Browns GCD algorithm for Z[x1,x2,...,xn]

October 6, 2021 9:51 PM

$$
\begin{tikzcd}
a,b \in \mathbb{Z}[x,y,z] \arrow[rr, "\text{Prim. E.A.}"] \arrow[d, "\phi_{p_i}"'] & \text{MGCD} & g = \gcd(a,b) \\
a_i,b_i \in \mathbb{Z}_{p_i}[z][x,y] \arrow[rr, "?\ \text{PGCD}"] \arrow[d, "\phi_{z=\alpha_{ij}} \in \mathbb{Z}_{p_i}"'] & & g_i = \gcd(a_i,b_i) \arrow[u, "\text{CRT: Solve } h \equiv g_i \bmod p_i"'] \\
a_{ij},b_{ij} \in \mathbb{Z}_{p_i}[y][x] \arrow[rr, "\text{PGCD}"] \arrow[d, "\phi_{y=\alpha_{ijk}} \in \mathbb{Z}_{p_i}"'] & & g_{ij} = \gcd(a_{ij},b_{ij}) \arrow[u, "\text{Interpolate } z."'] \\
a_{ijk},b_{ijk} \in \mathbb{Z}_{p_i}[x] \arrow[rr, "\text{Euc. Alg.}"] & & g_{ijk} = \gcd(a_{ijk},b_{ijk}) \arrow[u, "\text{Interpolate } y."']
\end{tikzcd}
$$

icontent(a)
$C_a \leftarrow cont(a) \in \mathbb{Z}$
$C_b \leftarrow cont(b) \in \mathbb{Z}$
$C_g \leftarrow \gcd(C_a, C_b)$
$a \leftarrow a/C_a$
$b \leftarrow b/C_b$.

? $p_i \nmid LC(a)$.

$g = pp(h) \cdot C_g$.

monic?

$\gamma \leftarrow \gcd(\underline{LC(a)}, \underline{LC(b)}) \in \mathbb{Z}$.
$g_i \leftarrow \gamma g_i \bmod p_i$.

Unlucky primes in MGCD.

$$a = (13x^2+3y^3)(yx^2+\overset{\bar{a}}{7}x+y)$$
$$b = (13x^2+3y^3)(yx^2+\overset{\bar{b}}{7}x+12y)$$
$$g = \underline{13}x^2+\underline{3}y^3$$

Fix a monomial ordering.
Use $>_{lex}$ with $x>y$.
This defines
$LC(g)=13 \quad LM(g)=x^2$.

	p_i	g_i	$\deg(g_i,x)$	$\deg(g_i)$	$LM(g_i)$
✓	$p_i=5$	$g_i \sim (3x^2+3y^3)\cdot 1$	2	3	x^2
X	$p_i=7$	$g_i \sim (6x^2+3y^3)\cdot y$	2	4	x^2
X	$p_i=11$	$g_i \sim (2x^2+3y^3)(yx^2+7x+y)$	4	6	x^4y.
~~X~~	~~$p_i=13$~~	~~$g_i \sim 3y^3\cdot 1$~~	~~0~~	~~3~~	~~y^3~~

✗	~~$p_i = 13$~~	~~$g_i \sim 3y^3 \cdot 1$~~	~~0~~	~~3~~	~~y^3~~
✓	$p_i = 3$	$g_i \sim 1 \cdot x^2 \cdot 1$	2	2	x^2

Avoid $p_i \mid LC(a) \rightarrow$ avoid $p = 13$ (bad prime).

✗ Keep g_i of smallest degree in x ($p_i = 7$).

✗ Keep g_i of smallest total degree (infinite loop).

✓ Keep g_i with smallest $LM(g_i)$ in $>_{lex}$.

Lemma 7.3′ Let $a, b \in \mathbb{Z}[x_1, \ldots, x_n]$. Assume lex with $x_1 > x_2 > \cdots > x_n$. Let p_i be a prime.
Let $g_i = \gcd(\phi_{p_i}(a), \phi_{p_i}(b))$.
If $p_i \nmid LC(a)$ then
(i) $LM(g_i) \geq_{lex} LM(g)$.
(ii) if $LM(g_i) = LM(g)$ then $g_i \sim \phi_{p_i}(g)$.

Proof (exercise). Assume $LC(ab) = LC(a) LC(b)$
$LM(a \cdot b) = LM(a) \cdot LM(b)$.

Maple. `lc := lcoeff( a, [x,y,z], 'lm' );`
lex with $x > y > z$

Unlucky evaluation points in PGCD

$$\left.\begin{aligned}
a &= ((z-13)x^2 + (z-3)y^3)(yx^2 + (\overset{\bar{a}}{z}-7)x + y) \\
b &= ((z-13)x^2 + (z-3)y^3)(yx^2 + (\underset{\bar{b}}{z}-7)x + (z-10)y) \\
g &= ((z-13)x^2 + (z-3)y^3)
\end{aligned}\right\} \in \mathbb{Z}_p[z][x,y]$$

$p = 17 \mid z = 5$	$g_{i1} \sim (-8x^2 + 2y^3) \cdot 1 \sim g(x,y,5)$ ✓		$LM(g_{ij})$
			x^2

$LM(g_{ij})$

$p=17$

| $z=5$ $\quad g_{ij} \sim (-8x^2+2y^3)\cdot 1 \sim g(x,y,5)$ ✓ $\qquad x^2$

| $z=11$ $\quad g_{ij} \sim (-2x^2+8y^3)\cdot(yx^2+4x+y)$ × $\qquad x^4y$

| $z=7$ $\quad g_{ij} \sim (-6x^2+4y^3)\cdot y$ × ← unlucky eval. pts $\qquad x^2y$

~~| $z=13$ $\quad g_{ij} \sim 10y^3\cdot 1$ × ← bad eval. pt.~~ $\qquad y^3$

| $z=3$ $\quad g_{ij} \sim (-10x^2+0)\cdot 1$ ✓ $\qquad x^2$

$LC(a) = z-13.$ $\qquad$ Avoid evaluation points $z=\alpha$ s.t. $LC(a)(\alpha)=0$.

lex $x>y$

Keep g_{ij} with least $LM(g_{ij})$.

Maple. $\quad$ lc := lcoeff(a, [x,y], 'lm'); $\to z-13$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \downarrow$ x^4y.

What about the leading coefficient problem in PGCD?

$\mathbb{Z}_p[z][x,y]$ $\quad a = \underbrace{(z^3-1)}_{C_a}\overbrace{(zx+y)(zx}(+y^2+1) = (z^5-z^2)x^2+\cdots+(z^3-1)\cdot 1$

$b = \underbrace{(z^4-1)}_{C_b}(zx+y)(zx+y+12).$

$g = \underbrace{(z-1)}_{C_g}$

Maple

coeffs(a,[x,y]) $\to$ $z^5-z^2, \ldots, z^3-1$.

$$a = \sum_{ij} C_{ij}(z)\cdot x^i y^j$$

Define $\quad \text{cont}_{xy}(a) = \gcd(C_{ij}(z)) \in \mathbb{Z}_p[z]$

$C_g \leftarrow \gcd(\text{cont}_{xy}(a), \text{cont}_{xy}(b)) = z-1.$

Content(a, [x,y]) mod p ;

Define … $= (zx+y)(zx+y^2+1)$

Content(a, [x,y]) mod p ;

Define $pp_{xy}(a) = a/cont_{xy}(a). = (zx+y)(zx+y^2+1).$

Primpart(a, [x,y]) mod p ;

$a \leftarrow pp(a) = (zx+y)(zx+y^2+1)$ $\longrightarrow$ $1 \cdot x + \bullet y$

$b \leftarrow pp(b) = (zx+y)(zx+y+12).$

Let $\gamma(z) =$ Gcd(lcoeff(a, [x,y]), lcoeff(b, [x,y])) mod p

$g_{ij} \leftarrow \gamma(\alpha_{ij}) \cdot g_{ij}$

$LC(g_{ij}) = 1.$

We interpolate $h = z(zx+y) = z^2 \cdot x + zy$ using 3 α_{ij} (points for Z)

Test if $pp(h) = (zx+y) \mid a$ and $pp(h) \mid b.$ in $\mathbb{Z}_p[x,y,z]$

Maple ~~if~~ Divide(a, pp(h)) mod p
and Divide(b, pp(h)) mod p ;

Alternative stopping criterion.

In MGCD we could bound $\|g\|_\infty$ and require $M = \prod p_i > 2 \cdot \gamma \cdot \|g\|_\infty.$

Lemma [Gelfond 1952] Let $a, g \in \mathbb{Z}[x_1, x_2, \ldots, x_n].$
Let $d_i = \deg(a, x_i) \geq 0.$ Then
if $g \mid a$ then $\|g\|_\infty \leq e^{d_1+d_2+\cdots+d_n} \cdot \|a\|_\infty.$

Lemma (n=1) [Mignotte 1974] Let $d = \deg(a).$
if $g \mid a$ then $\|g\|_\infty \leq 2^d \sqrt{d+1}\, \|a\|_\infty$

Gelfand $(n=1)$ $\|g\|_\infty \le e^{d} \cdot \|a\|_\infty$.