Polynomials and the Extended Euclidean Algorithm

01017

Discrete Mathematics

Date: 04 December 2025 **Semester:** Fall 2025

Rasmus Rosendahl-Kaa

An example of a polynomial

$$\begin{aligned} f(x) &= x^2 - 4x + 3 \\ g(x) &= 2x - 3 \\ h(x) &= 7 \end{aligned} \tag{1}$$

The curve on the graph is called a parabola

What we say for polynomials with real coefficients also applies to the ones with complex coefficients

Definition (Polynomial of degree n)

$$P(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n, \quad a_n \neq 0, a_i \in \mathbb{R} \text{ or } \mathbb{C} \tag{2}$$

- a_n is called the leading term
- a_0 is called the constant term.
- n is the degree

Definition (Addition of polynomials)

Same $P(x)$ as before

$$Q(x) = b_0 + b_1 x + ... + b_m x^m, \quad m \leq n \tag{3}$$

$$\begin{aligned} P(x) + Q(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_m + b_m)x^m \\ + a_{m+1}x^{m+1} + ... + a_n x^n \end{aligned} \tag{4}$$

$$\deg(P(x) + Q(x)) \leq n \text{ with equality if } m < n \tag{5}$$

Definition (Multiplication)

Same $P(x), Q(x)$ as before

$$\begin{aligned} P(x) \cdot Q(x) = a_0 \cdot b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + ... + \\ a_n b_m x^{n+m} \end{aligned} \tag{6}$$

$$\deg(P(x) \cdot Q(x)) = n + m = \deg(P(x)) + \deg(Q(x)) \tag{7}$$

When multiplying you basically do:

$$P(x) \cdot Q(x) = a_0 \cdot Q(x) + a_1 x \cdot Q(x) + ... + a_n x^n Q(x) \tag{8}$$

Divisible

Definition (Divisible)

$M(x)$ divides $N(x)$ (we write $M(x) \mid N(x)$) if $N(x) = Q(x) \cdot M(x)$

$Q(x)$ is some polynomial.

We have: $\deg(N) = \deg(Q) + \deg(M)$, so $\deg(M) \leq \deg(N)$

So basically, you need to find a polynomial $Q(x)$ so that $Q(x) \cdot M(x) = N(x)$, then $M(x)$ divides $N(x)$

If $M(x) \mid N(x)$ and $N(x)|M(x)$, then they must have the same degree. And then $\deg(Q)$ must have degree 0 and be a constant.

$\exists \alpha \in \mathbb{R} : N(x) = \alpha \cdot M(x)$

Common divisor

$D(x)$ is a common divisor of $M(x), N(x)$ if $D(x) \mid M(x)$ and $D(x) \mid N(x)$

Greatest common divisor

Definition

$D_1(x)$ is *a* greatest common divisor (gcd) of $M(x), N(x)$ if and only if D is a common divisor and $D_1(x)$ also satisfies:

$$(D_1(x) \mid M(x) \land D_1(x) \mid N(x)) \Rightarrow D_1(x) \mid D(x) \tag{9}$$

If $D_1(x)$ is a greatest common divisor, then $D_1(x)$ times a constant is also a greatest common divisor

Suppose $D_2(x)$ is also a $\gcd(M(x), N(x))$, then $D_2(x) \mid D_1(x)$ and $D_1(x) \mid D_2(x)$ so $D_2 = \alpha D_1$

Note

There can be more than one greatest common divisor

Given $N(x), M(x)$, find a gcd.

Note (For integers (repetition))

For integers: n, m, find $\gcd(n, m)$.

Euclid

$$\begin{aligned}
n &= q_1 \cdot m + r_1, \quad 0 \leq r_1 < r_0 = m \\
r_0 &= q_2 \cdot r_1 + r_2 \\
r_1 &= q_3 \cdot r_2 + r_3 \\
&\vdots \\
r_{k-3} &= q_{k-1} \cdot r_{k-2} + r_{k-1} \\
r_{k-2} &= q_k \cdot r_{k-1} + r_k \\
r_{k-1} &= q_{k+1} \cdot r_k + 0
\end{aligned} \tag{10}$$

r_k is the greatest common divisor.

Why is it a divisor

It is the divisor because looking at the last line: r_k divides r_{k-1}, r_k

We can go a line up: r_{k-1} divides r_{k-2}, r_{k-1}, but r_k must also divide them.

Can go up a line again: r_k divides r_{k-3}, r_{k-2} up until we get r_k divides n, m

Why is it the greatest common divisor

r_k can be written as a linear combination of r_{k-2} and r_{k-1} which coefficients are integers.

You can go a line up and write r_{k-1} as a linear combination, which you can input into r_k's linear combination. Continue until you get:

$$r_k = A \cdot N + B \cdot M \tag{11}$$

Definition (GCD for polynomials)

$\deg(M) = m < n = \deg(N)$

$$\begin{aligned} N(x) &= Q_1(x) \cdot M(x) + R_1(x), \quad \deg(R_1) < \deg(M) \\ M(x) &= Q_2(x) \cdot R_1(x) + R_2(x), \quad \deg(R_2) < \deg(R_1) \\ &\vdots \\ R_{k-2}(x) &= Q_k(x) \cdot R_{k-1}(x) + R_k(x), \quad \deg(R_k) = 0 \\ R_{k-1}(x) &= Q_{k+1}(x) \cdot R_k(x) + 0 \end{aligned} \tag{12}$$

$R_k(x) = A(x) \cdot N(x) + B(x) \cdot M(x)$

$A(x), B(x)$ are some polynomials.

$\deg(R_k(x)) = \deg(N(x)) - \deg(M(x))$

Example

Find the greatest common divisor of

$$\begin{aligned} N(x) &= x^4 + x^3 - 2x^2 + 2x - 2 \text{ and} \\ M(x) &= x^2 + 2x - 3 \end{aligned} \tag{13}$$

Divide:

$$\begin{array}{r} \underline{x^2 + 2x - 3} \,|x^4 + 3x^3 - 2x^2 + 2x - 2|\, \underline{x^2 - x + 3} \\ \underline{x^4 + 2x^3 - 3x^2} \\ -x^3 + x^2 + 2x - 2 \\ \underline{-x^3 - 2x^2 + 3x} \\ 3x^2 - x - 2 \\ \underline{3x^2 + 6x - 9} \\ -7x + 7 \end{array} \tag{14}$$

So:

$$N(x) = (x^2 - x + 3)M(x) + (-7x + 7) \tag{15}$$

Now continue with the two new polynomials you found:

$$\begin{array}{r} \underline{-7x+7}|x^2+2x-3| \underline{-\frac{1}{7}x - \frac{3}{7}} \\ \underline{x^2 - x} \\ 3x - 3 \\ \underline{3x - 3} \\ 0 \end{array} \tag{16}$$

So:

$$M(x) = \left(-\frac{1}{7}x - \frac{3}{7}\right) \cdot (-7x + 7) + 0 \tag{17}$$

Now we're finished as we have 0. The greatest common divisor is $-7x + 7$ We can write:

$$D(x) = -7x + 7 = N(x) - (x^2 - x + 3) \cdot M(x) \tag{18}$$

To find $D_1(x)$ (a divisor of $D(x)$: Remember: $D_1(x) = D(x) \cdot \alpha$ where α is a constant

$$D_1(x) = -x + 1 \tag{19}$$

Note

Both $D(x)$ and $D_1(x)$ are greatest common divisors of $N(x), M(x)$. as $D(x) = 1 \cdot D(x)$ (constant here is just 1).

Roots of polynomials

For the polynomial $ax^2 + bx + c$, the roots are: $\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

Let's assume $\gcd(N(x), M(x)) = D(x)$ then α is a common root of $N(x), M(x) \Leftrightarrow \alpha$ is a root in $D(x)$

$$\begin{aligned} N(x) &= D(x) \cdot Q_1(x) \\ M(x) &= D(x) \cdot Q_2(x) \end{aligned} \tag{20}$$

If α is a root in $D(x)$, then it must also be a root in $M(x)$ and $N(x)$. The reason is that we can write N, M as above

$$D(x) = A(x)N(x) + B(x)M(x) \tag{21}$$

α is a root of $P(x) \Leftrightarrow (x - \alpha)|\ P(x)$ which means $\exists Q(x) : P(x) = Q(x)(x - \alpha) + \beta$ where β is a constant

We can find β by calculating $P(\alpha)$:

$$
\begin{aligned}
P(\alpha) &= Q(\alpha)(\alpha - \alpha) + \beta \\
P(\alpha) &= Q(\alpha)(0) + \beta \\
P(\alpha) &= \beta
\end{aligned} \tag{22}
$$

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