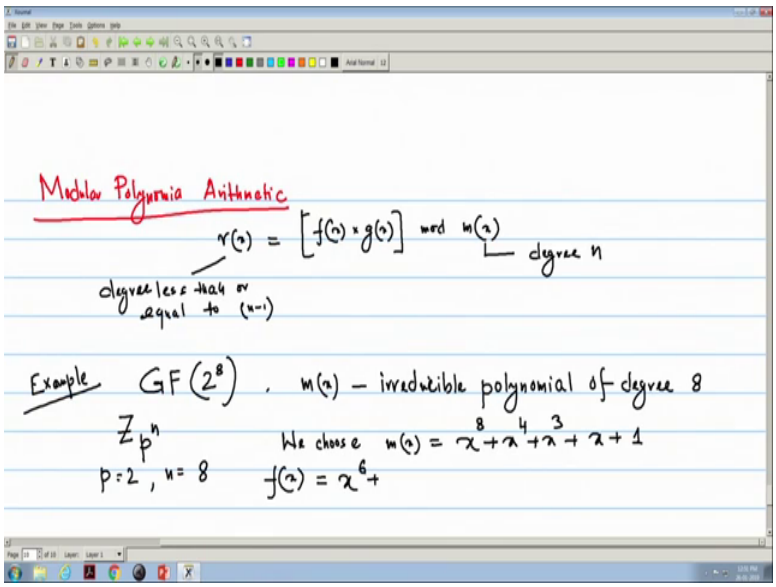
Discrete Structures
Prof. Dipanwita Roychoudhury
Department of Computer Science & Engineering
Indian Institute of Technology, Kharagpur

Lecture - 59
Finite Field and Applications (Contd.)

So, in the last lecture we have seen that how that some polynomials we get. And we can do or we can perform computation or under modular polynomial arithmetic. Now our main objective is that how one field can be constructed under modular polynomial arithmetic. Even that normal modular arithmetic that is not a field and Z 8 and Z to 2 to the power 3 is the example we have given.

(Refer Slide Time: 01:05)



So, we continue our lecture on modular polynomial arithmetic. And then mainly if I summarize the last lecture what we have read, we have 2 polynomials f x and g x and if I divide that thing by a irreducible polynomial of degree n. And we get the remainder r x then we will be working on this set r x because r x is of degree n minus 1.

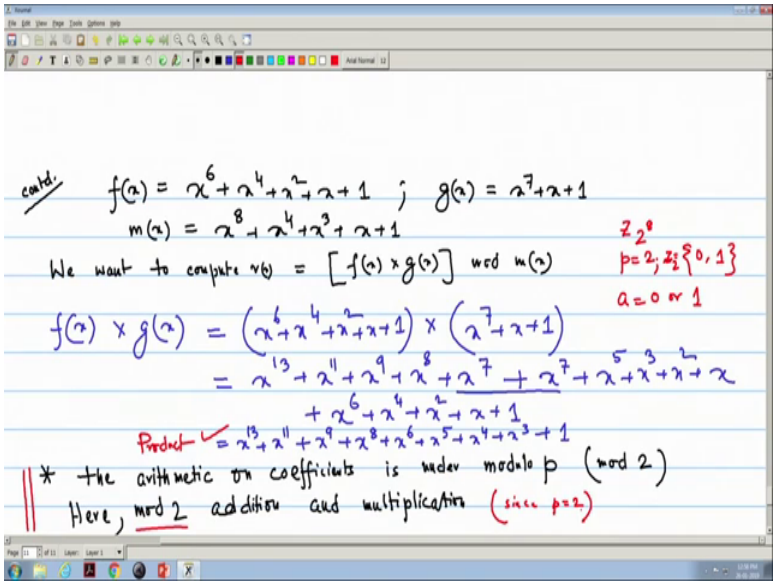
Since, m x m x has degree n irreducible polynomial. So, r x must be less than n; that means, less than or equal to n minus 1, degree less than or equal to n minus 1. So, first we see one example or that how we do this a division, because in previous lecture we have seen that addition and multiplication and subtraction. So, now, we see the how we

can divide and take the remainder. So, we are taking one example, where we choose the irreducible polynomial, where we work in it is of Galois Field of GF 2 to the power 8.

So, we have to take a m x is an irreducible polynomial of degree n; that means, here n equal to 8 p to the power n. So, polynomial of degree 8, because we told that we are forming the field g f p to the power n. So, p equal to 2 n equal to 8 ok. So, first we choose the m x. Now, there are many irreducible polynomial of degree 8, we choose here one very popular irreducible polynomial of degree 8 normally this is used in the standard algorithm of AES in cryptography.

So, we choose m x equal to x to the power 8 plus x 4 x to the power 3 plus x plus 1. This is one of the irreducible polynomial; there are many irreducible polynomials of degree 8. So, we take one irreducible polynomial here. And, we take f x now we have 2 polynomials was less than degree less than 8.

(Refer Slide Time: 04:58)



So, let f x equal to x to the power 6 take that polynomials f x equal to x to the power 6 plus x to the power 4 plus x square plus x plus 1 and g x is x to the power 7 plus x plus 1.

We remember that my m x again I repeat m x is x to the power 8 plus x to the power 4 plus x cube plus x plus 1. Now, we have to do f x into g x modulo m x. So, first we multiply because we want to compute since we are doing the modular polynomial arithmetic.

So, we want to compute r x, which is equal to the f x into g x modulo m x. So, first we have to multiply. So, we multiply f x into g x see f x is x to the power 6 plus x to the power 4 plus x square plus x plus 1 and x to the power 7 plus x plus 1. So, if I just multiply. Normal multiplication this is so, x to the power 13, if I multiply with x to the power 7 plus x to the power 11 x to the power 9 x to the power 8 plus x to the power 7.

Now, I write in the x term that x to the power 7 plus x to the power 5 plus x cubed plus x square plus x 1 is left. So, 1 into this means the f x only so, x to the power 6 x to the power 4 x squared plus x plus 1.

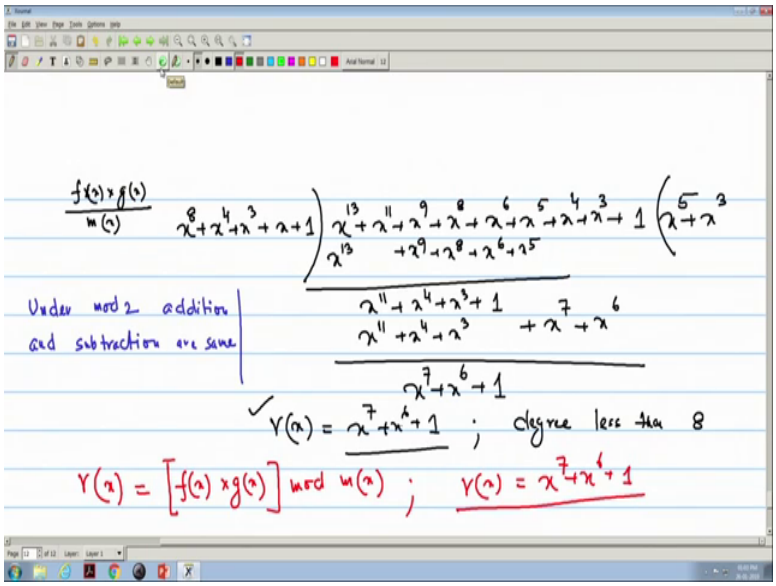
Now, see the coefficients are either 1 or 0, because that it is we are considering 2 to the power 8; that means, my p is 2 if we remember my field is I am taking Z 2 to the power 8. So, my p equal to 2; that means, thus it will be in 0 and 1 Z p is Z 2. So, Z 2 is 0 Z 2 is 0 or 1. So; that means, my coefficients can be either; that means, my a can be either 0 or 1. Now, if I take since it is Z 2 so, the my addition will these computation will be coefficients when will be taking.

So, one thing we remember the coefficients or the arithmetic on coefficients is under modulo p; that means, here modulo 2; that means, mod 2 addition and multiplication will be doing.

So, here I will be doing here it will be modulo 2 addition and multiplication. So, what will happen; that means, if I take it will be x to the power 13 will be there x to the power 11 x to the power 9 x to the power 8, but see x to the power 7 and 7 since 1 plus 1 is 0. So, there will be no x to the power 7 term because it is modulo 2. So, 2 plus 2 modulo 2 is 0. So, there will be no x to the power 7. Now, x to the power 6 x to the power 5 x 4 x cube. Now, again 1 x square and x, so, 2 x square and 2 x so, it will be 0 so, only 1.

So, my this is my the product. So, my product is so, my this is my product is 1 plus x cube plus x 4 plus x 5 plus x 6 x 8 x 9 11 x to the power 11 and x to the power 13, and we remember that the coefficients the arithmetic we are following for coefficients, then that is modulo 2 addition and multiplication since peaced we here modulo 2 since oh details since p equal to 2.

(Refer Slide Time: 11:24)



Now, we have to divide. So, we if I divide by m x now I have to do f x into g x divide by m x, because r x is the remainder we have to take. So, if I do that thing we remember our m x is x to the power 8 plus x 4 plus x cube plus x plus 1. Now, we divide and my product f x into g x is x to the power 13 x to the power 11 x to the power 9 x to the power 8 x to the power 6 5 x to the power 4 plus x cube plus 1.

So, now polynomial I have it is 8 and thirteen. So, if I multiply by 5 my quotient is 5 then I can get x to the power 13 see 4 plus 5 I have x to the power 9. So, I have I write since I have 1 x to the power 9 term. So, I can write here x to the power 9, then x to the power 8, I have I have x to the power 6 also and I have x to the power 5. So, then this is normal addition and since under modulo 2 addition the addition and subtraction are same. So, that is why we are not using any minus sign, we write that under modulo 2 addition and subtraction are same. So, we are not using any minus sign.

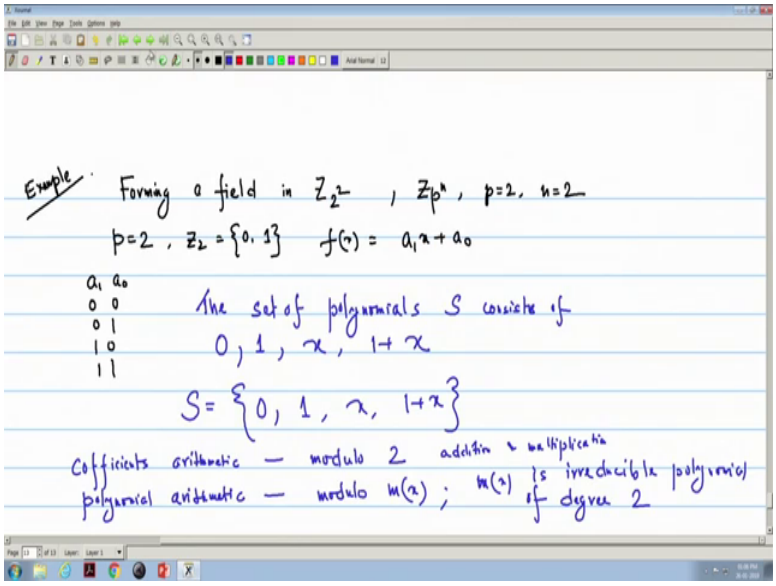
So, it is only x to the power, it is only x to the power 11. Then this will all cancel out then x to the power 4 plus x cube plus 1. So, since x to the power 8, so, I can take x to the power 3. So, it will be x to the power 11 then see x to the power 7. So, I do not have any x to the power 7 term. So, I write x to the power 7 here x to the power 6 I do not have an x to the power 6 term, then x to the power 4 I write x to the power 4 then x cube. So, again if I give I get x to the power 7 x to the power 6 plus 1.

Now, see that m x is of degree 8 and I get some remainder r x. So, this is my r x I get some r x equal to x to the power 7 plus x to the power 6 plus 1 whose degree less than equal to degree less than 8 degree less than 8; that means, the degree of m x 8 is the degree of m x. So, this is my this is the how we can form the remainder. So, this is modular polynomial arithmetic.

So, now, we can use instead of this; that means, my what it becomes that I can write that r x I compute r x is f x into g x modulo m x and I got this for these f x and g x value the here my r x is I am getting r x is x to the power 7 plus x to the power 6 plus 1.

So, the similar to my polynomial arithmetic I normal modular arithmetic I got the modular polynomial arithmetic. Now, we will be using this thing to form a field ok.

(Refer Slide Time: 16:25)



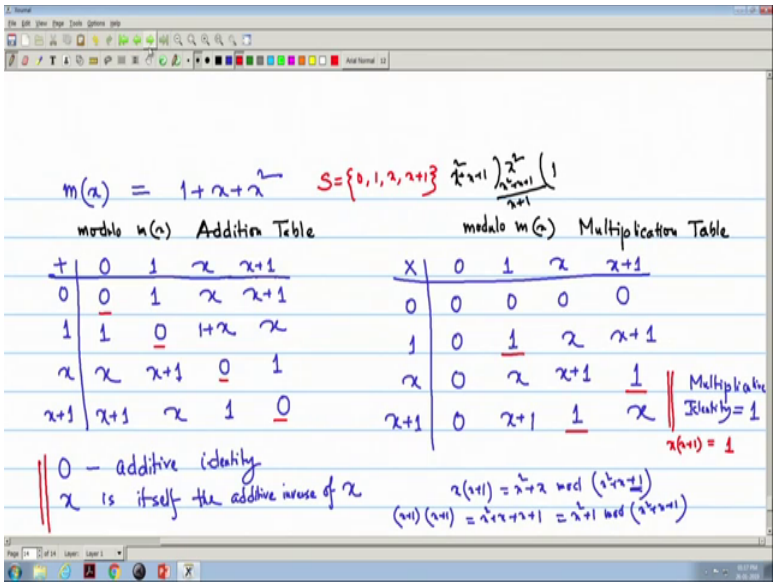
Now, we take our p is 2 and a 2 degree polynomial we take; that means, Z we take one example and how we can example that forming a field in Z 2; that means, when we are telling Z p to the power n that p equal to 2 n equal to 2.

So, again first we see what are the polynomials? Because, p equal to 2 means it is in Z 2 Z 2. So, that is 0 and 1 coefficients can be only 0 and 1 and it is n equal to 2. So, my polynomial is f x is a 1 x plus a 0 only 2 values we know that all possible values of a 1 and a 0; that means, a 1 a 1 is 0 can take 0 0 0 1 1 0 1 1 these are the 4 values, the way we have represented. So, my f x I can directly write that f x the set of f x better I write

the polynomials the set the set of polynomials is consists of the of the polynomials 0 0 means 0, then 0 1 which is 1, then x and 1 plus x.

So, these are the this is my polynomial set; that means, S is 0 1 x and 1 plus x. So, these are my 4 polynomials now we remember that when will be coefficients for coefficients arithmetic will be for coefficients arithmetic, that it is the under modulo 2 addition, because modulo 2 addition, and multiplication and multiplication, and for the set of polynomials. For polynomials arithmetic we will be considering, for polynomial arithmetic will be considering modulo m x where here is this is of since they are less degree 1. So, m x is of modulo m x m x is irreducible polynomial of degree 2.

(Refer Slide Time: 20:00)



So, if we just do that thing that we know that for degree 2 there are only 2 irreducible polynomials. I take 1 plus x plus x square m x equal to I take this is 1 irreducible polynomials. Now, if we do the addition and modulo addition and multiplication table. So, if I consider addition and multiplication table. So, this is modulo m x addition table I have 0 1 x and x plus 1, these are my 4 polynomials 0 1 x and x plus 1 4 polynomials I am doing modulo addition.

So, 0 plus 0 it is 0 0 plus 1 1 x x plus 1 simple modular and simple polynomial addition 1 plus 0 1. Now, 1 plus 1 2 and this is this becomes 0 because it is modulo 2 addition, so, it is 0. Now, 1 plus x, now 1 plus x plus 1 so, x plus 1 plus 1 2 because coefficient arithmetic is modulo 2 so, this becomes x because 1 plus 1 cancelled. Then x plus 0 x x

plus 1 x plus 1 x plus S again it will cancel, then x plus x plus 1 this becomes 1 x plus 1, then this is x this is 1, this is 0.

Now, we see 0 plus 0 0 1 plus 1 that is 0 x x plus x 0 x plus 1 plus x plus 1 0 and 0 is the additive identity. So, 0 is additive identity and x is itself the additive inverse said the additive inverse of x, additive inverse of x. Now, if I consider modulo m x multiplication ok. So, we consider now modulo m x multiplication table.

Now, for multiplication if the product becomes the degree is greater than the n, here it is 2 1 multiplication table then we have to divide by this irreducible polynomial m x and we have to take the remainder. So, again if I do the table 0 1 x and x plus 1, here if I give the modular m x multiplication, I will take 0 1 x and x plus 1. So, 0 if I multiply the coefficients so, it will it will be non-arithmetic modulo 2. So, it will be 0 only 0 only 1 if I multiply then the number itself, so, 1 into x x 1 into x plus 1.

Now, x into 0 this will be 0 x into 1 this is x. Now, x into x this becomes x square now see I do not have any x square in this element. Because, that my if I remember the that my set my set was S S was 0 1 x and x plus 1 I do not have an x square, because the degree 2 is greater than this m x has degree 2. So, I have to divide x square by 1 plus x plus x square. And, if I do that thing just you we will be getting that, if I divide x square, if I divide x square by 1 plus or x square plus x plus 1 m x, then I will be getting 1 and this becomes x square plus x plus 1. So, remainder is x plus 1.

So, I will be giving this remainder instead of x square I will take the remainder this is x plus 1 that is modulo m x we are doing. Similarly, if it is x square plus 1 and now we we we understand that if I divide by it is x square plus x plus 1. So, simply the x square plus 1 will go. So, this becomes x. Similarly, now it is 0 it is x plus 1 and here x into x plus 1 is x into x plus 1 is x square plus x and if I take modulo x square plus x plus 1 my m x, then if I divide simply x square plus x and x square plus x will vanish so, it will be 1.

And, now if I multiply x plus 1 into x plus 1, then x plus 1 into x plus 1 this becomes x square plus x plus x plus 1 is x square plus 1 again this is degrees more. So, I have to take modulo x square plus x plus 1 and then x square plus 1 will go and x I will get.

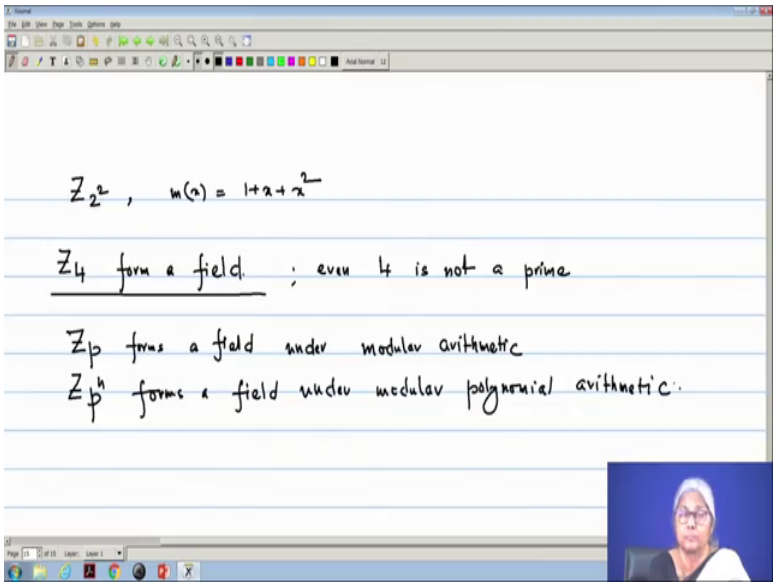
Now, we see that if here it was multiplicative identity sorry additive identity was 0. Here, we see that other than 0 the way we have defined, we have for 1 we got multiplicative

identity 1, for x x x square this will be this will be 1, because x square plus x the 1 will be there one. So, I get multiplicative inverse identity 1 here also I get 1.

That means here my additive identity it was there. And, similarly here I get my multiplicative identity I get multiplicative identity for all elements other than 0 exist and that is equal to 1. So, I have multiplicative inverse for all element other than 0, because I am getting 1 for 1 multiplicative inverse is 1, for x multiplicative inverse is x plus 1, for x plus 1, multiplicative inverse is x, because x into x plus 1 equal to 1. Since, I can write for x x into say x into x plus 1 equal to 1. So, multiplicative inverse of x is x plus 1 or the diverse multiplicative inverse of x plus 1 is x and for 1 it is 1 only.

So, what we see that the inverse exists so; that means, it will now it forms a it will form a field.

(Refer Slide Time: 30:18)



So, I can conclude that, we have taken Z p to the power n Z 2 square and the irreducible module m x we have taken 1 plus x plus x square, this is important because selection of different irreducible polynomial will give a different results. And, but it will that it Z 2 square what we see that Z 2 square means Z 4. See, is it is not a prime Z 2 square it is 4 is not a prime still Z 4 forms a field. A when we have converted this is the this operation in modular or computation is modular polynomial arithmetic. And then Z 4 just now what we seen even the 4 is even 4 is not prime.

So, what earlier we have seen that in normal arithmetic normal modular arithmetic if only Z p Z p forms a field is not a prime. But, we have so, we have now we take that Z p Z p earlier we have seen from say field under normal modular arithmetic. And, what Z p to the power n forms a field under modular polynomial arithmetic. So, this is the conclusion that we make that Z p to the power n forms a failed. We will continue this lecture with some example the we started in the next class.