Polynomials (Green Group)

Po-Ru Loh

June 22, 2010

A Few Fun Facts

- **Interpolation.** Given n points $(x_1, y_1), \ldots, (x_n, y_n)$ with distinct x-coordinates, there is a unique polynomial $p(x)$ of degree at most $n-1$ which passes through all of these points. *Lagrange interpolation* gives a useful formula for this polynomial:

$$\begin{aligned} f(x) &= y_1 \cdot \frac{(x-x_2)(x-x_3)\cdots(x-x_n)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)} + y_2 \cdot \frac{(x-x_1)(x-x_3)\cdots(x-x_n)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_n)} + \\ &\quad y_n \cdot \frac{(x-x_1)(x-x_2)\cdots(x-x_{n-1})}{(x_n-x_1)(x_n-x_2)\cdots(x_n-x_{n-1})}. \end{aligned}$$

  The trick is that each term vanishes at all but one point x_k, so that its coefficient determines the value of $f(x)$ at that x_k without disturbing the values at the other points.

  In the special case that $x_1, \ldots, x_n$ are consecutive integers, *Newton interpolation* gives another way of finding the interpolating polynomial. Assuming for convenience that $x_k = k-1$, we observe that the binomial coefficient

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}$$

  vanishes at $x = 0, 1, 2, \ldots, k-1$ and takes on the value 1 at $x = k$. It follows that we may successively choose coefficients of $\binom{x}{k}$ to match the desired values $y_1, \ldots, y_n$. (Each successive choice will modify "future" values of the polynomial but will leave "previous" values alone.) Explicitly, the Newton interpolation formula can be written in terms of forward differences:

$$f(x+a) = \sum \binom{x}{k} \Delta^k[f](a),$$

  where

$$\Delta^n[f](x) = \sum_{k=0}^{n} (-1)^{n-k} f(x+k).$$

  The exact form of the coefficients is often unneeded, however; knowing that polynomials can be decomposed as linear combinations of binomial coefficients may be enough—for instance, it allows us to characterize all polynomials that take only integer values at integers.

- **Roots.** A number r is a root of a polynomial f if and only if $x-r$ divides $f(x)$. This fact is just the beginning of a long and intriguing story...

- **Complex Roots.** All polynomials factor completely over the complex numbers:

$$f(x) = c(x - r_1)\dots(x - r_n),$$

where $r_1, \dots, r_n$ are the (complex) roots of f (with multiplicity). It follows that the coefficients of f can be expressed as *elementary symmetric polynomials* in $r_1, \dots, r_n$. Taking $c = 1$ for convenience and letting $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x_1 + a_0$, we have

$$\begin{aligned} a_0 &= (-1)^n r_1 \cdots r_n, \\ a_1 &= (-1)^{n-1}(r_2r_3\cdots r_{n-1} + r_1r_3\cdots r_n + \cdots + r_2r_3\cdots r_n), \\ &\dots \\ a_{n-1} &= -(r_1 + \cdots + r_n). \end{aligned}$$

Of course, polynomials do not generally factor completely over the reals or the rationals, resulting in many more fun facts.

- **Real Roots.** Polynomials with real coefficients factor as products of linear and quadratic factors: the linear terms correspond to real roots and the quadratic terms correspond to complex conjugate pairs. It is generally difficult to say much about the real roots of a polynomial just by looking at it (other than that polynomials of odd degree have an odd number of real roots), but *Descartes' Rule of Signs* occasionally gives a little more information: the number of positive roots of a real polynomial is congruent to the number of sign changes between consecutive coefficients (mod 2).

- **Rational Roots.** The *Rational Root Theorem* states that if $q = \frac{r}{s}$ is a rational root of an integer polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ and $\gcd(r, s) = 1$, then $r \mid a_0$ and $s \mid a_n$.

- **Factorization.** Polynomials over the complex numbers, reals, rationals, and integers all enjoy *unique factorization*, although the first three cases are slightly better-behaved because $\mathbb{C}, \mathbb{R}$, and $\mathbb{Q}$ are closed under division. In particular, polynomials $f(x)$ and $g(x)$ can be divided (with remainder) via long division:

$$f(x) = q(x)g(x) + r(x)$$

where $r(x)$ has degree less than $g(x)$ (assuming $g(x)$ is nonconstant). It follows that the *Euclidean algorithm* works as usual, allowing us to find the GCD $d(x)$ of $f(x)$ and $g(x)$ and express it as a combination

$$d(x) = a(x)f(x) + b(x)g(x).$$

Note that this does *not* work over the integers: the GCD of x and 2 is 1, but 1 clearly cannot be expressed as a combination of x and 2. (In fancier terms, this says that $\mathbb{Z}[x]$ is not a *principal ideal domain.*)

Fortunately, factorization over the integers can be understood nicely via factorization over the rationals (which is well-behaved): if a polynomial with integer coefficients factors over the rationals, then all of its factors can actually be chosen to have integer coefficients—a very handy fact!

Additionally, it can sometimes help to consider factorizations mod p: if an integer polynomial factors over $\mathbb{Z}$, then it factors over $\mathbb{Z}/p\mathbb{Z}$ (but the converse does not hold).

Finally, as a slight aside, a polynomial f has a square factor if and only if f and f' (the *formal derivative*) share a common factor, which can be checked simply by using the Euclidean algorithm.

- **Irreducibility.** A polynomial that does not factor at all is called *irreducible*. This topic is more advanced and we only touch on it here. *Eisenstein's Criterion* is probably the least-technical way of proving irreducibility: it states that if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ has integer coefficients satifying $p \mid a_0, a_1, \ldots, a_{n-1}, p \nmid a_n$, and $p^2 \nmid a_0$, then $f(x)$ is irreducible over the rationals. As an example, it follows immediately that $x^n - p$ is irreducible for any n. A trickier example is to show that $x^p - 1$ factors completely as $(x-1)(x^{p-1}+\cdots+1)$: the trick to showing that the second factor (a *cyclotomic polynomial*) is irreducible is to replace x by $x+1$ before applying Eisenstein.

  Lastly, a root r of a *monic* (i.e., leading coefficient 1) irreducible polynomial$f(x)$ is called an *algebraic integer*. In this case $f(x)$ is called the *minimal polynomial* of r and divides all polynomials of which r is a root.

Puzzling Problems

1. [APMO 01/4] A point in the Cartesian coordinate plane is called a *mixed point* if one of its coordinates is rational and the other one is irrational. Find all polynomials with real coefficients such that their graphs do not contain any mixed point.

2. [USAMO 02/3] Prove that any monic polynomial of degree n with real coefficients is the average of two monic polynomials of degree n with n real roots.

3. [Russia 01] Let a, b, and c be integers such that $b \neq c$. If $ax^2 + bx + c$ and $(c-b)x^2 + (c-a)x + (a+b)$ have a common root, prove that $a + b + 2c$ is divisible by 3.

4. [Russia 01] Two polynomials $P(x) = x^4 + ax^3 + bx^2 + cx + d$ and $Q(x) = x^2 + px + q$ take negative values on some common real interval I of length greater than 2, and outside of I they take on nonnegative values. Prove that $P(x_0) < Q(x_0)$ for some real number x_0.

5. [China 01?] For each integer $k > 1$, find the smallest integer m greater than 1 with the following property: there exists a polynomial $f(x)$ with integer coefficients such that $f(x) - 1$ has at least 1 integer root and $f(x) - m$ has exactly k distinct integer roots.

6. [India 01] Let $a \geq 3$ be a real number and $p(x)$ be a polynomial of degree n with real coefficients. Prove that
$$\max_{0 \leq j \leq n+1} \{|a^j - p(j)|\} \geq 1.$$

7. [Romania 01] Let $f(x) = a_0 + a_1 x + \cdots + a_m x^m$, with $m \geq 2$ and $a_m \neq 0$, be a polynomial with integer coefficients. Let n be a positive integer, and suppose that:

   (i) $a_2, a_3, \ldots, a_m$ are divisible by all the prime factors of n;

   (ii) a_1 and n are relatively prime.

   Prove that for any positive integer k, there exists a positive integer c such that $f(c)$ is divisible by n^k.

8. [Korea 02]

   Let $n \geq 3$ be an integer. Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be positive real numbers, where the b_i are pairwisedistinct.

   (a) Find the number of distinct real zeroes of the polynomial

   $$f(x) = (x - b_1)(x - b_2) \cdots (x - b_n) \sum_{j=1}^{n} \frac{a_j}{x - b_j}.$$

   (b) Writing $S = a_1 + a_2 + \cdots + a_n$ and $T = b_1 b_2 \cdots b_n$, prove that

   $$\frac{1}{n-1} \sum_{j=1}^{n} \left(1 - \frac{a_j}{S}\right) b_j > \left(\frac{T}{S} \sum_{j=1}^{n} \frac{a_j}{b_j}\right)^{1/(n-1)}.$$

9. [Vietnam 02]

   Find all polynomials $p(x)$ with integer coefficients such that

   $$q(x) = (x^2 + 6x + 10)(p(x))^2 - 1$$

   is the square of a polynomial with integer coefficients.

10. [Balkan 01]

    Prove that if a convex pentagon satisfies the following conditions, then it is a regular pentagon:

    (i) all the interior angles of the pentagon are congruent;

    (ii) the lengths of the sides of the pentagon are rational numbers.

11. [Czech-Slovak-Polish 02]

    Let $n \geq 2$ be a fixed even integer. We consider polynomials of the form

    $$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1$$

    with real coefficients, having at least one real root. Determine the least possible value of the sum $a_1^2 + \cdots + a_{n-1}^2$.