~~$\alpha_{k+l}(X) = X^{q^{k+l}} = X^{q^k \cdot q^l} = (X^{q^k})^{q^l} = \alpha_l(\alpha_k(X))$ mod f.~~

~~Pf $g_l(X) - X^{q^l} = f(X)\, g_l(X)$ for some pol. $g(X)$~~

$\alpha_l(X) \equiv X^{q^l}$ mod f

~~$\Rightarrow \alpha_l(\alpha_k(X)) = \alpha_l(X^{q^k}) = (X^{q^k})^{q^l} + f(X^{q^k})\, g_l(X^{q^k}) \equiv X^{q^{k+l}}$ mod f(X)~~

~~Warning: in general, $\beta(x)$ mod $f(x)$ doesn't imply $f(X)^{q^k}$ $\alpha(\beta(x)) \equiv \beta(\beta(x))$ mod $f(x)$!~~

Modular composition problem

Given polynomials $\alpha(X), \beta(X), f(X)$ of degree $< n$,

compute $\alpha(\beta(X))$ mod f.

(Note that it's in general not enough to know $\alpha(X)$ mod $f(X)$!)

Rmk Evaluating α at $\beta(X)$ using "Cor 5.3" takes time $\tilde{O}(n^2)$.

degree of β

It can be done faster, but I won't explain a better alg. for modular composition. Instead, we'll use a "cheat":

Evaluating a pol. of degree n at n points is not much harder than evaluating it at a single point(!):

Lemma 10.1.3 Assume we can do arithmetic in R in $O(1)$.

Let $f \in R[X]$ be a pol. of degree $\leq n$ and let $c_1, \ldots, c_n \in R$.

We can compute $f(c_1), \ldots, f(c_n)$ in $\tilde{O}(n)$.

Pf $f(c_i) = f(X)$ mod $X - c_i$.

Using the modulo tree ("Thm 5.5"), we can compute f mod $X - c_1, \ldots, f$ mod $X - c_n$ in $\tilde{O}(n)$. □

Cor 10.1.4 Let $f \in \mathbb{F}_q[X]$ be a pol. of degree n. We can compute $\alpha_k(X) = X^{q^k} \bmod f$ for $k = 1, \dots, n$ in $\tilde{\mathcal{O}}(n^2 + n \log q)$.

Pf First, compute $\alpha_1(X) = X^q$ in $\tilde{\mathcal{O}}(n \log q)$ using fast exponentiation. Afterwards:

Claim: We can compute $\alpha_1, \dots, \alpha_{2^r}$ in $\tilde{\mathcal{O}}(n^2 r)$ for $r \le \lceil \log_2 n \rceil$.

Pf Assume we've computed $\alpha_1, \dots, \alpha_{2^{r-1}}$.

Then, $\alpha_{2^{r-1}+i}(X) = \underbrace{\alpha_{2^r}(\alpha_i(X))}_{\substack{\text{value of the pol. } \alpha_{2^r}(X) \\ \text{at } \alpha_i(X) \text{ in the ring} \\ \mathbb{F}_q[X]/(f).}}^{\bmod f}$ for $i = 1, \dots, 2^{r-1}$.

Arithmetic in $\mathbb{F}_q[X]/(f)$ takes time $\tilde{\mathcal{O}}(n)$.

$\Rightarrow$ Since $2^{r-1} \le n$, by Lemma 10.1.3, we can compute $\alpha_{2^{r-1}+i}$ for $i = 1, \dots, 2^{r-1}$ in $\tilde{\mathcal{O}}(n^2)$ after computing α_j for $j = 1, \dots, 2^{r-1}$ in $\tilde{\mathcal{O}}(n^2(r-1))$. $\square$

$\square$ (Cor)

Cor 10.1.5 Let $f \in \mathbb{F}_q[X]$ of degree n and $g \in \mathbb{F}_q[X]$ of deg. $< n$. We can compute $g(X)^{q^k} \bmod f(X)$ for $k = 1, \dots, n$ in $\tilde{\mathcal{O}}(n^2 + n \log q)$.

Pf $g(X)^{q^k} \equiv g(X^{q^k}) \equiv g(\alpha_k) \bmod f$.
$\Rightarrow$ It suffices to evaluate g at $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q[X]/(f)$. $\square$

Summary We can compute the degree k parts of f for $k = 1, \dots, n$ in $\tilde{\mathcal{O}}(n^2 + n \log q)$.

Rmk ~~This can actually be done in $\tilde{\mathcal{O}}(n^{\frac{3}{2}+\varepsilon}(\log q)^{1+\varepsilon} + n^{1+\varepsilon}(\log q)^{2+\varepsilon})$ **bit** operations (not the more expensive operations in $\mathbb{F}_q$!) (see Kedlaya, Umans: Fast pol. factorization and modular composition)~~

They use a faster modular [illegible]

10.2. Equal-degree factorization

Lemma 10.2.1 Let $f \in \mathbb{F}_q[X]$ be ~~a pol. of degree n = km which~~ the product of m irred. pol. of degree d (so $n = \deg(f) = km$, $f \mid \frac{X^{q^d} - X}{\prod_{e \mid d, e \neq d} (X^{q^e} - X)}$).

Assume we are given the pol. $\alpha_i = (X^{q^i} \bmod f)$ for $i = 0, \dots, d-1$. Then, we can find a random splitting $f = \dots$ into pol. $g, h \in \mathbb{F}_q(X)$ in time $\tilde{O}(n^2 + n \log q)$ where ~~the prob. that deg(g) = ... is~~

$$\mathbb{P}(\deg(g) = kd) = \binom{m}{k} p^k (1-p)^{m-k} \text{ for } l = 0, \dots, m,$$

where $p = \frac{\lceil \frac{1}{2} q \rceil}{q}$.

Pf Let $f = f_1 \cdots f_m$ be the factorisation of f.

$$\underset{CRT}{\Rightarrow} \mathbb{F}_q[X]/(f) \cong \prod_{i=1}^{m} \mathbb{F}_q[X]/(f_i) \cong \prod_{i=1}^{m} \mathbb{F}_{q^d}.$$

Pick $a_0, \dots, a_{n-1} \in \mathbb{F}_q$ uniformly at random.

$\Rightarrow \varphi_a := a_0 + \dots + a_{n-1} X^{n-1} \bmod f$ is a uniformly random element of $\mathbb{F}_q(X)/(f) \cong \prod_{i=1}^{m} \mathbb{F}_{q^d}$.

Consider the trace map Tr sending X to $X + X^q + X^{q^2} + \dots + X^{q^{d-1}}$ (linear [illegible])

$= \alpha_0 + \alpha_1 + \dots + \alpha_{d-1}$.

On $\mathbb{F}_{q^d}$, it's the (field) trace map $\mathrm{Tr}_{\mathbb{F}_{q^d}|\mathbb{F}_q} : \mathbb{F}_{q^d} \to \mathbb{F}_q$.

$\rightsquigarrow$ We get a map $\prod \mathbb{F}_{q^d} \to \prod \mathbb{F}_q$.

linear surjective

Each element of $\prod \mathbb{F}_q$ has the same number of preimages.

$\Rightarrow$ $\mathrm{Tr}(\varphi_a)$ is a uniformly random element of $\prod \mathbb{F}_q$.

$$\mathrm{Tr}(\varphi_a) = \varphi_a(x) + \varphi_a(x)^q + \dots + \varphi_a(x)^{q^{d-1}}$$

can be computed in $\tilde{O}(n^2)$.

Let $v_q(X) = \begin{cases} X^{(q+1)/2} - X \\ \sum X^{2^i} \end{cases}$ as in Lemma 8.3.

Now, $\gcd(f, v_q(\mathrm{Tr}(\varphi_a)))$ is divisible by f_i if and only if the image of $v_q(\mathrm{Tr}(\varphi_a))$ in the i-th factor $\mathbb{F}_q$ is 0.

Since $v_q(x)$ has $\lceil \frac{1}{2} q \rceil$ roots in $\mathbb{F}_q$, this happens with prob. p.

The events for different i are all independent. $\square$

Cor 10.2.2 We can factor any f as in Lemma 10.2.1 in expected time $\tilde{O}(n^2 + n \log q)$.

Pf like Thm 8.4. $\square$

Combining all factorization steps (squarefree, distinct-degree, equal-degr

Thm 10.2.3 (von zur Gathen, Shoup: Computing Frobenius maps and factoring polynomials) ~~Let $f \in \mathbb{F}_q[X]$ be a pol. of degree n~~

We can factor a pol. $f \in \mathbb{F}_q[X]$ of degree n in time $\tilde{O}(n^2 + n \log q)$.

Rmk This is a factor of $\tilde{O}(n + \log q)$ worse than the triv. lower bound $\Theta(n)$.

There are faster algorithms (improving n, but not $\log q$)

Kaltofen-Shoup: Subquadratic-time factoring of polynomials over finite fields
(baby-step/giant step alg.)

Kedlaya-Umans: Fast polynomial factorization and modular composition
(better modular comp. + baby step/giant step)

essentially: $n + \log q \rightsquigarrow n^{1/2} + \log q$

[Don't know how to improve the $\log q$ factor even when just counting linear factors!]

11. Factoring over nonarchimedean local fields

Let K be a nonarch. local field with

normalised valuation v : map $v: K \to \mathbb{Z} \cup \{\infty\}$ s.t. $v(x)=\infty \Leftrightarrow x=0$, $v(xy)=v(x)+v(y)$, $v(x+y) \geq \min(v(x),v(y))$

uniformiser π : el. $\pi \in K$ s.t. $v(\pi)=1$

ring of integers $\mathcal{O} = \{x \in K : v(x) \geq 0\}$

prime ideal $\mathfrak{p} = \{x \in K : v(x) \geq 1\} = (\pi)$

(finite) residue field $k = \mathcal{O}/\mathfrak{p} = \mathbb{F}_q$

~~Let $r_1, \dots, r_q \in K$ be representatives of the~~

Ex $K = \mathbb{Q}_p = \{\frac{x}{y} : x,y \in \mathbb{Z}_p, y \neq 0\}$, $v(x)$ = nr. of times x is divisible by p,
$\pi = p$, $\mathcal{O} = \mathbb{Z}_p$, $\mathfrak{p} = (p)$, $k = \mathbb{F}_p$, $q = p$.

~~Assume we can do arithmetic in $k = \mathbb{F}_q$ in $O(1)$.~~

~~Let $a_1, \dots, a_q \in K$ be representatives~~

~~Let $r_1, \dots, r_q \in K$ be~~

In computations, we won't work with elements of $\mathcal{O}$ (or K), but with mod $\mathfrak{p}^k$-approximations in $\mathcal{O}/\mathfrak{p}^k$.

Assume we can do arithmetic in $\mathcal{O}/\mathfrak{p}^k$ in $O(k)$.

[In part., we can do arithmetic in $k = \mathcal{O}/\mathfrak{p}$ in $O(1)$.]

Ex For $K = \mathbb{Q}_p$, this involves arithmetic on base p integers with $O(k)$ digits.