The Berlekamp-Hensel Procedure
(Hans Zassenhaus ~ 1972)

<u>Input</u> $A \in \mathbb{Z}[x]$ s.t.

$d > 1$

$A = a_d x^d + \cdots + a_0$

$\operatorname{cont}(A) = 1$

$\gcd(A, A') = 1$

<u>Output</u> $f_1, f_2, \ldots, f_m \in \mathbb{Z}[x]$ s.t.

f_i irreducible over $\mathbb{Q}$

$A = f_1 f_2 \cdot \cdots \cdot f_m$

ϕ_p

① Pick p s.t.

$p \nmid \operatorname{lc} A = a_d$

$\gcd(A, A') = 1$ in $\mathbb{Z}_p[x]$

$A \in \mathbb{Z}_p[x]$

② Factor $A \in \mathbb{Z}_p[x]$

Cantor-Zassenhaus

$O(d^3 \log^3 p)$

$A \equiv a_d \cdot g_1 g_2 \cdots g_l, \quad l \geq m$

$g_i \in \mathbb{Z}_p[x]$, monic, irreducible

③ For $j = 1, 2, \ldots, l$ Hensel lift g_j using $u_0 = g_j$, $w_0 = a_d \cdot \prod_{i \neq j} g_i$ until $p^n > 2 a_d \cdot \|f_i\|_\infty$ to obtain

$A \equiv a_d\, g_1^{(n)} \cdot g_2^{(n)} \cdots g_l^{(n)} \pmod{p^n}$

④ Test if $pp(a_d \cdot g_i^{(n)} \bmod p^n) \mid A \;\; \forall i$

Test if $pp(\underbrace{a_d \cdot g_i^{(n)} \cdot g_j^{(n)}}_{\text{expand}} \bmod p^n) \mid A \;\; \forall i \neq j$

⋮ etc.