8. ~~Factoring polynomials~~ Finding roots over finite fields

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

and select an element of $\mathbb{F}_q$ uniformly at random

<u>Thm 8.1</u> We can determine the number of distinct roots of a pol. $f \in \mathbb{F}_q[X]$ of degree n in $\mathbb{F}_q$ in time $\tilde{O}(n \log q)$.

<u>Rmk</u> Realistically we can't do arithmetic in $\mathbb{F}_q$ in $O(1)$, but only in $\tilde{O}(\log q)$, so there would be an additional factor of $\log q$.

<u>Pf</u>
$$\prod_{t \in \mathbb{F}_q} (X-t) = X^q - X$$

$$\Rightarrow \prod_{\substack{t \in \mathbb{F}_q:\\ f(t)=0}} (X-t) = \gcd(f, X^q - X) = \gcd(f, \underbrace{X^q - X \bmod f}_{\substack{\text{compute } X^q \bmod f \\ \text{using fast exponentiation} \\ \tilde{O}(n \log q)}})$$

compute gcd using fast Eucl. alg. $\tilde{O}(n)$

$$\Rightarrow \#\{t \in \mathbb{F}_q : f(t) = 0\} = \deg(\gcd(\dots))$$

$\square$

<u>Joke</u> $f \in \mathbb{Z}[X]$. $\Rightarrow \#\{t \in \mathbb{Z} : f(t) = 0\} = \deg(\gcd(f, g))$,

where $g(X) = \sin(\pi X)$.

__Lemma 8.2__ Let $f \in \mathbb{F}_q[X]$ be a pol. of degree n with n distinct roots in $\mathbb{F}_q$ (i.e. dividing $X^q - X$). We can find a random splitting $f = gh$ into pol. $g, h \in \mathbb{F}_q[X]$ in time $\mathcal{O}(n \log q)$ [on an $\mathcal{O}(n)$-bit RAM], where the probability that $\deg(g) = k$ is given by a binomial distribution:

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

where $p = \dfrac{\lceil \frac{1}{2} q \rceil}{q} \; \left(\approx \frac{1}{2}\right)$.

[So generally $\deg(g) \approx \frac{n}{2}$.]

[We'll use:]

__Lemma 8.3__ The following pol. has $\lceil \frac{1}{2} q \rceil$ (distinct) roots in $\mathbb{F}_q$:

$$u_q(X) = \begin{cases} X^{\frac{q+1}{2}} - X, & q \text{ odd} \\ \sum_{i=0}^{r-1} X^{2^i}, & q = 2^r \end{cases}$$

__Pf__ If q is odd, the roots of $u_q(X)$ are the squares in $\mathbb{F}_q$.

(Also, $\underbrace{u_q(X)}_{\frac{q+1}{2} \text{ roots}} \underbrace{(X^{\frac{q-1}{2}} - 1)}_{\frac{q-1}{2} \text{ roots}} = X(X^{q-1} - 1) = \underbrace{X^q - X}_{q \text{ roots}}$).

If $q = 2^r$, then

$$\underbrace{u_q(X)}_{2^{r-1} = \frac{q}{2} \text{ roots}} \underbrace{(u_q(X) + 1)}_{2^{r-1} = \frac{q}{2} \text{ roots}} = u_q(X)^2 + u_q(X)$$

$$= u_q(X^2) + u_q(X)$$

$x \mapsto x^2$ is a hom. in $\mathbb{F}_q$

$$= X^{2^r} - X = \underbrace{X^q - X}_{q \text{ roots}}$$

$\square$

[We'll use the following special case:]

<u>Lemma 8.3</u> We have $X^q - X = u_q(X)\, v_q(X)$, where

$$u_q(X) = \begin{cases} X^{\frac{q+1}{2}} - X, & q \text{ odd} \\ \sum_{i=0}^{r} X^{2^i}, & q = 2^r \end{cases}$$

$$v_q(X) = \begin{cases} X^{\frac{q-1}{2}} - 1, & q \text{ odd} \\ u_q(X) + 1, & q = 2^r. \end{cases}$$

<u>Rmk</u> $\deg(u_q) = \lceil \frac{q}{2} \rceil$, so u_q has $\lceil \frac{q}{2} \rceil$ distinct roots in $\mathbb{F}_q$
and v_q has $\lfloor \frac{q}{2} \rfloor$ — " — .

<u>Rmk</u> If q is odd, the roots of u_q are exactly the squares in $\mathbb{F}_q$.

Pf of Lemma 8.2 Let $r_1, \dots, r_n \in \mathbb{F}_q$ be the roots of f.

Consider the (linear) Vandermonde map

$$\mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$

$$a = (a_0, \dots, a_{n-1}) \longmapsto \Big(\underbrace{a_0 + a_1 r_i + \dots + a_{n-1} r_i^{n-1}}_{\varphi_a(r_i)}\Big)_{i=1,\dots,n}$$

It is an isomorphism because $r_1, \dots, r_n$ are distinct.

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

$\Rightarrow (s_i)_{i=1,\dots,n} = (\varphi_a(r_i))_{i=1,\dots,n}$ is a uniformly random el. of $\mathbb{F}_q^n$.

Compute

$$g(x) := \gcd\big(f(x), v_q(\varphi_a(x))\big) = \prod_{\substack{1 \le i \le n: \\ v_q(s_i) = 0}} (X - r_i)$$

and $h(x) := \frac{f(x)}{g(x)}$. (Note that we can compute $v_q(\varphi_a(x)) = \begin{cases} \varphi_a(x)^{\cdots} - \varphi_a(x) \\ \sum \varphi_a(x)^{2^i} \end{cases}$ modulo $f(x)$ in $\mathcal{O}(n \log q)$!)

The probability that $\deg(g) = k$ is the probability that

exactly k coordinates s_i of a random elements of $\mathbb{F}_q^n$ are roots of $v_q(x)$, which is $\binom{n}{k} p^k (1-p)^{n-k}$. $\square$

Thm 8.4 We can find all roots of a pol. $f(X) \in \mathbb{F}_q[X]$ of degree n in average time $\tilde{O}(n \log q)$ using randomizati

Rmk It's unknown whether there's a deterministic alg. that does this in polynomial time (in n, $\log q$).

Pf W.l.o.g. $f(X) \mid X^q - X$ (replace f by $\gcd(f, X^q - X)$).

Use Lemma 8.2 to find a splitting $f = gh$ and recursively apply the alg. to g and h.

We have $\mathbb{E}(\deg(g)) = np$ and

$$\mathbb{P}\left((\deg(g) - \mathbb{E}(\deg(g)))^2 \geq \Delta \right) \leq \frac{\mathrm{Var}(\deg(g))}{\Delta} = \frac{np(1-p)}{\Delta},$$

where $p = \frac{\lceil \frac{1}{2} q \rceil}{q} \in [\frac{1}{2}, \frac{2}{3}]$.

$$\Rightarrow \mathbb{P}\left(\deg(g) \in [\tfrac{1}{4}n, \tfrac{3}{4}n] \right) \geq \frac{1}{2}$$

for sufficiently large n.

This shows that the average running time is $\tilde{O}(n \log q)$ (with one more factor of $\log n$ than in Lemma 8.1.2.) $\square$

9. Squarefree factorisation

Let K be a perfect field and assume we can do arithmetic in K in $\mathcal{O}(1)$. (for $K=\mathbb{F}_q$, realistically $\tilde{\mathcal{O}}(\log q)$)

If char $(K)=p>0$, assume we can compute the p-th root of $x\in K$ in $\mathcal{O}(1)$. (for $K=\mathbb{F}_q$ realistically $\mathcal{O}(\log_2 q\cdot \log \frac{q}{p})$ using the formula

$$x^{1/p}=x^{q/p}$$ and fast exponentiation)

Rmk If $p\neq 0$, then $(\sum a_i x^i)^p=\sum a_i^p x^{ip}$, so we can determine whether a pol. $f(x)\in K[x]$ of deg n is a p-th power, and if so determine its p-th root, in $\mathcal{O}(n)$.

Thm 9.1 Let $f(x)\in K[x]$ be a monic pol. of degree n.

We can compute all polynomials

$$s_k(x)=\prod_{\substack{t\in K[x] \text{ monic irred.}\\ \underbrace{v_t(f)}_{\boxed{\text{nr. of times } t(x) \text{ divides } f(x)}}=k}} t(x) \qquad \text{for } k=1,\dots,n$$

(so that $f(x)=\prod_{k=1}^{n} s_k(x)^k$ with squarefree $s_k(x)$)

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

~~INSERT (1)~~ for Lemma 9.2

~~Alg for~~

[All gcds are assumed to be monic!]

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

For $k=1,\dots,\overbrace{n}^{\min(p-1,n)}$, compute

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

Then, $r_k=a_k$ for all $k\leq \min(p-1,n)$.