

**Lecture - 67**  
**Polynomials Over Fields and Properties**

(Refer Slide Time: 00:26)

**Lecture Overview**

- Properties of polynomials over fields and rings
- Division of polynomials over fields
- Factorization of polynomials
  - ❖ Reducible and irreducible polynomials



Hello everyone, welcome to this lecture so, in this lecture we will continue our discussion on polynomials over rings. And we will see in this lecture, polynomials over fields and we will also discuss about how to divide polynomials over fields. And we will also discuss about factorization of polynomials using which we will define the notion of reducible and irreducible polynomials.

(Refer Slide Time: 00:52)

**Division of Polynomials Over Integers**

$x^2 + 3x + 2$   
↑  
 Divisor

$x^4 + 4x^3 + x^2 + 3x + 4$   
○

$x^2 + x - 4$   
←  
 Quotient

$$\begin{array}{r}
 x^4 + 4x^3 + x^2 + 3x + 4 \\
 \underline{x^4 + 3x^3 + 2x^2} \\
 x^3 - x^2 + 3x \\
 \underline{x^3 + 3x^2 + 2x} \\
 -4x^2 + x + 4 \\
 \underline{-4x^2 - 12x - 8} \\
 13x + 12
 \end{array}$$

Can the above division be performed for polynomials over rings/fields?

$13x + 12$   
←  
 Remainder

$x^4 + 4x^3 + x^2 + 3x + 4 = (x^2 + x - 4)(x^2 + 3x + 2) + (13x + 12)$

So, let us start with the usual division of polynomials that we are familiar with. So, if I consider 2 arbitrary polynomials where the coefficients are integers and we are my plus and

dot operations are the usual integer addition and integer multiplication then this is the way we perform the division. So, you will be given a divisor and you will be given a number which you want to divide.

And then what we do is basically say in this example my power is currently  $x^4$  my divisor has  $x^2$ . So that is why I try to multiply my divisor with something so that I can get something of the form  $x^4$  so that  $x^4$  and  $x^4$  cancels out and whatever is left that will be treated as my next value or the next thing which I want to divide. So, in each step basically we are slowly and slowly and slowly trying to reduce the power of the number which I want to divide.

And I keep on doing this till I cannot do anything further in the sense that the remainder that I obtain is a polynomial whose degree is less than the degree of my divisor. If I reach that stage then I cannot proceed further. And then I can say that safely that the number which I wanted to divide; that my original number is basically the product of divisor and quotient plus some remainder. That is the usual way of performing division of polynomials over the integers.

Now the interesting question here is the following in the last lecture we have defined or we have extended the notion of polynomials to rings and we have seen how to do addition of polynomials over rings which are more or less similar to the way we perform addition and multiplication of polynomials over the integers. What about the division operation? Can we do something similar for polynomials which are defined over rings or fields.

(Refer Slide Time: 03:04)

## Polynomials Over Rings: Properties

□  $a(x) = a_n x^n + \dots + a_0$ ,  $b(x) = b_m x^m + \dots + b_0$  over  $(\mathbb{R}, +, \cdot)$ , with  $n \geq m$

<p>❖ Degree of <math>a(x) + b(x)</math> can be less than <math>n</math> <span style="float: right;"><math>\mathbb{Z}_3 = \{0, 1, 2\}</math></span></p> <p>➤ Ex: <math>a(x) = 2x^2 + 2x + 1</math> and <math>b(x) = x^2 + x + 2</math>, over <math>(\mathbb{Z}_3, +, \cdot)</math></p> <p>➤ Then <math>a(x) + b(x) = 3x^2 + 3x + 3 = 0</math> --- degree 0</p>
<p>❖ Degree of <math>a(x)b(x)</math> can be less than <math>n + m</math> <span style="float: right;"><math>a_n \in \mathbb{R}</math> <math>b_m \in \mathbb{R}</math></span></p> <p>➤ Coefficient of <math>x^{n+m} = a_n b_m</math>, which can be 0, even if <math>a_n \neq 0</math> and <math>b_m \neq 0</math></p> <p>➤ Ex: <math>a(x) = 2x^2 + x + 4</math> and <math>b(x) = 3x + 1</math>, over <math>(\mathbb{Z}_6, +, \cdot)</math> <span style="float: right;"><math>\mathbb{R} = \{0, \dots, 5\}</math></span></p> <p>➤ Then <math>a(x)b(x) = 5x^2 + x + 4 = 0</math> --- degree 2</p> <p style="text-align: center;"><math>\rightarrow 6x^3 + \dots \quad (2 \cdot 3) = 0</math></p>

So, for that again let us recall the definition of polynomials over rings and further explore some more properties regarding the polynomials over rings. So, imagine you are given 2 arbitrary polynomials over an abstract ring  $\mathbb{R}$ . That means all your coefficients  $a_n, a_{n-1}, a_0, b_m, b_{m-1}, b_0$  are elements of this set  $\mathbb{R}$ . And all this plus and dot operations are your ring plus and dot operations.

Now as we have demonstrated in our last lecture itself it might be possible that the summation of  $a(x)$  and  $b(x)$  has a degree which is less than  $n$  even if your  $n \geq m$  it might be possible that when you take the summation of these 2 polynomials the resultant degree is less than  $n$ , that is quite possible. So, again to demonstrate my point let us take these 2 polynomials  $a(x)$  and  $b(x)$  over, where the coefficients are elements of the set  $0, 1, 2$ .

And this plus operation is plus modulo 3 and this dot operation is multiplication modulo 3. And if these are my  $a(x) (2x^2 + 2x + 1)$  and  $b(x) (x^2 + x + 2)$  polynomial then the coefficient of  $x^2$  will be  $2 + 1$  and  $2 + 1$  will be 3 and 3 modulo 3 will be 0; in the same way the coefficient of  $x$  will be 0 the constant coefficient will be 0. So, even though  $a(x)$  and  $b(x)$  none of them is numerical is 0, the 0 polynomial, in this case the summation of these 2 polynomials actually turns out to be a 0 polynomial. In the same way if I multiply 2 polynomials over rings then again it is not necessary that its degree will be exactly  $n + m$  which is the case if I multiply 2 integer polynomials but when I multiply 2 ring polynomials that may not be the case because the coefficient of  $x^{n+m}$  when I do multiplication of ring polynomials will be this value  $a_n b_m$ , and now since my  $a(n)$  is an element of the ring and my  $b(m)$  is also an element of the ring it might be possible that neither  $a(n)$  nor  $b(m)$  are 0 elements but still their product is a 0 element, this is quite possible if you are taking the coefficients over the ring remember this is not possible over a field. In a field if the product of 2 elements is a 0 element and definitely 1 of them has to be 0 but that may not be the case in a ring again let me demonstrate this.

So, my ring  $\mathbb{R}$  here is set  $\mathbb{Z}_6$  namely the elements 0 to 5 and of course my plus operation is plus modulo 6 and my dot operation is multiplication modulo 6 then what can I say about the product of these 2 polynomials  $(2x^2 + x + 4) (3x + 1)$ . So, if I consider the coefficient of  $x^3$  the coefficient of  $x^3$  will be  $6x^3$  but what will be 6? So the coefficient of  $x^3$  will be basically 2 into 3 where this into is multiplication modulo 6 and 2 multiplied with 3 modular 6 is basically 0.

So, the coefficient of  $x^3$  vanishes and now you can see that the degree of the product polynomial here is less than the summation of the degrees of  $a(x)$  and  $b(x)$  polynomial.

(Refer Slide Time: 07:11)

## Polynomials Over Fields : Properties

- $a(x) = a_n x^n + \dots + a_0, b(x) = b_m x^m + \dots + b_0$  over  $(\mathbb{F}, +, \cdot)$
- $\text{degree}(a(x)b(x)) = \text{degree}(a(x)) + \text{degree}(b(x))$
- ❖ Coefficient of  $x^{n+m}$  in  $a(x)b(x) = a_n b_m$
- ❖  $a_n b_m$  will be 0 over  $(\mathbb{F}, +, \cdot)$ , only if  $a_n \neq 0$  or  $b_m \neq 0$
- **Theorem (Division of Polynomials over  $\mathbb{F}$ ):** Let  $a(x)$  and  $b(x)$  be polynomials over  $(\mathbb{F}, +, \cdot)$ , with  $b(x) \neq 0$ . Then there exist **unique polynomials**  $q(x)$  and  $r(x)$  over  $(\mathbb{F}, +, \cdot)$ , such that
 
$$a(x) = q(x)b(x) + r(x)$$
 where  $r(x)$  is either the zero-polynomial or  $\text{degree}(r(x)) < \text{degree}(b(x))$
- $g(x)$  is said to be a **divisor (factor)** of  $f(x)$  in  $\mathbb{F}[x]$ , if there exists some  $h(x)$ :
 
$$g(x)h(x) = f(x)$$

Now, what we can say about the addition of polynomials and multiplication of polynomials over fields? So, we can extend the definition of polynomial addition and multiplication that we have given for rings to fields as well because remember fields after all is a special type of ring. Now in a field we can definitely say that the degree of the product polynomial will be exactly equal to the sum of degree of the individual polynomials.

Which was not the case if I perform the multiplication of polynomials over rings we have already demonstrated that; this is because now the coefficient of  $x^{n+m}$  in the product polynomial will be the product of  $a_n$  and  $b_m$ . And remember in the last lecture we proved that the product of  $a_n$  and  $b_m$  can be 0 only if  $a_n$  was 0 or  $b_m$  was 0 that means you are at the first place your polynomial  $a(x)$  was not of degree  $n$  or your polynomial  $b(x)$  was not of degree  $m$ .

It can never happen that even though your  $a_n$  and  $b_m$  are both non 0 but still when you multiply  $a_n$  and  $b_m$  over a field you get a 0 element that is not possible that is why the coefficient  $a_n$  times  $b_m$  will survive. And that is why the  $x$  term with  $x^{n+m}$  will be present in your product polynomial. Now based on this observation we can give a theorem regarding the division of polynomials over a field.

And this is kind of generalization of your usual division property. What do we mean by the usual division property? We know that in the integer world if you are given 2 arbitrary integers  $a$  and  $b$  then I know; that of course where  $b$  is not 0. And I know that I can always express  $a$  in the form of some quotient times  $b$  plus some remainder  $r$  where the remainder  $r$  will be in the range 0 to  $b - 1$ . That is the usual divisibility theorem with respect to the integers.

We are now trying to extend that property that theorem in the context of polynomials over fields so you can interpret that now  $a$  is replaced by a polynomial. It is no longer just a single value but rather it is a polynomial where the quotients of the polynomial are from some field. In the same way your element  $b$ ; the number  $b$ ; is now generalized to a polynomial of some degree. And similar to the case of divisibility property that we have in the integer world where  $b$  is not allowed to be 0 because division by 0 is not well defined.

So that is why we are not allowing  $b(x)$  to be 0 here then this theorem basically says that you can express your  $a(x)$  as some quotient times divisor plus some remainder namely some quotient polynomial times your divisor polynomial plus some remainder polynomial where the degree of your remainder polynomial will be strictly less than the degree of your divisor polynomial.

So, this is your divisor polynomial,  $q(x)$  is the quotient polynomial and  $r(x)$  is your remainder polynomial. Again we can prove this very easily but due to interest of time I am not going to prove that and the interesting part of the theorem here is that the quotient and the remainders will be unique here similar to the case of integer division. If you divide  $a$  by  $b$  you get a unique quotient and a unique remainder where the remainder is in the range 0 to  $b - 1$ .

Now if my remainder turns out to be 0 then I will say that  $a(x)$  is completely divisible by  $b(x)$  or in some sense  $b(x)$  is a divisor or factor of your  $a(x)$  so in other words consider a polynomial  $g(x)$  I will say that  $g(x)$  is a divisor of  $f(x)$  if  $f(x)$  is completely divisible by  $g(x)$  that means you get no remainder that means if you get a remainder but that remainder is actually a 0 polynomial.

In other words there exists some polynomial  $h(x)$  over the field which when multiplied with your  $g$  polynomial will give you the polynomial  $f(x)$  if that is the case then I will say  $g(x)$  is a

factor of your  $f(x)$  polynomial, of course if  $g(x)$  is a factor of  $f(x)$  polynomial then so is  $h(x)$  polynomial.

(Refer Slide Time: 12:39)

### GCD of Polynomials Over Fields

- $d(x) \in \mathbb{F}[x]$  is said to be a **GCD** of  $a(x), b(x) \in \mathbb{F}[x]$ , if:
  - ❖  $d(x)$  is a **divisor** of  $a(x)$  and  $b(x)$  maximum
  - ❖ **Any divisor** of  $a(x)$  and  $b(x)$  is also a divisor of  $d(x)$
- Over  $\mathbb{F}[x]$ , GCD of two polynomials need not be unique
  - ❖ Over  $\mathbb{F}[x]$ , if  $d_1(x)|d_2(x)$  and  $d_2(x)|d_1(x) \neq d_1(x) = d_2(x)$
  - Over  $\mathbb{Z}_7[x]$ , polynomials  $(3x + 5)$  and  $(6x + 3)$  divide each other
 

$(6x + 3) = 2(3x + 5)$   
 $d_1(x)$

$(3x + 5) = 4(6x + 3)$   
 $d_2(x)$
- **Euclid's GCD algorithm** can be extended to find a GCD of two polynomials over  $\mathbb{F}[x]$

$d_1 | d_2$   
 $d_2 | d_1 \Rightarrow d_1 = d_2$   
**GCD(a, b)**  
 $d$   
 $a(x)$   $b(x)$   
 $d(x)$   
 $d_1(x)$   $d_2(x) \dots$

So, once we have given the definition of division of polynomials over field the next thing that we want to define is the GCD of polynomials over field. So, again this will be a generalization of the GCD of 2 numbers that we had discussed earlier in our module on number theory. So,  $d$  is said to be the GCD of  $a$  and  $b$  if it is the greatest common divisor of both  $a$  and  $b$ ; in the same way imagine you are given 2 arbitrary polynomials  $a(x)$  and  $b(x)$  over the field then another polynomial  $d(x)$  over the field will be considered as the GCD of these 2 polynomials and the following 2 properties are satisfied. Of course the  $d(x)$  polynomial has to divide both the  $a(x)$  polynomial as well as the  $b(x)$  polynomial because after all it is a common divisor and it is greatest in the sense that you take any divisor of  $a(x)$  and  $b(x)$  it is also a divisor of  $d(x)$  in that sense you can imagine that  $d(x)$  is actually kind of a maximal possible common divisor of both  $a(x)$  and  $b(x)$ .

So, pictorially you can imagine that you are given  $a(x)$  polynomial  $b(x)$  polynomial and there can be multiple common divisors of both these 2 polynomials call them  $d_1(x)$ ,  $d_2(x)$  and so on. Among all those common divisors you can interpret that there is another divisor  $d(x)$  which is kind of sitting on top of the hierarchy in the sense that all these divisors  $d_1(x)$ ,  $d_2(x)$ ,  $d_3(x)$ ,  $d_n(x)$  they also divide  $d(x)$  in that sense  $d(x)$  is sitting at the top of the hierarchy among all the common divisors of  $a(x)$  and  $b(x)$ .

And that sense it is the maximal possible common divisor of  $a(x)$  and  $b(x)$ . The reason we are defining GCD in this sense is because we cannot define what we call as maximum when we are considering polynomials over the fields. So, again in the case of integer GCDs where we are given 2 integer values  $a$  and  $b$ ,  $d$  was the GCD in the sense it has the maximum possible common divisor there is no other common divisor whose value is more than  $d$ .

There the notion of more is very well defined but when it comes to polynomials over field I cannot define that  $d(x)$  is the maximum possible common divisor of  $a(x)$  and  $b(x)$ . I cannot define a notion like maximum common divisor polynomial; this is because it turns out that if I consider polynomials over fields then the GCD of 2 polynomials need not be unique at the first place. And that is why you can have multiple possible GCDs of 2 arbitrary polynomials.

This is because if I consider polynomials over fields and if you are having a situation where you have 2 divisor polynomial say  $d_1(x)$  is a common divisor of both  $a(x)$ ,  $b(x)$  and so is the  $d_2(x)$  polynomial that is also a common divisor of both  $a(x)$  and  $b(x)$  and say the divisor polynomial  $d_1$  divides  $d_2$  and say  $d_2$  is a divisor of  $d_1$  then I cannot conclude that the polynomials  $d_1(x)$  and  $d_2(x)$  are same.

And this is not the case in the usual integer world. In the usual integer world I know that if there is a number  $d_1$  which divides  $d_2$  and if it is the case that  $d_2$  divides  $d_1$  as well then I can conclude that  $d_1$  and  $d_2$  are the same numbers; but when I consider polynomials over fields and if I have 2 polynomials where the first polynomial divides the second polynomial and the second polynomial divides the first polynomial I cannot necessarily conclude that both polynomials are identical.

So, for instance if I consider the field  $\mathbb{Z}_7$  namely my elements are 0 to 6 and my operations are addition modulo 7 and multiplication modulo 7 and suppose I take these 2 polynomials  $(3x + 5)$  and  $(6x + 3)$ . It turns out that these 2 polynomials divide each other because if you divide  $6x + 3$  by  $3x + 5$  you will get the quotient polynomial 2 which is the constant polynomial and 0 remainder whereas if you divide  $3x + 5$  by  $6x + 3$  you will get the quotient polynomial 4 and 0 remainder, this is your  $d_1(x)$  and this is your  $d_2(x)$ .

But you can see here that even though  $d_1$  divides  $d_2$ ,  $d_2$  divides  $d_1$  they are different polynomials and that means if say for instance both  $3x + 5$  as well as  $6x + 3$  are common

divisors of  $a(x)$  and  $b(x)$  then it can be very much possible that  $3x + 5$  as well as  $6x + 3$  are both GCD of  $a(x)$  and  $b(x)$ , that is possible. That means I cannot say that when I consider polynomials over fields that I will have unique GCDs you can have multiple possible GCDs.

And this is unlike GCDs over integers so that is why I cannot define what I call as a maximum possible polynomial which is a common divisor polynomial of both  $a(x)$  and  $b(x)$ . That is why I define what I call as maximal. You take any divisor of  $a(x)$  and  $b(x)$  it will be a divisor of your  $d(x)$ . Now once we have defined GCD of polynomials of over field and next question is how do we find out?

And it turns out that the beautiful Euclid's GCD algorithm that we had discussed in our module on number theory it can be extended to even find GCD of 2 polynomials namely the GCD algorithm based on repeated division. The same algorithm if I extend to the case of polynomial, if I just extend it will work and it will give you GCD of 2 polynomials defined over the fields.

(Refer Slide Time: 20:03)

### Euclidean Algorithm for Polynomials Over Fields

Extended Euclid Algorithm  
 Theorem: Let  $d(x)$  be a GCD of  $a(x), b(x)$  over  $\mathbb{F}[x]$ . Then there are polynomials  $\lambda(x), \mu(x) \in \mathbb{F}[x]$ , such that:

$$d(x) = \lambda(x)a(x) + \mu(x)b(x)$$

$$\begin{aligned} d &= \text{GCD}(a, b) \\ d &= sa + tb \end{aligned}$$

Find GCD of  $a(x) = x^3 + 2x^2 + x + 1$  and  $b(x) = x^2 + 5$  over  $\mathbb{Z}_7[x]$

The diagram shows the following steps:

- Division 1:**  $x^3 + 2x^2 + x + 1$  divided by  $x^2 + 5$ . The quotient is  $x + 2$ . The remainder is  $2x^2 + 3x + 1$ .
 
$$\begin{array}{r} x^2 + 5 \overline{) x^3 + 2x^2 + x + 1} \\ \underline{-x^3 \phantom{+ 2x^2} + 5x} \phantom{+ 1} \\ 2x^2 + 3x + 1 \end{array}$$
- Division 2:**  $2x^2 + 3x + 1$  divided by  $x^2 + 5$ . The quotient is  $2$ . The remainder is  $3x + 5$ .
 
$$\begin{array}{r} \phantom{x^2 + 5} \overline{) 2x^2 + 3x + 1} \\ \underline{-2x^2 \phantom{+ 3x} + 10} \\ 3x + 5 \end{array}$$
- Extended Euclidean Algorithm:**
  - $x - 5x = -4x \xrightarrow{7-4} 3x$
  - $1 - 3 = -2 = 5$
  - $1 + 4 = 5$

In fact we can get what we call as the extended Euclid GCD algorithm for polynomials over fields and find out what we call as Bezout coefficients which we had seen in our module on number theory. So, remember if  $d$  is the GCD of 2 integer values  $a$  and  $b$  then the Bezout's theorem says that I can always find out linear combiners  $s$  and  $t$  such that integer linear combiners such that  $s$  times  $a$  +  $t$  times  $b$  is actually your GCD  $d$ .



That means GCD is always; I can always express GCD as the linear combination of my 2 numbers  $a$  and  $b$  itself and we know how to find out this Bezout's coefficients using the extended Euclid algorithm. The same theorem holds even for the case of polynomials over fields. So, basically what the theorem says here the following: if you are taking 2 polynomials over the field and say  $d(x)$  is one of the GCDs, again remember there can be multiple GCDs possible.

So, if  $d(x)$  is one of the GCDs then I can always find out the corresponding Bezout's polynomials. So, you can find out this combiners  $\lambda(x)$  and  $\mu(x)$  which will be now polynomials because now everything is extended to polynomials such that your GCD can be expressed as a combination of your original polynomial say  $a(x)$  and  $b(x)$  where the combiners will be your  $\lambda(x)$  polynomial and  $\mu(x)$  polynomials.

So, I would not be going into the exact details of how to find out this Bezout's coefficients and how to find out the GCD's but I will work out an example here. So, say for instance I want to find out the GCD of this  $a(x)$  ( $x^3 + 2x^2 + x + 1$ ) and  $b(x)$  ( $x^2 + 5$ ) polynomials where all the operations are performed over  $\mathbb{Z}_7$ . So,  $\mathbb{Z}_7$  has all the elements from 0 to 6 and my plus operation will be addition modulo 7, my multiplication operation will be multiplication modulo 7.

So, what we do in the GCD algorithm: we take the higher number and divide it by the smaller number but the numbers now here are the polynomials. So, we will take the polynomial with the higher degree and divide it by the polynomial with the lower degree. So, this is my  $a(x)$  this is my current  $a$  and this is my current  $b$ . And now you can see the way I am performing the division here, it is something similar to the way we perform division over the integers.

But instead of all the operations being performed over integers, the operations will be performed over  $\mathbb{Z}_7$ . So, for instance my current power here is  $x^3$  and my divisor has the highest power  $x^2$  so that is why I am putting an  $x$  here if I multiply  $x$  with  $x^2 + 5$ , I will get  $x^3$ . The coefficient here will be 1, 1 modulo 7 will be 1 and 5 into  $x$ . So, coefficient here will be 5, 5 modulo 7 will be 5.

Now I have to take the difference here. I have to subtract so  $x^3$  and  $x^3$  cancels out  $2x^2$  is taken as it is here. And now what will happen if I subtract  $5x$  from  $x$  so  $x - 5x$  will be  $-4x$ .

But there is no -4. -4 in this field  $\mathbb{Z}_7$  will be treated as +3 because by -4 I mean  $7 - 4$ . Basically I am talking about because remember all the operations are plus mod 7, and all the multiplication operation are multiplication modulo 7. So that is why  $-4x$  will be treated as  $+3x$  so that is why will have  $+3x$  and this  $+1$  will be retained as it is. Now I have to take care of this  $2x^2$  so that is why I take my next term in the quotient as 2 so if I now multiply 2 with  $x^2 + 5$ , 2 times  $x^2$  will be retained as it is whereas 2 into 5 will be 10 but 10 modulo 7 will be 3.

So that is why this is 3 this is not 10 and now I will be taking the difference here. So, 3 of  $x$  retains goes as it is now  $1 - 3$  will be  $-2$  and  $-2$  will be treated as  $7 - 2$  namely 5. If you are wondering how exactly we are getting this so  $-3$  is basically  $+4$ . And  $1 + 4$  is 5,  $-3$  in this field  $\mathbb{Z}_7$  is  $+4$  and  $+4$  and  $+1$  modulo 7 will be 5 so that is why I get  $3x + 5$ .

And now you can see that the degree of  $3x + 5$  is less than the degree of my divisors. So, this will be treated as my remainder and I cannot proceed further. So, this will complete the first iteration of your Euclid GCD algorithm.

(Refer Slide Time: 26:15)

## Euclidean Algorithm for Polynomials Over Fields

*Extended Euclid Algorithm*

□ **Theorem:** Let  $d(x)$  be a GCD of  $a(x), b(x)$  over  $\mathbb{F}[x]$ . Then there are polynomials  $\lambda(x), \mu(x) \in \mathbb{F}[x]$ , such that :

$$d(x) = \lambda(x)a(x) + \mu(x)b(x)$$

$d = \text{GCD}(a, b)$   
 $d = Sa + Tb$

□ Find GCD of  $a(x) = x^3 + 2x^2 + x + 1$  and  $b(x) = x^2 + 5$  over  $\mathbb{Z}_7[x]$

$b(x) \overline{) a(x)}$

$$\begin{array}{r} x+2 \\ x^2+5 \overline{) x^3+2x^2+x+1} \\ \underline{-x^3 \phantom{+2x^2} +5x} \phantom{+1} \\ 2x^2+3x+1 \\ \underline{-2x^2 \phantom{+3x} +3} \\ 3x+5 \end{array} \quad r(x)$$

$2 \cdot 5 = 10 \equiv 3$

GCD =  $3x + 5$

$b(x) \overline{) a(x)}$

$$\begin{array}{r} 5x+1 \\ 3x+5 \overline{) x^2+5} \\ \underline{-x^2+4x} \\ 3x+5 \\ \underline{-3x+5} \\ 0 \end{array} \quad r(x)$$

$15 \cdot 2 = 30 \equiv 2$   
 $25 \cdot 2 = 50 \equiv 1$   
 $4 \cdot 2 = 8 \equiv 1$

So, this was my  $b(x)$  this was my  $a(x)$  and this is my  $r(x)$ . In the next iteration my  $b(x)$  becomes  $a(x)$ . And my remainder becomes the next  $b(x)$  and now you can see that if I perform the division. Here my highest term is  $x^2$  here it is  $3x$ . So, if I multiply  $3x$  with  $5x$  I will get  $15x^2$  but this coefficient 15 has to be reduced modulo 7, 15 modulo 7 will be 1 so  $1x^2$  which is what I want to cancel out  $x^2$ .

So that is why I multiply with 5x and 5x with 5 will give you 25x. Now this 25 has to be reduced to modulo 7 so it becomes 4 so 4x so that is why I get 4x. Now if I subtract 5 goes as it is and I will get -4x. Now this coefficient -4 modulo 7 will be +3 so that is why -4x goes and becomes +3x. And now 3x + 5 is completely divisible by your divisor. If I put 1 as the next term in my quotient so, I get my remainder polynomial r(x) which is now a 0 polynomial. And that is why now I can say that my GCD is 3x + 5.

(Refer Slide Time: 27:54)

## Euclidean Algorithm for Polynomials Over Fields

**Theorem:** Let  $d(x)$  be a GCD of  $a(x), b(x)$  over  $\mathbb{F}[x]$ . Then there are polynomials  $\lambda(x), \mu(x) \in \mathbb{F}[x]$ , such that:

*Extended Euclid Algorithm*

$$d(x) = \lambda(x)a(x) + \mu(x)b(x)$$

$d = \text{GCD}(a, b)$   
 $d = sa + tb$

Find GCD of  $a(x) = x^3 + 2x^2 + x + 1$  and  $b(x) = x^2 + 5$  over  $\mathbb{Z}_7[x]$

$$\begin{array}{r} x+2 \\ x^2+5 \overline{) x^3+2x^2+x+1} \\ \underline{-x^3} \phantom{+2x^2} \phantom{+x} \phantom{+1} \\ 2x^2+3x+1 \\ \underline{-2x^2} \phantom{+3x} \phantom{+1} \\ 3x+5 \end{array}$$

$2 \cdot 5 = 10 \equiv 3$

GCD =  $3x + 5$

$$x^3 + 2x^2 + x + 1 = (x^2 + 5)(x + 2) + (3x + 5)$$

$$3x + 5 = (x^3 + 2x^2 + x + 1) - (x + 2)(x^2 + 5)$$

$$3x + 5 = (x^3 + 2x^2 + x + 1) + (6x + 5)(x^2 + 5)$$

$\lambda(x) = 1 \quad \mu(x) = (6x + 5)$

Now if I want to find out the corresponding Bezout polynomials for this GCD I can do the following. So, I can say that if I take my original a(x) in terms of divisors, quotients and remainder; I can write my a(x) in this form. And my goal is to express my GCD in terms of a(x) and b(x) polynomial. So, I can write down my GCD here and the remaining things I take to the left hand side I get this expression.

And now what I can do here is the following: I can say that this is my a(x) ( $x^3 + 2x^2 + x + 1$ ) and this is my b(x) ( $x^2 + 5$ ). So, I can treat my  $\lambda(x)$  to be the constant 1. And I can treat my  $\mu(x)$  to this value, so I can say that my  $\lambda(x)$  is the polynomial 1 and my  $\mu(x)$  is the polynomial  $-(x + 2)$  but wait  $-(x + 2)$  is -x -2 but -x means the coefficient is -1 times x and -2. So -1 is not there in  $\mathbb{Z}_7$  I have to reduce it modulo 7.

So, -1 becomes 6 so it becomes 6x and in the same way -2 goes and becomes +5. So that is why my final Bezout polynomials will be this. That is the way I can find GCD and the corresponding Bezout combiners.

(Refer Slide Time: 29:57)

## Polynomial Factorization

□ **Trivial Factorization:** There exist **trivial factorizations** of any  $f(x) \in \mathbb{F}[x]$ :

$$f(x) = \alpha(\alpha^{-1}f(x)), \text{ where } \alpha \in \mathbb{F}$$

Any **constant multiple** of  $f(x)$  is always a factor of  $f(x)$  over  $\mathbb{F}$

□ **Irreducible Polynomial:** A **non-constant polynomial** which **cannot be factored** into **product** of two **non-constant polynomials**

❖  $f(x) \in \mathbb{F}[x]$  is called **irreducible**, if the following hold:

➤  $f(x)$  is a **non-constant** polynomial

➤ If  $f(x) = g(x)h(x)$ , then **either**  $g(x)$  **or**  $h(x)$  is a **constant polynomial**

□ Over  $\mathbb{Z}_3[x]$ ,  $x^2+x+2$  is irreducible, while  $x^4+1$  is reducible

$$x^4+1 = (x^2+x+2)(x^2+2x+2)$$

$$f(x) = \gamma \in \mathbb{F}$$

$$\mathbb{F} = \mathbb{Z}_3 = \{0, 1, 2\}$$

So, now the next thing that once we have seen polynomial division over the fields and GCD of polynomials we can define what we call as factorization. So, a trivial factorization that is possible for any polynomial is the following form. So, you are given the polynomial  $f(x)$ , a trivial factorization will be the following: you take any constant from the field and you take that constant  $\alpha$  multiplied with the multiplicative inverse of  $\alpha$  of course  $\alpha$  is not 0 here.

Otherwise the inverse is not well defined it does not exist. So, if I take any non 0  $\alpha$  from the field and multiply  $\alpha$  and  $\alpha^{-1}$  with that polynomial  $f(x)$  I will get back the original polynomial  $f(x)$  itself in that sense I can always say that there is a trivial factorization of  $f(x)$  namely  $\alpha$  and  $\alpha^{-1}$  are trivial factors for any  $f(x)$ . So, now what we want to define is what we call as irreducible polynomial.

Namely polynomials which cannot be factored into products of lower degree polynomials. That is a rough idea of what we call as irreducible polynomial. So, let us now formally define, so intuitively it is a non constant polynomial which cannot be factored into product of two non constant polynomials. And why we are taking the case that it cannot be factored into product of two non constant polynomials.

Because of this trivial factorization, because if you give me any polynomial  $f(x)$  I can always factorize it, I can always say that  $\alpha$  and  $\alpha^{-1}$  are trivial factors of  $f(x)$  but when I am defining irreducible polynomials I am not interested in the trivial factorization so that is why to exclude the trivial factorization I am explicitly putting a condition that the polynomial  $f(x)$  should not be factored into the product of non constant polynomials.

So, more formally I take a polynomial over a field I will call it irreducible if the following holds. First that polynomial has to be a non constant polynomial that means it should have some term of the form  $x^i$ . It is not a constant polynomial that means it is not of the form say some  $\gamma$  where  $\gamma$  my  $f(x)$  is not of the form  $f(x)$  equal to some  $\gamma$  where  $\gamma$  is an element of the field that is not the form of  $f(x)$ .

I am not interested in such polynomials when I am defining irreducible polynomials. And the second condition is that I can always decompose  $f(x)$  as per trivial factorization. But when I am defining irreducible polynomials my requirement is that I should not be able to write  $f(x)$  into the product of 2 other polynomials  $g(x)$  and  $h(x)$  where either  $g(x)$  or  $h(x)$  is a constant polynomial because I can always write  $f(x)$  in the form of  $f(x) \alpha$  into  $\alpha^{-1}$ .

And  $\alpha$  into  $\alpha^{-1}$  can be treated as an element 1. So, I can always say that  $f(x) = f(x)$  into 1. So, namely 1 is always a trivial factor of  $f(x)$  that is not considered as a violation of this definition. So, my irreducibility property demand here that my  $f(x)$  should not be factorized; it should not be possible to factorize  $f(x)$  into non trivial factors. If at all it can be factorized only when one of the factors is a constant polynomial that is allowed that would not be considered as a violation of the property of an irreducible polynomial.

So, to give you some examples here if I consider my field to be  $\mathbb{Z}_3$  namely the set 0, 1, 2 where all the operations are addition modulo 3 and multiplication modulo 3 and if I consider polynomials over this field then this polynomial  $(x^2 + x + 2)$  is irreducible, we can prove that. We will see later how do we show whether a polynomial is irreducible or not.

But you can see, you have to believe me that this is not reducible in the sense I cannot factorize it out into other than the trivial factorization; but this polynomial  $x^4 + 1$  is reducible because I can write it in the form of this product of 2 polynomials  $(x^2 + x + 2)(x^2 + 2x + 2)$  where none of these 2 polynomials is a constant polynomial. So that is why it is reducible, reducible in the sense it is non trivially factorisable.

**(Refer Slide Time: 33:52)**

## Factor Theorem for Polynomials Over Fields

□ **Factor Theorem:** Let  $f(x) \in \mathbb{F}[x]$ , where  $(\mathbb{F}, +, \cdot)$  is a field. Then

$$(x - \alpha) \text{ is a factor of } f(x) \iff f(\alpha) = 0 \text{ over } \mathbb{F}$$

❖ **Proof:**  $(x - \alpha)$  is a factor of  $f(x) \implies f(\alpha) = 0$  over  $\mathbb{F}$

$$f(x) = (x - \alpha)g(x) \implies f(\alpha) = (\alpha - \alpha)g(\alpha) = 0g(\alpha) = 0$$

❖ **Proof:**  $f(\alpha) = 0$  over  $\mathbb{F} \implies (x - \alpha)$  is a factor of  $f(x)$

➤ From **Division theorem**, let  $f(x) = (x - \alpha)q(x) + r(x)$

$$\text{degree}(r(x)) < \text{degree}(x - \alpha) \text{ OR } r(x) = 0$$

➤  $f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha)$  } If  $\text{degree}(r(x)) < \text{degree}(x - \alpha)$ ,  
 $0 = r(\alpha)$  } then  $r(x)$  is a **non-zero constant polynomial**, so  $r(\alpha) = 0$  not possible

So, the next thing that we want to define is the factor theorem for polynomials over fields. So, the factor theorem states the following. If you take any polynomial over the field then the polynomial  $(x - \alpha)$  will be considered as a factor of your polynomial  $f(x)$  if and only if the polynomial  $f(x)$  when evaluated at  $x = \alpha$  gives you the element 0, where 0 is the additive identity.

And since this is an if and only if statement we have to give 2 proofs here we have to give proof both in the forward direction as well as in the reverse direction. So, let us see the proof in the direction where we assume that  $(x - \alpha)$  is a factor of  $f(x)$ , assuming that I have to show that the polynomial  $f$  evaluated at  $x = \alpha$  will give you 0. So, we will give a direct proof a very simple proof here.

So, since  $(x - \alpha)$  is a factor of  $f(x)$ , that means I can express my  $f(x)$  as the product of two polynomials with one of them being  $(x - \alpha)$  the remaining thing I can write it as some  $g(x)$  polynomial; that means what can I say about the value of the polynomial  $f$  evaluated at  $\alpha$  that will be same as the product of  $\alpha - \alpha$  with the polynomial  $g(\alpha)$  but  $\alpha - \alpha$  will give you the additive identity 0.

Because  $-\alpha$  is the additive inverse of  $\alpha$  and 0 multiplied with  $g(\alpha)$  will give you 0 element, that is a simple proof. Let us see the proof in the reverse direction. So imagine your polynomial  $f$  is such that when evaluated at  $\alpha$  gives you 0. If that is the case then I have to show that  $(x - \alpha)$  is a factor of  $f(x)$ . So, I utilize my division theorem and as per the division

theorem I can say that my  $f(x)$  when divided by  $(x - \alpha)$  will give me some quotient and some remainder. This comes from your division theorem.

And my goal is to show that  $r(x)$  is 0 that is my goal. So, how do I show that  $r(x)$  is the 0 polynomial well I know that the degree of  $r(x)$  polynomial is strictly less than the degree of  $(x - \alpha)$  because  $(x - \alpha)$  is treated as a divisor here or I know that  $r(x) = 0$ . If  $r(x)$  is definitely 0 my proof is done because then I show that  $f(x)$  is equal to the product of  $q(x)$  and  $(x - \alpha)$  and  $(x - \alpha)$  is a factor of  $f(x)$ .

But I cannot definitely claim that  $r(x)$  is always 0 I have to logically conclude that. So, again if this is the form of  $f(x)$  I can say that  $f(\alpha)$  will be this. And now I use my premise my premise says that  $f(\alpha)$  is 0. So, if  $f(\alpha)$  is 0 I substitute this value and this term is anyhow 0. So, I get that  $r$  polynomial evaluated at  $\alpha$  is 0. And now I can logically argue that indeed if  $r$  polynomial evaluated at  $\alpha$  is 0 then I get a contradiction to this case.

So, remember my 2 possible cases for  $r(x)$  is that either its degree is less than the degree of  $(x - \alpha)$  or  $r(x)$  is 0. Now if  $r(x)$  polynomial has a degree less than the degree of  $(x - \alpha)$  polynomial then what can I say about  $r(x)$  polynomial. I can say that  $r(x)$  polynomial is a constant polynomial because the degree of  $(x - \alpha)$  is 1 and if degree of  $r(x)$  is less than 1 the only possible degree which is less than 1 is 0.

That means I am actually considering the case when  $r(x)$  is a constant polynomial but if  $r(x)$  is a constant polynomial then it does not matter whether I evaluate it at  $\alpha$ ,  $\beta$  I should get the same value. But here I am getting that  $r$  polynomial evaluated at  $\alpha$  is a 0 value. So these 2 things these 2 conditions goes against each other that means this case is not at all possible that means you cannot have degree of  $r(x)$  strictly less than the degree of  $(x - \alpha)$ .

Because if that is the case then that goes against this conclusion that  $r$  polynomial evaluated at  $\alpha$  is 0. That means the only case that is left is that your  $r(x)$  polynomial is 0 polynomial which shows that this is 0 polynomial and hence  $f(x)$  is completely divisible by  $(x - \alpha)$  showing that  $(x - \alpha)$  is a factor of  $f(x)$ .

**(Refer Slide Time: 41:49)**

## Roots of a Polynomial Over Fields and Properties

**Root of a Polynomial:**  $\alpha \in \mathbb{F}$  is called a root of the equation  $f(x) = 0$ , where  $f(x) \in \mathbb{F}[x]$ , provided  $f(\alpha) = 0$  over  $\mathbb{F}$

How many roots, if  $f(x)$  has **degree**  $n$ ?

**Theorem:** If  $f(x) \in \mathbb{F}[x]$  has degree  $n \geq 1$ , then  $f(x) = 0$  has **at most**  $n$  **roots**

❖ Let  $\alpha_1, \dots, \alpha_m$  be the **roots** of  $f(x) = 0$  // We want to show that  $m \leq n$

❖  $f(\alpha_1) = \dots = f(\alpha_m) = 0$  over  $\mathbb{F}$   $n =$

❖  $(x - \alpha_1), \dots, (x - \alpha_m)$  are **divisors** of  $f(x)$  // Using **Factor theorem**

❖  $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m)g(x)$  for some  $g(x) \in \mathbb{F}[x]$

➤  $(x - \alpha_1), \dots, (x - \alpha_m)$  are **irreducible polynomials** over  $\mathbb{F}[x]$  }  $m \leq n$

❖ Over  $\mathbb{F}$ , **degree of a product** = **sum of the degrees of the factors**

Now based on this factor theorem what we define is the root of a polynomial. So, a value  $\alpha$  from the field will be considered as the root of this equation  $f(x) = 0$  where  $f(x)$  is a polynomial over the field provided the polynomial evaluated at  $\alpha$  gives you the value 0 over the field. So, again this is kind of a generalization of the notion of roots that we are familiar with.

Now the next question is that how many roots I can have if my polynomial has degree  $n$ , so I can prove a familiar result. So, we know that for the regular polynomials if we have degree  $n$  then it can have at most  $n$  roots in the same way I can show that if my polynomial is over a field then this equation  $f(x) = 0$  can have at most  $n$  roots how do we prove this? So, imagine that  $\alpha_1$  to  $\alpha_m$  are the roots of your equation  $f(x) = 0$ .

And we want to show that  $m$  is less than equal to  $n$  upper bounded by  $n$  that is my goal. Now as per the definition of a root since  $\alpha_1 \alpha_2$  each of them is a root I know that the  $f$  polynomial evaluated at  $\alpha_1$ ,  $f$  polynomial evaluated at  $\alpha_2$ ,  $f$  polynomial evaluated at  $\alpha_m$  all of them will give you the value 0 over the field. And if they give the value 0 over the field that means I can say that each of these polynomials as per the factor theorem are divisors of my polynomial  $f(x)$ .

That means I can say that I can write down my  $f(x)$  polynomial as the product of these  $m$  individual degree 1 polynomials followed by some leftover polynomial  $g(x)$  where  $g(x)$  could be some polynomial over the field. And an important thing to notice here is that each of these



polynomials  $(x - \alpha_1), (x - \alpha_2), (x - \alpha_m)$  they are irreducible polynomials because they are already any how polynomials of degree 1.

And they are non constant polynomials and I also know that over a field if I multiply several polynomials then the resultant polynomial will have a degree which is actually the sum of the degrees of the individual factors. This is possible over a field but this is not true over a ring we already proved that. So, now if I apply this fact over this statement.

I know that the degree of  $f(x)$  is  $n$ . And I know that this  $f(x)$  is definitely at least a product of  $m$  factors plus there is something else as well  $g(x)$  is another additional factor. So, the degree of  $f(x)$  is  $n$  that is given to me and since it is the product of at least  $m$  factors, I can say that definitely  $n$  is greater than equal to  $m$  which is what I wanted to show because each of these factors contribute 1 to the overall degree of  $f(x)$  which is  $n$ .

(Refer Slide Time: 45:59)

### Finding Irreducible Factors of a Polynomial

- Simple methods for finding irreducible factors of small-degree polynomials over  $\mathbb{Z}_p[x]$ 
  - ❖ Irreducible factors serve the same role as prime factors of an integer
  - ❖ Interesting case: when the polynomial to be factored and factors are monic

Degree  $d$  monic polynomial: coefficient of  $x^d$  is 1

- Ex: Find all (monic) irreducible factors of  $f(x) = x^4 + 1$  over  $\mathbb{Z}_3[x]$ 
  - ★ Checking for linear factors //  $(x - \alpha)$  is a factor, provided  $f(\alpha) = 0$
  - $f(0) = 1$      $f(1) = 2$      $f(2) = 2$
  - ❖ Since  $f(x)$  has no linear factors, it can have two quadratic factors

$x^4 + 1 = (x^2 + Ax + B)(x^2 + Cx + D)$ , where  $A, B, C, D \in \mathbb{Z}_3$

(1) $A + C = 0$	(3) $B + D + AC = 0$	<ul style="list-style-type: none"> <li>❖ From (1), <math>A = -C</math> and from (4), <math>B = D</math></li> <li>❖ If <math>B = D = 2</math>, then from (3), <math>AC = 2</math> and <math>A = -C</math></li> <li><math>A = 1, C = 2</math> satisfies all conditions</li> </ul>
(2) $AD + BC = 0$	(4) $BD = 1$	

$B = D = 0$   
 $B = D = 1$   
 $B, D \in \{0, 1, 2\}$

So, now the next thing is; next question is how exactly we find irreducible factors of a polynomial how exactly we do the factorization. So, it turns out that we do have some simple methods for finding irreducible factors for the special case where my polynomials are over  $\mathbb{Z}_p[x]$  and where my polynomials are of small degrees. And if you are wondering what exactly is the whole purpose of finding out the irreducible factors basically the problem is something similar to finding the prime factorization of an integer.

So, you are given an integer you want to factorize it in the same way you are given polynomial and say if it reducible I want to find out its irreducible factors. So, there are some

well known methods for that we will discuss one of the methods for a special case when the polynomial that we want to factor is a monic polynomial as well as the factors which we want to find out they are also monic.

By the way what is a monic polynomial? A polynomial is called as a monic polynomial and degree  $d$  if the coefficient of  $x^d$  is 1. So, now let us see this method, by the way this method is mechanical and it will work only when your polynomial is of small degrees. So, suppose this polynomial  $(x^4+1)$  is given to me and I already showed you the factors of this polynomial but now let us try to find it out.

So, if at all this polynomial has a factor it will have either linear factors; it will have several linear factors possible or it can have 2 possible quadratic factors or it can have 1 linear factor and 1 cubic factor and so on these are the various possibilities because the degree of  $f(x)$  is 4. So, now let us check for linear factors that means can I write  $f(x)$  as product of some  $(x - \alpha)$  and another polynomial where  $\alpha$  is some element from  $\mathbb{Z}_3$ .

So, remember that if at all  $(x - \alpha)$  is a factor of this  $f(x)$  then this  $f(x)$  polynomial evaluated at  $\alpha$  should give me the value 0. So, let us check whether  $\alpha$  can be 0 or not or  $\alpha$  can be 1 or not or  $\alpha$  can be 2 or not why only these 3 values? Because everything is allowed to be from  $\mathbb{Z}_3$ . Now it turns out that neither  $f(0)$  nor  $f(1)$ , nor  $f(2)$ , is 0 by the way all the operations are performed over  $\mathbb{Z}_3$  namely all the addition and multiplications are modulo 3.

That means I can rule out the possibility of linear factors. Now since linear factors are not possible the next thing that we I want to check is whether it can have 2 quadratic factors possible. Now if at all it has quadratic factors it can have 2 quadratic factors. So, let me write down it in the form of 2 quadratic factors and remember I am interested to find out the monic factors so that is why one of the monic quadratic factors I am writing like this  $(x^2 + Ax + B)$ .

And another unknown monic quadratic factor I am writing like this  $(x^2 + Cx + D)$ ; my goal is to find out whether I can find out A, B, C, and D or not. Where A, B, C, D are allowed to be from  $\mathbb{Z}_3$  not  $\mathbb{Z}_3[x]$ . So, now if at all this  $f(x)$  polynomial can be expressed as the product of 2 quadratic factors these 4 conditions should be satisfied : (1)  $A + C = 0$  (2)  $AD + BC = 0$  (3) B

+ D + AC = 0 (4) BD = 1. Why so? Because you see what will be the coefficient of  $x^3$  as per my right hand side? It will be  $(A + C)x^3$ .

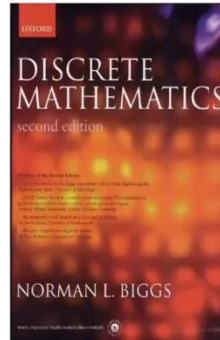
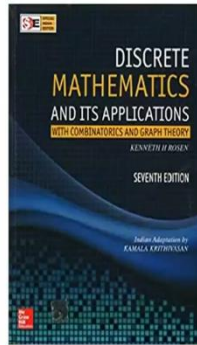
Because  $Ax$  into  $x^2$  will give me  $A$  times  $x^3$  and  $Cx$  multiplied with  $x^2$  will give me  $Cx^3$ . So, the coefficient of  $x^3$  will be  $A + C$  and I want that  $A + C$  should be 0 because in my left hand side there is no coefficient of  $x^3$  in the same way I am basically just comparing the various powers of  $x$  in the LHS and RHS and arriving at these 4 equations. Now I have to check whether I can satisfy all these 4 equations simultaneously given that my  $A, B, C, D$  can take values from the set  $\mathbb{Z}_3$ .

Now from the first equation I can conclude that  $A$  should be minus  $C$ . And from my fourth equation I can conclude that  $B$  should be equal to  $D$  why  $B$  should be equal to  $D$ ? Because my  $B$  and  $D$  are allowed to be only from the set 0, 1, 2. So,  $B$  and  $D$  are both allowed to be from the set 0, 1, 2. So, I cannot have different values of  $B$  and  $D$  from this set 0, 1, 2. But when multiplied together and then taken modulo 3 gives me the value 1. So, the only possibility that  $B, D$  gives me 1 is when both  $B$  and  $D$  are 1 or both  $B$  and  $D$  are 2. Now I can simply rule down the possibility of  $B = D = 0$  that is not allowed because if that is the case  $B$  into  $D$  cannot be 1. But I cannot have  $B$  and  $D$  both equal to 1 because a both  $B$  and  $D$  are equal to 1 then my third equation gives me that product of  $A$  and  $C$  should be 1.

And then as per the same logic  $A$  should be equal to  $C$  but that goes against the conclusion that I get from the first equation  $A = -C$ . So, I can rule down  $B$  and  $D$  equal to 1 as well. So, the only option left is check whether  $B$  and  $D$  can be 2 and if  $B$  and  $D$  are 2 then as per the equation 3 I get  $AC$  should be equal to 2. And if  $AC = 2$ , I can satisfy it by saying that  $A = 1$  and  $C = 2$  and that does not violate this condition that  $A = -C$ .

**(Refer Slide Time: 52:51)**

## References for Today's Lecture



That means I can now safely say that  $A = 1, B = 2, C = 2, D = 2$  satisfies these condition and hence I can factorize my  $x^4 + 1$  as product of 2 quadratic monic factors with that I conclude today's lecture. Thank you.