CSS.307.1: Algebra, Number Theory and Computation

Instructor: Mrinal Kumar

TIFR 2025, Aug-Dec

Scribe: Soham Chatterjee

soham.chatterjee@tifr.res.in
Website: sohamch08.github.io

Contents

Chapter 1

Basic Algebra

Chapter 2

Polynomial Arithmetic

2.1 Multiplication

2.2 Fast Division

Polynomial Division
Input: $f, g \in \mathbb{F}[X]$, $\deg(f, g) \leq d$
Output: Quotient and reminder when f is divided by g.

Suppose $\deg f = a$ and $\deg g = b$. Let $(q, r) \in \mathbb{F}[X]$ are the quotient and remainder when f is divided by g i.e. $f = qg + r$. Therefore $\deg q = a - b$ and $m := \deg r < b$.

We can follow the long division algorithm to find (q, r). This algorithm takes $O(a - b) = O(d)$ many iteration to find q. And in each iteration we subtract a polynomial from another polynomial by multiplying one of them with power of x. For the multiplying with power x is just shifting of the coefficients. For the subtraction of polynomials it takes $O(d)$ time. Therefore each iteration of the algorithm takes $O(d)$ time complexity. Therefore the long division algorithm takes $O(d^2)$ time complexity.

If we can obtain q from f, g then we can get r by following the equation $r = f - gq$.

2.2.1 Reversal of Polynomials

Idea. *Reversal of Polynomials i.e. if $f \in \mathbb{F}[X]$ such that $f = f_0 + f_1 X + \cdots + f_a X^a$ then*

$$rev(f) = f_0 X^a + f_1 X^{a-1} + \cdots + f_a = f\left(\frac{1}{X}\right) X^a$$

Note:-
We have $\deg f \geq \deg(rev(f))$. Degree of $rev(f)$ can be strictly lesser than the degree of f. For example if $f_0 = 0$ and $f_1 \neq 0$, since $rev(f) = X^a f\left(\frac{1}{X}\right)$ the degree of $rev(f)$ is $a - 1$.

So using reversal we will review the equation $f = gq + r$:

$$\begin{aligned}
& f = qg + r \\
\iff & X^a f\left(\frac{1}{X}\right) = X^a \left[q\left(\frac{1}{X}\right) g\left(\frac{1}{X}\right) + r\left(\frac{1}{X}\right)\right] \\
\iff & X^a f\left(\frac{1}{X}\right) = X^a q\left(\frac{1}{X}\right) g\left(\frac{1}{X}\right) + X^a r\left(\frac{1}{X}\right) \\
\iff & rev(f) = rev(q) rev(g) + X^{a-m} rev(r)
\end{aligned}$$

Now we know $a \geq b > m \implies a - m \geq b - m > 0$. Therefore $X^{a-m} rev(r)$ is multiple of some nontrivial power of X. Now also we have

$$a - m > a - b = \deg q \geq \deg(rev(q))$$

Therefore we have

$$rev(f) \equiv rev(q)rev(g) \bmod X^{a-m}$$

Since $a - m \geq a - b + 1$ we have

$$rev(q) \bmod X^{a-m} \equiv rev(q) \bmod X^{a-b+1} \equiv rev(q)$$

Therefore we have

$$rev(f) \equiv rev(q)rev(g) \bmod X^{a-b+1}$$

Hence it suffices to recover $rev(q)$ in order to recover q from here. So the problem now reduced to finding a solution $h \in \mathbb{F}[X]$ for the system $\tilde{f} - h\tilde{g} \equiv 0 \bmod X^N$.

2.2.2 Find solution of $\tilde{f} - h\tilde{g} \equiv 0 \bmod X^N$

SOLVE $\tilde{f} - h\tilde{g} \equiv 0 \bmod X^N$
Input: $\tilde{f}, \tilde{g} \in \mathbb{F}[X]$, $\deg(f, g) \leq d$, $\tilde{f}(0), \tilde{g}(0) \neq 0$ with $N \in \mathbb{N}$
Output: Find solution h for the equation $\tilde{f} - h\tilde{g} \equiv 0 \bmod X^N$

Lemma 2.2.1
There is an unique $h \in \mathbb{F}[X]$ satisfying $\tilde{f} - h\tilde{g} \equiv 0 \bmod X^N$.

Proof: Let $\deg \tilde{f} = k$ and $\deg \tilde{g} = l$. Then Suppose $\tilde{f} = \sum_{i=0}^{k} \tilde{f}_i X^i$ and $\tilde{g} = \sum_{i=0}^{l} \tilde{g}_i X^i$. Then we can write the equation $\tilde{f} - h\tilde{g} \equiv 0 \bmod X^N$ as a linear system like the following:

$$\begin{bmatrix} \tilde{g}_0 & & & \\ \tilde{g}_1 & \tilde{g}_0 & & \\ \tilde{g}_2 & \tilde{g}_1 & \tilde{g}_0 & \\ \vdots & & & \ddots \\ & & & \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ \vdots \\ h_{k-l} \end{bmatrix} = \begin{bmatrix} \tilde{f}_0 \\ \tilde{f}_1 \\ \vdots \\ \tilde{f}_k \end{bmatrix}$$

Lets call the matrix G. Since $\tilde{g}_0 \neq 0$ the G has nonzero elements in the diagonal. Since the G is lower triangular the determinant of the G is nonzero. Therefore there exists unique solution solution for h. ∎

But we don't know how to find inverse of G in near linear time. So we cannot find h like this.

Idea. *Find a power series solution for* $h = \frac{\tilde{f}}{\tilde{g}} \bmod X^N$ *in* $\mathbb{F}[\![X]\!] \supseteq \mathbb{F}[X]$ *since in* $\mathbb{F}[\![X]\!]$ *inverse of* $\tilde{g}$ *exists*

Lemma 2.2.2
For every power series $P = \sum_{i=0}^{\infty} P_i X^i \in \mathbb{F}[\![X]\!]$, P has a multiplicative inverse iff $_0 \neq 0$.