

September 18, 2026

Admin: minor corrections to HW 1

- problem 1(a)
 - problem 1(b)
 - problem 1(c)
 - problem 4(d)
- typos
— slightly easier

See updated pdf on course website or Crowdmark.

When $sf + tg = \gcd(f, g)$, call s & t the Bézout coefficients of f & g .

Lemma: $\gcd(f, g) \neq 1$ iff $\exists s, t \in \mathbb{C}[x]$ such that

- $sf + tg = 0$
- $\deg(s) < \deg(g)$
- $\deg(t) < \deg(f)$

Proof

$\Rightarrow$: let $\gcd(f, g) = h \neq 1$.

take $s = g/h$, $t = -f/h$.

$$sf + tg = fg/h - fg/h = 0.$$

$\Leftarrow$: Since $sf + tg = 0$, $sf = -tg$,
so $f \mid tg$.

If $\gcd(f, g) = 1$, then $f \nmid t$,
which implies $\deg(t) < \deg(f) \Rightarrow \Leftarrow \square$

$$\mathbb{C}[x]_{<d} := \{ \text{polynomials of } \deg < d \}$$

Given $f, g \in \mathbb{C}[x]$, $n = \deg(f)$
 $m = \deg(g)$

let

$$\varphi : \mathbb{C}[x]_{<m} \times \mathbb{C}[x]_{<n} \rightarrow \mathbb{C}[x]_{<n+m}$$

$$s, t \mapsto sf + tg$$

Fact φ is a linear map of vector spaces.

Lemma φ is an isomorphism iff $\gcd(f, g) = 1$.

Proof

$$\dim(\mathbb{C}[x]_{<m} \times \mathbb{C}[x]_{<n}) = \dim(\mathbb{C}[x]_{<n+m})$$

$$\Rightarrow \varphi \text{ isomorphism} \Leftrightarrow \varphi \text{ injective}$$

lemma from $\begin{matrix} \text{prev} & \text{page} \end{matrix}$ $\Leftrightarrow \gcd(f, g) = 1. \quad \square$

Use bases $1, x, x^2, \dots, x^{m-1}$ for $\mathbb{C}[x]_{<m}$

$$1, x, \dots, x^{n-1} \text{ for } \mathbb{C}[x]_{<n}$$
$$1, x, \dots, x^{n+m-1} \text{ for } \mathbb{C}[x]_{\leq n+m-1}$$

$$\begin{aligned} f &= f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 \\ g &= g_m x^m + g_{m-1} x^{m-1} + \dots + g_1 x + g_0 \end{aligned}$$

The matrix corresponding to φ is the Sylvester matrix of f and g

$$\begin{array}{c} \text{\tiny T} \\ n+m \\ \text{rows} \end{array} \left(\begin{array}{ccccccc} f_n & & & g_m & & & \\ f_{n-1} & & & g_{m-1} & & & \\ \vdots & & & \vdots & & & \\ f_0 & & & g_0 & & & \\ & f_n & & & & & \\ & f_{n-1} & & & & & \\ & \vdots & & & & & \\ & f_0 & & & & & \\ & & f_n & & & & \\ & & \vdots & & & & \\ & & f_0 & & & & \\ & & & g_m & & & \\ & & & g_{m-1} & & & \\ & & & \vdots & & & \\ & & & g_0 & & & \end{array} \right) \begin{array}{cc} m & n \\ \text{cols} & \text{cols} \end{array}$$

Def The resultant of f & g is

$$\text{res}(f, g) := \det \text{Syl}(f, g)$$

↑ Sylvester matrix
of f and g .

Corollary $\text{res}(f, g) \neq 0$ iff $\gcd(f, g) = 1$

Examples:

$$\begin{aligned} \bullet \text{res}(ax + b, cx + d) &= \det \begin{pmatrix} a & c \\ b & d \end{pmatrix} \\ &= ad - bc \end{aligned}$$

$$\text{res}(ax + b, cx + d) = 0$$

$$\Leftrightarrow a/b = c/d \Leftrightarrow \begin{array}{l} ax + b \text{ \& } cx + d \\ \text{have common} \\ \text{root.} \end{array}$$

- $f = ax^2 + bx + c, a \neq 0$

$$\text{res}(f, f') = \det \begin{pmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{pmatrix}$$

$$= a(4ac - b^2)$$

$$\text{res}(f, f') = 0 \Leftrightarrow b^2 - 4ac = 0$$

$\Leftrightarrow f$ has a double root

In general, $\text{res}(f, f') =: \text{disc}(f)$ is called the discriminant of f .

- $\text{res}(ax^2 + bx + c, dx^2 + ex + f)$

$$= \det \begin{pmatrix} a & 0 & d & 0 \\ b & a & e & d \\ c & b & f & e \\ 0 & c & 0 & f \end{pmatrix} = a^2 f^2 - abef - 2acdf + b^2 df + ace^2 - bcde + c^2 d^2$$

Resultants determine if $\gcd(f, g) = 1$.
Analogue for higher degree?

Need to analyze degrees of s_i, t_i
appearing in Extended Euclid

Recall: $s_i f + t_i g = r_i$
 $\uparrow$ i th remainder

Lemma $\deg(s_i) = \sum_{j=2}^{i-1} \deg(q_j)$ for $i \geq 2$
 $\deg(t_i) = \sum_{j=1}^{i-1} \deg(q_j)$ for $i \geq 1$

Proof Will compute $\deg(s_i)$. Similar proof for $\deg(t_i)$.

Obs $\deg(q_j) > 0$ for $j \geq 2$.

$$s_i = s_{i-2} - q_{i-1} s_{i-1}$$

$$\deg(s_{i-2}) < \deg(s_{i-1}) \text{ by induction}$$

$$\begin{aligned} \text{So } \deg(s_i) &= \deg(q_{i-1}) + \deg(s_{i-1}) \\ &= \sum_{j=2}^{i-1} \deg(q_j) \quad \square \end{aligned}$$

Obs $\deg(s_i) = \deg(g) - \deg(r_{i-1})$
 $\deg(t_i) = \deg(f) - \deg(r_{i-1}).$

If $\deg(r_i) = d$, then

- $\deg(s_i) = m - \deg(r_{i-1}) < m - d$
- $\deg(t_i) = n - \deg(r_{i-1}) < n - d$
- $s_i f + t_i g = r_i$

Low-degree linear combinations like this can only arise from Extended Euclid.

Lemma. let $r \in \mathbb{C}[x]$, $d = \deg(r)$
 $t \in \mathbb{C}[x]$, $\deg(t) < \deg(f) - d$, $t \neq 0$
If $sf + tg = r$, then
 (s, t, r) is an entry of the Extended Euclidean scheme of f and g .

up to scaling by some $a \in \mathbb{C}[x]$

Proof let $\hat{r}$ be the highest-deg remainder in $\text{EES}(f, g)$ among those of degree $\leq d$.

$$\hat{s}f + \hat{t}g = \hat{r}$$

$$\hat{r} = r_j \quad \left| \begin{array}{l} \deg(r_j) \leq \deg(r) \\ \leq \deg(r_{j-1}) \end{array} \right.$$

$$\begin{aligned}\hat{s}f + \hat{t}g &= \hat{r} \\ sf + tg &= r\end{aligned}$$

$$\begin{pmatrix} \hat{s} & \hat{t} \\ s & t \end{pmatrix} \begin{pmatrix} f \\ g \end{pmatrix} = \begin{pmatrix} \hat{r} \\ r \end{pmatrix}$$

Claim $\hat{s}t = s\hat{t}$.

Proof. If not,

$$f = \frac{\begin{vmatrix} \hat{r} & \hat{t} \\ r & t \end{vmatrix}}{\begin{vmatrix} \hat{s} & \hat{t} \\ s & t \end{vmatrix}}.$$

But $\deg(f) = n$ and

$$\begin{aligned}\deg(\hat{r}t) &\leq d + \deg(t) \\ &< d + n - d = n\end{aligned}$$

$$\begin{aligned}\deg(r\hat{t}) &\leq d + \deg(\hat{t}) \\ &= d + n - \deg(r_{j-1}) \\ &< n.\end{aligned}$$

Contradiction.

$$\text{So } s\hat{t} = \hat{s}t.$$

Claim $\gcd(\hat{s}, \hat{t}) = 1.$

Proof. Induction.

Prove stronger statement that

$$s_i t_{i+1} - t_i s_{i+1} = (-1)^i$$

for s_i, t_i in EES.

□

$$s\hat{t} = \hat{s}t \Rightarrow \hat{t} \mid \hat{s}t$$

$$\gcd(\hat{t}, \hat{s}) = 1 \Rightarrow \hat{t} \mid t$$

$$\Rightarrow t = a \cdot \hat{t}, \quad a \in \mathbb{C}[x]$$

$$s\hat{t} = \hat{s}t = a\hat{s}\hat{t},$$

$$\text{so } s = a \cdot \hat{s}.$$

$$\text{then } r = sf + tg = a(\hat{s}f + \hat{t}g) = a\hat{r} \quad \square$$

Let $d \in \mathbb{N}$, $f, g \in \mathbb{C}[x]$.
 $n = \deg(f)$ $m = \deg(g)$.

$$\varphi_d: \mathbb{C}[x]_{< m-d} \times \mathbb{C}[x]_{< n-d} \rightarrow \mathbb{C}[x]_{< n+m-2d}$$

$$s, t \mapsto (sf + tg) \text{ quo } x^d$$

$\uparrow$
 drop coeffs of
 $x^{d-1}, \dots, 1$

Lemma φ_d isomorphism iff EES(f, g) contains a degree- d remainder.

Proof:

$\Rightarrow$: Suppose no deg- d remainder. pick j st
 $\deg(r_j) < d < \deg(r_{j-1})$.

then $\deg(s_j f + t_j g) < d$,
 so $\varphi_d(s_j, t_j) = 0$.

$\Leftarrow$: Suppose $\varphi_d(s, t) = 0$.
then $sf + tg = r$ for $\deg(r) < d$.

Previous lemma $\Rightarrow$ $s = as_j$
 $t = at_j$
 $r = ar_j$

$$d_j = \deg(r_j) \leq \deg(r) < d$$

$$n - d_{j-1} = \deg(t_j) \leq \deg(t) < n - d$$

$$\Rightarrow d_j < d < d_{j-1},$$

so no $\deg = d$ remainder appears. $\square$

Matrix of φ_d :

$$\begin{pmatrix} f_n & & & g_m & & \\ f_{n-1} & & & g_{m-1} & & \\ & & f_n & & & g_m \\ & & \vdots & & & \vdots \\ & & f_{2d-m+1} & \dots & f_d & g_{2d-n+1} \dots g_d \end{pmatrix}$$

Def $\text{Det}(\overset{\uparrow}{}) =: \sigma_d(f, g)$, the d^{th} subresultant of f and g .

Fact $\text{res}(f, g) = \sigma_0(f, g)$.

Thm $\sigma_d(f, g) \neq 0$ iff $\text{EES}(f, g)$ has a degree- d remainder.

Cor $\deg \gcd(f, g) = d$ iff
 $\sigma_0(f, g) = \dots = \sigma_{d-1}(f, g) = 0$
 $\sigma_d(f, g) \neq 0$.

This gives us an alternate algorithm to compute the Extended Euclidean Scheme.

- To decide if $\deg-d$ remainder is present, compute $\sigma_d(f, g)$

- If $\sigma_d(f, g) \neq 0$, compute

$$(s, t) = \varphi_d^{-1}(1)$$

$$r = sf + tg$$

By construction, $\deg(r) = d$
 $\deg(s) < m-d$
 $\deg(t) < n-d$

uniqueness

lemma $\Rightarrow$

(r, s, t) is an entry
in $EES(f, g)$

Next time: surprising algos for
linear algebra.