Fast Polynomial Division

September 9, 2021 5:24 PM

Assignment #1 due Wednesday September 22nd.

$m \geq n$

Let $a, b \in F[x]$, F a field. $a = a_0 + a_1 x + \cdots + a_m x^m$, $b = b_0 + b_1 x + \cdots + b_n x^n$

Let $\boxed{a = bq + r}$ with $r = 0$ or $\deg r < \deg b$. If $m = 2n$ the classical $\div$ algorithm does $\leq \underline{(n+1) \cdot n}$ multiplications and subtractions.

$$\begin{array}{r} \cdot x^n + \cdots + \cdot \\ \cdot x^n + \cdots + \cdot \,\big)\, \overline{\cdot x^{2n} + \cdots + \cdot} \end{array}$$

① Compute q then ② $r = a - bq$ ← one fast mult.

Define $a^r = a_m + a_{m-1} x + \cdots + a_0 x^m$ the reciprocal polynomial.

Idea 1 Compute $q^r = \frac{a^r}{b^r}$ truncated to $O(x^{m-n+1})$

$m-n+1$ ← $\deg q + 1$

$a = 6x^2 + 8x + 2$ $\quad a^r = 2x^2 + 8x + 6$

$b = 2x + 4$ $\quad b^r = 2 + 4x$

$\underline{\deg q = 1}$

$$\begin{array}{rl} & q^r \\ & \boxed{3 - 2x} + 5x^2 \\ b^r = 2 + 4x \,\big) & a^r = 6 + 8x + 2x^2 \\ - & 6 + 12x \\ \hline & -4x + 2x^2 \\ - & (-4x - 8x^2) \\ \hline & 10x^2 \end{array}$$

This algorithm is $O(\deg q^2)$.

Idea 2 Compute $\frac{1}{b^r}$ to $O(x^{m-n+1})$ as a power series Then

$q^r = \frac{1}{b^r} \cdot a^r$ to $O(x^{m-n+1})$

a second fast multiplication.

$$\begin{array}{rl} & \frac{1}{2} - x \\ b^r = \;\;+4x \,\big) & 1 \\ & -(1 + 2x) \\ \hline & -2x \\ & -2x - 4x^2 \end{array}$$

$1/b^r \cdot a^r \qquad \frac{a^r}{b^r}$

$(\frac{1}{2} - x) \cdot (6 + 8x) = 3 + 4x - 6x - 8x^2$

$= 3 - 2x$

$= q^r$

Recall the Newton iteration to solve $f(y)=0$.

$y_0 =$ initial approx.

$y_{k+1} = y_k - f(y_k)/f'(y_k)$

To compute $y=\frac{1}{b}$ use $\boxed{f(y)=b-\frac{1}{y}}$ $\quad f'(y)=+\frac{1}{y^2}$

so $\underline{f(y)=0} \Rightarrow b-\frac{1}{y}=0 \Rightarrow b=\frac{1}{y} \Rightarrow \underline{y=\frac{1}{b}}$.

$$y_{k+1} = y_k - \frac{b-\frac{1}{y_k}}{\frac{1}{y_k^2}} = y_k - by_k^2 + y_k$$

$$= 2y_k - by_k^2$$

No $\div$

$b = b_0 + b_1 x + \cdots$

two more fast multiplications.

$y_0 = \frac{1}{b_0}$

Theorem 9.2 (MCA)

Let R be a comm. ring with 1_R.

Let $f \in R[x]$ $f = f_0 + f_1 x + \cdots$ with $f_0^{-1} \in R$.

Let $y_0 = f_0^{-1}$ and $y_i = 2y_{i-1} - f y_{i-1}^2 \bmod \underline{x^{2^i}}$ for $i>0$.

Then $f\cdot y_i \equiv 1 \bmod x^{2^i}$ for $i \geq 0$.

Proof. (by induction on i).

We will prove $\boxed{1-f\cdot y_i \equiv 0}$ mod x^{2^i}

$(i=0)$ $\quad 1-f\cdot y_0 = 1-(f_0+f_1x+\cdots)\cdot\frac{1}{f_0} \bmod x^1 = 0$

$(i>0)$ $\quad 1-f\underline{y_i} = 1-f(2y_{i-1}-f\cdot y_{i-1}^2)$

$$= 1-2fy_{i-1}+f^2y_{i-1}^2$$

$$= (\underline{1-fy_{i-1}})^2$$

By induction on i $\quad \underline{1-fy_{i-1}} \equiv 0 \bmod \underline{x^{2^{i-1}}}$

$$=(0+0x+\cdots+0x^{2^{i-1}-1}+\cdot x^{2^{i-1}}+\cdot x^{2^{i-1}+1}+\cdots)^2$$

$$\searrow \qquad = \left(0 + 0x + \cdots + 0x^{2^{i-1}-1} + \cdot x^{2^{i-1}} + \cdot x^{2^{i-1}+1} + \cdots\right)^2$$

$$= \cdot x^{2^i} + \cdot x^{2^i+1} + \cdots$$

$$\equiv 0 \bmod x^{2^i}.$$

Example. Compute $\frac{1}{\boxed{1-x+x^2}=b} \bmod x^4$ using a N.I.

$y_0 = \frac{1}{1} = 1. \bmod x^1$

$i=1 \qquad y_1 = 2y_0 - b \cdot y_0^2 \bmod \underline{x^2}$

$\qquad = 2 \cdot 1 - (1-x) \cdot 1$

$\qquad = 1 + x \qquad\qquad y_1^2 = 1 + 2x + x^2$

$i=2 \qquad y_2 = 2y_1 - by_1^2 \bmod x^{\underline{4}}$

$\qquad = 2(1+x) - (1-x+x^2)(1+2x+x^2)$

$\qquad = 2 + \underline{2x} - 1 - \underline{2x} - \cancel{x^3} + \underline{x} + \cancel{2x^2} + x^3 - \cancel{x^2} - 2x^3 - x^4$

$\qquad = 1 + x - x^3 \bmod x^4$

Let $M(n)$ be the cost of multiplying two polynomials of degree n.
Let $I(n)$ be the cost of computing $\frac{1}{b} \bmod x^n$.

$\frac{1}{b_0} \qquad I(1) = 1 = c.$

$$I(\underline{n}) \leq I\left(\frac{n}{2}\right) + \underbrace{\underline{M\left(\frac{n}{2}\right)}}_{(y_{i-1})^2} + \underbrace{\underline{M(n)}}_{b \cdot y_{i-1}^2} + O(n).$$

Exercise Assuming $M(n) > 2M\left(\frac{n}{2}\right)$ show that

$$I(n) < \underline{3}\, M(n) + O(n).$$

Let $D(n)$ be the cost of computing $\overset{\deg \leq 2n-1}{a} \div \overset{\deg = n}{b}$.

$$D(n) = I(n) + \underbrace{M(n)}_{\frac{1}{b^r} \cdot a^r} + \underbrace{M(n)}_{b \cdot q} + O(n) \leq 5M(n) + O(n).$$

It is possible (Paul Zimmermann et. al.) using the middle product to compute $\frac{1}{b} \bmod x^n$ in $\underline{2}M(n) + O(n)$.