Lec11C Algorithm ModGCD, Michael Monagan

February 23, 2021 11:24 AM

The Leading coefficient problem

$a = 8x^2 - x - 1 = (2x-1)(4x+1)$

$b = 4x^2 - 1 = (2x-1)(2x+1)$

$g = 2x - 1$. $\tilde{g} = 1 \cdot x - \frac{1}{2}$ monic associate over $\mathbb{Q}$

$p_1 = 5$ $g_1 = 1 \cdot x + 2 \xrightarrow{\times 2} 2x + 4$

$p_2 = 7$ $g_2 = 1 \cdot x + 3 \xrightarrow{\times 2} 2x + 6$

$1 \cdot x + 17$ $2 \cdot x + 34$

symmetric range $\equiv 2x - 1 \pmod{35}$

CRT

$M = 5 \cdot 7 = 35$

We don't know g so we don't have $lc(g) = 2$.

But $lc(g) \mid lc(a)$ and $lc(g) \mid lc(b) \Rightarrow lc(g) \mid \gamma = \gcd(lc(a), lc(b)) = 4$.

$p_1 = 5$ $g_1 = 1 \cdot x + 2 \xrightarrow{\times 4} 4x + 3$

$p_2 = 7$ $g_2 = 1 \cdot x + 3 \xrightarrow{\times 4} 4x + 5$

$4 \cdot x + 33$ symmetric range mod $M = 35$ $\equiv 4x - 2 \xrightarrow{pp} 2x - 1$.

a and b are primitive $\Rightarrow g$ is primitive.