(**)
[This follows from:]

Lemma 9.2

Let char$(k)=p$ (≥ 0). We can compute all pol.

$$a_k(X) = \prod_{\substack{t:\\ \underbrace{v_t(f)\equiv k \bmod p}_{(\Leftrightarrow\, v_t(f)=k \text{ if } \mathrm{char}(k)=p=0 \text{ or } p>n)}}} t(X) \quad \text{for } 1 \leq k \leq N := \begin{cases} \min(p-1,n), & p \neq 0 \\ n, & p=0. \end{cases}$$

in time $\tilde{O}(n)$.

Pf of Thm 9.1 (using Lemma 9.2)

Clear if $p=0$ or $p>n$, so assume $2 \leq p \leq n$.

The polynomial

$$h(X) = \frac{f(X)}{\prod_{1\leq k\leq p-1} a_k(X)^k} \quad \text{is a } p\text{-th power.}$$

Recursively apply the alg. (from the Thm.) to the pol. $\sqrt[p]{h(X)}$ of degree $\leq \frac{n}{p}$.

$$\rightsquigarrow \sigma_l(X) = \prod_{\substack{t:\\ \underbrace{v_t(\sqrt[p]{h})=l}_{\Leftrightarrow\, v_t(h)=lp}}} t(X) \quad \text{for } l=1,\dots,\left\lfloor \tfrac{n}{p} \right\rfloor.$$

$$\Rightarrow s_{k+lp} = \gcd(a_k, \sigma_l) \text{ for } 1\leq k\leq p-1, \ 1\leq l\leq \left\lfloor \tfrac{n}{p}\right\rfloor.$$

$$s_k = \frac{a_k}{\prod_{l\geq 1} s_{k+lp}} \quad \text{for } 1\leq k\leq p-1$$

$$s_{lp} = \frac{\sigma_l}{\prod s_{k+lp}} \quad \text{for } 1\leq l\leq \left\lfloor \tfrac{n}{p}\right\rfloor. \qquad \square$$

Alg for Lemma 9.2

(All gcds are assumed to be monic)

Compute $g = \gcd(f, f')$, $b_0 = \frac{f}{g}$, $c_0 = \frac{f'}{g} - b_0'$

For $k = 1, \ldots, N$:

Compute $a_k = \gcd(b_{k-1}, c_{k-1})$, $b_k = \frac{b_{k-1}}{a_k}$, $c_k = \frac{c_{k-1}}{a_k} - b_k'$

<u>Claim</u> (correctness) We have

$$a_k = \prod_{\substack{t: \\ v_t(f) \equiv k \bmod p}} t(x) \qquad \text{for } k = 1, \dots, N$$

$$b_k = \prod_{\substack{t: \\ v_t(f) \not\equiv 0, \dots, k \bmod p}} t(x) \qquad \text{for } k = 0, \dots, N$$

$$c_k = \sum_{\substack{t: \\ v_t(f) \not\equiv 0, \dots, k \bmod p}} (v_t(f) - (k+1)) \cdot \frac{t'(x)}{t(x)} \cdot b_k(x). \qquad \text{for } k = 0, \dots, N$$

<u>Pf (by ind. over k)</u>

<u>$k=0$:</u>

$$f(x) = \prod_t t(x)^{v_t(f)}$$

$$\Rightarrow f'(x) = \sum_{t:} v_t(f) \cdot \frac{t'(x)}{t(x)} \cdot f(x)$$

If $v_t(f) = 0$, then $v_t(g) = 0$.

<u>Otherwise</u>: If $v_t(f) \not\equiv 0 \bmod p$, then $v_t(f') = v_t(f) - 1$ (because $t' \neq 0$) $\Rightarrow v_t(g) = v_t(f) - 1$.
(so $v_t(f) \neq 0$ in k)

If $v_t(f) \equiv 0 \bmod p$, then $v_t(f') \geq v_t(f)$. $\Rightarrow v_t(g) = v_t(f)$.
(so $v_t(f) = 0$ in k)

$$\Rightarrow g(x) = \prod_{\substack{t: \\ v_t(f) \not\equiv 0}} t(x)^{v_t(f)-1} \cdot \prod_{\substack{t: \\ v_t(f) \equiv 0}} t(x)^{v_t(f)}$$

$$\Rightarrow b_0(x) = \frac{f(x)}{g(x)} = \prod_{\substack{t: \\ v_t(f) \not\equiv 0}} t(x)$$

$$c_0(x) = \frac{f'(x)}{g(x)} - b_0'(x) = \sum_{\substack{t: \\ v_t(f) \not\equiv 0}} (v_t(f) - 1) \frac{t'(x)}{t(x)} \cdot b_0(x)$$

$k-1 \to k$:

- Let $t \mid b_{k-1}$.

Then, $v_t(c_{k-1}) = \begin{cases} 1, & v_t(f) \equiv k \mod p \\ 0, & v_t(f) \not\equiv k \mod p \end{cases}$

$\Rightarrow a_k$ is as claimed.

$\Rightarrow b_k$ — —

$$b_k'(x) = \sum_{\substack{t: \\ v_t(f) \not\equiv 0,\dots,k}} \frac{t'(x)}{t(x)} \cdot b_k(x).$$

$\Rightarrow c_k$ is as claimed. $\square$

Claim: The alg. has running time $\tilde{O}(n)$.

Running time $= \tilde{O}\left(\sum \deg(a_k) + \sum \deg(b_k) + \sum \deg(c_k)\right)$.

$\deg(a_k) \leq \deg(b_{k-1})$

$\deg(c_k) \leq \deg(b_k)$

$$\sum_k \deg(b_k) \leq \sum_t v_t(f) \cdot \deg(t)$$
$$= \deg\left(\prod t(x)^{v_t(f)}\right)$$
$$= \deg(f) = n. \qquad \square$$

10. Factoring over finite fields

~~10.1: Distinct degree factors~~

You've seen one method (Berlekamp–Zassenhaus) on problem set

(Expected running time $\tilde{O}(n^{\omega} + n\log q)$)

There are faster algorithms that work more like the root-finding alg. in section 8:

10.1. Distinct-degree factorisation

Lemma 10.1.1

$$X^{q^k} - X = \prod_{\substack{t \in \mathbb{F}_q[X] \\ \text{monic irred} \\ \deg(t) \mid k}} t(X).$$

Pf: If t is irred. of degree $d \mid k$, then its splitting field is $\mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^k}$

$\Rightarrow$ Each ~~root~~ r of t satisfies $r^{q^k} = r$

$\Rightarrow$ RHS $\mid$ LHS.

On the other hand, each root r of $X^{q^k} - X$ lies in $\mathbb{F}_{q^k}$.

Now, $\mathbb{F}_q \subseteq \mathbb{F}_q(r) \subseteq \mathbb{F}_{q^k}$, so $\mathbb{F}_q(r) = \mathbb{F}_{q^d}$ for some $d \mid k$. The min. pol. of r has degree d.

$\Rightarrow$ LHS $\mid$ RHS. $\square$

Cor 10.1.2 Let $f \in \mathbb{F}_q[X]$ be a pol. of degree n and assume we are given the n polynomials $X^{q^k} \bmod f$ for $k=1,\dots,n$. Then, we can compute the degree k parts

$$g_k(X) = \prod_{\substack{t \mid f \text{ monic irred} \\ \deg(t)=k}} t(X) \quad \text{of } f(X) \text{ for } k=1,\dots,n$$

in time $\tilde{O}(n^2)$.

Rmk If f is squarefree, then $f(X) = g_1(X)\cdots g_n(X)$.

Alg Let $h_0 = f$. w.l.o.g. f is squarefree (after using Thm 9.1 and replacing $f(X)$ by $s_1(X)\cdots s_n(X)$.)

For $k=1,\dots,n$:

compute $g_k = \gcd(h_{k-1}, X^{q^k}-X)$

and $h_k = \dfrac{h_{k-1}}{g_k}$. □

~~If $g_k = 1$, we "compute" $h_k = h_{k-1}$ in $O(1)$!~~

Q How to compute $\alpha_k = X^{q^k}$ (mod f) for $k=1,\dots,n$?

~~Rmk Fast exponentiation takes time $\tilde{O}(n \log q^k) = \tilde{O}(nk \log q)$.~~

Rmk $\alpha_k(X) = \alpha_{k-1}(X)^q$, so using fast exponentiation, we can compute α_k from α_{k-1} in $\tilde{O}(n \log q)$.

$\Rightarrow$ Total time $\tilde{O}(n^2 \log q)$.

We can do faster!

Rmk $\alpha_{k+l}(X) \equiv X^{q^{k+l}} \equiv (X^{q^k})^{q^l} \equiv \alpha_l(\alpha_k(X)) \bmod f(X)$.

Warning In general, if $\alpha(X) \equiv \beta(X) \bmod f(X)$, then $\alpha(\gamma(X)) \equiv \beta(\gamma(X)) \bmod f(\gamma(X))$

not $\bmod f(X)$!

Pf of Rmk $\alpha_l(X) \equiv X^{q^l} \bmod f(X)$

$\Rightarrow \alpha_l(\alpha_k(X)) \equiv \alpha_k(X)^{q^l} \bmod f(\alpha_k(X))$.

Since $f(\alpha_k(X)) \equiv f(X^{q^k}) \equiv f(X)^{q^k} \equiv 0 \bmod f(X)$,

$\boxed{\alpha_k(X) \equiv X^{q^k} \bmod f(X)}$

$\boxed{Y \mapsto Y^{q} \text{ is a hom. on } \mathbb{F}_q(X) \text{ and fixes the coeff. of } f}$

this implies

$$\alpha_l(\alpha_k(X)) \equiv \alpha_k(X)^{q^l} \equiv (X^{q^k})^{q^l} \equiv X^{q^{k+l}} \equiv \alpha_{k+l}(X) \bmod f(X)$$

$\square$