POLYNOMIALS

Gabriel D. Carroll, 11/14/99

The theory of polynomials is an extremely broad and far-reaching area of study, having applications not only to algebra but also ranging from combinatorics to geometry to analysis. Consequently, this exposition can only give a small taste of a few facets of this theory. However, it is hoped that this will spur the reader's interest in the subject.

1 Definitions and basic operations

First, we'd better know what we're talking about. A *polynomial in the indeterminate x* is a formal expression of the form

$$f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + x_0 = \sum_{i=0}^{n} c_i x^i$$

for some coefficients c_i. Admittedly this definition is not quite all there in that it doesn't say what the coefficients are. Generally, we take our coefficients in some *field*. A field is a system of objects with two operations (generally called "addition" and "multiplication"), both of which are commutative and associative, have identities, and are related by the distributive law; also, every element has an additive inverse, and everything except the additive identity has a multiplicative inverse. Examples of familiar fields are the rational numbers $\mathbb{Q}$, the reals $\mathbb{R}$, and the complex numbers $\mathbb{C}$, though plenty of other examples exist, both finite and infinite. We let $F[x]$ denote the set of all polynomials "over" (with coefficients in) the field F. Unless otherwise stated, don't worry about what field we're working over.

A few more terms should be defined before we proceed. First, if $f(x) = \sum_{i=0}^{n} c_i x^i$ with $c_n \neq 0$, we say n is the *degree* of the polynomial, written $\deg f$. Thus the degree simply means the highest power of x that occurs. The zero polynomial $f(x) = 0$ is usually held to have no degree, though some folks like to say it has degree $-\infty$; when it is convenient we will assume it has degree less than any other polynomial. The polynomials of degree 0, together with the zero polynomial, are called *constant polynomials.*

If $f(x) = \sum_{i=0}^{n} c_i x^i$ with $c_n \neq 0$, then c_n is the *leading coefficient* and c_0 is the *constant term.* A *monic* polynomial is one with leading coefficient 1. For convenience, we'll usually that we write our polynomials so that $c_n \neq 0$. But when that makes life annoying, we can equivalently say that $c_i = 0$ for $i > \deg f$ (and for $i < 0$, while we're at it).

Polynomials are useful because we can look at them either as purely algebraic objects or as functions of the variable x. For now let's get some algebraic properties down. We can't write any equations until we know what equality means, so let's write $f = g$ if the coefficients match, i.e. in the form $f(x) = \sum_{i=0}^{n} c_i x^i, g(x) = \sum_{j=0}^{m} d_j x^j$ we have $n = m$ and $c_i = d_i$ for each i. Now we can clearly add two polynomials, by adding like terms: if $f(x) = \sum_{i=0}^{n} c_i x^i$ and $g(x) = \sum_{j=0}^{m} d_j x^j$, then

$$f + g(x) = \sum_{i=0}^{n} c_i x^i + \sum_{j=0}^{m} d_j x^j = \sum_{i=0}^{\max(m,n)} (c_i + d_i)x^i.$$

Multiplying by a scalar (an element of our field) is even easier: for a scalar c, define cf by

$$cf(x) = \sum_{i=0}^{n} (cc_i)x^i.$$

We can also multiply two polynomials. To do this, we first expand the product in the usual way, then group terms according to the power of x. We get

$$fg(x) = \Big(\sum_{i=0}^{n} c_i x^i\Big)\Big(\sum_{j=0}^{m} d_j x^j\Big) = \sum_{i=0}^{n}\sum_{j=0}^{m} c_i d_j x^{i+j} = \sum_{k=0}^{n+m}\Big(\sum_{i+j=k} c_i d_j\Big)x^k.$$

It shouldn't be hard to see that $\deg cf = \deg f$ for $c \neq 0$ and that $\deg f+g \leq \max(\deg f, \deg g)$, henceforth pretending that 0 has degree less than any other polynomial. (Beware! We may not have equality; take $f(x) = x + 47, g(x) = -x$. However, if $\deg f \neq \deg g$ then equality occurs.) Almost as obvious is

Proposition 1 *If* $\deg f = n, \deg g = m$, *then* $\deg fg = n + m$.

Proof: Write $f = \sum c_i x^i, g = \sum d_j x^j$ and note that when the product fg is expanded, each term is $c_i d_j x^{i+j}$; since $i \leq n, j \leq m$ we see no term has a power of x higher than $n + m$. On the other hand, the only x^{n+m} term possible is $c_n d_m x^{n+m}$, and this coefficient is nonzero since $c_n, d_m \neq 0$; our result follows. ■

It's not hard to see that our operations obey the usual laws - associativity, commutativity, distributivity.

Since polynomials can be treated as functions, one can ask what happens under function composition. Generally we get a big worthless mess, but in simple cases this operation can be useful.

Recall that the binomial coefficient $\binom{n}{k} = n!/(k!(n-k)!)$ is the number of ways of choosing k from among n given objects. The following is well known; we omit the proof.

Lemma 2 *(Binomial Theorem)* $(x + y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$ *for positive integers* i. ■

Corollary 3 *If* $f(x) = \sum_{i=0}^{n} c_i x^i$, *then* $f(x + y) = \sum_{i=0}^{n} (\sum_{j=i}^{n} \binom{j}{i} c_j y^{j-i}) x^i$.

Proof: Write out $f(x + y) = \sum_j c_j (x + y)^j$, then expand each term according to the binomial theorem and regroup the resulting terms according to powers of x. ■

That result lets us evaluate compositions of the form $f(x + a)$ where a is constant. The following is also sometimes nice, especially when c is a root of unity (which we'll go into soon enough).

Proposition 4 *For any scalar* c, $f(cx) = \sum_i (c^i c_i) x^i$.

Proof: Both sides equal $\sum_i c_i (cx)^i$. ■

Let's go back to addition and multiplication. Under these operations, polynomials over a given field behave just like integers in many ways. For example, we can talk about divisibility. We write $g \mid f$, pronounced "*g divides f*," if $f = gq$ for some polynomial q. Since $\deg gq = \deg q + \deg g \geq \deg g$ if $gq \neq 0$, we see that g does not divide any nonzero polynomial of smaller degree than g; hence divisibility is a nontrivial notion. In fact, when we restrict ourselves to monic polynomials, divisibility defines a *partial ordering*, meaning it is reflexive, antisymmetric, and transitive:

Lemma 5 *For polynomials* f, g, h*:*

(a) $f \mid f$*;*

(b) if $f \mid g$ *and* $g \mid f$ *then* $g = cf$ *for a scalar* c *and, in particular, if* f, g *are both monic, then* $f = g$*;*

(c) if $f \mid g$ *and* $g \mid h$ *then* $f \mid h$.

Proof: (a) is obvious since f = 1f. (c) is also clear, since if $g = fp, h = gq$ then $h = f(pq)$. For (b), assume f, g are nonzero (otherwise we're done), and let $g = fp, f = gq$ and note that $\deg f = \deg g + \deg q \geq \deg g = \deg f + \deg p \geq \deg f$ so we have equality throughout and, in particular, $\deg p = 0$, so p is a constant, $p = c$. The last statement of (b) is clear from looking at leading coefficients. ■

It should be clear that sums and multiples of polynomials divisible by f are themselves divisible by f.

Just like integers, even if we can't divide cleanly, we can divide with remainder.

Lemma 6 *(Division algorithm) For polynomials* f, g *with* $g \neq 0$, *we can write* $f = gq + r$ *for polynomials* q, r *such that* $\deg r < \deg g$.

Proof: Fix g and use induction on $\deg f$. If $\deg f < \deg g$ then take $q = 0, r = f$. This is the base case. Otherwise, write $f(x) = \sum_{i=0}^{n} c_i x^i, g(x) = \sum_{j=0}^{m} d_j x^j$, so $n - m \geq 0$. Note that the polynomial $f(x) - (c_n/d_m)x^{n-m} g(x)$ has degree less than n. (Proof: each of $f(x), (c_n/d_m)x^{n-m} g(x)$ has degree n, and their x^n terms both have coefficient c_n, so when we subtract, these terms cancel and we are left with a polynomial of lower degree.) Hence by the induction hypothesis, we have $f(x) - (c_n/d_m)x^{n-m} g(x) = gq' + r$ for $\deg r < \deg g$, and then we get $f = g(q' + (c_n/d_m)x^{n-m}) + r$ which meets our requirements. ■

It's not hard to show that q and r are uniquely determined.

Another resemblance between polynomials and integers is the notion of a greatest common divisor. d is called a *greatest common divisor* of f and g (written $d = \gcd(f, g)$ or just $d = (f, g)$) if $d \mid f, d \mid g$, and, for every d' such that $d' \mid f, d' \mid g$, we have $d' \mid d$. For uniqueness, we usually require d to be monic. (Since two gcds must divide each other, lemma 5 assures that this really does give uniqueness.) Before imposing this formal restriction, though, let us show existence:

Lemma 7 *If $f, g \neq 0$ then, of all nonzero polynomials expressible in the form $sf + tg$ (s, t polynomials), let d be one of minimal degree. Then d is a gcd of f and g.*

Proof: Write $d = sf + tg$; by the division algorithm, we have $f = qd + r$ with $\deg r < \deg d$. Then $r = f - qd = (1 - qs)f + (-qt)g$ and minimality implies $r = 0$; thus $d \mid f$, and likewise $d \mid g$. Also, if $d' \mid f, d' \mid g$ then we have $d' \mid sf + tg = d$, as needed. ■

This mechanical groundwork can get boring. Soon, however, we'll put it to work to prove something of interest: unique factorization. Of course, we can't define factorization until we know about primes, so there's a modicum of tedium remaining. The nonconstant polynomial f will be called *irreducible* if it cannot be written as the product gh where g, h are both nonconstant polynomials.

Lemma 8 *f is irreducible iff, for every polynomial g, we have either $f \mid g$ or $(f, g) = 1$.*

Proof: Suppose f is irreducible; we have $(f, g) \mid f$ and so this gcd must either be a constant or a multiple of f, which is easily seen to imply our statement. Conversely, if $f = gh$ for $\deg g, \deg h > 0$ then (f, g) is a scalar multiple of g, which is neither f nor 1; this gives the reverse implication. ■

Lemma 9 *If f is irreducible and $f \mid gh$, then $f \mid g$ or $f \mid h$.*

Proof: Suppose $f \not| g$; then $(f, g) = 1$ and, by lemma 7, $1 = sf + tg$ for some s, t. Then $h = sfh + tgh$; since $f \mid sfh$ and $f \mid gh \mid tgh$ we have $f \mid h$, as claimed. ■

By induction we can extend this to arbitrarily many factors: if $f \mid g_1 g_2 \cdots g_r$ then $f \mid$ some g_i.

Yes!! Now we can prove something interesting.

Theorem 10 *(Unique factorization) Every nonzero polynomial f is expressible in the form $f = cf_1 f_2 \cdots f_r$, where c is a scalar and the f_i are monic irreducibles; this expression is unique up to reordering of the f_i.*

Proof: (We will assume the empty product - where $r = 0$ - equals 1.) First we prove the existence of such a factorization, by strong induction on $\deg f$. If $\deg f = 0$ then $f = c$ and $r = 0$; this is our base case. Otherwise, we have two possibilities. If f is irreducible then let c be the leading coefficient of f and $f_1 = f/c$. Otherwise, we can write $f = gh$ with $\deg g, \deg h < \deg f$; by the induction hypothesis, each of g, h can be written as a scalar times a product of irreducibles, and then we can combine these into a factorizaion for f by multiplying the scalars and juxtaposing the irreducible factors.

Now we must prove uniqueness. Suppose $cf_1 \cdots f_r = f = c' f'_1 \cdots f'_s$ are factorizations meeting the conditions in the statement of the theorem. We see that c and c' must both equal the leading coefficient of f, since all other factors are monic; hence we can divide out by these for simplicity, and we are left with $f_1 \cdots f_r = f'_1 \cdots f'_s$. We work by induction on r. The base case is $r = 0$, which means the product on the left is the empty product, 1; then also $s = 0$ since otherwise the right side would have degree > 0, a contradiction. Thus both sides are equal, giving the base case. Now if $r > 0$, note that $f_1 \mid f'_1 \cdots f'_s$, so, from lemma 9, $f_1 \mid f'_j$ for some j. Thus $f'_j = f_1 q$, but since f'_j is irreducible and f'_1 is nonconstant (because it is irreducible) we see that q is a scalar, and monicity implies $q = 1 \Rightarrow f_1 = f'_j$. So these factors are equal, and we can divide out f_1 on both sides; the induction hypothesis then tells us the remaining factorizations are equal (up to ordering), so our original factorizations were also equal, as desired. ■

Unique factorization can solve many multiplicative problems about polynomials. We will return to irreducibility and factorization later. First, however, we will look at these creatures from another perspective.

If we let x take values (in our field) rather than merely being a placeholder, our polynomial is transsubstantiated from an abstract, formal entity to a function that can be evaluated. Often, a good deal can be learned about a polynomial from the values it takes on. Of central importance is the notion of a *root* or *zero* of a polynomial f: a number a such that $f(a) = 0$.

What do the roots of a polynomial tell us about the polynomial? A heck of a lot, that's what. We'll bring up some basic facts first; then, in the next section, the importance of roots will appear in full bloom.

Lemma 11 *The polynomial f has a as a root iff $x - a \mid f(x)$.*

Proof: If $f(a) = 0$, then use the division algorithm to write $f(x) = (x - a)q(x) + r(x)$; since $\deg r < \deg(x-a)$ we see that r is constant. Letting $x = a$ we have $0 = f(a) = (a-a)q(a)+r = r$, so $f(x) = (x-a)q(x)$ as claimed. Conversely, if $x - a \mid f$, then $f(x) = (x - a)q(x)$, so $f(a) = (a - a)q(a) = 0$. ■

Corollary 12 *If $a_1, a_2, \ldots, a_n$ are distinct roots of f, then $(x - a_1)(x - a_2)\cdots(x - a_n) \mid f$. In particular, if f has degree n, then $f = c(x - a_1)\cdots(x - a_n)$ for some scalar c.*

Proof: We prove the first assertion by induction on n. If $n = 0$ this amounts to $1 \mid f$ which is clear. If $n > 0$ then by the previous result we can write $f(x) = (x - a_n)q(x)$; letting $x = a_i$ for $i < n$ we see $0 = (a_i - a_n)q(a_i)$ so that a_i is a root of q. By the induction hypothesis, $(x - a_1)\cdots(x - a_{n-1}) \mid q$ which implies what we want. The second assertion now follows easily by consideration of degrees. ■

Corollary 13 *A nonzero polynomial of degree n has at most n roots.*

Proof: If the polynomial has more than n roots, then by the previous result, it is divisible by a polynomial of degree $> n$, an impossibility. ■

Corollary 14 *If $\deg f, \deg g < n$ and there are n distinct values of x such that $f(x) = g(x)$, then $f = g$.*

Proof: The polynomial $f - g$ has degree $< n$ but it has at least n roots, so by the preceding result, it must be 0. ■

2 Some applications

We now know more than enough to solve some problems, so let's get to work.

Example 1 *(USAMO 1975) Suppose $P(x)$ is a polynomial of degree $n \geq 1$ such that $P(k) = k/(k + 1)$ for $k = 0, 1, 2, \ldots, n$. Find $P(n + 1)$.*

Solution: Let $Q(x) = (x+1)P(x) - x$ and observe that Q is a polynomial of degree $n+1$; moreover, the $n+1$ numbers $0, 1, \ldots, n$ are roots of Q. Hence we can write $Q(x) = cx(x-1)\cdots(x-n)$. To determine c, note that $Q(-1) = (-1+1)P(-1)-(-1) = 1$; thus we have $c(-1)(-2)\cdots(-1-n) = 1$ and so $c = (-1)^{n+1}/(n+1)!$. Now plug in $x = n + 1$ and obtain $Q(n + 1) = c(n + 1)(n)\cdots(1) = (-1)^{n+1}$; since $Q(x) = (x + 1)P(x) - x$ we conclude that $P(n + 1) = (n + 1 + (-1)^{n+1})/(n + 2)$. ■

More interesting are applications where polynomials do not explicitly appear; very often, introducing polynomials can be useful in proving algebraic identities.

Example 2 *Let $0 \leq m \leq n$ with m even. Prove that $|\binom{n}{0}\binom{n}{m} - \binom{n}{1}\binom{n}{m-1} + \binom{n}{2}\binom{n}{m-2} - \cdots + \binom{n}{m}\binom{n}{0}| = \binom{n}{m/2}$.*

Solution: The factorization $(x - 1)(x + 1) = (x^2 - 1)$ yields $(x - 1)^n(x + 1)^n = (x^2 - 1)^n$. We will obtain our desired identity from looking at coefficients of these polynomials. On one hand, by the binomial theorem, we have $(x - 1)^n = \sum_{i=0}^n \binom{n}{i}(-1)^{n-i}x^i$ and $(x + 1)^n = \sum_{i=0}^n \binom{n}{i}x^i$; therefore, from our expression for multiplying polynomials, we have

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

On the other hand, we can simply expand $(x^2 - 1)^n$ by the binomial theorem and obtain $\sum_{i=0}^n (-1)^{n-i}\binom{n}{i}x^{2i}$. These polynomials are equal, so we can equate coefficients of x^m to see that $(-1)^n \sum_{i+j=m}(-1)^i\binom{n}{i}\binom{n}{j} = (-1)^{n-(m/2)}\binom{n}{m/2}$. This yields our desired result, with a bonus (the sign of the left side). ■

The technique of turning a list of numbers into the coefficients of a polynomial and using the properties of the polynomial to study its coefficients is common and extremely useful. Such polynomials are called *generating functions*; they "generate" their coefficients. More commonly, generating functions are infinite rather than finite polynomials (properly called *power series*); tragically, these are outside the scope of this talk. Still, finite-degree generating functions can be pretty useful.

To make better use of coefficients, we examine a common situation. Say $f = \sum_{i=0}^{n} c_i x^i$. It might happen that f *splits* into linear factors, i.e. we can write

$$f(x) = c(x - r_1)(x - r_2) \cdots (x - r_n)$$

for a scalar c. (Note the number of factors must equal $\deg f$.) Then the r_i are necessarily roots of f, and it is easy to see they are the only possible roots (since whenever $f = 0$ some factor must be 0). Indeed, we have seen that this situation must occur if f has n distinct roots. If not, it can still happen; then some factor $x - r_i$ occurs more than once and we say this r_i is a *multiple root.* Its *multiplicity* is the number of times it occurs.

So what's so great about splitting? Well, if we multiply out the expression $c(x - r_1) \cdots (x - r_n)$, we get a new polynomial in x whose coefficients are expressed in terms of the roots. But this polynomial was equal to f, and so we can equate coefficients. What we get is $c_n = c, c_{n-1} = -c(r_1 + r_2 + \cdots + r_n), c_{n-2} = c[(r_1r_2 + r_1r_3 + \cdots + r_1r_n) + (r_2r_3 + \cdots + r_3r_n) + \cdots + r_{n-1}r_n]$ and, in general, c_{n-i} is $(-1)^i c$ times the sum of all possible products of i of the roots. In particular, $c_0 = (-1)^n r_1 r_2 \cdots r_n$. These expressions for the coefficients of a polynomial in terms of its roots (most convenient to state when f is monic, i.e. $c = 1$) are called Viète's formulas.

Also, one particularly important polynomial is $x^n - 1$ for positive integers n. In the complex plane, it is well known that $\zeta = \cos 2\pi/n + i \sin 2\pi/n$ (abbreviated cis $2\pi/n$) is a root of this polynomial; this follows from DeMoivre's theorem, $(\text{cis } \theta)^n = \text{cis } n\theta$. Moreover, the numbers $1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}$ are all different and (by trusty DeMoivre again) are all roots of $x^n - 1$. It follows that we can write

$$x^n - 1 = (x - 1)(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1}).$$

The roots of this polynomial are called *nth roots of unity.* Viète's formulas applied to this polynomial give some neat identities. We'll have more to say about roots of unity later; for now, suffice it to say: they rock. Now let's go back to problemland and apply what more we've learned.

Example 3 *Let $P_1P_2 \cdots P_n$ be a regular n-gon inscribed in a circle of unit radius. Find the product of distances: $P_1P_2 \cdot P_1P_3 \cdot P_1P_4 \cdots P_1P_n$. (This can be used to find the product of all the sides and diagonals of the polygon.)*

Solution: Let $\zeta = \text{cis } 2\pi/n$. From our factorization of $x^n - 1$, we conclude that $(x - \zeta)(x - \zeta^2) \cdots (x - \zeta^{n-1}) = (x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \cdots + x + 1$. Now consider the points $1, \zeta, \cdots, \zeta^{n-1}$ in the complex plane; these form a regular n-gon inscribed in the unit circle (centered at the origin). Consequently, we can let $P_i = \zeta^{i-1}$ and then the product we are looking for is just $|1 - \zeta| \cdot |1 - \zeta^2| \cdots |1 - \zeta^{n-1}| = |(1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{n-1})| = |1^{n-1} + 1^{n-2} + \cdots + 1| = n.$ ■

The next example is more difficult, but it would be absolutely criminal to leave without one little application of Viète's formulas.

Example 4 *(MOP 1998) Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be two sequences of distinct numbers such that $a_i + b_j \neq 0$ for all i, j. Suppose c_{jk} are n^2 numbers (each of j, k can range from 1 to n) such that, for fixed i and k, we have the relation*

$$\sum_{j=1}^{n} \frac{c_{jk}}{a_i + b_j} = \begin{cases} 1 & \text{if } i = k \\ 0 & \text{otherwise.} \end{cases}$$

Show that the sum of all the c_{jk} is $a_1 + \cdots + a_n + b_1 + \cdots + b_n$.

Solution: We define the polynomial

$$f(x) = (x + b_1)(x + b_2) \cdots (x + b_n) - \sum_{j=1}^{n} \sum_{k=1}^{n} c_{jk}(x + b_1)(x + b_2) \cdots (x + b_{j-1})(x + b_{j+1}) \cdots (x + b_n).$$

(Thus the last product contains all factors $(x+b_l)$ except when $l=j$.) Observe that the polynomial f is monic of degree n. Moreover, the coefficient of x^{n-1} is $\sum_{l=1}^n b_l - \sum_{j=1}^n \sum_{k=1}^n c_{jk}$. Now, we claim that a_i is a root of this polynomial for each i. Then, since these numbers are distinct, they are all the roots of f and so, by Viète, the coefficient of x^{n-1} is $-\sum_{i=1}^n a_i$. Equating this with our previous expression will yield our result.

To prove our claim, choose a value of i. We consider the given identity and multiply both sides by $(a_i+b_1)(a_i+b_2)\cdots(a_i+b_n)$. The result is

$$\sum_{j=1}^n c_{jk}(a_i+b_1)\cdots(a_i+b_{j-1})(a_i+b_{j+1})\cdots(a_i+b_n) = \begin{cases} (a_i+b_1)(a_i+b_2)\cdots(a_i+b_n) & \text{if } i=k \\ 0 & \text{otherwise.} \end{cases}$$

If we add over all possible values of k, then since we have $i=k$ exactly once we get $\sum_j \sum_k c_{jk}(a_i+b_1)\cdots(a_i+b_{j-1})(a_i+b_{j+1})\cdots(a_i+b_n) = (a_i+b_1)(a_i+b_2)\cdots(a_i+b_n)$. But this implies $f(a_i)=0$, which demonstrates our claim and completes the proof. ■

3 Analytic behavior

When we treat a polynomial as a function which can be evaluated, many questions about its behavior arise. In particular, we can ask when and where it has roots. If we are looking at a polynomial over $\mathbb{R}$ or $\mathbb{C}$, the question of "where" becomes particularly imbued with meaning because the real line and the complex plane lend themselves to natural geometric interpretation. Indeed, over the reals in particular, the graph of a polynomial has some basic visual properties worthy of investigation. Unfortunately, because these fields are objects from analysis, this purely algebraic talk cannot draw on them directly, and so some proofs will necessarily be omitted.

One striking result concerns when a polynomial splits. It turns out that, if we are working over $\mathbb{C}$, this is always true.

Theorem 15 *(Fundamental theorem of algebra) If $f(x) = \sum_{i=0}^n c_i x^i$ is a polynomial over the complex numbers, then*

$$f(x) = c_n(x-r_1)(x-r_2)\cdots(x-r_n)$$

for some complex numbers r_i. ■

Everyone calls this the "fundamental theorem of algebra," but, strictly speaking, everyone's wrong. It is actually a theorem of analysis (hence the absentee proof). However, it has substantial algebraic implications. For example, we can now identify exactly which polynomials in $\mathbb{C}[x]$ are irreducible. Every linear polynomial is irreducible, since if it could factor into two nonconstant polynomials, its degree would be $\geq 1+1>1$, contradiction. However, the fundamental theorem tells us that any polynomial of higher degree splits into linear factors, and so the linear polynomials are the only irreducibles. (The property of $\mathbb{C}$ stated in the theorem - that every polynomial splits - has a name; we say $\mathbb{C}$ is *algebraically closed.*)

We can also identify the irreducible polynomials over the reals using this result.

Lemma 16 *If $a+bi$ is a complex root of the polynomial $f \in \mathbb{R}[x]$, where a,b are real, then $a-bi$ is also a root of f.*

Proof: Note that complex conjugation (the function on the complex plane sending $a+bi$ to $a-bi$) preserves sums and products. Since a polynomial is a function computable by a finite sequence of sums and products, we see that the complex conjugate of $f(x)$ is $\bar{f}(\bar{x})$, where the bars denote conjugation and $\bar{f}$ means the polynomial whose coefficients are the conjugates of those of f. But since f is real, each coefficient is its own conjugate, i.e. $f=\bar{f}$ and so we have $0 = f(a+bi) = f(\overline{a+bi}) = f(a-bi)$. ■

This lemma is useful in its own right - it implies that the nonreal roots of a real polynomial come in complex conjugate pairs. A stronger version - that each root has the same multiplicity as its conjugate - can be proved from the following:

Corollary 17 *The irreducible polynomials in $\mathbb{R}[x]$ are the linear polynomials and the quadratics of the form $ax^2 + bx + c$ for which $b^2 - 4ac < 0$.*

Proof: We know that linear polynomials are irreducible. These quadratics are also irreducible: any quadratic which is reducible must reduce to two linear factors, and every linear polynomial has a root; thus every reducible quadratic has real roots, but by the quadratic formula, our particular polynomials have no real roots. Now, we must show that these are the only irreducibles. Note that if a quadratic satisfies $b^2 - 4ac \geq 0$ then its roots r_1, r_2 are real and it is a scalar multiple of $(x - r_1)(x - r_2)$, so it is reducible. Hence we need look only at polynomials f of degree $n > 2$.

By the fundamental theorem, such a polynomial has a complex root. If this root r is real, f is divisible by $x - r \in \mathbb{R}[x]$ and so is reducible over $\mathbb{R}$. On the other hand, if we have a nonreal root $a + bi$, then by the last lemma, $a - bi$ is a root and, by corollary 12, f is divisible by $(x-a-bi)(x-a+bi) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$; thus it has a factor of degree $2 < n$ and so is again reducible. ■

Let's now consider some distinctly graphical properties of polynomials over the real numbers. One easy question is end behavior: where does $f(x)$ go as x goes to $\pm\infty$? We know that x^n becomes large and positive when x goes either way if n is even, and it becomes large of the same sign as x if n is odd. Unamazingly, any monic polynomial of degree n does the same, since the leading term "dominates" the others. The proof is an unremarkable computational argument, which we omit.

Proposition 18 *Let $f \in \mathbb{R}[x]$ be monic of degree n, and choose $y \in \mathbb{R}$. If n is even, we can choose x_0 such that $f(x) > y$ when $x > x_0$ and x_1 such that $f(x) > y$ when $x < x_1$. If n is odd, we can choose x_0 such that $f(x) > y$ when $x > x_0$ and x_1 such that $f(x) < y$ when $x < x_1$.* ■

We can generalize this to any polynomial: the same result holds if the leading coefficient is positive; if it is negative, just switch the signs. Also, a corollary is that a polynomial of even degree cannot take on both positive and negative values of arbitrarily large magnitude: let it be monic for simplicity; then it has positive values for sufficiently large positive or negative x, so it can have negative values for only a bounded set of x's, and by the Extreme Value Theorem (another analytic result), these values must be bounded.

Now, it follows from the Intermediate Value Theorem (yet more analysis) that if a real polynomial has negative value at x_0 and positive value at x_1, it must have a zero somewhere between x_0 and x_1. In particular, using $y = 0$, the preceding proposition shows that every polynomial of odd degree has both positive and negative values and therefore has a real root. Note we could also have proven this using corollary 17, since if there are no real roots, the polynomial factors entirely into quadratics, but no polynomial of odd degree can do this.

Let's look at another aspect of real polynomials: behavior near roots. In particular, we wonder when the polynomial crosses the x-axis.

Proposition 19 *Let r be a real root of $f \in \mathbb{R}[x]$ with multiplicity m. Then, in any small enough neighborhood of r (i.e. open interval containing r), all values of f are of the same sign if m is odd, and f takes on values of opposite signs if m is even.*

Proof: We know we can factor $f(x) = (x - r)^m g(x)$ where $x - r \not| \, g$, i.e. r is not a root of g. Since g has finitely many roots, they have a minimum distance from r, so for our "small enough" intervals we can simply choose those containing no roots of g. By the intermediate value theorem, then, g must have the same sign throughout such an interval; assume it is positive (the other case is analogous). If m is even then $(x - r)^m \geq 0$ for all x, so $f(x) = (x - r)^m g(x) \geq 0$ throughout our interval. Conversely, if m is odd then $(x - r)^m > 0$ for $x > r$ and < 0 for $x < r$, so $f(x) > 0$ for $x > r$ and < 0 for $x < r$, giving what we need. ■

This technique of inequalities allows one to estimate all the roots of $f(x) + \epsilon$ for small ϵ if the factorization of f (into linears) is known. It can also be shown (using calculus methods) that the graph of f is tangent to the x-axis at r iff r is a multiple root.

There are other techniques which are useful for estimating the population and location of roots; we state a couple of the most common without proof. The first is a special case of Rolle's Theorem from calculus; the second is algebraic, but we omit the proof anyway, in accordance with contemporary custom.

Theorem 20 *(Rolle) Take the real polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$ and define the formal derivative $f'(x) = \sum_{i=1}^{n} i c_i x^{i-1}$. Then between any two distinct roots of f there lies a root of f'.* ■

Theorem 21 *(Descartes's Rule of Signs) Take the real polynomial $f(x) = \sum_{i=0}^{n} c_i x^i$ and suppose there are m sign changes. Then the number of positive real roots of f equals $m - 2k$ for some nonnegative integer k. This rule applied to $f(-x)$ also estimates the number of negative roots of f. (To be precise, a sign change means a pair of exponents $(i,j), i < j$, such that $c_i c_j < 0$ and there does not exist any k for which $i < k < j$ and $c_k \neq 0$.)* ■

4 More identities!

There are several more interesting elementary computational formulas, so these will now be presented, albeit in a desultory and chaotic manner.

If $f_0, f_1, \ldots, f_{n+1}$ are polynomials of degree at most n, one can show, using techniques of linear algebra, that there exist constants $c_0, c_1 \ldots, c_{n+1}$, not all zero, such that $c_0 f_0 + c_1 f_1 + \cdots + c_{n+1} f_{n+1} = 0$. In other words, the polynomials can be linearly combined to obtain the zero polynomial. Let's now look at an interesting special case of this.

For a polynomial f of degree n, we can define the *finite difference* Δf by $\Delta f(x) = f(x) - f(x-1)$. Write $f(x) = \sum_{i=0}^{n} c_i x^i$; then, by corollary 3, we know that $f(x-1) = \sum_{i=0}^{n} (\sum_{j=i}^{n} \binom{j}{i} c_j (-1)^{j-i}) x^i$. What matters is that it has degree n and leading coefficient c_n. So in the difference $f(x) - f(x-1)$, the leading coefficients cancel and we're left with a polynomial of degree strictly less than n. Now keep taking finite differences, and see what we get:

Proposition 22 *If f is a polynomial of degree n, then $\sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} f(x-i) = 0$ for all x.*

Proof: Define $\Delta^0 f = f$ and $\Delta^{k+1} f = \Delta(\Delta^k f)$ inductively. We claim both sides of our equation equal $\Delta^{n+1} f$. The right side is easy: it's not hard to see by induction (since Δ decreases degrees) that $\Delta^k f$ has degree $\leq n-k$; in particular, $\Delta^{n+1} f$ has degree less than 0 and so is zero.

For the left side, we claim that $\Delta^k f = \sum_{i=0}^{k} (-1)^i \binom{k}{i} f(x-i)$ for all polynomials f, and our result will follow. This claim is shown by induction. For $k = 0$ it is trivial. If it holds for k, then let $g = \Delta^k f$, so $\Delta^{k+1} f = g(x) - g(x-1) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} f(x-i) - \sum_{j=0}^{k} (-1)^j \binom{k}{j} f(x-1-j) = \sum_{i=0}^{k+1} (-1)^i \binom{k}{i} f(x-i) - (-1)^{i-1} \binom{k}{i-1} f(x-i)$ (from the substitution $i = j+1$) $= \sum_{i=0}^{k+1} (-1)^i \binom{k+1}{i} f(x-i)$ as claimed. ■

Corollary 23 *If f has degree n, then for any scalar a, $\sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} f(x-ia) = 0$.*

Proof: Apply the proposition to the function $f(ax)$, making a change of variables as needed. ■

Now let's go back to a more practical task: retrieving a polynomial from some values. We've seen that one can get plenty of information of the roots of a polynomial are known. We also saw (in example 1) that a clever trick that creates roots of a new polynomial may lead us to an answer in special cases. But what if you only know the values at some random places? With a tolerance for mild ugliness, one can always reconstruct a polynomial given enough values. In particular, given a list of distinct field elements $x_0, x_1, \ldots, x_n$ and (not necessarily distinct) values $y_0, y_1, \ldots, y_n$, one can find a degree-n polynomial f satisfying $f(x_i) = y_i$.

First consider a special case. Fix k and suppose all the y_i are 0 for $i \neq k$. The polynomial $(x-x_0)(x-x_1)\cdots(x-x_{k-1})(x-x_{k+1})\cdots(x-x_n)$ (seen it before?) then has degree n, value 0 when $x = x_i \neq x_k$ (since the factor $x - x_i$ is 0), and value $(x_k - x_0)\cdots(x_k - x_{k-1})(x_k - x_{k+1})\cdots(x_k - x_n) \neq 0$ at $x = x_k$. From here it's not too hard to see the general case looming on the horizon.

Proposition 24 *(Lagrange interpolation) Let $x_0, \ldots, x_n$ be distinct numbers, and let $y_0, \ldots, y_n$ also be given. Then there exists a unique polynomial f of degree at most n such that $f(x_i) = y_i$ for $y = 0, 1, \ldots, n$. If we abbreviate $f_k(x) = (x-x_0)\cdots(x-x_{k-1})(x-x_{k+1})\cdots(x-x_n)$, then our function is given by*

$$f(x) = \frac{y_0}{f_0(x_0)} f_0(x) + \frac{y_1}{f_1(x_1)} f_1(x) + \cdots + \frac{y_n}{f_n(x_n)} f_n(x).$$

Proof: Uniqueness comes from corollary 14, so we need only prove that the given formula works. Since the ith term is a scalar multiple of f_i (and is defined because its denominator is nonzero), which has degree n, it is clear that the sum does indeed have degree at most n. And, evaluating $f(x_i)$, we see that the ith term is $[y_i / f_i(x_i)] f_i(x_i) = y_i$ and all other terms are zero, so we have $f(x_i) = y_i$. ■

Corollary 25 *If $x_1, \ldots, x_n$ are distinct numbers and $y_1, \ldots, y_n$ are also given, there exists a unique monic polynomial f of degree n satisfying $f(x_i) = y_i$ for all i.*

Proof: By the interpolation formula there exists g of degree $\leq n-1$ such that $g(x_i) = y_i - x_i^n$ for each i, so $f(x) = x^n + g(x)$ does the trick. To see that it is unique, suppose two monic polynomials of degree n have the desired values; then their difference is of degree $\leq n-1$ (since leading coefficients cancel) and has the n roots $x_1, \ldots, x_n$, so by corollary 13 it is zero and our two polynomials are equal. ■

In principle, we now know how to retrieve a polynomial from its values. However, the task could be real drudgery if we don't have nice numbers, so Lagrange interpolation is not always the best way to extract information about a polynomial. There are some common special cases where happier methods are available.

One is the situation of "value matching." Suppose we are given a polynomial f of large degree. We are also given distinct $x_0, \ldots, x_n$ as usual, and we want a polynomial g of degree at most n such that $g(x_i) = f(x_i)$. Thus, from the vantage point of the x_i, f and g are indistinguishable, but we want to limit the degree of g. This turns out to be simple: let g be the remainder when f is divided by $(x-x_0)\cdots(x-x_n)$. Indeed, g has degree less than $\deg(x-x_0)\cdots(x-x_n) = n+1$, and since $f-g$ is divisible by $(x-x_0)\cdots(x-x_n)$, each x_i is a root of $f-g$, so that $f(x_i) = g(x_i)$. Also, if we are given just n values of x and the requirement that g be monic, we can again apply this process by the same method as in corollary 25: find $h(x)$ of degree at most $n-1$ which matches the values of $f(x) - x^n$, and then $g(x) = h(x) + x^n$ meets our needs.

A cooler situation (working over $\mathbb{C}$) is when the x_i are roots of unity. Specifically, suppose we are given the values of f at mth roots of unity for some m. If $m > n$ we have a slick formula for coefficients of f. If $m \leq n$ we can't find out all the coefficients, but we can still get some useful info. In fact, we'll provide a more general result: stuff that happens when we know the values of f at products of each root of unity with some constant.

Lemma 26 *Let $\zeta = cis\ 2\pi/m$. For positive integers k, we have $1 + \zeta^k + \zeta^{2k} + \cdots + \zeta^{(m-1)k} = m$ if m divides k and 0 otherwise.*

Proof: In the first case, we have $\zeta^{ik} = 1^i = 1$ and the result is clear. In the second case, $\zeta^k \neq 1$. Since we can write $1 + x + x^2 + \cdots + x^{m-1} = (x^m - 1)/(x-1)$, the given sum equals $(\zeta^{mk} - 1)/(\zeta^k - 1) = 0$, since $\zeta^m = 1$ and the denominator is nonzero. ■

Proposition 27 *Let $f = \sum_{i=0}^n c_i x^i$ be an arbitrary polynomial and $\zeta = cis\ 2\pi/m$. Then $f(x) + f(\zeta x) + f(\zeta^2 x) + \cdots + f(\zeta^{m-1} x) = m \sum_{m \mid i} c_i x^i$. (The sum is over all i divisible by m.)*

Proof: Our sum is $\sum_{j=0}^{n-1} f(\zeta^j x) = \sum_{j=0}^{n-1} \sum_{i=0}^n c_i (\zeta^j x)^i = \sum_{i=0}^n \sum_{j=0}^{n-1} c_i (\zeta^j)^i x^i = \sum_{i=0}^n c_i x^i (\sum_{j=0}^{n-1} \zeta^{ij})$. By the lemma the inner sum is m if i is divisible by m and is 0 otherwise, which gives what we need. ■

Corollary 28 *If $f = \sum c_i x^i$ and $\zeta = cis\ 2\pi/m$, then $\sum_{i=0}^{m-1} f(\zeta^i x)/\zeta^i = m \sum_i c_i x^i$, where the latter sum is over all i such that $i \equiv k \pmod{m}$.*

Proof: Since $\zeta^{-jk} = \zeta^{(m-k)j} = (\zeta^j)^{m-k}$, this follows from the preceding result, using the polynomial $x^{m-k} f(x)$ in place of f and dividing out by x^{m-k} afterward. ■

Thus, for example, if $m = 2$, we can extract the terms with even powers of x as $(f(x) + f(-x))/2$ and those with odd powers of x as $(f(x) - f(-x))/2$. Also note that, if $m > n$, then the sum in corollary 28 gives us a single term, and then plugging in $x = 1$ easily gives us the coefficients when we know the values of f at mth roots of unity.

We now ramble into trigonometry, an arena for applying our knowledge of polynomials (and roots of unity). The key connection is the representation of an angle θ by the complex number cis θ. Using the familiar equality $\text{cis}\,\theta\,\text{cis}\,\psi = \text{cis}\,(\theta + \psi)$, we can perform some operations on these and obtain useful trigonometric identities after extracting real and imaginary parts. Hopefully it becomes clear soon how this is done.

We can consider what happens to cis θ under the polynomial x^n. We know (from DeMoivre if nowhere else) that the value is cis $n\theta$, or, explicitly, $(\cos\theta + i\sin\theta)^n = \cos n\theta + i \sin n\theta$. If we expand the left side by the binomial theorem and look at its real part, this part consists of all terms where i occurs to an even power, which means the exponent of $i\sin\theta$ must be even and so we have some power of $\sin^2\theta$ in each term.

By rewriting these terms using $\sin^2\theta = 1 - \cos^2\theta$, we can turn $\cos n\theta$ into a polynomial function of $\cos\theta$. Doing this for each n leads to the Chebyshev polynomials, which are so all-important that they are the central topic of an upcoming BMC session.

A related topic is the expressibility of $\tan n\theta$ as a *rational function* (i.e. ratio of two polynomials) of $\tan\theta$. Assuming $|\theta| < \pi/2$, let $x = 1 + i\tan\theta$. Although x is not on the unit circle, it does have argument (angle) θ, and so x^n has argument $n\theta$. However, this means $\tan n\theta$ is the ratio of the imainary and real parts of $x^n = (1 + i\tan\theta)^n$, which are easily seen to be polynomials in $\tan\theta$ (with integer coefficients). Thus $\tan n\theta$ can be expressed as a rational function of $\tan\theta$. In like manner, one can derive the expression for the tangent of a sum of distinct angles in terms of their individual tangents.

We can apply polynomials in a more substantial way. There exist formulas (not necessarily pleasant ones) for sums of sines and cosines of angles in arithmetic progressions. The conventional proofs involve somewhat tedious trigonometric manipulations; we shall remedy that, so that only the formulas themselves are ugly.

Suppose we want to find $\cos(\theta)+\cos(\theta+\psi)+\cos(\theta+2\psi)+\cdots+\cos(\theta+(n-1)\psi)$ or the sum of the sines of these angles. These are, respectively, the real and imaginary parts of $\sum_{j=0}^{n-1} \text{cis } (\theta+j\psi) = \sum_{j=0}^{n-1} \text{cis } \theta \,\text{cis } j\psi = \text{cis } \theta \sum_{j=0}^{n-1} (\text{cis } \psi)^j$. From our knowledge of polynomial factorizations we see that the sum is expressible as $([\text{cis } \psi]^n - 1)/(\text{cis } \psi - 1) = (\text{cis } n\psi - 1)/(\text{cis } \psi - 1)$. Now we have a closed-form expression, and with a little more work, we can extract its real and imaginary parts. However, the resulting formulas are not presented here, for the sake of space. (See the problems.) Further trigonometric identities may be obtained by a similar analysis of other polynomials, but right now, there's better stuff to do.

5 Integers and rationals

Let's look now at polynomials defined over $\mathbb{Q}$. This turns out to be a deep topic, so we'll just touch on some key ideas. First, however, considering that the structures of the rationals $\mathbb{Q}$ and the integers $\mathbb{Z}$ are closely related, it might make sense to look at polynomials over $\mathbb{Z}$.

Earlier it was said we would only consider polynomials over a field. That was a lie. $\mathbb{Z}$ is not a field; it is, however, an *integral domain*, which is like a field, except that the hypothesis of having multiplicative inverses is replaced by the weaker statement that any two nonzero elements have nonzero product. Many of the results from Section 2 are still valid over an integral domain with only slight changes. Thus, we can still find greatest common divisors and can still define irreducibles; irreducible polynomials in $\mathbb{Z}[x]$ are either constant polynomials of prime value or nonconstant polynomials which cannot be factored into two nonconstant polynomials and whose coefficients are relatively prime. We can also carry out the division algorithm as long as the divisor has leading coefficient ± 1.

First, let's take a light-spirited look at some properties of polynomials over the integers.

Lemma 29 *For all integers a, b and positive integers n, $a^n - b^n$ is divisible by $a - b$.*

Proof: $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1})$. ■

Corollary 30 *If f is an integer polynomial and a, b are integers, then $f(a) - f(b)$ is divisible by $a - b$.*

Proof: Write $f(x) = \sum_{i=0}^{n} c_i x^i$, so that $f(a) - f(b) = \sum_{i=0}^{n} c_i(a^i - b^i)$. By the lemma, each term is divisible by $a - b$, so the sum is also. ■

A large part of the study of rational (and integer) polynomials involves identifying irreducibles. We'll go further into this from a serious angle, but first here's one nice sample result.

Proposition 31 *Let $x_1, x_2, \ldots, x_n$ be distinct integers, where n is odd. Then the polynomial $f(x) = (x - x_1)\cdots(x - x_n) + 1$ is irreducible in $\mathbb{Z}[x]$.*

Proof: Since the polynomial is monic, its coefficients are relatively prime, so we need only consider nonconstant factorizations. Thus suppose $f = gh$ where g, h have integer coefficients and are nonconstant. Since $f(x_i) = 1$ for each i, we see we have $g(x_i), h(x_i) = \pm 1$ since they must be integers. In particular, by the pigeonhole principle, there are at least $(n+1)/2$ values of i for which $g(x_i)$ has the same sign - say, $+1$. Then we see that $g(x)-1$ has at least $(n+1)/2$ roots, so $g(x)-1$ (which is nonconstant) has degree at least $(n+1)/2$

and so does g. Similarly, h has degree at least $(n+1)/2$. But this implies $n = \deg f = \deg g + \deg h \geq n+1$, a contradiction. ■

With a bit more work and the aid of corollary 30, this result can be strengthened to hold for any integer $n \geq 5$.

We can look briefly at polynomials $f(x)$ with integer values whenever x is an integer; these need not actually have integer coefficients. If f has degree n and takes on integer values for $x = 0, 1, \ldots, n$, then $f(x)$ is an integer whenever x is an integer; this follows easily using the recursion from proposition 22 and an induction argument. A complete characterization of these polynomials appears in the problems, along with some other fun stuff.

Now let's look at the structural relationships between $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. Some obvious connections exist: for example, everything in $\mathbb{Z}[x]$ is a scalar multiple of something monic in $\mathbb{Q}[x]$ (just divide by the leading coefficient), and conversely, everything in $\mathbb{Q}[x]$ is a scalar multiple of something in $\mathbb{Z}[x]$ (just multiply by the product of all the coefficients' denominators). However, there are more important relations. Gauss's lemma (one of a zillion results with that name) lends insight here.

Lemma 32 *Suppose p is a prime and $f, g \in \mathbb{Z}[x]$ are such that fg is divisible by p (i.e. each coefficient of fg is a multiple of p). Then either f or g is divisible by p.*

Proof: Write $f(x) = \sum_{i=0}^{n} c_i x^i, g(x) = \sum_{j=0}^{m} d_j x^j$. Suppose our result is not true, so each of our factors has a coefficient not divisible by p. Let i_0 be the smallest exponent for which c_{i_0} is not divisible by p, and define j_0 similarly. Now look at the coefficient of $x^{i_0+j_0}$ in the product fg. We know it can be expressed as $\sum_{i+j=i_0+j_0} c_i d_j$; now consider all the pairs (i,j) involved. If $i > i_0$ then $j < j_0$ and d_j is divisible by p; if $i < i_0$ then c_i is divisible by p. So every term in our sum is divisible by p except $c_{i_0} d_{j_0}$, which is not divisible by p, since neither c_{i_0} nor d_{j_0} is. Consequently the sum is not divisible by p, but since the sum is a coefficient of fg, we get a contradiction. ■

Proposition 33 *(Gauss's lemma) If $f \in \mathbb{Z}[x]$ is nonconstant and irreducible, then it is irreducible in $\mathbb{Q}[x]$.*

Proof: We will show something stronger: if $f = gh$ where $g, h \in \mathbb{Q}[x]$, then we can also write $f = (ag)(bh)$ where $ag, bh \in \mathbb{Z}[x]$ (and $a, b \in \mathbb{Q}$). Then our result follows, since assuming that f can be written as a product of two nonconstant polynomials over $\mathbb{Q}$ leads to a contradiction in $\mathbb{Z}[x]$.

If we let a be the (positive) least common multiple of all coefficients of g, and define b similarly for h, then ag, bh have integer coefficients and we have $(ab)f = (ag)(bh)$. Thus we have shown some positive integer k exists for which kf can be written as a product of scalar multiples of g and h with both of these multiples lying in $\mathbb{Z}[x]$. Now choose the smallest possible k with this property. We seek to show that $k = 1$, since then we have an expression for f in the desired form. So assume $k > 1$ and let p be a prime factor of k. Writing $p(k/p)f = (ag)(bh)$ for some $ag, bh \in \mathbb{Z}[x]$, we see by the lemma that either ag or bh is divisible by p. Hence we can write $(k/p)f = (ag/p)(bh)$ or $(ag)(bh/p)$ such that both factors on the right have integer coefficients. Since $k/p < k$ is a positive integer, we have violated the minimality of k, giving the needed contradiction. ■

Gauss's lemma is key to understanding irreducible polynomials over $\mathbb{Q}$, since it is generally easier for us to work over $\mathbb{Z}$ than over $\mathbb{Q}$. So, let's go hunt down some irreducibles! One place to start is the famous Eisenstein criterion:

Proposition 34 *(Eisenstein criterion) Let $f \in \mathbb{Z}[x]$, and suppose p is a prime such that the leading coefficient of f is not divisible by p but all other coefficients are; further suppose that the constant term is not divisible by p^2. Then f is irreducible over $\mathbb{Q}$.*

Proof: We can safely divide out any common factor of all coefficients of f, so assume now the gcd of the coefficients is 1. Then, by Gauss's lemma, it suffices to show that f is not a product of two nonconstant polynomials over $\mathbb{Z}$. Suppose, then, that $f(x) = g(x)h(x)$ with $g(x) = \sum_{i=0}^{n} c_i x^i, h(x) = \sum_{j=0}^{m} d_j x^j$ with the coefficients integers. Since the leading coefficient of f is $c_n d_m$, we see that neither g nor h has leading coefficient divisible by p. Now choose the smallest i_0 with c_{i_0} not divisible by p (since we know some such exists) and analogously choose the smallest possible j_0. Just as in the proof of lemma 32, we see that the coefficient of $x^{i_0+j_0}$ in the product $f = gh$ is not divisible by p, and so it must be the leading coefficient: $i_0 + j_0 = n + m \Rightarrow i_0 = n, j_0 = m$. By the assumption that g, h are nonconstant, the minimality of i_0, j_0

implies that c_0 and d_0 are divisible by p. But then the constant term of $f = gh$ is $c_0 d_0$, divisible by p^2. This is a contradiction. ■

This criterion can be applied in some fairly obvious ways; for example, $x^{279} - 2$ is irreducible (take $p = 2$). We include the classic example of a not-so-obvious application; we assume slight number-theoretic foreknowledge.

Example 5 *Let p be a prime; show that $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible over the rationals.*

Solution: The Eisenstein criterion cannot be applied in the present state. However, consider that $f(x) = g(x)h(x)$ iff $f(x+1) = g(x+1)h(x+1)$, and it follows that it suffices to show the irreducibility of $f(x+1)$. Now $f(x) = (x^p - 1)/(x-1)$, so $f(x+1) = ([x+1]^p - 1)/([x+1] - 1) = ([x+1]^p - 1)/x$. By the binomial theorem, we have $(x+1)^p = \sum_{i=0}^{p} \binom{p}{i} x^i$ and it follows that $f(x+1) = \sum_{i=1}^{p} \binom{p}{i} x^{i-1}$. Now every coefficient is divisible by p except the leading coefficient (which is 1); moreover, the constant term is p which is not divisible by p^2. So now we can apply Eisenstein and obtain our result. ■

Another way of finding irreducibles of small degree is by the rational root theorem. If a polynomial of degree 2 or 3 factors, it must break into two linears or a linear and a quadratic, respectively; since every linear polynomial has a root, we can show irreducibility of anything of degree 2 or 3 if we can show the nonexistence of roots. There's a tool for this: we can restrict the set of possible roots so we only have finitely many things to test.

Theorem 35 *(Rational root) Suppose $f(x) = \sum_{i=0}^{n} c_i x^i$ is an integer polynomial, and assume it has a rational root expressible in lowest terms as p/q. Then $p \mid c_0$ and $q \mid c_n$.*

Proof: We can write $f(p/q) = 0$ or $\sum c_i (p/q)^i = 0$; multiplying by q^n gives $\sum c_i p^i q^{n-i} = 0$. On the left side, every term except the last is clearly divisible by p, so the $c_0 q^n$ term must also be divisible by p. Since p, q are relatively prime we conclude p divides c_0. Similarly, all terms but the first have clear factors of q, so the first term $c_n p^n$ is also divisible by q and $q \mid c_n$. ■

Now let's look at the complex roots of polynomials with rational coefficients. Often (for example, when the polynomial is irreducible and nonlinear) these roots will not themselves be rational. Thus, $x^2 - 2$ has the irrational root $\sqrt{2}$. A complex number which is a root of a rational polynomial is called an *algebraic number.* (Also, a root of a monic integer polynomial is an *algebraic integer.*) Algebraic number theory is a substantial branch of modern mathematics, crammed with interesting results. One interesting fact is that the set of algebraic numbers is a field and, moreover, is algebraically closed. We're not getting that far here, but a few easier results seem worthwhile.

Proposition 36 *For any algebraic number α there is a unique monic rational polynomial of lowest degree having α as a root; we call it the minimal polynomial of α. Every polynomial with α as a root is divisible by this polynomial, and the minimal polynomial is irreducible over $\mathbb{Q}$.*

Proof: Since α is algebraic it is a root of some polynomial; dividing by the leading coefficient gives a monic polynomial. So α is a root of some monic polynomial, and then we can certainly choose one with lowest possible degree. To see uniqueness, note that given two different such polynomials of degree n, their difference has degree $< n$ and then dividing by the leading coefficient gives a new monic polynomial, contradicting minimality of n. For the second part, if f is the minimal polynomial and $g(\alpha) = 0$, then use the division algorithm and get $g = qf + r$; then $0 = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$. Since r has lower degree than f, the minimality of f shows that $r = 0$ and so $f \mid g$. Finally, if f were not irreducible then we could write $f = gh$ where g, h have lower degree than f, but then $0 = f(\alpha) = g(\alpha)h(\alpha)$ implies that one of g, h has α as a root and so is divisible by f, a contradiction. ■

The *degree* of an algebraic number is the degree of its minimal polynomial. It is not hard to see that every monic irreducible is the minimal polynomial for each of its roots. Also, two numbers with the same minimal polynomial are called *conjugates.* We can use minimal polynomials to get a nice result:

Corollary 37 *Any two rational polynomials with a common complex root have a common (nonconstant) factor in $\mathbb{Q}[x]$.*

Proof: Both are divisible by the minimal polynomial of the common root. ■

Let's take this just one step further and prove a result about roots of irreducibles. If $f(x) = \sum_{i=0}^{n} c_i x^i$, recall the *formal derivative* $f'(x) = \sum_{i=1}^{n} i c_i x^{i-1}$. The following property from calculus will be proven algebraically:

Lemma 38 *For any polynomials f, g, we have $(fg)' = f'g + fg'$.*

Proof: Write $f(x) = \sum c_i x^i, g(x) = \sum d_j x^j$. Then $f' = \sum i c_i x^{i-1}, g' = \sum j d_j x^{j-1}$. We can write out some products: $fg(x) = \sum_k (\sum_{i+j=k} c_i d_j) x^k$, $f'g(x) = \sum_k (\sum_{i-1+j=k} i c_i d_j) x^{i-1+j}$, $fg'(x) = \sum_k (\sum_{i+j-1=k} j c_i d_j) x^{i+j-1}$. Then, adding the last two expressions and making a change of variables (k to $k+1$), we get $f'g + fg'(x) = \sum_k (\sum_{i+j=k} (i+j) c_i d_j) x^{k-1} = \sum_k k (\sum_{i+j=k} c_i d_j) c^{k-1}$ which is just the derivative of our expression for fg. ■

Observe that the formal derivative of a degree-n (rational) polynomial has degree $n-1$. Now we can prove:

Proposition 39 *An irreducible polynomial over $\mathbb{Q}$ has no multiple roots.*

Proof: Suppose α is a multiple root of f, so we can write $f(x) = (x-\alpha)^2 g(x)$. The derivative of $(x - \alpha^2)$ is found to be $2(x-\alpha)$, so lemma 38 gives $f'(x) = (x-\alpha)^2 g'(x) + 2(x-\alpha)g(x)$ which is divisible by $x - \alpha$. Thus f and f' have the common root α, so by corollary 37 they have a common factor. But this factor has smaller degree than f since it divides f'; hence, f is not irreducible. ■

What has been presented in this talk is just the tip of the iceberg. There are far more topics on polynomials to examine, including rational functions, power series, polynomials in multiple variables, and applications to finite fields. However, this should be enough to think about in one day. If you're still eager for more brain fodder, proceed to the next section...

6 Problem time

Some of these are easy, most are hard, and the collection as a whole is long. Do whatever interests you.

1. For positive integers n, m, show that n divides m iff $x^n - 1$ divides $x^m - 1$.

2. If F is a finite field, prove that $F[x]$ contains infinitely many irreducible polynomials. (In fact, it contains irreducibles of every positive degree, but this is harder to show.)

3. Show that any monic polynomial of degree $2n$ (over any field) can be written as $q^2 + r$, where q, r are polynomials and $\deg r < n$.

4. Let r, s, t be the roots of the complex polynomial $x^3 + ax^2 + bx + c$. Find (in terms of a, b, c) a cubic polynomial whose roots are $rs + t, st + r, tr + s$. **Hint:** Viète!

5. Find explicitly three complex numbers x, y, z such that $x + y + z = xy + yz + zx = 3, xyz = 9$.

6. (IMO 1998 proposal) If f is a polynomial of degree n such that $f(i) = 2^i$ for $i = 0, 1, \ldots, n$, find $f(n+1)$.

7. Let $a_0, a_1, \ldots, a_n$ and $b_0, b_1, \ldots, b_n$ be complex numbers such that, for $0 \le k \le 2n$, $\sum_{i+j=k} a_i b_j = 0$ if k is odd and $= a_{k/2}$ if k is even. Assume that $a_0 a_n \neq 0$. Show that $|a_0| = |a_n|$.

8. (Russia 1998) Two lines parallel to the x-axis meet the (real) graph of $y = ax^3 + bx^2 + cx + d$ in the points A, D, E and B, C, F respectively, in alphabetical order from left to right. When the segments AB, CD, EF are projected onto the x-axis, prove that the length of the projection of CD equals the sum of the lengths of the other projections.

9. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be $2n$ distinct complex numbers, where n is even. Form the $n \times n$ matrix whose (i, j)-entry is $a_i + b_j$. If the product of the elements in each row is 1, prove that the product of the elements in each column is -1.

10. Let f be a real polynomial of degree n, and suppose constants $c_0, c_1, \dots, c_n$ satisfy $c_0 f(x) + c_1 f(2x) + c_2 f(4x) + \cdots + c_n f(2^n x) = 0$. Show that $c_i = 0$ for all i.

11. (USAMO 1989) Let P be a polynomial in a complex variable, with real coefficients. Suppose $|P(i)| < 1$. Show that there exist real numbers a, b such that $P(a + bi) = 0$ and $(a^2 + b^2 + 1)^2 < 4b^2 + 1$.

12. If f is a real polynomial of degree n, show that there exists a polynomial g of degree $n + 1$ such that $\sum_{i=1}^{k} f(i) = g(k)$ for every positive integer k.

13. (MOP 1999) Let n and $a_1, a_2, \dots, a_m$ be positive integers. Define the function f as follows: for each integer k let $f(k)$ be the number of ordered m-tuples $(c_1, \dots, c_m)$ of integers such that $c_1 + \cdots + c_m \equiv k \pmod{n}$ and $1 \le c_i \le a_i$ for each i. Show that f is constant if and only if n divides at least one of $a_1, \dots, a_m$.

14. (MOP 1999) Several points are given on a unit circle so that the product of the distances from any point on the circle to the given points does not exceed 2. Prove that the given points are the vertices of a regular polygon. **Hint:** Sums over roots of unity.

15. For angles θ, ψ ($\cos\psi \neq 1$) and positive integer n, find the closed-form expressions for $\sum_{j=0}^{n-1} \cos(\theta + j\psi)$ and $\sum_{j=0}^{n-1} \sin(\theta + j\psi)$.

16. (USAMO 1974) Let P be a polynomial with integer coefficients. Show that there do not exist distinct integers a, b, c with $P(a) = b, P(b) = c, P(c) = a$.

17. Suppose $f \in \mathbb{Z}[x]$, and that there are infinitely many integers x such that $f(x) > 0$. Show that not all such values of $f(x)$ are prime. (Amazingly, this is not true over multiple variables; cf. *Quantum* Jan/Feb 1999, p. 16.)

18. Suppose $f \in \mathbb{C}[x]$ is a polynomial of degree n such that, whenever x is a (real) integer, $f(x)$ is an integer. Denote $f_k(x) = x(x-1)\cdots(x-k+1)/k!$. Show that we can write $f = c_0 f_0 + c_1 f_1 + \cdots + c_n f_n$ for some integers $c_0, c_1, \dots, c_n$. (Note: these are not the coefficients of f.)

19. (USAMO 1995) Suppose $q_0, q_1, \dots$ is an infinite sequence of integers such that $m - n$ divides $q_m - q_n$ for all m, n and that there exists a polynomial P satisfying $|q_n| < P(n)$ for all n. Prove that there exists a polynomial Q with $q_n = Q(n)$ for all n.

20. (Romania 1997) Let $P(x) = \sum_{i=0}^{n} c_i x^i$ be a monic polynomial with positive integer coefficients of degree ≥ 2, and suppose that $c_i = c_{n-i}$ for $i = 0, 1, \dots, n$. Show that there exist infinitely many pairs (x, y) of positive integers such that $P(x)$ is divisible by y and $P(y)$ is divisible by x.

21. For any odd integers a, b, show that the polynomial $x^4 + ax + b$ is irreducible over the rationals.

22. (IMO 1993) For integers $n > 1$, show that $x^n + 5x^{n-1} + 3$ is irreducible in $\mathbb{Z}[x]$. **Hint:** Generalize Eisenstein.

23. Let p be an odd prime; prove that $\sum_{i=0}^{p-2} (p - 1 - i)x^i$ is irreducible over the rationals.

24. (Romania 1997) Let P, Q be monic irreducible polynomials over the rational numbers. Suppose $P(x)$ and $Q(x)$ have respective roots α and β such that $\alpha + \beta$ is rational. Prove that $P(x)^2 - Q(x)^2$ has a rational root.

25. Let $\zeta = \operatorname{cis} 2\pi/n$. The nth *cyclotomic polynomial* Φ_n is defined by $\Phi_n(x) = (x - \zeta)\cdots(x - \zeta^{n-1})$, where the product consists of all factors of the form $(x - \zeta^k)$ where $0 < k < n$ and k, n are relatively prime. (We set $\Phi_1(x) = x - 1$.)

    (a) Show that the product of $\Phi_d(x)$ over all d dividing n is just $x^n - 1$.

    (b) Show that $\Phi_n \in \mathbb{Z}[x]$.