September 16, 2026

Admin

- HW 0 due
- HW 1 out, due Oct 2 at 2:30pm

Today: Polynomial GCD

Recall: given $f, g \in \mathbb{C}[x]$, $h = \gcd(f,g)$ if

1) $h \mid f$ 2) $h \mid g$

3) if $p \mid f$ and $p \mid g$, then $p \mid h$.

Remark If h is a gcd of f & g, then so is $a \cdot h$ for any $a \in \mathbb{C} - \{0\}$.

When we say "the" gcd, we mean the gcd with leading coeff 1. (monic gcd)

Can compute gcd using the Euclidean algorithm.

EUCLID(f, g):

$r_0 \leftarrow f \qquad r_1 \leftarrow g$

$i \leftarrow 1$

while $r_i \neq 0$:

$r_{i+1} \leftarrow r_{i-1} \text{ rem } r_i$

$i \leftarrow i+1$

return r_{i-1}

f rem g = remainder of f divided by g.

Complexity: if $\deg(f), \deg(g) \leq n$, $\leq n$ iterations, each costs $O(n \lg n)$ ops $\Rightarrow$ $O(n^2 \lg n)$ ops

More careful accounting:

if $f = qg + r$, compute q & r using $O(\deg(f)\deg(q))$ ops via long division.

$\sum_i \deg(q_i) \leq n \Rightarrow O(n^2)$ ops suffice.

Correctness:

Lemma $\gcd(f,g) = \gcd(f-hg, g)$.

Proof If $d \mid f$ and $d \mid g$, then $d \mid f - hg$, so

$$\gcd(f,g) \mid \gcd(f-hg, g).$$

If instead $d \mid (f-hg)$ and $d \mid g$, then $d \mid hg$ and hence $d \mid f$. So

$$\gcd(f-hg, g) \mid \gcd(f,g). \quad \square$$

Corollary $\gcd(f,g) = \gcd(g, r_2)$

$$= \gcd(r_2, r_3)$$

$$\vdots$$

$$= \gcd(r_\ell, 0) = r_\ell.$$

Extended Euclidean algorithm

We will track remainders r_i and polynomials s_i, t_i such that

$$s_i f + t_i g = r_i.$$

EEA(f,g):

$r_0 \leftarrow f$ $\quad s_0 \leftarrow 1$ $\quad t_0 \leftarrow 0$

$r_1 \leftarrow g$ $\quad s_1 \leftarrow 0$ $\quad t_1 \leftarrow 1$.

$i \leftarrow 1$

while $r_i \neq 0$:

$$q_i = r_{i-1} \text{ quo } r_i$$

$$r_{i+1} = r_{i-1} \text{ rem } r_i \quad (= r_{i-1} - q_i r_i)$$

$$s_{i+1} = s_{i-1} - q_i s_i$$

$$t_{i+1} = t_{i-1} - q_i t_i.$$

$\ell \leftarrow i-1$

return $(r_i, s_i, t_i)_{i=0}^{\ell}$.

Claim: $s_i f + t_i g = r_i \quad \forall i.$

Proof: Induction on i. Clear for $i = 0, 1$.

For $i \geq 2$,

$$\begin{aligned} & s_i f + t_i g \\ &= (s_{i-2} - q_{i-1} s_{i-1}) f + (t_{i-2} - q_{i-1} t_{i-1}) g \\ &= (s_{i-2} f + t_{i-2} g) - q(s_{i-1} f + t_{i-1} g) \\ &= r_{i-2} - q_{i-1} r_{i-1} = r_i \end{aligned}$$

□

Application: modular inverse & finite field arithmetic

A field is a number system supporting addition, subtraction, multiplication, and division.

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$

($\mathbb{Z}/p\mathbb{Z}$: integers modulo p, p prime)

In $\mathbb{Z}/5\mathbb{Z}$, we can add, subtract, & multiply modulo 5. What about division?

$\frac{1}{3} \bmod 5$ should be a number x satisfying $3x = 1 \bmod 5$

$x = 2$ works. We say

$$\frac{1}{3} \equiv 2 \bmod 5.$$

Non-examples of fields:

$\mathbb{Z}/4\mathbb{Z}$: $\frac{1}{2}$ does not exist!

($2x = 1 \bmod 4$ has no solution)

$\mathbb{Z}/6\mathbb{Z}$: $2 \cdot 3 = 0 \bmod 6$

In a field, products of nonzero elements must be nonzero.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are infinite fields.

$\mathbb{Z}/p\mathbb{Z}$ is a <u>finite</u> field.

Finite fields are extremely useful in cryptography, coding theory, algebra, ...

<u>Extended Euclid</u> (for integers) is used for arithmetic in $\mathbb{Z}/p\mathbb{Z}$.

Extended Euclid (for polynomials) can implement arithmetic in more exotic finite fields.

Fact: $(\mathbb{Z}/2\mathbb{Z})[x] / (x^2 + x + 1)$

is a finite field of size 4.

$(\mathbb{Z}/2\mathbb{Z})[x]$: polynomials whose coeffs are integers mod 2

$(x^2 + x + 1)$: Every poly $p(x)$ is replaced w/ $p(x)$ rem $x^2 + x + 1$

Addition:

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Multiplication

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Everything has an inverse!

$$\frac{1}{x} = x+1$$

$$\frac{1}{x+1} = x$$

Why is $x \cdot (x+1) = 1$ in $(\mathbb{Z}/2\mathbb{Z})[x]/(x^2+x+1)$?

$$x \cdot (x+1) = x^2 + x$$

$$= 1 \cdot (x^2 + x + 1) + 1 \pmod 2$$

$$1 = (x^2 + x) \text{ rem } (x^2 + x + 1) \mod 2$$