- For $\mathbb{F}_p$-root finding (for exp. large p), a new idea is needed & randomization.

Cantor & Zassenhaus (CZ) algo.

- Wlog $p>2$ is an odd prime.
- f preprocessed as before.
- Consider $g := f(x-a)$, s.t. two roots of g have different quadratic residuosity. (q.r.)

Lemma: α is a square (or q.r.) in $\mathbb{F}_p^* \iff \alpha^{\frac{p-1}{2}} \equiv_p 1$

Pf: • Let γ generate $(\mathbb{F}_p^*, \cdot)$. Let $\alpha = \gamma^i$.

$(\Rightarrow)$: $\alpha = \beta^2 \Rightarrow \alpha^{p-1/2} = \beta^{p-1} \equiv 1$.

$(\Leftarrow)$: Say, $\alpha^{p-1/2} \equiv 1 \Rightarrow \gamma^{i(p-1)/2} \equiv 1$

$\Leftrightarrow (p-1) = \mathrm{ord}(\gamma) \mid i(p-1)/2$

$\Leftrightarrow 2 \mid i$

$\Leftrightarrow \alpha = (\gamma^{i/2})^2$ is a square. $\square$

- In the literature, $\alpha^{\frac{p-1}{2}} : \mathbb{F}_p \to \{0, \pm 1\}$ is denoted $\left(\frac{\alpha}{p}\right)$, called Legendre symbol.

$\triangleright$ $\Pr_{\alpha \in \mathbb{F}_p^*}[\alpha \text{ is a square}] = \frac{(p-1)/2}{p-1} = 1/2.$

Pf: $\alpha =: \gamma^i$. α is sq. iff i even $\in [0, .., p-2]$. $\square$

- Idea of CZ (1981):

Pick $a \in_R \mathbb{F}_p$. It's expected that the roots of $f(x-a)$ have different quad. residuosity.

GCD $f(x-a)$ with $(x^{\frac{p-1}{2}}-1)$.

→ Say $\alpha+a \in Z(f(x-a))$ & it's a square.

$\Rightarrow$ $\alpha+a$ is a root of $\gcd(\cdot,\cdot)$.

<u>Input</u>: $f \in \mathbb{F}_p[x]$ of deg-d; preprocessed.

<u>Output</u>: nontrivial factor of f.

<u>Algo</u>:
0) Pick $a \in_R \mathbb{F}_p$.
1) OUTPUT $h(x) := \gcd(f(x), (x+a)^{\frac{p-1}{2}} - 1)$.

<u>Analysis:</u> • Let $\alpha_1 \neq \alpha_2 \in Z_{\mathbb{F}_p}(f(x))$ ↙ $\mathbb{F}_p$- zeros of f.

$\Rightarrow \alpha_1 + a \neq \alpha_2 + a \in Z(f(x-a))$.

– They've same residuosity iff

$$(\alpha_1 + a)^{(p-1)/2} \equiv (\alpha_2 + a)^{(p-1)/2} \quad \text{------} (1)$$

→ It is an eqn. in 'a' of deg $= (p-3)/2$.

$\Rightarrow$ # bad a's $\leq (p-3)/2$

$\Rightarrow$ # a's for which (1) fails $\geq (p+3)/2$.

$\Rightarrow \Pr_{a \in \mathbb{F}_p} [\, h(x) \text{ is nontrivial} \,] > 1/2$.

• Time $\leq (\lg p) \cdot \tilde{O}(d \lg p) + \tilde{O}(d \lg p) \leq \tilde{O}(d \cdot \lg^2 p)$. □

→ Overall, factoring over $\mathbb{F}_q$ takes $\tilde{O}(d^{\omega} \cdot \lg^2 q)$.

– (Kedlaya & Umans, 2011) gave a subquadratic randomized factoring algo., in time $\tilde{O}(d^{1.5} \lg q + d \cdot \lg^2 q)$.

OPEN: 1) Deterministic poly-time (e.g. $\sqrt{a} \bmod p$)?

2) Randomized $\tilde{O}(d \cdot \lg^2 q)$-time ?