Lecture 12C Multivariate GCDs Michael Monagan

February 25, 2021 1:58 PM

The modular gcd algorithm in $\mathbb{Z}[x]$ uses $\phi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ and the CRT. What about gcds in $\mathbb{Z}[x,y,z,\ldots]$ and $\mathbb{F}_q[x,y,z,\ldots]$??

Eg. $\gcd(x^4 - t^4, x^6 - t^6)$ in $\mathbb{Z}[t][x] = 1 \cdot x^2 - t^2$.

$(x^2-t^2)(x^2+t^2)$, $(x^2-t^2)(x^4+t^2x^2+t^4)$

unlucky eval. point.

$\phi_{t=0}$ $\gcd(x^4, x^6) = x^4$

$\phi_{t=1}$ $\gcd(x^4-1, x^6-1) = 1 \cdot x^2 - 1$.

$\phi_{t=2}$ $\gcd(x^4-2^4, x^6-2^6) = 1 \cdot x^2 - 4$

$\phi_{t=3}$ $\gcd(x^4-81, x^6-3^6) = 1 \cdot x^2 - 9$

$\phi_{t=4}$ $\gcd(x^4-256, x^6-4^6) = 1 \cdot x^2 - 16$

Interpolate.

$\gcd(x^4+t^4, x^6+t^6)$ in $\mathbb{Z}_2[t][x] = x^2+t^2$

$\phi_{t=0}$ $\gcd(x^4, x^6) = x^4$ $t=0$ is unlucky.

$\phi_{t=1}$ $\gcd(x^4+1, x^6+1) = x^2+1$. ✓

We have only 2 evaluation points in $\mathbb{Z}_2$.
Where can we get more evaluation points from?