Polynomials

Reid Barton

June 21, 2005

There are three basic ways to think about a polynomial $P(x)$:

1. in terms of its coefficients $(a_0, a_1, \ldots, a_n)$, where $P(x) = a_0 + a_1 x + \cdots + a_n x^n$;
2. in terms of its roots $\{r_1, \ldots, r_n\}$, where $P(x) = c(x - r_1) \cdots (x - r_n)$;
3. as a function from $\mathbb{R}$ to $\mathbb{R}$ (or $\mathbb{C}$ to $\mathbb{C}$, $\mathbb{Z}$ to $\mathbb{Z}$, etc.) by evaluation.

Interesting problems are those which involve multiple viewpoints on the same polynomial, so we need ways to relate these different aspects.

For the first two to be equivalent ways of looking at polynomials, we need to know whether any polynomial $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ can be written as a product of linear factors. This follows from the **Fundamental Theorem of Algebra**, if we are willing to use complex numbers:

> Every non-constant polynomial with complex coefficients has a complex root.

The relationship between the coefficients and the roots of a polynomial is given by **Vieta's formulas**:

$$\begin{aligned} c &= a_n, \\ -c(r_1 + \cdots + r_n) &= a_{n-1}, \\ &\vdots \\ (-1)^n c r_1 \cdots r_n &= a_0, \end{aligned}$$

where generally a_k is the sum of all products of the r_i taken $n - k$ at a time, multiplied by $(-1)^{n-k}c$. Of course, it is not so easy to determine the roots of a polynomial from its coefficients, as evidenced for example by the unsolvability of the general fifth degree equation in quadratics. Nevertheless, the equations above already form the basis for some interesting problems.

Problem 1. (USAMO '77) Prove that the product of the two real roots of $x^4 + x^3 - 1$ is a root of $x^6 + x^4 + x^3 - x^2 - 1$.

Problem 2. (Canada?) If α, β, γ are the roots of $x^3 - x - 1$, then find

$$\frac{\alpha - 1}{\alpha + 1} + \frac{\beta - 1}{\beta + 1} + \frac{\gamma - 1}{\gamma + 1}.$$

Problem 3. Let M be a finite set of non-zero real numbers. Prove that there exists a constant C with the following property: if $P(x)$ is a polynomial of degree n with n real roots (possibly repeated), all of whose coefficients belong to M, then $n \leq C$.

A couple results relating to real roots of polynomials which are good to know:

> If $P(x)$ is a polynomial with real coefficients of odd degree, then $P(x)$ has at least one real root;

and **Descartes' Rule of Signs**,

> Let $P(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial with real coefficients, and let D be the number of sign changes in the sequence $(a_0, a_1, \ldots, a_n)$ (we ignore terms equal to zero). Then the number of positive real roots of $P(x)$ is $D - 2k$ for some nonnegative integer k. (To find the number of negative real roots, apply the rule to $P(-x)$.)

Given a polynomial in terms of its coefficients or roots, it is a simple matter to evaluate at any given real or complex number. The reverse problem is more interesting—given a function from $\mathbb{R}$ to $\mathbb{R}$, is it determined by a polynomial $P(x)$, and if so can we reconstruct the coefficients of P? The **Lagrange Interpolation Formula** gives one kind of answer to this question:

> If (x_0, y_0), (x_1, y_1), ..., (x_n, y_n) are points in the plane with distinct x-coordinates, then there exists a unique polynomial $P(x)$ of degree at most n passing through these points, and it is given by the expression
>
> $$P(x) = \sum_{i=0}^{n} y_i \frac{(x-x_0)\cdots\widehat{(x-x_i)}\cdots(x-x_n)}{(x_i-x_0)\cdots\widehat{(x_i-x_i)}\cdots(x_i-x_n)}. \tag{1}$$

It is easy to check that this polynomial takes on the value y_i at the point x_i. Uniqueness follows from the following important **equality principle**:

> If $P(x)$ and $Q(x)$ are two polynomials of degree at most n and $P(x) = Q(x)$ for $n+1$ distinct values of x, then $P(x)$ and $Q(x)$ are the same polynomial.

The proof is that $P(x) - Q(x)$ is a polynomial of degree at most n with $n+1$ distinct roots, hence must be zero. Thus if we know the value of a polynomial of degree n at $n+1$ points, its value at any other point is determined by the expression (1)—but this expression is usually unwieldy and other techniques tend to be more useful, as in the problems below.

Problem 4. A polynomial $P(x)$ of degree 2005 satisfies $P(k) = 2^k$ for $k = 0, 2, \ldots, 2003$. Find $P(2004)$.

Problem 5. (USAMO '75) A polynomial $P(x)$ of degree n satisfies $P(0) = 0$, $P(1) = 1/2$, $P(2) = 2/3$, ..., $P(n) = n/(n+1)$. Find $P(n+1)$.

Problem 6. (USAMO '84) Find all values of n for which there exists a polynomial $P(x)$ of degree $3n$ satisfying the following equations:

$$P(0) = P(3) = \cdots = P(3n) = 2;\ P(1) = P(4) = \cdots = P(3n-1) = 1;\ P(2) = P(5) = \cdots = P(3n-2) = 0;$$
$$P(3n+1) = 730.$$

Problem 7. (MOP '96) Let $z_1, \ldots, z_n$ be distinct complex numbers, and for $1 \le k \le n$, put

$$Z_k = (z_k - z_1)\cdots(z_k - z_{k-1})(z_k - z_{k+1})\cdots(z_k - z_n).$$

Let P be a complex polynomial of degree at most $n-1$ with leading coefficient 1. Prove that

$$\frac{P(z_1)}{Z_1} + \cdots + \frac{P(z_n)}{Z_n} = \begin{cases} 0 & \deg P < n-1 \\ 1 & \deg P = n-1 \end{cases}.$$

As an illustration of these ideas, we will introduce the notion of **roots of unity**, the n complex roots of the polynomial $x^n - 1$. These are the numbers $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, where $\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n)$. They have countless applications to many kinds of problems, so this discussion will necessarily be brief.

Problem 8. Prove that the sum of the nth roots of unity is zero for $n \ge 1$. More generally, find the sum of the kth powers of the nth roots of unity for n, k positive integers.

Problem 9. (USAMO '76) The polynomials $A(x)$, $B(x)$, $C(x)$, $D(x)$ satisfy the equation

$$A(x^5) + xB(x^5) + x^2C(x^5) = (1 + x + x^2 + x^3 + x^4)D(x).$$

Show that $A(1) = 0$.

Problem 10. Find the product of the lengths of all sides and diagonals of a regular n-gon.

Problem 11. Let $P_1P_2\cdots P_n$ be a regular polygon inscribed in the unit circle, and let X be a point on the unit circle. Find the maximum value of $P_1X \cdot P_2X \cdot \cdots \cdot P_nX$.

Problem 12. A sequence $a_1, a_2, \ldots, a_n$ is called *k-balanced* if $a_1 + a_{k+1} + \cdots = a_2 + a_{k+2} + \cdots = \cdots = a_k + a_{2k} + \cdots$. Suppose the sequence $a_1, a_2, \ldots, a_{50}$ is k-balanced for $k = 3, 5, 7, 11, 13, 17$. Prove that all the values a_i are zero.

It turns out that polynomials in one variable over the rational (or real or complex) numbers behave a lot like integers. For example, there is a notion of divisibility: a polynomial $P(x)$ divides another polynomial $Q(x)$ if there exists a third polynomial $R(x)$ such that $P(x) = Q(x)R(x)$. One way to determine divisibility of polynomials uses complex factorization: $P(x)$ divides $Q(x)$ iff every root of $P(x)$ appears as a root of $Q(x)$ with at least as high a multiplicity.

Problem 13. (USAMO '77) For which pairs of positive integers (a, b) does $x^a + \cdots + x + 1$ divide $x^{ab} + x^{ab-b} + \cdots + x^{2b} + x^b + 1$?

There is also an analogue to the **division algorithm**:

> If $P(x)$ and $Q(x)$ are two non-zero polynomials then there exist polynomials $R(x)$ and $S(x)$ such that
> $$P(x) = Q(x)S(x) + R(x),$$
> and $\deg R < \deg P$. (The degree of the zero polynomial is conventionally taken to be $-\infty$.)

A consequence is that, like the integers, polynomials have unique factorization, up to constant factors, and one can define the notion of the greatest common divisor of two polynomials. Analogously to the integers, the GCD of two polynomials $P(x)$ and $Q(x)$ is the polynomial of smallest degree which can be written in the form $A(x)P(x) + B(x)Q(x)$.

Problem 14. (Part of IMO '96 SL) For each positive integer n, show that there exists a positive integer k for which there exist polynomials $f(x)$, $g(x)$ with integer coefficients such that

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

The problem of factoring polynomials over the complex numbers is solved by the Fundamental Theorem of Arithmetic, and the situation over the reals is only slightly more complicated; any polynomial factors as a product of linear terms and quadratic terms with negative discriminant. However, when we restrict ourselves to the rational numbers, things become much more interesting. We call a polynomial $P(x)$ **reducible** if it can be written as a product of two polynomials each of degree at least one, otherwise **irreducible**. It turns out that questions of reducibility are equivalent whether we work over the rationals or integers, according to **Gauss's Lemma**:

> Let $P(x)$ be a polynomial with integer coefficients which is reducible over the rationals. Then $P(x)$ is reducible over the integers.

So in subsequent discussions of reducibility we will only consider polynomials with integer coefficients. There are many irreducible polynomials, for example by **Eisenstein's Criterion**:

> Let $P(x) = a_0 + a_1x + \cdots + a_nx^n$ be an integer polynomial and let p be a prime such that $p \mid a_0$, $p \mid a_1, \ldots, p \mid a_{n-1}$, but p does not divide a_n and p^2 does not divide a_0. Then $P(x)$ is irreducible.

There are many other techniques for proving irreducibility, however.

Problem 15. Show that $P(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible for any prime p.

Problem 16. Find all values of n such that the polynomial $P(x) = x^n - 64$ is reducible.

Problem 17. Find all reducible polynomials of the form $(x - a_1)(x - a_2)\cdots(x - a_n) \pm 1$ with a_1, a_2, $\ldots$, a_n distinct integers.

Problem 18. (IMO '93) Let $n \geq 2$ and let $P(x) = x^n + 5x^{n-1} + 3$. Prove that $P(x)$ is irreducible.

Problem 19. Show that for any positive integer n, the polynomial $P(x) = (x^2 + x)^{2^n} + 1$ is irreducible.

Let's return to our multiple viewpoints on polynomials, this time considering conditions of integrality. For example, if a polynomial with integer coefficients is evaluated at an integer, the result must be an integer. However, looking at two points at a time, one can say slightly more:

If $P(x)$ is a polynomial with integer coefficients, then for any distinct integers a and b, $a-b$ divides $P(a)-P(b)$.

Problem 20. Let $P(x)$ be a polynomial with integer coefficients, and let n be an odd positive integer. Suppose $x_1, x_2, \ldots, x_n$ is a sequence of integers such that $x_2 = P(x_1)$, $x_3 = P(x_2)$, $\ldots$, $x_n = P(x_{n-1})$, and $x_1 = P(x_n)$. Prove that all the x_i are equal.

Problem 21. (IMO '97 SL) Find all positive integers k for which the following statement is true: if $P(x)$ is a polynomial with integer coefficients satisfying the condition $0 \le P(c) \le k$ for $c = 0, 1, \ldots, k+1$, then $F(0) = F(1) = \cdots = F(k+1)$.

In the opposite direction, we have the following result:

A polynomial $P(x)$ of degree n has integral value at every integer iff $P(x)$ can be written in the form

$$P(x) = a_0\binom{x}{0} + a_1\binom{x}{1} + \cdots + a_n\binom{x}{n}$$

for some integers $a_0, a_1, \ldots, a_n$. (Note that $P(x)$ need not have integer coefficients.)

Finally, some miscellaneous extra problems, arranged roughly in increasing order of difficulty.

Problem 22. Proble that every polynomial over the complex numbers has a nonzero polynomial multiple whose exponents are all divisible by 10^9.

Problem 23. (USAMO '92) A complex polynomial $P(z)$ has degree 1992 and distinct zeros. Show that we can find complex numbers z_n, such that if $Q_1(z) = z - z_1$ and $Q_n(z) = Q_{n-1}(z)^2 - z_n$, then $P(z) \mid Q_{1992}(z)$.

Problem 24. (MOP '97) Find, with proof, all nonzero polynomials $P(x)$ such that $P(x^2)+P(x)P(x+1) = 0$.

Problem 25. (MOP '96) Find all polynomials $P(x)$ with real coefficients for which there exists a polynomial $Q(x)$ with real coefficients such that $P(x^2) = Q(P(x))$.

Problem 26. (MOP '97) Let $S = \{s_1, s_2, \ldots, s_n\}$ be a set of n distinct complex numbers, for some $n \ge 9$, exactly $n-3$ of which are real. Prove that there are at most two quadratic polynomials $f(x)$ with complex coefficients such that $f(S) = S$ (that is, f permutes the elements of S).

Problem 27. (IMO '97 SL) Let $P(x)$ be a polynomial with real coefficients such that $P(x) > 0$ for all $x \ge 0$. Prove that there exists a positive integer n such that $(1+x)^n P(x)$ is a polynomial with nonnegative coefficients.

Problem 28. (USAMO '88) Let $P(x)$ be the polynomial $(1-x)^{a_1}(1-x^2)^{a_2}\cdots(1-x^{32})^{a_3 2}$, where a_1, a_2, $\ldots$, a_{32} are nonnegative integers. When expanded in powers of x, the coefficient of x^1 is -2 and the coefficients of x^2, x^3, $\ldots$, x^{32} are all zero. Find k.

Problem 29. (MOP '96) Let $P(x)$ be a monic polynomial of degree n with real coefficients. Prove that for any distinct integers $a_0, \ldots, a_n$, there exists $i \in \{0, \ldots, n\}$ such that $|P(a_i)| \ge n!/2^n$.

Problem 30. (The rest of Problem 14) Find the smallest such value of k.

Problem 31. (MOP '97) Let $x_1, x_2, \ldots, x_n$ be distinct real numbers, and define the polynomials

$$\begin{aligned} P(x) &= (x-x_1)(x-x_2)\cdots(x-x_n) \\ Q(x) &= P(x)\left(\frac{1}{x-x_1} + \cdots + \frac{1}{x-x_n}\right). \end{aligned}$$

Let $y_1, \ldots, y_{n-1}$ be the roots of Q. Show that

$$\min_{i\ne j} |x_i - x_j| \le \min_{i\ne j} |y_i - y_j|.$$

Problem 32. Prove that there exists a polynomial $P(x,y)$ with real coefficients such that $P(x,y) \ge 0$ for all real numbers x, y, but $P(x,y)$ cannot be written as the sum of squares of polynomials with real coefficients.