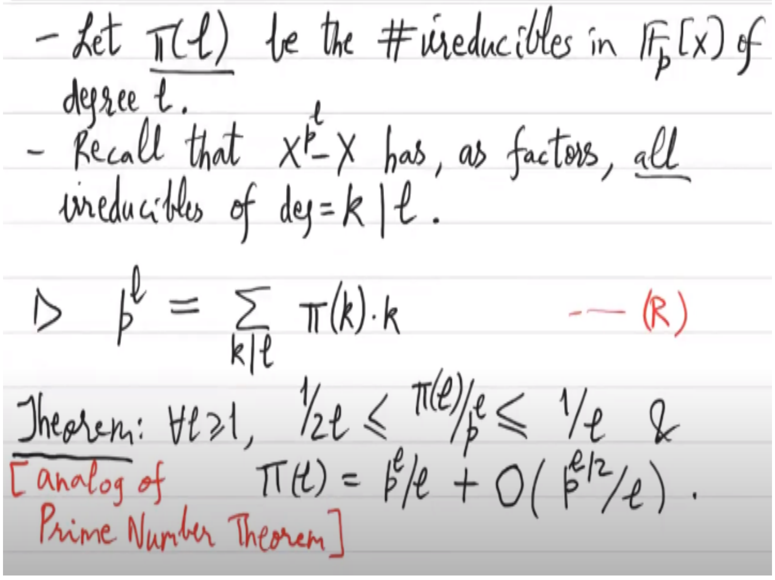
Computational Number Theory and Algebra
Prof. Nitin Saxena
Department of Computer Science and Engineering
Indian Institute of Technology-Kanpur

Lecture – 15

(Refer Slide Time: 00:16)



- Let $\pi(\ell)$ be the #irreducibles in $\mathbb{F}_p[x]$ of degree ℓ.
- Recall that $x^{p^\ell}-x$ has, as factors, all irreducibles of $\deg = k \mid \ell$.

$$\triangleright \quad p^\ell = \sum_{k\mid\ell} \pi(k)\cdot k \qquad \text{--- (R)}$$

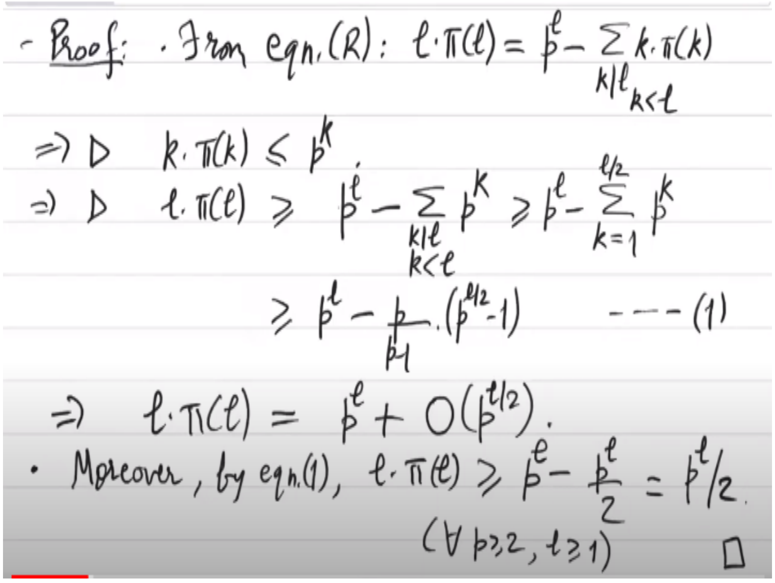
Theorem: $\forall \ell \geq 1$, $\frac{1}{2\ell} \leq \pi(\ell)/p^\ell \leq 1/\ell$ &

[analog of Prime Number Theorem] $\pi(\ell) = p^\ell/\ell + O(p^{\ell/2}/\ell)$.

So last time we were, so you wanted to estimate the number of irreducible polynomials over F p of degree l. And this estimate is like a prime number theorem. So it says that the number of l degree irreducibles in the space of p raised to l polynomials, that much degree is roughly 1 over l in density. Okay, and the error term is also very precise, it is square root of that, roughly.

So we will show this by invoking this identity. Let us call this, this is the recurrence, let us call it R. So we will use the recurrence R to prove this. So proof in few lines.

(Refer Slide Time: 01:28)



- Proof: · From eqn. (R): $\ell\cdot\pi(\ell) = p^{\ell} - \sum_{\substack{k|\ell \\ k<\ell}} k\cdot\pi(k)$

$\Rightarrow$ ▷ $k\cdot\pi(k) \leqslant p^{k}$.

$\Rightarrow$ ▷ $\ell\cdot\pi(\ell) \geqslant p^{\ell} - \sum_{\substack{k|\ell \\ k<\ell}} p^{k} \geqslant p^{\ell} - \sum_{k=1}^{\ell/2} p^{k}$

$$\geqslant p^{\ell} - \frac{p}{p-1}\cdot(p^{\ell/2}-1) \qquad \text{---} (1)$$

$\Rightarrow$ $\ell\cdot\pi(\ell) = p^{\ell} + O(p^{\ell/2})$.

· Moreover, by eqn.(1), $\ell\cdot\pi(\ell) \geqslant p^{\ell} - \frac{p^{\ell}}{2} = p^{\ell}/2$.

$(\forall p\geqslant 2, \ell\geqslant 1)$ □

So from R what you get is l times pi l is k divides l and k less than l. So k less than l in this case will mean, can k be l – 1? It has to divide l, right. So it is l by 2 or less. So it only goes up to l by 2. That is the reason actually why you will get p raised to l by two. So this is the error term and this is significantly smaller than p raised to l. That is what you will see.

So this is in particular implying that, so first thing you observe is that k pi k is less than p raised to k. Just from the above expression, because l pi l is smaller than p raised to l and this is true for all l. So we can observe that k times pi k is always smaller than p raised to k. And then you use this inequality in the sum, for the sum, upper bound the sum, right?

So you will get that l pi l is then greater than equal to p raised to l minus p raise to k, which is greater than equal to p raised to l minus. So we can overestimate the sum for all k from 1, 2l by 2 and that will give you the result. So this you can now simply estimate by geometric sum, geometric series. So p raised to l, right? Is at least this. So that is roughly p raised to l by 2, slightly more than that. So that is the error term.

So this means that l pi l is equal to p raised to l plus big O of p raised to l by 2, right. So main term is p raised to l and the error term is square root of that. So that is the second statement in the theorem. From this you can now deduce inequalities as well. So you can observe at the inequality level here that l pi l is at least p raised to l minus p raised to l by 2.

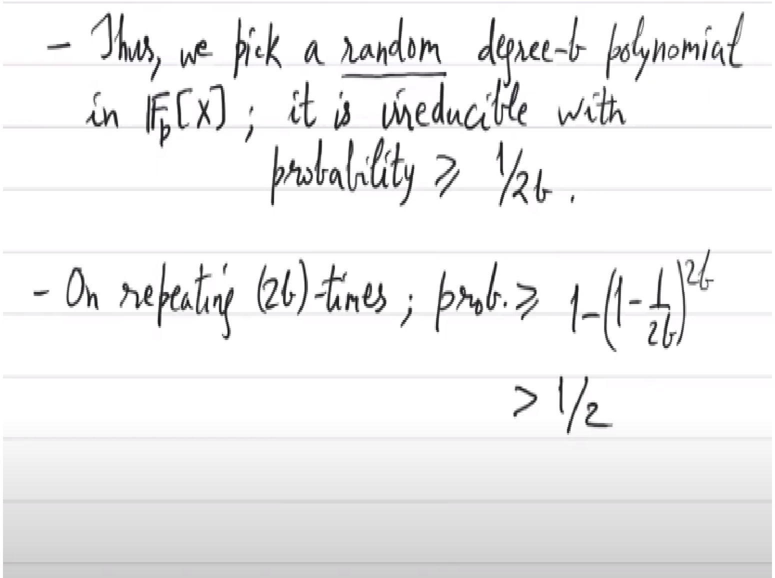
Basically in equation 1 this expression p raised to l by 2 times p over p – 1. That you can see is at least is at most, it is at most p raised to l by 2 for every l, right. So that minus thing is then greater than equal to minus of p raised to l by 2. So that gives you p raised to l by 2 as the lower bound, okay. So l pi l is at most p raised to l and it is at least half of that. Any questions? Fine. So this is true for all p at least 2 and l at least 1.

That you can check. It is always true. So what this tells you is we wanted to construct finite fields, finite field of size p raised to l, now you will construct it by just picking a random l degree polynomial. And you will check irreducibility very efficiently. So if it is irreducible then you have the finite field construction and the probability that it is when you randomly pick up a polynomial it is irreducible or it is irreducible the probability is at least 1 over l, right.

So is that a good probability? Or 1 over 2l. So is that a good probability? Why? Yeah, so if l was say 1000, you wanted 1000 degree polynomial. So this probability seems to be 1 over 2000 which is quite small probability, but you can amplify it by repeating. So you can for example, pick 4000 random polynomials and calculate the probability that at least one of those is irreducible.

So in other words, the probability that all of them are reducible becomes very small, okay. So you can actually make it arbitrarily close to 1 getting an irreducible polynomial at the cost of more experiments. But that is fine. So this is a fast algorithm. So in practice this is what is used.

(Refer Slide Time: 08:39)



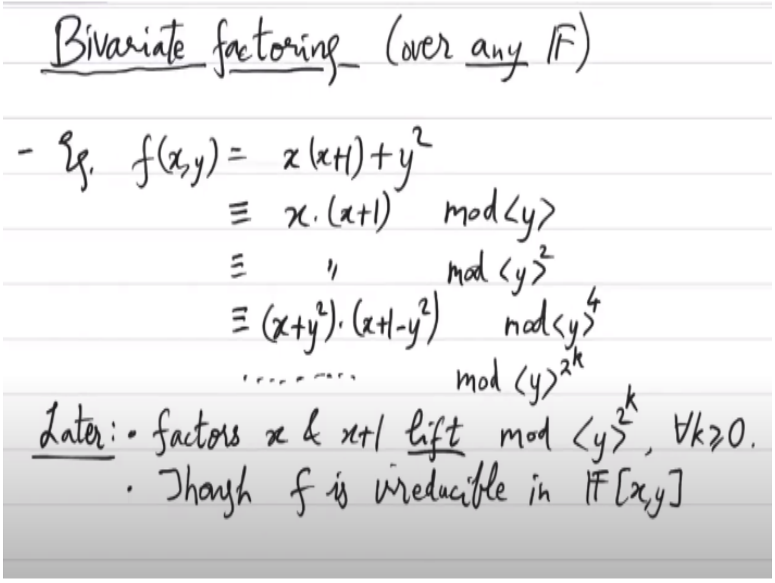
- Thus, we pick a <u>random</u> degree-b polynomial in $\mathbb{F}_p[x]$; it is irreducible with probability $\geqslant 1/2b$.
- On repeating $(2b)$-times ; prob. $\geqslant 1-\left(1-\frac{1}{2b}\right)^{2b}$ $> 1/2$

Thus, we pick a random degree b polynomial and it is irreducible with probability at least 1 over 2b and if you repeat it 2b times say just 2b times then this probability is at least, so the chance that each of the 2b choices are bad that is 1 minus 1 over 2b raised to 2b and then complement of that. And that you can check is more than half, okay. So here is an algorithm that will that is polynomial time and it will give you an irreducible with probability at least 50%.

You can also increase it by just taking instead of 2b times you can take it 10b times. Just simply a constant multiple will give you very large success probability. So any questions? This solves the first problem of finite field construction for codes. So you can now construct finite fields on demand. Second problem was the question of factoring bivariate polynomials, right. So for that we have currently no algorithm.

I mean, we have not seen any algorithm in this class. Only when we saw was for univariate. So now we will reduce bivariate to univariate factorization.

(Refer Slide Time: 11:17)



Bivariate factoring (over any $\mathbb{F}$)

- Eg. $f(x,y) = x(x+1)+y^2$
  $\equiv x\cdot(x+1) \mod \langle y\rangle$
  $\equiv$ " $\mod \langle y\rangle^2$
  $\equiv (x+y^2)\cdot(x+1-y^2) \mod \langle y\rangle^4$
  ...... $\mod \langle y\rangle^{2^k}$

Later: • factors x & $x+1$ lift $\mod \langle y\rangle^{2^k}$, $\forall k\geq 0$.
• Though f is irreducible in $\mathbb{F}[x,y]$

We will actually give a general reduction. So this will be over any field. So over any field F we will reduce bivariate factoring to univariate factoring. And then if you have a univariate factoring algorithm, you can just plug and play, right? So over finite fields you have 1. Over other fields for example, over integers or rationals we still have to find some algorithm. So that will be our long term goal in the course.

This will also raise the question what about trivariate polynomials and n-variate polynomials. So this reduction will actually generalize to some extent. But to really go to n-variate, we have to use a different method. Okay, that will be another topic to study in this course. So a lot of time will be invested actually now spent in these problems in the course. Half of the remaining time will be spent on these questions.

Each of these questions have widespread applications in different areas of computer science. The result, let us look at an example first. So suppose you are given a polynomial bivariate x (x + 1) + y square. Well, this happens to be irreducible, but how do you know, right? How do you show that this is irreducible? So because for bivariates, you do not even know how to test irreducibility, right.

So this polynomial, intuitively you can see, you can immediately see that this is irreducible, but what if it is not? So you want to factorize this, right. So what is the method that you can try. So in particular, to reduce this to univariate factoring. Basically, you want to eliminate one variable, so what you can do is you can fix that variable, right. So in this case, you can fix y to be 0.

And then you see factorization, x times x + 1. But that is really no good because that does not really tell you for sure whether F is the factors x and x + 1 of F mod y. Do they really correspond to factors of F without any mod, right, absolute factors. But anyways, what we can do is we can look at it mod y, then we can look at it mod y square, which is actually the same again, x, x + 1.

But then you can go to mod y to the 4, right and then it becomes slightly different because x is not a factor anymore, mod y to the 4 and you go to mod y to the 8 and so on. So how does it work? So first you get x times x + 1 mod y ideal. Then the same thing mod y square and mod y 4. What do you get?

So dutifully the x mod y square should lift mod y to the 4, right which means that you have to perturb x by some multiple of y square and similarly x + 1 you have to perturb by a multiple of y square. So what are these perturbations? So this will work. So if you look at this then in the y square coefficient you are getting x + 1 – x. So that is 1. And y to the 4, next is y to the 4, which is 0 mod y to the 4, right.

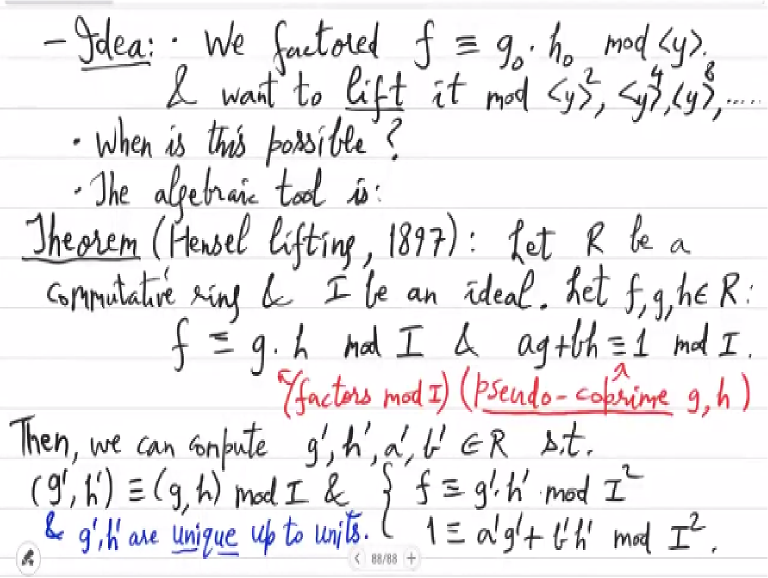
So this is actually equal to F. These are the factors. And believe it or not this will actually go on ad infinitum. So for any y to the k you will get a factorization, okay. **"Professor - student conversation starts"** Sir, can you explain this step once again? **"Professor - student conversation ends".** There is nothing to explain. You can just multiply and see that it is F. Oh well you go to the next 2 power.

If it is true for next 2 power everything below is covered subsumed. So but yeah, so this dotted thing will be a theorem that we will do next, but what I have written that you can just check by calculation. So and this will actually go on that will be subject of a theorem which is coming next. Yeah, so this factorization will continue like this. But as you can easily believe that this f is actually irreducible, okay.

So it is an irreducible polynomial, but when you do this fixing thing, or going modulo an ideal it happens to be reducible, right? So this connection from bivariate to univariate is not so easy. So we will actually do it in steps. So we will prove some of these things. And later, we will see how from this information by doing some more algebraic operations, some more algorithmic steps, how can you deduce what f really is?

Is F absolutely reducible or is F absolutely irreducible? Okay, so we will do it in steps. We will add the algorithmic parts in steps. So first step will be to just understand this. How is this factorization lifting, okay. This we call lift. So factors x and x + 1 lift mod y raised to 2 raised to k for all k. That we will see next. Although f is irreducible in any field, right. You do not expect f to factor over any field actually finite field or q. Okay fine. Let us understand this step.

(Refer Slide Time: 19:24)



- Idea: • We factored $f \equiv g_0 \cdot h_0 \mod \langle y \rangle$.
& want to lift it mod $\langle y \rangle^2, \langle y \rangle^4, \langle y \rangle^8, \ldots$

• When is this possible?

• The algebraic tool is:

Theorem (Hensel lifting, 1897): Let R be a commutative ring & I be an ideal. Let $f, g, h \in R$:

$$f \equiv g \cdot h \mod I \ \& \ ag + bh \equiv 1 \mod I.$$

(factors mod I) (pseudo-coprime g, h)

Then, we can compute $g', h', a', b' \in R$ s.t.

$(g', h') \equiv (g, h) \mod I$ & $\begin{cases} f \equiv g' \cdot h' \mod I^2 \\ 1 \equiv a'g' + b'h' \mod I^2. \end{cases}$

& g', h' are unique up to units.

So what we are doing here is we factored f general f as g 0 times h 0 mod y. So which is in other words you factored f x, 0. That is a univariate so you factored that by some means. And then you want to lift this factorization mod y square, y 4, y 8 and so on. So under what conditions is this possible? So this is a lower order problem. Instead of looking at f absolutely, we only want its factors mod y to the 2 raised to k, right.

We just want to check whether it is factorizing for all of these. This is a lower order problem. So firstly we will solve this. We will give a formula. Some of you actually already know this trick, because you used it in the mid sem, I saw. Okay, this is called Hensel lifting. So that is the algebraic tool here. So this is what in this course we will call it Hensel lifting.

It is a very old technique, which was designed to start a new sub area in algebra called p-adic analysis. But it is also important in the case of polynomials, which is what we used in the mid sem, basically for division of polynomials. So this technique is used both in numbers and in the polynomial ring. So we will do it in the polynomial ring. So let R be a in fact, for now it is a general ring. Let R be a commutative ring.

And I be an ideal. So let f, g, h be in the ring. So if you do not want it to abstract you can think of R as the polynomial ring okay, just like we had before in this example. R is the bivariate polynomial ring and there are three polynomials f g, h, and g, h are the factors so such that f is congruent to g times h, modulo this ideal. Again this ideal you can think of as the ideal y or its square or its square and so on.

So when you are at a at an intermediate step f, g f equal to g, h mod I, lifting means that you want to lift g to mod I square, the factorization mod I square, right. So when is that possible? It is not always possible, we will see an example later. So we need more conditions here. One condition is that g and h should be somehow coprime, which will be, which will not make sense for every ring.

But what will make sense is Bezout identity. So we will actually assume Bezout identity. So we will assume that ag + bh b H is 1 mod I. So this is what is called pseudo-coprimality. So you want g, h to be somehow coprime and this these are the factors mod I. So these are pseudo-co prime factors mod I. Okay, this is what you start with. And then you want to go to the next step.

You want to lift this picture mod I square, which means you want g prime h prime, a prime, b prime. You want four things to be lifted. So yeah, so formally there is a lot of equations. So let us write that. So it says that we can compute which is very efficiently, can efficiently compute g prime, h prime, a prime, b prime in R such that. So g prime should be in fact let us use Tuple notation.

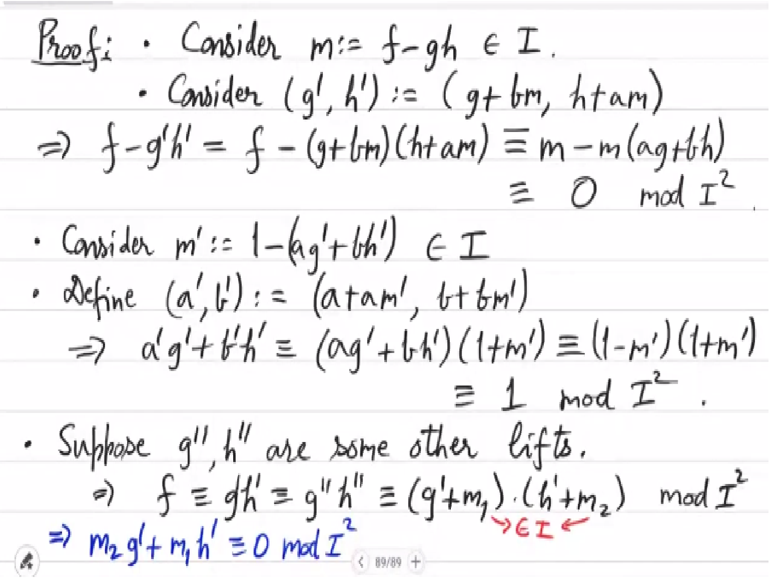
So g prime, h prime would be the same as respectively g and h mod I. Okay, this is a condition which is important for lifting that. g and g prime should look the same mod I. But different mod I square possibly. And f is g prime, h prime mod I square. What is I square? I thing we defined it in the first class. This is just, yeah pick any two elements in I and multiply them.

So you have these products and then you generate the ideal by them. That is called I square. It is simplest to understand in the case of principal ideal like when you had y, ideal y then squaring is just squaring the single generator. But this theorem or Hensel lifting is very general. So it will work for any ideal, okay. Principal ideal will have no utility here. And second is that they are pseudo-coprime.

And as if this was not enough, the last property is that g prime, h prime are unique up to unit multiplication, right. So factorization, even the polynomial ring it is unique, unique only up to unit multiplication. You can always multiply by 2 and divide by 2 in the factors, right. So those things you can do here also. But up to those unit multiplication g prime, h prime are unique.

So g prime in particular is unique. That is the last and g prime, h prime are unique up to units. So this is a big statement. Any questions about the statement? Proof will be equally long. Sorry? Yeah. So you are jumping ahead. What is the meaning of degree in a ring R? It has no meaning. We are first proving a general statement. Hensel lifting in the most general form is this. Yeah, so if the statement is clear, then let us move to the proof of this.

(Refer Slide Time: 29:12)



Proof: • Consider $m := f - gh \in I$.

• Consider $(g', h') := (g + bm, h + am)$

$\Rightarrow f - g'h' = f - (g+bm)(h+am) \equiv m - m(ag+bh)$

$\equiv 0 \mod I^2$.

• Consider $m' := 1 - (ag' + bh') \in I$

• Define $(a', b') := (a + am', b + bm')$

$\Rightarrow a'g' + b'h' \equiv (ag' + bh')(1+m') \equiv (1-m')(1+m')$

$\equiv 1 \mod I^2$.

• Suppose g'', h'' are some other lifts.

$\Rightarrow f \equiv g'h' \equiv g''h'' \equiv (g'+m_1) \cdot (h'+m_2) \mod I^2$

$\to \in I \leftarrow$

$\Rightarrow m_2 g' + m_1 h' \equiv 0 \mod I^2$

Yeah any ideas? How will you how will you get g prime? You have g, h, a, b. From these four things you want to get g prime. What is the formula? Yes, so g prime has to be g mod I. So which means that you want to perturb g by an element in I, right. So that element you want to find. But obviously it has to be a very special element.

At this point, it is not even clear why that will exist, because it has to satisfy all these conditions congruences mod I square which is the next precision. So in terms of precision actually we are increasing the precision, right. Because I square is a smaller ideal. So when you go modulo a smaller ideal, you have to do more, I mean here you will get a more precise answer.

So most precise answer you will get mod 0, right. That is your limiting case. So you have to increase precision, that is the, that is a non-trivial thing. So what actually we will use is what is already given, which is f - gh; f - gh is an element in the ideal. We will try to use that in the perturbation. So consider m to be f - gh, which is an element in the ideal. And for that you define g prime, h prime as follows.

g + bm and h + am. Okay a and b were given to you; m is also kind of given to you because gh were given. So if you look at this, this actually works. So obviously, you will find this in a by doing some calculations which I am skipping. I am just directly giving you the answer. Okay, but it is but they are these are easy to find. So once you have this you can just check that f – g prime h prime is which is so f - gh is m.

And then you have in the product you are getting coefficient of m bh + ag. Then you are getting m square. But m square we will actually call it zero by going mod I square, right. And what is 1 – ag – bh? That is again an element in I. N is also in I. So this is actually 0 in I, I square. So that is it, that is the check, right. So the algorithm is then very simple. Given ab, f, gh you have designed g prime h prime.

It is a completely closed form expression. Next thing to show is why are these g prime h prime pseudo-coprime. So we have to give a prime, b prime. Yeah, so that again you can reverse engineer. I will just give you the expression. So that will be, now you consider m prime to be 1 – ag prime + bh prime. So this m prime is also in I. Do you see this? This is 0 mod I. Why is that? Yes, because g prime and h prime are g, h.

And then 1, then ag + bh is 1 mod I. So this actually remains in I. We will use this to perturb a and b. So define a prime, b prime as follows. And then just check what you are getting when you calculate a prime g prime, b prime h prime. So this is ag prime + bh prime times 1 + m prime. So we are doing this now mod I square, right. That is the modulus. What is ag prime plus bh prime?

That is 1 + m prime by definition, 1 - m prime which is 1 mod I square. Is it clear? This product is 1 - m prime square; m prime square is in I square. So this is 1. So which shows that g prime h prime that we have constructed they are also pseudo-coprime and you get the Bezout identity explicitly, okay. Any questions? Why are these why is this construction unique?

So I just gave you one construction right? Why is there no other construction possible of g prime? So that you have to separately prove. So suppose it is possible. Suppose there are some other lifts of g and h respectively. Then what do you have, f is gh and also g prime prime h prime prime mod I square sorry I. This is prime.

So mod I square you have two factorizations g prime h prime as before as defined or constructed and g prime prime h prime prime which somebody else gives you. So let us look at the difference of g prime and g prime prime. Okay, let us look at that. So let me just put it here directly. So this is g prime + m 1 and this is h prime + m 2; m 1 is g prime prime minus g prime and so is m 2 analogous to h prime prime minus h prime.

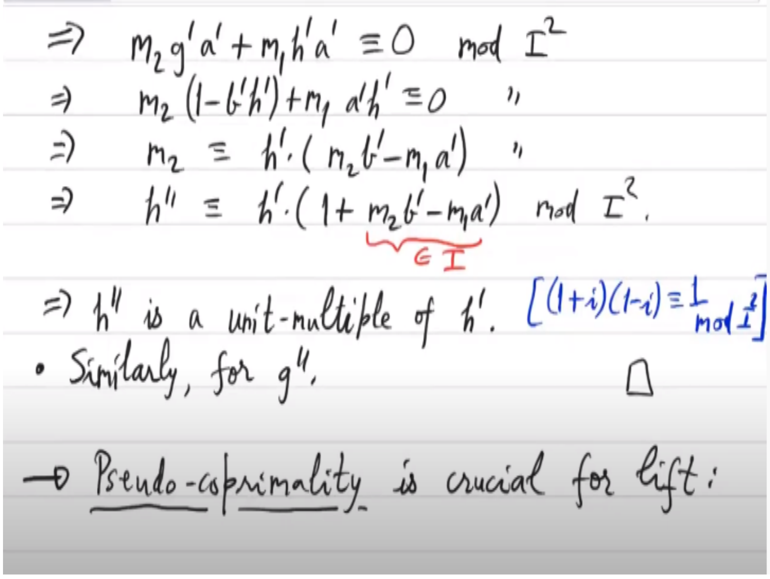
So where does that put m 1 in? Yeah, you cannot see I square, you can only say I. So you know that both g prime prime and g prime they are same mod I. So the difference is actually zero mod I, right. So m 1 and m 2 are in I, okay. So what do we do next? Yeah, I think we just multiply and take the difference just, so basically g prime h prime is equal to this product. So you minus g prime h prime from this side and that result is zero.

Let us write down that congruence. So that congruence is m 2 g prime plus m 1 h prime is 0 mod I square. Because m 1, m 2 is 0 mod I square and g prime h prime has been cancelled. So you actually get a relationship between m 1, m 2 right? These, m

1, m 2 given to you by somebody else are actually related this way. What do you do next? Yeah, use the Bezout identity for g prime h prime.

Yeah, you might want to cancel these things out. But that is actually not legal, may not be legal in this arithmetic. So the correct the only thing you can do is multiply or add. It is a ring right? So let us just multiply g prime by a prime and then kind of cancellation effect will happen.

(Refer Slide Time: 40:16)



$\Rightarrow \quad m_2 g'a' + m_1 h'a' \equiv 0 \mod I^2$

$\Rightarrow \quad m_2 (1 - b'h') + m_1 a'h' \equiv 0 \quad "$

$\Rightarrow \quad m_2 \equiv h' \cdot (m_2 b' - m_1 a') \quad "$

$\Rightarrow \quad h'' \equiv h' \cdot (1 + \underbrace{m_2 b' - m_1 a'}_{\in I}) \mod I^2 .$

$\Rightarrow$ h'' is a unit-multiple of h'. $[(1+i)(1-i) \equiv 1 \bmod I^2]$

- Similarly, for g''. □

→ Pseudo-coprimality is crucial for lift:

So what you will get is, so we had m 2 g prime a prime plus m 1 h prime a prime is 0 mod I square. And what is a prime g prime? So okay where does that take us? So we are getting m 2, h prime we will take out; m 2 b prime minus m 1 a prime mod I square, okay. Remember m 2 was, how did we define? Right. So this means that h prime prime is now h prime 1 plus this thing. So that is it.

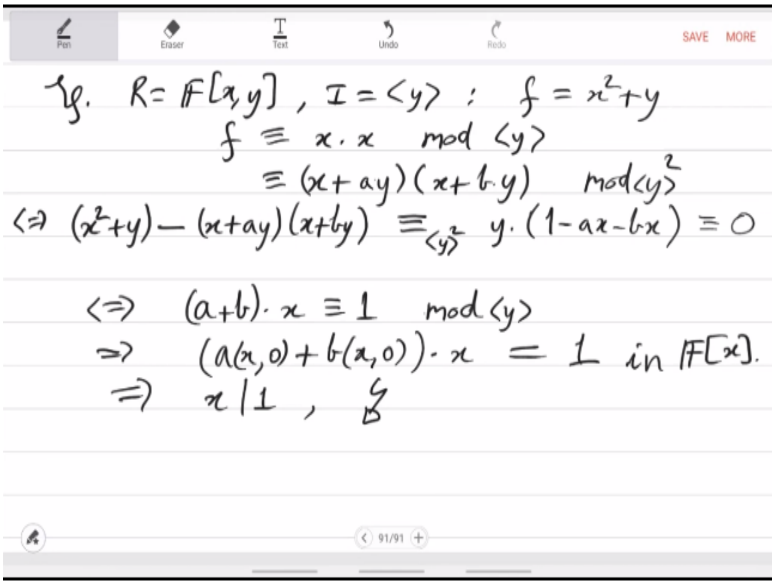
We have now actually a relationship between h prime prime and h prime, right; h prime is what we had what our algorithm had constructed; h prime prime is something totally arbitrary given to us, arbitrary solution given to us. It is actually just a multiple of h prime. What can you say about this multiplying factor 1 + m 2 b prime – m 1 a prime? What did you say about m 2 m 1? They were in I, right?

So this difference is also in I because I is an ideal. So what can you say about 1 + I? This is actually a unit. What is the inverse of this? Yeah. So mod I square it is a unit because if it was 1 + i then you multiply it by 1 – i and that gives you 1. So this is actually an invertible element. So that is it. So this is this whole thing is a unit. So the reason is just that (1 + i) (1 – i) is 0 mod I square, sorry 1.

Because I square is zero mod big I square okay. So as promised h prime prime and then analogously g prime prime they are actually just unit, multiplication by a unit of what we had constructed. Right, so we have proved everything that was claimed; g prime h prime have a very simple form. They are coprime and there is no other solution. So that completely solves this problem of lifting.

Well okay, there was one thing that, is this assumption needed, the assumption of coprimality? This extra condition that we needed, ag + bh = 1 mod I. What if gh is a non coprime factorization? Will it lift mod I square? That is the only issue left. So actually that condition is required. Otherwise, lift may not exist. Let us see that. Is crucial for lift. So let us see an example for that.

(Refer Slide Time: 45:12)



Eg. $R = \mathbb{F}[x,y]$, $I = \langle y \rangle$: $f = x^2 + y$

$$f \equiv x \cdot x \quad \text{mod } \langle y \rangle$$

$$\equiv (x + ay)(x + b \cdot y) \quad \text{mod} \langle y \rangle^2$$

$$\Leftrightarrow (x^2 + y) - (x + ay)(x + by) \equiv_{\langle y \rangle^2} y \cdot (1 - ax - bx) \equiv 0$$

$$\Leftrightarrow \quad (a + b) \cdot x \equiv 1 \quad \text{mod} \langle y \rangle$$

$$\Rightarrow \quad (a(x,0) + b(x,0)) \cdot x = 1 \text{ in } \mathbb{F}[x].$$

$$\Rightarrow \quad x \mid 1 \text{ , } ↯$$

So the bivariate example with ideal y. So let us take f to be x square plus y. So mod y the factorization of this is x times x which is non-coprime. Will that lift? So suppose it lifts, right. What do you get? Say it lifts like this x plus multiple of y. So some a perturbation and here is some other perturbation mod y square. So which will mean what? So you take the difference of these two sorry not these two.

You take the difference of actual f. So x square plus y minus this mod y square is what? So x square will cancel and this y square will also disappear. So what will you get is, what you get is 1 from here and ax + bx right is 0. So y square divides this meaning that y has to divide this other factor, right. You deduce this. This is if and only if. This is also if and only if. And so can this happen?

Can there be bivariate polynomials a and b such that this thing happens. So what is this thing? So this is a at x, 0. And this is b at x, 0 times x should be equal to 1, right. This is a equality in the univariate polynomial, which cannot happen, right. Because this in particular means either x divides 1 or left hand side is 0. Actually either way x has to divide 1, which is a contradiction, right.

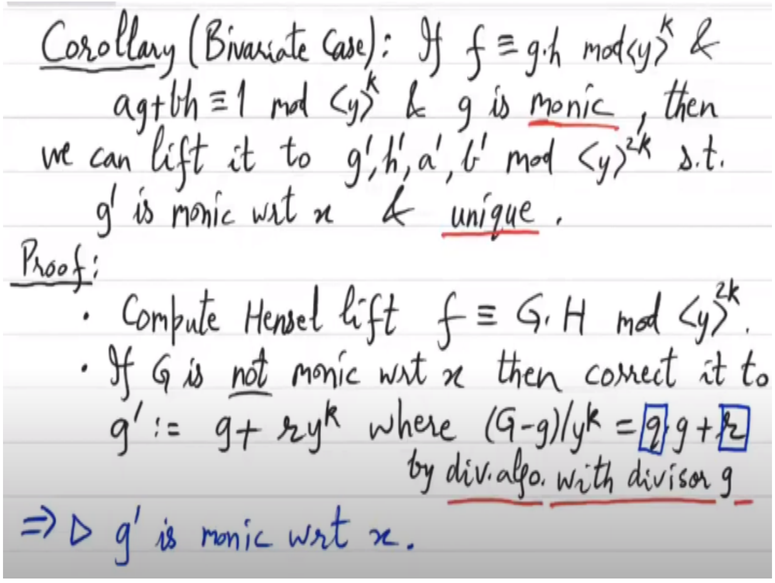
So this cannot happen. So this means that actually there is no lift mod y square of that factorization, right. So you have to assume coprime factorization. So which actually gives you a complete understanding by, Hensel lifting theorem gives you a complete understanding of how lifts happen. Factorization has to be coprime and when it is coprime then it can be lifted to coprime in a unique way, in a very simple way, okay.

Yeah last thing that remains is what Ashish was worried about that what happens to degrees when we are talking about bivariate example. So the special case of this Hensel lifting theorem, when R is bivariate and say you started with a nice factorization of f into g and h where both g and h are monic. So g is of degree d prime and h is of degree d - d prime in terms of x and degree of f is say in terms of x it is d.

So you start with a nice monic coprime factorization. What is the degree of g prime with respect to x? Does it remain the same as before D prime? Can it decrease, increase? So those questions. So basically you want nice factorizations to lift to nice factorizations also in the bivariate case. I mean in the bivariate case we want more properties than what we are promising here.

Because here we did not talk about degree. So that actually is again a long calculation in itself, the special case. So let us do that next.

(Refer Slide Time: 51:03)



Corollary (Bivariate Case): If $f \equiv g \cdot h \bmod \langle y \rangle^k$ & $ag + bh \equiv 1 \bmod \langle y \rangle^k$ & g is monic, then we can lift it to $g', h', a', b' \bmod \langle y \rangle^{2k}$ s.t. g' is monic wrt x & unique.

Proof:

- Compute Hensel lift $f \equiv G \cdot H \bmod \langle y \rangle^{2k}$.
- If G is not monic wrt x then correct it to $g' := g + r y^k$ where $(G-g)/y^k = \boxed{q} g + \boxed{r}$ by div. algo. with divisor g

$\Rightarrow \triangleright$ g' is monic wrt x.

So a corollary of Hensel lifting. So this is for the bivariate case because this is actually the case in which you were originally interested in. So we will have some factorization mod y to the k and then from there we will want to go to mod y to the 2k. That is the motivating case, right? So this we will now give the extra calculations here. So say f g times h mod y to the k and this is coprime, so there is ag + bh.

Moreover g is monic. Actually I do not want, I do not need everything monic. Just yeah g is given to be monic. So that is kind of the key which is key new thing you want to study that what happens to a monic factor, right? Monic again remember is g is bivariate in x and y and look at the leading the highest monomial in x. The coefficient of that is 1, right. That is what monic means.

So suppose this is a so in so this is actually interesting when g is giving you a root of f right? So x – a (y) for example. When g is of this type x - a (y). So a (y) is actually a root of f with respect to y. So the what you want to study is when g is of this type, what happens to it when you lift it? Does it retain that form? That is the motivating case. So obviously, the conclusion or the claim is that we will be able to achieve that form.

So then we can lift it to g prime, h prime, a prime, b prime mod y raised to 2k such that g prime is monic with respect to x and it is unique. Yeah, this will lead more care than what we did before. Because you have to make sure that garbage monomials in x are not added in g, right because we want to make a statement about the highest degree x monomial. So nothing greater than that should be added in g when you are trying to lift.

So the proof correction will not be that difficult. So what you do is compute the lift by previous Hensel lemma, previous algorithm. So just use the previous the theorem algorithm in the theorem that will give you big G and big H in higher precision y to the 2k. You started with low precision small g times small h mod y raised to k and lift that to this.

Now the problem is that this big G may not be monic anymore, because certain things were added in G where higher degree x monomials most probably have been added. You are not careful about that in the proof. So in the bad case G is not monic. Then we change it. So let us correct it to g prime to g prime which is it will basically be, sorry? Yeah, it is not immediately visible here.

So we will perturb g by ry to the k where r is given by a big G in a very specific way. So r is by the division algorithm. So use division algorithm with the g as small g as divisor. So why is that possible? So this big G minus small g that by Hensel lift is divisible by y raised to k. So you can divide that, we can get a polynomial. And that bivariate polynomial you want to run division algorithm where the divisor is small g.

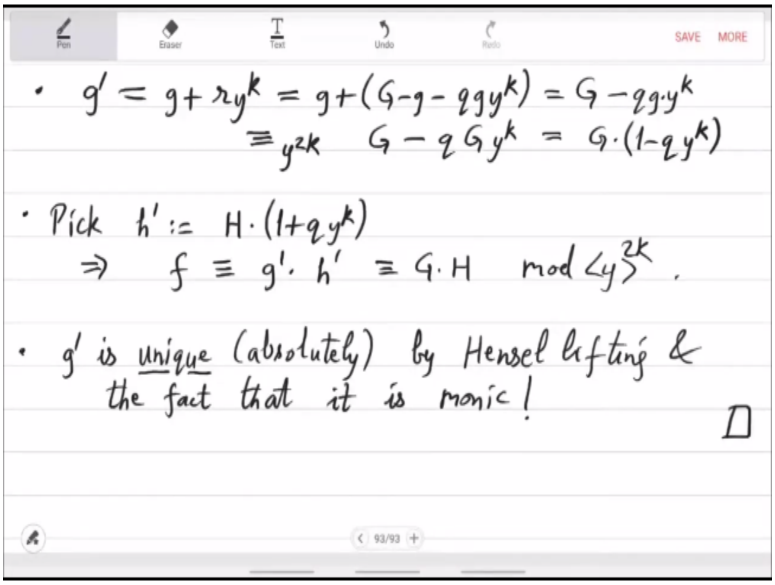
But remember that this these are bivariate polynomial. So how do you do division? Sometimes you cannot do cannot run division algorithm in bivariate. The problem the only problem is that g small g may not be monic. So small g it is leading monomial in x may have some polynomial sitting in y. And then you cannot run the division algorithm. But here that problem is not there because small g is monic.

So small g is something like x square plus y. And you can run the division algorithm with respect to x, right. So you do that. That is the fast algorithm. And you will get q and r. So that is the output you get from the division algorithm. Okay, so r is something whose degree is less than the degree of g with respect to x, right? And you discard q. You use r to define g prime. That is all.

Okay, that is the modification. Yeah, why this works is just a simple calculation now. The algorithmic steps are only this. So just observe that g prime is monic with respect to x. Why is that? Well, because by this division algorithm r has a lower degree in x. And we are perturbing g only by lower degree multiplying by y raised to k. But that would not affect the monic assumption on g.

So the remaining the new polynomial g prime is also monic. Okay, that is the trick. And why is this g prime a factor of f? So that is a simple calculation. It is a factor only mod y to the 2k. Okay, it is a factor of f mod y raised to 2k. So why is that? Yeah, that is fine h will change. But why is g prime a factor? No. You cannot make a non-factor a factor, g prime already has to be a factor. So why is it a factor independent of h? So let us do that calculation.

(Refer Slide Time: 1:01:29)



- $g' = g + ry^k = g + (G - g - qgy^k) = G - qg\cdot y^k$

  $\equiv_{y^{2k}} \; G - qGy^k = G\cdot(1 - qy^k)$

- Pick $h' := H\cdot(1+qy^k)$

  $\Rightarrow \; f \equiv g'\cdot h' \equiv G\cdot H \mod \langle y\rangle^{2k}$.

- g' is unique (absolutely) by Hensel lifting & the fact that it is monic!

$\square$

So g prime is g + ry raised to k. And just from the previous slide, ry raised to k is this which is big G minus q small g y raised to k. Yeah, then you use the special modulus you have. You go to, you go mod y to the 2k. And when you go mod y to the 2k, this small g, you can replace by big G, because they are the same mod y to the k which is G (1 - q y) to the k, fine.

So actually in this special modulus y to the 2k g prime is nothing but just a unit multiple of big G. So obviously it is a factor of f, right? That is all. So yeah, now you can just suitably pick h prime. So h prime you can pick yeah H times the opposite sign. So 1 + qy raised to k. And then you will see that f congruent to g prime h prime mod which is also the same as G times H mod y to the 2k, okay.

So you basically mod y to the 2k you have two lifts, one that Hensel gives you that is big G big H. But if it happens, if big G happens to be non monic then you just do some basically do one division algorithm and modify it. The division algorithm is basically then giving you a q which you are using to multiply a big G with. Okay, you are basically doing that perturbation by multiplication.

And then in the end you get g prime to be monic. Okay, last thing was why is g prime unique? And here unique means without any restrictions, without any transformations. It is absolutely unique. It is absolutely unique because suppose you have g prime prime. So this g prime is monic, monic factor of f and g prime prime is also both lifts of g. By Hensel Lemma the yeah there should be a scaling factor which is a unit.

But that is not possible because monic means that the leading coefficients are both 1. So 1 divided by 1 is just 1. So they have to be identical, okay. So that uniqueness, it actually immediately follows from Hensel. So g prime is unique and that is without restriction. So absolutely by Hensel lemma by Hensel lifting. And the fact that it is monic, okay. Yeah, so that is the major engine of all future factoring algorithms.

Okay, this the first theorem is the major engine and this is a this special case is specialized for bivariate. But the first theorem itself has actually many interesting special cases. This is for bivariate. You can talk about number theoretic analogues. So for example, you have a factorization of a univariate modulo some prime p, then you can ask the question, will it lift to mod p square and mod pq and so on.

Both these special cases we will be using. Okay, the bivariate we will use immediately in the next class. The number theoretic one we will use when we try to factor integral polynomials, okay. So in all the future applications or studies we will be using this. And then finally, also in the n-variate factorization, we will use this in a more complicated way.

Okay so this, actually these calculations form the engine of much of what we will do before the end sem. Any questions? Okay, so thanks.