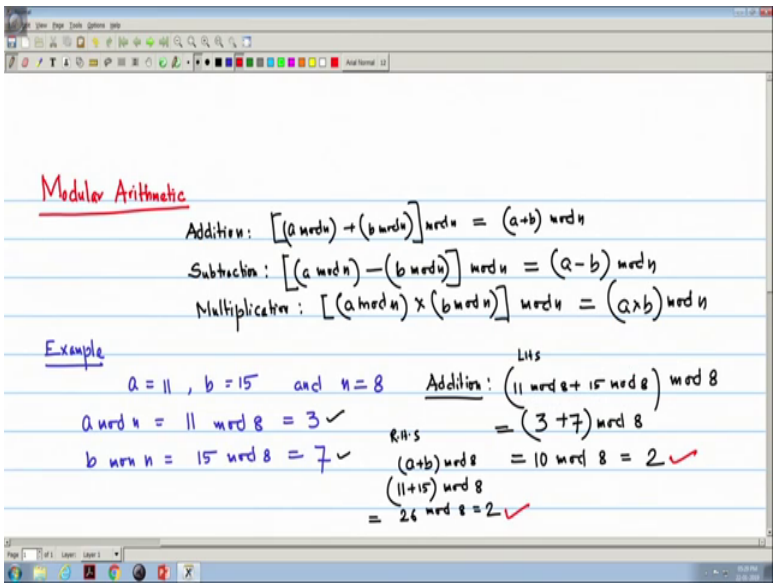
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 54
Ring and Modular Arithmetic (Contd.)

So, we are discussing the a modular arithmetic and in the last lecture, we have define that what do you mean by a modulo n and mainly that is nothing but the remainder when a is divided by n and the three basic arithmetic properties. Thus, addition, subtraction and multiplication and how actually they operates on the set 0 to n minus 1; since 0 to n minus 1 are the remainder when it is divided by n.

(Refer Slide Time: 00:57)



So, we will now continue the discussion on Modular Arithmetic because some more properties now we will read and some application areas that how that modular arithmetic, we can utilize for some computation purposes. So, if we quickly write the three basic arithmetic properties that we have read is the addition. I can write that a modulo n plus b modulo n and if I take the modulo whole this is nothing but the a plus b modulo n.

Similarly, we have given the subtraction and which is nothing but the same only instead of plus we take the minus. This is minus b modulo n a minus b modulo n and the

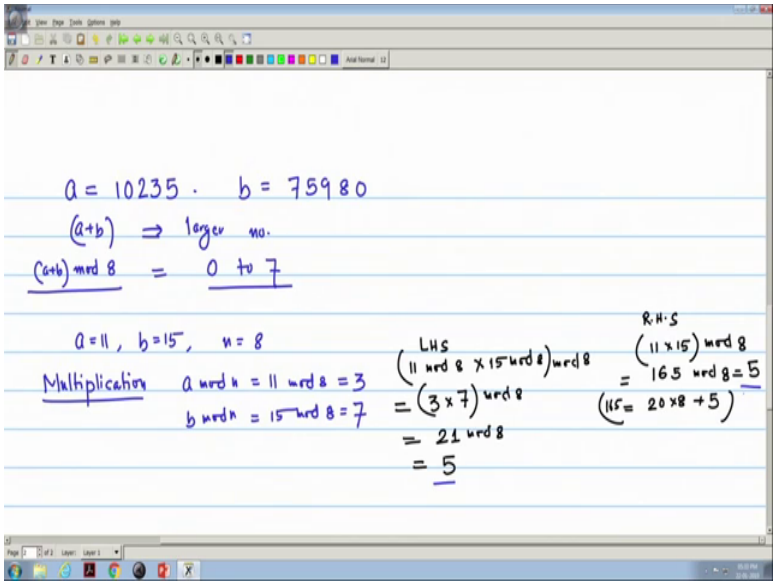
multiplication that a mod n into b modulo n take the modulo n which is a into b modulo n.

Now we take one example that how it is used for larger arithmetics; how it is what is the advantage of this thing? Now, we take one example. Say we take a equal to a equal to 11, b equal to 15 and n equal to 8. So, the addition will or a modulo n first we do. a modulo n is 11 modulo 8 which is 3. Similarly, I can write b modulo n is 15 modulo 8 and is equal to 7.

Now, if we do the addition; write addition, then 11 modulo 8 plus 15 modulo 8 this modulo 8; that means, my LHS; this is my left hand side. So, 11 modulo 8 we have seen 3; 15 modulo 8 we have seen 7; 7 plus 3 modulo 8 is 10 modulo 8 equal to 2. And if I do a plus b modulo n; so if I write the RHS a plus b modulo 8. So, this is simply 11 plus 15 modulo 8 and this equal to 26 modulo 8 which is 2. Now, we see that here it is 2; here it is 2. So, these 2 are required.

Now, what is the advantage? See here, I have taken a is 11 and b is 15, but and this is slightly larger 26 modulo 8. I get 2. Here my computing and I am doing only 11 mod 8 and 15 mod 8 not the and I got 3 plus 7. So, instead of 26, I got 10. So, if my a is very big say if I take my instead of a 11 and b 15 I can take my a is safe is a very large number 10235 like that or even larger and say is also 75980 or even larger.

(Refer Slide Time: 06:23)



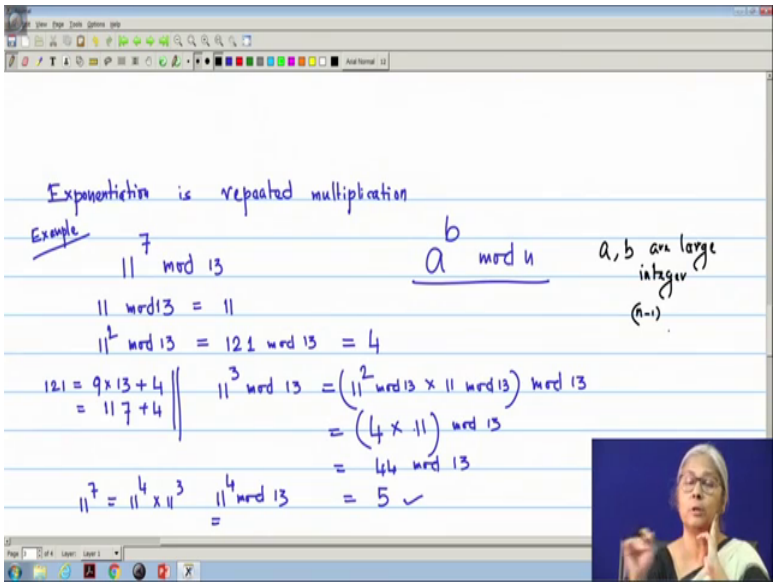
So, whatever be the thing, I do when I do that a plus b. Again, it will be a some larger number and that when I take the modulo, when I take the modulo a plus b. So, if whatever large number it is, if I take a plus b modulo 8, my module the result will be only 0 to 7 because my modulo 8; that means, only the remainder when it is divided by its 8, the remainder can be only 0 to 7 and this is a big advantage of when the large number will be dealing with large number the computation in large number. Particularly in the area of pictography, the coding that it is of tremendous use.

Now, with the same number that same example that a is 11 and b is 15 and n is 8, we can see the multiplication. Because all of we know the multiplication becomes the product will be even larger than the addition of two. So, if I take the a modulo n which is 11 mod 8 equal to 3 and my b mod n equal to 15 modulo 8 which is 7. Now, if I take the multiplication that means, in LHS again the similar way I can take, I can take the LHS. This is equal to the 11 mod 8 into 15 modulo 8. I take a modulo 8 and this becomes 11 mod 8 is 3 and 7 and this is modulo 8.

So, 3 into 7; both are very small numbers because that number cannot be larger than 7. So, at most this can be 49. So, this is 21 modulo 8 and this becomes 5. Now, if I do the RHS, then it is 11 into 15 modulo 8. Now, see 11 into 8, this is a larger multiplication complex multiplication and the similar way if I take a and b, then it will be even largest. So, this will be 165 modulo 8 and if I take the remainder this will be 5 because it is 20 into 8 plus 5. So, 165 is 165 is this. So, I can write thus 165 modulo 8 is equal to equal to 5.

So, when I am doing the multiplication, this advantages even more. Because multiplication of too large numbers are actually difficult complication and this will be never it will be more than the n minus 1; maximum it can be n minus 1. So, we say that these are in this way we can take that this 5 and 5 these are equal. So, in this we way we take.

(Refer Slide Time: 11:01)



Now, exponentiation because we know the exponentiation is nothing but the repeated multiplication. My exponentiation is nothing but repeated multiplication and just now, we have seen the multiplication is very easy; particularly large multiplications large multiplication of large numbers because the each one cannot be larger than n minus 1 when it is divided by n.

So, we take one example of that and we see how we can take the advantage of modular multiplication. Say we are taking or we want to compute say 11 to the power 7 modulo 13 ok. Now 11 to the power 7; that means, we have to multiply 11, 7 times and modulo 13. So, what we can do that? See we have to compute this thing. So, I write my 11 modulo 13 is nothing but 11 because 11 is less than 13 remainder should be 13 only.

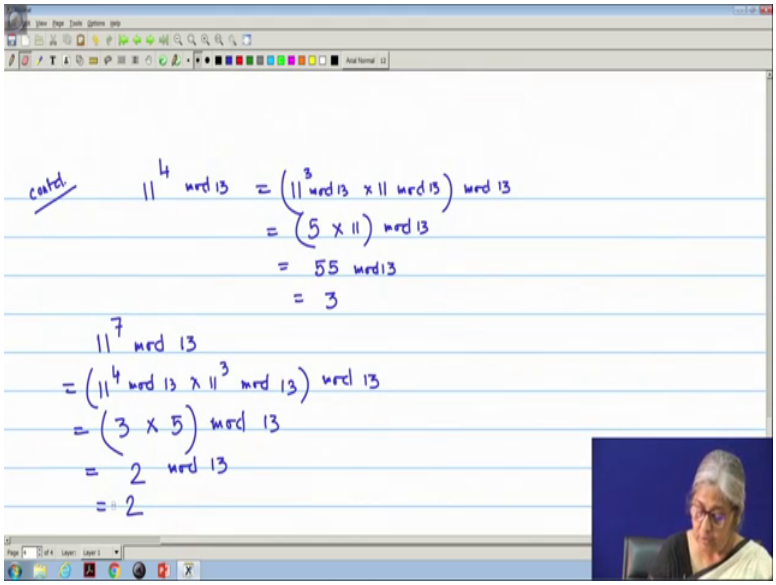
But 11 square modulo 13, if I apply multiplication that means, it is 11 mod 13 into 11 mod 13 that of mod 13. So, I have to write each one will be 121 modulo 13 and that will be. So, if I divide that what is my 121 121 is, 8. It is of 4; 4 plus 4 13 into 9 into 13; I think is 9 into 13 is 117 plus 4.

So, I can write 121 modulo 13 is equal to 4 ok. So, 121 is 4. Now, I can 11 square is modulo 13 is 4. So, I can write 11 to the power 4 modulo 13 or first I take 11 to the power cube 11 to the power cube modulo 13 is same as 11 square modulo 13; repeated multiplication 11 mod 13 and that of mod 13 just the rule of that modular multiplication.

So, 11 square we have just seen that 11 square modulo 13 is 4 and 11 mod 13 is 11. So, modulo 13 and that is 44 modulo 13. So, this will be 5 into 11.

Now, what is our I have to find out that 11 to the power 7. So, I can write 11 to the power 7. If I 11 to the power 7 can be written as 11 to the power 7 is 11 to the power 4 into 11 to the power 3. So, 11 to the power 4 we got 3 we got 5. So, and 11 to the power 11 square we got 4. So, that again I can write 11 square or what I can find out the 11 to the 4 only. So, I can write the 11 to the power the same way I can write the 11 cube.

(Refer Slide Time: 16:56)



So, 11 to the power 4 modulo 13, we have to compute that we can continue ok. 11 to the power 4 modulo 13 that we can write 11 modulo 13 into 11 or 11 cube 13 into 11 modulo 13 and mod 13 and 11 to the power cube we got 5 into 11 modulo 13 and 55 modulo 13. So, that is 3.

So, now if I write 11 to the power 7 modulo 13, I can write this as 11 to the power 4 modulo 13; 11 to the power 3 modulo 13 and 11 to the power 4 is 3 and because this is my multiplication rule and this cube is 5. So, 3 into 5 modulo 13 and this becomes 2 modulo 13 that means, this is equal to 2. 2 modulo 13 is we get that mean reminder is 2 ok. This is 2 mod I can write 2 modulo 13.

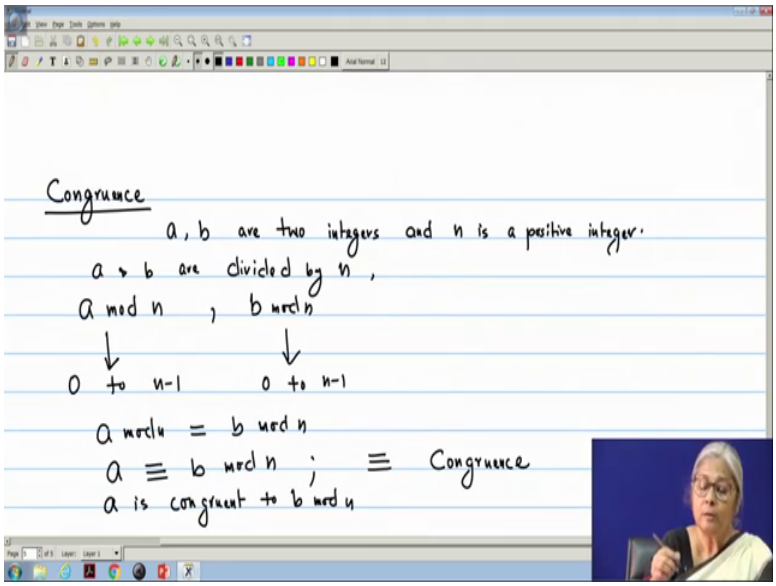
Now, see the way we have done this, this power can be is a large number that it can be some I can write some a to the power b and modulo n, where this a and b are very large

number. a and b are large integer say very large integer, but if we apply the modular multiplication to compute the exponentiation. Then, never the each multi modular multiplication results cannot be larger than n minus 1 because that remainder can be only n 0 to n minus 1.

So, in this way we compute my computation is much simpler. So, this is one particularly to get exponentiation that this is a big advantage and this is used this computation is used in cryptography. So, algorithms like RSA, algorithm we know that public cryptography this has a big advantage.

Now, we see some again some simple properties of modular n or before that we define a if congruence which is actually some I should tell some variant of modular operation. How we can define; the congruence or congruent modular n or congruence?

(Refer Slide Time: 20:24)

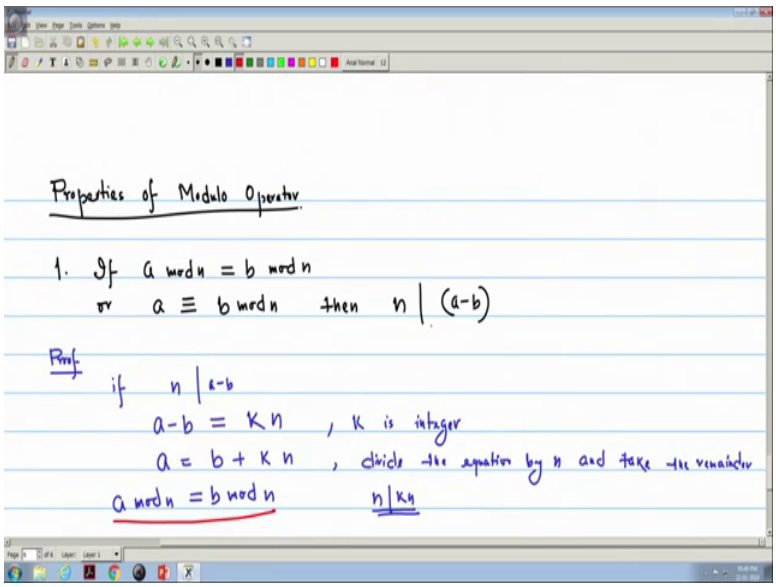


So, if a and b are 2 integers; a, b are 2 integers; and n is a positive integer and here a and b are divided by n separately by n and modulo's are that where we can write it is a modular n and when it is b is divided by n, the remainder we can write b modular n. Now, a modular n just now what we have read? The remainder can be only value 0 to n minus 1.

Similarly, b modular n whatever be the value b of b, this can be 0 to n minus 1. Now since if n is small or whatever be the n values, then it is a many to 1 mapping; that

means, for many a and b that will map to the same value because a and b can be any larger integer that we can get a the same value n. So, if we see that my a modular n equal to the b modular n that means, the remainders are same when a is divided by n b is divided by n. Then, we write that a is congruent to b mod n. So, this is the definition of congruence a is congruent to b mod n when a mod n equal to b mod n. So, we call this is the operation of that congruence and we write a is congruent to b modular n ok. Now, we see some property of this congruence.

(Refer Slide Time: 23:17)



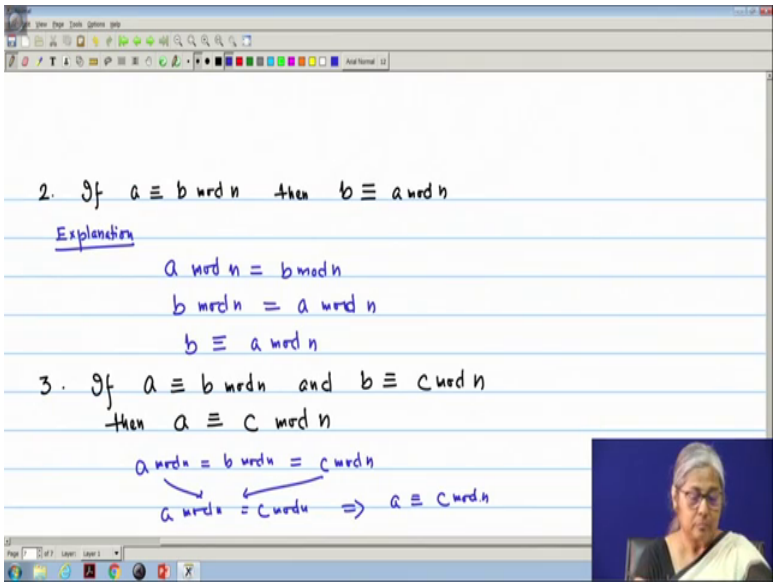
So, property one, the again these are also properties of I can tell the modular operator because congruence is nothing but the modular. So, again we read some of the properties of modular operator. So, many time we define or we the property that if a mod n equal to b mod n or I can write a is congruent to b mod n same thing just now we have defined, then n divides a minus b. Sometimes, this is also one definition of the congruence we write that n divides a minus b.

How we can explain this thing? See we start from this that I can write the proof or explanation whatever we call the proof or some explanation because it is trivial. Then, if n divides a minus b; that means, a minus b equal to K n because there is no remainder K is the quotient ok. K is integer and there is a quotient. So, a equal to b plus K n. Now, this equation if I divide by n and take the remainder. So, divide the equation by n and take the remainder. So, remainder will be K, then LHS will give a modular n and if I take

divided by n and take the remainder. So, K n since I am dividing by n. So, K n this portion has no remainder.

Because it is n divides n divides K n because it is divisible. So, I will be getting only b modulo n. So, which is my definition or what the statement is that if a mod n equal to b mod n, then divides a minus b. So, this is one property that will many times we use that thing.

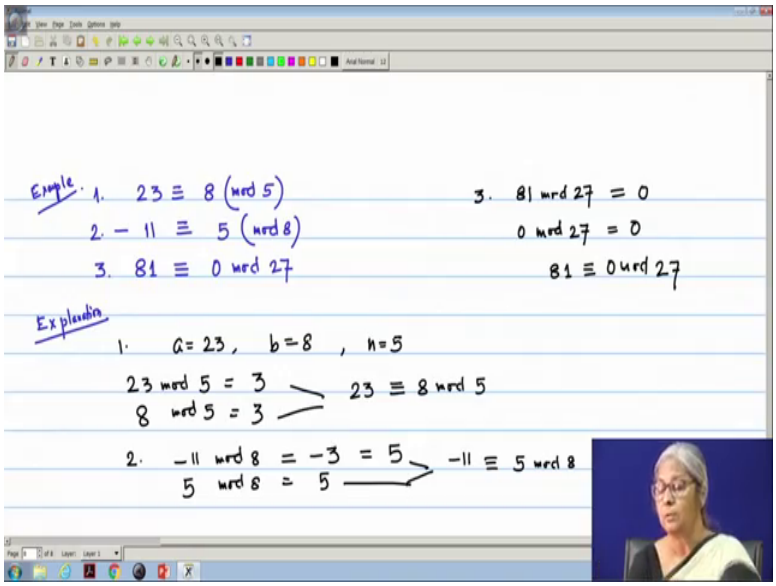
(Refer Slide Time: 26:34)



Now, other property I can write that this is very trivial that if a is congruent to b modular n, then we can write b is congruent to a modular n. And the explanation is very I should tell explanation instead of proof because it is mainly coming from the definition of modular that the way we have done that congruent is a mod n equal to b mod b mod n. So, I can just write this side b mod n equal to a mod n and this is the definition that b is congruent to a modular n. So, it is very trivial. Now, the third property that property 3, we can write that if a is congruent to b modular n and b is congruent to c modular n, then a is congruent to c modular n.

So, again I think this explanation is very simple because a is congruent to b mod n means a mod n equal to b mod n and b is congruent to c mod n is b mod n equal to c mod n. So, I can write; I can write a mod n equal to c mod n and which implies actually a is congruent to c mod n. So, these are some of the properties that if we see some example we see that.

(Refer Slide Time: 29:17)



Example, we take 23 is congruent to 8 modular 5 minus 11 is congruent to 5 modular 8. Similarly, I can write 81 is congruent to 0 modular 27. So, if we explain that first one; 23 is congruent to 8 modulo 5 because we see if I here n is 5 ok. I can write give some 1 2 3 and later, I write the explanation. So, number 1 explanation is my a equal to 23 b equal to 8 and n is 5. So, what you see that 23 modulo 5 is 3 and 8 modulo 5 is 3. So, from here I can write that 23 is congruent to 8 modulo 5.

Now, if we see the 2, that minus 11 is congruent to 5 mod 8 and directly I can write minus 11 modulo 8 is minus 3 and minus 3; we know minus 3 is nothing but plus 5. So, I get thing it will be positive number normally that is the convention. So, one thing you know that if it is a minus, then and it is modulo 8. So, if I get x then it is that n plus x; x is if x is minus 3, if it is negative or then it is n plus x that means, 8 minus 3, 5.

And 5 mod 8 is 5 because it is less than 8. So, 5 is the remainder only. So, from here and here I can write minus 11 is congruent to 5 modulo 8. Then similarly the 3, if we see 81 modulo 27 is 0 because there is no remainder 3 into 27 is 81 and this is 0 only. So, I can and 0 modulo 27 is 0 only because that divisible property or devices property of devices, we have seen that any b not equal to 0 divide 0. So, this is the property very trivial property. So, I can write 81 modulo 27 or 81 is congruent to 0 modulo 27 ok. So, 81 is congruent to 0 modulo 27.

So, congruence is actually one property of modular arithmetic. So, these are some of the basic properties of modular arithmetic and again, we will see some examples or other modular properties when particularly the addition and multiplication, we will see. Division now we will not considered and slowly we will see that what is the problem or how we can incorporate the division properties.

So, next lecture, we will continue again with the properties of modular arithmetic in particular the addition and the multiplication operation.