# Berlekamp's algorithm (1967)

- Idea: Factoring $f$ can be seen as factoring the quotient-algebra $A := \mathbb{F}_q[x]/\langle f \rangle$

▷ By CRT: $A \cong \bigtimes_{i=1}^{k} \mathbb{F}_q[x]/\langle f_i \rangle \cong \bigtimes_{i=1}^{k} \mathbb{F}_{q^l}$.

$\prod f_i = x^k$

$= \mathbb{F}_q^{d/k} =: \mathbb{F}_{q^l}$

▷ RHS is known, but the isomorphism we want to find. [Hence, find $f_i$'s]

▷ Any $g \in A$ is a $k$-tuple $(a_1, \ldots, a_k)$, $a_i \in \mathbb{F}_{q^l}$ $\forall i$ & $g \equiv a_i \bmod f_i$.

▷ If $a_1, \dots, a_k \in \mathbb{F}_p$ then $\boxed{g^p \equiv g}$ in $A$.

Pf: $\because a_i^p \equiv a_i \quad \forall i \in [k]$. Then, use CRT. □

– Qn: Find non-constant $g$ : $g^p \equiv g \bmod \langle f \rangle$? of deg $\in [1, d-1]$

▷ Such a $g$ gives a factor of $f$.

Pf: · $g^p - g \equiv 0 \bmod \langle f \rangle$.

$\Rightarrow \prod_{\alpha \in \mathbb{F}_p} (g-\alpha) \equiv 0$ "

$\Rightarrow \prod_{i=1}^{k} f_i \mid \prod_{\alpha \in \mathbb{F}_p} (g-\alpha)$

· Try $\gcd_x(f, g-\alpha)$, $\forall \alpha$.

$\Rightarrow \exists \alpha$, where gcd has deg $\in [1, d-1]$. □

▷ $\{ g \in \mathbb{F}_q[x] \mid g^p \equiv g \bmod f \}$ is a vector space over $\mathbb{F}_p$.

Pf:

- $(c_1 g_1 + c_2 g_2)^p \equiv (c_1 g_1)^p + (c_2 g_2)^p \equiv c_1 g_1^p + c_2 g_2^p$
  $\equiv c_1 g_1 + c_2 g_2$. □

- Let $\mathbb{F}_q =: \mathbb{F}_p[y] / \langle G(y) \rangle$ with $\deg G = n$.
- Write $g(x)$ as $\sum_{i=0}^{d-1} \left( x^i \cdot \sum_{j=0}^{n-1} c_{ij} \cdot y^j \right)$ with unknown $c_{ij} \in \mathbb{F}_p$.

$$\left( \sum_{i,j} c_{ij} x^i y^j \right)^p \equiv \left( \sum_{i,j} c_{ij} x^i y^j \right) \equiv \left( \sum_{i,j} c_{ij} \cdot x^{pi} y^{pj} \right) \bmod f.$$

- Berlekamp's algorithm is:

Step 1: Compute $V := \{ g \mid \boxed{g^p \equiv g \bmod f}, \; 0 \leq \deg g < d \}$

[ $\dim_{\mathbb{F}_p} V \leq d \cdot n$. Basis of $V$ requires linear-algebra algos.; in time $\tilde{O}((dn)^3 \cdot \lg p) + \tilde{O}(dn \cdot \lg p d \cdot \deg q)$. ]

Step 2: Pick a basis element $g \in V \setminus \mathbb{F}_p$. $\forall \, 0 \leq i < p$: If $h := \gcd(f, g - i) \neq 1$ then OUTPUT $h$.

[ Time taken $= p \times \tilde{O}(d \lg q)$. ]

**Theorem:** (Berlekamp '67): Poly. fact. is in $\tilde{O}(p \cdot (dn)^{\omega})$-time.

$\omega$ is MM-exponent.

- If $p$ is small $= (dn)^{O(1)}$, then this is a deterministic poly-time algorithm.
  - In many CS applications, it's good enough.

- Later we see an algorithm that's fast for large $p$; but it's randomized.

OPEN: General poly. fact. in det. poly-time?

# Berlekamp as a reduction method

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

- This requires a nice algebraic tool - Resultant.

- Defn: • Let $a, b \in \mathbb{F}[x]$. Euclid's gcd algo. gives:
$$ua + vb = (a,b) \; ; \; (\deg u, \deg v) < (\deg b, \deg a).$$
• Related to this, is a lin. system in $\deg(ab)$-many unknowns:
$$(u_0 + u_1 x + \dots + u_{\deg b - 1} x^{\deg b - 1}) \cdot a(x) +$$
$$(v_0 + v_1 x + \dots + v_{\deg a - 1} x^{\deg a - 1}) \cdot b(x) = \gcd_x(a,b).$$

- Comparing x-monomials on both sides, we get a matrix $M_{a,b}$, over $\mathbb{F}$, of deg $a \cdot b$ order.

▷ Entries of $M_{a,b}$ are coeffs. of $a(x), b(x)$ or zero.

$$M_{a,b} \cdot \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ v_0 \\ v_1 \\ \vdots \end{pmatrix}_{\deg(ab)} = \begin{pmatrix} \vdots \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \vdots \end{pmatrix}_R$$

coeffs of $\gcd_x(a,b)$.

- Resultant of $a, b$ is defined as:

$$\underline{\mathrm{Res}_x(a,b)} := \det(M_{a,b}) \in \mathbb{F}.$$

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

**Pf:**
- Recall the eqn. $ua + vb = (a,b)$.
- $|M_{a,b}| \neq 0 \iff M_{a,b}^{-1}$ exists.

$\iff$ $u, v$ exist & are unique.

$\iff$ $a, b$ are coprime. (?) [ $u'a = v'b = \frac{ab}{g}$

$\Rightarrow$ $ua + vb = (u-u')a + (v+v')b = g$ ]

[ $1 = ua + vb = u'a + v'b \Rightarrow (u-u')a = (v'-v)b$ □

$\Rightarrow$ $u - u' = v' - v = 0$. ]

- Resultant is very useful in computational algebra (& elimination theory).

– Consider $a, b \in \mathbb{F}[x_1, x_2]$ ; consider $c(x_1) := Res_{x_2}(a, b) \in \mathbb{F}[x_1]$.

<u>Corollary</u>: $c(\alpha) = 0 \implies \{a(\alpha, x_2), b(\alpha, x_2)\}$ have a common root (or factor).

[coprime over $\mathbb{F}(x_1)$]

<u>Lemma</u>: If $gcd_{x_2}(a, b) = 1$ then $\underline{u a + v b = Res_{x_2}(a, b)}$ where $(deg_{x_2} u, deg_{x_2} v) < (deg_{x_2} b, deg_{x_2} a)$ & $u, v \in \mathbb{F}[x_1, x_2]$.

<u>Pf</u>: • Bézout identity in $\mathbb{F}(x_1)[x_2]$: $\underline{u'} a + \underline{v'} b = 1$.

for $u', v' \in$

may not be in $\mathbb{F}[x_1, x_2]$

$\Rightarrow$ By clearing the denominator, we get

$u, v \in \mathbb{F}[x_1, x_2]$ & $w \in \mathbb{F}[x_1]$ s.t.

$ua + vb = w(x_1)$. [ $u := u' \cdot w$ & $v := v' \cdot w$ ]

- Consider the eqn. $M_{a,b} \cdot \begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} =: \overline{B}$

entries in $\mathbb{F}[x_1]$

- By Cramer's rule: $\begin{pmatrix} u' \\ v' \end{pmatrix} = \dfrac{\text{adj}(M_{a,b}) \cdot \overline{B}}{|M_{a,b}|}$

$\Rightarrow$ $w$ can be set to $\text{Res}_{x_2}(a, b)$.

□

▷ $\mathrm{Res}_{x_2}(a,b) \in \langle a,b \rangle_{\mathbb{F}[x_1,x_2]} \cap \mathbb{F}[x_1]$.

Earlier, ▷ For $a,b \in \mathbb{F}[x]$: $\mathrm{Res}_x(a,b) \in \langle a,b \rangle_{\mathbb{F}[x]} \cap \mathbb{F}$.

- Also, we've a degree bound for resultant:

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

$\leq 2 \cdot (\deg a) \cdot (\deg b)$.

⇝ Resultant is 'low'-degree.

# Reduction of factoring ($\mathbb{F}_q$ to $\mathbb{F}_p$)

- Recall univariate factoring over $\mathbb{F}_q$.
  - $f(x) \in \mathbb{F}_q[x]$ factors into $k$ equi-degree coprime irreducibles in $\mathbb{F}_q[x]$.

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

**Pf**:
- Berlekamp gives a $g(x)$ s.t. $0 < \deg g < \deg f =: d$ & $g^p \equiv g \bmod f$.
- $\mathrm{Res}_x(f(x), g(x)-y) =: h(y)$. ← Compute it.
  ▷ $\deg h \leq d$.

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

- Instead of searching for $\alpha \in \mathbb{F}_p$, simply factorize
  $$h_1(y) := \gcd(h(y), y^p - y).$$
  ▷ $h_1$ completely splits & has 'good' $\alpha$ as roots!
  ▷ $\deg h_1 \leq d$.
- All the steps are doable in poly$(d \lg q)$-time. □

Corollary ($\mathbb{F}_p$-root-finding): For poly. fact. over $\mathbb{F}_q$, it suffices to factor an $f \in \mathbb{F}_p[x]$, that completely splits into distinct $\mathbb{F}_p$-roots.