The Modular Gcd Algorithm

$$\begin{tikzcd}
\text{Input} & \text{Output} \\
\begin{array}{c} a,b \in \mathbb{Z}[x] \\ \text{(assume primitive)} \end{array} \arrow[r] \arrow[d, "\phi_{p_i}"', "M=\prod p_i > 2\|g\|_\infty"] & g = \gcd(a,b) \in \mathbb{Z}[x] \\
a_i,b_i \in \mathbb{Z}_{p_i}[x] \arrow[r, "\text{Euclidean Algorithm}", "O(n^2)\text{ operations in }\mathbb{Z}_{p_i}"'] & g_i = \gcd(a_i,b_i) \in \mathbb{Z}_{p_i}[x] \arrow[u, "\text{CRT}", "\begin{array}{l}\text{Solve } \bar{g} \equiv g_i \ (\text{mod } p_i) \text{ for} \\ g \in \mathbb{Z}_M[x].\end{array}"']
\end{tikzcd}$$