

Pen



Eraser



Text



Undo



Redo

SAVE

MORE

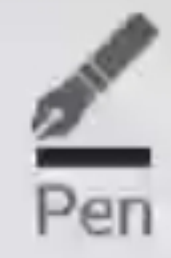
Polynomial Factorization

- Problem: Given $f(x) \in \mathbb{F}[x]$ of degree d .
 Compute $g(x) \in \mathbb{F}[x]$ of $\deg \in [d-1]$ s.t. $g | f$.
 \hookrightarrow in $\text{poly}(d)$ -many \mathbb{F} -operations?

Fact: $\mathbb{F}[x]$ is a unique factorization domain.
 I.e. each f factors as $f = \prod_i f_i^{e_i}$ uniquely,
 where f_i is irreducible & are mutually
coprime.

(exercise.)





Pen



Eraser



Text



Undo



Redo

SAVE MORE

- Factorization pattern depends on the field.
 (So do its algorithms.)

- eg. $f = x^2 + 2$ is irreducible over \mathbb{Q} ,
 but is reducible over \mathbb{F}_3 :

$$f \equiv_3 (x-1)(x+1)$$

$$\equiv_2 x^2$$

▷ [Gauss] Over \mathbb{C} , every polynomial factors!

[so, completely splits]

- Defn: Algebraically closed:



Pen



Eraser



Text



Undo



Redo

SAVE

MORE

Over finite fields

[later we'll do over \mathbb{Q} .]

- Finite fields are discrete objects useful in combinatorics & CS.

- Let p be a prime.

▷ $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ is a field.

▷ Let $f(x)$ be an irreducible poly. of degree n in $\mathbb{F}_p[x]$. Then, $\mathbb{F}_p[x]/\langle f \rangle =: \mathbb{F}_{p^n} = \mathbb{GF}(p^n)$

is the field of size $p^n =: q$. Bitsize = $O(\log q)$.



Pen



Eraser



Text



Undo



Redo

SAVE

MORE

- 2g. $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible.

$$\text{So, } GF(4) = \mathbb{F}_2[x] / \langle x^2 + x + 1 \rangle \\ = \{0, 1, x, 1+x\}.$$

- 2g. $F(x) = x^2 + x \in GF(4)[x]$
 $\equiv (x + x + 1)^2$

- $\therefore \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$ is a cyclic group of size $q-1$.

\Rightarrow

$$\triangleright \forall a \in \mathbb{F}_q^*, \quad a^{q-1} \equiv 1$$

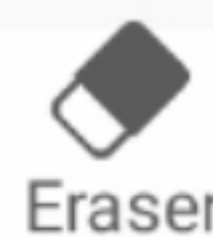
$$\triangleright \forall a \in \mathbb{F}_q, \quad a^q \equiv a. \quad [\text{Fermat's little thm.}]$$

[Frobenius action]





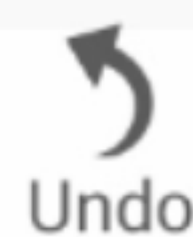
Pen



Eraser



Text



Undo



Redo

SAVE MORE

- These basic properties inspire an irreducibility test:

$$F \in \mathbb{F}_q[x], \quad (F(x), x^q - x) = ?$$

(Input bitsize $\approx d \cdot \log q$) $(F, x^{q^2} - x) = ?$ & so on.

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

Pf: \Rightarrow :

Let $h \mid F$ be an irreducible factor of
 $\deg d' \in [d-1]$. $\Rightarrow \mathbb{F}_q[x] / \langle h(x) \rangle = \text{GF}(q^{d'})$
 $\Rightarrow x^{q^{d'}} \equiv x \pmod{\langle h \rangle} \Rightarrow h \mid (F, x^{q^{d'}} - x)$.

\Leftarrow : Say, F is irreducible & let $i \in [d-1]$ be the least s.t. $(F, x^{q^i} - x) \neq 1$.

$$\Rightarrow F \mid x^{q^i} - x$$

$$\Rightarrow x^{q^i} \equiv x \pmod{\langle F \rangle}$$

$$\Rightarrow \forall a \in \mathbb{F}_q[x] / \langle F(x) \rangle =: \mathbb{F}_{q^d}, \quad a(x)^{q^i} \equiv a(x)$$

[$\because (y+z)^q \equiv y^q + z^q \pmod{p}$ by binomials.]

[$x \mapsto x^q$ by p is an \mathbb{F}_p -automorphism here.]

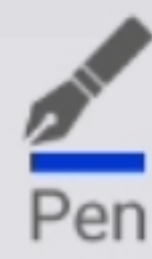
• $(\mathbb{F}_{q^d})^*$ is a cyclic group of size $q^d - 1$.

$$\Rightarrow q^d - 1 \mid q^i - 1 \Rightarrow d \leq i \Rightarrow \begin{matrix} \swarrow \\ \searrow \end{matrix}$$

\Rightarrow Converse holds!

[$d \mid i$]

□



Pen



Eraser



Text



Undo



Redo

SAVE MORE

Algorithm: (Input - deg = d poly. $F \in \mathbb{F}_2[x]$.)

Step 1:

For $1 \leq i \leq d/2$:

If $(F, x^{2^i} - x) \neq 1$ then OUTPUT Reducible.

\uparrow
reduce mod F by repeated-squaring

Step 2: OUTPUT Irreducible.

Time Complexity: $d \times [d \lg q \times \tilde{O}(d) + \tilde{O}(d)] \mathbb{F}_q$ -ops.

$\leq \tilde{O}(d^3 \lg q) \mathbb{F}_q$ -ops.

$\leq \tilde{O}(d^3 \lg^2 q)$ bit-ops.



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

Pf: Keep updating F as $F / \gcd(F, x^{2^i} - x)$ & continue with $i, \dots, (d-1)$. \square

\rightarrow Thus, we could assume F to have equideg. irreducible factors. (wlog)

- What if $h^2 \mid f$? [square-full f]
e.g. $f = x^2$ vs. $(x+1)(x+2)$



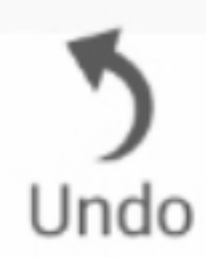
Pen



Eraser



Text



Undo



Redo

SAVE MORE

- In the square-full case we can use the (formal) derivative:

- Defn: For $f(x) = \sum_{i=0}^d a_i x^i$, derivative
 $\partial_x f := \sum_{i=0}^d i a_i x^{i-1} \in \mathbb{F}_q[x]$.

▷ For a nonzero f , $\partial_x f = 0$ iff $f = g(x^p) = h^p$ for some $g, h \in \mathbb{F}_q[x]$.

Pf: \Rightarrow : Say, $f = \sum_{i \in S} a_i x^i$ s.t. $\forall i \in S, a_i \neq 0$.
 $\Rightarrow \partial_x f = \sum_{i \in S} \underbrace{i a_i x^{i-1}} = 0$.
 $\Rightarrow \forall i \in S, p | i$.



$$\Rightarrow f(x) = \underline{g(x^p)} := \sum_{i \in S} a_i (x^p)^{i/p}$$

• Define $\underline{h} := \sum_{i \in S} (a_i^{1/p}) \cdot (x^{i/p}) \in \mathbb{F}_q[x]$.

$$\Rightarrow h^p = f. \quad [\Delta^{p=p^n} \Rightarrow a_i^{1/p} = a_i^{p^{n-1}} \in \mathbb{F}_q]$$

□

Lemma: $h^2 \mid f \Rightarrow h \mid \partial_x f$.

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

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

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



Pen



Eraser



Text



Undo



Redo

SAVE

MORE

Algo: 0) If $\partial_x f = 0$ then output $f^{1/p}$.
1) If $\gcd(f, \partial_x f) \neq 1$ then output it.

▷ Algo. above works if f is square-full.

→ Now we can assume that f has coprime equidegree irreducible factorization:

$$f = \prod_{i \in [k]} f_i \quad ; \quad f_i \text{ is irreducible in } \mathbb{F}_q[x] \text{ of deg} = d/k.$$

