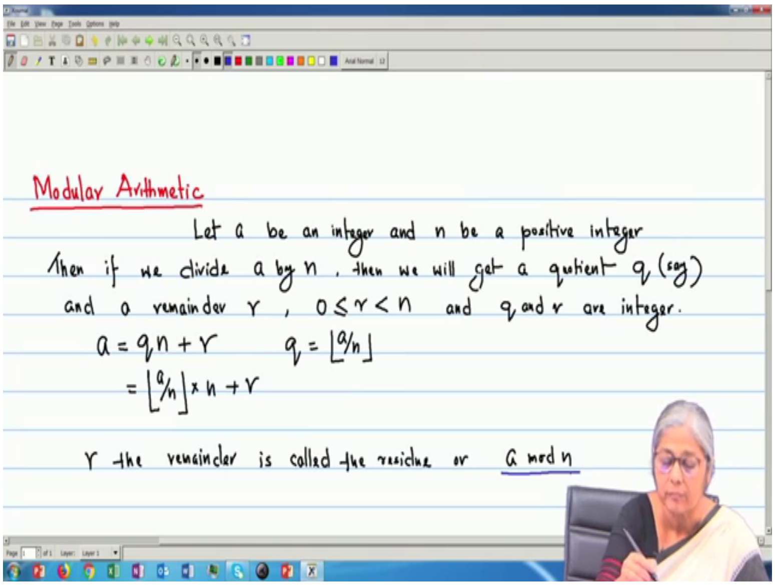
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 53
Ring and Modular Arithmetic (Contd.)

So, we have discussed the Algebraic structures and number of algebraic systems, mainly based on some properties we have read and almost all the algebraic systems like group or the semi group, monoid or the last algebraic systems that we have read is the Ring. There everywhere we considered one example, where some modular operation we have discussed or we considered. Now, we have defined there in very short that what do you mean by the modular n, a modulo n or a modular b. Now, today we will see or we will read in details the modular arithmetic. Because this has a very important role in algebra; algebraic systems or particularly this modern algebra.

(Refer Slide Time: 01:32)



Modular Arithmetic

Let a be an integer and n be a positive integer Then if we divide a by n, then we will get a quotient q (say) and a remainder r, $0 \leq r < n$ and q and r are integer.

$a = qn + r \qquad q = \lfloor a/n \rfloor$

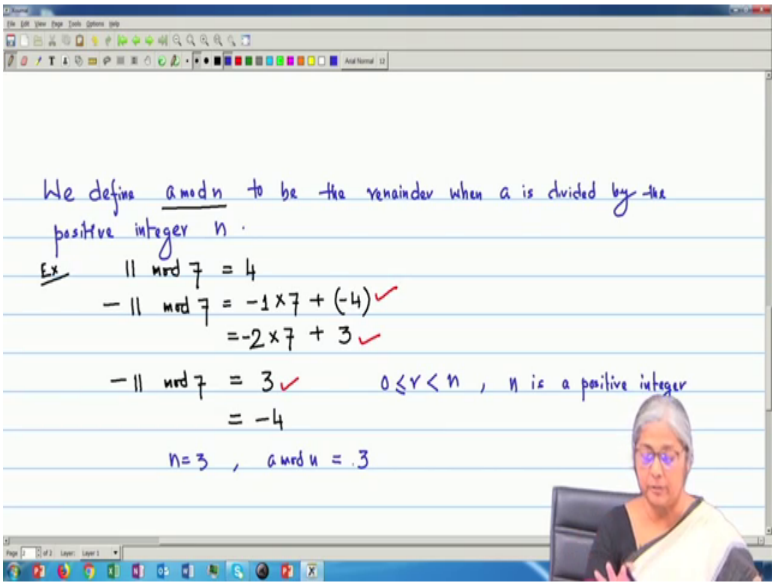
$= \lfloor a/n \rfloor \times n + r$

r the remainder is called the residue or a mod n

So, today we will mainly consider the modular arithmetic, its definition, the different properties and some application areas. So, first we define that what do you mean by Modular. So, let a be an integer and n be a positive integer. Then if we divide a by n, then we will get a quotient; get a quotient or integer quotient say q; say q and a reminder r, where 0 less than equal to r less than n and q and r integer.

So, we can write that a equal to q n plus r or q that r remainder is greater than 0 greater than equal to 0 or less than n, if it is divisible by n; a is divisible by n; that means, there is no reminder. That means, it is 0 or it is less than n and q, I can tell that q is floor a by n; floor a by n earlier we have defined that it is the largest integer less than or equal to a by n. So, I can write that this is floor a by n into n plus r. Now this r is sometimes called the r the remainder r is called the residue or that it is the remainder of when a is divided by n, it is called that a modulo n or a mod n. So, mainly the remainder when a is divided by n, like it is called that a modulo n.

(Refer Slide Time: 06:08)



We define $\underline{a \bmod n}$ to be the remainder when a is divided by the positive integer n.

$\underline{Ex}$ $11 \bmod 7 = 4$

$-11 \bmod 7 = -1 \times 7 + (-4)$ ✓

$= -2 \times 7 + 3$ ✓

$-11 \bmod 7 = 3$ ✓ $\quad 0 \leq r < n$, n is a positive integer

$= -4$

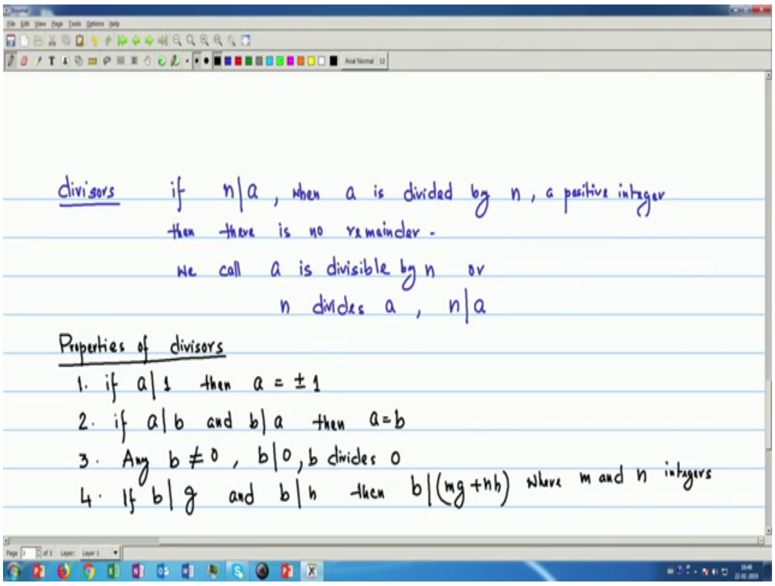
$n = 3$, $a \bmod n = 3$

So, we defined that a mod n, we defined a mod n to be the remainder when a is divided a is a integer a is divided by the positive integer n; positive integer n. Example we gave give. So, this is my definition of a modulo n ok. If I give an example simple example, if we see that modular see 11 modular 7 that means, when 11 is divided and we know it is nothing but 4.

So, what will be minus 11 mod 7? Minus 11 mod 7. This can be minus can be minus 3 which can be the quotient. I am sorry minus 1 be the question and then 4 is so I can write this thing as minus 1 into 7 plus minus 4; this is minus 11 or same thing I can write that 2 into 7 minus 2 into 7 plus 3. So, this can be since the way we have define it is the remainder. So, it this can be the remainder minus 4 or this can be the remainder. So, minus 11 mod 7, I can write this is 3 or even sometimes we can write minus 11 mod 7 is minus 4, but normally the convention is that we give the as a give as a positive integer. Because the remainder we have defined that if you remember that we have defined that my r is 0 less than equal to r less than n and n is a positive integer; n is a positive integer.

So, since r greater than 0 equal to 0, so this is positive and less than n. So, here say this n is 7; in this case n is 7. So, my a modulo n a modulo n is 3. So, this is my definition of my modulo. Now all of we know, but again I repeat that sometimes we call that devisors.

(Refer Slide Time: 10:00)



divisors if $n|a$, when a is divided by n, a positive integer then there is no remainder.

we call a is divisible by n or n divides a, $n|a$

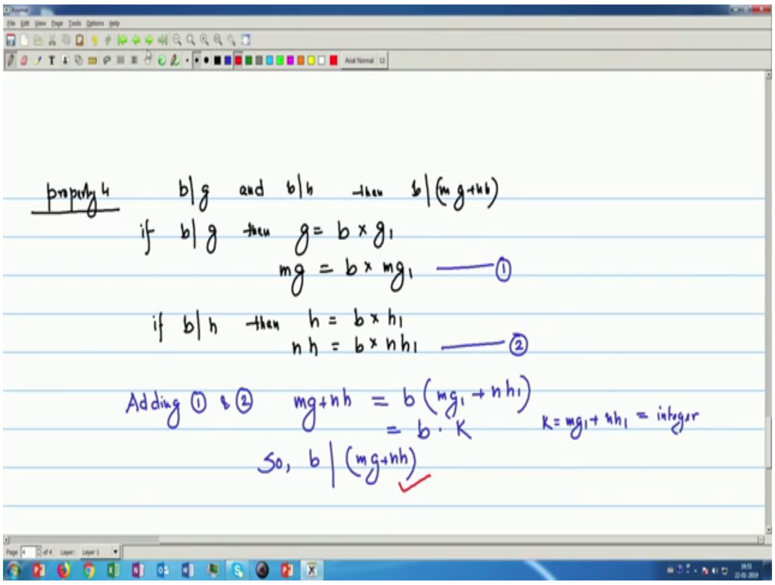
Properties of divisors

1. if $a|1$ then $a = \pm 1$
2. if $a|b$ and $b|a$ then $a=b$
3. Any $b \neq 0$, $b|0$, b divides 0
4. If $b|g$ and $b|h$ then $b|(mg+nh)$ where m and n integers

So, normally divisor is when there will be no remainder. So, divisors that if say n divides a. We normally we write in this way n divides a that means, when a is divided by n, a positive integer; a positive integer, then there is no remainder. We call (Refer Time: 11:08) or we mention call that a is divisible by n or I can tell that n divides a and normally, the notation is n divides a. So, the divisors have some a property. Though it is very primitive, but we require for this explanation of the different property of a modular n so, we quickly write those things.

The some of the properties of divisors, we can write that 1 if a divides 1; if a divides 1, then a equal to plus minus 1. If a divides b and b divides a, then a equal to b. If any b any b not equal to 0, divides 0; b divides 0, then b divides 0. We call b. we call b divides 0 and if b divides. If b divides g and b divides h, then b divides mg plus in n h; where, m and n are positive integer or m and n are integers. So, we can explain that fourth property because all the properties 1, 2 and 3 are very trivial all of we know that thing.

(Refer Slide Time: 14:25)



property 4 $b \mid g$ and $b \mid h$ then $b \mid (mg+nh)$

if $b \mid g$ then $g = b \times g_1$

$mg = b \times mg_1$ —— ①

if $b \mid h$ then $h = b \times h_1$

$nh = b \times nh_1$ —— ②

Adding ① & ② $mg+nh = b(mg_1 + nh_1)$

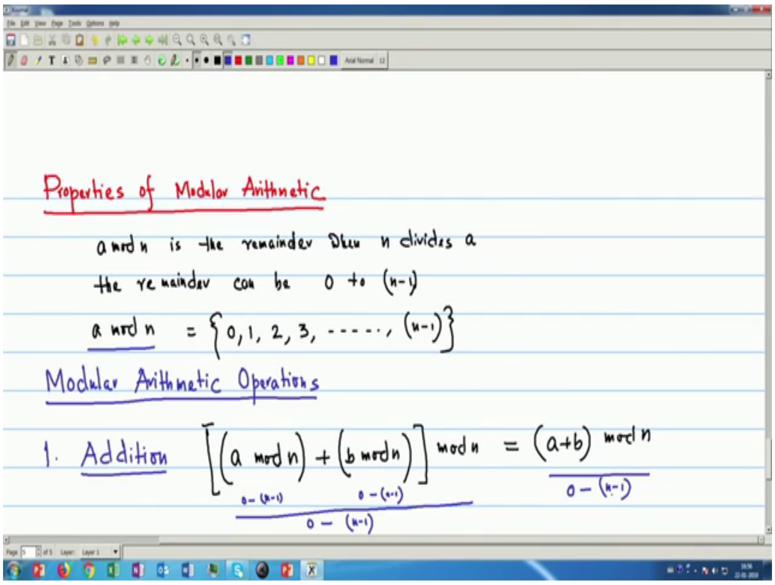
$= b \cdot K$ $K = mg_1 + nh_1 = \text{integer}$

So, $b \mid (mg+nh)$ ✓

So, we just explain the property 4; it tells that b divides g and b divides h. Then b divides m g plus n h ok. So, if b divides g that means, we can write that g equal to then g equal to some b into some g 1. Because it divides that means, there is no remainder; only quotient. So, if I multiply both sides by g m, then m g is b into mg 1. Similarly, if b divides h; then, h equal to b into h 1 and n h equal to b into n h 1.

So, now if I add this 1 and 2; so, adding 1 and 2, we get mg plus n h equal to b m g 1 plus n h 1. So, m g 1 plus n h 1, this is one integer. So, we can write that. So, some if I write or this equal to b into some say K one integer. So, K equal to mg 1 plus n 1 is one integer. So, b divides can write that b divides mg plus n h. So, the property 4, it is proved. We can explain in this way. Now, we go to some properties of modular operator.

(Refer Slide Time: 17:36)



Properties of Modulor Arithmetic

a mod n is the remainder when n divides a

the remainder can be 0 to (n-1)

a mod n = {0, 1, 2, 3, ------, (n-1)}

Modular Arithmetic Operations

1. Addition $\underbrace{\left[\underbrace{(a \bmod n)}_{0-(n-1)} + \underbrace{(b \bmod n)}_{0-(n-1)}\right] \bmod n}_{0\,-\,(n-1)} = \underbrace{(a+b) \bmod n}_{0-(n-1)}$

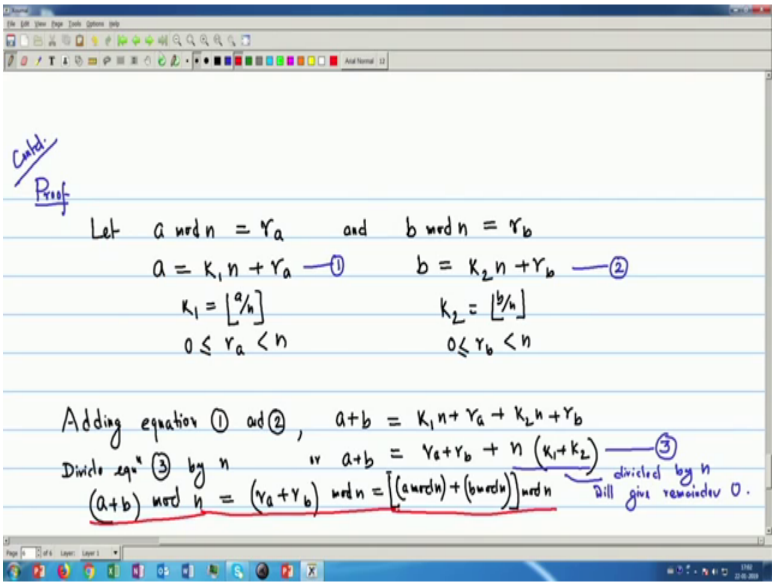
Because just now, I have seen some only our normal division that some of the properties, when it is properly divisible or if some remainder is there. If some remainder is there, then actually our modular operation comes into picture. Now, if a modular n, we have defined that a modular n. We write a mod n. a mod n is the remainder, when a is when n divides a ok. Now, n divides a. Now, if n is a positive integer and we a is divided by n, then the remainder can be 0 to n minus 1.

So, when a is divided by n the remainder, the remainder can be 0 to n minus 1. These are my remainders. So, a modulo n is the set, I can write that this is 0, 1, 2, 3 up to n minus 1. Now, we will see some arithmetic that which works on this set only or we will see the whether our ordinary addition subtraction division or multiplication, how it works or whether at all the similar way it works on this set. Because the modular arithmetic now I tell that a mod n is nothing but this, these it can be only the set of elements from 0 to n minus 1. So, first we see the modular arithmetic operations.

So, first we consider the addition or consider the addition. So, addition we can write that a modulo n plus b modular n, if I take the or I can write in this way a mod n plus b mod n and I again modular n; then, I will be getting a plus b modular n. First, we see that see. Here my a modulo n is a set any elements from 0 to n minus 1. So, this is a set from 0 to n minus 1; any elements. Now, similarly b modular n because it is divided by n. So, this will be again 0 to n minus 1. So, these are two numbers and then again, if I take modular n. So, the whole thing that this thing again is becomes 0 to n minus 1.

And similarly, if a plus b now whatever be the number large whatever large number it is, when I am dividing it by n and since a mod n is nothing but the remainder. So, again this thing is from 0 to n minus n n minus 1. So that means, this we know that this is a modulo n plus b modular n, if I take the modular n then this will be the a plus b modular n.

(Refer Slide Time: 23:04)



Contd.

Proof

Let $a \bmod n = r_a$ and $b \bmod n = r_b$

$a = k_1 n + r_a$ — ① $\quad b = k_2 n + r_b$ — ②

$k_1 = \lfloor a/n \rfloor \quad k_2 = \lfloor b/n \rfloor$

$0 \leq r_a < n \quad 0 \leq r_b < n$

Adding equation ① and ②, $a+b = k_1 n + r_a + k_2 n + r_b$

or $a+b = r_a + r_b + \underbrace{n(k_1+k_2)}_{}$ — ③ divided by n will give remainder 0.

Divide eqn ③ by n

$\underline{(a+b) \bmod n = (r_a + r_b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n}$

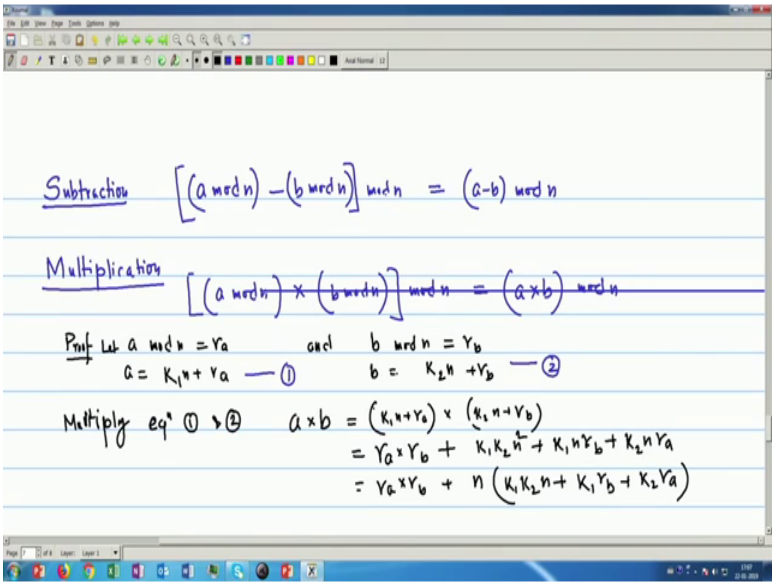
So, how we can prove? We see the proof. So, let this is continued. Let a modulo n that means, when a is divided by n is actually r a and b modular n, when b is divided by n the remainder is r b. So, I can write a equal to sum K 1 n plus r a. K 1 is the quotient, when a is divided by n.

Similarly, I can write b equal to K 2 n plus r b. So, here I can write that my K 1 is K 1 is floor a by n and 0 less than equal to r a less than n. Similarly, here I can write K 2 is floor b by n and 0 less than equal to r b less than n. Now, if I if I add this equation 1 and equation 2; equation 1 and equation 2, if we add; then, we will be getting that adding equation 1 and 2, we write that a plus b equal to K 1 n plus r a plus K 2 n plus r b.

So, equal to I can write r a plus r b plus n K 1 plus K 2. Now if I take divide a this equation. So, I can write a plus b. Now, say this equation I give name equation 3. So, if I divide equation 3 by n. So, divide equation 3 by n, this will give and if I take the remainder of that. So, this will be a plus b modular n is the remainder from left hand side and from right side, this will be my r a plus r b modular n because here n into K 1 plus K 2. So, this is when I am dividing by n. So, there will be no reminder for this part. So, for this part since is n into; so, divided by n will give 0 remainder; will give remainder 0.

Now, a plus b mod n equal to r a plus r b mod n that gives what is r a plus r b see that r a is a mod n. So, this is nothing but r a plus r b is a mod n; r a is a modulo n ok. I can write here. So, a modulo n plus r b is b modular n and this mod n. So, this is mod n. So, the property 1 or the addition property, the addition property is proved that a plus b mod n equal to a plus a mod n plus b mod n mod n. Now the totally similar way, that similar way I can prove the subtraction.

(Refer Slide Time: 28:36)



Subtraction $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

Multiplication $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

Proof Let $a \bmod n = r_a$ and $b \bmod n = r_b$

$a = K_1 n + r_a$ — ① $\quad b = K_2 n + r_b$ — ②

Multiply eqn ① & ② $\quad a \times b = (K_1 n + r_a) \times (K_2 n + r_b)$

$= r_a \times r_b + K_1 K_2 n^2 + K_1 n r_b + K_2 n r_a$

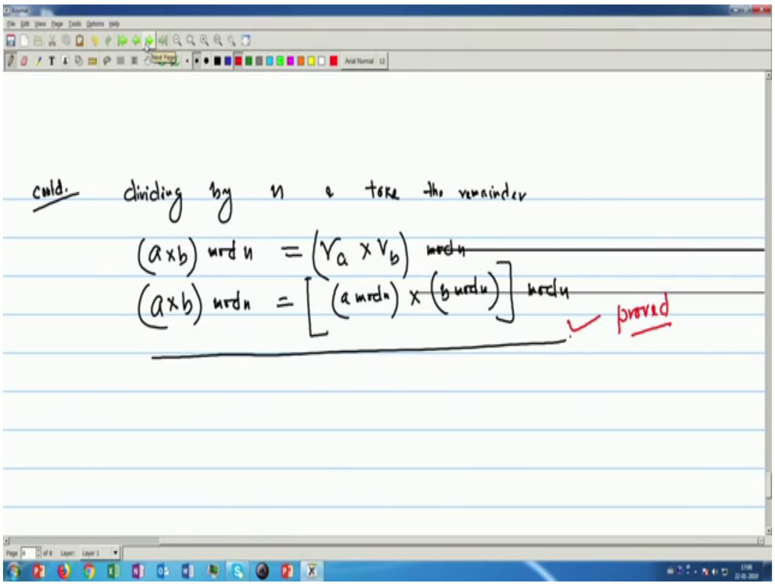
$= r_a \times r_b + n(K_1 K_2 n + K_1 r_b + K_2 r_a)$

So, the property of subtraction that we can write that subtraction that a modulo n minus b modular n. If I take a modular n, this will be a minus b modular n and the way we have proved that my addition property for modular operator that totally similar way, we can take; only that when we have added adding that time, we have to subtract equation 2 from equation 1 and the remaining things are same. So, if I write the multiplication property that we have to write that that a modulo n into b modular n, we take again modular n is a into b mod n.

Now, the way we have proved if the same thing we can do so multiplication proof, we can now take that a similar way we take that a mod n equal to r a. So, let a mod n equal to r a. So, a equal to the way we have taken K 1 n plus r a and b mod n equal to r b we can take b equal to K 2 plus K 2 n plus r b; K 2 n plus r b. Now, what is my a b? Because when we have proved the addition property, we have taken the equation 1 and 2, we have taken the sum. Now, we have to multiply. So, if I multiply equation 1 and 2 will be getting a into b equal to K 1 n plus r a into K 2 n plus r b and will be getting r a into r b plus that we can take K 1 K 2 n square plus K 1 n r b plus K 2 n r a.

So, this will be r a into r b plus if I take common n. So, I will be getting K 1 K 2 n plus K 1 r b plus K 2 r a. Now, see similarly if I divide a into b by n.

(Refer Slide Time: 32:39)



cntd. dividing by n & take the remainder

$$(a \times b) \bmod n = (r_a \times r_b) \bmod n$$

$$(a \times b) \bmod n = \left[(a \bmod n) \times (b \bmod n)\right] \bmod n$$

✓ proved

So, dividing by n and take the remainder, we get a into b modular n is only r a into r b because again here n is there. So, when I will be taking dividing by n this part will give the 0 remainder. So, this is if we reminder that a cross b modular n is r is my ok. This is r a r b modular n, then these will be a mod n into b mod n n into mod n. So, it is proved. But see we cannot do this thing for division property. We have only multiplication, subtraction and the addition ok.

So, just the basic properties that modular operation holds that we have read here and some more properties when it is repeated multiplication or repeated addition and that will be reading in the next lecture.