Lecture 16 — Basic Polynomials and Irreducibility

Shri Ganeshram

4/2/2011

In mathematics, especially competitive mathematics, polynomials are always being explored.

We shall begin this lecture with an introduction to polynomials, taken from the upcoming free and open source OMC Number Theory book.

Note that about half of this lecture was taken from the book and the other half will probably be added to the book.

This lecture goes from basic to intermediate and is good for a student of any level. I plan to write and release a more rigorous, advanced lecture that builds from this one and extends to domains that aren't as standard as seen here.

1 Introductory Stuff

Definition 1.1: An integer polynomial, the only type we will deal with unless noted otherwise, is a function, $P(x)$, of the form:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$$

where $a_n, a_{n-1}, \ldots, a_0$ are integers.

Definition 1.2: We can evaluate a polynomial for any number, y, by substituting y for x.

$$P(y) = a_n y^n + a_{n-1}y^{n-1} + ... + a_1 y + a_0$$

For example, given that $P(x) = x^2 + 1$, calculate $P(2)$.

$$P(2) = 2^2 + 1 = 5.$$

Definition 1.3: A **zero (or root)** of a polynomial is a number t such that P(t)=0

For example, given $P(x) = x^2 - 1$, find the zeros (roots) of $P(x)$.

If t is a root of $P(x)$, we have the following relationship:

$$P(t) = t^2 - 1 = 0.$$

So, we may simply solve the equation $t^2 - 1 = 0$.

$$t^2 - 1 = 0 \implies t^2 = 1 \implies t = \pm 1.$$

Note that $\implies$ symbolizes the word "implies"

Definition 1.4: Factors of an integer polynomial, $P(x)$, are integer polynomials, $Q(x)$, such that $P(x)$ can be expressed in terms of $Q(x)$ and another integer polynomial, $R(x)$, as $P(x) = Q(x) \cdot R(x)$.

For example, let $P(x) = x^3 + x^2 - x - 1$.
Since $x^3 + x^2 - x - 1 = (x^2 + 2x + 1)(x - 1)$ both $x^2 + 2x + 1$ and $x - 1$ are factors of $x^3 + x^2 - x - 1$.

Definition 1.5: An **irreducible integer polynomial** P is one whose only integer polynomial factors are ± 1 and $\pm P$.

For example, let $P(x) = x^2 + x + 1$.
Since the only integer polynomial factors of $x^2 + x + 1$ are $\pm(x^2 + x + 1)$ and ± 1, it is irreducible.

Definition 1.6: The **factorization** of an integer polynomial, $P(x)$, is the expression of $P(x)$ as a product of irreducible integer polynomials.

For example, let $P(x) = x^3 + x^2 - x - 1$.
The factorization of $P(x)$ is:

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

Proposition 1.7: The zeros of the irreducible integer polynomials that an integer polynomial factors into are the zeros of that polynomial.

Earlier we found that the zeros of $x^2 - 1$ are ± 1.

The factorization of $x^2 - 1$ is $(x + 1)(x - 1)$. The zero of $x + 1$ is -1 and the zero of $x - 1$ is $+1$, giving us ± 1.

Theorem 1.8 (The Rational Root Theorem)**:** Given the polynomial $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, all rational roots are in the form $\pm\frac{p}{q}$, where p is an integer factor of a_0 and q is an integer factor of a_n.

This theorem will help us find the zeros of polynomials!

Let's try an example! Find the zeros of $P(x) = 3x^2 + 4x + 1$.
Applying the Rational Root Theorem, we have that the possible zeros of this polynomial are: $\pm\frac{1}{1,3}$. This means our possible roots are $\frac{1}{1}$, $-\frac{1}{1}$, $\frac{1}{3}$, and $-\frac{1}{3}$. We substitute these values for x in the polynomials to see which ones yield values of zero. We have that -1 and $-\frac{1}{3}$ are the roots since $P(-1) = 0$ and $P(-\frac{1}{3}) = 0$.

Proposition 1.9 (The Relationship Between Roots and Factors in an Integer Polynomial)**:** Given a root $\frac{m}{n}$, $\gcd(m, n) = 1$ (the fraction is completely reduced), of a polynomial, $P(x)$, there is an irreducible integer polynomial factor of $P(x)$ in the form $(nx - m)$.

In the last example, we found that the zeros of $P(x) = 3x^2 + 4x + 1$ are -1 and $-\frac{1}{3}$. We treat -1 as $-\frac{1}{1}$ and apply the relationship above:

$$\begin{aligned} -\frac{1}{1} \text{ is a root} &\implies (x+1) \text{ is an irreducible integer factor of } P(x) \\ -\frac{1}{3} \text{ is a root} &\implies (3x+1) \text{ is an irreducible integer factor of } P(x) \end{aligned}$$

Multiplying the two factors, we have $(3x + 1) \cdot (x + 1) = 3x^2 + 4x + 1$. We know that the product of all of the irreducible integer polynomial factors of a polynomial yields the polynomial. We also intuitively see that $P(x)$ has at most two irreducible integer polynomial factors as the highest powered term is x^2 and the product of more than two irreducible integer polynomial factors will yield a highest powered term of at least x^3.

We know that $P(x) = 3x^2 + 4x + 1$ and that $P(x) = A(3x + 1) \cdot (x + 1)$ for some nonzero constant A; a quick check would show that the second statement is true $A = 1$, so the proposition checked out positive!

Definition 1.10: Given the polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, we define the **degree** of $P(x)$ to be n, the highest power of any x term. If a polynomial is of 1st degree (highest powered term is $a_1 x^1$), it is called **monic**.

(The following theorem and examples are from Holden Lee's January 29th, 2011 lecture on OMC concerning Polynomials.)

Theorem 1.11 (Vieta's Formula)**:** Let $r_1, \ldots, r_n$ be the roots of $P(x) = \sum_{i=0}^{n} a_i x^i$, and let

$$s_j = \sum_{1 \le i_1 < \ldots < i_j \le n} r_{i_1} \cdots r_{i_j}.$$

Then $s_j = (-1)^j \frac{a_{n-j}}{a_n}$.

Proof. We can factor the polynomial as

$$P(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_n).$$

Dividing by a_n gives

$$\left(x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \cdots + \frac{a_1}{a_n} x + \frac{a_0}{a_n} \right) = (x - r_1)(x - r_2) \cdots (x - r_n).$$

In the expansion of the right-hand side, the terms containing x^{n-j} are of the form $(-r_{i_1}) \cdots (-r_{i_j}) x^{n-j}$—they contain a product of j roots. Summing them up, the coefficient of x^{n-j} is $(-1)^j s_j$. Setting this equal to the coefficient on the left-hand side, $\frac{a_{n-j}}{a_n}$, gives the desired result. □

Example 1.12: Let r_1, r_2 be the roots of the quadratic $ax^2 + bx + c = 0$. Find

1. $r_1 + r_2$

2. $r_1^2 + r_2^2$

3. $r_1^3 + r_2^3$

Solution.

1. From Vieta's formula, $r_1 + r_2 = -\frac{b}{a}$.

2. Also from Vieta's formula, $r_1 r_2 = \frac{c}{a}$. We need to combine these two expressions in some way to form $r_1^2 + r_2^2$. The following identity does the trick.

$$r_1^2 + r_2^2 = (r_1 + r_2)^2 - 2r_1 r_2.$$

Thus $r_1^2 + r_2^2 = \left(-\frac{b}{a}\right)^2 - 2\left(\frac{c}{a}\right) = \frac{b^2-2ac}{a^2}$.

3. Noting the cube, we first cube $r_1 + r_2$ to get $r_1^3 + 3r_1^2 r_2 + 3r_1 r_2^2 + r_2^3$. We need to get rid of $3r_1^2 r_2 + 3r_1 r_2^2$. But we are in luck, since this equals $3r_1 r_2(r_1 + r_2)$. Hence

$$r_1^3 + r_2^3 = (r_1 + r_2)^3 - 3r_1 r_2(r_1 + r_2).$$

(Another way to see this is to use the factorization $r_1^3 + r_2^3 = (r_1 + r_2)(r_1^2 - r_1 r_2 + r_2^2) = (r_1 + r_2)((r_1 + r_2)^2 - 3r_1 r_2)$.) We get $r_1^3 + r_2^3 = \left(-\frac{b}{a}\right)^3 - 3\left(\frac{c}{a}\right)\left(-\frac{b}{a}\right) = \frac{-b^3+3abc}{a^3}$.

1.1 Problems

1. (2010 AIME 1) Let $P(x)$ be a quadratic polynomial with real coefficients satisfying $x^2 - 2x + 2 \leq P(X) \leq 2x^2 - 4x + 3$ for all real numbers x, and suppose $P(11) = 181$. Find $P(16)$.

2. (From Algebra By Izrail Moiseevich Gelfand, Alexander Shen) Prove that the equation $x^2 + px + q = 0$ has two solutions having different signs if and only if $q \leq 0$.

3. (USAMO 1984) The product of two of the four zeros of the quartic equation $x^4 - 18x^3 + kx^2 + 200x - 1984 = 0$ is -32. Find k.

4. (Shri Ganeshram) Find all solutions to the following system:

$$\begin{aligned} x + y &= z + 4 \\ (x + y)z &= xy - 77 \\ xyz + 360 &= 0 \end{aligned}$$

5. Find all integer polynomials $f(x)$ such that:
$xf(x-1) = (x - 2010)f(x)$.

6. (IMO 1988, Problem 6). Let a and b be positive integers so that $ab + 1$ divides $a^2 + b^2$. Prove that $\frac{a^2+b^2}{ab+1}$ is a perfect square. (Hint: Use Vieta's formula)

2 Some Theorems of Irreducibility

Let us begin with one incredibly powerful theorem of irreducibility discovered independently by both Schonemann and Eisenstein.

Theorem 2.1 (Eisenstein's/Schönemann's Criterion)**:** Suppose we have the following polynomial with integer coefficients:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0.$$

If there exists a prime number p such that:

1. p divides each a_i for $i \neq n$,

2. p does not divide a_n, and

3. p^2 does not divide a_0,

then $P(x)$ is irreducible over the rationals.

For example, prove that $x^7 + 5x^4 + 35$ is irreducible.

We take p to be 5. Notice that 5 does not divide the coefficient x^7 and that 5 divides the coefficients of $x^6, \dots, x^0$, which are $(0, 0, 5, 0, 0, 0, 35)$. Finally, we check whether p^2, 25, divides a_0, 35, or not. We see that 25 does not divide 35 and that the function satisifies Eisenstein's Criterion for $p = 5$, so we are done. The polynomial is irreducible!

This next irreducibility criterion is just as interesting!

Theorem 2.2 (Cohn's Irreducibility Criterion)**:** Given a prime, p, whose base 10 representation is

$$a_n 10^n + a_{n-1}10^{n-1} + \ldots + a_1 10^1 + a_0 10^0$$

where $0 \leq a_i \leq 9$, the polynomial

$$P(x) = a_n x^n + \cdots + a_1 x^1 + a_0$$

is irreducible.

Remark 2.3: The theorem also holds for any base besides 10.

For example, prove that $x^3 + 7x^2 + 3x + 3$ is irreducible.

We notice that 1733 is prime. $1733 = 1 \cdot 10^3 + 7 \cdot 10^2 + 3 \cdot 10^1 + 3 \cdot 10^0$. We are done.

One last result that might come in handy is the following:

Theorem 2.4: For any $t \in R$, $f(x) = (x - t)g(x) + f(t)$.

2.1 Problems

1. (Shri Ganeshram) Find the minimum a such that $P(x) = x^3 + 2x^2 + a$ has real roots.

2. (Shri Ganeshram) Suppose $\frac{d}{dx}P(x) = (6x+5)$. If $P(x)$ is a reducible, integer polynomial, find with proof all possible polynomials $P(x)$.

3. (Classical) Show that $f(x+1)$ is irreducible, given that $f(x) = x^{p-1} + ... + x + 1$, p is prime.

   (Hint: Eisenstein)

4. (Easy) Show that a quadratic polynomial with odd coefficients is irreducible in Z.

5. Let $f(x)$ be an integer polynomial. Show that if $f(0)$ and $f(1)$ are both odd, then $f(x)$ is irreducible in Z.

3 A Sneak Peek of What's Coming Up in the Next Lecture

Before we see more theorems, we shall define the division and the modulus of polynomials. (Recall that the modulus is the remainder when dividing.)

Dividing polynomials is very similar to dividing integers. Let us learn through an example.

Calculate $\frac{3x^3+4x^2-1}{2x+1}$.
Solution. When dividing polynomials, we look at the highest powered term in the divisor. We have $2x+1$. We notice that $\frac{3}{2}x^2 \cdot 2x = 3x^3$. So, we write down $\frac{3}{2}x^2$, and multiply $\frac{3}{2}x^2$ and $2x+1$ (the divisor) and subtract from $3x^3+4x^2-1$ (the quotient).

$$(3x^3+4x^2-1) - \frac{3}{2}x^2 \cdot (2x+1) = \frac{1}{2}x^2 - 1$$
$$\frac{3x^3+4x^2-1}{2x+1} = \frac{5}{2}x^2 + \frac{\frac{5}{2}x^2-1}{2x+1}.$$

So now we must divide $\frac{\frac{5}{2}x^2-1}{2x+1}$. We take $2x$ again and notice that the product of $2x$ and $\frac{5}{4}x$ gives us $\frac{5}{2}x^2$, the highest powered term in the dividend. So, we take the product of $2x+1$ and $\frac{5}{4}x$ subtract it from $\frac{5}{2}x^2-1$.

$$\left(\frac{5}{2}x^2 - 1\right) - \frac{5}{4}x \cdot (2x+1) = -\frac{5}{4}x - 1$$
$$\frac{3x^3+4x^2-1}{2x+1} = \frac{3}{2}x^2 + \frac{5}{4}x + \frac{-\frac{5}{4}x-1}{2x+1}.$$

Finally, we have the division $\frac{-\frac{5}{4}x-1}{2x+1}$. We see that $-\frac{5}{8}$ multiplied with $2x$ yields $-\frac{5}{4}x$ and do as we did before.

$$\left(-\frac{5}{4}x - 1\right) - \left(-\frac{5}{8}\right) \cdot (2x+1) = -\frac{3}{8}$$
$$\frac{3x^3+4x^2-1}{2x+1} = \frac{3}{2}x^2 + \frac{5}{4}x - \frac{5}{8} - \frac{\frac{3}{8}}{2x+1}.$$

We are done as the highest powered term of $2x + 1$ is greater in power than the highest powered term of $-\frac{3}{8}$.

Finding the modulus. In the above problem, we were dividing by $2x+1$ and our remainder was $-\frac{3}{8}$, which means $3x^3+4x^2-1 \bmod 2x+1 = -\frac{3}{8}$. Since we are modding by $2x+1$, anything of the form $(-\frac{3}{8}+P(x)(2x+1)) \bmod 2x+1 = (3x^3+4x^2-1) \bmod 2x+1 = -\frac{3}{8}$, where $P(x)$ is an integer polynomial.

Polynomials mod p. An integer polynomial, $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, is equivalent to

$$(a_n \bmod p)x^n + (a_{n-1} \bmod p)x^{n-1} + \cdots + (a_0 \bmod p) \in \mathbb{Z}/p\mathbb{Z}[x]$$

(the integers mod p where $p \in \mathbb{Z}$ is prime).

For example, given $P(x) \in \mathbb{Z}$, $P(x) = 35x^n + 7x^{n-1} + 6x + 1$, find $P(x) \in \mathbb{Z}/7\mathbb{Z}$ such that $P(x)$ is in a simpler form.

Solution. Consider the coefficients modulo 7. Since $(35, 7, 6, 1) \bmod 7 = (0, 0, 6, 1) = (0, 0, -1, 1)$,

$$P(x) \bmod 7 = 0x^n + 0x^{n-1} + 6x + 1 = -x + 1$$

Theorem 3.1: Given $P(x) \in \mathbb{Z}[x]$, if $P(x)$ is irreducible (non-factorable) modulo p for some prime $p \in \mathbb{Z}$, then $P(x)$ is irreducible in $\mathbb{Z}$.

The above theorem is advanced and isn't of much use to us now. I just included this early to show off the power of considering $\mathbb{Z}/p\mathbb{Z}$. This theorem will be explained in more depth in a later, follow up lecture.

Theorem 3.2: Given $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $P(x)$ is irreducible if $|a_0| > |a_1| + \cdots + |a_n|$ when $|a_0|$ is prime.

This theorem shows up in many problems and can kill those problems. More important the theorem is the proof, which will be included in a later, more advanced lecture. (Try proving it yourself.) As without the proof, this claim will not be useful in contest mathematics, and the ideas behind the proof can be used in more general situations.

Theorem 3.3: (Perron's Criterion) Given $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, $P(x)$ is irreducible if $|a_{n-1}| > |a_0| + |a_1| + \cdots + |a_{n-2}| + 1$ and $a_0 \neq 0$.

This theorem is also highly useful and can kill many high level problems. Though the proof is super important, so we shall discuss this in more detail in a further lecture.

3.1 problems(-s)

(MOP 2007) Show that for any f with integer coefficients that is nonconstant there are infinitely many integers n such that $f + n$ is irreducible in Z. (See how easily this hard USA MOP problem can be killed with the above techniques? Get pumped for the second part of this lecture!)

4 Closing Remarks

There will be a follow up lecture to this one in n weeks, where $\infty \gg n > 0$. (It is highly dependent on how quickly I become more proficient at working with irreducibility and abstract algebra, which will be a focus for the next segment (into AMSP 2011) of my life)

I hope you enjoyed the lecture; if you spot any errors, email me: shrig94@gmail.com. I would like to fix this up as the majority of it will become part of the OMC Number Theory Book! (and also because I dislike lectures with lots of mistakes) The nature of this lecture, given my experience, can lead to many foul mistakes, so please report them so that I can fix them. :)

Thanks,
Shri Ganeshram