$\gcd(f, x^{2^{d_1}} - x)$ is divisible by h_1 but not h_2. □

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

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

- In this case the derivative is used.

Defn: 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 $\exists g$, $f = g(x^p)$.

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 $g(x^p)$. □

– 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 $\mathbb{F}_q[x]$.

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

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

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

▷ 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

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

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

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

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

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

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

- Since we know that

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

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

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

Pf:

- Say, $g \equiv \alpha$ in $\mathcal{A}$ for some $\alpha \in \mathbb{F}_p$.
  $\Rightarrow (a_1 - \alpha, \dots, a_k - \alpha) \equiv 0$ in $\mathcal{A}$.
  $\Rightarrow a_1 \equiv a_2 \equiv \dots = a_k \equiv \alpha$ in $\mathcal{A}$,
  which is a contradiction. □

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

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

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

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

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 $p \cdot \tilde{O}(d^2 \cdot \lg q)$.]