Algorithm Linear P-adic Lifting

Inputs: p an odd prime (to recover -ve coeffs)
$f(u) \in \mathbb{Z}[x][u]$, $u_0 \in \mathbb{Z}_p[x]$ s.t. $f(u_0)=0 \wedge f'(u_0) \neq 0$
$B \in \mathbb{Z}$ s.t. $\|\tilde{u}\|_\infty < B$, a lifting bound

Output $\tilde{u} \in \mathbb{Z}[x]$ s.t. $f(\tilde{u}) = 0$ or FAIL meaning there is no such $\tilde{u}$ with $\tilde{u} \equiv u_0 \bmod p$.

$(\sqrt{\ })$

$\tilde{u} \leftarrow u_0$

$d \leftarrow f'(u_0) \bmod p$ $\quad (d = -2u_0)$

for $k = 1, 2, 3, \ldots$

$e_k \leftarrow f(\tilde{u})$ $\quad (a - \tilde{u}^2)$

if $e_k = 0$ output $\tilde{u}$

if $p^k > 2B$ output FAIL

$t \leftarrow -\frac{e_k}{p^k} \bmod p \in \mathbb{Z}_p[x]$

if $d \nmid t$ in $\mathbb{Z}_p[x]$ output FAIL

$u_k \leftarrow t/d$

$\tilde{u} \leftarrow \tilde{u} + u_k p^k$

Remark $a - \tilde{u}^2$ is expensive.