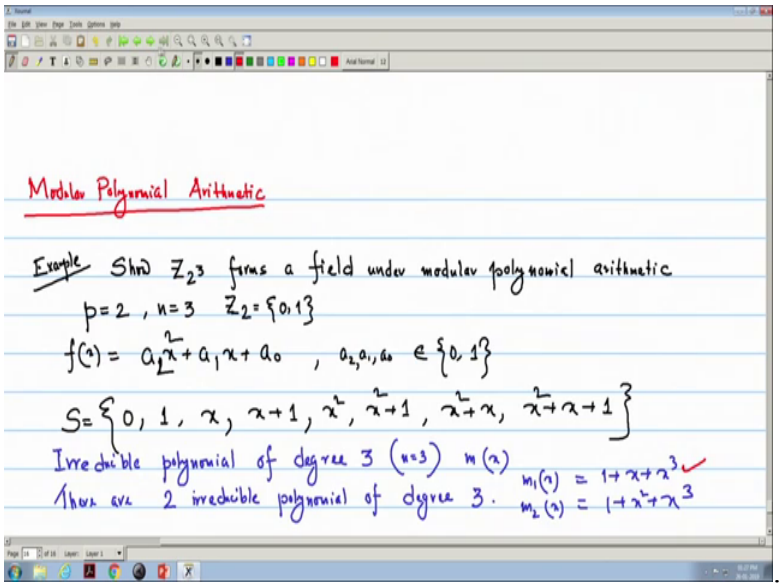
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 60
Finite Field and Applications (Contd.)

So, we are discussing about modular polynomial arithmetic and in the last lecture we have seen that how Z p to the power n forms a field under modular polynomial arithmetic. We will continue with this lecture with another example since we started our discussion with an example that Z 8 forms a ring, but not a field because under Z 8 multiplicative inverse does not exist. We have seen Z 7 because 7 is a prime number so, it forms a field.

Now, this example will show that Z 8 under normal modular arithmetic it does not form a field, but Z 8 under modular polynomial arithmetic it forms a field and will show this thing.

(Refer Slide Time: 01:20)



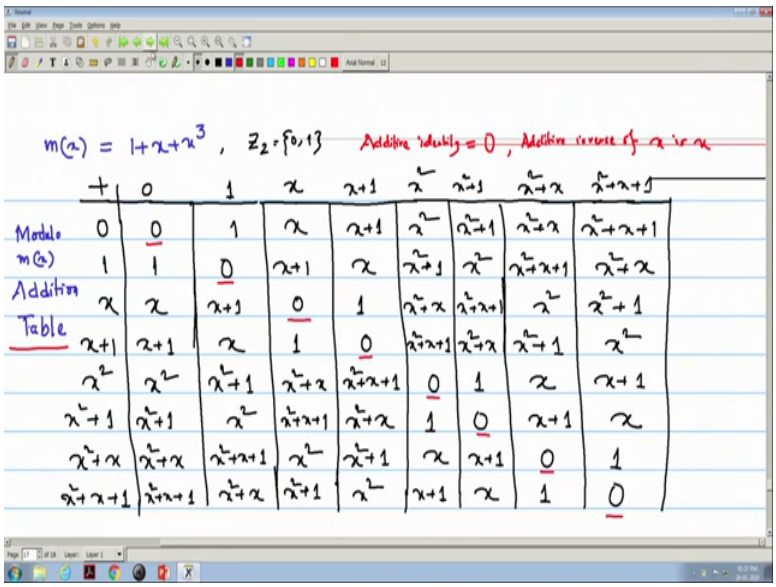
So, we continue our discussion on Modular Polynomial Arithmetic. So, we here; we have to; we are considering the example; example of we are taking it is Z 2 to the power 3 because we want to show Z 2 to the power 3 Z 8 forms a field under modular polynomial arithmetic. So, first we have to take the set of polynomials.

Again what are the; we see the set of polynomials since it is p to the power n, p equal to 2, n equal to 3; p equal to 2 is p is Z p is 0 and 1 because it is Z 2. So, we write it is Z 2 is 0 1 1, n equal to 3. So, the polynomials are f x is of the form a 1 x square a 2 x square a 1 x plus a 0 and earlier we have seen already this set of polynomials S; if I consider the set of polynomials S equal to 0, 1, then x, x plus 1, then x square, x square plus 1, x square plus x earlier one example we have seen that already we have read this part that how we get the full set of polynomials, because this is nothing but all possible combinations of a 2, a 1, a 0 where a 2, a 1, a 0, a 2, a 1, a 0 all are elements of 0 and 1; Z 2.

So, now this is my set of polynomials and we have to show that under a modular polynomial arithmetic this thing so, I need a polynomial irreducible polynomial. So, what is my irreducible polynomial; m x we have last class we have defined a irreducible polynomial of degree 3 here because my degree n say n equal to 3 for this example. Now there are 2 irreducible polynomial m x. There are 2 irreducible polynomial of degree 3; of degree 3 and they are I can write one is m 1 x what is 1 plus x plus x cube, another I can write m 2 x is 1 plus x square plus x cube. So, I have to choose any one of this.

Let we will choose the m 1 x; we consider m 1 x and we start to form the addition table and the multiplication table.

(Refer Slide Time: 07:02)



So, first we formed our modular; the first we our m x we have chosen m x is 1 plus x plus x cube I write later, since I have polynomial 0, then I have polynomial 1, I have

polynomial x, I have polynomial x plus 1, I have polynomial x square, then I have polynomial x square plus 1, I have polynomial x square plus x and x square plus x plus 1 these are my 8 polynomials.

First I do the addition and we are considering the m x is 1 plus x plus x cube, now I have 0, 1, x, x plus 1, these are my elements of the sets the all polynomials x square plus 1, x square plus x and x square plus x plus 1. So, here I have to do modular addition. This becomes 0, 1, x because already we have seen additive identity is 0, x plus 1. So, we will be getting the polynomial only, x square plus 1, x square plus x, x square plus x plus 1, if it is 1 plus 0 1 plus 1 modulo 2 since my it is Z 2 is 0, 1 so, modulo 2 addition. So, this becomes 0, this becomes x plus 1, this is x, x square plus 1, this is x square, because 1 will vanish, this becomes x square plus x plus 1, this becomes x square plus x.

If I add x this becomes x plus 1, 0, 1, x square plus x, then x square plus x plus 1, then x square, then x square plus 1, x plus 1, x no x will vanish because x plus x 0 again this becomes 0, then x square plus x plus 1. Now x plus 1 plus x square plus 1 means 1 will vanish; x square plus x, x plus 1, x will vanish; x square plus 1 and this becomes x square, first against the similar way I can compute the sum this becomes 0, this becomes 1, this becomes x, this becomes x plus 1, because x square plus x square 0.

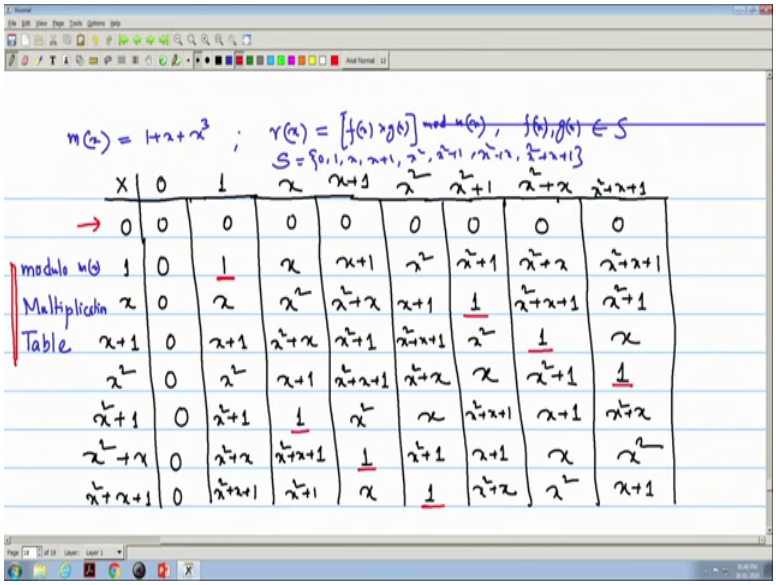
This is x square plus 1, this is x square, this is x square plus x plus 1, then this is x square plus x, this is 1, this is 0 and this is x plus 1 and this is x. Now if I add x square plus x x square plus x plus 1, then x square, then x square plus 1 because x will vanish, now x, then x plus 1, then x square plus x; x x will be 0, x square plus x this will be 1. Now x square plus x plus 1, x square plus x, x square plus 1, now x square, now this becomes x plus 1, now this becomes x, this becomes 1, this becomes 0.

So, we observe some properties here; see the first thing is all the rules if I consider that the consists of all the elements of the set every row; that means, 0, 1, x, x plus 1, x square, but in different order it is there. Now we see the additive identity 0 plus 0 0, 1 plus 1 0, x plus x 0, because we are taking the modulo 2 sum. So, additive inverse exist, if it is first thing is this is additive identity. So, I write additive identity is 1 sorry additive identity is 0 and additive identity that is 0 and then if I take the see additive inverse there must be additive inverse. So, I get 0 plus 0 0, 1 plus 1 0, x plus x 0; that means, additive inverse is the element itself. So, additive inverse of x is x itself; is x.

And see this is a closure property, because already we have seen that that table contents only the set of elements of S only those polynomials. And since I want the additive identity 0 and additive inverse and again it will be associative and closure, then commutative, all the properties will be satisfied. So, under modulo addition that modulo m x addition; it satisfiy all the property. Now if we consider the modulo multiplication. So, we write that this is our addition modulo, addition table modulo m x addition table.

Now, we consider the multiplication table.

(Refer Slide Time: 17:01)



So, I consider multiplication I have 0, 1, x, x plus 1, x square, x square plus 1, I have x square plus x, and I have a x square plus x plus 1 the all set of polynomials. Then I have 0 same 0, 1, x, x plus 1, x square, then x square plus 1 and I have x square plus x and x square plus x plus 1.

Now, I write my m x because this time I have to take r x m x equal to 1 plus x plus x cube and I have to do here since it is multiplication. So, I have to take the r x which is f x into g x modulo m x and here my f x and g x is belongs to S, where S is the set of all these polynomials. So, S 0, 1, x, x plus 1, x square, x square plus 1, x square plus x and x all 8 polynomials x plus 1.

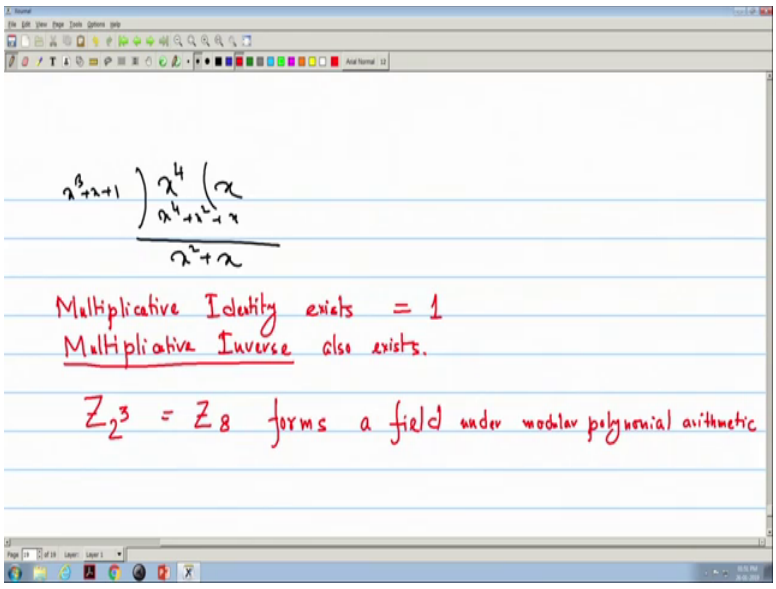
Now, if we do the multiplication modulo m x then 0 so, it will be 0 only, because 0 multiplied by any polynomial it will be 0. Now it is multiplied by 1 only so, the

polynomial itself. If I multiply with x; now this time I if the degree of the product polynomial is more than the; more than 3 then I have to take the remainder. So, x into 0 is 0, x into 1 is x, x square so less than x cube so, x square I put this is x square plus x, this is x cube, now it is x cube so, I have to take the remainder. So, that mean x cube divided by 1 plus x plus x cube and we have seen that is nothing but x plus 1.

Now, again x into x square plus 1. So, it is x cubed plus x, x cube plus x and this is x cube plus x is there so, it will be 1 only. Similarly x cube plus x square so, now, if I divide x cube x square so, this becomes x cube will vanish, but x square plus x plus 1, now this becomes product is x cube plus x square plus x so, this will be x square plus 1. So, I now I have to take the remainder. So, similarly if I now compute that this will be 0, this is x plus 1, now x square plus x, now x plus 1 into x plus 1, earlier we have seen this is x square plus 1 if I multiply and then take modulo m x then this is x square plus x plus 1, it is x square, then it is x plus 1 into this, this becomes 1 and this becomes x only.

Similarly we can for x square x square into 1 is x square this is x cube. So, divided by this; these becomes x plus 1 again x plus 1 into x square. So, x cube plus x square x cube plus x square I can do the divided by this so, x square plus x plus 1 x square plus x plus 1. Now, x 4 x to the power 4 if I divide then x 4 plus x square plus 1 so, this becomes x square plus x. We can do quickly here that x square and if it is x to the power 4.

(Refer Slide Time: 23:59)



Just if I see that x to the power 4 and I divide it by x cube plus x plus 1 so, it will be x only so, x to the power 4 plus x square plus x so, this becomes x square plus x; so we write x square plus x. Now similarly if I do the this one it becomes x it is x square plus 1 and this becomes 1.

Now, this is 0, this is x square plus 1, this is x cube plus x so, this becomes 1, now this becomes x square, this is x, this is x square plus x plus 1, now x plus 1 and this becomes x square plus 1 into this; this becomes x square plus x. Similarly this becomes 0 x square plus x now x cube plus x square so, this becomes x square plus x plus 1, now this is 1, this becomes x square plus 1, this is x plus 1, now x and this becomes if I multiply it will be getting x square modulo m x we are taking.

Now, this is 0, this is x square plus x plus 1, now this is x square plus 1 because if I multiply x cube plus x square plus x so, x and x cube will go x square plus 1. So, this becomes x, this becomes 1, x square plus x, this becomes x square and this becomes x plus 1. Now again if we observe the properties first other than 0; other than 0 elements we see that we have the 1 multiplicative identity in each row; that means, for all elements I am getting 1; multiplicative identity is there and again here also we see that for each the every row if we observe that all the elements appear in each row; that means, for every multiplication modulo m x for one element we are getting all the set of full set of elements.

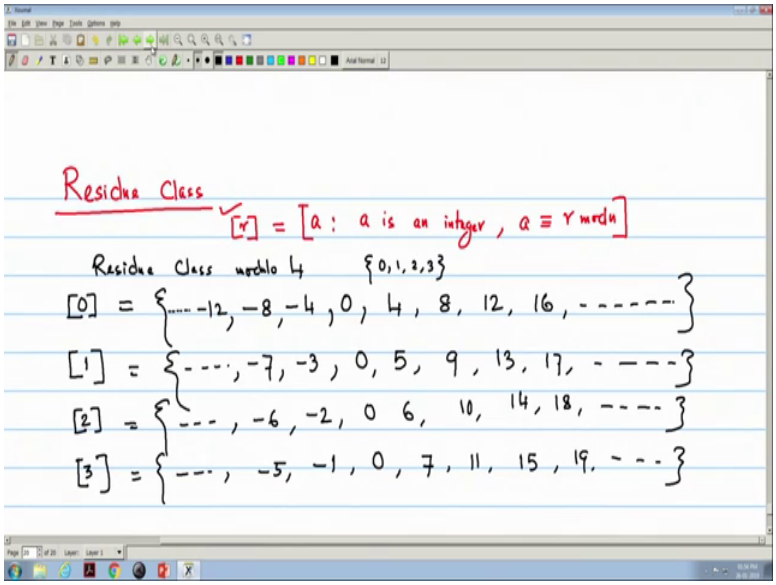
So, multiplicative identity is there we write this thing is the modulo m x multiplication table. So, what we observe that first is multiplicative identity exists and that is equal to 1 and we get also multiplicative inverse. Since for each element we are getting multiplicative inverse like if we see that say for 1 it is 1 for x multiplicative identity is x squared plus 1, for x plus 1 multiplicative identity is x square plus x because x x plus 1 in terms of it is 1.

So, we will be getting the multiplicative identity and if we remember that for under modulo m x multiplication we will see also that it is a closure since all the set full set of elements which we have seen that all the elements are under S. So, it is a closure property then associative under because it is polynomial multiplication that already we have seen and now we see that it is and again since it is multiplication of polynomial. So, commutative also now multiplicative identity exists and multiplicative inverse also

exists. So, mainly multiplicative inverse is there; so it is integral domain now it is inverse is there so, it forms a; this forms a field.

So, what we see that Z 8; that means, Z 8 forms a field under modulo under modular polynomial arithmetic. Now we can see the how we can get the you can find the GCD also by this method, since we know that GCD a b equal to 1; that means, there will be no factor; we can use that thing. Now another thing is we or sometimes we use in many applications it is called the residue class.

(Refer Slide Time: 30:44)

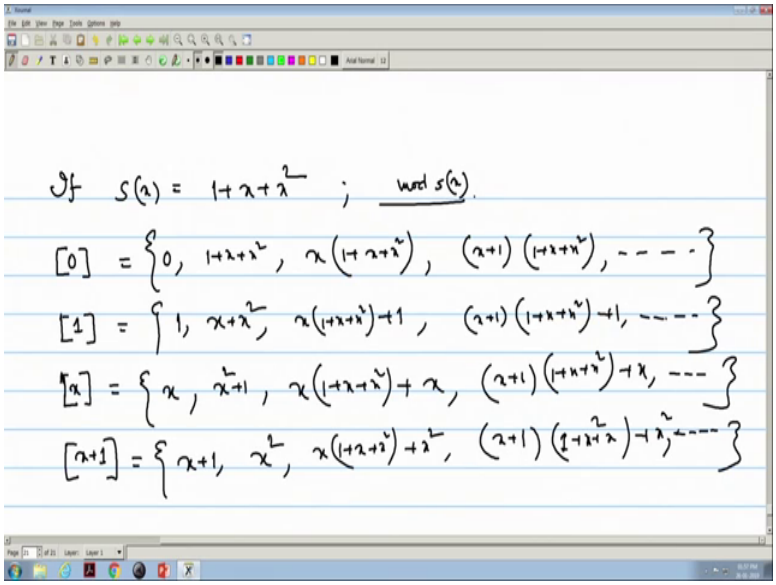


For particularly for modular arithmetic this is very important so, we just do that thing residue class see if it is defined normally that we here mainly that modular arithmetic we use the remainder.

So, we can write this that as if a, when a is an integer; earlier we have defined and a is congruent to r modulo n. So, we can write all r's whose remainder is same a is congruent r modulo n so, we can define this as a residue class. So, quickly if I just see; that means, if we take residue class modulo 4; if I consider residue class modulo 4, then I can write modulo 0 or class 0 this will be say if I start with 0 then 0, 4, 8, 12, all the elements I will be getting that are multiple of 4. I will be getting that remainder 0 and here negative also I will be getting minus 4, minus 8, all these elements I will be getting.

So, this is my set; now if I consider since modulo 4 means I have only set 0, 1, 2, 3. So, it is 1; if I write then similarly I can write it will be 5, 4 plus 1 9, 13, 17, like that and similarly here minus 3, minus 4, plus 1, minus 7, etcetera and I give 2; then it is minus 6, minus 2, 0, 6, 10, 14, 18, I again I add and 3; I will be getting similar way minus 5, minus 1, 0, 7, because 7 modulo 4 is 3, then 11, 15, 19 in this way.

(Refer Slide Time: 33:52)



Now, when I am taking the polynomial this same thing we can do that if say if my S x is 1 plus x plus x square then I can write because I am taking the modular S x. So, I can write similar way that this 0 is I take the set it is 0, 1 plus x plus x square, then x into 1 plus x plus x square this will be the multiple of 1 plus x plus x square and my set is x x plus 1. So, in this way I will I will be getting similarly if it is 1 we have to add 1 just the way we have done 0 plus 1, 1.

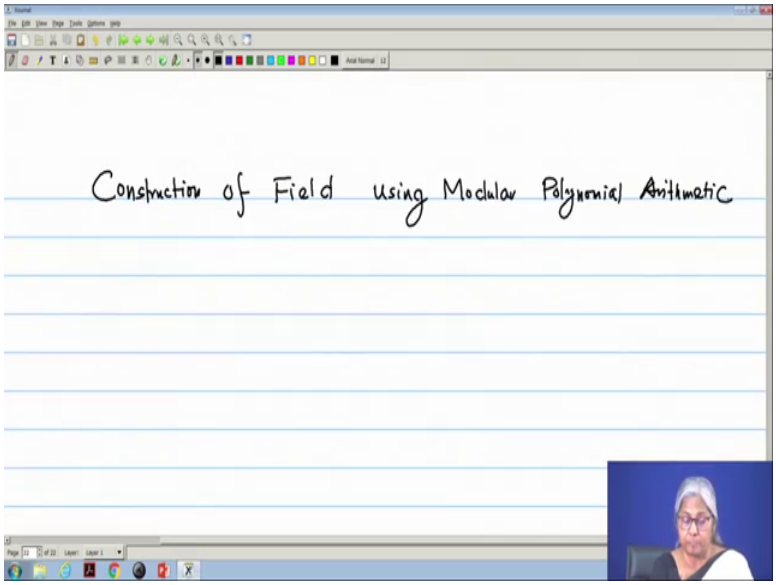
So, 1 plus x plus x square this become x plus x square now, these x into 1 plus x plus x square plus 1, then this is x plus 1, into 1 plus x plus x square, plus 1 in this way we will be getting. And if I continue I can get this is 2 then it is sorry this is 0 1 x sorry this is polynomial we are taking. So, this is I have to take the x. So, this becomes x, now 1 plus x plus x square this become x square plus 1, then this become x into 1 plus x plus x square plus x, this becomes x plus 1, into 1 plus x plus x square, plus x and so on.

So, similarly in this way I can the I can form this residue class and it is of very important when I have we do some applications and application area particularly in cryptography

we use and coding theory also we use this thing. So, we can write the totally similar way only the we are considering the polynomial is modulo S x we are doing.

So, here we are doing the modulo S x. So, in this lecture what we see that how we can form the finite field and even that it is normal modular arithmetic it is not a field, but using modular polynomial arithmetic it forms a field.

(Refer Slide Time: 37:06)



So, actually this lecture we have mainly considered the construction of field using modular polynomial arithmetic and there mainly we have used some of the some concepts irreducible polynomials as if a like a prime and we have taken the remainders when or the residues now I can take because just now we have defined the residue class. So, residues when it is divided by that irreversible polynomial; result is divided so, we have taken.

So, with this we finish our finite field and these applications of finite field lectures and with this finite field lecture also we actually our discrete mathematics class ends here. I hope that some I have tried to explain the basics of discrete mathematics and it will be of use and particularly in computer science and mathematics other branches also that how it will be used, how the basic mathematics; the discrete mathematics is used. So, this class will be useful to understand all those things.

Thank you.