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

- Eg. $f(x,y) = x(x+1) + y^2$

$$\equiv x\cdot(x+1) \quad \bmod \langle y\rangle$$

$$\equiv \quad " \quad \bmod \langle y\rangle^2$$

$$\equiv (x+y^2)\cdot(x+1-y^2) \quad \bmod \langle y\rangle^4$$

$$\cdots\cdots\cdots \quad \bmod \langle y\rangle^{2^k}$$

Later: • factors x & $x+1$ lift $\bmod \langle y\rangle^{2^k}$, $\forall k \geq 0$.

• Though f is irreducible in $\mathbb{F}[x,y]$.

- 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 $f, g, h \in R$:

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

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

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

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

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

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.

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

$\rightarrow \in I \leftarrow$

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

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

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

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

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

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

- Similarly, for g''. □

→ Pseudo-coprimality is crucial for lift:

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

$$f \equiv x \cdot x \mod \langle y \rangle$$

$$\equiv (x + ay)(x + by) \mod \langle y \rangle^2$$

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

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

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

$$\Rightarrow x \mid 1, \quad \lightning.$$

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 $(G - g)/y^k = q \cdot g + r$ by div. algo. with divisor g

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

- $g' = g + ry^k = g + (G - g - qgy^k) = G - qg \cdot y^k$
$\equiv_{y^{2k}} \quad G - qGy^k = G \cdot (1 - qy^k)$

- Pick $h' := H \cdot (1 + qy^k)$
$\Rightarrow \quad f \equiv g' \cdot h' \equiv G \cdot H \mod \langle y \rangle^{2k}$.

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

□

- Qn: What to do when $f(x,y) \bmod \langle y \rangle$ is square-full?

- Eg. $f(x,y) = x^2+y \longmapsto x^2+y-1 \equiv_{\langle y \rangle} x^2-1$

→ ∃ shift of y s.t. f is square-free $\bmod \langle y \rangle$

[except when f was Sq-full in $\mathbb{F}[x,y]$]

- Qn: When do you stop the lift?

Idea: Suppose we reach the lift $f \equiv g_k \cdot h_k \bmod \langle y \rangle^{2^k}$.

→ g_k may, or may not, correspond to an actual factor of f.

- But, Hensel lifting tells us: some multiple of g_k, say $g' := g_k \cdot l_k$ is a factor of $f(x,y)$ in $\mathbb{F}[x,y]$
$= (\mathrm{mod} \langle y \rangle^{2^k}$?)

- We do need to go up to $2^k > \deg f$.

▷ $0 < \deg_x g' < \deg_x f$ & $\deg_y g' \leq \deg_y f$.

▷ $\deg_x l_k < \deg_x f$ & $\deg_y l_k < 2^k$.

- Solve the linear system to find $g'(x,y)$.

Output $\gcd_x(f, g')$.

- This motivates the actual algorithm:

Input: $f \in \mathbb{F}[x,y]$ (with no univariate factors)

Output: A nontrivial factor of f (if it exists). (say, with a factor with $\deg_x <$ $\deg_x f$, or irreducible)

Algo: 1) Preprocess f s.t. f & $f(x,0)$ are both square-free. Insure $\deg_x f = \deg f(x,0) \geq 1$.

Define $d := \deg f$.

2) Factor $f \equiv g_0 \cdot h_0 \mod \langle y \rangle$ s.t. g_0 is monic wrt x, g_0 is irreducible in $\mathbb{F}[x]$ & $0 < \deg g_0 < \deg_x f$.

3) Hensel lift k times s.t. $2^k \geq 2d^2$.

Let $f \equiv g_i \cdot h_i \mod \langle y \rangle^{2^i}$, $\forall\, 0 \leq i \leq k$.

4) Solve the linear system for $\underline{g'}$ & $\underline{\ell_k}$ s.t.

$$g' \equiv g_k \cdot \ell_k \mod \langle y \rangle^{2^k},$$

(deg. bounds as before)

5) Output $\gcd_x(f, g')$.

Analysis:

Step 1: - Say, f is square-full:

- either $\partial_x f = 0 \Rightarrow f = g(x^p, y)$ & $\mathrm{ch}\,\mathbb{F} =: p$
- Or $\partial_x f \neq 0 \Rightarrow \gcd_x(f, \partial_x f)$ factors f.

$\Rightarrow$ We reduce factoring to smaller f.

- Say, $f(x,0)$ is square-full (but f is sq-free):

- For an $\alpha \in \mathbb{F}$, $f(x,\alpha)$ is sq-full
  iff $\gcd_x(f(x,\alpha), \partial_x f(x,\alpha)) \neq 1$
  iff $\mathrm{Res}_x(f, \partial_x f)|_{y=\alpha} = 0$.

$0 \neq r(y) := c(y)$

- $\deg r(y) < 2d^2$.
  $\Rightarrow$ Try $(2d^2)$-many α's in $\mathbb{F}$ (or in its extension) & fix one for which $f(x,\alpha)$ is sq-free.

▷ lead-coeff$_x(f)$ has deg $\leq d$ $\Rightarrow$ Try d-many α's.
→ Overall, try $(d+2d^2)$-many α's in $\mathbb{F}$.

Step 4: f is reducible in $\mathbb{F}[x,y] \Rightarrow (g', l_k)$ exists.

Proof:

- Since, g_0 is an irreducible factor of $f \bmod \langle y \rangle$
  $\Rightarrow g_0$ has to divide some irreducible factor of f,
  say $g \in \mathbb{F}[x,y]$ (& $g \mid f$).

$\Rightarrow \begin{cases} f = g \cdot h \text{ in } \mathbb{F}[x,y] \ \& \\ g \equiv g_0 \cdot l_0 \bmod \langle y \rangle \end{cases}$, for some l_0.

- Hensel lifting (k times) gives us:

$$g \equiv g_k' \cdot l_k' \bmod \langle y \rangle^{2^k} \text{ with } \operatorname{monic}_x g_k' \equiv g_0 \bmod \langle y \rangle$$

$$\Rightarrow f \equiv g_k' \cdot \underbrace{l_k' \cdot h}_{h_k} \bmod \langle y \rangle^{2^k}$$

$\Rightarrow g_k \mid h_k$ by uniqueness! $\Rightarrow g \equiv g_k l_k'$

Step 5 - Using g', this step factors f.

- Suppose not; then $\gcd_x(f, g') = 1$.

$\Rightarrow \exists\, u, v \in \mathbb{F}[x, y]$: $u \cdot f + v \cdot g' = Res_x(f, g')$

$\Rightarrow u \cdot g_k h_k + v \cdot g_k l_k \equiv Res_x(f, g') \mod \langle y \rangle^{2^k}$.

$\Rightarrow g_k \cdot (u h_k + v l_k) \equiv$ " " .

- Since, g_k is monic in x & it <u>has</u> x-monomial, while $Res_x(f, g')$ is x-free.

$\Rightarrow u h_k + v l_k \equiv 0 \mod \langle y \rangle^{2^k}$.

$\Rightarrow Res_x(f, g') \equiv$ " " .

$\Rightarrow Res_x(f, g') = 0$ $[\because 2^k \geq 2d^2] \Rightarrow \gcd_x(f, g') \neq 1$, ↯

Theorem (Kaltofen 1982): Bivariate factoring reduces in det. poly-time to univariate " .

- **Corollary:** It generalizes to n-variate polynomials. For degree d, n-variate, the time-complexity is polynomial in $\binom{n+d}{n} \approx d^{O(n)}$, $n^{O(d)}$.

- **Corollary:** Factoring over $\mathbb{F}_q$ doable in $\text{poly}(d^n, \lg q)$ time (randomized).

Qns: 1) Could we improve on $d^{O(n)}$?
2) Factoring over $\mathbb{Q}$?