- In the decoding of RS codes we needed two <u>new</u> algebraic operations:
1) construction of a finite field, &
2) factoring a bivariate polynomial.

<u>Constructing the field $\mathbb{F}_q$</u>.

- Let $q = p^t$. Then, we want to find an irreducible polynomial over $\mathbb{F}_p$ of deg t.

- We will show that a random choice works!

- Let $\pi(\ell)$ denote the number of irreducible polynomials in $\mathbb{F}_p[X]$ of degree ℓ.

- Recall that the polynomial $X^{p^\ell} - X$ has, as factors, <u>all</u> irreducible polynomials of degree $k \mid \ell$.

▷ Thus, $p^\ell = \sum_{k \mid \ell} k \cdot \pi(k)$.

- This identity leads to a "prime number thm" for polynomials.

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

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

<u>Proof</u>: • From the previous identity, we deduce:

$$\ell \cdot \pi(\ell) = p^\ell - \sum_{\substack{k|\ell \\ k<\ell}} k \cdot \pi(k)$$

$$\geq p^\ell - \sum_{k|\ell, k<\ell} p^k$$ [$\because$ the above identity gives $k \cdot \pi(k) \leq p^k$.]

$$\geq p^\ell - \sum_{k=1}^{\lfloor \ell/2 \rfloor} p^k \geq p^\ell - \frac{p}{p-1} \cdot (p^{\ell/2} - 1).$$

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

• Moreover, $\frac{p}{p-1} \cdot (p^{\ell/2} - 1) \leq \frac{1}{2} \cdot p^\ell$, $\forall p \geq 2, \ell \geq 1$.

$\Rightarrow \ell \cdot \pi(\ell) \geq p^\ell/2$ (& $\leq p^\ell$). $\square$

- Thus, if we pick a random degree b polynomial in $\mathbb{F}_p[X]$, then it will be <u>irreducible</u> with probability $\geq 1/2b$.

- On repeating this experiment $2b$ times, the probability of success is $\geq 1-\left(1-\frac{1}{2b}\right)^{2b}$

$$= 1-\left(1-2b\cdot\frac{1}{2b}+\frac{2b\cdot(2b-1)}{2}\cdot\frac{1}{4b^2}-\cdots\right) > \frac{1}{2}.$$

Bivariate factoring

- Idea: • Given $f \in \mathbb{F}[x,y]$, view it as a univariate over $\mathbb{F}(y)$ & factor it by fixing y in $\mathbb{F}$.
  - Say, we factored $f(x,0) = g_0 \cdot h_0$ in $\mathbb{F}[x]$. Can we recover factors of $f(x,y)$?
  - View this as $f(x,y) \equiv g_0 \cdot h_0 \pmod{y}$, & lift this factorization $\pmod{y^2}$, $\pmod{y^4}$, ...

- The algebraic tool is:

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

$f \equiv g\cdot h \pmod{I}$ [I.e. factors mod I) and $\exists a, b \in R$, $ag + bh \equiv 1 \pmod{I}$

[I.e. g, h are "coprime" mod I]

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

$(g', h') \equiv (g, h) \pmod{I}$ [i.e. g', h' are <u>lifts</u>]

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

Moreover, g' & h' are <u>unique</u> up to units.

<u>Proof</u>:

- Consider $m := f - gh$.
- A natural lift would be by the multiples of m: $(g', h') = (g + bm, h + am)$.

$$\Rightarrow f - g'h' \equiv f - (g+bm)\cdot(h+am)$$
$$\equiv m - (ag+bh)\cdot m \pmod{I^2}$$
$$\equiv 0 \pmod{I^2}.$$

- Consider now $m' := 1 - (ag' + bh')$. A natural lift of a, b is by the multiples of m':

$$(a', b') = (a + am', b + bm').$$

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

$$\equiv (1-m') + (1-m')m' \equiv 1 \pmod{I^2}.$$

- Suppose g'', h'' are <u>other</u> lifts of g, h.
- Let $(m_1, m_2) = (g''-g', h''-h')$. [$m_1, m_2 \in I$]

$\Rightarrow f \equiv g''\cdot h'' \equiv g'\cdot h' \pmod{I^2}$.

$\Rightarrow (g'+m_1)\cdot(h'+m_2) \equiv g'\cdot h' \pmod{I^2}$

$\Rightarrow m_2 \cdot g' \equiv -m_1 \cdot h' \pmod{I^2}$

- On multiplying by a', we get

$m_2\cdot(1-b'h') \equiv -m_1\cdot a'h' \pmod{I^2}$

$\Rightarrow m_2 \equiv h'\cdot(b'm_2 - a'm_1) \pmod{I^2}$

$\Rightarrow h'' \equiv h'\cdot(1+u) \pmod{I^2}$ [$u := b'm_2 - a'm_1$]

- Since $u \in I$, $(1+u)$ is a unit mod I^2.
- Similarly, for g''. $\square$

– In our current context, $R = \mathbb{F}[x,y]$ & $I = (y^k)$.

We can strengthen the <u>uniqueness</u> conclusion by starting with a <u>monic</u> g.
(i.e. leading coeff. is 1)

<u>Corollary</u>: If $f \equiv g\cdot h \pmod{y^k}$ s.t. $ag + bh \equiv 1 \pmod{y^k}$