

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

Lecture - 58
Finite Field and Applications (Contd.)

So, we are discussing the Finite Fields and their Applications. And, mainly how we can construct a finite field? So, today we will continue that lecture on that polynomial arithmetic, as we have read the last lecture that polynomial addition, subtraction, multiplication, and then finally, how again we are able to do the polynomial division. So, once the we can do the polynomial division; that means, multiplicative inverse exist over Z_p today we will see that modular polynomial arithmetic, how they govern to make or to construct some field.

So, first we will read them modular polynomial arithmetic.

(Refer Slide Time: 01:11)

Modular Polynomial Arithmetic

Z_p , p is a prime
 Z_p forms a field under modular addition and multiplication
then Z_{p^n} also forms a field, n is integer.
 Z_8 does not form a field since multiplicative inverse does not exists
 Z_7 forms a field.
 $8 = 2^3$ p^n form. $p=2 \vee n=3$
 Z_{2^3} becomes a field.

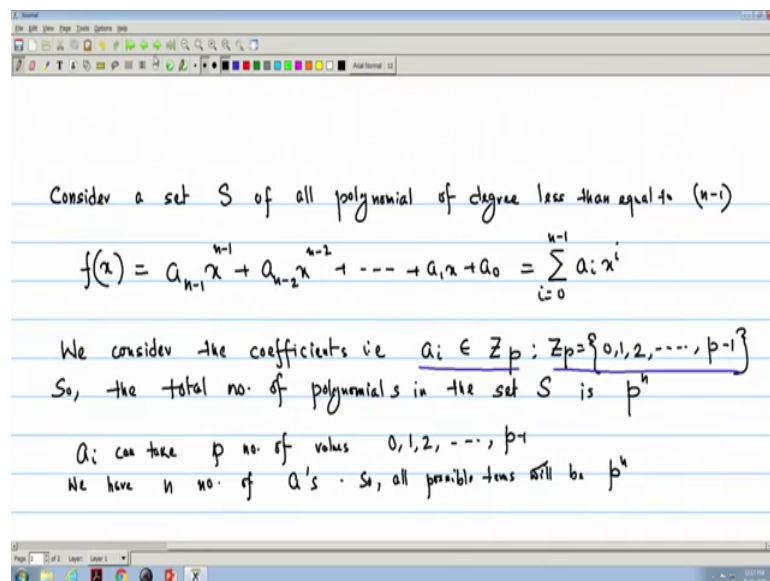
So, if we remember that the example we have done that, first we have taken the field of field we have done Z_8 and we have seen that is not a actually that is not a field. If whenever the all properties we have studied, but if we do the operation on modulo 7, it has it becomes a field. And we concluded that actually the if we take the field the field is Z_p , where p is a prime and the modular arithmetic operations and modular addition and multiplication.

Now, if Z_p is a Z_p forms a field under modular addition and multiplication, then Z_p to the power n also forms a field. Here p is prime and n is some integer n is positive integer. Now, if we remember that whenever we have done the Z_8 , that we have studied the properties we have seen that Z_8 does not form a field. It is a ring, but since multiplicative inverse does not exist for all elements of Z_8 whereas, Z_7 that is p equal to seven forms a field.

Now, 8 is 2 to the power 3. So, it is of p to the power n form p to the power n form where p equal to 2 and n equal to 3. So, just now we have seen that or we just mentioned that Z_8 is not a we have earlier read that thing also Z_8 does not form a field, but now we are doing that comments we are making that Z_2 to the power 3, how this becomes a Z_2 to the power 3 becomes a field becomes a field. And for that we will do the polynomial arithmetic or modular polynomial arithmetic. So, this is our intention of this lecture.

Now, first we will see that we consider a set of polynomials.

(Refer Slide Time: 05:21)

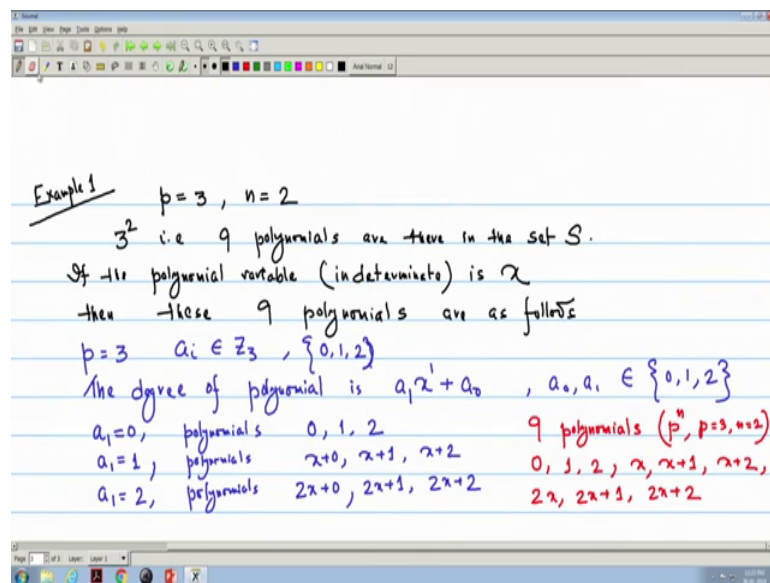


A set is of all polynomials of degree less than equal to n minus 1. So, we can write the polynomials we write $f(x)$ equal to $a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0$ and we can write i equal to 0 to n minus 1 $a_i x$ to the power i .

Now, we consider the coefficients the coefficients that is the value of i that is a i this belongs to $\sum \mathbb{Z}_p$; that means, we know we have defined \mathbb{Z}_p is 0 to p minus 1. So, the total number of polynomials in the set S is p to the power n since a can take p to the power n number of values, because each a_i a_i can take p number of values, a_i can take p number of values, that is 0 1 2 to p minus 1, because as we wrote that a_i belongs to \mathbb{Z}_p and \mathbb{Z}_p is 0 to p minus 1.

And see I have n number of coefficients a_0 to n minus 1. And so, if I consider as it places. So, we have n number of a 's, so, the total number of terms in the polynomial or all possible terms that will give 1 polynomial. So, all possible terms will be p to the power n ok. So, there will be p to the power n number of polynomials in the set. Now, we take some example.

(Refer Slide Time: 09:27)



We consider that p equal to 3 for example, 1 we consider p equal to 3 and n equal to 2.

So, p to the power n is 3 square; that means, 9 polynomials are there in the set S . So, if we consider the polynomial variable normally we call the indeterminate, if is x if the polynomial variable that is the indeterminate is x it is then, what are the polynomials then the these 9 polynomials these 9 polynomials are as follows see n equal to 2. That means, my a_i can be only 0 and 1 p equal to sorry p sorry p equal to 3. So, a_i will a_i belongs to \mathbb{Z}_p and \mathbb{Z}_p is 0 1 2.

So, a i can take value 0 1 2 and n equal to 2. So, the degree of polynomial will be n minus 1 polynomial is 1; that means, a $1 x$ to the power 1 plus a 0 . So, and this a 0 a 1 can take value from 0 1 2. So, if I take a 1 equal to 0 if a 1 equal to 0, then the first term will be 0 and a 0 can be 0 1 2. So, the polynomial the 3 polynomials we get the polynomials 0 1 2. Now, if I get a 1 equal to 1, because a 1 can take. So, for a 1 equal to 1 we get the polynomials x because 1 into x . So, x plus 0 x . So, I get x plus 0 x plus 1 x plus 2.

Now, a 1 equal to 2 the polynomials or $2 x$ plus 0, $2 x$ plus 1, and $2 x$ plus 2 so, these are my 3 9 polynomials. So, these 3 square because p to the power n . So, these 9 polynomials when for p to the power n , I write p equal to 3 n equal to 2. So, are 0 1 2 then x , x plus 1, x plus 2, then $2 x$ plus 1, $2 x$, $2 x$ plus 1, and $2 x$ plus 2. So, these are my 9 polynomials.

(Refer Slide Time: 14:33)

Example 2
 $p = 2$ and $n = 3$
 $p^n = 2^3$ i.e. there will be 8 polynomials in S .
 $p = 2, Z_p = \{0, 1\}$
 $n = 3$, The polynomial $f(x) = a_2 x^2 + a_1 x + a_0$
 $(n-1) = 2$

| | |
|-----------------------------|----------------|
| $a_2 = 0, a_1 = 0, a_0 = 0$ | $f(x) = 0$ |
| $a_2 = 0, a_1 = 0, a_0 = 1$ | $f(x) = 1$ |
| $a_2 = 0, a_1 = 1, a_0 = 0$ | $f(x) = x$ |
| $a_2 = 0, a_1 = 1, a_0 = 1$ | $f(x) = x + 1$ |

$a_2 = 0$

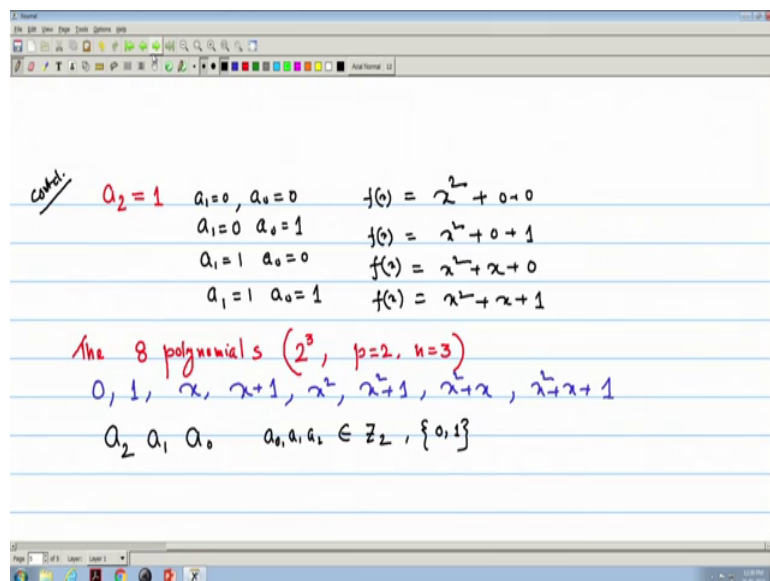
Now, if we consider another example, we consider another example 2; where we write p equal to 2 and n equal to 3. So, that since p to the power n so, is 2 to the power 3, that is there will be 8 polynomials in the set S . And what are those polynomials? Similarly, if I consider the indeterminate as x so, here p equal to 2. So, p equal to 2 that is Z_p will be only 0 and 1 because it is 0 to p minus 1 and n equal to 3. So, the degree of polynomial so, the polynomial if I write $f(x)$ equal to it will be a $2 x$ square because n minus 1 is 2 n equal to 3.

So, n minus 1 equal to 2 that should be my maximum degree of the polynomial, then a 1 x plus a 0 so, this time there will be 3. Now, we take if we consider a 2 if a 2 equal to now I have to take all possibilities of a 2 a 1 a 0. So, I can write a 2 equal to a 1 equal to a 2 equal to 0 and a 1 equal to 0, a 2 equal to 0 a 1 equal to 0, then a 0 it can be 0 or 1, a 0 equal to 0 a 2 equal to 0 a 1 equal to 0 then a 0 equal to 1. So, the polynomial is here $f(x) = x^2$ here $f(x) = x^2 + 0x + 0$.

Now, I consider a 2 equal to 0, but a 1 is 1 because they can take 0 or 1 values. So, if a 1 equal to 1, then if a 0 equal to 0 then, $f(x) = x$, if a 2 equal to 0; that means, all possibilities we are taking a 1 equal to 1 and a 0 equal to 1 then $f(x) = x + 1$. So, now, for we have taken a 2 equal to 0 all these values. So, now, for same thing we can do for a 2 equal to 1.

So, this is actually for we have done a 2 equal to 0 for a all a 2 equal to 0.

(Refer Slide Time: 18:39)



Now, we do for. So, this is if we continued, then for a 2 equal to 1 I can write again all 4 values; that means, a 1 equal to 0 a 0 equal to 0, a 1 equal to 0 a 0 equal to 1, a 1 equal to 1 a 0 equal to 0, a 1 equal to 1 and a 0 equal to 1.

So, since a 2 equal to 1 so, always I get this x^2 term should be always there. So, first I write for all the polynomials here I get x^2 . Then it is all 0, then here it is 0 plus 1, here it is x plus 0, here it is x plus 1. So, the 8 polynomials we got these the 8

polynomials; that means, here 2 to the power 3, where p equal to 2 and n equal to 3, the polynomials are that we got $0 \ 1 \ x \ x \ plus \ 1$.

So, polynomials are $0 \ 1 \ x \ x \ plus \ 1$, then here we get $x \ square \ x \ square \ plus \ 1$, $x \ square \ plus \ x$ and $x \ square \ plus \ x \ plus \ 1$. Now, we can also represent these polynomials by binary codes. How see, here I have 3 terms. Since I have the polynomial is of the form $a_2 \ x \ square \ a_1 \ x \ and \ a_0$, then mainly that whatever the value of $a_2 \ a_1$ is 0. So, that gives me these all these polynomials. So, if I write say here mainly we are getting this for $a_2 \ a_1 \ a_0$ where this $a_0 \ a_1 \ a_2$ can take values from Z_2 , because my p equal to 2; that means, 0 and 1; that means, 0 and 1.

So, if I take all possible values of these. And we will see here there are 8 and we know from $0 \ 0 \ 0$ to $1 \ 1 \ 1$.

(Refer Slide Time: 22:11)

| coefficient | x^2 | x^1 | x^0 | polynomial |
|-------------|-------|-------|-------|------------|
| | a_2 | a_1 | a_0 | |
| | 0 | 0 | 0 | 0 |
| | 0 | 0 | 1 | 1 |
| | 0 | 1 | 0 | x |
| | 0 | 1 | 1 | $1+x$ |
| | 1 | 0 | 0 | x^2 |
| | 1 | 0 | 1 | x^2+1 |
| | 1 | 1 | 0 | x^2+x |
| | 1 | 1 | 1 | x^2+x+1 |

$\forall a_i \in Z_2 \{0,1\}$
 have binary representation of Polynomial
 $x^2+1 = 1 \cdot x^2 + 0 \cdot x + 1$
 Binary = 101 representation.

So, if I continue the next page if I write all possible values that $a_2 \ a_1 \ a_0$, we give the values $0 \ 0 \ 0, 0 \ 0 \ 1, 0 \ 1 \ 0, 0 \ 1 \ 1, 1 \ 0 \ 0, 1 \ 0 \ 1, 1 \ 1 \ 0, 1 \ 1 \ 1$. So, we will we will give that see $0 \ 0 \ 0$ means now if I write now the polynomials. So, the polynomial will be here 0.

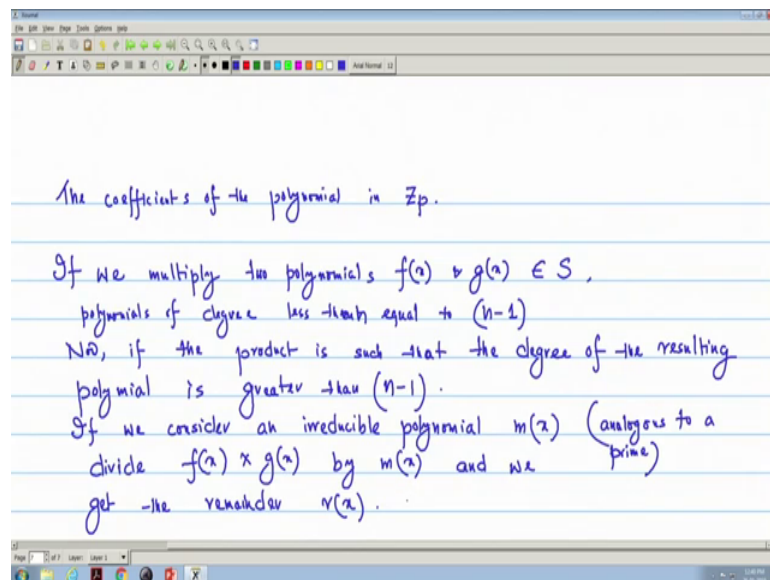
As if this is my 0th term or if I again write that x to the power 0 if the position wise you can we can write that as if this is my x to the power 0 term, this is x to the power 1 term, and x to the power 2 term, because it is $a_2 \ x \ square \ a_1 \ x \ and \ a_0 \ x \ 0$. So, I can write then it is $0 \ 0$ and this is $1 \ x \ to \ the \ power \ 0 \ is \ 1$. So, this is polynomial 1. Since it is only 1

so, x , so, this is x this is 1 plus x , this is x square, this is x square plus 1 , this is x square plus x and this is x square plus x plus 1 .

So, actually the binary values when these it is in Z_2 ; that means, it can take only 0 and 1 . So, that is why this is same as that of our binary codes and this gives this is the binary representation of this polynomials. So, sometimes so, you also use this binary representation if it is in Z_2 ; that means, if my a_i is are in if a_i is belongs to Z_2 since it is in binary; that means, Z_2 is 0 and 1 . So, though we can there can be binary representation of polynomial; that means if that particular term or is there a polynomial. On that particular polynomial term is there then that coefficient is 1 that particular a_i value is 1 , if that particular term is not there then the particular it is 0 , like here they take an example of x square plus 1 we take example of x square plus 1 .

So, x square plus 1 we can write x square; that means, 1 into x square plus 0 into x because x term is not there and 1 . So, this is actually binary representation is 101 . So, binary representation is 101 ok. So, now, we have read that rules of arithmetic for the following when it is the coefficients are in Z_2 or Z_p .

(Refer Slide Time: 26:17)



So, the coefficients, coefficients of the polynomial in Z_p .

Now, once we get the set of polynomials and now we can do the modular polynomial arithmetic; that means, that we can divide one polynomial by another polynomial and the

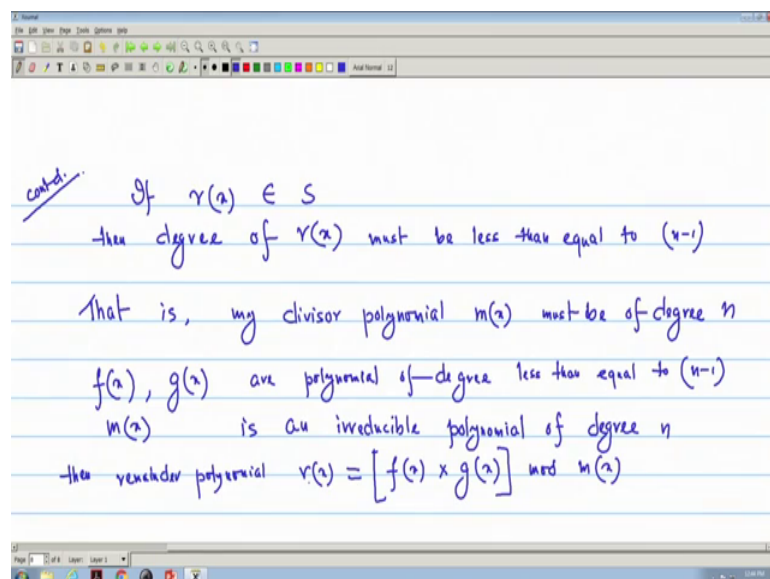
remainder will get we can use that thing. So, what we can write that if we multiply, if we multiply two polynomials of set S , say $f(x)$ and $g(x)$ two polynomials $f(x)$ and $g(x)$ that belongs to S . And, then we have considered the polynomial this is the polynomial S is the set of polynomial of degree less than equal to n minus 1. So, S consists of polynomials of polynomials of degree less than or equal to n minus 1.

Now, if the product becomes or the product is such that the degree that the degree of the result polynomial; that means, the product polynomial degree of the resulting polynomial is greater than n , because if we multiply two polynomials whose degree can be n minus 1 then the it can be greater than n , n minus 1 because I have taken $f(x)$ and $g(x)$ maximum degree can be up to n minus 1, then that will not be this result polynomial will not be in this set S .

So, the way we have done the modular arithmetic. Now, if we consider a an irreducible polynomial irreducible polynomial $m(x)$, which is analogous to a prime analogous to a prime. And, that is why we call prime polynomial also, we have read that definition and we divide the product by $m(x)$; that means, divide $f(x)$ into $g(x)$ the product by $m(x)$ and we get the remainder $r(x)$.

See then, if I want these remainder must polynomials must be in the set S . So; that means, the degree of the polynomial $r(x)$ must be less than equal to n my less than equal to n minus 1.

(Refer Slide Time: 31:557)



cond. If $r(x) \in S$
 then degree of $r(x)$ must be less than equal to $(n-1)$

That is, my divisor polynomial $m(x)$ must be of degree n

$f(x), g(x)$ are polynomial of degree less than equal to $(n-1)$

$m(x)$ is an irreducible polynomial of degree n

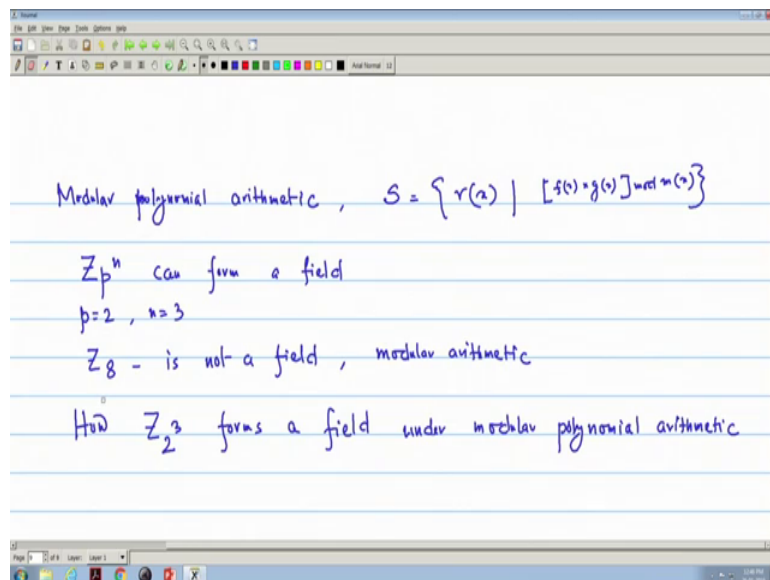
then remainder polynomial $r(x) = [f(x) \times g(x)] \text{ mod } m(x)$

So, if $r(x)$ belongs to S we want that all remainder, then degree of all $r(x)$ remainder polynomials must be less than equal to $n - 1$, because we have considered the set is a set of polynomial with degree less than equal to $n - 1$. So, when can I get some polynomials as the remainder whose degree will be less than equal to $n - 1$, when my divisor polynomial is of degree n ; that means, that is my divisor polynomial my divisor polynomial that $m(x)$ must be of degree n must be of degree n .

So, now if we summarize that $f(x) = g(x) + r(x)$ again $f(x)$ and $g(x)$ are polynomials of degree $n - 1$, less than equal to $n - 1$ I should write degree less than equal to $n - 1$; $m(x)$ is an irreducible polynomial irreducible means that if it has no factor that we have read the earlier. So, $m(x)$ is a irreducible polynomial of degree n .

Then $r(x)$ equal to the remainder polynomial, the remainder polynomial $r(x)$ equal to $f(x)$ into $g(x)$ modulo $m(x)$; that means, if it is remainder I can take modulo $m(x)$. Now, this is totally similar as a of modular arithmetic because $m(x)$ is analogous to some prime number p and this is a product. So, $a \pmod n$ and the remainder I can take. So, now, with all this set of polynomials, because $r(x)$ is of degree $n - 1$.

(Refer Slide Time: 35:35)



So, $r(x)$ is belongs to S and now that we these $r(x)$ gives the if we now consider the modular polynomial arithmetic; modular polynomial arithmetic, then we will be using my all my S the set with that all $r(x) \in S$ all my $r(x)$ that $r(x)$ is the $r(x)$ is I can write that $f(x) = g(x)$

mod m . So, this is the set and with this this is totally similar and we can now we will be using this set to form the form a field.

So, we will we started our lecture that how Z_p to the power n can form a can form a field and what we have seen a p equal to 2 as an example n equal to 3. So; obviously, Z_8 we have earlier seen that normal modular arithmetic Z_8 is not a field Z_8 is not a field under for modular arithmetic, normal modular arithmetic. Now, what we have done that we have got 8 polynomials.

So, now, under will show how we have to show how Z_2 to the power 3 forms a field under modular polynomial arithmetic. Since now we have 8 polynomials in the set. And in the next lecture we will continue this is topic and we will see how we can form a field under modular polynomial arithmetic.