Modular GCD Algorithm's for Z[x1,x2,...,xn]

October 6, 2021 9:41 PM

Collins (1969) $\mathbb{Z}[x]$

Brown (1971) $\mathbb{Z}[x_1, x_2, \ldots, x_n]$

Zippel (1979) $\mathbb{Z}[x_1, x_2, \ldots, x_n]$

⋮

Hu & Monagan (2016) $\mathbb{Z}[x_1, \ldots, x_n]$

The modular gcd algorithm for $\mathbb{Z}[x]$

Let $a, b \in \mathbb{Z}[x]$, $g = \gcd(a,b)$, $\bar{a} = \frac{a}{g}$, $\bar{b} = \frac{b}{g}$.

$$a, b \in \mathbb{Z}[x] \xrightarrow{\text{Prim Euc. Alg.}} g \in \mathbb{Z}[x]$$

$C_a \leftarrow \gcd(a_0, \ldots, a_d)$ $\quad a = a_0 + \cdots + a_d x^d$

$C_b \leftarrow \gcd(b_0, \ldots, b_d)$ $\quad b = b_0 + \cdots + b_d x^d$

$C_g \leftarrow \gcd(C_a, C_b)$

$a \leftarrow a / C_a = pp(a)$

$b \leftarrow b / C_b = pp(b)$

ϕ_{p_i}, $p_i \nmid LC(a)$

if $pp(h) \mid a$ and $pp(h) \mid b$ then output $pp(h) \cdot C_g$

CRT: solve $\{ h \equiv g_i \pmod{p_i} \}$ for $h \in \mathbb{Z}_M[x]$, $M = \prod p_i$

[use g_i of least degree]

$$a_i, b_i \in \mathbb{Z}_{p_i}[x] \xrightarrow[O(d^2)]{\text{E.A.}} \text{monic } g_i = \gcd(a_i, b_i) \in \mathbb{Z}_{p_i}[x]$$

$\rightarrow \gamma \leftarrow \gcd(LC(a), LC(b))$

$g_i \leftarrow \gamma g_i \bmod p$.

Unlucky primes

$a = \overset{g}{(13x - 11)}\overset{\bar{a}}{(5x+18)}$

$b = (13x - 11)\underset{\bar{b}}{(5x+1)}$

$g = 13x - 11$.

p_i	$g_i = \gcd(a,b) \bmod p_i$	$\deg(g_i)$
× 17	$(13x+6)(5x+1)/(13 \cdot 5)$	2
× 13	$+2 \cdot 1/2$	0
2	$(x+1) \cdot 1$ ✓	1
5	$(3x+4) \cdot 1/3$ ✓	1

A prime p is unlucky if $\deg(\gcd(\phi_p(\bar{a}), \phi_p(\bar{b}))) > 0$. [$p = 17$]

Theorem. p is unlucky $\Rightarrow p \mid \operatorname{res}(\bar{a}, \bar{b}, x) \in \mathbb{Z}$.

$\Rightarrow$ a finite # of unlucky primes.

Lemma 7.3. [GLC] Let $a, b \in \mathbb{Z}[x]$, $a \neq 0$, $b \neq 0$, $g = \gcd(a,b)$.
Let p_i be a prime, $g_i = \gcd(\phi_{p_i}(a), \phi_{p_i}(b)) \in \mathbb{Z}_{p_i}[x]$.
If $p_i \nmid LC(a)$. [exclude $p = 13, 5$] Then

(i) $\deg(g_i) \geq \deg(g)$.

(ii) $\phi_{p_i}(g) \mid g_i$

$\Rightarrow$ if $\deg(g_i) = \deg(g)$ Then $g_i = s \cdot \phi_{p_i}(g)$ for $s \in \mathbb{Z}_p$.
equivalently $g_i \sim \phi_{p_i}(g)$

Collin's idea: Pick p_i s.t. $p_i \nmid LC(a)$ to avoid $p = 13, 5$.
Compute $g_1, g_2, \ldots$ and keep the ones of least degree.

The leading coefficient problem

How do we recover $g = \boxed{13}x - 11$ from monic images $g_i = 1 \cdot x - \frac{11}{13} \bmod p_i$?
Multiply g_i by $\gamma = \gcd(LC(a), LC(b)) = \underline{13} \cdot 5$
Then the CRT recovers $h = 5 \cdot (13x - 11) = 65x - 55 \bmod \prod p_i$
Compute $pp(h) = h/5 = 13x - 11$.
Return $pp(h) \cdot \gcd(\underline{cont(a), cont(b)})$.

When to stop? Stop when h does not change and
$pp(h) \mid a$ and $pp(h) \mid b$.