Lec7A Pseudo Division

January 30, 2021 10:47 PM

How can we compute $g := \gcd(a,b)$ where $a,b \in \mathbb{Z}[x_1, x_2, \dots, x_n]$?

not a Euc. Alg.

$$\frac{a}{b} = \frac{a/g}{b/g} = \frac{x-y+1}{x+y+1}.$$

Content & Primitive Part

content primitive part

In $\mathbb{Z}[x]$ $\quad a = 4x^2+12x+8 = 4\cdot(1x^2+3x+2)$

$\quad b = 12x^2+6x+6 = 6\cdot(2x^2+x+1)$

$$\gcd(a,b) = \gcd(4,6)\cdot\gcd(x^2+3x+2, 2x^2+x+1).$$

$\gcd(4,6)$: $\mathbb{Z}$ (Euclid). ??

In $\mathbb{Z}[x,y]$ $\quad a = 6x^2y - 6y^3,\ b = 9x^2y + 18xy^2 + 9y^3$

In $\mathbb{Z}[y][x]$ $\quad a = (6y)x^2 + (-6y^3) = 6y\cdot(x^2-y^2)$

$\quad b = (9y)x^2 + (18y^2)x + (9y^3) = 9y(x^2+2y\,x+y^2)$

content primitive part.

$$\gcd(a,b) = \gcd(6y,9y)\cdot\gcd(x^2-y^2, x^2+2yx+y^2).$$

$\gcd(6y,9y) = 3y$??

is a gcd in one less variable — recursively.

Let R be a UFD (gcd's exist) $a \in R[x]$ where

$a = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$ with $a_n \neq 0$.

Def The content of a is $\text{cont}(a) = \gcd(a_n, a_{n-1}, \dots, a_0)$

$= \gcd(a_n, \gcd(a_{n-1}, \gcd(\dots, a_0)))$

Def a is primitive if $\text{cont}(a)$ is a unit in R.

Def The primitive part of a is $pp(a) = a/\text{cont}(a)$.

Thus $a = \text{cont}(a)\cdot pp(a)$.

Observe $\gcd(a,b) = \gcd(\text{cont}(a)\cdot pp(a), \text{cont}(b)\cdot pp(a))$

$= \gcd(\text{cont}(a), \text{cont}(b))\cdot\gcd(pp(a), pp(b))$.

Suppose $g \mid 3x^4 + 5x^3 + 15x^1$ in $\mathbb{Z}[x]$ $\Rightarrow$ $\text{cont}(g) = $ a unit.

Lemma If $\text{cont}(a) = 1$ (a is primitive) and $g \mid a$ then $\text{cont}(g) = 1$ (g is primitive).

TAC Suppose $\text{cont}(g) = c$ (c is not a unit) $\Rightarrow g = c\cdot\bar{g}$ and $g \mid a \Rightarrow c \mid a$

$\Rightarrow \text{cont}(a) = c\cdot\square$ $\boxed{X}$

Maple.
```
content(a,x);     c:= content(a,x,'pp');
primpart(a,x);    pp:= primpart(a,x,'c');
```

Maple. content(a, x); primpart(a, x);

c := content(a, x, 'pp'); pp := primpart(a, x, 'c');

Pseudo division in $D[x]$. — $\mathbb{Z}[x]$, $\mathbb{Z}[y][x]$, $\mathbb{Q}[y][x]$.

Let D be an integral domain, $a, b \in D[x]$, $b \neq 0$.

In general the quotient and remainder of $a \div b$ are not in $D[x]$.

E.g. $\mathbb{Z}[x]$.

$$b = 5x^2 - 3x + 1 \overline{\big)\, 3x^3 + x^2 + x + 5} = a$$

$$q = \frac{3}{5}x + \frac{14}{25}$$

$$-\left[3x^3 - \frac{9}{5}x^2 + \frac{3}{5}x\right]$$

$$0 + \frac{14}{5}x^2 + \frac{2}{5}x + 5$$

$$\left[\frac{14}{5}x^2 - \frac{42}{25}x + \frac{14}{25}\right]$$

$$r = \frac{52}{25}x + \frac{111}{25}$$

So $a = bq + r$

$\Rightarrow 25a = b(25q) + 25r$

$25a = b(\underbrace{15x + 14}_{\tilde{q}}) + \underbrace{52x + 111}_{\tilde{r}}$.

Consider $25a \div b$.

$$5x^2 - 3x + 1 \overline{\big)\, 75x^3 + 25x^2 + 25x + 125}$$

$$15x + 14 \leftarrow \tilde{q}$$

$$-(75x^3 - 45x^2 + 15x)$$

$$0 + 70x^2 + 10x + 125$$

$$-(70x^2 - 42x + 14)$$

$$0 + 52x + 111 \leftarrow \tilde{r}$$

NO FRACTIONS!

Theorem. Let $a = a_\ell x^\ell + \cdots + a_0$ and $b = b_n x^n + \cdots + b_0$ with $a_\ell \neq 0$, $b_n \neq 0$, with $\ell \geq n \geq 0$. Then $\exists$ a unique pseudo-quotient $\tilde{q}$ and pseudo-remainder $\tilde{r}$ in $D[x]$

s.t. $ma = b \cdot \tilde{q} + \tilde{r}$ where $\tilde{r} = 0$ or $\deg \tilde{r} < \deg b$ and $m = \mathrm{lc}(b)^{\ell - n + 1}$

max # of division step.

Proof (uniqueness). Suppose

(1) $ma = b\tilde{q}_1 + \tilde{r}_1$ where $\tilde{r}_1 = 0$ or $\deg \tilde{r}_1 < \deg b$.

(2) $ma = b\tilde{q}_2 + \tilde{r}_2$ where $\tilde{r}_2 = 0$ or $\deg \tilde{r}_2 < \deg b$.

(1)−(2) $\quad 0 = b(\tilde{q}_1 - \tilde{q}_2) + (\tilde{r}_1 - \tilde{r}_2) \Rightarrow b(\tilde{q}_1 - \tilde{q}_2) = \tilde{r}_2 - \tilde{r}_1$

$\Rightarrow b \mid \underbrace{\tilde{r}_2 - \tilde{r}_1}_{\deg < b} \Rightarrow \tilde{r}_2 - \tilde{r}_1 = 0 \Rightarrow \tilde{r}_2 = \tilde{r}_1$

$b(\tilde{q}_1 - \tilde{q}_2) = 0 \Rightarrow \tilde{q}_1 - \tilde{q}_2 = 0 \Rightarrow \tilde{q}_1 = \tilde{q}_2$.

Divide $x^2 - 2yx + 1$ by $b = yx + 1$ in $\mathbb{Z}[y][x]$ using pseudo $\div$.

$$b = (y)x^1 + 1 \overline{\big)\, y^2x^2 + (-2y^3)x + y^2} = ma.$$

$$y \cdot x + (-2y^2 - 1) \cdot 1 \leftarrow \tilde{q}$$

$$-(y^2x^2 + y \cdot x)$$

$m = y^{2-1+1} = y^2$

$$-(y^2x^2 + y\cdot x)$$

$$= (-2y^3-y)x^1 + y^2$$

$$-\left((-2y^3-y)x + (-2y^2-1)\right)$$

$$= 0\cdot x + 3y^2 + 1 \leftarrow \tilde{r}$$