# SMT-Final Algebra: Polynomials

Mattias Akke

Matteläger Stockholm 2026

*A brief introduction to efficient ways of working with polynomials in one dimension and some ideas on how to approach functional equations in competitive mathematics.*
*Greatly adapted from Mathematical Buffet (2016) by Victor Ufnarovski, Jana Madjarova, and Frank Wikström. The lecture contains problems that require full solutions and questions that mainly require proofs up to the reader's own satisfaction. I have sometimes left space for answers, which may come in handy for the reader later in the lecture.*

Let's begin with some prerequisites.

**Modulus**

**Q.1:** Determine the remainder when $13^{2026}$ is divided by 12.

**Q.2:** Determine the remainder when $P(x) = x^3 - 3x + 1$ is divided by $p(x) = x - 1$?

**Q.3:** Find the smallest positive integer $x$ such that $x \equiv 2 \pmod 3$ and $x \equiv 3 \pmod 5$.

**Q.4:** Find the greatest common divisor of $2n + 1$ and $n$ for any integer $n$.

**Q.5:** If $\gcd(a, b) = d$, what is the value of $\gcd(\frac{a}{d}, \frac{b}{d})$?

**Q.6:** Use the Euclidean algorithm to find $\gcd(96, 72)$

**Combinatorials & Binomial Expansion**

**Q.7:** State the binomial expansion. .....

**Q.8:** Calculate the binomial coefficient $\binom{5}{2}$.

**Q.9:** What is the coefficient of $x^2$ in the expansion of $(x + 2)^4$?

It is also useful to know the general binomial coefficient, valid for any $a \in \mathbb{C}, k \in \mathbb{Z}_+$

$$\binom{a}{k} = \frac{a(a-1)(a-2)...(a-k+1)}{k!}$$

**Q.10:** Find a closed formula for $\binom{-n}{k}$ .....

**Problem 1:** Show that for $|x| < 1$:

$$1 + nx + \binom{n+1}{2}x^2 + \binom{n+2}{3}... = \frac{1}{(1-x)^n}$$

**Factorization**

The following are "*some identities worth remembering*" of which I have only used 2 so far myself.

$$x^n - y^n = (x-y)\big(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}\big)$$

$$x^n + y^n = (x+y)\big(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1}\big), \quad \text{if } n = 2k+1$$

$$(x^2 + ax + 1)(x^2 - ax + 1) = x^4 + (2 - a^2)x^2 + 1$$

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 + y^2 + z^2 - xy - xz - yz)$$

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

**Q.11:** Factorize $x^5 - 1$

**Q.12:** Derive the geometric sum $a + ax + ax^2 + ... + ax^n = a\frac{1-x^{n+1}}{1-x}$

**Q.13:** What do we get when $x = 1$ in Q.12?

## Polynomials in One Dimension

Cool bananas. We can now move on to discuss general polynomials of the shape

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$$

where we say $\deg f = n$ if $a_0 \neq 0$. If $a_0 = 1$ we call $f$ *monic* (sv. *monisk*).

**Q.14:** Prove

$$\deg f(g(x)) = \deg\, f(x) \times \deg\, g(x)$$

We can similarly show

$$\deg\, f(x)g(x) = \deg\, f(x) + \deg\, g(x)$$

$$\deg f(x) + g(x) = \max(\deg\, f(x), \deg\, g(x))$$

Many concepts we are used to for integers directly translate to polynomials. By writing a polynomial $f$ as $f(x) = g(x)q(x) + r(x)$, we directly see concepts such as the *reminder* $r(x)$ (sv. *restterm*) and *quotient* $q(x)$ (sv. *kvot*) when dividing $f$ by $g$. If $r(x) = 0$, we can say $g(x)|f(x)$ (read $g$ *divides* $f$).

**Q.15:** What is the rest term when dividing the polynomial $P(x)$ by $p(x) = x - a$?

**Problem 2:** Let $f(x)$ be a monic polynomial of degree $n$ with integer coefficients. Show that all rational roots are integers. An extension of the proof above is the rational root theorem:

**Theorem 1: (Rational root theorem – sv. Satsen om rationella rötter)**

Let $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n$ be a polynomial with integer coefficients. Then for all rational roots $f(p/q) = 0$: $p|a_n$ and $q|a_0$.

We can similarly talk about the *greatest common divisor* written as $(f(x), g(x))$, and use the Euclidean algorithm to find it. If $(f(x), g(x)) = 1$, we say the polynomials $f$ and $g$ are *relatively prime* – just as for integers.

**Problem 3:** Let $P(x), Q(x)$ be two polynomials without any shared roots and integer coefficients. Show that there exists polynomials $A(x), B(x)$ with integer coeffients so that, for some $N \in Z$,

$$A(x)P(x) + B(x)Q(x) = N$$

In the above problem, we have essentially proved a special case of Bézout's Lemma applied to polynomials.

**Theorem 2: (Bézout's Lemma)**

Let $f(x)$ and $g(x)$ be two relatively prime polynomials. Then there exists $u(x)$ and $v(x)$ so

$$u(x)f(x) + v(x)g(x) = 1$$

**Theorem 3: (Gauss Lemma)**

Denote by $\text{cont}(f(x))$ the greatest common divisor of all coefficients of $f(x)$. If $f$ and $g$ are polynomials in $\mathbb{Z}[x]$, then $\text{cont}(f(x)g(x)) = \text{cont}(f(x)) \times \text{cont}(g(x))$.

It is often useful to define what class of numbers the coefficients belong to, and we then write $f(x) \in \mathbb{K}[x]$ for some class $\mathbb{K}$. Depending on what class we are working with, we can define an analog of prime numbers: *irreducible* polynomials (sv. *oreducerbara*). For example, the polynomial $p(x) = x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, but not in $\mathbb{R}[x]$ as $p(x) = (x - \sqrt{2})(x + \sqrt{2})$ or in $\mathbb{Z}_7[x]$ as $p(x) = x^2 - 2 = (x - 3)(x + 4)$ here.

**Problem 4:** Let $p(x)$ be an irreducible polynomial in $\mathbb{Z}[x]$. Show $p(x)$ has no multiple roots.

**Problem 5:** Show that for a polynomial $f(x) \in \mathbb{Z}[x]$, the following statements are equivalent:
$f(x)$ is irreducible in $\mathbb{Z}[x] \Leftrightarrow f(x)$ is irreducible in $\mathbb{Q}[x]$ Using the statement you so exquisitely proved, we can formulate a condition for $f(x)$ to be irreducible in $\mathbb{Z}[x]$:

**Theorem 4: (Eisenstein's Criterion)**

Let $f(x) = a_0x^n + ... + a_{n-1}x + a_n \in \mathbb{Z}[x]$ and $p$ a prime. If $p|a_i$ for $i > 0$ but $p \nmid a_0$ and $p^2 \nmid a_n$ then $f(x)$ is irreducible in $\mathbb{Q}[x]$ (and $\mathbb{Z}[x]$).

**Q.16:** Is $x^7 + 10x^3 + 5$ irreducible?

**Problem 6:** Show that for every prime $p$, the polynomial $f(x) = x^{p-1} + x^{p-2} + ... + x + 1$ is irreducible.

Building on this, we get the less useful but very interesting theorem

**Theorem 5**

Write a prime $p$ as $p = a_0b^n + a_1b^{n-1} + ... + a_n$ in a base $b > 1$. Then the polynomial $p(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n \in \mathbb{Z}[x]$ is irreducible.

**Q.17:** Is $x^2 + x + 3$ irreducible?

**Problem 7:** Consider the polynomial $p(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n \in \mathbb{Z}[x]$, with $|a_n|$ prime and

$$|a_n| \geq |a_0| + |a_1| + ... + |a_{n-1}|$$

Show that $p(x)$ is irreducible.

A similar statement is

**Theorem 6: (Perron's Criterion)**

Let $P(x) = x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$ be a polynomial with $a_n \neq 0$ and

$$|a_1| > 1 + |a_2| + |a_3| + ... + |a_n|$$

then $P(x)$ is irreducible.

## Symmetric polynomials

A very common occurrence in competitive mathematics is that of symmetric polynomials. We say a polynomial $p(x_1, x_2, ..., x_n)$ is *symmetric* (sv. *symetrisk*) if switching any two variables does not change the polynomial value.

**Q.18:** Determine symmetry: $a(x, y) = x^3 + xy - y^3 + 1$, $b(x, y, z) = x + y + z$, $c(x, y) = x - y$,

Symmetric polynomials can prove especially useful to understand the relation between a polynomial's roots and coefficients. Let's think about the general polynomial once again:

$$f(x) = x^n + a_1x^{n-1} + ... + a_n = (x + y_1)(x + y_2)...(x + y_n)$$

We find a clear relation between the roots and the coefficients (e.g., for $n = 3$):

$a_1 = y_1 + y_2 + y_3 := s_1(y_1, y_2, y_3)$, $a_2 = y_1y_2 + y_2y_3 + y_3y_1 := s_2(y_1, y_2, y_3)$, $a_3 = y_1y_2y_3 := s_3(y_1, y_3, y_3)$

Symmetrical polynomials $s_i$ that appear here are what are called *elementary symmetric polynomials* (sv. *elementära symmetriska polynom*).

**Theorem 7: (Vieta's theorem)**

he coefficients in a monic polynomial are the elementary symmetric polynomials of its roots (up to a sign): $a_i = (-1)^i s_i$

**Problem 8:** $p(x) = x^n + a_1x^{n-1} + ... + a_{n-1}x + 1$ is a polynomial with non-negative coefficients and $n$ real roots. Prove that $p(2025) \geq 2026^n$.

Although this is not an "inequalities" lecture, it is relevant to note the following theorem, generalising you beautiful proof used above.

**Theorem 8: (Maclaurin's inequality)**

If $x_i \geq 0$, then

$$S_1 \geq S_2^{1/2} \geq ... \geq S_k^{1/k} \geq ... \geq S_n^{1/n}$$

where $S_k = s_k / \binom{n}{k}$

A nice property of these is that every symmetric polynomial $p(x_1, x_2, ..., x_n)$ can be expressed uniquely using only the symmetrical polynomials.

**Q.19:** Express $p(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ using elementary symmetric polynomials. .....

**Problem 9:** Show that

$$x_1^2 + x_2^2 + x_3^2 \geq x_1x_2 + x_2x_3 + x_3x_1$$

## Trigonometric Polynomials

Before we conclude this lecture, we will look at trigonometric polynomials, which are critical to functional analysis but also prove useful when working with polynomial-related problems.

**Theorem 9**

For every trigonometric polynomial

$$f(x) = c_0 + c_1 cos(x) + c_2 cos(2x) + ... + c_n cos(nx)$$

there exists a polynomial $T(x)$ with highest coefficient $2^{n-1}c_n$ for which $f(x) = T(cosx)$ and the expression $T(cosx)$ can be rewritten as a trigonometric polynomial for every polynomial $T(x)$.

The trigonometrically inclined may want to attempt to prove the statement.

**Problem 10:** Prove Theorem 9.

Specifically polynomials of shape $T_n(cosx) = cosnx$ are called *Chebyshev polynomials*, which you will likely encounter in functional analysis if you have not already.

**Problem 11:** Let $p(x) = x^n + a_1 x^{n-1} + ... + a_{n-1}x + a_n$ be a polynomial. Show that

$$|p(\hat{x})| \geq \frac{1}{2^{n-1}}$$

for some $\hat{x} \in [-1, 1]$

## Problems, unsorted

**Problem 12: [SMT Qualif. 1971]**
Let $ax^2 + bx + c$ be a second-order polynomial with real coefficients and roots. Show that

$$a + b + c \leq \frac{9}{4} \max(a, b, c)$$

**Problem 13: [SMT Final 1976]**
$p(x)$ is a fith degree polynomial such that $(x-1)^3 \mid p(x) + 1$ and $(x+1)^3 \mid p(x) - 1$. Find $p(x)$

**Problem 14: [SMT Final 1970]**
Given $p = (x - x_1)(x - x_2)(x - x_3)$ where $x_i \in \mathbb{R}$, show that

$$p(x)p''(x) \leq (p'(x))^2$$

**Problem 15: [SMT Final 1985]**
$p(x)$ is a polynomial with real coefficients of degree $n$ such that $p(x) \geq 0 \ \forall \ x$. Show that for all $x$

$$p(x) + p'(x) + p''(x) + ... + p^{(n)}(x) \geq 0$$

**Problem 16: [SMT Final 2007]**
Show that the only real solutions $x = a$ to

$$nx^n - x^{n-1} - x^{n-2} - ... - 1 = 0$$

where $n$ is an integer greater than 0, are $a = 1$ or $-1 < a < 0$

**Problem 17:** **[SMT Final 2009]**
Find all real solutions to

$$(1+x^2)(1+x^3)(1+x^5) = 8x^5$$

**Problem 18:** Let $q$ and $\cos q\pi$ be rational numbers. Show that $\cos q\pi \in \{0, \pm\frac{1}{2}, \pm 1\}$

**Problem 19:** Let $p$ be prime. Show that $f(x) = x^{p-1} + 2x^{p-1} + 3x^{p-3} + ... + (p-1)x + p$ is irreducible.

**Problem 20:** **[IMO 1993 Problem 1]**
Let $f(x) = x^n + 5x^{n-1} + 3$ where $n > 1$ is an integer. Show that $f(x)$ can not be expressed as the product of two non-constant polynomials with integer coefficients.

**Problem 21:** Show that $P(x) = (x^2 + x)^{2^n} + 1$ is irreducible over the integers for any $n \in \mathbb{N}$.

**Problem 22:** **IMO 1996 Shortlist**
For every positive integer $n$, show that there exists a positive integer $k$ so that

$$k = f(x)(x+1)^{2n} + g(x)(x^{2n} + 1)$$

for some polynomials $g, f \in \mathbb{Z}[x]$. Find the smallest such $k$ as a function of $n$.

# Hints (Problems)

**Problem 1.** Use the general expression for $(x+1)^a$ where $|x| < 1$.

**Problem 2.** Set $f(p/q) = 0$ for two relatively prime integers.

**Problem 3.** Use the Euclidean algorithm

**Problem 4.** Remember that no two different polynomials of the same degree can share all roots.

**Problem 5.** Use Gauss Lemma

**Problem 6.** Try a change in variables

**Problem 7.** Attempt root hunting.

**Problem 8.** Use AM-GM and symmetric polynomials

**Problem 9.** Try rewriting as symmetric polynomials

**Problem 10.** Attempt induction with basis $n = 1, 2$

**Problem 11.** Use the theorem

**Problem 12.**

**Problem 13.**

**Problem 14.**

**Problem 15.**

**Problem 16.**

**Problem 17.** Trick question, your polynomial skills may here be your enemy!

**Problem 18.** Chebyshev polynomials

**Problem 19.**

**Problem 20.** Proof by contradiction

**Problem 21.**

**Problem 22.**

# Solutions (Problems)

**Problem 1.** Set $a = -n$ and $x = -x$ in the general expression of $(x+1)^a$

**Problem 2.** Setting $f(p/q) = 0$ for two relatively prime integers into $f(x) = x^n + ... + a_n$ gives $q|p^n \Leftrightarrow q = 1$

**Problem 3.** No shared roots gives us $(P(x), Q(x)) = 1$. The Euclidean algorithm now gives us $r_0 = P(x), r_1 = Q(x), r_n = 1$. We then show any $r_k = a_k(x)P(x) + b_k(x)Q(x)$ where $a_k(x), b_k(x) \in \mathbb{Q}[x]$ through induction, and finally write $a_n = A(x)/N, b_n = B(x)/N$ where $A(x), B(x) \in \mathbb{Z}[x]$ to get the final statement.

**Problem 4.** Assume $p$ has double root at $y_0$ implies $p(y_0) = p'(y_0) = 0$. Gauss: $\gcd_{p \in \mathbb{Q}[x]}(p, p') = 1$. Bézout's: $A(x)p(x) + B(x)p'(x) = 1$. Setting $x = y_0$, we get $0 = 1$ and a contradiction.

**Problem 5.** Assume $f(x)$ is irreducible in $\mathbb{Z}[x]$ but $f(x) = f_1(x)f_2(x)$ for $f_i(x) \in \mathbb{Q}[x]$. We can then get $zf(x) = g_1(x)g_2(x)$, $g_i(x) = z_i f_i(x) \in \mathbb{Z}[x]$ for a large integer $z = z_1 z_2$, and $z \times \text{cont}(f(x)) = \text{cont}(g_1(x)) \times \text{cont}(g_2(x)) = z$. This mean we can write $g_i(x) = \text{cont}(g_i(x))h_i(x)$ for some primitive $h_i(x) \in \mathbb{Z}[x]$. Hence, $f = h_1(x)h_2(x)$. However, this contradicts our assumption that $f(x)$ is irreducible in $\mathbb{Z}[x]$. $f(x)$ must therefore also be irreducible in $\mathbb{Q}[x]$. The other direction is similar.

**Problem 6.** Set $x = y + 1$ to get $f(x) = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{1}y^{p-2} + ... + \binom{p}{p-2}y + \binom{p}{p-1}$ and apply Eisenstein's criterion.

**Problem 7.** Suppose $f(x) = g(x)h(x)$ with $g, h \in \mathbb{Z}[x]$. Then $f(0) = g(0)h(0) = a_n$. Since $|a_n|$ prime we can say WLOG $|g(0)| = 1$. Say $b_0$ is the first coefficient in $g$, then by using elementary symmetric polynomials, we have $|y_0 y_1 ... y_k| = 1/|b_0| \leq 1,\ k < n$, implying at least one $|y_i| \leq 1$. However, we also have $f(y_i) = 0 \Leftrightarrow |a_n| = |a_0 y_i^n + ... + a_{n-1} y_i| \leq |a_0 y_i^n| + ... + |a_{n-1} y_i| \leq |a_0| + |a_1| + ... + |a_{n-1}|$ which would be a contradiction to the problem statement, concluding the proof.

**Problem 8.** All roots $x_i$ are negative and set $y_i = -x_i$ to simplify. Vieta's gives $a_n = y_1 y_2 ... y_n = 1$. The coefficient $a_k$ will contain $\binom{n}{k}$ combinations of roots $y_i$ – e.g., for $a_2$ we have $\binom{n}{2}$ terms $x_i x_j, i \neq j$. AM-GM then gives us

$$s_k \geq \binom{n}{k} \sqrt{(x_1 x_2 ... x_n)^{\binom{n-1}{k-1}}} = \binom{n}{k}$$

Putting it into $p(x)$ we get $p(x) \geq x^n + \binom{n}{1} x^{n-1} + ... + \binom{n}{n-1} x + 1 = (x+1)^n$ and hence $p(2025) \geq (2025+1)^n = 2026^n$

**Problem 9.** The statement is equivantly $s_1^2 - 2s_2 \geq s_2 \Leftrightarrow s_1^2 \geq 3s_2 \Leftrightarrow s_1 \geq \sqrt{3s_2} \Leftrightarrow s_1/3 \geq \sqrt{s_2/3}$ which is exactly Maclaurin's inequality.

**Problem 10.** Induction. Basis for $n = 1, 2$ is trivial. Assume the statement holds for $T_m(cosx) = cos(mx)$and $T_{m-1}(cosx) = cos((m-1)x)$. Now, $cos((m+1)x) = 2cos(x)cos(mx) - cos((m-1)x) = 2tT_m(t) - T_{m-1}(t)|_{t=cosx} = T_{m+1}(t)$ which is a polynomial of degree $m+1$. Since the statement holds for $T_m$, the highest coefficient is $2^{m-1}c_m = 2^{m-1}$ a by our definition of $T_m$, meaning the highest coefficient of $T_{m+1}$ is $2^m$. We can then simply define $f_{n+1}(x) = f(x) = c_0 + c_1 cos(x) + c_2 cos(2x) + ... + c_n cos(nx) + c_{n+1} cos((n+1)x) = P_n(cosx) + c_{n+1} T_{n+1}(cosx) = P_{n+1}(cosx)$ which hence is a sum of two polynomials, therefore also a polynomial, and of which the highest coefficient is $2^n c_{n+1}$ which concludes the proof.

**Problem 11.** First, set $x = cos(t)$ to guarantee the limits, and define $p(cos(t)) = f(t) = c_0 + c_1 cos(t) + ... + c_n cos(nt)$. We now know $c_n = 1/2^{n-1}$. Then, we hunt orthogonalities in $f$ until we arrive at

$$\sum_{k=0}^{2n-1} (-1)^k \cos\left(\frac{mk\pi}{n}\right) = \begin{cases} 0, & m = 0, 1, \ldots, n-1, \\ 2n, & m = n. \end{cases}$$

from which we can write

$$|c_n| = \left| \frac{1}{2n} \sum_{k=0}^{2n-1} (-1)^k f\left(\frac{k\pi}{n}\right) \right| \leq \max_{0 \leq k \leq 2n-1} |$$

f$\left(\frac{k\pi}{n}\right)$ . It therefore exists a $\hat{x} = cos(k\pi/n) \in [-1, 1]$ solving the proposition

**Problem 12.**

**Problem 13.**

**Problem 14.**

**Problem 15.**

**Problem 16.**

**Problem 17.** Set $x < 0$. Now VL $> 0$ and HL $< 0$. No solutions. $x = 0$ trivially has no solutions. Now set $x > 0$. AM-GM on each term in VL quickly gives you VL $\geq$ HL with equality for $x = 1$.

**Problem 18.** Chebyshev, then rational root theorem, then trigonometry.

**Problem 19.**

**Problem 20.**

**Problem 21.**

**Problem 22.**

## Solutions (Questions)

**Q.1.** The remainder is 1

**Q.2.** The remainder is $-1 = P(1)$ by the Polynomial Remainder Theorem.

**Q.3.** $x \equiv 8 \pmod{15}$.

**Q.4.** The GCD is 1 (they are coprime).

**Q.5.** The GCD is 1 (they are again coprime).

**Q.6.** The GCD is 24.

**Q.7.** $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

**Q.8.** 10

**Q.9.** The coefficient is $\binom{4}{2} \cdot 2^2 = 6 \cdot 4 = 24$.

**Q.10.** $(-1)^k \binom{n+k-1}{k}$

**Q.11.** $(x-1)(x^2+x+1)$.

**Q.12.** Set $x = 1, y = x, n = n+1$ in the first usefull identity and multiply with $a$.

**Q.13.** $(n+1)a$

**Q.14.** Multiply arbitrary polynomials and find largest degree.

**Q.15.** $P(a)$

**Q.16.** yes (set $p = 5$).

**Q.17.** yes. e.g. $10^2 + 10 + 3 = 113, 4^2 + 3 + 3 = 23$, which are prime.

**Q.18.** a: no, b: yes, c: no

**Q.19.** $s_1^2 - 2s_2$