Polynomials

Matthew Rognlie

Department of Mathematics
Duke University

November 11, 2009

Fundamental Theorem of Algebra

The fundamental theorem of algebra states that any polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

has at least one complex root. In fact, a polynomial of degree n will have *exactly* n roots, counting multiplicities. (A root x_i of $P(x)$ has multiplicity m if m is the highest integer such that $(x - x_i)^m$ divides $P(x)$.)

Fundamental Theorem of Algebra

The fundamental theorem of algebra states that any polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

has at least one complex root. In fact, a polynomial of degree n will have *exactly* n roots, counting multiplicities. (A root x_i of $P(x)$ has multiplicity m if m is the highest integer such that $(x - x_i)^m$ divides $P(x)$.)

Thus any such $P(x)$ can be factored uniquely as:

$$P(x) = a_n(x - x_1)(x - x_2) \cdots (x - x_n)$$

where $x_1, x_2, \ldots, x_n$ are its roots, repeated according to multiplicity.

Vieta Relations

If we multiply out the factorization of $P(x)$ on the previous page and equate the resulting coefficients with the coefficients of $P(x)$, we get the following set of relations between symmetric expressions in the roots and the coefficients of $P(x)$:

$$x_1 + x_2 + \ldots + x_n = -\frac{a_{n-1}}{a_n}$$

$$x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n}$$

$$\ldots$$

$$x_1x_2 \cdots x_n = (-1)^n \frac{a_0}{a_n}$$

Make sure you're comfortable with them!

Vieta Relations: Example

Here is an example from the 2009 Duke Math Meet that involves primarily grunt work using with these relations.

Problem

Let r_1, r_2, r_3 be the three (not necessarily distinct) solutions to the equation $x^3 + 4x^2 - ax + 1 = 0$. If a can be any real number, find the minimum possible value of

$$\left(r_1 + \frac{1}{r_1}\right)^2 + \left(r_2 + \frac{1}{r_2}\right)^2 + \left(r_3 + \frac{1}{r_3}\right)^2$$

Vieta Relations: Example

Here is an example from the 2009 Duke Math Meet that involves primarily grunt work using with these relations.

Problem

Let r_1, r_2, r_3 be the three (not necessarily distinct) solutions to the equation $x^3 + 4x^2 - ax + 1 = 0$. If a can be any real number, find the minimum possible value of

$$\left(r_1 + \frac{1}{r_1}\right)^2 + \left(r_2 + \frac{1}{r_2}\right)^2 + \left(r_3 + \frac{1}{r_3}\right)^2$$

Solution

First, note that

$$\begin{aligned} &\left(r_1 + \frac{1}{r_1}\right)^2 + \left(r_2 + \frac{1}{r_2}\right)^2 + \left(r_3 + \frac{1}{r_3}\right)^2 \\ = \ &(r_1^2 + r_2^2 + r_3^2) + (1/r_1^2 + 1/r_2^2 + 1/r_3^2) + 6 \end{aligned}$$

Solution (Continued)

Solution

We will relate these expressions to the coefficients of the polynomial.
First:

Solution (Continued)

Solution

We will relate these expressions to the coefficients of the polynomial. First:

$$\begin{aligned} r_1^2 + r_2^2 + r_3^2 &= (r_1 + r_2 + r_3)^2 - 2(r_1 r_2 + r_1 r_3 + r_2 r_3) \\ &= (-4)^2 - 2(-a) = 16 + 2a \end{aligned}$$

Solution (Continued)

Solution

We will relate these expressions to the coefficients of the polynomial. First:

$$\begin{aligned} r_1^2 + r_2^2 + r_3^2 &= (r_1 + r_2 + r_3)^2 - 2(r_1 r_2 + r_1 r_3 + r_2 r_3) \\ &= (-4)^2 - 2(-a) = 16 + 2a \end{aligned}$$

The second is a little more challenging:

$$\begin{aligned} & 1/r_1^2 + 1/r_2^2 + 1/r_3^2 \\ = \; & (r_1^2 r_2^2 + r_1^2 r_3^2 + r_2^2 + r_3^2)/(r_1^2 r_2^2 r_3^2) \\ = \; & ((r_1 r_2 + r_1 r_3 + r_2 r_3)^2 - 2(r_1^2 r_2 r_3 + r_2^2 r_1 r_3 + r_3^2 r_1 r_2))/(r_1 r_2 r_3)^2 \\ = \; & ((-a)^2 - 2(r_1 r_2 r_3)(r_1 + r_2 + r_3))/1^2 \\ = \; & a^2 - 8 \end{aligned}$$

Solution (Continued)

Solution

Now we conclude:

$$\begin{aligned}
&\left(r_1 + \frac{1}{r_1}\right)^2 + \left(r_2 + \frac{1}{r_2}\right)^2 + \left(r_3 + \frac{1}{r_3}\right)^2 \\
= \;& (r_1^2 + r_2^2 + r_3^2) + (1/r_1^2 + 1/r_2^2 + 1/r_3^2) + 6 \\
= \;& (16 + 2a) + (a^2 - 8) + 6 \\
= \;& a^2 + 2a + 14 \\
= \;& (a+1)^2 + 13
\end{aligned}$$

which clearly has minimal value 13 at $a = -1$.

Look for Symmetry

If you spend enough work cranking it out, **any** symmetric polynomial of $r_1, \ldots, r_n$ can be expressed in terms of the *elementary symmetric polynomials* $r_1 + r_2 + \ldots + r_n$, $r_1 r_2 + r_1 r_3 + \ldots + r_{n-1} r_n$, etc.

Look for Symmetry

If you spend enough work cranking it out, **any** symmetric polynomial of $r_1, \ldots, r_n$ can be expressed in terms of the *elementary symmetric polynomials* $r_1 + r_2 + \ldots + r_n$, $r_1 r_2 + r_1 r_3 + \ldots + r_{n-1} r_n$, etc.

In general, **looking for symmetry** is a very valuable tool when dealing with polynomials. For instance, a *reciprocal polynomial* is a polynomial $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ where $a_i = a_{n-i}$ for all $i = 0, \ldots, n$. If you have a reciprocal polynomial $f(x)$ of degree $2n$, it is always possible to substitute $z = x + \frac{1}{x}$ and write $f(x) = x^n g(z)$, where $g(z)$ is a polynomial of degree n:

Look for Symmetry

If you spend enough work cranking it out, **any** symmetric polynomial of $r_1, \ldots, r_n$ can be expressed in terms of the *elementary symmetric polynomials* $r_1 + r_2 + \ldots + r_n$, $r_1 r_2 + r_1 r_3 + \ldots + r_{n-1} r_n$, etc.

In general, **looking for symmetry** is a very valuable tool when dealing with polynomials. For instance, a *reciprocal polynomial* is a polynomial $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ where $a_i = a_{n-i}$ for all $i = 0, \ldots, n$. If you have a reciprocal polynomial $f(x)$ of degree $2n$, it is always possible to substitute $z = x + \frac{1}{x}$ and write $f(x) = x^n g(z)$, where $g(z)$ is a polynomial of degree n:

$$\begin{aligned} f(x) &= a_0 x^{2n} + a_1 x^{2n-1} + \ldots + a_1 x + a_0 \\ &= x^n (a_0 x^n + a_1 x^{n-1} + \ldots + a_1 x^{-(n-1)} + a_0 x^{-n}) \\ &= x^n (a_0 (x^n + x^{-n}) + a_1 (x^{n-1} + x^{-(n-1)}) + \ldots) \end{aligned}$$

and each term $(x^k + x^{-k})$ can be expressed as a function of $(x + \frac{1}{x})$

Lagrange Interpolation

Say that we have n points $(x_1, y_1), \ldots, (x_n, y_n)$ in the plane, and we want to find a polynomial $f(x)$ such that the line $y = f(x)$ passes through all these points. We will always be able to find such a polynomial of degree at most $n - 1$ — if we write it out, determining this polynomial becomes a simple matter of solving a system of n simultaneous linear equations.

Lagrange Interpolation

Say that we have n points $(x_1, y_1), \ldots, (x_n, y_n)$ in the plane, and we want to find a polynomial $f(x)$ such that the line $y = f(x)$ passes through all these points. We will always be able to find such a polynomial of degree at most $n - 1$ — if we write it out, determining this polynomial becomes a simple matter of solving a system of n simultaneous linear equations.

In fact, the polynomial of degree at most $n - 1$ that passes through these points is **unique**. After all, if there were two polynomials $P(x)$ and $Q(x)$ of degree at most $n - 1$ passing through these points, then their difference $P(x) - Q(x)$ would also have degree at most $n - 1$, but it would have at least n roots $(x_1, \ldots, x_n)$, which is impossible.

Lagrange Interpolation (Continued)

Luckily, it turns out that there is an explicit way to write the polynomial that passes through these points, without doing any work ourselves. This polynomial is:

$$L(x) = \sum_{j=1}^{n} y_j \ell_j(x)$$

where

$$\ell_j(x) = \prod_{i=1, i \neq j} \frac{x - x_i}{x_j - x_i}$$

This satisfies $L(x_j) = y_j$ for $j = 1, \ldots, n$, as desired.

Roots of Unity

The polynomial $x^n - 1$ has roots $1, \omega, \omega^2, \ldots, \omega^{n-1}$, where the nth root of unity ω is defined as $e^{2\pi i/n} = \cos(2\pi i/n) + i \sin(2\pi i/n)$. (These are n evenly spaced points on the unit circle in the complex plane.)

Roots of Unity

The polynomial $x^n - 1$ has roots $1, \omega, \omega^2, \ldots, \omega^{n-1}$, where the nth root of unity ω is defined as $e^{2\pi i/n} = \cos(2\pi i/n) + i \sin(2\pi i/n)$. (These are n evenly spaced points on the unit circle in the complex plane.)

These are useful in many situations involving polynomials. For instance:

Roots of Unity

The polynomial $x^n - 1$ has roots $1, \omega, \omega^2, \ldots, \omega^{n-1}$, where the nth root of unity ω is defined as $e^{2\pi i/n} = \cos(2\pi i/n) + i\sin(2\pi i/n)$. (These are n evenly spaced points on the unit circle in the complex plane.)

These are useful in many situations involving polynomials. For instance:

Problem

Let $n \geq 3$ be an integer. Let $f(x)$ and $g(x)$ be polynomials with real coefficients such that the points $(f(1), g(1)), (f(2), g(2)), \ldots, (f(n), g(n))$ in $\mathbb{R}^2$ are the vertices of a regular n-gon in counterclockwise order. Prove that at least one of $f(x)$ and $g(x)$ has degree greater than or equal to $n - 1$. (2008 Putnam A5)

Roots of Unity

The polynomial $x^n - 1$ has roots $1, \omega, \omega^2, \ldots, \omega^{n-1}$, where the nth root of unity ω is defined as $e^{2\pi i/n} = \cos(2\pi i/n) + i\sin(2\pi i/n)$. (These are n evenly spaced points on the unit circle in the complex plane.)

These are useful in many situations involving polynomials. For instance:

Problem

Let $n \geq 3$ be an integer. Let $f(x)$ and $g(x)$ be polynomials with real coefficients such that the points $(f(1), g(1)), (f(2), g(2)), \ldots, (f(n), g(n))$ in $\mathbb{R}^2$ are the vertices of a regular n-gon in counterclockwise order. Prove that at least one of $f(x)$ and $g(x)$ has degree greater than or equal to $n - 1$. (2008 Putnam A5)

Any guesses?

Solution

Here is the first solution given by Kiran Kedlaya and Lenny Ng.

Solution

Here is the first solution given by Kiran Kedlaya and Lenny Ng.

Let's form the complex polynomial $P(z) = f(z) + ig(z)$. It suffices to show that $P(z)$ must have degree at least $n-1$. By replacing $P(z)$ with $aP(z) + b$ for some suitable $a, b \in \mathbb{C}$, we can force the regular n-gon to have vertices $1, \omega, \omega^2, \ldots, \omega^{n-1}$ for $\omega = e^{2\pi i/n}$. It now suffices to show that there is no $P(z)$ of degree $n-2$ or lower such that $P(k) = \omega^k$ for $k = 0, 1, \ldots, n-1$.

Solution

Here is the first solution given by Kiran Kedlaya and Lenny Ng.

Let's form the complex polynomial $P(z) = f(z) + ig(z)$. It suffices to show that $P(z)$ must have degree at least $n-1$. By replacing $P(z)$ with $aP(z) + b$ for some suitable $a, b \in \mathbb{C}$, we can force the regular n-gon to have vertices $1, \omega, \omega^2, \ldots, \omega^{n-1}$ for $\omega = e^{2\pi i/n}$. It now suffices to show that there is no $P(z)$ of degree $n-2$ or lower such that $P(k) = \omega^k$ for $k = 0, 1, \ldots, n-1$.

Supposed to the contrary that there is such a $P(k)$, of degree $d \leq n-2$. Let $Q(z) = P(z+1) - \omega P(z)$. Then $Q(z)$ has degree at most $d \leq n-2$, but Q has roots at $0, 1, \ldots, n-2$, which is a contradiction.

Solution

Here is the first solution given by Kiran Kedlaya and Lenny Ng.

Let's form the complex polynomial $P(z) = f(z) + ig(z)$. It suffices to show that $P(z)$ must have degree at least $n-1$. By replacing $P(z)$ with $aP(z) + b$ for some suitable $a, b \in \mathbb{C}$, we can force the regular n-gon to have vertices $1, \omega, \omega^2, \ldots, \omega^{n-1}$ for $\omega = e^{2\pi i/n}$. It now suffices to show that there is no $P(z)$ of degree $n-2$ or lower such that $P(k) = \omega^k$ for $k = 0, 1, \ldots, n-1$.

Supposed to the contrary that there is such a $P(k)$, of degree $d \leq n-2$. Let $Q(z) = P(z+1) - \omega P(z)$. Then $Q(z)$ has degree at most $d \leq n-2$, but Q has roots at $0, 1, \ldots, n-2$, which is a contradiction.

Note: This problem can also be solved using Lagrange Interpolation—in fact, that's what many people did on the actual contest.

Irreducibility

Often we have a polynomial $P(x)$ with integer coefficients and want to know whether it can be factored into two or more polynomials with integer coefficients of lower degree. The *Eisenstein Criterion* gives us a way of determining cases where this is hopeless, and the polynomial is **irreducible**.

Irreducibility

Often we have a polynomial $P(x)$ with integer coefficients and want to know whether it can be factored into two or more polynomials with integer coefficients of lower degree. The *Eisenstein Criterion* gives us a way of determining cases where this is hopeless, and the polynomial is **irreducible**.

Eisenstein Criterion

Suppose that the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ has integer coefficients a_i and that there is a prime number p for which:

Irreducibility

Often we have a polynomial $P(x)$ with integer coefficients and want to know whether it can be factored into two or more polynomials with integer coefficients of lower degree. The *Eisenstein Criterion* gives us a way of determining cases where this is hopeless, and the polynomial is **irreducible**.

Eisenstein Criterion

Suppose that the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ has integer coefficients a_i and that there is a prime number p for which:

1. p is not a divisor of the leading coefficient a_n;

Irreducibility

Often we have a polynomial $P(x)$ with integer coefficients and want to know whether it can be factored into two or more polynomials with integer coefficients of lower degree. The *Eisenstein Criterion* gives us a way of determining cases where this is hopeless, and the polynomial is **irreducible**.

Eisenstein Criterion

Suppose that the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ has integer coefficients a_i and that there is a prime number p for which:

1. p is not a divisor of the leading coefficient a_n;
2. p is a divisor of every other coefficient $a_{n-1}, \ldots, a_0$;

Irreducibility

Often we have a polynomial $P(x)$ with integer coefficients and want to know whether it can be factored into two or more polynomials with integer coefficients of lower degree. The *Eisenstein Criterion* gives us a way of determining cases where this is hopeless, and the polynomial is **irreducible**.

Eisenstein Criterion

Suppose that the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ has integer coefficients a_i and that there is a prime number p for which:

1. p is not a divisor of the leading coefficient a_n;
2. p is a divisor of every other coefficient $a_{n-1}, \ldots, a_0$;
3. p^2 does not divide the constant coefficient a_0.

Irreducibility

Often we have a polynomial $P(x)$ with integer coefficients and want to know whether it can be factored into two or more polynomials with integer coefficients of lower degree. The *Eisenstein Criterion* gives us a way of determining cases where this is hopeless, and the polynomial is **irreducible**.

Eisenstein Criterion

Suppose that the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ has integer coefficients a_i and that there is a prime number p for which:

1. p is not a divisor of the leading coefficient a_n;
2. p is a divisor of every other coefficient $a_{n-1}, \ldots, a_0$;
3. p^2 does not divide the constant coefficient a_0.

Then the polynomial $P(x)$ is irreducible over the integers.

Irreducibility

Often we have a polynomial $P(x)$ with integer coefficients and want to know whether it can be factored into two or more polynomials with integer coefficients of lower degree. The *Eisenstein Criterion* gives us a way of determining cases where this is hopeless, and the polynomial is **irreducible**.

Eisenstein Criterion

Suppose that the polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ has integer coefficients a_i and that there is a prime number p for which:

1. p is not a divisor of the leading coefficient a_n;
2. p is a divisor of every other coefficient $a_{n-1}, \ldots, a_0$;
3. p^2 does not divide the constant coefficient a_0.

Then the polynomial $P(x)$ is irreducible over the integers.

For instance, $2x^4 + 21x^3 - 6x^2 + 9x - 3$ is irreducible over $\mathbb{Z}$ because 3 divides every coefficient but the leading one, and 9 does not divide the constant term.

Irreducibility: Example

From problem 183 in *Putnam and Beyond*:

Problem

Show that $P(x) = 1 + x + x^2 + \ldots + x^{p-1}$, *where* p *is a prime, is irreducible.*

Irreducibility: Example

From problem 183 in *Putnam and Beyond*:

Problem

Show that $P(x) = 1 + x + x^2 + \ldots + x^{p-1}$, *where* p *is a prime, is irreducible.*

Solution

Note that $P(x) = (x^p - 1)/(x - 1)$. *Moreover, if* $P(x)$ *is reducible, so is* $P(x + 1)$. *But*

$$P(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-1}$$

All coefficients of this polynomial are divisible by p *except the first. The last,* $\binom{p}{p-1} = p$, *is not divisible by* p^2, *and Eisenstein's criterion therefore implies that the polynomial is irreducible.*

Factorizations of Note

$$x^2 - y^2 = (x + y)(x - y)$$
$$x^3 - y^3 = (x - y)(x^2 + xy + y^2)$$
$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + y^{n-1})$$
$$(a - b)|(P(a) - P(b)) \qquad \text{(for all polynomials } P \text{ and integers } a, b)$$

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2)$$
$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \ldots + y^{n-1}) \quad \text{(for odd } n)$$

$$x^4 + 4y^4 = (x^2 + 2y^2)^2 - (2xy)^2 = (x^2 + 2xy + 2y^2)(x^2 - 2xy + 2y^2)$$
$$a^2 + b^2 + c^2 - ab - ac - bc = ((a - b)^2 + (a - c)^2 + (b - c)^2)/2$$
$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc)$$

Derivatives and Roots

Say we have

$$P(z) = a_n(z - z_1)(z - z_2)\cdots(z - z_n)$$

Then applying the product rule, we find:

$$\frac{P'(z)}{P(z)} = \frac{1}{z - z_1} + \ldots + \frac{1}{z - z_n}$$

If a root of $P(z)$ has multiplicity greater than 1, then it must be a root of $P'(z)$ as well.

Derivatives and Roots

Say we have

$$P(z) = a_n(z - z_1)(z - z_2)\cdots(z - z_n)$$

Then applying the product rule, we find:

$$\frac{P'(z)}{P(z)} = \frac{1}{z - z_1} + \ldots + \frac{1}{z - z_n}$$

If a root of $P(z)$ has multiplicity greater than 1, then it must be a root of $P'(z)$ as well.

This famous result helps characterize the roots of the derivative of a polynomial:

Theorem (Lucas)

The roots of $P'(z)$ lie within the convex hull of the roots of $P(z)$ in the complex plane. (The convex hull of a set of points $z_1, \ldots, z_n$ is the set of all points $t_1z_1 + \ldots + t_nz_n$, where $t_1 + \ldots + t_n = 1$.)