Lec7B Pseudo Division The Primitive Euclidean Algorithm

January 30, 2021 10:46 PM

Lemma. Let a,b be non-zero primitive polynomials in $D[x]$ where D is a UFD e.g. $D = \mathbb{Z}$.

E.g. $a = x^2+3x+2$, $b = 2x^2+x-1$ in $\mathbb{Z}[x]$.

Let $m \in D$, $\tilde{r}, \tilde{q} \in D[x]$ satisfy $ma = b\tilde{q}+\tilde{r}$ with $\tilde{r}=0$ or $\deg \tilde{r} < \deg b$.

Then

$$\gcd(\overset{\deg 3}{a},\overset{\deg 2}{b}) \sim \gcd(\overset{\deg<2}{pp(\tilde{r})},\overset{\deg b.}{b}).$$

Proof. Let $g = \gcd(a,b)$ and $h = \gcd(pp(\tilde{r}),b)$.

We must show $g|h$ and $h|g$ in $D[x]$.

$(g|h)$. $g = \gcd(a,b) \Rightarrow g|a \wedge g|b \Rightarrow g|\overset{= c\cdot\square}{\tilde{r}}$
a & b are primitive $\Rightarrow$ g is primitive $\Big\}$ $g \mid pp(\tilde{r})$.

$(h|g)$ $h|pp(\tilde{r}) \Rightarrow h|\tilde{r} \Rightarrow h|ma$ $\Big\} \Rightarrow$ $h|a$. $\Rightarrow h|g$.
$h|b$ $\Rightarrow$ h is primitive $\qquad\qquad$ $h|b$

Example in $\mathbb{Z}[x]$.

primitive.

$a = 1\cdot x^2+3x+2$
$b = 2x^2+x-1.$

$\tilde{r}_2 = \text{prem}(a \div b) = 1\cdot x+1.$

$\gcd(a,b) = \gcd(\tilde{r}_2,b) = \gcd(b,\tilde{r}_2) = \gcd(\underset{a}{2x^2+x-1}, \underset{b}{x+1}).$

$\gcd(a,b) = \gcd(b,\tilde{r})$
$= \gcd(0, x+1)$
$= x+1.$

Maple prem(a,b,x).

$m=2$

$$\begin{array}{rl} & 1 = \tilde{q} \\ b = 2x^2+x-1 \,\big) & 2\cdot x^2+6x+4 = ma \\ & -(2x^2+x-1) \\ \hline & 5x+5 = \tilde{r} \end{array}$$

$m = 1^2 = 1$

$$\begin{array}{rl} & 2x-1 = \tilde{q}_3 \\ b = 1\cdot x+1 \,\big) & 2x^2+x-1 \\ & -(2x^2+2x\ \ ) \\ & -x-1 \\ & -(-x-1) \\ \hline & 0 - \tilde{r}_3 \end{array}$$

Algorithm 2.3 Primitive Euclidean Algorithm.

Input $a,b \in R[x_1,\ldots,x_n]$, $\overset{= \mathbb{Z}}{R}$ is a UFD and $a\neq 0$, $b \neq 0$.
Output $\gcd(a,b)$. # No polynomial factorization.

Step ① If $n=0$ then $(a,b \in R)$ output $\gcd_R(a,b)$.

Step ② Write a,b in $R[x_2,\ldots,x_n][x_1]$

Step ① If $n=0$ then $(a,b \in R)$ output g in R

Step ② Write a,b in $R[x_2,\dots,x_n][x_1]$

So $a = \underline{a_n} x^n \underline{+} \cdots \underline{+} \underline{a_0}$, $b = b_m x^m + \cdots + b_0$ where $a_i, b_i \in R[x_2,\dots x_n]$.

Step ③ $c := \gcd(\underline{\text{cont}(a)}, \underline{\text{cont}(b)})$

$= \gcd(a_n,\dots,a_0, b_m,\dots,b_0)$

Do this recursively (one less variable).

Step ④ # Primitive Polynomial remainder sequence.

```
$r_0 \leftarrow a/\underset{\uparrow\, x_1}{\text{cont}}(a) = pp(a)$.        $\div$ in $D[x_2,\dots,x_n]$.
$r_1 \leftarrow b/\underset{\uparrow}{\text{cont}}(b) = pp(b)$.
$k \leftarrow 1$.
while $\boxed{r_k \neq 0}$ do
    $r_{k+1} \leftarrow \text{prem}(r_{k-1} \div r_k)$
    if $r_{k+1} \neq 0$ then $r_{k+1} \leftarrow r_{k+1}/\underset{\uparrow}{\text{cont}}(r_{k+1}) = pp(r_{k+1})$.
end.     ↙ gcd of the contents
$g \leftarrow c \cdot r_{k-1}$ ← gcd of pps.  Lots of gcds in $D[x_2,\dots,x_n]$
Output $n(g)$.
```

In $\mathbb{Z}[x_2,\dots,x_n]$, the coefficients of r_k grow.

The growth of the integers is linear in $\deg(a)$.

The growth of r_k in x_i is linear in $\deg(a)$.

The $\deg(r_k, x_1)$ is drops.

See demo.