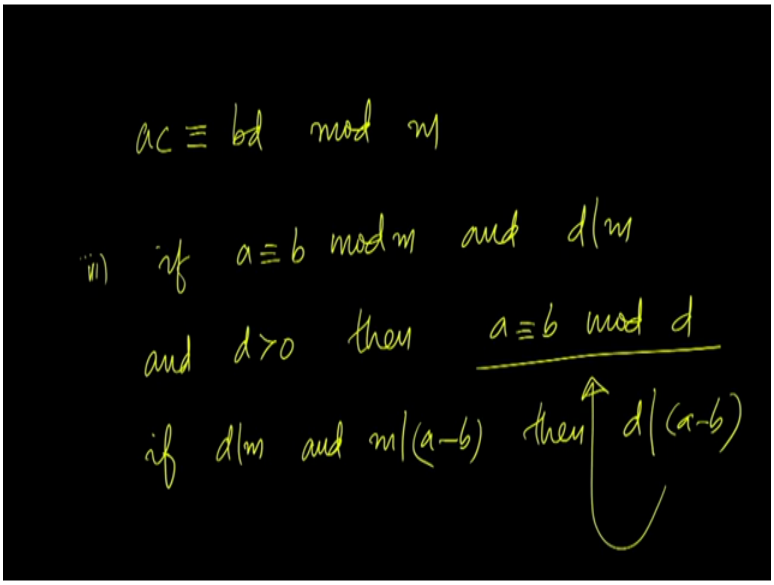
Or in other words ax plus cy is bx plus dy mod m, which is precisely what we seek to prove.

(Refer Slide Time: 03:21)



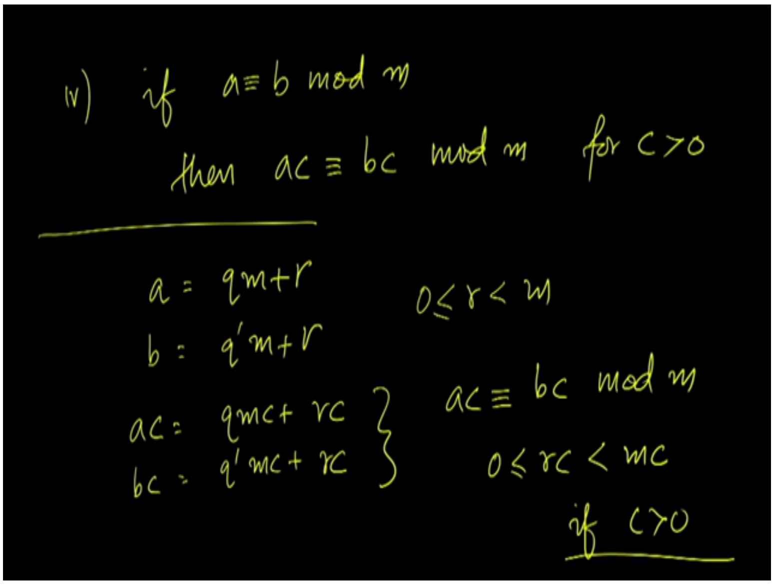
Another result is that, if a equal to b mod m and c equal to d mod m then ac equal to bd mod m. If a equal to b mod m then, let us say a is q1 m plus r 1, r 1 is the remainder. In that case b will also produce the same remainder, b would be some q 2 m plus r 1. Let us say c is q 3 m plus r 2 and d is q 4 m plus again r 2. That is because c and d are congruent mod m; both of them will produce the same remainder. Therefore, if you take ac, you find that ac would be r 1 r 2 mod m. Similarly, bd is also r 1 r 2 mod m. Every other term of the product would be a multiple of m.

(Refer Slide Time: 04:53)



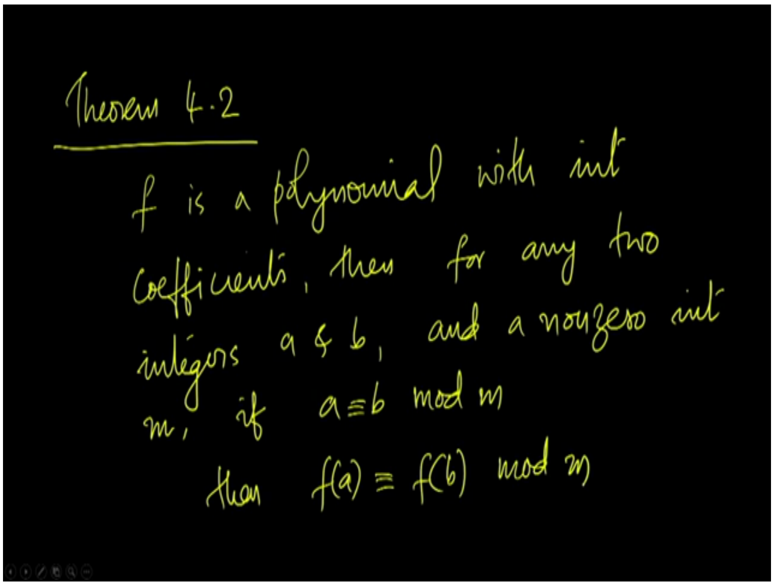
Therefore, ac is congruent to bd mod m as is required. The third statement is that if a is b mod m and d divides m and d greater than 0 then a equal to b mod d. If d divides m and m divides a minus b which would be the case if a is congruent to b mod m then by transitivity of divisibility d divides a minus b which means a is congruent to b mod d as is required.

(Refer Slide Time: 05:55)



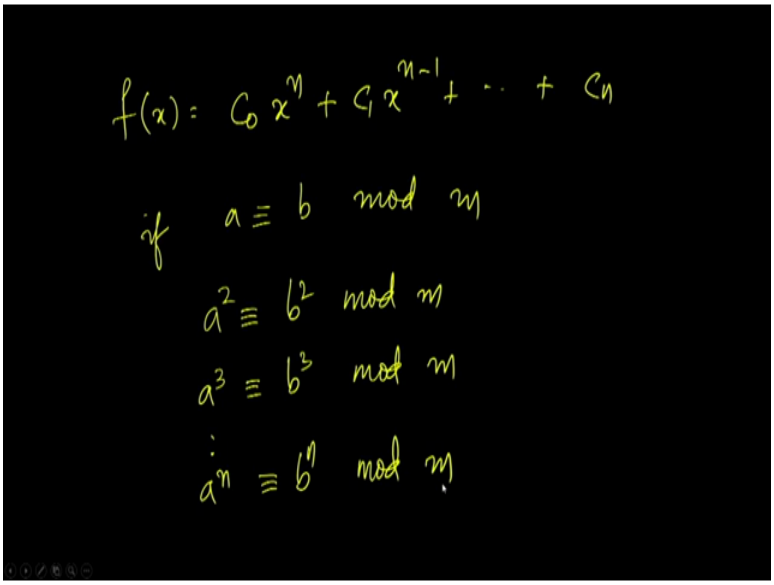
If a is congruent to b mod m, then ac is congruent to bc mod m for any c greater than 0. So, say a is qm plus r and b is q prime m plus r. The two produce the same remainder, that is why they are congruent to each other mod m. So here 0 less than or equal to r less than m. Then ac is qmc plus rc and bc is q prime mc plus rc, which means ac is congruent to bc mod m. Both of them produce the same remainder rc. We have that 0 less than or equal to rc less than mc if c greater than 0. So, if c greater than 0, we do have the result that we want.

(Refer Slide Time: 07:32)



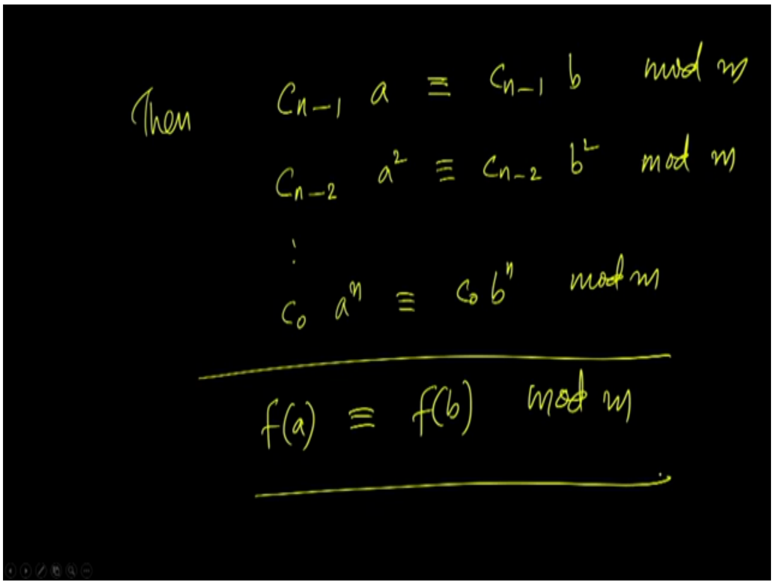
The next theorem says this, if f is the polynomial with integer coefficients, then for any two integers a and b and the non-zero integer m, if a is congruent to b mod m, then f of a is congruent to f of b mod m. This follows from the previous theorems.

(Refer Slide Time: 08:44)



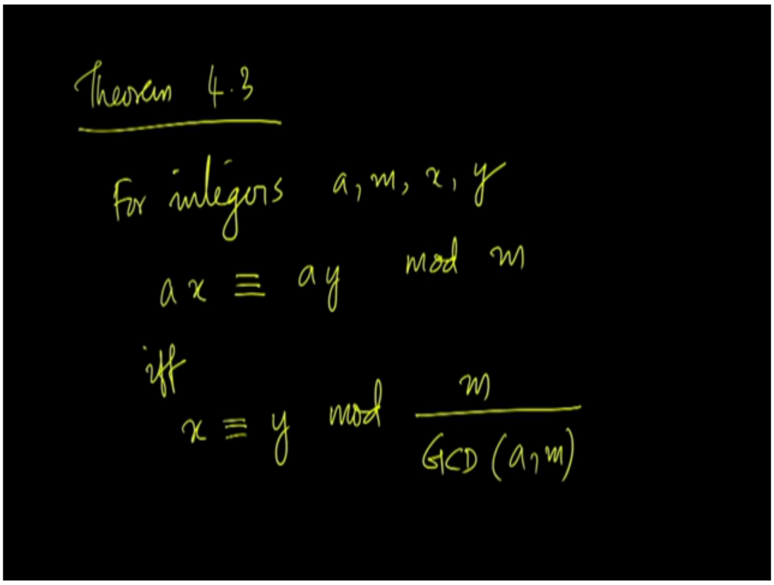
Let us say f of x is C 0 x power n plus C 1 x power n minus 1 so on up to C n. C 0, C 1, C 2 et cetera are all integers. If a congruent to b mod m, then from the previous theorem we know that a square is congruent to b square mod m, a cube is congruent to b cube mod m and so on. a power n congruent to b power n mod m.

(Refer Slide Time: 09:33)



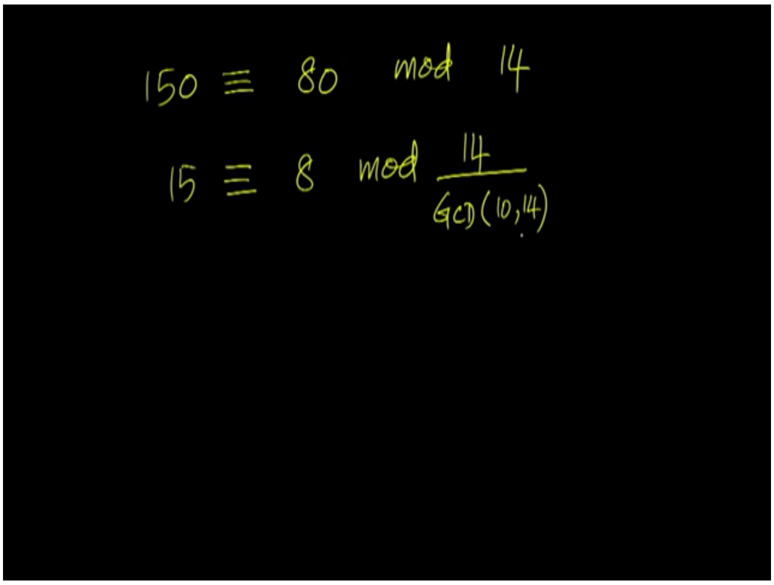
Then C power n minus 1 a is congruent to C power n minus 1 b mod m. Since C n minus 1 is constant, C n minus 1 a is congruent to C n minus 1 b. C n minus 2 a square is congruent to C n minus 2 b square, since C n minus 2 is an integer and so on. Therefore, adding all of them together, we have f of a is congruent to f of b mod m, the desired result.

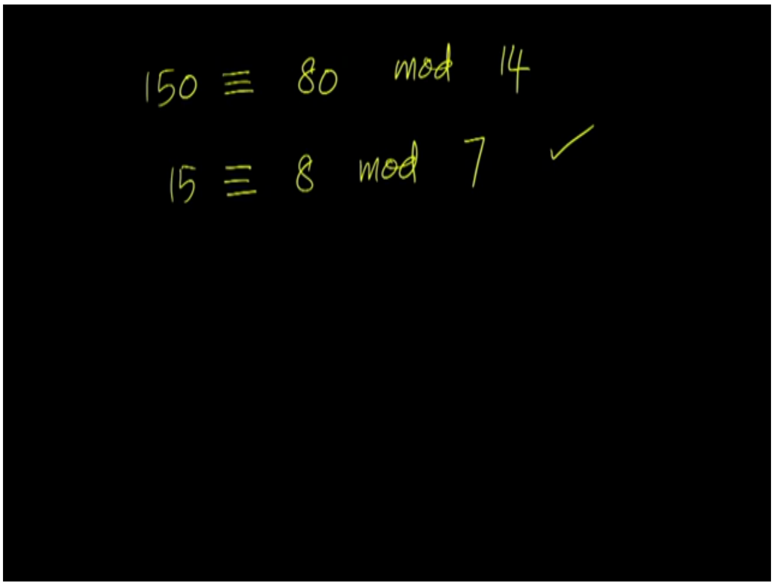
(Refer Slide Time: 10:31)



For integers a, m, x, and y, ax is congruent to ay mod m if and only if x is congruent y mod m, y mod m divided by GCD of a, m. That is if you choose to cancel a from either side of a congruence then m will have to be divided by the GCD of a and m.

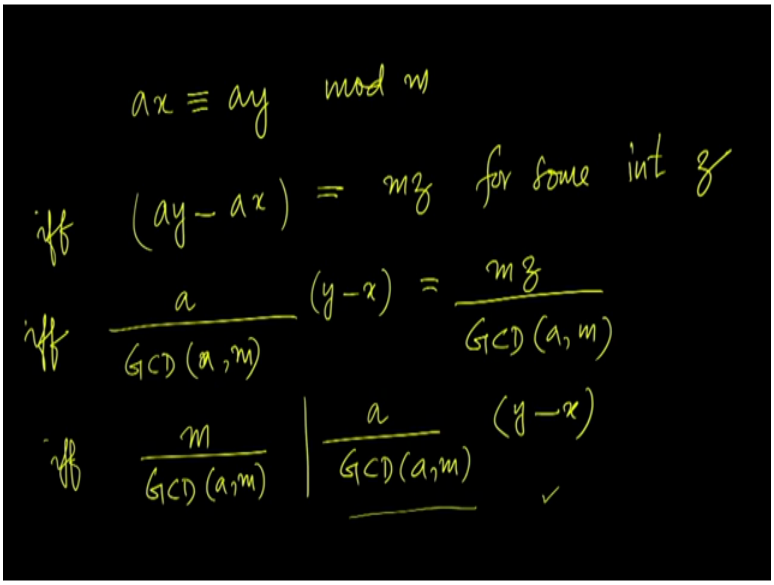
(Refer Slide Time: 11:26)





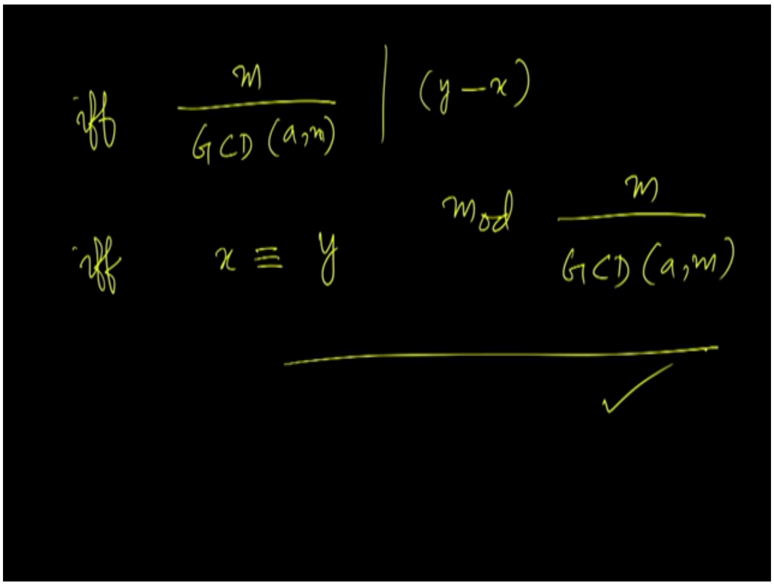
For example, 150 is congruent to 80 mod 14. So, if you divide both sides by 10, we have 15 congruent to 8 but then 14 will have to be replaced by GCD of 10 and 14. The number with that we are seeking to cancel, but GCD of 10 and 14 is 2, therefore we will have to replace this with 7 which is indeed the case.

(Refer Slide Time: 12:18)



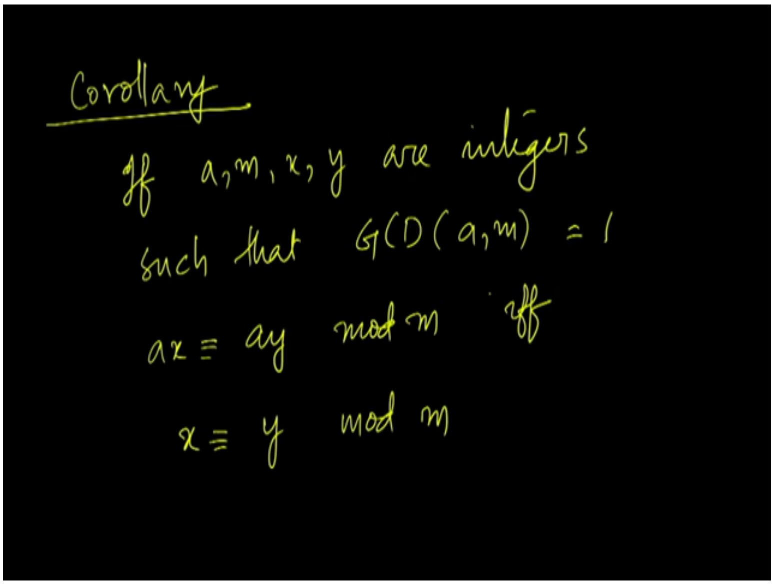
So, how do we prove the theorem? Let us say, ax is congruent to ay mod m but this is if and only if ay minus ax is m into z for some integer z, then both sides of equation can be divided with GCD of a, m, but then this is if and only if m divided by GCD of a, m divides the left hand side which is a divides GCD of a, m multiplied by y minus x. Now, m pi GCD of a, m and a by GCD of a, m are relatively prime the GCD being 1. Therefore, since m does not divide the first factor here it should divide the second factor.

(Refer Slide Time: 13:58)



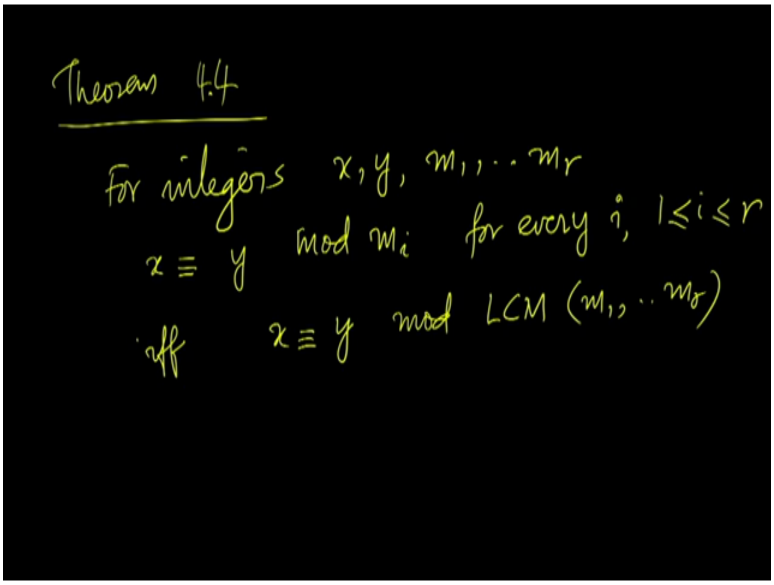
Therefore, this is if and only if m divided by GCD of a, m divides y minus x but this is precisely the condition for x being congruent to y mod m divided by GCD of a, m as is required in the theorem. Hence the theorem.

(Refer Slide Time: 14:34)



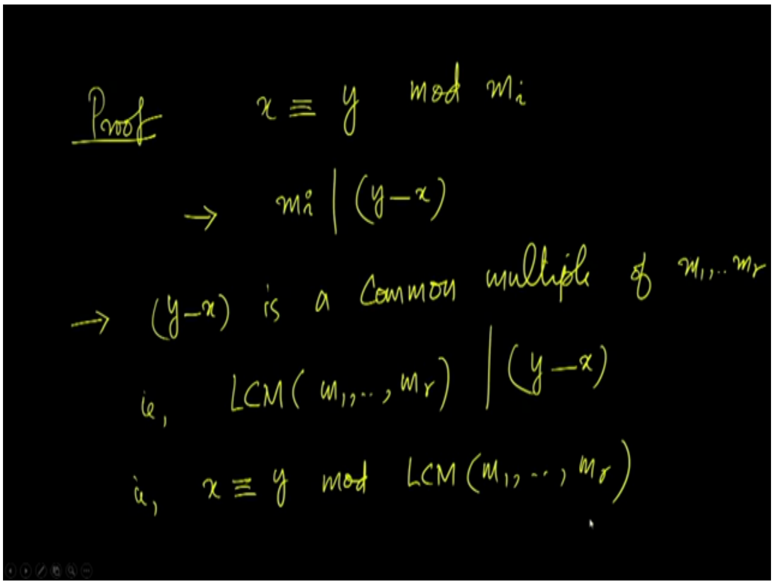
As a corollary we find that, if a, m, x, y are integers such that GCD of a, m is 1. a and m are relatively prime, then ax is congruent to ay mod m if and only if x is congruent y mod m. So, this is when a can be cancelled from each side of the congruence without affecting the modulus. The cancelled number should be relatively prime to the modulus.

(Refer Slide Time: 15:32)



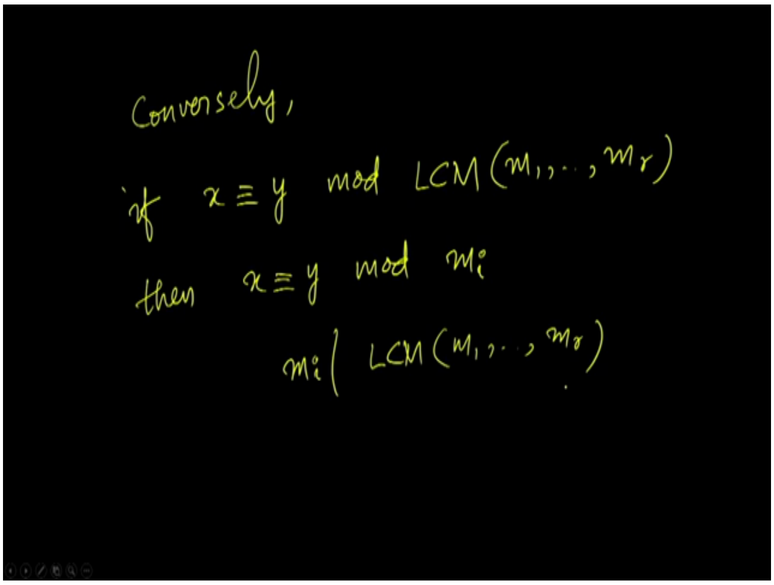
The next theorem says that, for integers x, y, m 1 through m r if x is congruent y mod m i for every i from 1 to are, this is if and only if x is congruent y mod LCM of m 1 through m r. m1 through m r are integers, x is congruent y modulus each of them then x is congruent y modulo the LCM of these numbers.

(Refer Slide Time: 16:49)



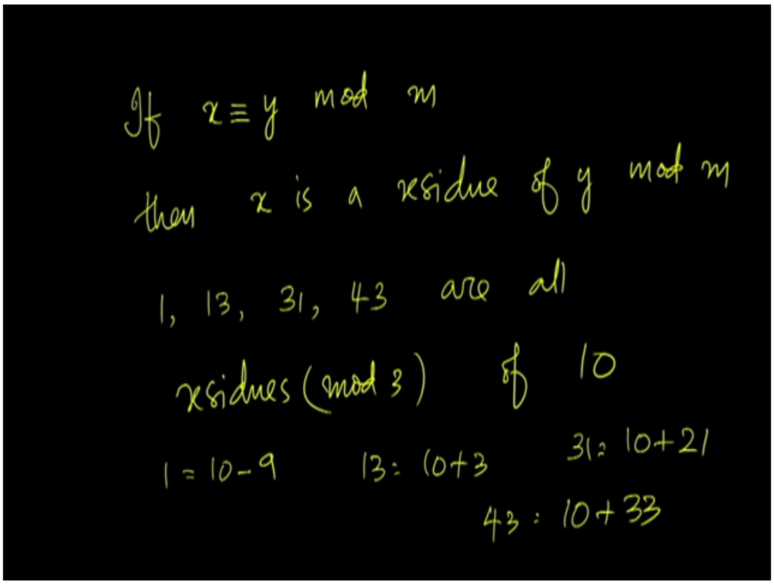
To prove this, we know that x is congruent y modulo m i for each m i, then m i divides y minus x for each i, that means y minus x is a common multiple of m 1 through m r. That is LCM of m 1 through m r which then must divide every common multiple of m 1 through m r divides y minus x, that is x is congruent y mod LCM of m 1 through m r as is required.

(Refer Slide Time: 18:05)



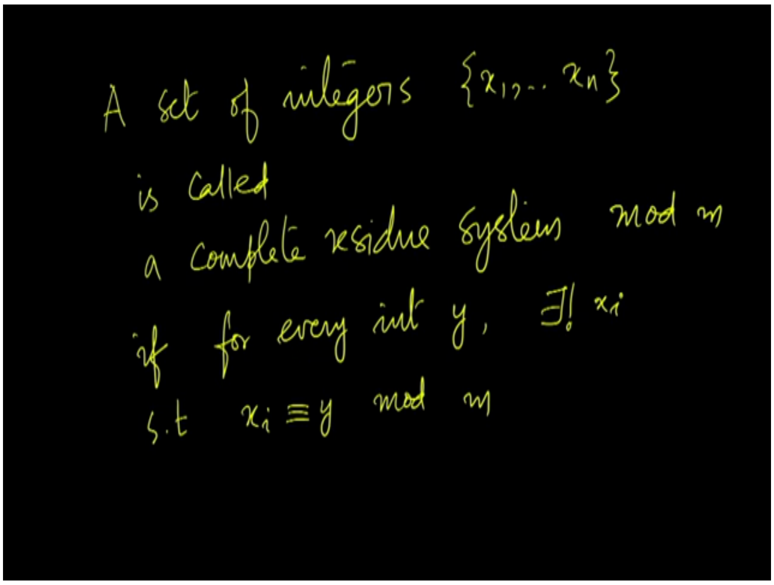
Conversely, if x is congruent y mod the LCM, then x is congruent y mod m i that is because m i divides the LCM. Hence the theorem.

(Refer Slide Time: 18:45)



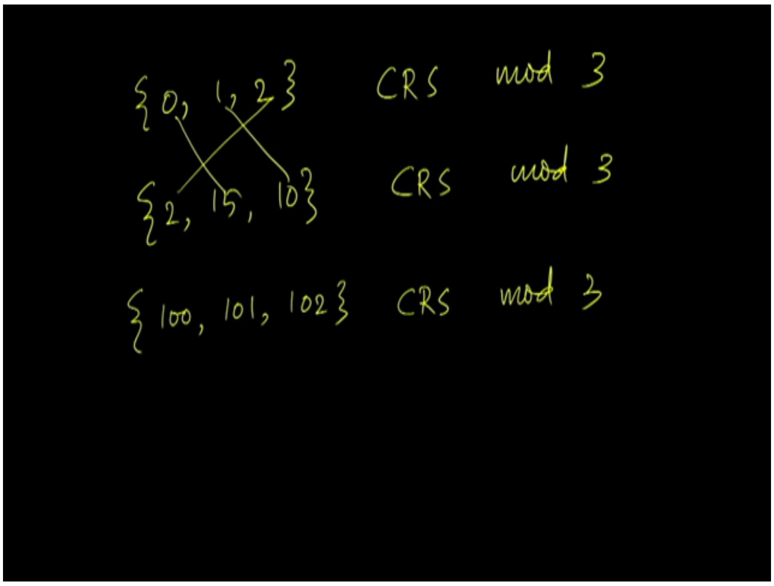
If x is congruent y modulo m, then we say x is residue of y modulo m. For example, 1, 13, 31, 43 are all residues modulo 3 of 10. That is because 1 is 10 minus 9 a multiple of 3, 13 is 10 plus 3 a multiple of 3, 31 is 10 plus a multiple of 3 namely 21, 43 is 10 plus 33 again a multiple of 3. So, these are all residues mod 3 of 10.

(Refer Slide Time: 19:53)



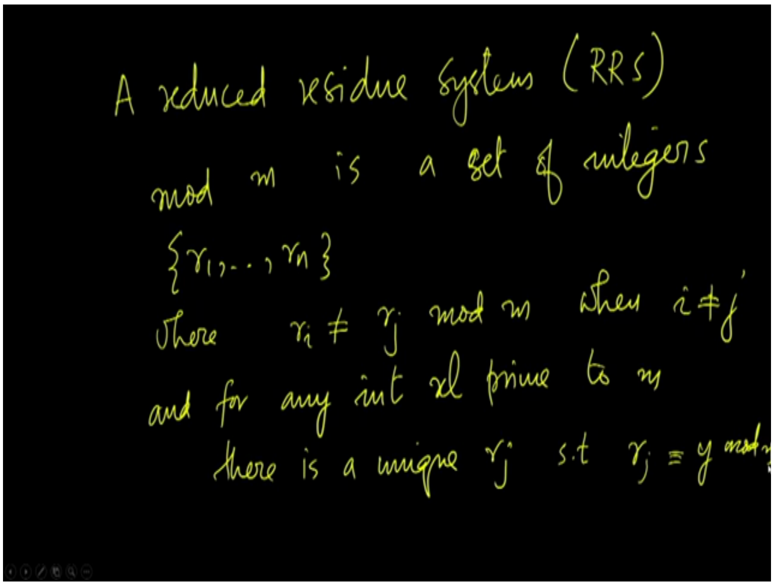
A set of integers is called a complete residue system modulo m if for every integer y there is a unique x i, so that x i is congruent to y modulo m. So, here the set of integers considered as x 1 through x n. So, a set of integers x 1 through x n is called a complete residue system modulo m if our every integer y, there is unique x i in the set such that x i is y mod m. So, for every single integer you will find the residue within the system. In that case it is called a complete residue system.

(Refer Slide Time: 21:07)



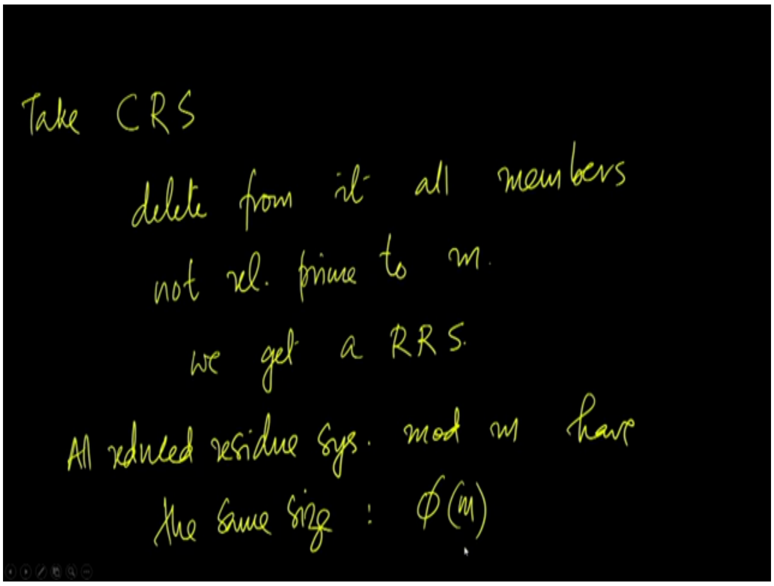
0, 1, 2 it is a complete residue system modulo 3. Take any integer that will be one of these three modulo 3. Equivalently, 2, 15, 10 is also a complete residue system mod 3. The mapping goes like this: 2 is 2 mod 3, 15 is 0 mod 3, 10 is 1 mod 3. So, we essentially have the same integers modulo 3. Similarly, 100, 101 and 102, 102 is 0 mod 3, 101 is 2 mod 3 and 100 is 1 mod 3. Therefore, this is also a complete residue system mod 3.

(Refer Slide Time: 22:22)



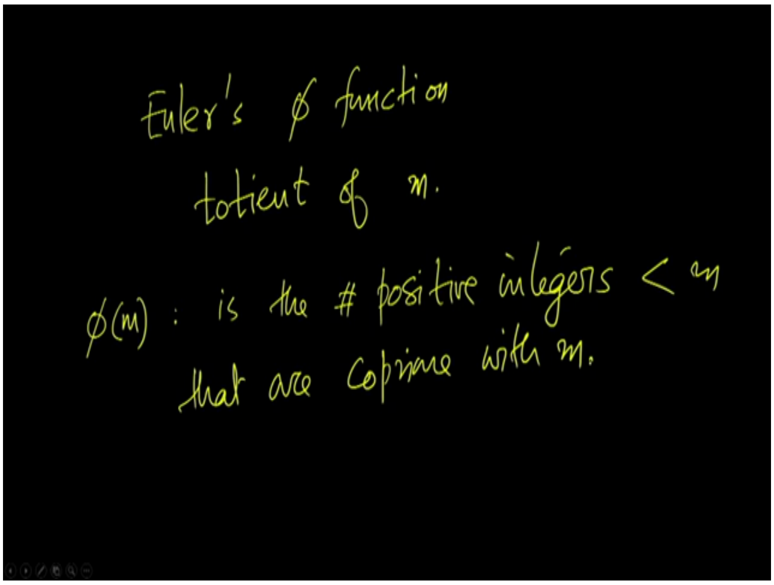
A reduced residue system it is called RRS. Modulo m is a set of integers r 1 through r n where r i is not equal to r j mod m when i is not equal to j. That is no two members are congruent mod m and for any integer relatively prime to m there is a unique r j so that r j is y mod m.

(Refer Slide Time: 23:53)



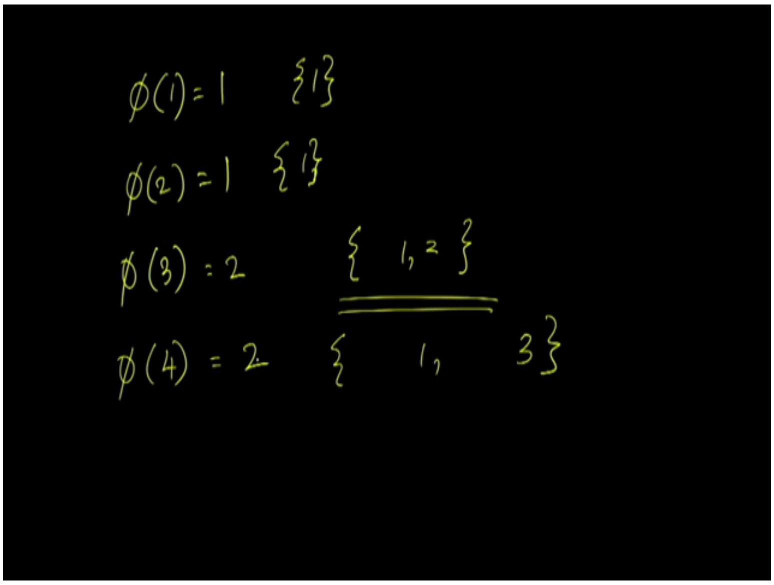
If you take the CRS that is the complete residue system, delete from it all members not relatively prime to m, we get reduced residue system. All reduced residue systems mod m have the same size. This is denoted as phi of m.

(Refer Slide Time: 24: 55)



This is called Euler's phi function or totient of m. In other words, phi of m is the number of positive integers less than m that are coprime with m.

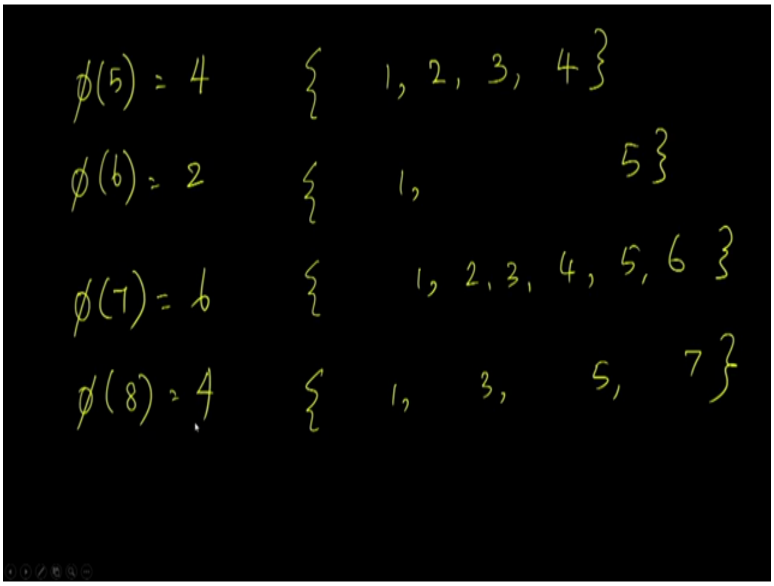
(Refer Slide Time: 25:43)



Let us consider reduced residue systems for various values. To find phi 1, the singleton 1 is the reduced residue system for 1 therefore phi 1 equal 1. The reduced residue system modulo 2 is again the singleton 1. Phi of 1 is defined as 1 by default and phi of 3 there is residue system would be obtained from 0, 1 and 2 and then the numbers which are relatively prime with 3 are deleted. So what remain are 1 and 2. Therefore, phi of 3 is 2. The reduced residue system would consist of this 1 and 2.

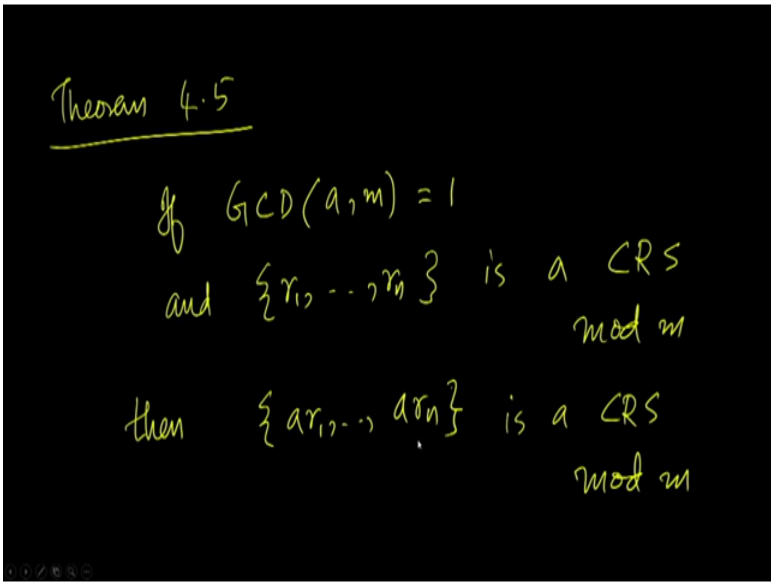
To find phi of 4, we consider the complete residue system which would contain 0, 1, 2 and 3. Of these 0 and 2 are not relatively prime with 4, therefore they are deleted, what remained are 1 and 3. Therefore phi of 4 is 2.

(Refer Slide Time: 27:21)



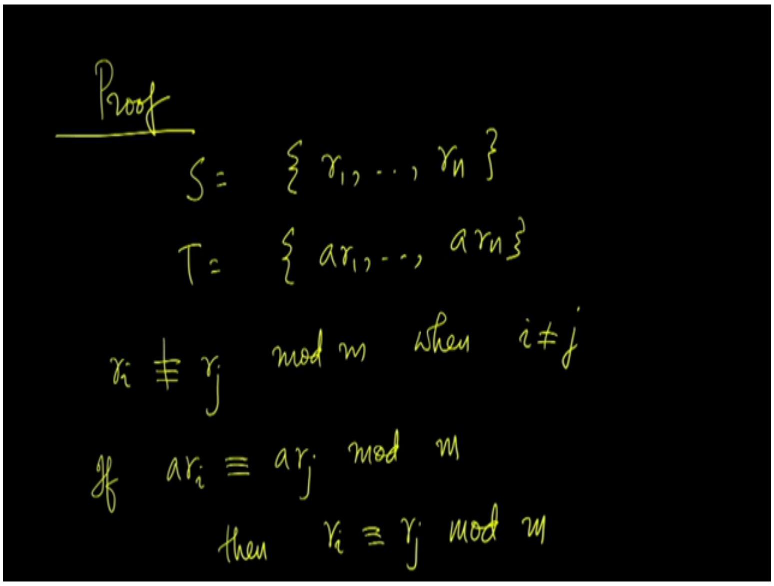
Coming to 5, we consider the complete residue system 0, 1, 2, 3 and 4, of this 0 is not relatively prime with 5 so that is removed. Therefore phi of 5 is 4. For 6, we considered all integers less than 6, delete all numbers which are not relatively prime with 6, what remain are 1 and 5, so phi of 6 is 2. When we come to 7, we have 6 remaining, 7 is relatively prime with all of these, therefore phi of 7 is 6. Coming to 8, we have, we find that every even number is not relatively prime with 8. So, deleting them, we have 4 elements remaining, so phi of 8 is 4.

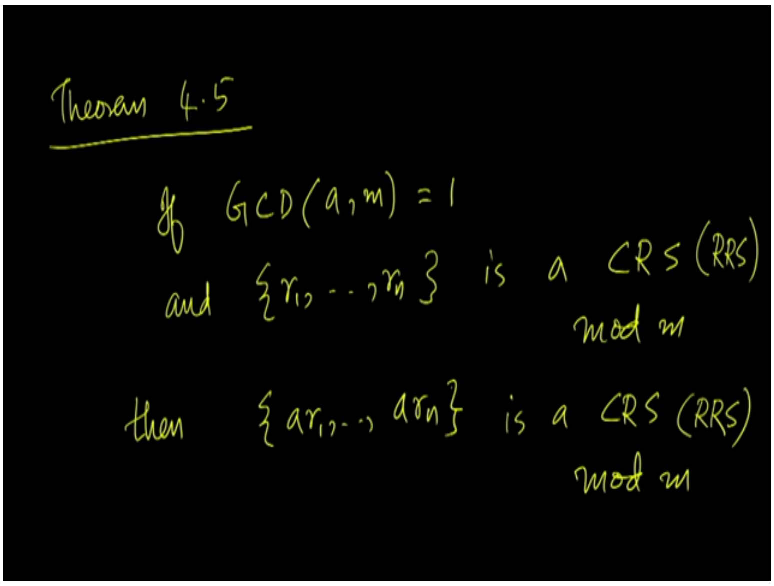
(Refer Slide Time: 28:53)



If GCD of a, m is 1 and r 1 through r n is a complete residue system, modulo m then a r 1 through a r n is a complete residue system mod m as well. This is the case when GCD of a, m is 1. That is a and m are relatively prime.

(Refer Slide Time: 29:52)

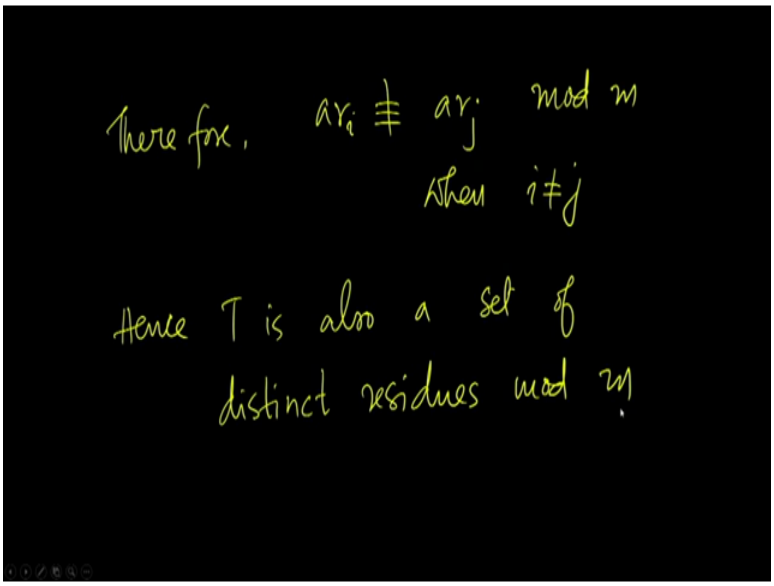




To prove this, suppose S is r 1 through r n then T is a r 1 through a r n. By the way this theorem will hold even if CRS is replaced with RRS. That is even if we are considering a reduced residue system r 1 through r n then a r 1 through a r n would be a reduced residue system mod m when a and m are relatively prime with each other.

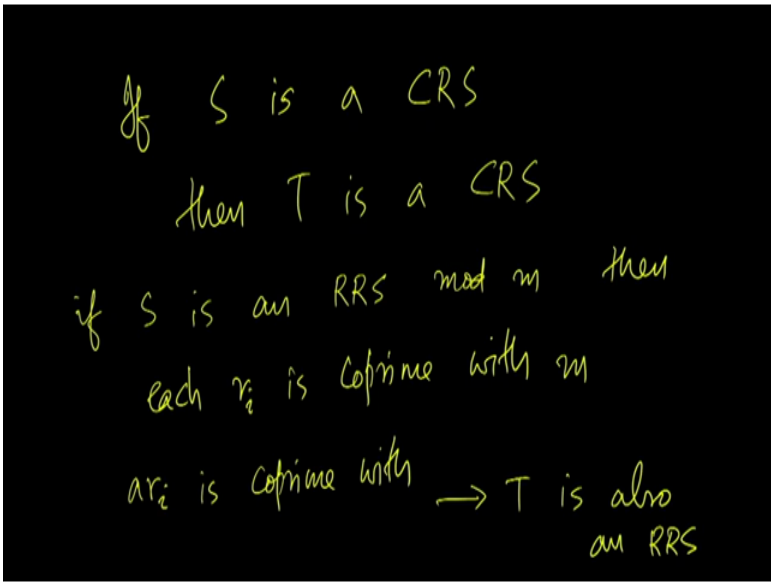
So, let S be r 1 through r n and T be a r 1 through a r n, if S is either a CRS or an RRS modulo m, we have that r i is not congruent to r j mod m when i not equal to j. If a r i is congruent to a r j mod m, assume there is one such pair within T, one such pair i j so that a r i is congruent to a r j even when i not equal to j. Then since GCD of a and m is 1, we can cancel a from both sides and we would have r i congruent to r j mod m. Since GCD of a and m is 1, the modulus does not change.

(Refer Slide Time: 31:49)



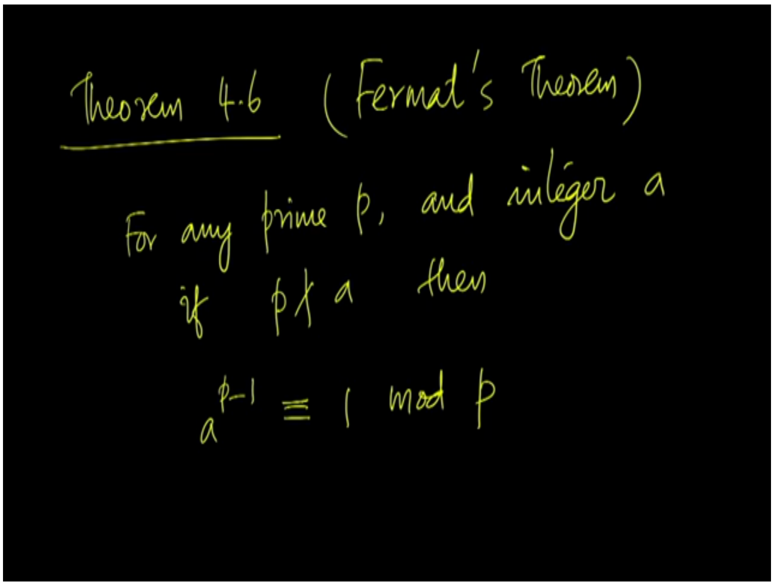
It is the contradiction therefore, a r i is not congruent to a r j mod m, when i not equal to j. Hence, T is also a set of distinct residues, exactly the way S is.

(Refer Slide Time: 32:32)



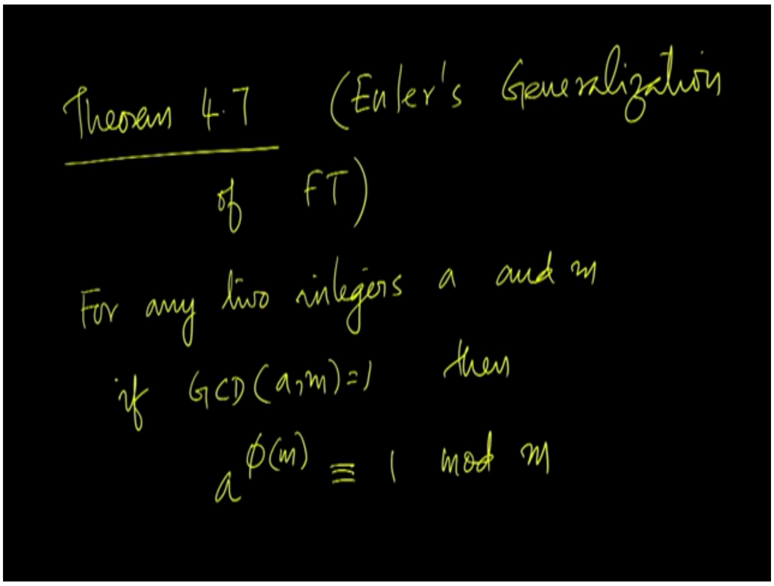
If S is a CRS, then T is a CRS as well. S has a size of m then T also has a size of m. On the other hand, if S is an RRS modulo m then each r i is coprime with m. We obtain an RRS by taking a CRS and cancelling out every r i which is not coprime with m. So, whatever that remains would be coprime with m. So, if S is an RRS then each r i is coprime with m. Therefore a r i is coprime with m. That is because a is coprime with m and now r i is also coprime with m, so a r i is coprime with m. Therefore, T is also an RRS, hence the theorem.

(Refer Slide Time: 33:55)



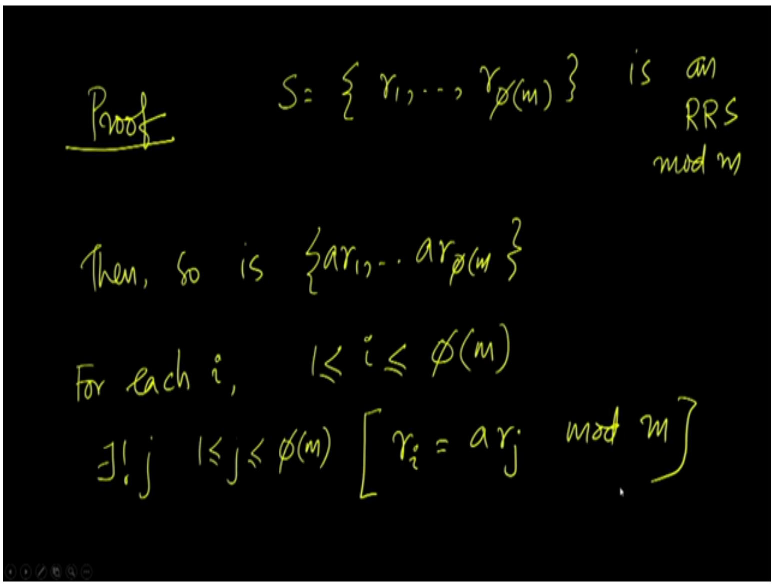
The next theorem is famous as Fermat's Theorem, which says that for any prime p and integer a, if p does not divide a then a power p minus 1 is congruent to 1 modulo p. For any prime p and an integer a, if p does not divide a then a power p minus 1 is congruent to 1 modulo p.

(Refer Slide Time: 34:44)



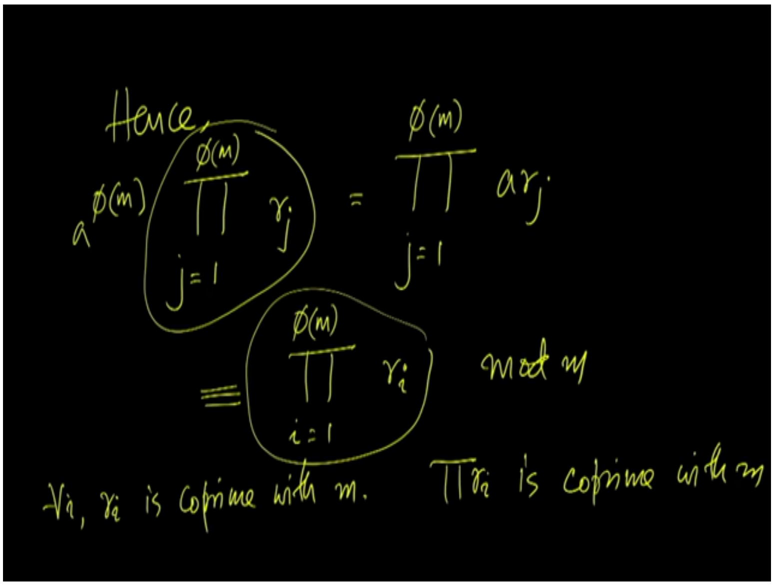
We will prove a generalization of this, which is called Euler's Generalization of Fermat's Theorem. Fermat lived in the sixteenth century, Euler lived almost a century later, so Euler had a generalization of Fermat's theorem. Euler's generalization states this: For any two integers a and m, that are relatively prime with each other, so their GCD is 1, then a power phi m is 1 mod m. So, phi m is the size of the reduced residue system modulo m.

(Refer Slide Time: 36:01)



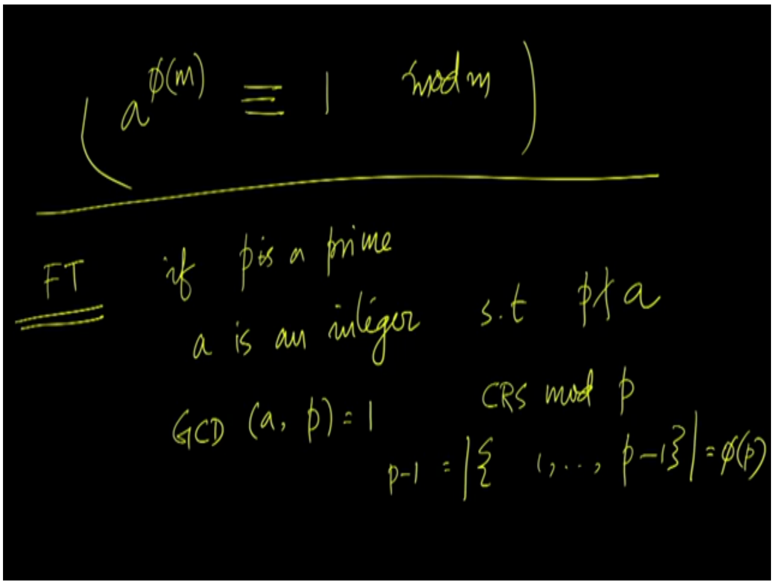
So, we prove it this way, suppose S which is denoted as r 1 through r phi m is an RRS, reduced residue system modulo m. Then so is a r 1 through a r phi m as we have just seen. For each i, where i is from any integer between 1 and phi m, there is a unique j in the range 1 to phi m so that r i equals a r j mod m.

(Refer Slide Time: 37:14)



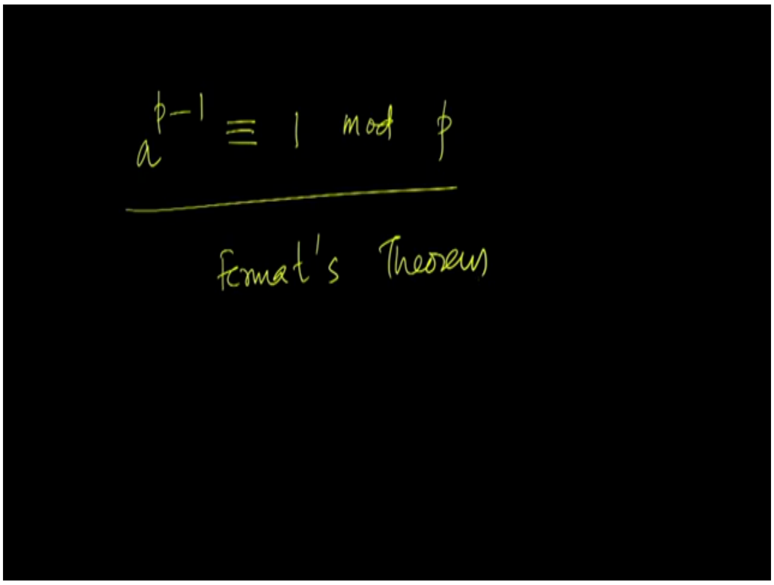
Hence, a power phi m multiplied by the product of r j for j varying from 1 to phi m, let us compute this product. Taking a power phi m inside, we can write this as the product with j varying from 1 to phi of m of a r j. But this is congruent to the product with i varying from 1 to phi m of r i. That is because for every j, there is an i so that a r j is congruent to r i mod m. So this congruence is mod m. But r i is coprime with m for every i, therefore the product of r i is also coprime with m. Now, this product appears here too. So, you can cancel this from both sides of the equation. Since the cancelling quantity is relatively prime with m, the modulus does not change when we cancel.

(Refer Slide Time: 39:14)



Therefore, what I have is this, a power phi of m is congruent to 1 mod m as the theorem claims. So, that proves the generalization of Euler's for Fermat's theorem. Now, coming to Fermat's theorem, suppose p is prime and a is an integer, such that p does not divide a. Then GCD of a, p equal to 1. So, p is prime and a is an integer so that p does not divide a, so GCD of a, p is 1. Now, consider the complete residue system modulo p. This will contain these numbers, of this 0 is not relatively prime with p, therefore what remains are these, this would then be the phi value of p. Phi of p would be the cardinality of this which is p minus 1.

(Refer Slide Time: 40:58)



Therefore, plugging this in Euler's generalization we find that, a power p minus 1 is 1 mod p. This is precisely what Fermat's theorem says. So, Fermat's theorem can be obtained as the corollary of Euler's theorem. So, that is it from this lecture, hope to see you in the next. Thank you.