Algorithm Distinct Degree Factorization 8.8

Input: $a \in \mathbb{Z}_p[x]$, $d = \deg a > 0$, $\gcd(a, a') = 1$.

Output: $g_1, g_2, \ldots, g_m$ s.t $a = \prod g_k$ and g_k is a $\prod$ of irreducibles of degree k.

$k \leftarrow 1$
$w \leftarrow x$
while $k \leq \lfloor \deg a / 2 \rfloor$ do

$w \leftarrow \text{rem}(w^p, a)$ $\quad = x^{p^k} \bmod a$
$g_k \leftarrow \gcd(w - x, a)$

$a \leftarrow a / g_k$
$k \leftarrow k + 1$

od
if $a \neq 1$ then $g_k \leftarrow a$ else $k \leftarrow k - 1$
return $g_1, g_2, \ldots, g_k$