Polynomial factorization

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

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

  ($\mathbb{F}$: field)

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

I.e. each $f(x)$ factors as $f = \prod_i f_i^{e_i}$ uniquely, where f_i's are irreducible polynomials in $\mathbb{F}[x]$.

(assume f & f_i is monic; coprime)

- 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 ireducible polynomial of degree n in $\mathbb{F}_p[x]$.
Then, $\mathbb{F}_{p^n} := \mathbb{F}_p[x]/\langle f \rangle$ is <u>the</u> field of size $p^n =: q$.

- Eg. x^2+x+1 is ireducible 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

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

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

- These basic properties inspire an irreducibility test:

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

Proof:

$\Rightarrow$: 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 $q^{d'}$.

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

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

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

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

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

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

(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).

$\Rightarrow q^d - 1 \leq q^i - 1$

$\Rightarrow i = d$. [$\because$ we have $i \leq d$ already.] $\square$

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

Step 1: For $0 < i < d$:

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

Step 2: Output Irreducible.

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.

$\Rightarrow$ steps $= d \log q \cdot \tilde{O}(d) + d \cdot \tilde{O}(d^2)$

$= \tilde{O}(d^3 \cdot \log q)$ $\mathbb{F}_q$-operations.

$= \tilde{O}(d^3 \cdot \log^2 q)$ 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 $\tilde{O}(d^3 \cdot \log^2 q)$ time.

Pf:

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