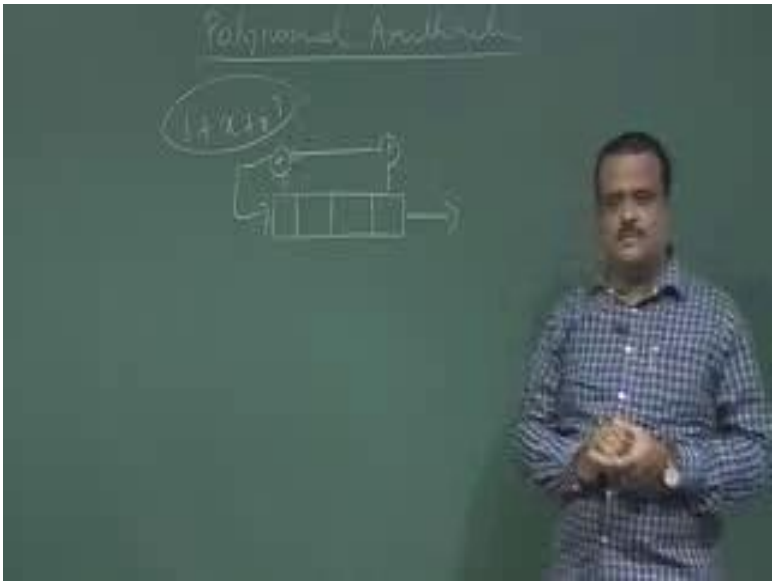
**Internetwork Security**
**Prof. Sourav Mukhopadhyay**
**Department of Mathematics**
**Indian Institute of Technology, Kharagpur**

**Lecture - 20**
**Polynomial Arithmetic**

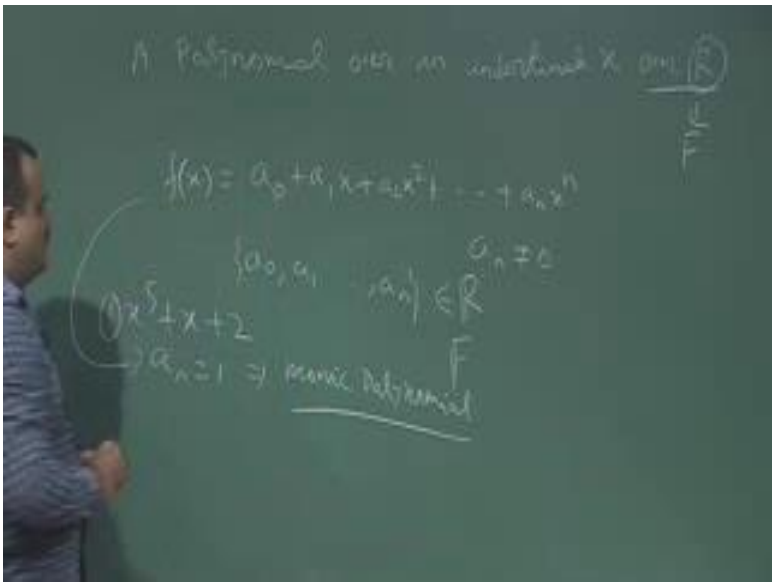
So, we talk about polynomial arithmetic, so we have seen for LFSR we have used something called primitive polynomial like 1 plus x plus x to the power of 4. So, this type of polynomial we have seen in the LFSR, where LFSR are showed 4 bit LFSR.

(Refer Slide Time: 00:31)



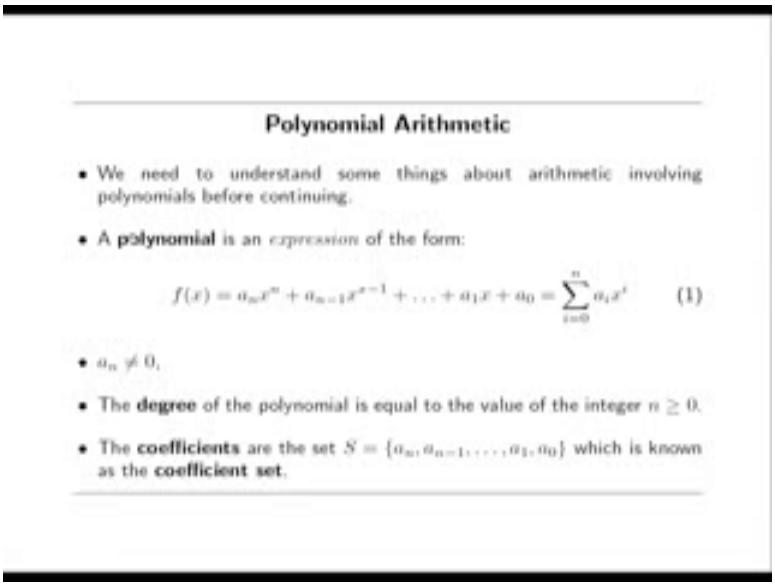
So, every LFSR is associated with a polynomial, so this polynomial is basically we have a connection over here and we have a connection over here. So, this is the LFSR corresponding to this polynomial and we have seen this LFSR is a good LFSR, good sequence generator; pseudo random number generator because it is give us the full period and it satisfies some good statistical properties also. So, we have seen this is called primitive polynomials, so this is the today's lecture we will talk about details of the polynomials, what is primitive polynomial, what is irreducible polynomials.

(Refer Slide Time: 01:34)



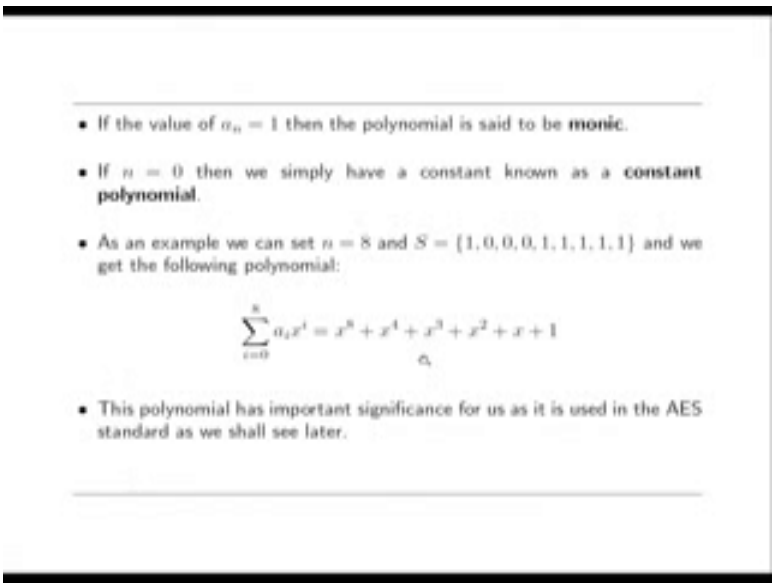

So, basically what is the polynomial? So a polynomial over an indeterminant x; x is a very well over an indeterminant x. So, it is in terms of x and it is over a usually defined over a ring, but this is sometimes it is a field to have some properties of what is called Galois Field we will formally define the Galois Field. So, it is basically the expression like this a 0 plus a 1 x plus a 2 x square plus a n x to the power of n; this form and this is denoted by F of x. So, this is called a this expression is called a polynomial of degree n provided this a n is not equal to 0 and these are called coefficients; these a 0, a 1 these are basically coming from some set these are coming from say some field or some ring or so. So, polynomial can be defined over a ring, so these are the elements are coming from some ring or it could be coming from some field for certain property to have, so we will formally define those.

(Refer Slide Time: 03:13)




So, let us go the slide please, so this is the expression for the polynomials. So, any expression of this type is called polynomial where this should be called n degree polynomial; if a n is not equal to 0 and these are called a 0, a 1, a 2, a n are called coefficient set or these are called coefficient of the polynomial. So, these coefficients are basically coming from some ring or it could be come from some field.

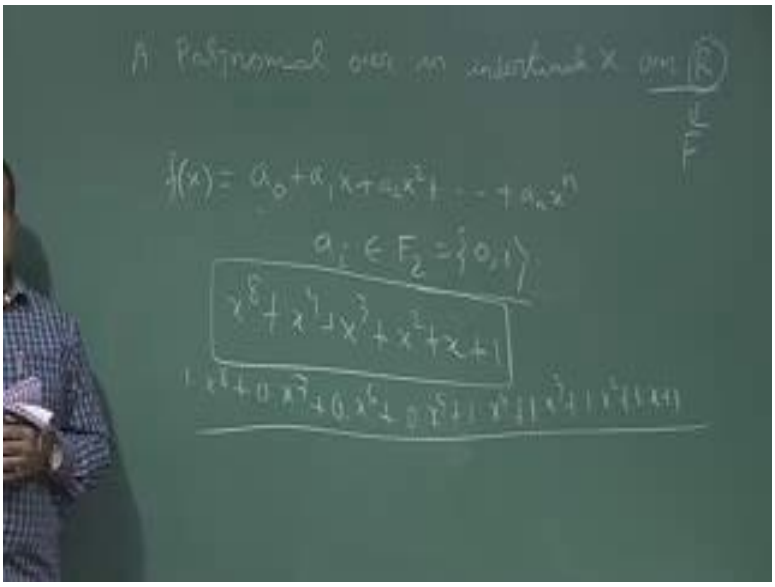
(Refer Slide Time: 03:45)




So, now this polynomial will be called monic polynomial; if the coefficient of a n is 1 so; that means, if this is 1 then it is called monic , so polynomial like this x to the power of 5

plus x plus 2. So, this is a monic polynomial because the coefficient corresponding to the highest degree is 1, so if a n is 1 then it is called monic polynomial; (Refer Time: 04:26) is the degree of this polynomial. So, this is if the highest degree is 0 then this is basically a constant.

(Refer Slide Time: 04:54)



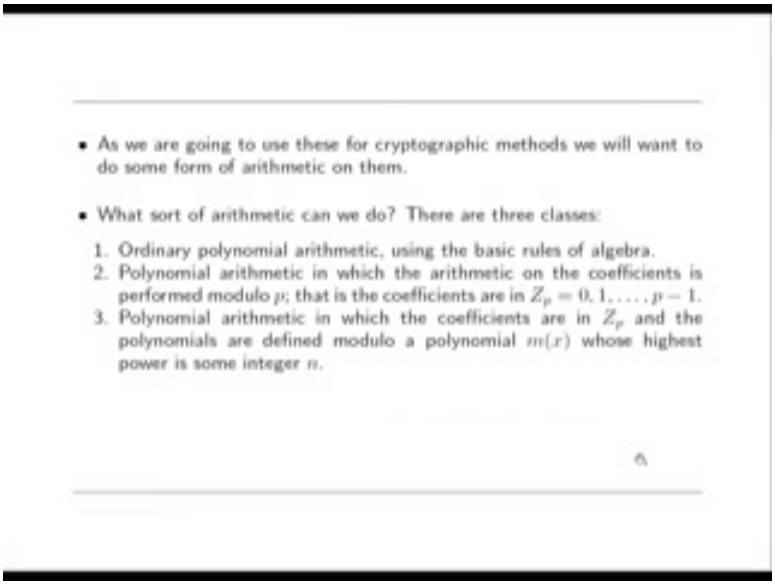
So, now let us take an example suppose n is 8 and suppose the polynomial coefficients are coming from 0, 1. So, the coefficients are coming from 0 1, so that is basically a F two, so if you take this polynomial where a i's are coming from F 2; F 2 is a field this binary, so these are all binary bits this a 1, a 2 are all are binary bits. So, if you take this polynomial and we will see this particular form of this polynomial is x to the power of 8 plus, x to the power 4 plus x 3 plus x square plus x plus 1. So, this polynomial is used in the AES, so when you talk about the block cipher, standard AES; Advanced Encryption Standard, the Rendell we will talk in a futures talk lectures.

So, there the designer used this polynomial; so this polynomial is basically over F 2 coefficients are basically 0 or 1 because coefficient of; so this is basically 1 into x to power of 8 plus 0 into x to the power of 7 plus 0 into x to power of 6 plus 0 into the x to the power of 5 plus 1 into the x to the power of 4 plus 1 into the x cube plus 1 into x square plus 1 into x plus 1, so these are the coefficients sets of this polynomial.

So, this is the 8 degree polynomial; this is the irreducible we will talk about what do you mean by irreducible polynomial. So, this is the irreducible polynomial of degree 8 over

this F 2. So, this is the polynomial and this polynomial has important significance for us as it is used in AES standard.

(Refer Slide Time: 06:38)

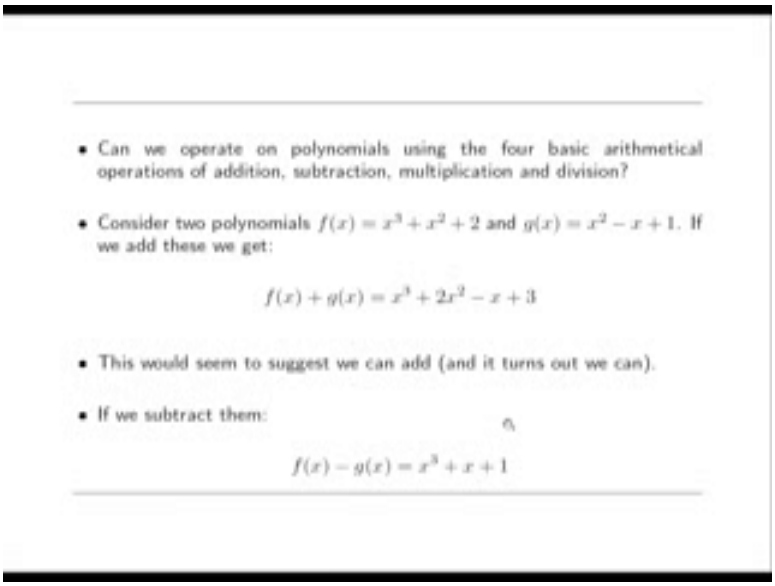



So, now for our cryptographic purpose what we will do in this polynomial arithmetic. So, we will basically do the ordinary polynomial arithmetic like how to add two polynomial, how to multiply polynomial, how we can divide two polynomial like this. So, those are polynomial arithmetic addition, multiplication, division so and also we will talk about polynomial arithmetic, but the coefficients are (Refer Time: 07:12).

So, here the ordinary polynomial arithmetic means the coefficients are real number, it is coming from real number field. Now the polynomial we will talk about for our cryptographic purpose over z p, so Z p means p is the prime Z p is that 0 1 up to p minus 1. So, this is the residue class, so Z p; so now, we will our coefficients are coming from Z p then we will talk about addition of two polynomial, multiplication of two polynomial over some polynomial which is m; x which is a irreducible polynomial you should take then it will form a group that we will talk about this in more details.

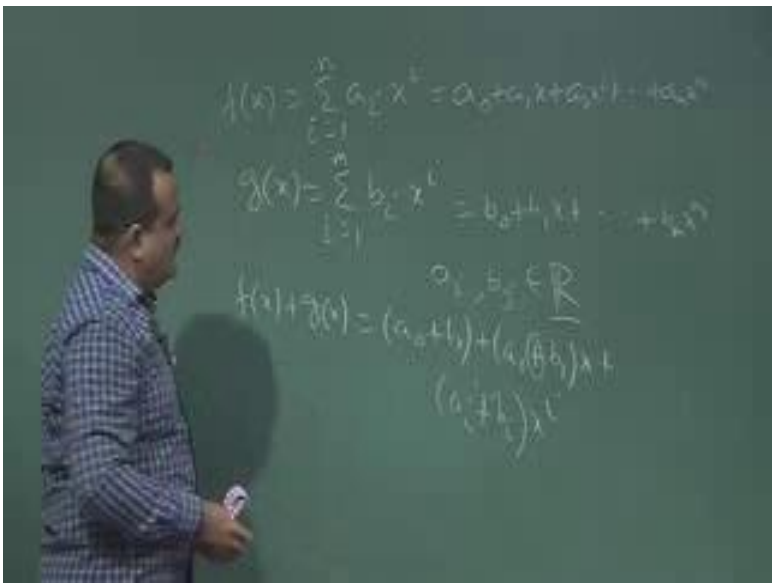
So, we take a polynomial m x which is typically irreducible polynomial like we have if this is m x; this polynomial then we will talk we consider all polynomial mod m x basically, so that set. So, we have to define those issues in our; these polynomial arithmetic class; so the coefficients are coming from Z p; so if p is 2 it is coming from z 2; 0 1.

(Refer Slide Time: 08:34)




Now, let us talk about ordinary polynomial addition, so if we have two polynomials say f x and G x and if their degrees are different; say suppose we have. So, this is the ordinary polynomial addition, so we have polynomial f x which is basically summation of a i; x i x i is equal to 1 to n. So, this is basically a 0 plus a 1 x plus a 2 x square plus a n x to power n; can you please go to the board please.

(Refer Slide Time: 09:28)



So, then we have another polynomial G x; which is basically b i x to the power i; i is equal to 1 to m. So, this is basically b 0 plus b 1 x plus b n or b m x to the power of n, so

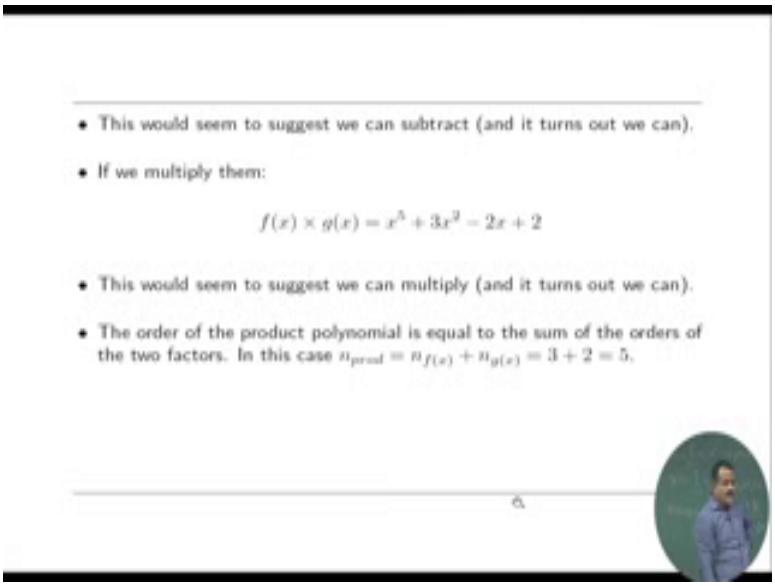
two different degree polynomial. So, and this a I, b i's are coming from a ring or field; this could be a ring or it could be a field. We need this to be a field to have that polynomial set irreduce that polynomial mod some irreducible polynomial to be a cyclic group, so this is called Galois Field; we will talk about that.

So, the addition is simply the addition of the coefficient because this; so f x plus G x is basically a 0 plus b 0 plus a 1 plus b 1 x plus like this. So, a i plus b i x to the power i, so this plus is basically the field addition operation or the ring addition operation. So, in the ring or in the field we have two operation; addition and multiplication. So, there we can add two coefficients, two number, two element, so these are the element coming from that ring or field; so we can add these. So this operation is basically operation in that ring of the field, so basically we are doing the addition over the coefficients; so this is the basic addition operation.

So, if you take for example, if you take two polynomials slide please. So, if you take two polynomial f x and G x; so f x and G x. So, f x is basically x cube plus x square plus 2 this is this, now if you add these two. So, x cube is now the coefficient 1 there is no x cube, so for x square you have coefficient 1 and here 1. So, it will give us 2 and for x there is no 1 there is minus 1, so it is minus 1 then constant 1 a 0, b 0 is 2 and 1; so it is 3; so it is basically the addition of f x plus G x.

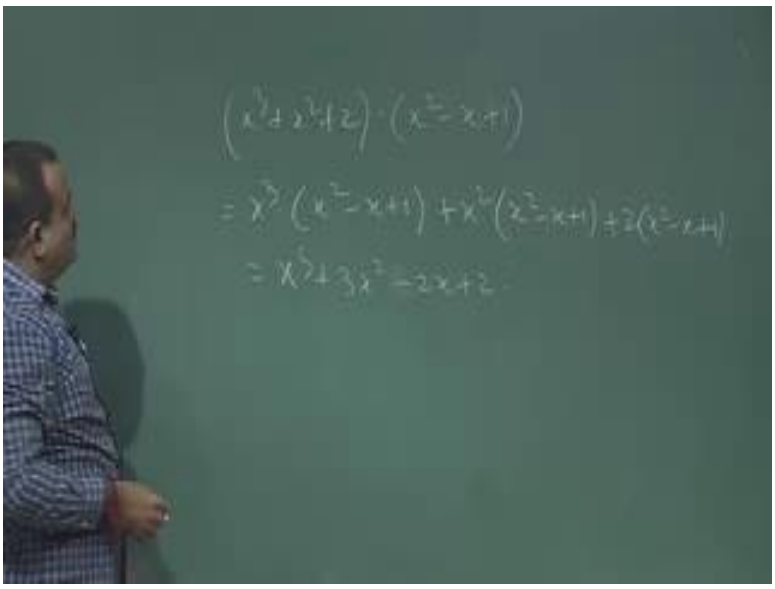
Now we can similarly we can define the subtraction; subtraction is basically we will just take the minus of G x; minus of G x is basically we will the minus of a i's of the coefficients then we take the addition.

(Refer Slide Time: 12:19)




And then the multiplication is basically, if you want to multiply a 2 polynomial that f x; G x, so multiplication is basically we just take this into this. So, we first multiply; so this is the simple multiplication operation. So, here x is just a symbol; it is the indeterminant variable and all the operations will be over the coefficients.

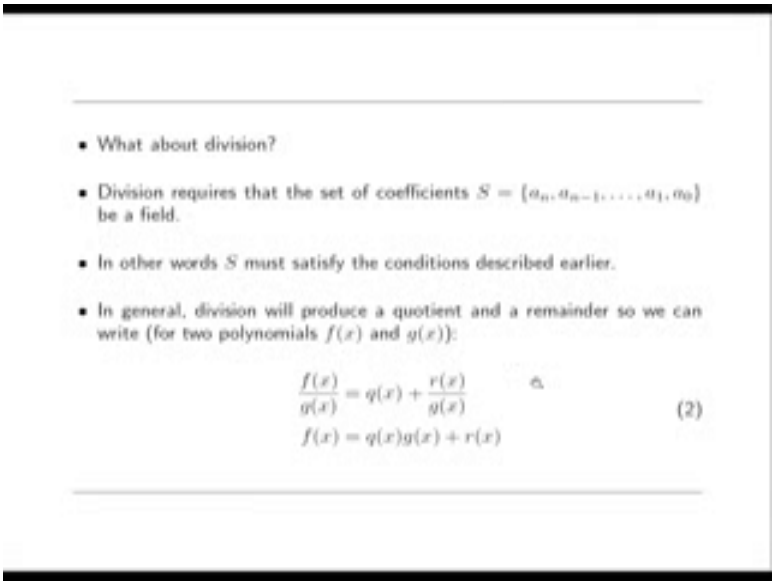
(Refer Slide Time: 12:51)



So, if we have two polynomials x cube plus x square plus 2; this is one polynomial, if you want to multiply this with another polynomial; x square minus x plus 1. So, this multiplication is simply we will while first take the x cube into x square minus x plus 1

then plus x square x plus 1 then plus 2 x square minus x plus 1. So, this will basically give us x to the power 5; this will give us x to the power of 5 plus and so here we need to do the addition operation over the ring or over the field. So, minus 2 x plus 2; so simple multiplication operation and that degree will be basically degree of this polynomial plus degree of this polynomial; so this is 5.

(Refer Slide Time: 14:01)




So the order or degree of the product polynomial is basically degree of the sum of their degree. So now how to divide two polynomials? So if you have two polynomials f x and G x. Now suppose f x has degree more and G x has degree less, so now we want to divide f x by G x. So, this is we know the real number divisions, so if you want divide say two real number say 12 and 5; so we have two real number a is 12 and b is 5.

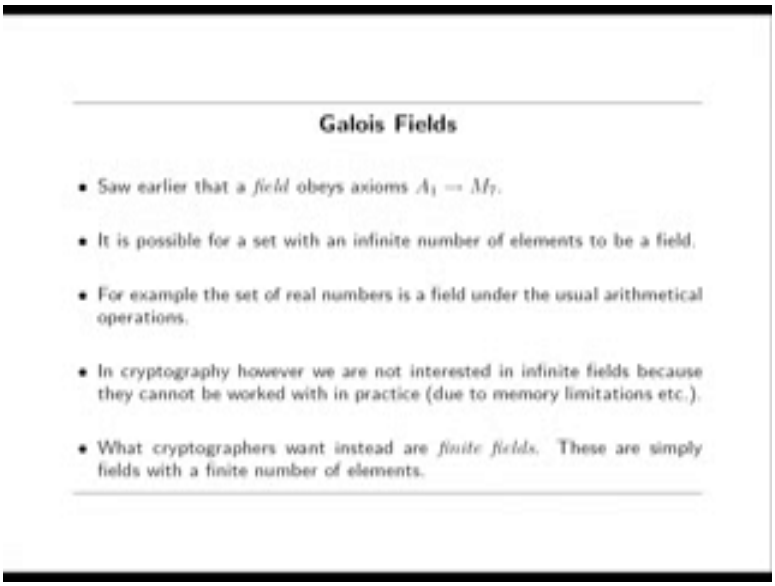
(Refer Slide Time: 14:55)

So, how to divide two real number? So a is 12 and b is 5; so we want to divide 12 by 5. So, 12 can be written as 2 into 5 by 5 plus 2. So, 12 can be written as 25 by 2, so this 2 is basically a coefficient; so this is basically a by b; this is basically 2 and this is the remainder. So, similarly for polynomial also if you have two polynomial f x and G x, if the degree of f x is more. So, now we want to divide f x by G x so that means; so f x should be written as some q x, G x plus r x and this r x is called remainder polynomial and the degree of r x must be less than degree of G x, otherwise we have to divide again and this is called quotient; so then the degree of r x must be less than degree of G x.

Now if r x is 0 then we call G x divides F x; so G x is a factor of f x then you say G x divides f x; that means, G x is a factor of f x. Now we called a polynomial to be a irreducible polynomial, if it has no factor; if such G x will not exist then we called the polynomial will be an irreducible polynomial, for irreducible polynomial it has no factors we cannot reduce further. So, like this if we have say some polynomial x cube plus x square plus x; this polynomial is not irreducible polynomial because this polynomial can be factor like this, x into x square plus x plus 1.

So, this is not irreducible polynomial; so there exists a G x such that it divides f x. So a polynomial will be called irreducible polynomial if it has no factor. So, let us come back to the division, so this is the division arithmetic for two polynomial f x and G x and this q x is called quotient and this r x is called remainder polynomial.

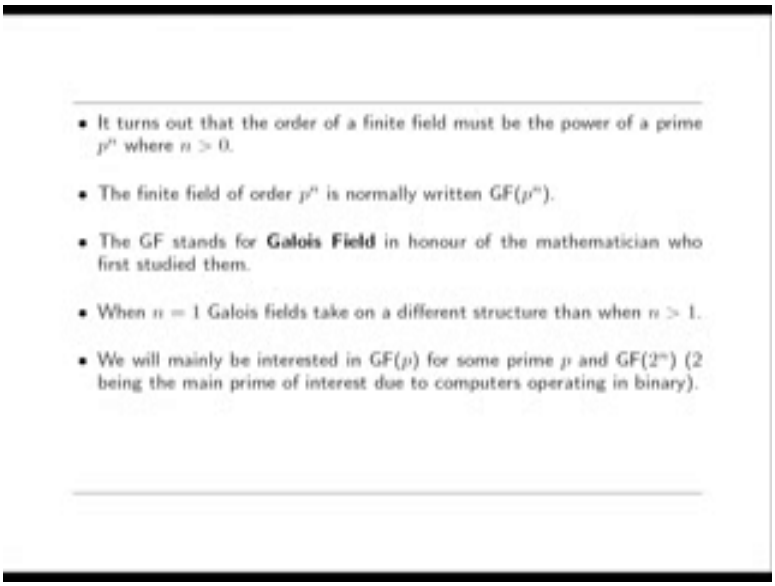
(Refer Slide Time: 17:45)



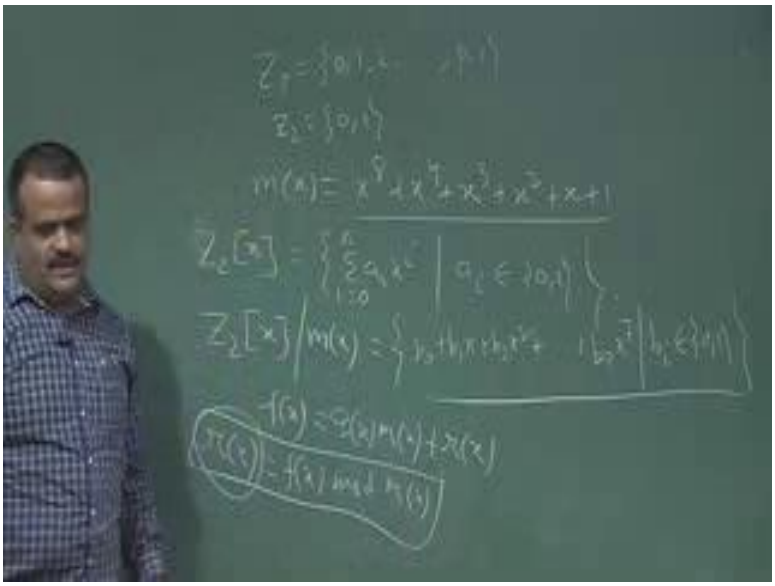

So, now we talk about Galois Field or over the polynomial, so far now for field operation we have seen there are some properties like these are the properties are there when we talk about field. So, these are the properties; it should obey for the set to be field under this two operation plus and dot and this field could to be infinite, we have seen the real number field; set of real number with the real addition and multiplication is a field and it is a infinite field, but infinite field is not about interest because of; we cannot take infinite number in a memory or computerized finite memory.

So, for memory limitation and everything, so we need to talk about finite field; that means, the set on which we are talking about field should be finite, the number of elements should be finite in that set.

(Refer Slide Time: 19:02)




(Refer Slide Time: 19:12)



So, how to get such finite field; so we have seen the field like z p, now we want to have a polynomial field, so we have seen the Z p; Z p is basically 0, 1, 2 up to p minus 1 and z 2 is basically just the 0 and 1. Now if you take a irreducible polynomial over z 2; say we have a example of irreducible polynomial; we have just seen which is used for AES.

So let us take that example; we can take another there are many irreducible polynomial. So, suppose let us take a irreducible polynomial, the same irreducible polynomial we have; so now let us consider all the polynomial which is basically z 2 x, z 2 x is basically

this is the set of all polynomials summation of a i; x i to the power of i; i is from 0 to n; n could anything and a i's are coming from z 2. So, suppose we take; so we take all possible polynomial whose coefficients are basically 0 1 and which is of any degree.

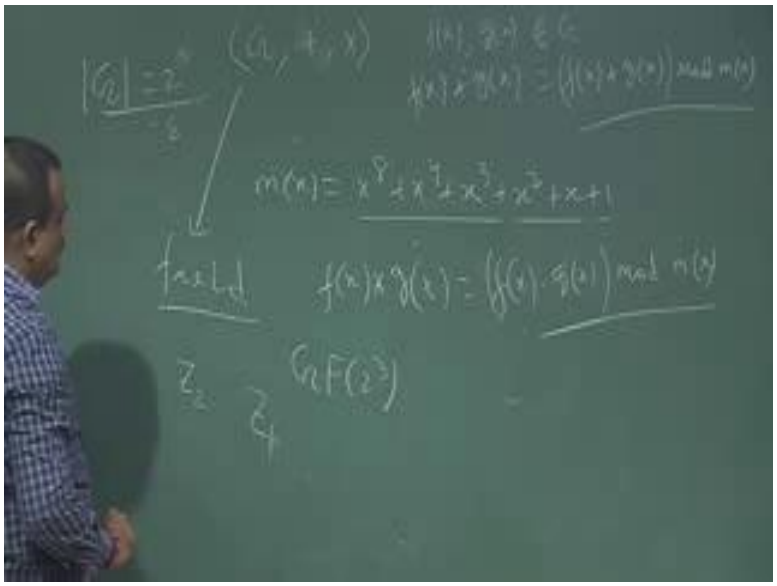
So, this is one polynomial 1 plus x 1 plus x square plus x to the power of 10, 1 plus x plus x to the power of 9; x to the power of 100 and 1 like this any such polynomial, but the coefficient must be coming from z 2. So, that set is denoted by z 2 x; this is the set of all polynomial which of any degree whose coefficients are basically binary bits.

Now we take the modular of irreducible modular of this polynomial. So, we take z 2 x m x, so this set is basically. So, we take any arbitrary polynomial of any arbitrary degree then we try to divide that with this irreducible polynomial. So, then the degree of that polynomial of the remainder then the degree will be of degrees maximum 7. So, this will be the set of all polynomial whose degree is like this b 0 plus b 1 x plus b 2 x square up to; this is from 0. So, b 1 x, so b 7, x to the power of 7 where b i's are coming from 0 and 1, so this set.

So, basically the idea is we take a arbitrary polynomial of any degree then we try to divide that polynomial with this degree. So, if you take any arbitrary polynomial of any degree; so if you try to divide by this then we will get some quotient and some remainder and the remainder is basically mod of that polynomial f x; mod m x. This remainder polynomial is the mod of that polynomial because that is the remainder polynomial and since the mx degree of m x is 8. So, the degree of this remainder polynomial will be maximum 7 otherwise we have to divide again.

Now, if you consider this polynomial and it can be shown that this polynomial will form a field under polynomial addition and multiplication and this, so this polynomial set. So this we denote by say G F; this is G F 2 basically 2; 2 to the power 2 or we can just anyway this is called Galois Field. So, sorry G 2 to the power 8 because what is the number of element which if this is the set case or G set.

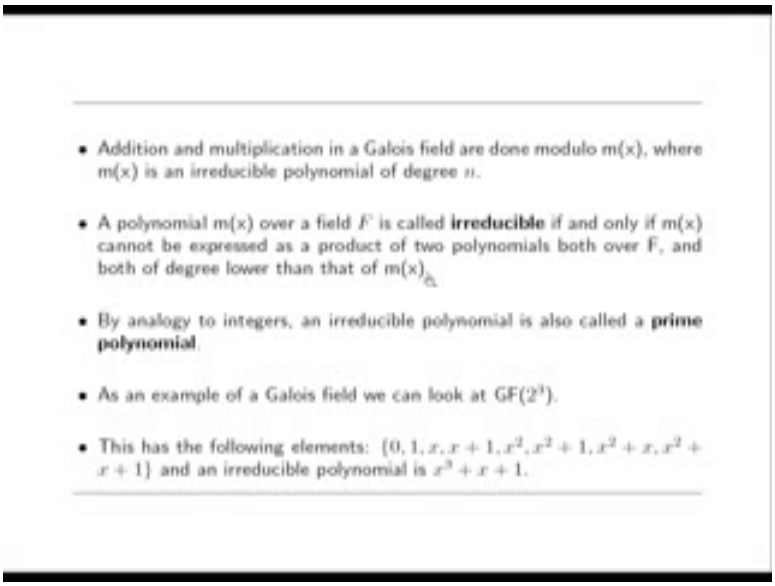
(Refer Slide Time: 23:26)



Now, what is the cardinality of G set cardinality of G set is all possible values of this b 0 and b 1. So, there are two possible 2 to the power 8, so this is a finite set and we can show that G with this plus and multiplication and this plus is basically if you take any 2 element f x and G x, form this set G this plus is basically G x. So, this polynomial plus mod that m x this is how we define this plus so; that means, we take any 2 polynomial of degree 7; we add it up and then we take the mod and similarly, so this is under modular operation of m x; so polynomial modulation modular operation of 7.

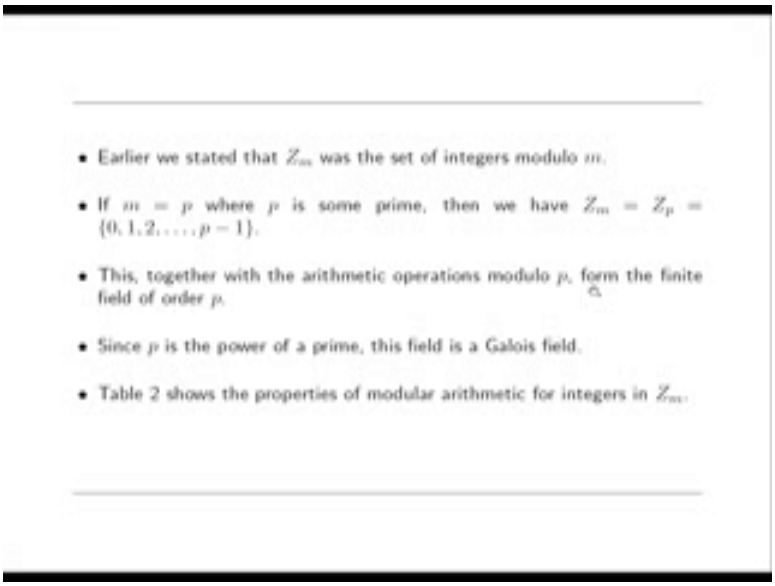
So, this is again similarly multiplication is also same under the modular operation, so if you take two polynomial f x and g x; f x into g x is basically the polynomial multiplication mod m x. So, it can be shown that this is a field, so this field is called finite field because the number of element is finite, so this is also called Galois Field.

(Refer Slide Time: 25:46)



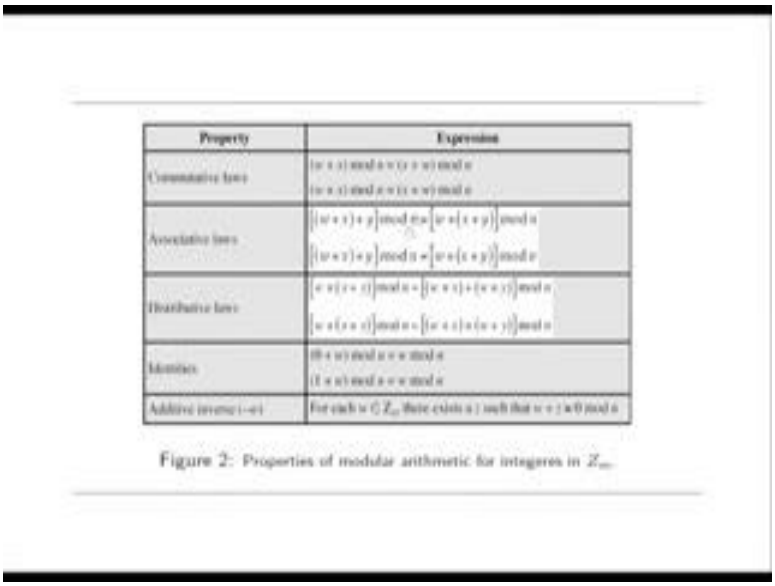

So, this is coming from the irreducible polynomial, so you have to choose a irreducible polynomial and then irreducible polynomial is also called a prime polynomial because it has no factor other than 1 and m x because it cannot be reduced further. So, that means, in the prime number we know if a number is prime; that means, it has only 1 it has 2 factor 1 and itself so; that means, similarly for m x also it has only it has no factors so; that means, so this is also called prime polynomial; not primitive polynomial; we will define primitive polynomial. So, this is called Galois Field of 2 to the power 3 because this is 8; 2 to the power of 3 that is 8, so this is called G F 2 to the power of 3. So, instead of z 2 we take Z p also, where p is the prime then it will be general group of G F p.

(Refer Slide Time: 26:54)



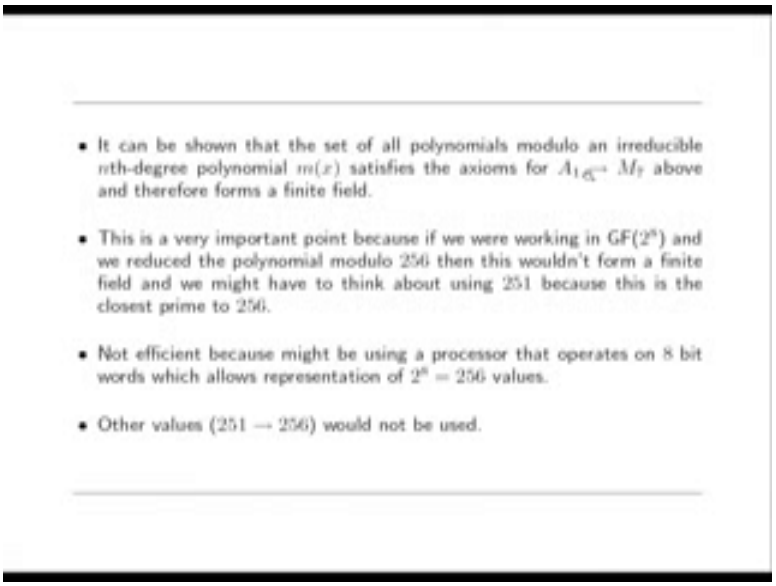

(Refer Slide Time: 27:01)

.




So, this is the, so we take p to be prime in order to have these groups, so these are the operations over this; this is just to recall to have the group this is the modular operation over mod m, so here we are choosing n to be p.

(Refer Slide Time: 27:15)




So, now this is under these two operations; we have already talked about this; so this is forming the group. Now how to define a primitive polynomial? So we know the Galois Field, so it is a group under both multiplication and the addition.

(Refer Slide Time: 27:37)


Now, a polynomial is called a primitive polynomial. If it is a generator of that cyclic group, if it is generator or the primitive element; generator is also called primitive element of the group that Galois Field; I mean 2 to the power of 3 say in general it is 2 to the power of G of p. So, this is a group; so this G; so it is a group under multiplication

also; so it is a cyclic group. So, if we take a polynomial say P x; it will be a; so first of all it has to be irreducible polynomial. So, every primitive polynomial is irreducible polynomial; on top of that it should have extra property that it should be the generator of that group. So, it should generate the group G in the multiplicative sense, so this is the primitive polynomial and we have seen this primitive polynomial in the context of LFSR.

Thank you.