Enrichment Lectures 2010
Some facts and problems about polynomials

Finbarr Holland,
Department of Mathematics,
University College Cork,
f.holland@ucc.ie;

February 18, 2010

1 A quick review of complex numbers

Although people had used complex numbers long before him, it was the Irish mathematician Hamilton (1805–1865) who axiomatised them. He defined them as ordered pairs (a, b) of real numbers that obeyed certain operations of addition and multiplication. Using the usual laws of addition and multiplication for real numbers, he defined the sum and product of two such pairs $(a, b), (c, d)$ by

$$(a, b) + (c, d) = (a + c, b + d),\ (a, b)(c, d) = (ac - bd, ad + bc),\ \forall a, b, c, d \in \mathbb{R}.$$

Since addition and multiplication of real numbers are *commutative* operations, it follows from the definitions just given that the same is true of the new operations:

$$(a, b) + (c, d) = (c, d) + (a, b),\ (a, b)(c, d) = (c, d)(a, b),\ \forall a, b, c, d \in \mathbb{R}.$$

Notice that multiplication *distributes* over addition:

$$(a, b)\left((c, d) + (e, f)\right) = (a, b)(c, d) + (a, b)(e, f),\ \forall a, b, c, d, e, f \in \mathbb{R}.$$

As well, the new operations are *associative*, properties which are inherited from the real numbers. For instance, $\forall a, b, c, d, e, f \in \mathbb{R}$,

$$\begin{aligned}(a, b) + ((c, d) + (e, f)) &= (a, b) + (c + e, d + f)\\ &= (a + (c + e)), b + (d + f))\\ &= ((a + c) + e, (b + d) + f)\\ &= (a + c, b + d) + (e, f)\\ &= ((a, b) + (c, d)) + (e, f).\end{aligned}$$

,

Exercise 1. *Prove that*

$$(a, b)\left((c, d)(e, f)\right) = \left((a, b)(c, d)\right)(e, f), \ \forall a, b, c, d, e, f \in \mathbb{R}.$$

This means that we can unambiguously define the sum, $u + v + w$, (respectively, the product uvw) of three complex numbers u, v, w as either $u + (v + w)$ or $(u + v) + w$ (respectively, as $u(vw)$ or $(uv)w$). In particular, we can define successive powers of a complex number in a clear way.
We denote the set of complex numbers by $\mathbb{C}$, and usually use the letter z as a generic complex number. The real numbers can be thought of as forming a subset of the complex numbers $\mathbb{R}$: this is because pairs of the form $(a, 0)$ have algebraic properties exactly similar to the real numbers, and we simply identify such pairs with a, i.e., we write a in place of $(a, 0)$. (Thus (an isomorphic copy of) $\mathbb{R}$ sits inside $\mathbb{C}$: $\mathbb{R} \subset \mathbb{C}$.) In particular, we write 1 for $(1, 0)$. The pair $(0, 1)$ is also singled out for special mention, and denoted by the letter i. It's square is given by

$$i^2 = (0, 1)(0, 1) = (0^2 - 1^2, 0 \times 1 + 1 \times 0) = (-1, 0) = -1.$$

Also, by the defining laws of operation,

$$a + bi = (a, 0)(1, 0) + (b, 0)(0, 1) = (a, 0) + (0, b) = (a, b), \ \forall a, b \in \mathbb{R}.$$

This gives the customary expression for a complex number, in which a is its *real part*, and b its *imaginary part*. Such expressions are manipulated according to the usual operations of real numbers with the *proviso* that whenever i^2 occurs it is replaced by -1. For example, treating everything as a real number,

$$\begin{aligned}(a + bi)(c + di) &= ac + a(di) + (bi)c + (bi)(di) \\ &= ac + adi + bci + bdi^2 \\ &= ac + (ad + bc)i - ad \\ &= (ac - bd) + (ad + bc)i,\end{aligned}$$

in agreement with the definition of multiplication given at the start of this discussion. If $z = a + bi$, where a, b are real, its *complex conjugate* is defined to be $\bar{z} = a - bi$, and its *modulus* by $|z| = \sqrt{a^2 + b^2}$.

Exercise 2. *Suppose* $z, w \in \mathbb{C}$. *Prove that*

$$\overline{z + w} = \bar{z} + \bar{w}, \ \overline{zw} = \bar{z}\bar{w}, \ |z| = \sqrt{z\bar{z}}.$$

Remark 1. *Under the usual laws of addition and multiplication of matrices, complex numbers can be viewed as* 2×2 *matrices of the form*

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}, \ a, b \in \mathbb{R}.$$

For,

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -b-d & a+c \end{bmatrix} = \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix},$$

and

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{bmatrix} = \begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix}.$$

Remark 2. *Buoyed by his success of defining complex numbers in the above manner, Hamilton tried for many years to find a method of defining operations on triplets of real numbers* (a, b, c) *so that they could be manipulated as if they were real numbers. But he didn't succeed—in fact, no such operations can be devised. However, on October 16, 1843, on his way to Dunsink Observatory along the Royal Canal, he discovered a way of multiplying quadruples of real numbers* (a, b, c, d)*, which he wrote as* $a + bi + cj + dk$*, and called* quaternions*. Crucially, this was a non-commutative operation. He scratched the defining rules that* i, j, k *should obey on Broom Bridge. The year 2005 was designated the* Hamilton Year *by the Irish Government. The Central Bank of Ireland issued a special 10 euro coin in his honour, and An Post struck a special stamp which carried the rules of the non-commutative algebra of quaternions:*

$$i^2 = j^2 = k^2 = ijk = -1.$$

Remark 3. *Quaternions can also be thought of as* 2×2 *matrices of pairs of complex numbers of the form*

$$\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}, \; z, w \in \mathbb{C}.$$

2 Polynomials

A polynomial is a function p defined on the complex numbers $\mathbb{C}$ whose value at $z \in \mathbb{C}$ is given by a linear combination of powers of z:

$$p(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n \;\; z \in \mathbb{C}.$$

The numbers $a_0, a_1, \ldots, a_n$ attached to the various powers of z are independent of z; they are called the *coefficients* of p, and can be real or complex numbers. A polynomial is known when these are specified. The highest power of z present in the display, by which is meant that the corresponding coefficient is non-zero, is called the *degree* of p. In the polynomial p displayed, its degree is n provided that $a_n \neq 0$. Polynomials of degree 0 are constants. Those of degree 1 are called *linear polynomials*, of degree 2, *quadratic polynomials*, of degree 3, *cubic polynomials*, of degree 4, *quartic polynomials*, of degree 5, *quintic polynomials*, and so on. For short, we may refer to them as lines, quadratics, cubics, etc.

A complex number z_0 is called a *root* or *zero* of a polynomial p if its value at z_0 is zero:

$$p(z_0) = 0.$$

A polynomial all of whose coefficients are real numbers may not have any *real* roots. The simplest example is the quadratic x^2+1. This has two *complex* roots, viz., $i, -i$.

Theorem 1. *A polynomial of odd degree whose coefficients are real numbers, has at least one real root.*

Intuitive solution. Consider their graphs in the plane. For instance, the graphs of ones of degree 1 are straight lines, which consist of sets of points of the plane that lie above and below the horizontal axis, and contain a point of it. Likewise, graphs of cubics occupy regions of the plane that lie above and below the horizontal axis. Since these regions are joined (??), their union must contain a point of the real axis. Generally, if the degree of

$$p(x) = a_n x^n + \cdots + a_0$$

is odd, for all sufficiently large $x > 0$, the sign of the output $p(x)$ matches that of a_n, while if x is large and negative, $p(x)$ has the same sign as $-a_n$. Thus, p takes both positive and negative values, and being a *smooth* function it must therefore assume the value zero. In other words, it must have a real root. □

The reality of the coefficients specified in this theorem is essential. For example, the linear polynomial $x - i$ has no real root.

Theorem 2 (Gauss)**.** *Every non-constant polynomial has at least one root, which may be complex. A polynomial of degree n has at most n distinct roots.*

This deep result is called the Fundamental Theorem of Algebra. We take it for granted.

Theorem 3. *Suppose p has real coefficients and z is one of its a complex roots. Then $\bar{z}$ is also one of its roots.*

Proof. Suppose

$$p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \; x \in \mathbb{C},$$

where $a_0, a_1, \ldots, a_n$ are real numbers. Then, by repeated application of Exercise 2,

$$\begin{aligned} 0 &= \overline{p(z)} \\ &= \overline{a_0 + a_1 z + a_2 z^2 + \cdots + a_n z^n} \\ &= \overline{a_0} + \overline{a_1 z} + \overline{a_2 z^2} + \cdots + \overline{a_n z^n} \\ &= \overline{a_0} + \overline{a_1}\bar{z} + \overline{a_2}\bar{z}^2 + \cdots + \overline{a_n}\bar{z}^n \\ &= a_0 + a_1\bar{z} + a_2\bar{z}^2 + \cdots + \bar{z}^n \\ &= p(\bar{z}). \end{aligned}$$

Thus $p(z) = 0$ implies $p(\bar{z}) = 0$. □
Some further information about polynomials is given in an Appendix.

3 Linear and quadratic polynomials

Here, we focus on linear and quadratic polynomials whose coefficients are real numbers, and restrict their domain of definition to be the set of real numbers. We can then consider their graphs and thence examine their properties in a geometric manner. These are functions of the form

$$ax + b, \ \ ax^2 + bx + c, \ \ x \in \mathbb{R},$$

where a, b, c are real, and $a \neq 0$.

3.1 Graphs of lines

While the Greeks worked out the geometry of the straight line, they had no away of representing them in an algebraic manner. It fell to Descartes to describe a way of doing this: one introduces the cartesian plane $\mathbb{R}^2$ of points with two coordinates, a procedure with which you are familiar. Graphs of functions are then identified as subsets of this plane whose intersection with every vertical line consists of at most a single point. As a consequence, a circle is not the graph of a function, nor is the parabola $\{(x, y) \in \mathbb{R}^2 : y^2 = 4x\}$.
If $c + mx$ is a linear polynomial, its *graph* in $\mathbb{R}^2$ is the set of points

$$\{(x, y); y = mx + c, \, x \in \mathbb{R}\} = \{(x, mx + c) : x \in \mathbb{R}\},$$

which is abbreviated to $y = mx + c$; m is its slope, and c its y-intercept.
Given two distinct points (x_1, y_1), (x_2, y_2) in its graph, so that

$$y_1 = mx_1 + c, \ \ y_2 = mx_2 + c,$$

in which case $x_2 \neq x_1$, we can solve these equations for m, c and, doing so, find that

$$m = \frac{y_2 - y_1}{x_2 - x_1}, \ \ c = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

Substituting these into the equation, and rearranging the resulting expression, we obtain the familiar formula for the equation of a line through two points which are not on the same vertical line:

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1).$$

Equivalently in this case,

$$(x_2 - x_1)(y - y_1) = (y_2 - y_1)(x - x_1).$$

But this formula works even if $x_2 = x_1$, provided that $y_2 \neq y_1$; or if $y_2 = y_1$ and $x_2 \neq x_1$. But we can't have $y_2 - y_2 = x_2 - x_1 = 0$ unless we wish to regard the entire plane as a line!
To cover all possibilities, then, the equation of a line in $\mathbb{R}^2$ is an expression of the form

$$ax + by + c = 0,$$

where $a^2 + b^2 > 0$. This is the graph of a linear polynomial iff $ab \neq 0$. It is the graph of a constant polynomial if $a = 0, b \neq 0$.

3.2 Distance formula

Various candidates present themselves that qualify as a 'distance' between a pair of points $P = (x_1, y_1)$, $Q = (x_2, y_2)$. The usual one—which you'll recognise—is given by

$$|PQ| \equiv d_2(P,Q) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}.$$

Another one—called the taxi-cab metric—is given by

$$d_1(P,Q) = |x_2 - x_1| + |y_2 - y_1|.$$

An even simpler one is given by

$$d_0(P,Q) = \begin{cases} 1, & \text{if } P \neq Q, \\ 0, & \text{if } P = Q. \end{cases}$$

If, for the moment, d is any one of these, L is a straight line, and $P_0 = (x_0, y_0)$ is any point, is there a point R in L which is 'nearest' to P_0? If so, is it unique? In other words, does there exist a point $R \in L$ such that

$$d(P_0, R) \leq d(P_0, X), \ \forall X \in L,$$

and, if so, is it unique?
This is an example of what's called an Existence and Uniqueness Problem, and possibly the first one of its kind that is encountered in second level mathematics. If $d = d_2$, the answer to both questions is in the affirmative, as you know: the foot of the perpendicular from P_0 onto L is the point that is nearest to P_0 in this metric. If $L = \{(x,y) : ax + by + c = 0,\ a^2 + b^2 > 0\}$, then

$$R = (\frac{ac - aby_0 + b^2x_0}{a^2 + b^2}, \frac{bc + a^2y_0 - abx_0}{a^2 + b^2}),$$

and

$$|P_0R| = \frac{|ax_0 + by_0 - c|}{\sqrt{a^2 + b^2}}.$$

However, by contrast, while the answer to the first question is still in the affirmative if we measure distance using either d_0 or d_1, we lose uniqueness. For instance, if we use d_0, then the distance between every point in L and P_0 is 1, unless $P_0 \in L$, in which case the distance between them is 0, and $R = P_0$.

Exercise 3. *Work out a solution to the problem when d_1 is used.*

Exercise 4. *Show that if P, Q, R are three points in the plane, then*

$$d_1(P,Q) \leq d_1(P,R) + d_1(R,Q).$$

3.3 Heron's problem

Given two distinct points P, Q on the same side of a line L, is there a point $R \in L$ such that

$$|PR| + |RQ| \leq |PX| + |XQ|, \ \forall X \in L?$$

This is another Existence and Uniqueness Problem that was first considered by Heron[1] who gave a beautiful solution based on the notion of the reflection of a point in a line. (Recall that P' is the reflection of P in L if both points are equidistant from L, and their mid-point belongs to L.)

Theorem 4 (Heron)**.** *Given two distinct points P, Q on the same side of a line L, there is a unique point $R \in L$ such that*

$$|PR| + |RQ| \leq |PX| + |XQ|, \ \forall X \in L.$$

Proof. Let P' be the reflection of P in L, so that if $X \in L$, then $|PX| = |P'X|$. Join P' and Q. The line M passing through these points meets L at the desired point R. For

$$\begin{aligned} |PX| + |XQ| &= |P'X| + |XQ| \ \text{(by reflection)} \\ &\geq |P'Q| \ \text{(by the triangle inequality)} \\ &= |P'R| + |RQ| \ \text{(since } R \in M \cap L) \\ &= |PR| + |RQ| \ \text{(again by reflection).}\square \end{aligned}$$

This result incorporates Heron's Principle of the Shortest Path of Light: If a ray of light propagates from point A to point B within the same medium, the path-length followed is the shortest possible.

Remark 4. *Snooker players use this fact instinctively!*

3.4 Graphs of quadratics

The simplest quadratic is the square function $x \to x^2$, whose graph in $\mathbb{R}^2$ is given by the set

$$\{(x, y) : y = x^2 : x \in \mathbb{R}\}.$$

This is a subset in the upper half-plane that is symmetric about the vertical axis, and the origin is the lowest point on it, which is its only 'turning point'. Also, the square function is convex.i.e., it is a smile. To see this, let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ be two distinct points on its graph, so that $y_1 = x_1^2, y_2 = x_2^2$. The line through P

[1] Heron (or Hero) of Alexandria (c. 10 70 AD) was a mathematician and engineer, who is said to be the greatest experimenter of antiquity. For instance, he is credited with inventing a vending machine to dispense water, and a windwheel to operate an organ.

and Q has equation

$$\begin{aligned} y &= y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) \\ &= x_1^2 + \frac{x_2^2 - x_1^2}{x_2 - x_1}(x - x_1) \\ &= x_1^2 + (x_2 + x_1)(x - x_1) \\ &= (x_2 + x_1)x - x_1 x_2. \end{aligned}$$

Thus, the line PQ lies above the arc $\widehat{PQ}$ since

$$x^2 - (x_2 + x_1)x + x_1 x_2 = (x - x_1)(x - x_2) \leq 0,$$

for all x between x_1, x_2, i.e.,

$$x^2 \leq (x_2 + x_1)x - x_1 x_2,$$

for all x between x_1, x_2, as required.
The square function separates the plane into two disjoint regions, viz., the sets of points above and below its graph. The set above it is $\{(x, y) : y > x^2\}$; the set below is $\{(x, y) : y > x^2\}$. The upper set is convex: the line segment joining any two of its points is wholly contained in it. The lower set is neither convex nor concave.
The graph of any quadratic can be reduced to that of the square function or to its reflection in the horizontal axis, by a process known as 'completing the square'.
To justify this, suppose

$$p(x) = ax^2 + bx + c$$

is a quadratic polynomial, so that $a \neq 0$. Then, if (x, y) is a point in its graph,

$$\begin{aligned} y &= ax^2 + bx + c \\ &= a(x^2 + \frac{b}{a}x) + c \\ &= a(x^2 + \frac{b}{2a}x + \frac{b^2}{4a^2}) + c - a\frac{b^2}{4a^2} \\ &= a(x + \frac{b}{2a})^2 + \frac{4ac - b^2}{4a}. \end{aligned}$$

Thus

$$y - \frac{4ac - b^2}{4a} = a(x + \frac{b}{2a})^2,$$

Or, changing the coordinate axes by translating the origin, we have $Y = aX^2$, where

$$Y = y - \frac{4ac - b^2}{4a}, \; X = x + \frac{b}{2a}.$$

Hence, the graph is convex, i.e., a smile if $a > 0$, and concave, i.e., a frown, if $a < 0$.

We can also conclude that the graph of p is symmetric about the line $x = -\frac{b}{2a}$, and that it has a single turning point at $(-\frac{b}{2a}, \frac{4ac-b^2}{4a})$. Moreover, this is a minimum point if $a > 0$, and a maximum point if $a < 0$, i.e.,

$$p(x) \begin{cases} \geq \frac{4ac-b^2}{4a}, & \text{if } a > 0, \\ \leq \frac{4ac-b^2}{4a}, & \text{if } a < 0, \end{cases}$$

with equality here iff $x = -\frac{b}{2a}$. In other words,

$$\min\{p(x) : x \in \mathbb{R}\} = \frac{4ac - b^2}{4a}$$

if $a > 0$, and

$$\max\{p(x) : x \in \mathbb{R}\} = \frac{4ac - b^2}{4a}$$

if $a < 0$.

Example 1. *If a, b, c are real numbers, and $a \neq 0$, then*

$$p(x) = ax^2 + bx + c \geq 0, \ \forall x \in \mathbb{R},$$

iff $a > 0, c \geq 0$ and $b^2 \leq 4ac$. These conditions hold iff p is the square of the modulus of a linear polynomial.

Proof. Suppose $p \geq 0$ on $\mathbb{R}$. Then, in particular, $c = p(0) \geq 0$. Next, for $x \neq 0$,

$$a + \frac{b}{x} + \frac{c}{x^2} = p(x)\frac{1}{x^2} \geq 0,$$

and so, letting $x \to \infty$, we deduce that $a \geq 0$. But, $a \neq 0$. Hence, $a > 0$, so that

$$\frac{4ac - b^2}{4a} = p(-\frac{b}{2a}) \geq 0,$$

whence $b^2 \leq 4ac$. Thus the stated conditions are necessary to ensure the nonnegativity of p. Conversely, if they hold, then, by completing the square, we see that

$$p(x) = a(x + \frac{b}{2a})^2 + \frac{4ac - b^2}{4a} \geq \frac{4ac - b^2}{4a} \geq 0, \ \forall x \in \mathbb{R},$$

from which it also follows that p is the square of the modulus of the linear polynomial

$$\sqrt{a}x + \frac{b + \sqrt{4ac - b^2}i}{2\sqrt{a}}$$

which has complex coefficients.□

Example 2. *The pairs of real numbers (m, c) such that $y = mx + c$ is a line below the graph of the square function comprise the set*

$$\{(m, c) : m^2 + 4c \leq 0\}.$$

Proof. Suppose (m, c) generates such a line. Then

$$mx + c \leq x^2, \ \forall x \in \mathbb{R}.$$

Equivalently, the quadratic polynomial $x^2 - mx - c$ is nonnegative for all real x. By the previous example, this occurs iff $m^2 \leq 4(-c)$. The result follows. □

4 Exercises

1. Sketch the graphs of the polynomials

   $$-3x+2, \ 2x-3, \ -3x^2+4x-2, \ 3x^2+4x-2, \ (x-\alpha)(x-\beta), \ -(x-\alpha)(x-\beta),$$

   where α, β are arbitrary real numbers.

2. Determine the minimum of each of the quadratics

   $$(x-1)(x-2), \ (x-3)(x-4), \ (x-1)(x-3), \ (x-2)(x-4).$$

3. Determine the minimum of the quadratic

   $$(x-1)^2 + (x-2)^2 + (x-3)^2 + (x-4)^2.$$

4. Determine the minimum of the quadratic

   $$a(x-\alpha)^2 + b(x-\beta)^2 + c(x-\gamma)^2,$$

   where $a, b, c, \alpha, \beta, \gamma$ are arbitrary real numbers, and at last one of a, b, c is non-zero.

5. Determine the minimum of each of the quartics

   $$(x-1)(x-2)(x-3)(x-4), \ (x-1)(x-2)+(x-1)(x-2)(x-3)(x-4)+(x-3)(x-4).$$

6. Let $P = (1, -1)$, $Q = (-1, 1)$. Show that there is a point R on the line L, whose equation is $x + y = 1$, such that

   $$|PR|^2 + |RQ|^2 \leq |PX|^2 + |XQ|^2, \ \forall X \in L.$$

7. Let P, Q be two points not necessarily on the same side of a line L. Prove that there is a unique point $R \in L$ such that

$$|PR|^2 + |RQ|^2 \leq |PX|^2 + |XQ|^2, \ \forall X \in L.$$

8. Let x, y be a pair of real numbers, prove that

$$x^2 + y^2 + 2 \geq (x+1)(y+1),$$

with equality iff $x = y = 1$.

9. Show that the set $\{(x, y) \in \mathbb{R}^2 : y \geq |x|\}$ is convex, and describe all the pairs (m, c) such that the line $y = mx + c$ lies below the graph of $y = |x|$.

10. Show that the semicircle $\{(x, y) : -1 \leq x \leq 1, y = -\sqrt{1 - x^2}\}$ is convex, and describe all the pairs (m, c) such that the line $y = mx + c$ lies below its graph.

11. For what real numbers $a \neq 0, b, c$ is the quadratic $ax^2 + bx + c$ nonnegative on the half-line $[0, \infty)$? On the interval $[0, 1]$?

5 Quartic polynomials

A quartic is a polynomial of degree 4, i.e., a linear combination of the simple monomials $1, x, x^2, x^3, x^4$, and is therefore of the form

$$p(x) = ax^4 + bx^3 + cx^2 + dx + e,$$

where the coefficients a, b, c, d, e are real or complex numbers, and $a \neq 0$.
Every quartic is a product of two quadratics. For, counting their multiplicity, such a polynomial has 4 roots, and if these are denoted by $\alpha, \beta, \gamma, \delta$, then

$$p(x) = a(x-\alpha)(x-\beta)(x-\gamma)(x-\delta) = a(x^2 - (\alpha+\beta)x + \alpha\beta)(x^2 - (\gamma+\delta)x + \gamma\delta),$$

a product of two quadratics, which evidently are not unique. Conversely, it's easy to see that the product of two quadratics is a quartic.

Theorem 5. *If a quartic has real coefficients, then it can be expressed as a product of two quadratics each having real coefficients.*

Proof. Suppose

$$p(x) = ax^4 + bx^3 + cx^2 + dx + e,$$

where a, b, c, d, e are real, and $a \neq 0$. The result is immediate if p has only real roots. If z is a complex root of p, then so is $\bar{z}$, by Theorem 3. Since p has at most 4 distinct roots, either they are all complex, and come in pairs, or at most two are non-real. If they are all complex, then we can write them as $\alpha, \bar{\alpha}, \beta, \bar{\beta}$, in which case

$$p(x) = a(x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha})(x^2 - (\beta+\bar{\beta})x + \beta\bar{\beta}) = a(x^2 - (\alpha+\bar{\alpha})x + |\alpha|^2)(x^2 - (\beta+\bar{\beta})x + |\beta|^2).$$

Since the coefficients of x in each factor are real numbers, the result follows in this case. If exactly two are non-real, they must be each other's complex conjugate, and so, this time, the roots can be denoted by $\alpha, \bar{\alpha}, \gamma, \delta$, where γ, δ are real numbers. As before,

$$p(x) = a(x^2 - (\alpha + \bar{\alpha})x + |\alpha|^2)(x^2 - (\gamma + \delta)x + \gamma\delta),$$

and, once more, we see that each factor has real coefficients. □

5.1 Graphs of quartics

Here, we consider quartics with real coefficients, and say a few words about their graphical representation in the cartesian plane.

The simplest quartic is $p(x) = x^4 = (x^2)^2$, whose graph is symmetric about $x = 0$ and convex; it is a large smile. Whereas the graph of every quadratic is symmetric about some vertical line, the graph of a quartic need not be symmetric about any such line. For example, the graph of the quartic $p(x) = x^4 + x$ is not symmetric about any vertical line. For, if for some real (or complex) h, $p(x + h) = p(h - x)$ for all x, then (?) every number is a root of the cubic $4hx^3 + (4h^3 + 1)x$, which is absurd.

Since x^4 is positive for all non-zero x, the sign of the general quartic $p(x) = ax^4 + bx^3 + cx^2 + dx + e$, $a \neq 0$, is the same as that of a, for all large values of x. In other words, if $a > 0$, the graph lies in the upper half-plane for all sufficiently large x; whereas, if $a < 0$, it lies in the lower half-plane for all sufficiently large x. Thus, to describe its graph completely we must examine the behaviour for all x in some symmetric interval. Thus, we need to determine its turning points, and points of inflexion, if any. These will provide information about the shape of the graph, and determine where it's convex, concave, increasing and decreasing. To do this, we must use calculus methods. The turning points, are found by finding the first and second derivative p', and solving the equation $p'(x) = 0$; the points of inflexion are found by determining the second derivative, p'', and solving $p''(x) = 0$. Since p' has real coefficients there must be at least one turning point, but there need not be any point of inflexion. For instance, this is the case when $p(x) = x^4 + 2x^2 + 1$, which is symmetric about $x = 0$, and convex. It has no real root, only one turning point at $x = 0$, where it has a local minimum, and no point of inflexion.

5.2 Exercises

1. Let p be an arbitrary quartic. Prove that

$$p(x + h) = p(h) + p'(h)x + \frac{p''(h)x^2}{2!} + \frac{p'''(h)x^3}{3!} + \frac{p^{(iv)}(h)x^4}{4!},$$

   where $p'(h), p''(h), p'''(h), p^{(iv)}(h)$ stand for the first, second, third and fourth derivatives of p evaluated at h.

2. Let p be a arbitrary quartic. Use the previous exercise to show that we may choose h so that the coefficient of x^3 in the expansion of $p(x+h)$ is zero.

3. Suppose the roots of $p(x) = ax^4 + bx^3 + cx^2 + dx + e,\ a \neq 0$, are in arithmetic progression. Prove that $b^3 - 4abc + 8a^2d = 0$.

4. Determine the roots of $x^4 - 12x^3 + 49x^2 - 78x + 40$. Show that it's graph is symmetric about $x = 3$.

5. Show that
$$(x-1)(x-2)(x-4)(x-5) \geq -9/4,\ \forall x.$$

6. Prove that the quartic $p(x) = ax^4 + bx^3 + cx^2 + dx + e,\ a \neq 0$ has no points of inflexion iff $3b^2 < 8ac$.

6 Cubic polynomials

We consider cubics of the form
$$p(x) = ax^3 + bx^2 + cx + d,$$
where $a \neq 0$.

Theorem 6. *Suppose a, b, c, d are real numbers. Then p has at least one real root.*

Proof. We've already outlined one proof of this fact based on the fact that $ap(x)$ is positive for large positive x and negative for large negative x, a statement which extends to cover the case of any polynomial of odd degree having real coefficients. Here's another approach which uses Theorem 2 due to Gauss. According to this, every cubic (with real or complex coefficients) has at least one root, which may be complex, and at most three distinct roots. So, p has three roots, which may not all be different. Since its coefficients are real, by Theorem 3, its complex roots come in pairs. Hence, one of the roots must be real. □

As the next example shows, this is the most we can say, in general.

Example 3. *Find the roots of $p(x) = x^3 - 1$.*

Solution. Clearly 1 is a root. Hence $x - 1$ is a factor of p. In other words, there is a quadratic q such that $p(x) = (x-1)q(x)$. It's straightforward to verify that $q(x) = x^2 + x + 1$. Now, the discriminant of the latter is $b^2 - 4ac = 1 - 4 = -3$, which is negative, and so, by the usual formula, the roots of q are complex, and equal to
$$\frac{-1 \pm \sqrt{3}i}{2}.$$
Thus, p has only one real root. □

It's standard to let

$$\omega = \frac{-1+\sqrt{3}i}{2},$$

so that

$$\omega \neq 1,\ \omega^3 = 1,\ \omega^2 + \omega + 1 = 0.$$

We'll refer to this later on.

6.1 Graphs of cubics

The simples cubic is $p(x) = x^3$. This has precisely one real root, of multiplicity three. Note that its first and second derivatives vanish at $x = 0$ also. While it has a point of inflexion there, since p takes on both positive and negative values in every neighbourhood of it, 0 is neither a local maximum nor a local minimum. Since, $p(-x) - p(x)$ for all x, p is an *odd* function, which means that its graph is anti-symmetric about the y-axis. Also, $p'(x) = 3x^2 \geq 0, \forall x$, which means that the graph is strictly increasing on $(-\infty, \infty)$. In addition, the graph is convex over the interval $(0, \infty)$, and concave over $(-\infty, 0)$. Putting these facts together we can sketch the graph of $y = x^3$.

Example 4. *Discuss the graph of $y = x^3 + 3x$.*

Solution. Since $x^3 + 3x = x(x^2 + 3)$, and $x^2 + 3$ has no real root, this cubic crosses the x-axis only at 0. Next, $p'(x) = 3(x^2 + 1)$, which signifies that the cubic has no tangent parallel to the x axis. Thus it has no turning points. But since p' is everywhere positive, the graph is strictly increasing on $(-\infty, \infty)$. Finally, $p''(x) = 6x$, which vanishes only when $x = 0$. From the fact that $p''(x) > 0$ if $x > 0$, we may conclude that the graph is convex on $(0, \infty)$. Since $p''(x) < 0$ if $x < 0$, the graph is concave on $(-\infty, 0)$. □

Theorem 7. *Suppose a cubic has three real roots. Then it has two turning points.*

Proof. Suppose

$$p(x) = (x-\alpha)(x-\beta)(x-\gamma) = x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\beta\gamma+\gamma\alpha)x - \alpha\beta\gamma,$$

where α, β, γ are real. Then

$$p'(x) = 3x^2 - 2(\alpha+\beta+\gamma)x + (\alpha\beta+\beta\gamma+\gamma\alpha),$$

which has real roots iff $b^2 \geq 4ac$. Now

$$\begin{aligned} b^2 - 4ac &= 4(\alpha+\beta+\gamma)^2 - 12(\alpha\beta+\beta\gamma+\gamma\alpha) \\ &= 4[(\alpha+\beta+\gamma)^2 - 3(\alpha\beta+\beta\gamma+\gamma\alpha)] \\ &= 4[\alpha^2+\beta^2+\gamma^2 - \alpha\beta - \beta\gamma - \gamma\alpha] \\ &= 2[(\alpha-\beta)^2 + (\beta-\gamma)^2 + (\gamma-\alpha)^2] \\ &\geq 0, \end{aligned}$$

with equality iff $\alpha = \beta = \gamma$. Thus p' has two real roots, which may be equal. □

Theorem 8. *Suppose p is a cubic, not necessarily with real coefficients, and*

$$p'(\alpha) = p'(\beta) = 0 = p''(\gamma).$$

Then

$$\gamma = \frac{\alpha + \beta}{2}.$$

Proof. Suppose

$$p(x) = ax^3 + bx^2 + cx + d, \ a \neq 0.$$

Then

$$p'(x) = 3ax^2 + 2bx + c, \ p''(x) = 6ax + 2b.$$

Hence

$$\gamma = \frac{-b}{3a}.$$

But also,

$$p'(x) = 3a(x - \alpha)(x - \beta) = 3a(x^2 - (\alpha + \beta)x + \alpha\beta),$$

which means that

$$-3a(\alpha + \beta) = 2b, \ \alpha + \beta = \frac{-2b}{3a} = 2\gamma. \square$$

This means the if a cubic with real coefficients has two turning points, then the mid-point of their first coordinates coincides with the point of inflexion.

6.2 Roots of cubics

To discuss the roots of a general polynomial with real coefficients, we need to compile some preliminary facts. We start with an identity which is useful in other situations as well.

Lemma 1. *Suppose x, y, z are real or complex numbers. Then*

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

Proof. Simply expand the RHS. □

Taking $y = 1, z = 0$ we get the more familiar factorisation:

$$x^3 + 1 = (x + 1)(x^2 - x + 1),$$

while the choice $y = -1, z = 0$ tells us that

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

More generally, the identities

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2),\ x^3 - y^3 = (x - y)(x^2 + xy + y^2),$$

hold for all real or complex x, y.
Recall the definition of ω

Lemma 2. *Suppose x, y, z are real or complex numbers. Then*

$$x^2 + y^2 + z^2 - xy - yz - zx = (x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z).$$

Proof. For,

$$\begin{aligned} & (x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z) \\ = \ & x^2 + xy(\omega^2 + \omega) + xz(\omega + \omega^2) + \omega^3 y^2 + yz(\omega^2 + \omega^4) + \omega^3 z^2 \\ = \ & x^2 - xy - xz + y^2 + yz(\omega^2 + \omega) + z^2 \\ = \ & x^2 + y^2 + z^2 - xy - yz - zx. \end{aligned}$$

Combining these factorisations we deduce that, for all x, y, z,

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z).\Box$$

As an immediate consequence, we have the following statement.

Corollary 1. *The roots of the cubic polynomial*

$$p(x) = x^3 - 3abx + a^3 + b^3$$

are given by

$$-(a + b),\ -(\omega a + \omega^2 b), -(\omega^2 a + \omega b).$$

We can exploit this to determine the roots of cubic polynomials of the form x^3+qx+r, as long as we can find a, b so that

$$-3ab = q,\ a^3 + b^3 = r. \tag{1}$$

Before discussing the general case, we look at a simple example.

Example 5. *Determine the roots of $p(x) = x^4 + 3x^2 - 3x + 4$.*

Solution. The first step is the eliminate the x^2 term. We can do this by shifting the x-axis. Noting that

$$p(x) = (x + 1)^3 - 6x + 3 = (x + 1)^3 - 6(x + 1) + 9,$$

its enough to find the roots of $X^3 - 6X + 10$. So, choose a, b so that

$$2 = ab,\ a^3 + b^3 = 9.$$

Plainly, the pair $a=1, b=2$ works. Hence,

$$X^3-6X+10=(X+3)(X+\omega+2\omega^2)(X+\omega^2+2\omega)=(X+3)(X-1+\omega^2)(X-1+\omega).$$

In other words,

$$p(x)=(x+4)(x+\omega^2)(x+\omega)$$

and $-4, -\omega, -\omega^2$ are the roots of p.
Return to (1). For these relations to hold, a^3, b^3 must be the roots of the quadratic

$$z^2-rz-\frac{q^3}{27},$$

and so can be determined by the usual formula,

$$a^3, b^3=\frac{r\pm\sqrt{r^2+\frac{4q^3}{27}}}{2}.$$

So, a, b can be determined by extracting cube roots of possibly complex numbers. We could, for instance, choose a to be one of the cube roots of

$$\frac{r+\sqrt{r^2+\frac{4q^3}{27}}}{2},$$

something we gloss over.
Turning to the determination of the roots of a general cubic $p(x)=ax^3+bx^2+cx+d$, $a\neq 0$, since the roots don't depend on the sign of a, we can suppose, for simplicity, that $a=1$. The first step to perform is to eliminate the term involving x^2 by shifting x. In fact,

$$\begin{aligned}
x^3+bx^2+cx+d &= (x+\frac{1}{3}b)^2-\frac{1}{3}b^2x-\frac{b^3}{27}+cx+d\\
&= (x+\frac{1}{3}b)^2+(c-\frac{1}{3}b^2)(x+\frac{1}{3}b)-\frac{b^3}{27}-(c-\frac{1}{3}b^2)(\frac{1}{3}b)+d\\
&= X^3+(c-\frac{1}{3}b^2)X+d-\frac{1}{3}bc+\frac{2b^3}{27}\\
&= X^3+qX+r,
\end{aligned}$$

where

$$X=x+\frac{1}{3}b,\ q=c-\frac{1}{3}b^2,\ r=d-\frac{1}{3}bc+\frac{2b^3}{27}.$$

Next we select a, b so that

$$-3ab=q,\ a^3+b^3=r;$$

this entails solving the quadratic equation $z^2-rz-q^3/27=0$. The final step is to use the factorisation in the above Corollary.

6.3 Exercises

1. Determine the roots of the cubic $x^3 - (a^2 + ab + b^2)x + ab(a + b)$.

2. Suppose $x_1 \neq x_2$ and $y_i = x_1^3, y_2 = x_2^3$. Write down the equation of the line through the points $(x_1, y_1), (x_2, y_2)$ and prove that it cuts the graph of $y = x^3$ at three points, two of which may coincide.

3. Prove that the cubic $y = x^3$ is convex on $(0, \infty)$, and concave on $(-\infty, 0)$.

7 Appendix

This contains additional information about polynomials and some IMO-type problems.

7.1 Some more facts

1. The collection of polys is closed under addition, multiplication and composition. In other words, if

$$p(x) = a_0 + a_1x + \cdots + a_nx^n, q(x) = b_0 + b_x + \cdots + b_mx^m,$$

are polys of degree n, m then $p + q$, pq, $p \circ q$, $q \circ p$ are polys and

$$\deg(p+q) \leq \max(\deg p, \deg q),\ \deg(pq) = m+n,\ \deg(p\circ q) = \deg(q\circ p) = mn.$$

2. The following are special polynomials. Let a be a fixed complex number and $n \in \mathbb{N}$:

$$x^n - a^n,\ \sum_{k=0}^{n-1} x^{n-k+1}a^k,\ \sum_{k=0}^{n} \binom{n}{k} x^{n-k}a^k,$$

where

$$\binom{n}{k} = \begin{cases} \frac{n!}{(n-k)!k!}, & \text{if } 0 \leq k \leq n, \\ 0, & \text{if } k < 0 \text{ or } k > n \end{cases}$$

are the Binomial coefficients.

Note that

$$x^n - a^n = (x - a)\sum_{k=0}^{n-1} x^{n-k+1}a^k,\ (x + a)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}a^k,$$

3. a is root (zero) of a poly p if $p(a) = 0$. If this is so, then we can factor p: there is a poly q, with $\deg q = \deg p - 1$, such that

$$p(x) = (x - a)q(x).$$

Note especially that if a is rational and all the coeffs of p are rational, then the coeffs of q are also rational.

If b is another root of p, then $q(b) = 0$, and so we can factor q: $q(x) = (x-b)r(x), \deg r = \deg q - 1$. Thus $p(x) = (x-a)(x-b)r(x)$, and so on: if $x_1, x_2, \ldots, x_n$ are roots of p, then

$$p(x) = c(x-x_1)(x-x_2)\cdots(x-x_n) = c\prod_{i=1}^{n}(x-x_i).$$

4. Suppose p/q, with $p, q \in \mathbb{Z}, (p,q) = 1, q \neq 0$, is a rational root of a poly $p(x) = a_n x^n + \cdots + a_0$ whose coeffs are integers. Then $p|a_0$, $q|a_n$.

   This is another theorem due to Gauss. It reduces the search for rational roots of polys with integer coeffs to an examination of a finite number of possibilities which arise by factorising the integers a_0, a_n.

5. How are the roots of a poly related to its coeffs? If ax^2+bx+c is a quadratic, so that $a \neq 0$, and its roots are x_1, x_2, then

   $$ax^2+bx+c = a(x-x_1)(x-x_2) = a(x^2-(x_1+x_2)x+x_1x_2,$$

   whence

   $$x_1+x_2 = -\frac{b}{a},\ x_1x_2 = \frac{c}{a}.$$

   If ax^3+bx^2+cx+d is a cubic, so that $a \neq 0$, and its roots are x_1, x_2, x_3, then

   $$\begin{aligned} ax^3+bx^2+cx+d &= a(x-x_1)(x-x_2)(x-x_3) \\ &= a(x^3-(x_1+x_2+x_3)x+(x_1x_2+x_2x_3+x_3x_1)x-x_1x_2x_3), \end{aligned}$$

   whence

   $$x_1+x_2+x_3 = -\frac{b}{a},\ x_1x_2+x_2x_3+x_3x_1 = \frac{c}{a},\ x_1x_2x_3 = -\frac{d}{a}.$$

   Similar relations hold for higher degree polynomials.

6. The poly $x^n - 1$ has roots $\omega^k, k = 0, 1, 2, \ldots, n$ where

   $$\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) = e^{\frac{i2\pi}{n}}.$$

   Thus

   $$x^n - 1 = \prod_{k=0}^{n-1}(x-\omega^k),$$

   so that, if x is a real number, then

   $$|x^n-1|^2 = \prod_{k=0}^{n-1}(x^2-2x\cos(\frac{2k\pi}{n})+1).$$

The complex number ω, which depends on n, is never equal to 1, unless $n = 1$; it is called an nth root of unity. Its powers $1, \omega, \omega^2, \ldots, \omega^{n-1}$ are also roots of $x^n - 1$, and form a cyclic group under multiplication. They are also the vertices of a regular n-gon inscribed in the unit circle. The perimeter of this n-gon is given by

$$\sum_{k=1}^{n} |\omega^k - \omega^{k-1}| = n|1-\omega| = 2n\sin(\frac{\pi}{n}),$$

which tends to 2π as $n \to \infty$.

7.2 Some identities

If

$$p(x) = \sum_{i\geq 0} a_i x^i, \; q(x) = \sum_{j\geq 0} b_j x^j$$

are two polys of degrees m, n, their product is also a poly of degree $m+n$, and

$$\begin{aligned} p(x)q(x) &= \sum_{i\geq 0} a_i x^i \sum_{j\geq 0} b_j x^j \\ &= \sum_{i,j\geq 0} a_i b_j x^{i+j} \\ &= \sum_{k\geq 0} \sum_{i+j=k} a_i b_j x^{i+j} \\ &= \sum_{k\geq 0} c_k x^k, \end{aligned}$$

where

$$c_k = \sum_{i+j=k} a_i b_j = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0, \; k = 0, 1, \ldots, m+n.$$

For instance, if $p(x) = (1+x)^m, q(x) = ax^2 + bx + c$, then

$$\begin{aligned} (1+x)^m(ax^2+bx+c) &\equiv (\sum_{i=0}^{m} \binom{m}{i} x^i)\,(b_0 + b_1 x + b_2 x^2) \\ &= \sum_{k=0}^{m+2} x^k \sum_{i+j=k, j\leq 2} \binom{m}{i} b_j \\ &= \sum_{k=0}^{m+2} x^k \sum_{0\leq j\leq 2} \binom{m}{k-j} b_j = \sum_{k=0}^{m+2} c_k x^k, \end{aligned}$$

where

$$c_0 = b_0 = c, \; c_1 = \binom{m}{1} b_0 + \binom{m}{0} b_1 = mc + b,$$

and, for $k \geq 2$,

$$c_k = \binom{m}{k} b_0 + \binom{m}{k-1} b_1 + \binom{m}{k-2} b_2 = \binom{m}{k} c + \binom{m}{k-1} b + \binom{m}{k-2} a.$$

Again,

$$\begin{aligned} (\sum_{i=0}^{m} \binom{m}{i} x^i)(\sum_{j=0}^{n} \binom{n}{j} x^j) &= (1+x)^m (1+x)^n \\ &= (1+x)^{m+n} \\ &= \sum_{k=0}^{m+n} \binom{m+n}{k} x^k, \end{aligned}$$

and comparing coeffs of powers of x,

$$\binom{m+n}{k} = \sum_{i+j=k} \binom{m}{i} \binom{n}{j}, \ k = 0, 1, 2 \ldots, m+n.$$

In particular, if $k = m = n$

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2.$$

Since $(1-x^2)^n = (1+x)^n (1-x)^n$, we see in the same way that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} x^{2k} = \sum_{i=0}^{n} \binom{n}{i} x^i \sum_{j=0}^{n} (-1)^j \binom{n}{j} x^j = \sum_{k=0}^{2n} x^k \sum_{i+j=k} \binom{n}{i} (-1)^j \binom{n}{j},$$

whence

$$\sum_{i+j=k} \binom{n}{i} (-1)^j \binom{n}{j} = \begin{cases} 0, & \text{if } k \text{ is odd,} \\ (-1)^{k/2} \binom{n}{k/2}, & \text{if } k \text{ is even.} \end{cases}$$

In particular,

$$\sum_{i=0}^{2m+1} \binom{2(2m+1)}{i} (-1)^i \binom{2(2m+1)}{2m+1-i} = 0, \ m = 0, 1, 2, \ldots$$

and

$$\sum_{i=0}^{2m} \binom{4m}{i} (-1)^i \binom{4m}{2m-i} = (-1)^m \binom{4m}{m}, \ m = 0, 1, 2, \ldots$$

7.3 Interpolation

As we've mentioned, if we know the roots of a poly and their multiplicities, we can determine the poly to within a constant multiple. What if we know the values that a poly takes on a prescribed set? Can we determine it? In geometric terms, can we always find a poly of smallest degree to pass through a finite set of points in the (x, y)-plane? Since a poly is a function, the x-coordinates of the points better be distinct, but the y-coordinates don't have to be.

Example 6. *Suppose x_1, x_2, x_3 are three distinct real numbers and y_1, y_2, y_3 are any given set of real numbers, determine the equation of the poly that passes through the points*

$$(x_1, y_1), (x_2, y_2), (x_3, y_3).$$

Let the desired poly be $p(x) = ax^2 + bx + c$. Then $p(x_i) = y_i$, $i = 1, 2, 3$, i.e.,

$$\begin{aligned} ax_1^2 + bx_1 + c &= y_1, \\ ax_2^2 + bx_2 + c &= y_2, \\ ax_3^2 + bx_3 + c &= y_3, \end{aligned}$$

three equations for three unknowns a, b, c, which can be solved by the process of elimination. □

Another approach is to solve three similar, but easier problems by letting two of the y's be 0 and the other 1. Then, say, $p_1(x_2) = p_1(x_3) = 0, p_1(x_1) = 1$. The first two conditions say that x_2, x_3 are roots of the quadratic p_1. So

$$p_1(x) = a(x - x_2)(x - x_3).$$

The third condition now fixes a and so p_1 :

$$a = \frac{1}{(x_1 - x_2)(x_1 - x_3)}, \; p_1(x) = \frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)}.$$

Cycling the points x_1, x_2, x_3 we determine p_2, p_3 as

$$p_2(x) = \frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)}, \; p_3(x) = \frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}.$$

Then

$$p(x) = y_1 p_1(x) + y_2 p_2(x) + y_3 p_3(x)$$

solves the problem.
This can be extended to deal with the general problem of finding a poly of degree n that passes through $n + 1$ points (x_i, y_i), $i = 1, 2, \ldots, n$ with distinct x-coordinates.

7.4 Some Olympiad style problems

1. The value of the polynomial x^2+x+41 is a prime number for $x = 0, 1, 2, \ldots, 39$. The value of the polynomial $x^2 - 81x + 1681$ is a prime number for $x = 0, 1, 2, \ldots, 80$. These examples might suggest that there is a poly p, with integer coeffs, such that $p(n)$ is a prime for every integer $n \geq 0$. This is false. *No such poly exists.* [Hint: If such a poly f exists, $p = f(0)$ is a prime and $p|f(mp), m = 0, 1, \ldots$, i.e., Hence $f(mp) = p, m = 0, 1, 2, \ldots$, which is absurd.]

2. For which $n \in \mathbb{N}$ is x^2+x+1 a factor of $x^{2n}+x^n+1$? [Hint: Say $x^{2n}+x^n+1 = (x^2+x+1)q(x)$, for some poly q.]

3. (IMO 1973) Find the minimum value of a^2+b^2, where a, b are real numbers for which the equation

$$x^4 + ax^3 + bx^2 + ax + 1 = 0$$

has at least one real root.

4. USAMO75. Let p be a poly of degree n and suppose that

$$p(k) = \frac{k}{k+1}, \quad k = 0, 1, 2, \ldots, n.$$

Determine $p(n+1)$. [Hint: Consider the poly $q(x) = (x+1)p(x) - x$.]

5. IRMO89. Let a be a positive real number, and let

$$b = \sqrt[3]{a + \sqrt{a^2+1}} + \sqrt[3]{a - \sqrt{a^2+1}}.$$

Prove that b is a positive integer if, and only if, a is a positive integer of the form $\frac{1}{2}n(n^2+3)$, for some positive integer n.

6. IRMO91. Find all polynomials

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

satisfying the equation

$$f(x^2) = (f(x))^2$$

for all real numbers x.

7. IRMO91. Find all polynomials

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

with the following properties:

(a) all the coefficients $a_1, a_2, \ldots, a_n$ belong to the set $\{-1, 1\}$

(b) all the roots of the equation

$$f(x) = 0$$

are real.

8. Let a, b, c and d be real numbers with $a \neq 0$. Prove that if all the roots of the cubic equation
$$az^3 + bz^2 + cz + d = 0$$
lie to the left of the imaginary axis in the complex plane, then
$$ab > 0,\ bc - ad > 0,\ ad > 0.$$

9. IRMO93. The real numbers α, β satisfy the equations
$$\alpha^3 - 3\alpha^2 + 5\alpha - 17 = 0,$$
$$\beta^3 - 3\beta^2 + 5\beta + 11 = 0.$$
Find $\alpha + \beta$.

10. IRMO93. Let $a_0, a_1, \ldots, a_{n-1}$ be real numbers, where $n \geq 1$, and let the polynomial
$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$$
be such that $|f(0)| = f(1)$ and each root α of f is real and satisfies $0 < \alpha < 1$. Prove that the product of the roots does not exceed $1/2^n$.

11. IRMO93. Let $a_1, a_2 \ldots a_n, b_1, b_2 \ldots b_n$ be $2n$ real numbers, where $a_1, a_2 \ldots a_n$ are distinct, and suppose that there exists a real number α such that the product
$$(a_i + b_1)(a_i + b_2) \ldots (a_i + b_n)$$
has the value α for $i = 1, 2, \ldots, n$. Prove that there exists a real number β such that the product
$$(a_1 + b_j)(a_2 + b_j) \ldots (a_n + b_j)$$
has the value β for $j = 1, 2, \ldots, n$.

12. IRMO94. Determine, with proof, all real polynomials f satisfying the equation
$$f(x^2) = f(x)f(x-1),$$
for all real numbers x.

13. IRMO95. Suppose that a, b and c are complex numbers, and that all three roots z of the equation

$$x^3 + ax^2 + bx + c = 0$$

satisfy $|z| = 1$ (where $|\ |$ denotes absolute value). Prove that all three roots w of the equation

$$x^3 + |a|x^2 + |b|x + |c| = 0$$

also satisfy $|w| = 1$.

14. IRMO97. Find all polynomials p satisfying the equation

$$(x - 16)p(2x) = 16(x - 1)p(x)$$

for all x.

15. Prove that $x^4 + x^3 + x^2 + x + 1$ is a factor of $x^{44} + x^{33} + x^{22} + x^{11} + 1$.

16. The coeffs of the cubic $ax^3 + bx^2 + cx + d$ are integers, ad is odd and$bc$is even. Prove that at least one root is irrational.

17. USAMO77. Suppose a, b are two roots of $x^4 + x^3 - 1$. Prove that ab is a root of $x^6 + x^4 + x^3 - x^2 - 1$.

18. Prove that if $x^3 + px^2 + qx + r$ has three real roots, then $p^2 \geq 3q$.

19. IMO93. Let $n > 1$. Show that the poly $x^n + 5x^{n-1} + 3$ cannot be written as a product of two non-constant polys with integer coeffs.

20. The coeffs of $p(x) = x^n + \cdots + 1$ are ≥ 0. Assume p has real roots. Prove that

$$p(2) \geq 3^n.$$

8 Some more facts about cubics

1. Suppose $f(x) = ax^3 + bx^2 + cx + d$ is a cubic poly with a, b, c, d real numbers and $a \neq 0$. For $x \neq 0$,

$$\frac{f(x)}{x^3} = a + \frac{b}{x} + \frac{c}{x^2} + \frac{d}{x^3}$$

and, apart from the first, the terms are small for large $|x|$. Precisely,

$$\lim_{|x| \to \infty} \frac{f(x)}{x^3} = a.$$

This means that for large $|x|$, $f(x)/x^3$ has the same sign as a. Hence, supposing $a > 0$, $f(x) > 0$ if $x > 0$ is large enough, and $f(x) < 0$ if $x < 0$ and $|x|$ is large enough. (If $a < 0$, then $xf(x) < 0$ if $|x|$ is large enough.) Hence, by the Intermediate-value theorem, the graph of $y = f(x)$ crosses the real axis at some point. Conclusion: f has at least one real roots.

Note that this is false without the assumption that the coeffs a, b, c, d are real. For instance, $x^3 - 3ix^2 - 3x - i = (x - i)^3$ has no real roots.

Notice too that the same reasoning applies to confirm that any poly of *odd* degree that has real coeffs has at least one real root.

2. The previous statement tells us that a cubic with real coeffs has at least one real root; the other roots may be complex numbers, and if they are, they are each other's complex conjugate, once more from the reality of the coeffs.

   Is there a formula for finding the roots? To answer this, we begin by reducing the general cubic to *normal form.* First divide across by a, obtaining a cubic which has the same roots as f. Renaming the coeffs, if necessary, we may as well suppose that $a = 1$, thereby getting a monic poly of the form $f(x) = x^3 + bx^2 + cx + d$. Now we seek another cubic which has no term involving x^2, using a procedure similar to completing the square in a quadratic. Consider

$$\begin{aligned} f(x+t) &= (x+t)^3 + b(x+t)^2 + c(x+t) + d \\ &= x^3 + (3t+b)x^2 + (3t^2 + 2bt + c)x + t^3 + bt^2 + ct + d \\ &= x^3 + \frac{f''(t)}{2}x + f'(t)x + f(t). \end{aligned}$$

   Now choose t so that $f''(t) = 3t + b = 0$ and let $q = f'(t), r = f(t)$. Then

$$f(x+t) = x^3 + qx + r.$$

   This is the normal form.

   (As a general principle, it is often a very good idea to convert a cubic to normal form, just as completing the square in a quadratic is often a good idea.) Observe, too, that x_0 is a root of f iff $x_0 - t$ is a root of the reduced form of f.

3. From now on we deal with a cubic in its the normal form $x^3 + qx + r$. We can proceed in two directions to solve this. Using the method previously suggested we can 'let' $q = -3uv, r = u^3 + v^3$ and then use the factorization

$$x^3 + qx + r = x^3 + u^3 + v^3 - 3uvx = (x + u + v)(x^2 - (u+v)x + u^2 + v^2 - uv),$$

   to confirm that $-(u+v)$ is one root and the other two are roots of the quadratic $x^2 - (u+v)x + u^2 + v^2 - uv$. Thus, we're down to solving the pair of equations

$q = -3uv, r = u^3 + v^3$ for u, v. It's easy to see that u^3, v^3 must be the roots of the quadratic equation.

$$z^2 - rz - \frac{q^3}{27} = 0.$$

Hence,

$$u^3, v^3 = \frac{r \pm \sqrt{r^2 + \frac{4q^3}{27}}}{2}.$$

So, let u be a cube root of one of these and let $v = -q/(3u)$. Then $-(u+v)$ is a root, possibly complex, of $x^3 + qx + r$. Having selected one cube root u of $(r + \sqrt{r^2 + \frac{4q^3}{27}})/2$, say, and setting $v = -q/3u$, the remaining roots can then be found by solving $x^2 - (u+v)x + u^2 + v^2 - uv = 0$, or by figuring out the other cube roots of $(r + \sqrt{r^2 + \frac{4q^3}{27}})/2$.

Notice that u^3 is real iff $27r^2 + 4q^3 \geq 0$. So, if this condition is satisfied, then $-(u+v)$ is a real root—possibly the only real root, as the following example shows. (In fact, it's not too hard to see that if $27r^2 + 4q^3 > 0$ holds, then $-(u+v)$ is the only real root of the cubic. What may happen if $27r^2 + 4q^3 = 0$?)

Example 7. *Solve* $x^3 + 3x + 1 = 0$.

Solution. For this, $uv = -1$, and u^3, v^3 are roots of $z^2 - z - 1 = 0$. So,

$$u^3, v^3 = \frac{1 \pm \sqrt{5}}{2}.$$

Say $u = \sqrt[3]{\frac{1+\sqrt{5}}{2}}$. Then (?) $v = \sqrt[3]{\frac{1-\sqrt{5}}{2}}$, and so

$$-\sqrt[3]{\frac{1+\sqrt{5}}{2}} - \sqrt[3]{\frac{1-\sqrt{5}}{2}}$$

is a real root of $x^3 + 3x + 1$. The remaining roots are given by

$$\frac{(u+v) \pm \sqrt{(u+v)^2 - 4(u^2 + v^2 - uv)}}{2} = \frac{(u+v) \pm \sqrt{3}i(u-v)}{2},$$

and are complex numbers.

4. The last remark raises an interesting question: what conditions on the coeffs q, r guarantee that *all* three roots of x^3+qx+r are real? To see what's involved, let a, b, c be the real roots of this cubic. Then $a + b + c = 0, ab + bc + ca = q, abc = -r$. Hence $r^2 = a^2b^2c^2$. Since the geometric mean of positive numbers doesn't exceed their arithmetic mean, we see that

$$\sqrt[3]{r^2} \leq \frac{a^2 + b^2 + c^2}{3} = \frac{(a+b+c)^2 - 2(ab + bc + ca)}{3} = \frac{-2q}{3}.$$

Hence $q \leq 0$ and

$$27r^2 + 8q^3 \leq 0$$

are *necessary* conditions for the cubic to have three real roots.

(This is an algebraic approach. What does a geometric approach suggest?)

5. Are these conditions *sufficient* In other words, if they hold, will x^3+qx+r have three real roots? (Answer: not necessarily; consider $2x^3 - 3x + 1$.) Suppose $q \leq 0$ to begin with, and see what effect this has on the shape of the graph of $y = x^3 + qx + r$. (It will help you to visualise the shape of such a cubic.) The graph has two turning points given by $x = \pm\sqrt{-q/3}$. The corresponding y values are

$$\pm\frac{2q}{3}\sqrt{\frac{-q}{3}} + r.$$

The smallest of these is

$$\frac{2q}{3}\sqrt{\frac{-q}{3}} + r.$$

The graph tells us that the cubic has three real roots if this is ≤ 0. This is so if

$$27r^2 \leq -4q^3.$$

In other words, the cubic has three real roots if $27r^2 + 4q^3 \leq 0$. (This implies that $q < 0$.)

This, then, is a sufficient condition, which implies the necessary condition obtained above, but the two conditions are different! Can the gap be closed between these two conditions? Is it the case, perhaps, that $27r^2 + 4q^3 \leq 0$ is true if the roots are real? To see that this is indeed the case, we revisit our attempt to derive a necessary condition assuming the roots are real. This time

$$\begin{aligned} 27r^2 + 4q^3 &= 27a^2b^2c^2 + 4(ab + bc + ca)^3 \\ &= 27a^2b^2(a + b)^2 - 4(a^2 + ab + b^2)^3 \\ &= 3a^4b^2 + 26a^3b^3 + 3a^2b^4 - 4a^6 - 12a^5b - 4b^6 - 12b^5a \\ &= -(a - b)^2(a + 2b)^2(b + 2a)^2 \\ &\leq 0. \end{aligned}$$

(Query: how did we factorize this expression? By the way, this also points up that the AM-GM inequality can sometimes be a blunt instrument.)

So, to sum up: the cubic $x^3 + qx + r$ has three real roots iff $27r^2 + 4q^3 \leq 0$. It has one real root and two complex roots iff $27r^2 + 4q^3 > 0$.

6. Here's an alternative method of solving $x^3 + qx + r = 0$ that relies on the trigonometric identity:

$$4\cos^3\theta = \cos(3\theta) + 3\cos\theta.$$

To utilize this, replace x by $\rho\cos(\theta)$ and multiply through by 4 to get

$$\rho^3\cos(3\theta) + \rho(3\rho^2 + 4q)\cos\theta + 4r = 0.$$

Now choose ρ so that $3\rho^2 + 4q = 0$. Then

$$\cos 3\theta = \frac{-4r}{\rho^3}.$$

Now solve this for θ! This is the strategy. When does it work? For the last equation to be solvable for real θ, we require ρ to be real and $-1 \leq \frac{-4r}{\rho^3} \leq 1$. Hence, we require $q \leq 0$ and $-1 \leq \frac{-4r}{\rho^3} \leq 1$ to hold, i.e., we require $27r^2 + 4q^3 \leq 0$, the same condition we encountered before that is necessary and sufficient for the roots to be real. (NB. The method can also be used even if these conditions aren't fulfilled, by allowing θ to be complex and using the fact that $\cos z = (e^{iz} + e^{-iz})/2$, which is valid for complex z. In particular, $\cos(i\theta) = (e^{\theta} + e^{-\theta})/2 = \cosh\theta$, the hyperbolic equivalent of cosine.)

9 Outline solutions to some problems on polys

1. (IMO 1973) Find the minimum value of $a^2 + b^2$, where a, b are real numbers for which the equation

$$x^4 + ax^3 + bx^2 + ax + 1 = 0$$

has at least one real root.

Solution. Denote by Γ the set of points (x, y) in the plane for which there is a real number w such that

$$w^4 + xw^3 + yw^2 + xw + 1 = 0.$$

Suppose $(x, y) \in \Gamma$. Letting

$$t = w + \frac{1}{w},\ t^2 = w^2 + \frac{1}{w^2} + 2 \geq 4,$$

we see that there is a real number t, with $|t| \geq 2$, such that

$$t^2 + xt + y - 2 = 0.$$

The reality of t requires that

$$x^2 - 4(y - 2) \geq 0,\ \forall (x, y) \in \Gamma.$$

Thus,

$$\Gamma \subset \{(x, y) : 4(y - 2) \leq x^2\}.$$

Moreover, since $t^2 \geq 4$ is a requirement,

$$\begin{aligned}(x,y) &\in \cup_{-2\leq t\leq 2}\{(x,y) : tx+y+2\leq 0\}\\ &= \{(x,y) : -2x+y+2\leq 0\}\cup\{(x,y) : 2x+y+2\leq 0\}.\end{aligned}$$

It's easily seen that the lines $-2x+y+2=0$, $2x+y+2=0$ are tangents to the parabola $x^2 = 4(y-2)$ at the points $(4,6),(-4,6)$, respectively, and intersect at $(0,-2)$. Hence

$$\{(x,y) : -2x+y+2\leq 0\}\cup\{(x,y) : 2x+y+2\leq 0\} \subset \{(x,y) : 4(y-2)\leq x^2\},$$

and so

$$\Gamma \subset \{(x,y) : -2x+y+2\leq 0\}\cup\{(x,y) : 2x+y+2\leq 0\}.$$

Plainly, equality holds here. What we seek is the square of the distance from Γ to the origin. It's clear from geometric considerations that the distance is given by the distance from the origin to one of the tangent lines, i.e., it is

$$\frac{|0+0+2|}{\sqrt{(\pm 2)^2+1}} = \frac{2}{\sqrt{5}}.$$

Hence the required minimum value is $4/5$.

2. USAMO75. Let p be a poly of degree n and suppose that

$$p(k) = \frac{k}{k+1}, \quad k = 0,1,2,\ldots,n.$$

Determine $p(n+1)$.

Consider the poly $q(x) = (x+1)p(x) - x$. Then (?)

$$q(x) = a\prod_{k=0}^{n}(x-k)$$

for some a. But $q(-1) = 1$. Hence a can be determined, whence

$$p(n+1) = \frac{(-1)^{n+1}(n+1)}{n+2}.$$

3. IRMO89. Let a be a positive real number, and let

$$b = \sqrt[3]{a+\sqrt{a^2+1}} + \sqrt[3]{a-\sqrt{a^2+1}}.$$

Prove that b is a positive integer if, and only if, a is a positive integer of the form $\frac{1}{2}n(n^2+3)$, for some positive integer n.

By direct computation it can be seen that b is a root of the cubic $x^3+3x-2a$. Hence, if b is a positive integer, then so is $2a = b^3+3b$. But the latter is even. Hence, a is a positive integer. Conversely, if a is of the form $\frac{1}{2}n(n^2+3)$, for some positive integer n, then n is also a root of the same cubic. But this cubic has only one real root. Thus $b = n$.

4. IRMO95. Suppose that a, b and c are complex numbers, and that all three roots z of the equation

$$x^3 + ax^2 + bx + c = 0$$

satisfy $|z| = 1$ (where $|\ |$ denotes absolute value). Prove that all three roots w of the equation

$$x^3 + |a|x^2 + |b|x + |c| = 0$$

also satisfy $|w| = 1$.

Denote the roots of $x^3 + ax^2 + bx + c = 0$ by p, q, r. Then

$$-a = p + q + r,\ b = pq + qr + rp,\ -c = pqr.$$

Hence $|c| = 1$, and

$$|b| = |(pqr)(\frac{1}{r} + \frac{1}{p} + \frac{1}{q})| = |\bar{r} + \bar{p} + \bar{p}| = |a|.$$

Thus

$$x^3 + |a|x^2 + |b|x + |c| = x^3 + |a|(x^2 + x) + 1 = (x+1)(x^2 + (|a|-1)x + 1);$$

and (?) since $||a|-1| \leq 2$, the roots of the quadratic $x^2 + (|a|-1)x + 1$ are complex numbers of unit modulus, the result follows.

5. Prove that $x^4 + x^3 + x^2 + x + 1$ is a factor of $x^{44} + x^{33} + x^{22} + x^{11} + 1$.

Since $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = 0$ we see that $x^{5n} = 1$ for every integer n. So $x^{44} + x^{33} + x^{22} + x^{11} + 1 = x^{8.5}x^4 + x^{6.5}x^3 + x^{4.5}x^2 + x^{2.5}x + 1 = x^4 + x^3 + x^2 + x + 1 = 0$. Thus every root of $x^4 + x^3 + x^2 + x + 1$ is a root of $x^{44} + x^{33} + x^{22} + x^{11} + 1$, and the Remainder Theorem does the rest.

6. The coeffs of the cubic $ax^3 + bx^2 + cx + d$ are integers, ad is odd and bc is even. Prove that at least one root is irrational.

Suppose all roots are rational, and apply the rational roots theorem. According to this, if p/q is a rational root with p, q in their lowest form, then p divides

d and q divides a. But ad is odd. Hence both of a, d are odd and so p, q are odd. Next note that

$$ap^3 + bp^2q + cpq^2 + dq^3 = 0.$$

The first and last terms are odd, so their sum is even, and since bc is even one of b, c is even. Hence one of bp^2q, cpq^2 is even. But their sum is even. Hence both are even. Hence b, c are even. Finally, if the roots are rational we can denote them by p_1/q_1, p_2/q_2, p_3/q_3, where, for $k = 1, 2, 3$, p_k, q_k are odd integers, with p_k, q_k having no common factors. Then

$$\frac{p_1}{q_1} + \frac{p_2}{q_2} + \frac{p_3}{q_3} = -\frac{b}{a},$$

whence we derive (?) a contradiction. Thus at least one root is irrational.

7. Suppose $m, n \geq 1$ and

$$f(x) = x^n + \cdots + a_1x + a_0,\ g(x) = b_mx^m + \cdots + b_1x + b_0,\ b_m \neq 0,$$

are two polynomials with integer coefficients and share a common real root. Prove that the common root is an integer. This is false! For instance $x^2 - 2, x(x^2 - 2)$ share a common real root, which is irrational.

To see what's involved, let $n = 3, m = 2$ and let x denote the common root. Then

$$0 = x^3 + a_2x^2 + a_1x + a_0 = b_2x^2 + b_1x + b_0.$$

Then

$$0 = b_2x^3 + a_2b_2x^2 + a_1b_2x + a_0b_2 = b_2x^3 + b_1x^2 + b_0x,$$

whence

$$0 = (a_2b_2 - b_1)x^2 + (a_1b_2 - b_0)x + a_0b_2 = b_2x^2 + b_1x + b_0.$$

Now eliminate the x^2 term and conclude that

$$[b_2(a_1b_2 - b_0) - b_1(a_2b_2 - b_1)]x + [a_0b_2^2 - b_0(a_2b_1 - b_1)] = 0.$$

It follows from this that if

$$[b_2(a_1b_2 - b_0) - b_1(a_2b_2 - b_1)] = 0,$$

then

$$[a_0b_2^2 - b_0(a_2b_1 - b_1)] = 0.$$

Otherwise, x is rational, and so a rational root of f. By the rational roots theorem, it must then be an integer.g