Algorithm Mod Gcd.

Inputs $\quad a, b \in \mathbb{Z}[x] \setminus \{0\}$, cont $a = 1$, cont $b = 1$.
Output $\quad g = \gcd(a, b)$

$$\gamma \leftarrow \gcd(\operatorname{lc} a, \operatorname{lc} b) \in \mathbb{Z}$$
$$G \leftarrow 0 \qquad \# \quad \text{CRT applied to previous images } g_i$$
$$M \leftarrow 1 \qquad \# \quad \text{product of previous primes}$$

Loop: pick a new prime p st. $p \nmid \operatorname{lc} a$.
$\qquad g_p \leftarrow \gcd(\phi_p(a), \phi_p(b)) \in \mathbb{Z}_p[x]$
$\qquad$ if $\deg g_p = 0$ then output 1.
$\qquad g_p \leftarrow \phi_p(\gamma) \cdot g_p \bmod p$

$\qquad$ if $G = 0$ then $G \leftarrow g_p$; $M \leftarrow p$;
$\quad$ elif $\deg g_p > \deg G$ then $\qquad \# \, p$ is unlucky
$\quad$ elif $\deg g_p < \deg G$ then $\qquad \#$ all previous primes
$\qquad\quad G \leftarrow g_p$; $M \leftarrow p$; $\qquad \#$ are unlucky
$\quad$ else
$\qquad\quad$ Solve $\{u \equiv G \bmod M, \ u \equiv g_p \bmod p\}$
$\qquad\quad$ for u in the symmetric range mod $M \cdot p$.
$\qquad\quad$ if $u = G$ then
$\qquad\qquad g \leftarrow u / \operatorname{cont}(u)$
$\qquad\qquad$ if $g | a$ and $g | b$ then output g.
$\qquad\quad G \leftarrow u$; $M \leftarrow M \cdot p$
$\quad$ end if
$\quad$ go to LOOP.