2. Quotients

Let K be a field and assume $\pm, \times, \cdot^{-1}$ in K and the image of an integer under the hom. $\mathbb{Z} \to K$ can be computed in $O(1)$.

2.1. Mult. inverse

~~Def~~ $\cancel{K[[X]] := \{ f = \sum_{n=0}^{\infty} a_n X^n \mid a_0, a_1, \dots \in K \}}$ ~~ring of power series~~

~~Rmk~~ $\cancel{K[[X]]^\times = \{ f = \sum a_n X^n \mid a_0 \neq 0 \}}$.

[Assume that we can multiply two pol. $f, g \in K[X]$ of degree $< n$ in time $O(\mu(n))$, where $\mu(n) \geq n$, $\mu(n+m) \geq \mu(n) + \mu(m)$. (We've shown that $\mu(n) = n \log n \log\log n$ works for large n.)]

Thm 2.1 Let $f \in (K[X]/X^n)^\times$ with $f \equiv a_0 + a_1 X + \dots + a_{n-1} X^{n-1} \bmod X^n$.

($\Rightarrow a_0 \neq 0$)

We can compute $f^{-1} \pmod{X^n}$ ($= b_0 + \dots + b_{n-1} X^{n-1}$) in time $O(\mu(n))$ on an $O(\log n)$-bit RAM.

Alg W.l.o.g. $n = 2^k$, $k \geq 1$.

Recursively compute $g := (f^{-1} \bmod X^{2^{k-1}})$.

Return $h := (2 - fg) g \bmod X^{2^k}$.

Pf by induction. $g \equiv f \bmod X^{2^{k-1}}$.

$\Rightarrow fg \equiv 1 \bmod X^{2^{k-1}}$. $\Rightarrow fg$

$\Rightarrow fh \equiv (2 - fg) \cdot fg \bmod X^{2^{k-1}}$

$\Rightarrow 1 - fh \equiv (1 - fg)^2 \equiv 0 \bmod X^{2^k}$.

Total time: $\ll \mu(2^k) + \underbrace{\mu(2^{k-1})}_{\leq \frac{1}{2}\mu(2^k)} + \dots + \underbrace{\mu(1)}_{\leq \frac{1}{2^k}\mu(2^k)} \leq 2\mu(2^k) \ll \mu(n)$. $\square$

Rmk This is Newton's approximation alg. for the function

$$\varphi(t) = \frac{1}{t} - f.$$

$$\rightsquigarrow t - \frac{\varphi(t)}{\varphi'(t)} = t - \frac{\frac{1}{t} - f}{-\frac{1}{t^2}} = t + (t - ft^2) = (2 - ft)t^2$$

Rmk The same algorithm can be used to invert an element of $(\mathbb{Z}/p^n\mathbb{Z})^\times$ $\left(x = \sum_{n=0}^{\infty} a_n \cdot p^n,\ a_0, a_1, \dots \in \{0, \dots, p-1\},\ a_0 \neq 0\right)$.

(Just replace X by p everywhere!)

Rmk ~~It can also be used~~

Similarly, Newton's method can be used to find the inverse of a real number $k \in \mathbb{R}$, given its leading $O(n)$ digits in time $O(n^2)$.

(up to a relative error of $O(2^{-n})$)

2.2. Quotient and remainder

Thm 2.2.1 Given pol. $f, g \in K[X]$ of degree $< n$ (with $g \neq 0$), we can compute the quotient $q \in K(X)$ and remainder $r \in K(X)$

$q = \lfloor \frac{f}{g} \rfloor$, $r = f \bmod g$

(such that $f = gq + r$, $\deg(r) < \deg(g)$) in time $\mathcal{O}(\mu(n))$ on an $\mathcal{O}(\log n)$-bit RAM.

Pf Let $f(X) = X^u \cdot \tilde{f}(\frac{1}{X})$, $g(X) = X^v \cdot \tilde{g}(\frac{1}{X})$,

$\tilde{f}, \tilde{g} \in K[Y]$, $\tilde{f}(0), \tilde{g}(0) \neq 0$.

(If $f(X) = a_u X^u + \dots + a_0$, then $\tilde{f}(Y) = a_u + a_{u-1}Y + \dots + a_0 Y^u$.)
$(a_u \neq 0)$

w.l.o.g. $u \geq v$. (Otherwise, $q = 0$, $r = f$.)

~~Let $h \in K(Y)$ s.t. $\tilde{g}\, h(Y) \equiv 1 \bmod Y^{u-v+1}$.~~

~~Let $i \equiv \tilde{f}(Y) \cdot h(Y) \bmod Y^{u-v+1}$.~~

~~$\Rightarrow \tilde{g}(Y)\, i(Y) \equiv \tilde{f}(Y) \bmod Y^{u-v+1}$~~

~~Then,~~

~~$q(X) = X^{u-v} \cdot i(\frac{1}{X}) \in K[X]$~~

~~and $g(X)q(X) = X^u \tilde{g}(\frac{1}{X})\, i(\frac{1}{X})$~~

Let $\tilde{q}(Y) = (\tilde{f}(Y) \cdot \tilde{g}(Y)^{-1} \bmod Y^{u-v+1})$. (This can be computed in $\mathcal{O}(\mu(n))$ because products and inverses can.)

Then, $q(X) := X^{u-v} \cdot \tilde{q}(\frac{1}{X})$ is the quotient pol:

- It's a polynomial because $\deg(\tilde{q}) \leq u - v$.
- Since $Y^u(f(\frac{1}{Y}) - g(\frac{1}{Y})q(\frac{1}{Y})) = \tilde{f}(Y) - \tilde{g}(Y)\tilde{q}(Y)$ is divisible by Y^{u-v+1} in $K[Y]$, we have $\deg(f - gq) \leq v - 1$.

$r := f - gq$ can also be computed in $\mathcal{O}(\mu(n))$. $\square$

A similar argument over $\mathbb{R}$ shows:

Thm 2.2.2 ~~we can~~ For (binary) integers x, y with $< n$ bits, $(y \neq 0)$

we can compute $q = \left\lfloor \frac{x}{y} \right\rfloor$ and $r = (x \bmod y)$ in $\mathcal{O}(n)$...

Pf It suffices to compute $\frac{x}{y} \in \mathbb{R}$ to ~~relative precision~~ absolute precision 1, so relative precision $\sim 2^{-n}$.

This leaves just ≤ 3 integers q to try.

$\square$

3. Greatest common divisor

Recall the Euclidean algorithm:

$a_0 = f$

$a_1 = g$

$a_{i+2} = a_i \bmod a_{i+1} = a_i - \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor \cdot a_{i+1}$ until $a_{k+1} = 0$.

$\Rightarrow \gcd(f,g) = a_k$.

Let $q_i = \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor$.

$$\Rightarrow \begin{pmatrix} a_{i+1} \\ a_{i+2} \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}}_{M_i} \begin{pmatrix} a_i \\ a_{i+1} \end{pmatrix} \quad \Rightarrow \begin{pmatrix} a_i \\ a_{i+1} \end{pmatrix} = M_{i-1} \cdots M_0 \begin{pmatrix} f \\ g \end{pmatrix}$$

until $\begin{pmatrix} \gcd(f,g) \\ 0 \end{pmatrix} = M_{k-1} \cdots M_0 \begin{pmatrix} f \\ g \end{pmatrix}$

Remk $\deg(q_i) = \deg(a_i) - \deg(a_{i+1})$

$$\sum_i \deg(q_i) = \deg(f) - \deg(\gcd(f,g)) \leq \deg(f),$$

so at least the total number of coefficients in the pol. q_i is linear (unlike the total number of coeff. in the pol. a_i).

~~Rough idea: To compute a matrix~~ $M \in GL_2(K[X])$ with $\det(M) = \pm 1$, ~~and such~~

Remk If $M \in GL_2(K[X])$ is a matrix with $\det(M) = \pm 1$ and such that $M \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} h \\ 0 \end{pmatrix}$, then $\gcd(f,g) = h$.

Pf Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. $\Rightarrow$ $h = af + bg$, $0 = cf + dg$ $\Rightarrow \gcd(f,g) \mid h$.

On the other hand, $dh = adf + bdg = (\det(M) + bc)f + bdg$
$= \pm f + b(cf + dg) = \pm f$,

so $h \mid f$.

Similarly, $h \mid g$. $\square$

~~**Idea** Let $\deg(f), \deg(g) < n$. To compute a matrix $M \in GL_2(K[x])$ with $\det(M) = \pm 1$ and such that $M\begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} h \\ r \end{pmatrix}$ for some r with $\deg(r) < n - k$, we only need to know the top (at most) $2k$ coefficients of f and g.~~

Idea Recursively find approximations to M: matrices M' s.t. $\det(M') = \pm 1$ and

$M'\begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} t \\ r \end{pmatrix}$ for some pol. t, r with smaller and smaller $\deg(t)$ (starting with $M' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, where $r = g$, and finishing with $M' = M$, where $r = 0$.)

Lemma 3.1 Let $f, g \in K[X]$, $\deg(f), \deg(g) \leq n$ and let $k \geq 1$ with $s := n - 2k \geq 0$. Let $M \in GL_2(K[X])$ s.t. $M = \begin{pmatrix} \deg \leq k & \deg \leq k \\ \deg \leq k & \deg \leq k \end{pmatrix}$

and $M \begin{pmatrix} \lfloor f/x^s \rfloor \\ \lfloor g/x^s \rfloor \end{pmatrix} = \begin{pmatrix} * \\ * \text{ of deg} < (n-s-k) = k \end{pmatrix}$.

Then,

$$M \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} * \\ * \text{ of deg.} < n-k \end{pmatrix}.$$

(Moral: To find M s.t. the lower entry has degree $< n-k$, we only need the top $2k$ coefficients of f, g.)

Pf

$$M \begin{pmatrix} f \\ g \end{pmatrix} = M \begin{pmatrix} x^s \cdot \lfloor f/x^s \rfloor + (f \bmod x^s) \\ \cdots \end{pmatrix}$$

$$= \underbrace{x^s \cdot \underbrace{M \begin{pmatrix} \lfloor f/x^s \rfloor \\ \lfloor g/x^s \rfloor \end{pmatrix}}_{\begin{pmatrix} * \\ \deg < n-s-k \end{pmatrix}}}_{\begin{pmatrix} * \\ \deg < n-k \end{pmatrix}} + \underbrace{\underbrace{M}_{\deg \leq k} \underbrace{\begin{pmatrix} f \bmod x^s \\ g \bmod x^s \end{pmatrix}}_{\deg < s}}_{\deg < k+s = n-k}$$

$\square$