- For completely splitting polynomials over $\mathbb{F}_p$, a new idea is needed — randomization.

Cantor-Zassenhaus' randomized algo. (CZ)

- Wlog, assume $p>2$.

- The plan is to shift $f(x)$, eg. consider $g(x) := f(x-a)$, such that the roots now have different quadratic residuosity.

Lemma: α is a square in $\mathbb{F}_p^*$ iff $\alpha^{\frac{p-1}{2}} = 1$.

Pf:

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

$\Leftarrow$:
Say, $\alpha^{(p-1)/2} = 1$ & g is a generator of $\mathbb{F}_p^*$. Let $\alpha = g^i$.

$\Rightarrow \quad g^{i(p-1)/2} = 1$

$\Rightarrow \quad (p-1) \mid i(p-1)/2$

$\Rightarrow \quad 2 \mid i$

$\Rightarrow \quad \alpha = g^i$ is a square. $\square$

- In the literature $\alpha^{\frac{p-1}{2}}$ is also denoted as $\left(\frac{\alpha}{p}\right)$, called the <u>Legendre symbol</u>.

  It indicates the <u>residuosity</u> of $\alpha \pmod p$.

▷ $\Pr_{\alpha \in \mathbb{F}_p}[\alpha$ is a square$] < 1/2$.

<u>Pf</u>: • If g generates $\mathbb{F}_p^*$, then the set $\{g, g^2, \ldots, g^{p-1}\}$ has half <u>quadratic residues</u>.

• Note that $g^{\frac{p-1}{2}} \equiv -1$, $(g^3)^{\frac{p-1}{2}} \equiv -1$, and so on. (So, $g, g^3, \ldots$ are non-residues) $\square$

- Idea of CZ algo. (1981):
Pick a random $a \in \mathbb{F}_p$. It is expected that the roots of $f(x-a)$ have <u>different</u> quad. residuosity.
So gcd with $(x^{\frac{p-1}{2}} - 1)$ should factor $f(x-a)$.

<u>Input</u>: $f \in \mathbb{F}_p[x]$ with coprime linear factors, $d := \deg f$.
<u>Output</u>: nontrivial factor of f.
<u>Algo</u>:
(1) Pick a <u>random</u> $a \in \mathbb{F}_p$.
(2) Output
$h(x) := \gcd(f, (x+a)^{\frac{p-1}{2}} - 1)$.

<u>Correctness</u>: • Let $S := \{\alpha_1, \dots, \alpha_d\} \subseteq \mathbb{F}_p$ be the roots of $f(x)$.
• The roots of $f(x-a)$ are $S+a := \{\alpha_i + a \mid i \in [d]\}$.

- $h(x) = 1 \iff S+a$ are all quad. nonresidues

$\iff (\alpha_1+a)^{p-1/2} = \cdots = (\alpha_d+a)^{p-1/2} = -1.$

- The number of a's that could satisfy

$$(\alpha_1+a)^{\frac{p-1}{2}} = (\alpha_2+a)^{\frac{p-1}{2}}$$

is at most $\left(\frac{p-1}{2} - 1\right)$.

- $h(x) = f(x) \iff S+a$ are all quad. residues.

$\iff (\alpha_1+a)^{p-1/2} = \dots = (\alpha_d+a)^{p-1/2} = 1$.

- Thus, the # a's in any of the above two cases is $\leq \frac{p-3}{2}$.

$$\Rightarrow \Pr_{a \in \mathbb{F}_p} [\, h(x) = 1 \text{ or } f \,] \leq \frac{(p-3)/2}{p} < \frac{1}{2}.$$

- Thus, the algo. factors $f(x)$ with probability $> 1/2$ (in one iteration).
- Time taken $= \lg p \cdot \tilde{O}(d \lg p) + \tilde{O}(d \cdot \lg p)$.

$\square$

- CZ is the factoring algo. of choice in many computer algebra systems.
- Theoretically, the above is quadratic-time & factoring overall takes time $> n^{\omega}$ (where ω is the matrix mult. exponent).
- (Kedlaya & Umans, 2011) gave a sub-quadratic randomized factoring algo. In time $\tilde{O}(d^{1.5} \cdot \lg q + d \cdot \lg^2 q)$.