Algorithm Univariate Hensel Lifting 6.5

Input $a \in \mathbb{Z}[x]$, p an odd prime s.t. $p \nmid lc(a)$
$u_0, w_0 \in \mathbb{Z}_p[x]$ s.t. $a - u_0 w_0 \equiv 0 \bmod p$
and $\gcd(u_0, w_0) = 1$ in $\mathbb{Z}_p[x]$.
$B > \|f\|_\infty$, $f | a$.

Output Either $u, w \in \mathbb{Z}[x]$ s.t. $a - u \cdot w = 0$
OR FAIL $\Rightarrow \nexists u, w \in \mathbb{Z}[x]$ s.t. $a - uw = 0$
with $u \equiv u_0 \bmod p$, $w \equiv w_0 \bmod p$

Solve $s w_0 + t u_0 = 1$ for $s, t \in \mathbb{Z}_p[x]$: $\deg(s) < \deg(u_0)$.
$u^{(1)} \leftarrow u_0$, $w^{(1)} \leftarrow w_0$, $k \leftarrow 1$
do
$e_k \leftarrow a - u^{(k)} \cdot w^{(k)} \in \mathbb{Z}[x]$
if $e_k = 0$ then output $u^{(k)}, w^{(k)}$
if $p^k > 2B$ then output FAIL
$c_k \leftarrow (e_k / p^k) \bmod p$
Solve $u_k w_0 + w_k u_0 = c_k$ for $u_k, w_k \in \mathbb{Z}_p[x]$
$(r, q) \leftarrow \text{rem}(c_k \cdot s, u_0), \text{quo}(c_k \cdot s, u_0)$
$u_k, w_k \leftarrow r, w_0 q + c_k t$
$u^{(k+1)} \leftarrow u^{(k)} + u_k p^k$
$w^{(k+1)} \leftarrow w^{(k)} + w_k p^k$
$k \leftarrow k + 1$