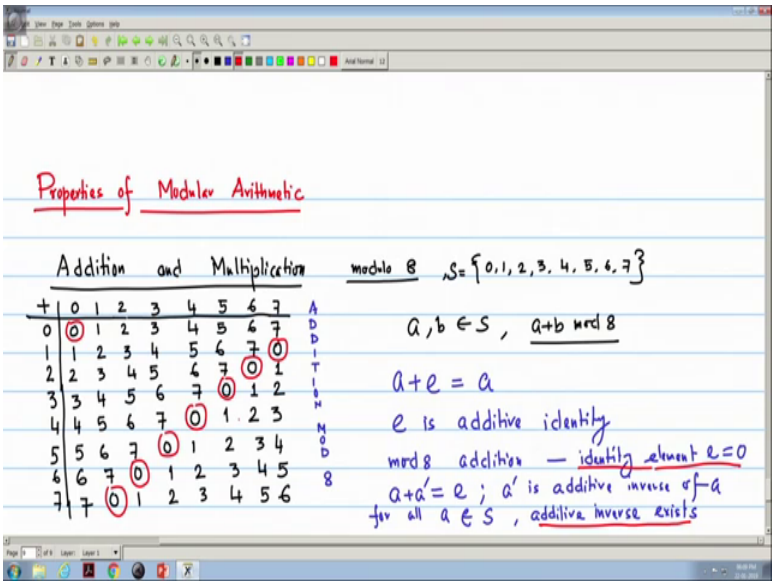
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture – 55
Ring and Modular Arithmetic (Contd.)

So, we continue our discussion on Modular Arithmetic and this lecture particularly will see how the addition and multiplication gives a particular type of algebraic system. Actually, these as the example or modular operation as the example already we have discussed for our group ring, and now we see in general that how these properties are giving the particular type of algebraic systems. So, again properties of modular arithmetic.

(Refer Slide Time: 01:06)



Properties of Modular Arithmetic

Addition and Multiplication modulo 8 , $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

ADDITION MOD 8

$a, b \in S$, $a+b \bmod 8$

$a + e = a$

e is additive identity

mod 8 addition — identity element $e = 0$

$a + a' = e$; a' is additive inverse of a

for all $a \in S$, additive inverse exists

So, this modular arithmetic as already I mentioned will consider the mainly the addition and multiplication ok. Now, and will see the, if we remember that whenever that we are define some algebraic systems like group ring some general properties we have set and based on those properties. What are those properties?

Like commutative associative whether additive inverse exist, additive identity, or the multiplicative inverse exist based on that we have define some algebraic systems. Now, now we see or we first prepare some our addition modulo table; that means, some table with the operation is the modular addition. Let, we take 1 example of and with these example where we define that thing um. So, addition and multiplication of modular arithmetic we take, the modulo say 8 ok. Now, modulo 8 means, that my set can be only 0 1 2 only 0 2 n minus 1 4 5 6 7 ok.

Now, if we make the addition table ok. First we do the we do the addition table. So, I write that 0 because my set will be 0 1 2 3 4 5 6 7. Here also this is my addition modulo 8, I am taking this is my addition and multiplication modulo 8. So, this is addition modulo table. Now, how we do that thing, that if we know the addition this is if a and b, say if this is my set s. Then, a and b belongs to s, then a plus b modulo 8 will be taking that is the modulo; that means, I will add 2 numbers and will take the remainder when it is divided by 8. Now, a is 0 to 7 a can be 0 to 7 b can also be 0 to 7.

So, will be adding these 2 numbers and taking the remainder by dividing it by 8. So, 0 plus 0 it is 0, it is 1 2, because if we add all the a plus b that will be less than 8. So, the remainder will be the same thing. Now, if it is 1 plus 0, it is 1 2 2 divide 2 divided by 8 remainder will be 2 3 4 5 6 7, now this becomes 1 plus 7 8 8 divided by 8 this remainder will be 0. Similarly, again 0 plus 2 3 4 5 2 plus 4 6 7 these becomes 6 plus 2.

So, 8 divided by 8 remainder 0 2 plus 7 9. So, 9 divided by 8 1. Similarly, now we can fill up quickly 5 6 7, now this becomes 0, this becomes 1, this becomes 2. Now, it is 4 5 6 this become 0 1 2 3, this is 7, because modulo 8 I am taking, this is 4 plus 3 7 7 modulo 8 is 7 8 modulo 8 0 1 2 3. Now, 5 it is become 5 6 7, now 0 1 2 3 4 6 7, now this becomes 0 1 2 3 4 5, now 7 is 7 0 1 2 3 4 5 6. So, we see that it is if I take that 0 plus 0 it is 0 1 plus 1 plus 7 is a or 1 plus 0 is 1 2 plus 0 is 2 3 plus 0 is 3 4 plus 0.

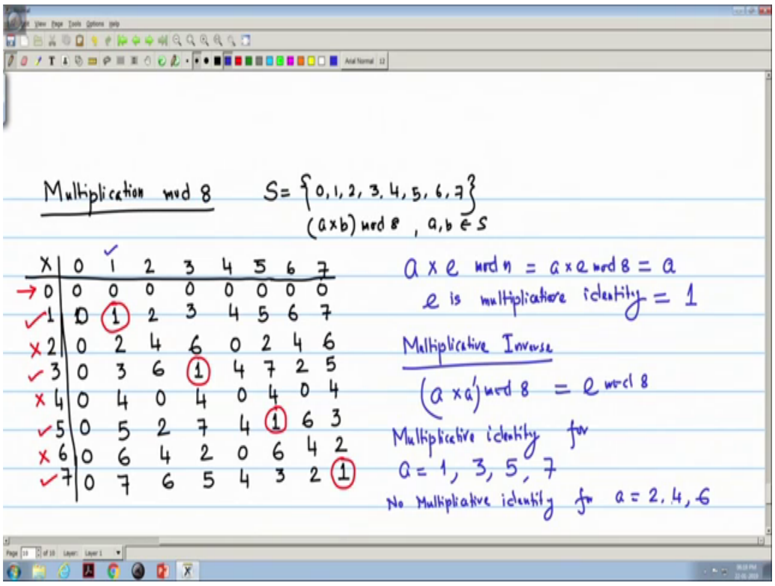
So, if we remember that my a plus e equal to a then e is my e is additive identity. So, here for modulo 8 addition modulo 8 addition the identity additive identity is 0 ok, addition I have written. So, I can write identity element is identity element is 0 identity element e is 0. Now, what about the additive inverse? Now, if we remember the if some a plus a dash equal to e or a dash plus a then a dash is the inverse of additive inverse of a.

Now, we see that if we that 0 plus 0 is 0 see 1 plus 7 is 0 2 plus 6 is 0 3 plus 5 is 0 4 plus 5 is 0 since 0 is my identity. So, for each element I am getting and if I add I am getting 1 element just to add I am getting the identity element; that means, for each element of this set from 0 to 7 that 1 inverse exist. So, for when a equal to 1 my a dash is 7, a equal to 2 my a dash is 6. Like that, so, my for all a I can write then for all a all a belongs to S, S is

0 to 7 that additive inverse exist later we will tabulate that thing what are the we now remember. So, additive inverse exist.

So, when we have considering addition modulo 8. So, this is my this is my addition modulo 8 we can write this is my addition modulo 8. So, at the) for addition modulo 8, my these are the things I get my identity element exist, which is equal to 0 and for all a the additive inverse exist, because just now we see that. Now, we take the multiplication we see the multiplication modulo multiplication modulo 8, see multiplication modulo 8 ok.

(Refer Slide Time: 11:22)



Multiplication mod 8 $S = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$(a \times b) \bmod 8 \; , \; a, b \in S$

X	0	$\overset{\checkmark}{1}$	2	3	4	5	6	7
→ 0	0	0	0	0	0	0	0	0
✓ 1	0	1	2	3	4	5	6	7
x 2	0	2	4	6	0	2	4	6
✓ 3	0	3	6	1	4	7	2	5
x 4	0	4	0	4	0	4	0	4
✓ 5	0	5	2	7	4	1	6	3
x 6	0	6	4	2	0	6	4	2
✓ 7	0	7	6	5	4	3	2	1

$a \times e \bmod n = a \times e \bmod 8 = a$

e is multipliative identity $= 1$

Multiplicative Inverse

$(a \times a') \bmod 8 = e \bmod 8$

Multiplicative identity for

$a = 1, 3, 5, 7$

No Multipliative identity for $a = 2, 4, 6$

The same thing that since here modulo 8 so, my s is 0 1 2 3 because only up to 7. So, when I am considering the modular arithmetic that, how these multiplication operation operate on this set? Ok.

So, we this is my multiplication and considering 0 1 2 4 5 6 7 here also we consider 0 1 now it is multiplication. So, have to take that a into b modulo 8 and a b belongs to S. So, 0 into 0 of because 0 into all this becomes 0 and 0 modulo 8 is 0. So, I write these are all 0 ok. Now, if I multiply then these becomes 1 into 0 1 sorry it is 0 and 1 into 1 1 1 modulo 8 1 2, since it is multiplied by 1 only. So, all are less than 8. So, remainder will be the same when divided by 8.

Now, it is 0 2 4 modulo 8 6 modulo 8 now 8 modulo 8 2 into 4 8 and 8 modulo 8 is 0. Now, 2 into 5 10 10 modulo 8 remainder is 2, 2 into 6 12 remainder is 4, 1 divided by 8 2 into 7 14 remainder is 6. Now, similarly 3 into 0 0 3 6 modulo 8 6 3 into 3 9 9 modulo 8 is 1, 12 modulo 8 is 4, 15 modulo 8 is 7, 18 modulo 8 is 2, then 21 modulo 8 is 5. Now, 4 into 0 4 8 modulo 8 0 this is 0 4 12 modulo 8 4.

Then, it is 0 16 modulo 8 0 4 24 is 0 28 is 4, 5 0 5 10 modulo 8 is 2 7 20 modulo 8 4 25 modulo 8 is 1, 30 modulo 8 is 6 35 modulo 7 modulo 8 is 3. Now, 0 6 4 this is 2 because 18 modulo 2 8 into 2 16 plus 2 24 modulo 8 0 then 30. So, it is 6 again 4 and 2 7 it is 0 7 14 is 6 21, it is 5, it is 4 28 35 it is 37 to 6 42 42 modulo 8 is 2 and 7 into 7 49 modulo 8 is 1. Now, we see that what will be my multiplicative identity ok.

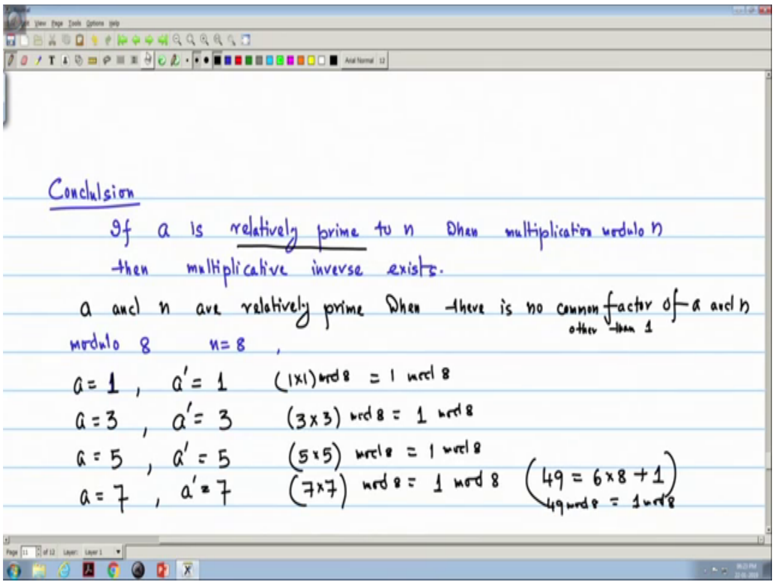
So, we see that if I consider 1, if I consider 1, then I am getting the 0 into 1 0 1 into 1 1 2 into 1 2. So, I can write that a into e some we know that operation that a into modulo n, in this case that a into e modulo 8 is e only a only that number only. So, e is my e is multiplicative identity.

And, equal to 1; that means, or multiplication or multiplicative modulo 8 is 1 ok. So, now, we remember the definition of inverse for multiplicative inverse we see multiplicative inverse, it will be we remember a into a dash modulo 8 should be e or e modulo 8 I I write a into e dash is e modulo 8. So, now, we see that e is 1. So, see for 0 0 is since we can see that 0 is if I multiply everything it will be 0. So, from 1 to 7 from 1 we are getting some identity that 1 into 1 identity.

See for 2 we are not getting any not getting any identity for 3 we are getting identity 1, but for 4 we are not getting, for 5 we are getting 1 identity, for 6 we are not getting, for 7 we are getting identity. So, if I summarize I can write that for we are getting multiplicative identity, identity for a equal to 1 3 5 and 7; that means, we are getting multiplicative identity I give a tick mark if I getting identity and I give a cross if I do not get.

So, I get for a equal to 1 3 5 7 I am getting and for we do not get no multiplicative identity for a equal to 2 4 6.

(Refer Slide Time: 20:41)



Conclulsion

If a is relatively prime to n When multiplication modulo n then multiplicative inverse exists.

a and n are relatively prime When there is no common factor other than 1 of a and n

modulo 8 $n = 8$,

$a = 1$, $a' = 1$ $(1 \times 1) \bmod 8 = 1 \bmod 8$

$a = 3$, $a' = 3$ $(3 \times 3) \bmod 8 = 1 \bmod 8$

$a = 5$, $a' = 5$ $(5 \times 5) \bmod 8 = 1 \bmod 8$

$a = 7$, $a' = 7$ $(7 \times 7) \bmod 8 = 1 \bmod 8$ $\left(\begin{array}{l} 49 = 6 \times 8 + 1 \\ 49 \bmod 8 = 1 \bmod 8 \end{array}\right)$

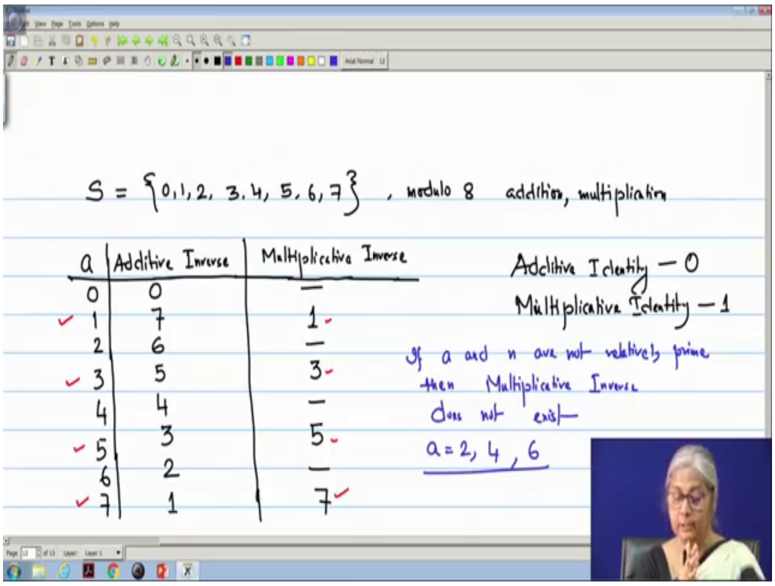
So, we can conclude the conclusion is that conclusion or if I tabulate first and conclusion is if a is relatively prime to n, when I am taking multiplication modulo n, then multiplicative inverse exists, then multiplication multiplicative inverse exists.

Now, what is relatively prime relatively prime to n; that means, a and n are relatively prime when there is no common factor between a and n. So, a and n are relatively prime when the when there is no common factor of a and n. So, if we see that when a equal to see I have taken modulo 8. So, my I am taking mod 8 operation on modulo 8 8. So, my n equal to 8 and when I take a is 1; that means, 1 and 8 other than. So, factor of n other than better I write other than 1.

See for 1 3 5 7 this is so 1 and so, a equal to 1 a equal to 1 and n is 8 always. So, 1 and a they are relatively prime, we are getting that some inverses 1 only ok. We are getting that a dash equal to 1, when a equal to 3 we are getting a dash equal to 3 since 3 into because 1 into 1 modulo 8 equal to 1 modulo 8 and 1 is my identity, 3 into 3 modulo 8 is my 9 modulo 8 is 1 modulo 8. What about a equal to 5 is 5 only because 25 is 25 should be the 5 into 5 8 into 3 plus 1.

So, a dash equal to 5. So, 5 into 5 modulo 8 equal to 1 modulo 8, then a equal to 7 we get a dash equal to 7 and this is 7 into 7 modulo 8 is 1 modulo 8. I think 1 we can see here 7 into 7 we can if I explain this is 49 equal to 6 into 8 plus 1. So, when I will be taking modulo and it will be 1 only, because it will there is remainder here. So, 49 modulo 8 it would be 1. So, 49 modulo 8 equal to 1 modulo 8 similar thing for other 3 examples.

(Refer Slide Time: 25:49)



$S = \{0, 1, 2, 3. 4, 5, 6, 7\}$, modulo 8 addition, multiplication

a	Additive Inverse	Multiplicative Inverse
0	0	—
✓ 1	7	1 ✓
2	6	—
✓ 3	5	3 ✓
4	4	—
✓ 5	3	5 ✓
6	2	—
✓ 7	1	7 ✓

Additive Identity – 0

Multiplicative Identity – 1

If a and n are not relatively prime then Multiplicative Inverse does not exist

a = 2, 4 , 6

So, now if I tabulate we write that, I have taken the set 0 1 2 3 4 5 6 7, since we are taking the modulo 8 addition and multiplication, 8 and modulo 8 addition and multiplication.

So, the previous 2 examples what we see that, if we now write the a the additive inverse and the multiplicative inverse ok. So, a can be 0 1 2 3 4 5 6 7 I take the additive inverse and multiplicative inverse, then what we have seen 0 additive identities. So, in I must write this 2 my additive identity is 0 my multiplicative must remember that we are taking modulo 8 operation multiplicative identity is 1, that earlier we have seen multiplicative identity is 1 modulo 8 1.

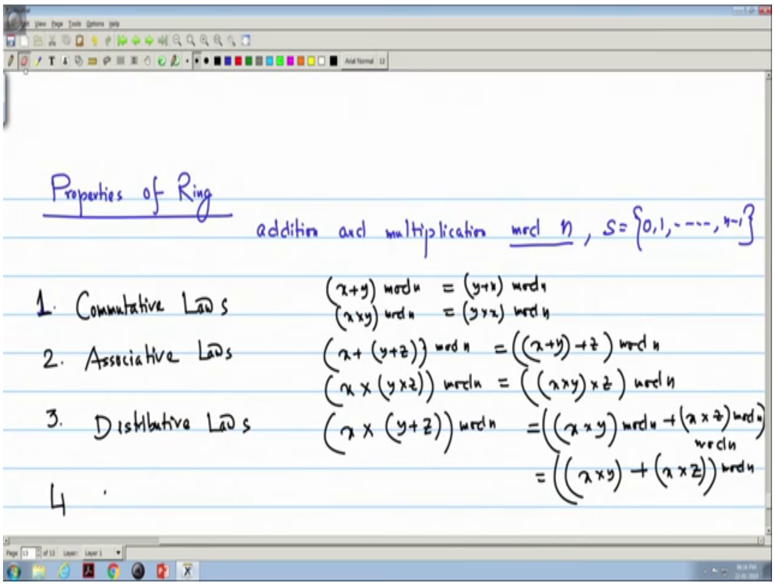
So, we have seen the additive modulo 0, because it is 1 plus 7 modulo 8 is 0, 2 plus 6 modulo 8 is 0, 3 plus 5 modulo 8 is 0 modulo 8, 4 plus 4 modulo 8, 5 plus 3 modulo 8, 6 plus 2 modulo 8, 7 plus 1 modulo 8. So, additive inverse exists what earlier we have seen. What about multiplicative inverse? Since, we do not consider 0, because that we know that there is no 0 devisors. So, will multiplicative inverse does not exists.

Now, for 7 we get the multiplicative inverse 7, because 7 into 7 is the 49 and just now we have seen that 49 modulo 8 1, but for 6 it does not exist then for 5 it is 5 sorry this is there are a is this one. So, we are taking multiplicative inverse say 1. Now, I made some mistake we are taking multiplicative inverse of 1. So, multiplicative inverse of 1 is 1 only 1 into 1 modulo 8 2 does not exist, 3 it is 3 only, then 4 does not exist for 5 for 5 it is 5 only, for 6 there is no multiplicative inverse, for 7 the multiplicative inverse is 7.

And, we have already conclude earlier the conclusion we have made that if a is relatively prime with n; that means, for my 1 3 5 and 7, then only we get the multiplicative inverse. And, if they are not relatively prime; that means, my a if a and n are not relatively prime are not relatively prime, then multiplicative inverse does not exist. And, that is for a equal to 2 4 6, because 2 4 6 and 8 n equal to 8, they are not relative prime relatively prime, they have some common factor. So, it is there.

Now, these will give as the another algebraic system, it is called the field what will be talking in the next lecture. So, that means, if multiplicative inverse is there, but if we remember that when we have read the ring.

(Refer Slide Time: 32:00)



Properties of Ring

addition and multiplication mod n, $S = \{0, 1, ----, n-1\}$

1. Commutative Laws $(x+y) \bmod n = (y+x) \bmod n$
   $(x \times y) \bmod n = (y \times x) \bmod n$
2. Associative Laws $(x + (y+z)) \bmod n = ((x+y)+z) \bmod n$
   $(x \times (y \times z)) \bmod n = ((x \times y) \times z) \bmod n$
3. Distributive Laws $(x \times (y+z)) \bmod n = ((x \times y) \bmod n + (x \times z) \bmod n) \bmod n$
   $= ((x \times y) + (x \times z)) \bmod n$

4

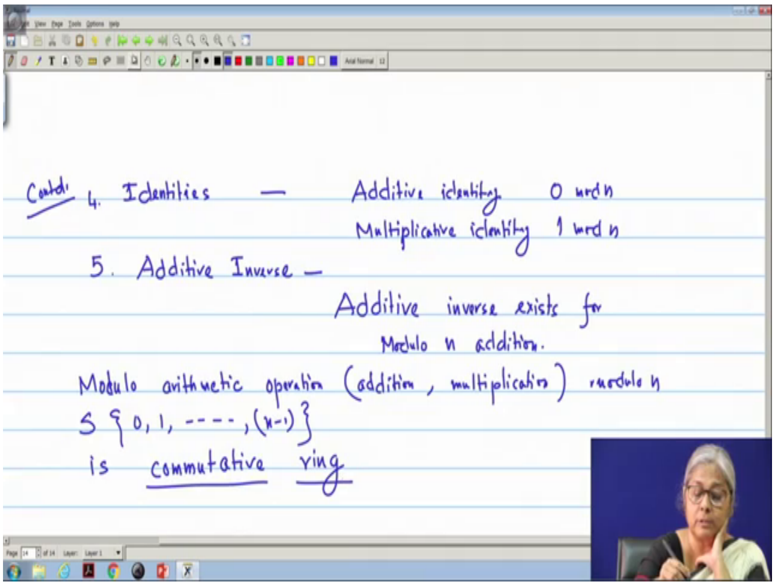
Now, if we see the properties of ring and properties of ring, what we have seen the when we have seen the ring that, if we consider the addition modulo addition um and the multiplication modulo 8, or some modulo operation modulo arithmetic the addition the operation is addition and multiplication modulo n I am writing modulo n then set; obviously, my set is my set is 0 to n minus 1 already we have discussed because remainder only, then what are the properties it holds, the first property holds is commutative laws ok.

So, the properties are commutative laws both for addition and multiplication that we know that if it is x plus n modulo n, we remember that x plus y modulo n is y plus x modulo n. And, same thing for multiplication x into y mod n is y into x mod n. Now, it is my associative laws.

We remember that now x y z we consider and we can write that x plus y plus z modulo n ok, equal to x plus y plus z modulo n. And, I can write x plus y into z modulo n is x into y into z modulo n. Now, my distributive laws we know the x cross y plus z modulo n that will be the x cross y modulo n plus x cross z modulo n mod n, or I can write together this mod n mod n, because it is same as that of if we remember the multiplication rule x this plus additive rule this is same I can take this mod n.

And, I can write x on that side also. So, if it is identities we go to the next we continue.

(Refer Slide Time: 36: 27)



Contd.

4. Identities — Additive identity 0 mod n

Multiplicative identity 1 mod n

5. Additive Inverse —

Additive inverse exists for Modulo n addition.

Modulo arithmetic operation (addition, multiplication) modulo n

S {0, 1, ----, (n-1)}

is commutative ring

So, if I take the identities already we have seen the additive identity additive identity 0 is 0 mod n and multiplicative mod multiplicative identity is 1 mod n and that exist because 0 and 1 always be the set now 4. So, this is my 4 and 5 is the additive inverse. So, what we have seen that additive inverse exists the additive inverse exists, when we have taken the modulo n operation modulo n addition exists for modulo n addition.

So, it is a ring or commutative ring. So, my modulo arithmetic modulo arithmetic operation.

The addition and multiplication 2 binary operations, the way the ring we have defined 2 binary operations and multiplication the modulo is a modulo n we are taking modulo n and the it is operated on set 0 1 to n minus 1, and it is a is a commutative ring. Because for multiplication also it is a it is commutative.

But, what we have seen the multiplicative inverse we cannot tell that for all the elements only those elements which are not relatively prime that it is they are inverse exists, but if they are relatively prime; that means, common factor exist between a and n, then no multiplicative inverse exist.

And, this particular property when we will consider, then it becomes a new algebraic system call the half field. So, next lecture we will discuss read about the algebraic system field; that means, we will see that when multiplicative inverse that property is satisfied when and how we can form that type of algebraic systems and their properties. So, with this we end our discussion on the modular arithmetic operations.