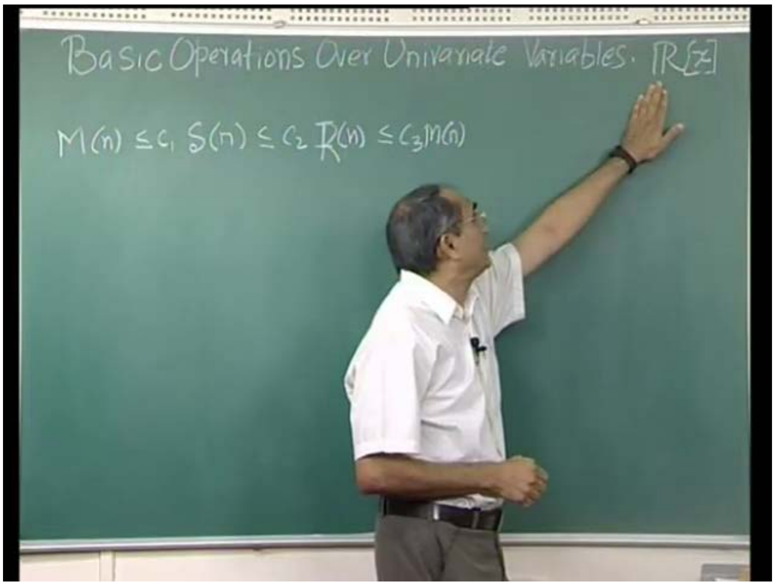
Computer Algorithms – 2
Prof. Dr. Shashank K. Mehta
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture - 19
Integer Polynomial Ops III

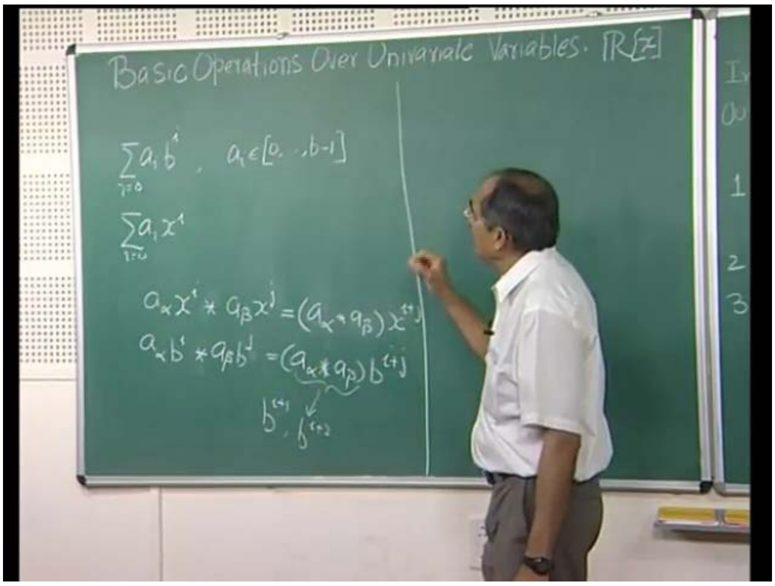
(Refer Slide Time: 00:21)


Basic Operations Over Univariate Variables. $\mathbb{R}[x]$
$M(n) \le c_1 S(n) \le c_2 R(n) \le c_3 M(n)$

In the last lecture, what we saw was that the basic operations on integers have the same complexity. That is we saw that the time complexity of multiplying 2 n bit numbers was bounded by the time complexity of 2 of a squaring an n bit number. So, that should be S of n, which was in turn bounded by a reciprocal, computation of the reciprocal of an n bit number, which in turn was again bounded by multiplying 2 n bit numbers, which means, if I have a good algorithm for anyone of these operations. I have a good algorithm for each one of those and observe that division is essentially, computing the reciprocal or may I put just put R there reciprocal and followed by a multiplication. So, that also has the same complexity.

Now, we would like to prove the same claim for the polynomials or 1 variable. So, that is the ring R x well it could be any field, really as long we assume that the all basic field operation state are constant time or order one time. So, let us first of all observe that, there is very close relationship between the integer operations and the polynomial operations.

(Refer Slide Time: 02:25)

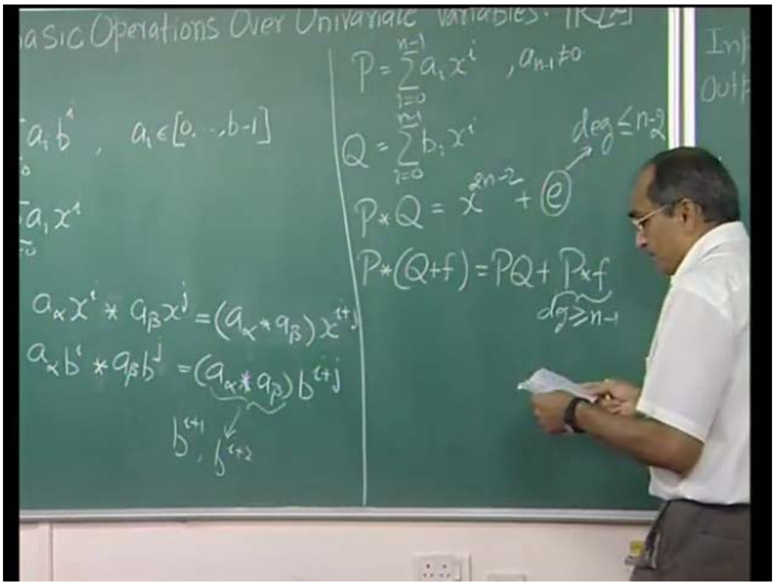

Basic Operations Over Univariate Variables. $\mathbb{R}[x]$
$\sum_{i=0} a_i b^i$, $a_i \in [0, \ldots, b-1]$
$\sum_{i=0} a_i x^i$
$a_\alpha x^i * a_\beta x^j = (a_\alpha * a_\beta) x^{i+j}$
$a_\alpha b^i * a_\beta b^j = (a_\alpha * a_\beta) b^{i+j}$
b^{i+1}, b^{i+2}

Let us take a look at the way, we represent integers. So, when a integer looks like a i b power i 0, onwards where d is a basis, we use to represent that integer a hand of course, each of these a i’s is in the range 0 to b minus 1. In case of a polynomials of one variable, we a write a i x power i 0 onwards. So, they do look very similar, but actually dealing with polynomials is easier for example, suppose we take 2 terms a 1 or I would probably say a alpha x i plus a beta x i, if you add these 2 terms in case of a polynomials all, we have to do is. On the other hand, if you have term in the expansion of an integer, you have a alpha b power i plus a beta b power i then this is a alpha plus a beta b power i.

But this need not be a valid term, the reason is that this may be outside the range namely 0 through b minus 1. So, this could actually create terms of higher order. So, it might go into terms corresponding to i plus 1, b i plus 1, b i plus 2 and so on; but does not happen here. So, similarly if you have a multiplication operation suppose, you are multiplying these 2 well. So, all we have is let us just take more general situation say and b x power a beta x power j, than the right hand side is a alpha times a beta x to the power i plus j. Once again, we have a similar situation; this is being multiplied sorry, to a beta b j.

So, this becomes a alpha times a beta into b power i plus j, once again the problem is that this number could exceed the range or 0 through b minus 1 and again it could actually, go and affect the higher terms. So, the moral of the story is that dealing with polynomials is easier and that is the reason, that similarity will tell us that, we can essentially use the same kind of algorithms, but they this simpler in case of polynomials. Now, we will again follow the similar steps, we will try to show that the complexity of computing the reciprocal of a polynomial is same as multiplication of 2 polynomials well, let us first of all decide what do we mean by reciprocal of a polynomial. So, we want another polynomial.

(Refer Slide Time: 06:53)

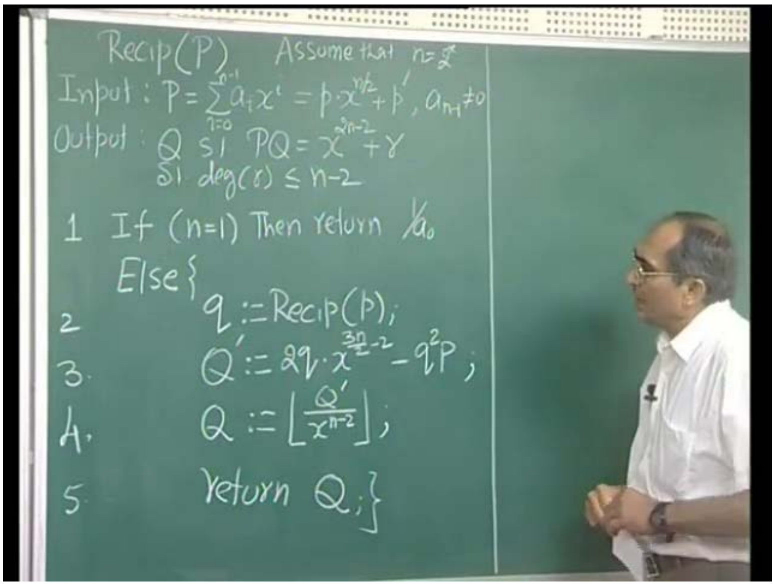

asic Operations Over Univariate variables: $\mathbb{K}[x]$
$a_i b^i$, $a_i \in [0, \ldots, b-1]$
$a_i x^i$
$a_\alpha x^i * a_\beta x^j = (a_\alpha * a_\beta) x^{i+j}$
$a_\alpha b^i * a_\beta b^j = (a_\alpha * a_\beta) b^{i+j}$
b^{i+1}, b^{i+2}
$P = \sum_{i=0}^{n-1} a_i x^i$, $a_{n-1} \neq 0$
$Q = \sum_{i=0}^{n-1} b_i x^i$
$\deg \leq n-2$
$P * Q = x^{2n-2} + e$
$P * (Q+f) = PQ + P*f$
$\deg \geq n-1$
Inp
Outp

So, let us suppose, we have a polynomial P a i x i say i from 0 2 minus 1 then and we will assume that the a n minus 1 is not 0. So, that degree is precisely n minus 1, then we would like to find another polynomial Q also of the same degree. So, we want something like this b i x power i, i going from 0 to n minus 1, such that P times Q, remember Q is suppose to be the reciprocal of P.

So, this should be effectively 1, but in this case that would be x to the power look the degrees the highest terms have power n minus 1 in the 2. So, it should be 2 n minus 2 plus some error well, let us call it error in a sense that these are something’s, we cannot get rid of what is this, well suppose, we replace Q by some other polynomial Q plus f then this will be P Q plus P times f, the degree of f can be 0 or more.

Hence the degree of this term is greater than or equal to degree is greater than equal to n minus 1, because the degree of P is n minus 1, this has to be 0 or more. So, this is the case, what it shows is that, we have access to the degrees n minus 1 or higher. So, we can actually, make sure by choosing suitable polynomial, we can get rid of all the terms up to n minus 1, but we cannot handle anything below n minus 1. So, the error can have degree less than or equal to n minus 2. So, this is the objective of computing the reciprocal of P is to compute this polynomial such that we have this equation.

(Refer Slide Time: 09:31)



```
Recip(P)      Assume that $n = 2^k$
Input : $P = \sum_{i=0}^{n-1} a_i x^i = p \cdot x^{n/2} + p'$, $a_{n-1} \neq 0$
Output : Q s.t. $PQ = x^{2n-2} + \gamma$
           s.t. $deg(\gamma) \leq n-2$
If (n=1) Then return $1/a_0$
Else {
        $q := Recip(p)$;
        $Q' := 2q \cdot x^{\frac{3n}{2}-2} - q^2 P$;
        $Q := \left\lfloor \frac{Q'}{x^{n-2}} \right\rfloor$;
        return Q; }
```

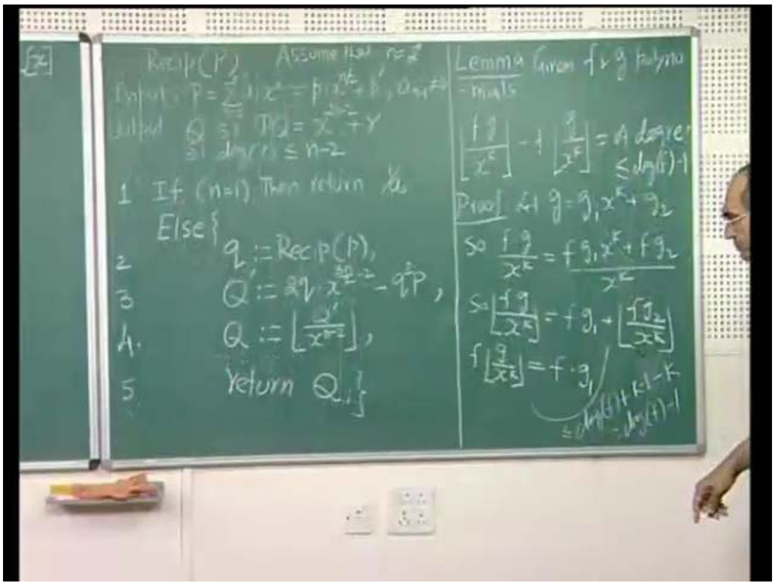
So, now we will as I said, we will adopt the polynomial the algorithm that, we had for a integers, but actually it is a simplest algorithm. The objective is given a polynomial P of degree n minus 1, we know that a n minus 1 is not 0, we split it into 2 sub polynomials and express P x P times x power n by 2, so this contains all the terms of degree n by 2 or more and this has degree less than n by 2, which is n by 2 minus 1 or less.

And the objective is of course, to compute a Q, such that P Q is x to the power 2 n minus 2 plus some remaining term, the degree less than equal to n minus 2 well in case n is 1, one more assumption, we will make without much loss, assume that n is a power of 2. In case it is not, you can always multiply by enough power of x, so that it raises it is degree to a power of 2 minus 1, because the degree is n minus 1. If n is 1, then simply written 1 over a 0 a n is 1, which means P is a 0 then Q should be 1 over a 0, so the product will be 1. Otherwise note that what, we have done here is, we extracted the upper half of the polynomial. So, this has degree n by 2 minus 1.

This we input this polynomial to the same sub routine and recursively compute, it is reciprocal Q and the next step is actually, a copy of the similar step in the integer computations. This step let me just make sure, this is clear what this says is that, if Q prime can be written as some a times x to the power n minus 2 plus b, which means all the terms of degree n minus 2 or more are put together as this by taking x to the power n minus 2 common.

And this is the remainder, which has degree n minus 3 or less then Q prime divided by x power n minus 2 floor means a, which means that, we ignore the lower terms, because it is floor in that sense, because all these b divided by this, we have degree less than 0 and here, we are getting a. So, with this interpretation of the operation, we compute Q and this is the desired polynomial, which we will show. So, now we are going to show that this indeed does the job as desired.

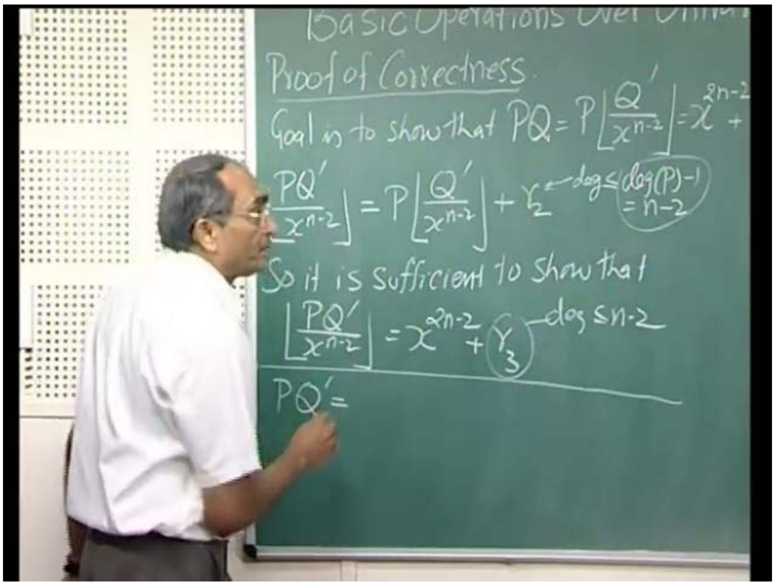
(Refer Slide Time: 13:29)


Recip(P) Assume that n=2
Input: P = Σ a_i x^i
Output Q st P·Q = x^{2n-2} + r
st deg(r) ≤ n-2
1 If (n=1) Then return 1/a_0
Else{
2 q := Recip(P),
3 Q' := 2q·x^{3n/2-2} - q^2 P,
4. Q := ⌊Q'/x^{n-2}⌋,
5 return Q.}
Lemma Given f & g polyno-mials
⌊fg/x^k⌋ - f⌊g/x^k⌋ = A degree ≤ deg(f)-1
Proof Let g = g_1 x^k + g_2
So fg/x^k = (f g_1 x^k + f g_2)/x^k
So ⌊fg/x^k⌋ = f g_1 + ⌊f g_2/x^k⌋
f⌊g/x^k⌋ = f·g_1
≤ deg(f)+k-1-k = deg(f)-1

So, to prove that, I need a small result, which says that given f and g polynomials f times g divided by x power k floor minus f times g divided by x power k is of degree less than or equal to degree of f minus 1. The difference between these 2 has degree less than that of f, to prove this let g be written as g 1 x to the power k plus g 2 all the terms of degree less than k are put here, so this has degree k minus 1 or less.

So, f times g divided by x power k is f times g 1 plus sorry, times x power k plus f times g 2 divided by x k. So, f times g by x k floor is nothing, but f g 1 plus f g 2 x k floor. On the other hand f times g over x k floor is g divided by x k floor is just g 1, because this goes away and we get f times g 1. So, the difference between these 2 is this term. And the degree of this term, the degree of this term is the degree of f plus or actually, this is less than or equal to I will put a bound degree of g 2 is k minus 1 or less. So, at most k minus 1 and then we divide by x power k, it goes away minus k. So, this is at most degree of f minus 1 as we want it. So, this is a result, we will use.

(Refer Slide Time: 16:58)



Basic Operations Over

Proof of Correctness

Goal is to show that $PQ = P\left\lfloor \frac{Q'}{x^{n-2}} \right\rfloor = x^{2n-2} +$

$\left\lfloor \frac{PQ'}{x^{n-2}} \right\rfloor = P\left\lfloor \frac{Q'}{x^{n-2}} \right\rfloor + r_2 \leftarrow \deg \leq \deg(P)-1 = n-2$

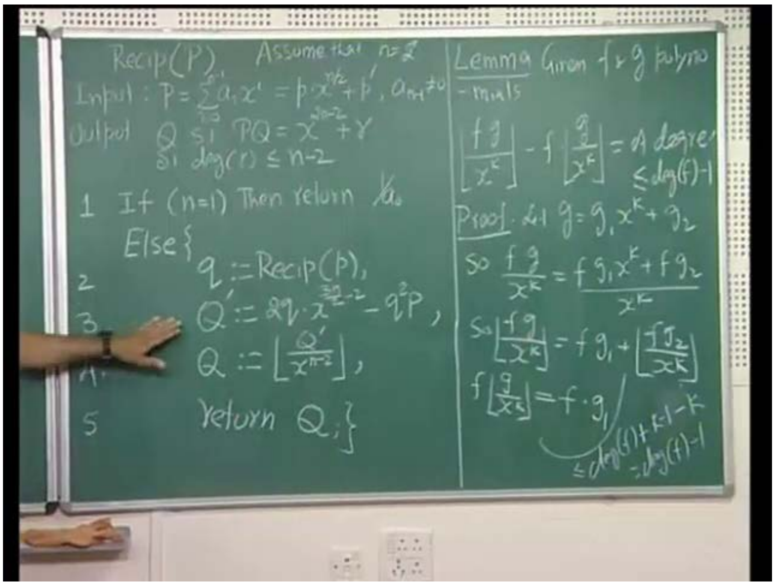
So it is sufficient to show that

$\left\lfloor \frac{PQ'}{x^{n-2}} \right\rfloor = x^{2n-2} + r_3$ — $\deg \leq n-2$

$PQ' =$

So, the proof of correctness as goes as follows, our goal is to show that, P Q and which is same as P floor Q prime by x to the power n minus 2 is equal to x to the power 2 n minus 2 plus r 1 with degree less than or equal to n minus 2. Now, let us take a look at this term, this from our lemma is equal to P Q prime our x n minus 2 plus a term r 2 of degree less than or equal to degree of P minus 1, but the degree of P is n minus 1. So, this is nothing, but n minus 2. So, what we notice that these 2 terms differ by this is correspondent to this by a term of degree n minus 2. So, it is sufficient to prove that this term. So, it is sufficient to show that, P Q prime by x to the power n minus 2 is x to the power 2 n minus 2 plus some r 3 with degree less than equal to n minus 2, because these 2 already differ by only a term of at most n minus 2. So, now, let us take this objective and we know the value of Q prime.

(Refer Slide Time: 20:10)



Recip(P) Assume that $n=2$

Input : $P=\sum_{i=0}^{n-1} a_i x^i = p\cdot x^{n/2}+p'$, $a_{n-1}\neq 0$

Output Q s.t. $PQ = x^{2n-2}+r$ s.t. $\deg(r)\leq n-2$

```
If (n=1) Then return $1/a_0$
Else{
    $q := \mathrm{Recip}(p)$,
    $Q' := 2q\cdot x^{\frac{3n}{2}-2} - q^2 P$,
    $Q := \left\lfloor \frac{Q'}{x^{n-2}} \right\rfloor$,
    return Q;}
```

Lemma Given f & g polynomials

$\left\lfloor \frac{fg}{x^k} \right\rfloor - f\left\lfloor \frac{g}{x^k} \right\rfloor$ = A degree $\leq \deg(f)-1$

Proof. Let $g = g_1 x^k + g_2$

So $\frac{fg}{x^k} = \frac{fg_1x^k + fg_2}{x^k}$

So $\left\lfloor \frac{fg}{x^k} \right\rfloor = fg_1 + \left\lfloor \frac{fg_2}{x^k} \right\rfloor$

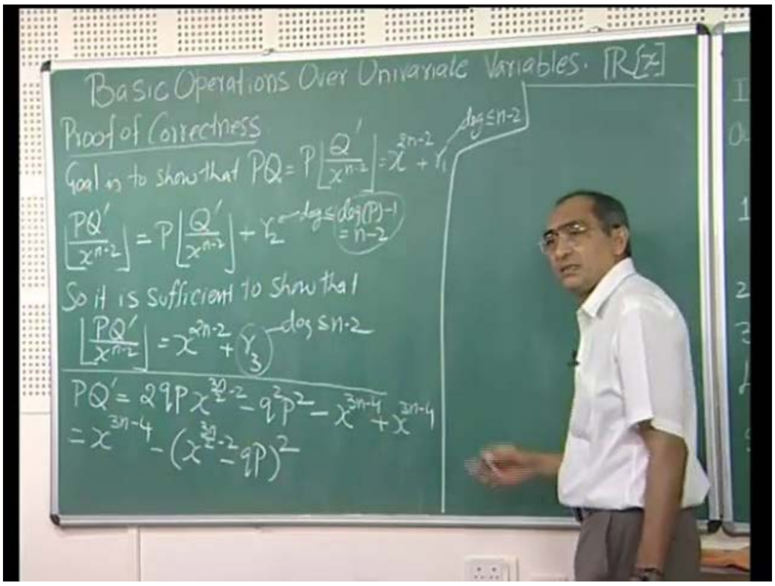
$f\left\lfloor \frac{g}{x^k} \right\rfloor = f\cdot g_1$

$\leq \deg(f)+k-1-k$

$=\deg(f)-1$

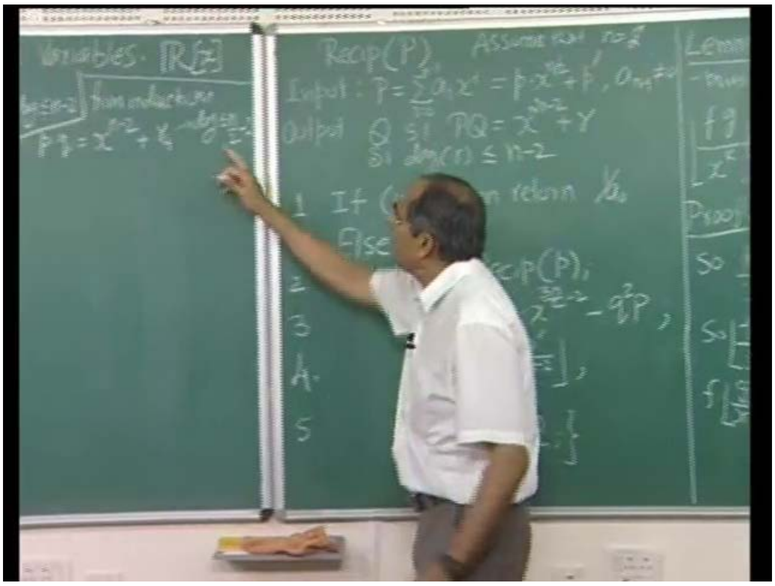
So, P times Q prime of from the value of Q prime.

(Refer Slide Time: 20:18)


Basic Operations Over Univariate Variables. $\mathbb{R}[x]$
Proof of Correctness
Goal is to show that $PQ = P\left\lfloor \frac{Q'}{x^{n-2}} \right\rfloor = x^{2n-2} + r_1$ deg ≤ n-2
$\left\lfloor \frac{PQ'}{x^{n-2}} \right\rfloor = P\left\lfloor \frac{Q'}{x^{n-2}} \right\rfloor + r_2$ deg ≤ deg(P)-1 = n-2
So it is sufficient to show that
$\left\lfloor \frac{PQ'}{x^{n-2}} \right\rfloor = x^{2n-2} + r_3$ deg ≤ n-2
$PQ' = 2qPx^{\frac{3n}{2}-2} - q^2P^2 - x^{3n-4} + x^{3n-4}$
$= x^{3n-4} - (x^{\frac{3n}{2}-2} - qP)^2$

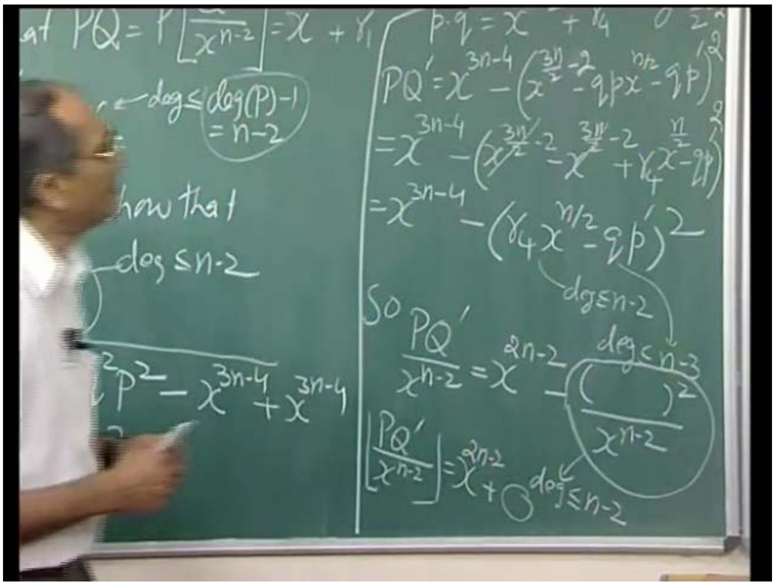
It becomes 2 q p x to the power 3 n by 2 minus 2 minus q square p square, this looks like a expression for, which we can do a whole square. So, we will add x to the power 3 n minus 4 and subtract. So, we have added and subtracted this term. So, that becomes x power 3 n minus n minus 4 minus x to the power 3 n by 2 minus 2 plus sorry, minus q p whole square. Now, recall that the small q is the reciprocal of small p and from induction hypothesis, it satisfies the condition that of reciprocal should satisfy.

(Refer Slide Time: 21:56)


Variables. $\mathbb{R}[x]$
from induction
$pq = x^{n-2} + r_4$ deg ≤ n-2
Recip(P) Assume that n = 2
Input: $P = \sum a_i x^i = p \cdot x^{n/2} + p'$, $a_{n-1} \neq 0$
Output: Q s.t. $PQ = x^{2n-2} + r$
s.t. deg(r) ≤ n-2
1 If ... return $1/a_0$
Else
2 ... Recip(P),
3 ... $x^{\frac{3n}{2}-2} - q^2P$,
4
5

So, from induction p times q is x to the power n minus 2 plus r 4 with degree less than or equal to n by 2 minus 2. This is precisely what capital P and capital Q should satisfy the only difference is now we are dealing with degree n by 2 minus 1 instead of n minus 1. So, let us use this in our expression.

(Refer Slide Time: 22:53)



So, we get P Q prime as x to the power 3 n minus 4 minus x to the power 3 n by 2 minus 2 and q p is q small p x to the power n by 2 and minus q p prime, whole square this square. So, let us plug in the value of q p from this expression, we are getting x 3 n minus 4 minus x n by 2 minus 2 minus q p is x to the power n minus 2 plus this term. So, we have n by 2.

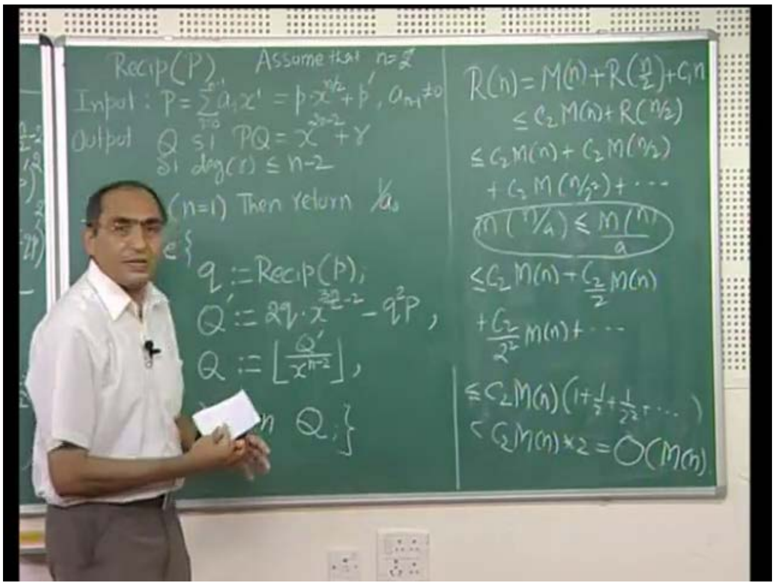
So, that makes it x to the power 3 n by 2 minus 2 plus r 4 x power n by 2 minus q p prime square, these cancel and we are left with x power 3 n minus 4 minus r 4 x to the power n by 2 minus q p prime square. Let us find out the degree of these terms, r 4 has degree n minus 2 at most and this adds up to n minus 2 at most n by 2 plus n by 2 minus 2 is n minus 2.

So, this has degree less than equal to n minus 2 q has degree n by 2 minus 1, this has the same degree as small p n by 2 minus 1, p prime has got degree n by 2 minus 2 or less. So, this has degree less than equal to n minus 3. So, overall the expression inside the parenthesis has degree n minus 2 or less or the whole thing has degree 2 n minus 2 or 4 or minus 4.

So, p q prime divided by x to the power n minus 2 is we subtract n minus 2, you are left with x to the power 2 n minus 2 plus or rather minus this whole expression square divided by x to the power n minus 2. The term here has degree at most 2 n minus 4, you are dividing by x to the power n minus 2.

So, this whole thing has degree less than or equal to n minus 2. So, what we get here is that p q prime over x to the power n minus 2 floor is indeed, x to the power 2 n minus 2 plus a term a term of degree at most n minus 2 and this is what, we wanted to establish. So, this shows the correctness of our algorithm. Now, let us take a look at the time complexity, this process involves in the worst case.

(Refer Slide Time: 28:12)



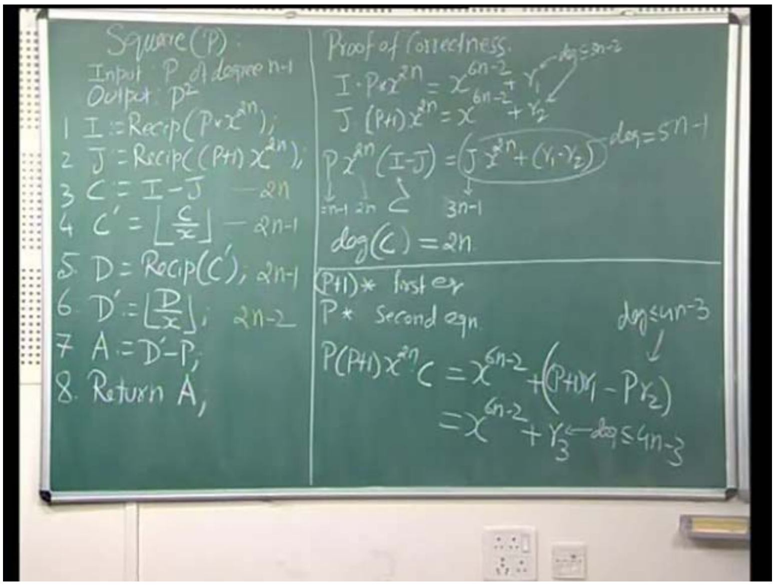
The reciprocal of a degree n minus 1 polynomial takes R n time, then this takes multiplication, this involves 1 multiplication, this is of degree n minus 1, this is of degree n by 2 minus 1 into, which is n minus 2. So, in the worst case each term has degree at most n minus 1. So, this involves 1 multiplication of 2 polynomials, each of degree n minus 1 at most this is really not complicated.

This just involves shifting of the term because this just adds that must power and this is receiving the power taking it back. And we have 1 recursive call of half size plus some linear operations, but we know that multiplication is at least linear well it is not even linear it is definitely worse than linear.

So, we can absorb this term in this and we can say this is less than equal to some C 2 m n plus R n by 2, we can absorb this here, if I expand this, I get this is less than equal to C 2 m n plus C 2 m n by 2 plus C 2 m n by 2 square and so on. Now, once again, we know that this is worse than linear. So, m of n by a is greater than equal to m of n by a. So, use this and we can show that my mistake there we wrong, that this is this is worse, because it is more than linear.

So, thing is equal to C 2 m n plus C 2 by 2 m n plus C 2 by 2 square m n and so on, hence this is this can be, if this were an infinite series, which is not this can be expressed as C 2 m n into the geometric series 1 plus 1 half 1 2 square and so on, which is less than C 2 m n times 2, which is order m n. So, what we have proved is that the reciprocal computation does not take more than order of time that a multiplication takes. So, next we are going to show that the squaring does not take more time than the reciprocal of a polynomial.

(Refer Slide Time: 32:18)



Square(P):

Input: P of degree n-1

Output: P^2

```
1 I := Recip(P * x^{2n});
2 J := Recip((P+1) x^{2n});
3 C := I - J          — 2n
4 C' = ⌊C/x⌋          — 2n-1
5. D = Recip(C');      2n-1
6. D' := ⌊D/x⌋;        2n-2
7 A := D' - P;
8. Return A;
```

Proof of Correctness.

$I \cdot P * x^{2n} = x^{6n-2} + r_1 \leftarrow \deg \leq 3n-2$

$J\,(P+1)x^{2n} = x^{6n-2} + r_2$

$P x^{2n}(I-J) = \left(J x^{2n} + (r_1 - r_2)\right) - \deg = 5n-1$

$\downarrow \; = n-1 \quad 2n \quad \sum \quad 3n-1$

$\deg(C) = 2n$

(P+1) * first eqn

P * Second eqn

$P(P+1)x^{2n}C = x^{6n-2} + \left((P+1)r_1 - P r_2\right)$ $\leftarrow \deg \leq 4n-3$

$= x^{6n-2} + r_3 \leftarrow \deg \leq 4n-3$

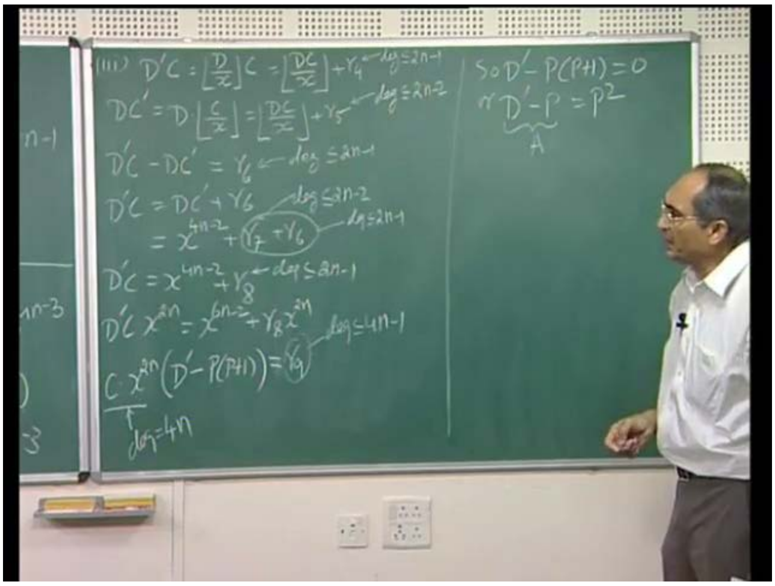
And the algorithm that, we are going to use is almost the same as the 1 that, we had used for integers, we are computing the reciprocal of p into x to the power 2 n minus 1, p has a degree n minus 1. So, this has degree 3 n minus 1, j is reciprocal of p plus 1 times x to the power 2 n minus 1 and so on. So, now, let us again show the correctness from the previous proof, we know that I times p times x to the power 2 n is x to the power 6 n minus 2 plus r 1 of degree less than equal to 3 n minus 2 j times p plus 1 x to the power 2 n is x to the power 6 n minus 2 plus r 2 also degree at most 3 n minus 2. So, we can now subtract 1 from the other and we get p times x to the power 2 n times i minus j equal to j times x to the power 2 n plus r 1 minus r 2, the degree of this is equal to n minus 2, this is 2 n, this is the reciprocal of this term.

So, it is degree is also 3 n, this is degree is 3 n minus 1. So, the right hand side has degree. So, the total term has degree equal and these have degree lower than 3 n minus 2. So, nothing can cancel any part of this. So, this has degree 5 n minus 1, these 2 together add up to 3 n minus 1. So, we know that the degree of C, this is C is precisely equal to 2 n. So, let us just note down.

The degrees of these terms, this has degree 2 n, this has to have degree 2 n minus 1 reciprocal of C prime. So, this has degree 2 n minus 1 and this has degree 2 n minus 2. So, now the next step is once again let us take these 2 equations and multiply them by p plus 1 and p respectively and subtract. So, p plus 1 times the first equation and p times the second equation well, if I multiply this by p plus 1 and I multiply this by p the left hand side and subtract then i get p times p plus 1 times x to the power 2 n times i minus j, which is C on this side, if I have a p plus 1 and p.

So, I am left with x to the power 6 n minus 2 that p plus 1. So, that 1 gives you this and plus p plus 1 times r 1 minus p times r 2. So, we have this equation the degrees of these terms, let us just put down that information the degree of this is a p as well as p plus 1 is n minus 1 and this of r 1 and r 2 is 3 n minus 2. So, this becomes 4 n or rather less than equal to 4 n minus 3, 3 n minus 2 plus n minus 1. So, now what I need is to show that. So, we can just write this down this as x to the power of 6 n minus 2 plus, we have now to use to any other r, so let us write down r 3 of degree less than equal to 4 n minus 3. Now let us take a the a third step, now let us take a look at the third step is we are trying to find out, what is D prime?

(Refer Slide Time: 38:27)


(iii) $D'C = \lfloor \frac{D}{x} \rfloor C = \lfloor \frac{DC}{x} \rfloor + r_4 \leftarrow deg \leq 2n-1$
$DC' = D \cdot \lfloor \frac{C}{x} \rfloor = \lfloor \frac{DC}{x} \rfloor + r_5 \leftarrow deg \leq 2n-2$
$D'C - DC' = r_6 \leftarrow deg \leq 2n-1$
$D'C = DC' + r_6$
$= x^{4n-2} + r_7 + r_6$
deg ≤ 2n-2
deg ≤ 2n-1
$D'C = x^{4n-2} + r_8 \leftarrow deg \leq 2n-1$
$D'C x^{2n} = x^{6n-2} + r_8 x^{2n}$
deg ≤ 4n-1
$C \cdot x^{2n} (D' - P(P+1)) = r_9$
deg = 4n
So $D' - P(P+1) = 0$
or $\underbrace{D' - P}_{A} = P^2$
n-1
n-3
3

So, let us compute D prime C, which is a D over x floor C and that is D C over x floor from our lemma, we wrote earlier plus a term r 4 of degree less than the degree of C, which is q n. So, this is less than equal to 2 n minus 1. Now, let us write down the degree of D C sorry sorry, the expression for D C prime, D C prime times C prime is C divided by x, that also can be written from our lemma as D C divided by x floor plus r 5. And the degree of this term is less than, here we had the degree of C, which is correct, now over here, we have a D outside, D is degree 2 n minus 1, so at most 2 n minus 2.

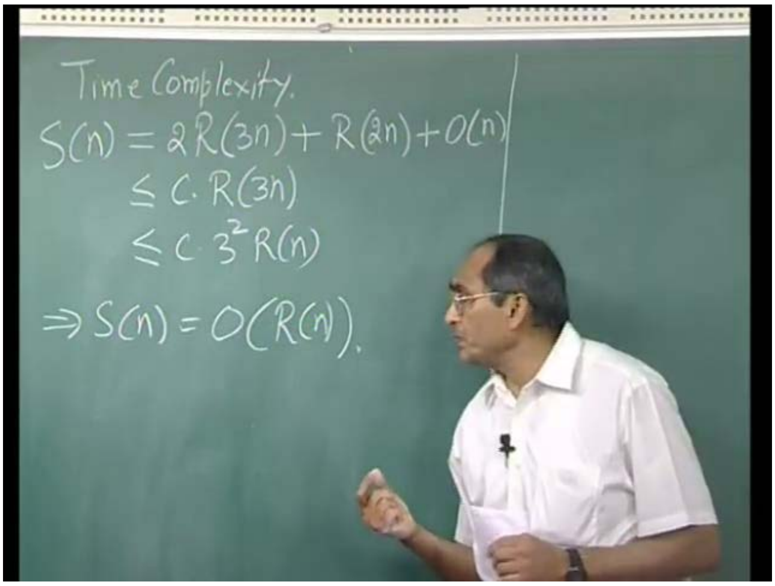
So, now, if I subtract 1 from the other, I have D prime C minus D C prime equal to r 6 this cancels out and this has degree less than equal to 2 n minus 1. So, let us compute, I will just rewrite this, let us compute what is D C prime D C prime D happens to be the reciprocal of C prime. So, from the definition of reciprocal and note that C prime had degree 2 n minus 1, D had degree 2 n minus 1.

So, this is x to the power 4 n minus 2 plus a term r 7 plus of course, r 6, this term has degree less than or equal to 2 minus 2, because each of the D prime C had degree 2 n minus 1. So, together this has degree less than equal to 2 n minus 1, because there is r 6 here. So, putting together I have expression for D prime C, which is x to the power 4 n minus 2 plus r 8 of less than equal to 2 n minus 1.

Now, I have got 2 interesting expressions p into p plus 1 and 2 x to the power 2 n C. So, compare this with this expression, I am going to multiply the both sides by x to the power 2 n. So, I have got D prime C x to the power 2 n is x power 6 n minus 2 plus r 8 x to the power 2 n, let us subtract this from this, we are going to get a C times x to the power 2 n d prime minus p times p plus 1. And this cancels out and we are left with this has degree 4 n minus 1, this has degree 4 n minus 3. So, I have some r 9 of degree less than equal to 4 n minus 1, the dominating degree is this let us take I think I made a mistake, this is equal to this is equal to.

Now, let us take a look at the left hand side a degree of C was 2 n degree of x power 2 n is 2 n. So, this thing has degree equal to 4 n and this is a polynomial cannot have a negative degree, but the right hand side has that degree 4 n minus 1. So, this can happen only, if the this term is 0. So, D prime minus p times p plus 1 is 0 or D prime minus p is equal to p square this our a, that we are returning. So, this proves the correctness of our algorithm.

(Refer Slide Time: 44:11)



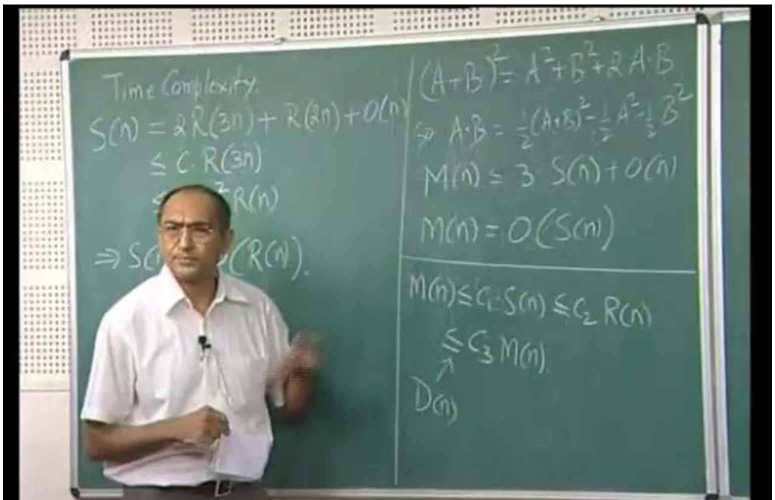
Time Complexity.

$$S(n) = 2R(3n) + R(2n) + O(n)$$
$$\leq C \cdot R(3n)$$
$$\leq C \cdot 3^2 R(n)$$
$$\Rightarrow S(n) = O(R(n)).$$

So, the time complexity of the squaring well what, we have done is, we have computed 2 reciprocals. So, S of n squaring of polynomial of degree of n minus 1, we have computed 2 reciprocals of degree 3 n each, because we multiplied p and p plus 1 both by x to the power 2 n. So, the degree was 3 n, we also computed a reciprocal of C prime at degree 2 n minus 1.

So, this is r of 2 n in addition to that, we have done is some linear operations, so this of the order n. So, we can say that this is less than equal to some constant times R of 3 n, the fact that, you can always do a long hand division, you can always do in order n square. So, we know that this is no more than C times 3 p square R of n, you can do in quadratic term. So, this is less than that. So, S of n is of the order R of n. So, further we have managed to bind R n by m n and S n by R n. Now, I am going to show that m n itself can be bounded by S n.

(Refer Slide Time: 46:09)



Time Complexity.

$S(n) = 2R(3n) + R(2n) + O(n)$

$\leq C \cdot R(3n)$

$\leq$ [illegible] $^2 R(n)$

$\Rightarrow S($[illegible]$(R(n))$.

$(A+B)^2 = A^2 + B^2 + 2A \cdot B$

$\Rightarrow A \cdot B = \frac{1}{2}(A+B)^2 - \frac{1}{2}A^2 - \frac{1}{2}B^2$

$M(n) \leq 3\ S(n) + O(n)$

$M(n) = O(S(n))$

$M(n) \leq C_1 \cdot S(n) \leq C_2\ R(n)$

$\leq C_3\ M(n)$.

$D(n)$

So, let us this is a very trivial task, I just assume the integers, let us take a look at 2 polynomials A and B and consider it square, it square is A square plus B square plus 2 A times B. So, A plus B is indeed 1 half A plus B square minus 1 half, A square minus 1 half B square. So, you can my mistake A times B. So, you can compute the product of 2 polynomials say both of degree n minus 1 by squaring these 3 polynomials, each is of degree n minus 1, because when you add the degree does not change. So, you have done 3 squaring, so this simply shows that M of n is less than equal to some 3 times S n plus some linear operations adding n, so on and so forth. But, again you know this is at least linear. So, I can absorb this inside this and I have m of n as bounded by S n.

So, now putting everything together, what we have found is that M n is less than equal to some constant times S n S n itself is bounded by reciprocation. So, C 2 times R n and R n is bounded by M n, hence all these 3 operations take the, you know it is same M n. So, they have the same time complexity and again the division is nothing, but 1 reciprocal and 1 multiplication. So, this also has the same time complexity is all of these.

So, today what we have established is that again, whatever happens in case of integers, the same happens in case of polynomials. Assuming of course, that all the field operations that is the operations on the coefficient are assumed to be order one. Later on we will show that, we will give one efficient algorithm for multiplication and that will imply that all these operations are also equally efficient, without trying to prove anything more, we will get that, that is all.