Polynomial factorization

– **Problem:** Given $f(x) \in \mathbb{F}[x]$ of degree d. Compute a $g(x) \mid f(x)$ of degree in $\{1, \ldots, d-1\}$.

field

(In poly(d)-many $\mathbb{F}$-operations?)

Fact: $\mathbb{F}[x]$ is a <u>unique factorization domain</u>.

assume f & f_i's monic

I.e. each $f(x)$ factors as $f = \prod_i f_i^{e_i}$ uniquely,

where f_i's are coprime <u>irreducible</u> polynomials in $\mathbb{F}[x]$.

– Factorization pattern depends on the specifics of the field $\mathbb{F}$.

– Eg. $f := x^2 + 2$ is irreducible over $\mathbb{Q}$, but factors, as $f = (x-1)(x+1)$, over $\mathbb{F}_3$.

(Gauss) ▷ Over $\mathbb{C}$, every polynomial factors!

Over finite fields

- Polynomial factorization over $\mathbb{Q}$ is trickier than that over $\mathbb{F}_2$.

- So, we first focus on finite fields.
(useful in combinatorics & computer science)

- Let p be a prime.

▷ $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field.

▷ Let $f(x)$ be an irreducible polynomial of degree n in $\mathbb{F}_p[x]$.
Then, $\mathbb{F}_{p^n} := \mathbb{F}_p[x]/\langle f\rangle$ is the field of size $p^n =: q$. Its bitsize is $O(\lg q)$.

- Eg. x^2+x+1 is irreducible in $\mathbb{F}_2[x]$.
So, $\mathbb{F}_2[x]/\langle x^2+x+1\rangle$ is the field $\mathbb{F}_4$.
It has 4 elements:
$\{0, 1, x, 1+x\}$.

- $\because$ $\mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ is an abelian group of size $(q-1)$, we get

▷ $\forall a \in \mathbb{F}_q^*$, $a^{q-1} = 1$.

▷ $\forall a \in \mathbb{F}_q$, $a^q = a$. (Fermat's little theorem)

- These basic properties inspire an <u>irreducibility test</u>:

<u>Theorem</u>: $f \in \mathbb{F}_q[x]$, of $\deg = d$, is reducible iff $\exists\, 0 < i < d$, $\gcd(f, x^{q^i} - x) \neq 1$.

<u>Proof</u>:

($\Rightarrow$): Let $h \mid f$ be an irreducible factor of $\deg = d' \in [d-1]$.

- $\mathbb{F}_q[x]/\langle h \rangle$ is a field of size $q^{d'}$.

$\Rightarrow$ $x^{q^{d'}} = x \pmod h$.

$\Rightarrow$ $h(x) \mid \gcd(f, x^{q^{d'}} - x)$.

$(\Leftarrow)$: Say, f is irreducible & let $0<i<d$ be the least s.t. $\gcd(f, x^{q^i}-x) \neq 1$.

$\Rightarrow f \mid (x^{q^i}-x)$.

$\Rightarrow x^{q^i} = x \pmod f$

$\Rightarrow a(x)^{q^i} = a(x)$, $\forall a \in \mathbb{F}_q[x]/(f)$.

(Use the fact $(y+z)^q = y^q + z^q \bmod p$.)

$\Rightarrow$ The group $(\mathbb{F}_q[x]/(f))^*$ has size at most $(q^i - 1)$.

$\Rightarrow \quad q^d - 1 \leq q^i - 1 \Rightarrow d \leq i$, $\lightning$

· The contradiction means that f is reducible. $\square$

<u>Algorithm</u>: (<u>Input</u>: $\deg = d$ $f \in \mathbb{F}_q[x]$)

<u>Step 1</u>: For $0 < i < d$:

If $(f, x^{q^i} - x) \neq 1$ then output <u>Reducible</u>.

<u>Step 2</u>: Output <u>Irreducible</u>.

Time analysis:

- For all i, first compute $x^{q^i} \pmod f$ using repeated squaring.

- Then, compute $(f, x^{q^i} - x)$ by Euclid's gcd algorithm.

$$\Rightarrow \text{steps} = d \cdot d \lg q \cdot \tilde{O}(d) + d \cdot \tilde{O}(d)$$
$$= \tilde{O}(d^3 \cdot \lg q) \quad \mathbb{F}_q\text{-operations}.$$

$$= \tilde{O}(d^3 \cdot \lg^2 q) \quad \text{bit-operations}.$$

Corollary: We can factor $f(x)$ as $\prod_i g_i$, where each $g_i(x) \in \mathbb{F}_q[x]$ is a product of equi-degree irreducible polynomials, in $\tilde{O}(d^3 \cdot \lg^2 q)$ time.

Pf:

- Observe that if f has irreducible factors h_1 resp. h_2 of degrees $d_1 < d_2$ resp., then

$\gcd(f, x^{q^{d_1}} - x)$ is divisible by h_1 but not h_2. $\square$

- Now we move to the case of a square-full f.

<u>Defn</u>: If there is an irreducible h s.t. $h^2 | f$, then $f(x)$ is called <u>square-full</u>. Else $f(x)$ is <u>square-free</u>.

- In this case the derivative is used.

<u>Defn</u>: If $f(x) = \sum_{i=0}^{d} a_i x^i$ then its <u>derivative</u>

is $\underline{\partial_x f} := \sum_{i=0}^{d} i \cdot a_i \cdot x^{i-1} \in \mathbb{F}_q[x]$.

▷ For a nonzero f, $\partial_x f = 0$ iff $\exists g, h$
$f = g(x^p) = h^p$.

Proof: • Say, $f = \sum_{i\in S} a_i x^i$ with $a_i \in \mathbb{F}_q^*$.

• Since, $\partial_x f = \sum_{i\in S} i \cdot a_i \cdot x^{i-1} = 0$,

we deduce that $\forall i \in S$, $i = 0$ in $\mathbb{F}_q$

$\Rightarrow \forall i \in S$, $p \mid i$.

$\Rightarrow$ f has the form $g(x^p)$. $\square$

– So, for factorization purposes, we assume that $\partial_x f$ is nonzero.

Lemma: If $h^2 \mid f$ then $h \mid \partial_x f$.

Proof:

• Let $f = g \cdot h^2$ in $\mathbb{F}_q[x]$.

$\Rightarrow \partial_x f = (\partial_x g) \cdot h^2 + g \cdot (2 \cdot h \cdot \partial_x h)$

$\Rightarrow h \mid \partial_x f$. $\square$

Algo: (1) Output $\gcd(f, \partial_x f) =: h$.

$\triangleright$ Works, if $f(x)$ is square-full!

$\deg h < \deg f$, > 0

- Thus, we can now assume that the unknown factorization is $f = \prod_{i\in[k]} f_i$, where f_i's are coprime irreducible polynomials in $\mathbb{F}_q[x]$ of $\deg = d/k$.

Berlekamp's algorithm (1967)

- The question of polynomial factoring can be seen as that of factoring the quotient-algebra

$$\mathcal{A} := \mathbb{F}_q[x]/(f).$$

- By CRT, $\mathcal{A} \cong \bigtimes_{i=1}^{k} \mathbb{F}_q[x]/(f_i)$.

▷ Note that $\mathbb{F}_q[x]/(f_i)$ are all isomorphic to the field $\mathbb{F}_{q^{d/k}} =: \mathbb{F}_{q'}$.

$\Rightarrow \mathcal{A} \cong \bigtimes_{i\in[k]} \mathbb{F}_{q'}$.

- Equivalently, every element $g \in A$ can be seen as a k-tuple $(a_1, \ldots, a_k)$, where $g(x) \equiv a_i(x) \pmod{f(x)}$.

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

- Since we know that (from FLT: $x^p - x = \prod_{\alpha \in \mathbb{F}_p} (x-\alpha)$.)

$$g^p - g = \prod_{\alpha \in \mathbb{F}_p} (g - \alpha),$$

we could use this to factor $f(x)$ when $\forall \alpha \in \mathbb{F}_p$, $g(x) \not\equiv \alpha \pmod{f}$.

▷ If $a_1, \ldots, a_k \in \mathbb{F}_p$ are <u>not all</u> equal, then $g = (a_1, \ldots, a_k) \not\equiv \alpha$ in A, $\forall \alpha \in \mathbb{F}_q$.

Pf:

- Say, $g \equiv \alpha$ in A for some $\alpha \in \mathbb{F}_q$.

  $\Rightarrow (a_1 - \alpha, \ldots, a_k - \alpha) \equiv 0$ in A.

  $\Rightarrow a_1 \equiv a_2 \equiv \ldots = a_k \equiv \alpha$ in A, which is a contradiction. $\square$

- Thus, there are $(p^k - p)$ solutions for $g^p \equiv g \mod \langle f \rangle$ such that $0 < \deg g < \deg f$.

- If we can find such a g then, since
$$\prod_{i \in [k]} f_i \;\Big|\; \prod_{\alpha \in \mathbb{F}_p} (g - \alpha) \quad \text{in } \mathbb{F}_q[x],$$
we can deduce that $\gcd(f, g-\alpha)$ will factor f for some $\alpha \in \mathbb{F}_p$.
[Else, $f \mid (g-\alpha)$ for some α & we get that $\deg(g-\alpha) \notin [d-1]$ $\lightning$]

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

Pf: · Note that $(c_1 g_1 + c_2 g_2)^p = c_1 g_1^p + c_2 g_2^p$ for $c_1, c_2 \in \mathbb{F}_p$. □

- Let $\mathbb{F}_q = \mathbb{F}_p[y]/\langle G(y) \rangle$ with $\deg G = n$. We shall write $g(x) = \sum_{i=0}^{d-1} \left(\sum_{j=0}^{n-1} c_{ij} y^j \right) x^i$, with unknowns $c_{ij} \in \mathbb{F}_p$.

- Berlekamp's algorithm is then:
(Say, $q = p^n$.)

$\dim_{\mathbb{F}_p} V < d \cdot n$

Step 1: Compute $\{ g \mid g^p \equiv g \pmod f,\ 0 \le \deg g < d \} =: V$.

[Note that V is an $\mathbb{F}_p$-vector-space. So, we can compute a basis of V using linear-algebra, in time $\tilde{O}(d^2 \cdot \lg p d \cdot \lg q) + \tilde{O}(d^3 n^3 \cdot \lg p)$.]

Step 2: Pick a basis element $g \in V$ that is not in $\mathbb{F}_p$. For all $0 \le i < p$:

If $h := \gcd(f, g-i)$ is a proper factor then output h.

[$\because$ $g^p \equiv g \pmod f$, we have $\prod_{i \in [k]} f_i \mid \prod_{j \in \mathbb{F}_p} (g-j)$. Since, g is a non-$\mathbb{F}_p$ element in A, one of the $(g-j)$ is guaranteed to factor f.]

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

Theorem (Berlekamp '67): Polynomial factoring can be done in $\tilde{O}(p.(dn)^{\omega})$ time.

[ω is the MM exponent.]

- If p is small $\approx (dn)^{O(1)}$ (eg. $p = 2, 3, \ldots$) then this is a deterministic poly-time algorithm.

- In many CS applications p is that small & Berlekamp is good enough.

- Later we will see an algorithm that is fast for all p, but it will be randomized.

- General polynomial factoring is still an open question!