Theorem (Berlekamp '67): Polynomial factoring can be done in $\tilde{O}(p \cdot d^3 \cdot n^3)$ time.

- If p is small (eg. $p=2,3,\ldots$) then this is a deterministic poly-time algorithm.

- Berlekamp's algorithm can be used to reduce polynomial factoring over $\mathbb{F}_q$ to that over $\mathbb{F}_p$, in det. poly-time.

- This requires a nice algebraic tool — Resultant.

Defn: • Let $a, b \in \mathbb{F}[x]$ be polys. Euclid's gcd algo. proved the existence of polys $u, v \in \mathbb{F}[x]$, with $(\deg u, \deg v) < (\deg b, \deg a)$, s.t. $ua + vb = \gcd(a,b)$.

[Exercise: Such u, v are unique iff $\gcd(a,b)=1$.]

- Related to this is a system of linear equations in $(\deg a\cdot b)$-many unknowns:

$$(u_0+u_1x+\dots+u_{\deg b-1}\cdot x^{\deg b-1})\cdot a(x) +$$

$$(v_0+v_1x+\dots+v_{\deg a-1}\cdot x^{\deg a-1})\cdot b(x)$$
$$= \gcd(a,b) .$$

[u_i, v_j are unknowns and the eqns. are obtained by comparing the coefficients of x^m on both the sides, $\forall m$.]

- This gives us a matrix $\underline{M_{a,b}}$, over $\mathbb{F}$, of $\deg a\cdot b$ order. Its entries are the coefficients of $a(x)$, $b(x)$ or zeroes.

$$M_{a,b}\cdot\begin{pmatrix} u_0\\ u_1\\ \vdots\\ v_0\\ v_1\\ \vdots \end{pmatrix} = \begin{pmatrix} \\ \\ \\ \end{pmatrix}$$

coeffs. in $\gcd(a,b)$

- $\underline{\text{Resultant}}$ of $a(x)$, $b(x)$ is defined as

$$\underline{Res(a,b)} := |M_{a,b}| .$$

Lemma: $\mathrm{Res}(a,b) \neq 0$ iff $\gcd(a,b) = 1$.

Pf:

- Referring to the previous system of eqns. $(ua+vb=(a,b))$:

$$|M_{a,b}| \neq 0$$

$\iff$ u, v exist & are unique

$\iff$ a, b are coprime. $\square$

— Resultant is a very useful tool in computational algebra.

Mainly, because when a, b are multivariates, say in $\mathbb{F}[x_1, x_2]$,

Variable elimination $\to$ then we can consider $\mathrm{Res}_{x_2}(a,b)$.

It is now a polynomial in $\mathbb{F}[x_1]$.

(It captures those x_1-pts. at which a, b have a common zero.)

▷ If $\gcd_{x_2}(a,b) = 1$ then $\exists\, u, v \in \mathbb{F}[x_1, x_2]$, with $(\deg_{x_2} u, \deg_{x_2} v) < (\deg_{x_2} b, \deg_{x_2} a)$ s.t.

$$ua + vb = \mathrm{Res}_{x_2}(a,b).$$

- Also, we have an easy degree bound:

▷ $\deg_{x_1} \mathrm{Res}_{x_2}(a,b) \leq \deg_{x_2} b \cdot \deg_{x_1} a + \deg_{x_2} a \cdot \deg_{x_1} b$

$\leq (\deg a)\cdot(\deg b)$.

Reduction from $\mathbb{F}_q$ to $\mathbb{F}_p$ —

— We move back to univariate factoring over $\mathbb{F}_q$.

Using resultant we could show:

Theorem: Factoring over $\mathbb{F}_q$ $\leq_p$ Factoring over $\mathbb{F}_p$.

Pf:

- Say, $f(x) \in \mathbb{F}_q[x]$ factors into k equi-degree coprime irreducible polynomials over $\mathbb{F}_q$.
- Using linear-algebra, compute a $g(x) \in \mathbb{F}_q[x]$, with $0 < \deg g < d$ & $g^p \equiv g \pmod f$.

- Compute $h(y) := res_x(f(x), g(x)-y)$.
  [We deduce $\deg h \leq d$.]

- By the properties of the resultant, we know that an $\mathbb{F}_p$-root α of h satisfies:
  $$\gcd(f, g-\alpha) \neq 1.$$

- So, instead of searching for such an α, we could simply factor
  $$h_1(y) := \gcd(h, y^p - y).$$
  [Note: $\deg h_1 \leq d$ & $h_1 \in \mathbb{F}_p[y]$.]

- Each of the steps above are polynomial in $d \cdot \lg q$.

$\square$

$\mathbb{F}_p$-root-finding

Corollary: For polynomial factoring over $\mathbb{F}_q$, it suffices to factor a polynomial $f \in \mathbb{F}_p[x]$, that completely splits & has distinct $\mathbb{F}_p$-roots.