Polynomials

Tyler Zhu

July 4, 2017

This handout details some interesting facts and useful techniques that involve polynomials, with instructional exercises.

Table of Contents

1 Polynomials

1.1 The Division Algorithm for Polynomials

We assume prior knowledge of what a polynomial is. Typically we will refer to polynomials by their name and the indeterminates they are defined on, such as $f(x, y, z)$ or $\sin x$.

Definition 1. A polynomial $g(x)$ is said to *divide* a polynomial $f(x)$ if there is some polynomial $h(x)$ such that $f(x) = g(x)h(x)$. We denote this as $g(x) \mid f(x)$.

Theorem 2 (Division Algorithm for Polynomials)**.** *Let $f(x)$ and $g(x)$ be polynomials of degree m and n respectively so that $m \geq n$. Then, there exist polynomials $q(x)$ and $r(x)$ such that*

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

where $r(x)$ is either zero or $0 \leq \deg r(x) < n$.

Remark. This theorem mimics the divison algorithm for integers; if we have integers a, b with $a \geq b$, then we can always find integers q and r (quotient and remainder) such that $a = b \cdot q + r$ where $0 \leq r < b$. It turns out that this concept of a division algorithm can hold for entities besides polynomials and integers as long as we have some notion of a "metric", like the degree; such structures are called *Euclidean Domains*.

One common application of the division algorithm will be to prove that $g(x)$ divides $f(x)$ by showing that $r(x)$ is zero if $f(x) = g(x)q(x) + r(x)$. This idea is demonstrated in the following two corollaries.

Corollary 3. *For a polynomial $f(x)$ and a number a, the remainder when $f(x)$ is divided by $x - a$ is $f(a)$.*

Corollary 4 (Factor Theorem)**.** *For a polynomial $f(x)$ and a number a, $x - a$ divides $f(x)$ if and only if a is a root of $f(x)$.*

1.2 Exercises

Exercise 1.1: Prove Corollary 3 and Corollary 4 using the Division Algorithm.

Exercise 1.2: $H(x)$ is a polynomial of degree 4 or greater where $H(1) = 2, H(2) = 3$, and $H(3) = 5$. Find the remainder when $H(x)$ is divided by $(x-1)(x-2)(x-3)$.

2 Root Hunting

2.1 The Fundamental Theorem of Algebra

Root hunting is when we determine a polynomial not by its coefficients, but by its roots and leading terms which uniquely determine every polynomial. This is formally stated as the **Fundamental Theorem of Algebra**.

Theorem 5 (Fundamental Theorem of Algebra)**.** *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with positive degree n and real coefficients. Then $f(x)$ has exactly n complex roots $z_1, z_2, \cdots, z_n$ so that*

$$f(x) = a_n(x - z_1)(x - z_2)\cdots(x - z_n).$$

Remark. Surprisingly, there is no simple proof of this "Fundamental" Theorem. The simplest proofs all require either fundamental groups (algebraic topology), Louiville's Theorem (complex analysis), Galois Theory (group/ring theory), or multivariable calculus. Further investigation suggests the theorem is neither fundamental, nor a theorem of (modern) algebra.

Example 2.1: Let $f(x) = 2x^2 + 10x + 12$. We can factor $f(x)$ as $f(x) = 2(x^2 + 5x + 6) = 2(x+2)(x+3)$, so its roots are -2 and -3. Alternatively, if we began by knowing that -2 and -3 were its only roots, or that $f(-2) = f(-3) = 0$, we would know that

$$f(x) = a(x - (-2))(x - (-3)) = a(x + 2)(x + 3).$$

However, we don't know what $f(x)$ is *exactly*! We need one value in order to uniquely determine $f(x)$. For example, if we also knew that $f(0) = 12$, then we can find a by plugging in 0.

$$f(0) = a(0 + 2)(0 + 3) = 12 \implies 6a = 12 \implies a = 2.$$

This turns out to be an important fact for us when hunting roots:
Fact: We need at least $n+1$ values in order to uniquely determine a polynomial of degree n.

Example 2.2: Let $P(x)$ be a cubic polynomial such that $P(1) = 2, P(2) = 2, P(3) = 2$, and $P(5) = 0$. Find $P(0)$.

Solution. We could write $P(x) = ax^3 + bx^2 + cx + d$, plug in our values, and solve a system of four equations, but that seems painful! Let's look for a better way.

One technique that we introduce here is to *translate* the polynomial. Here, we shift $P(x)$ down by 2, so that we get a new polynomial $Q(x) = P(x) - 2$ which still has degree 3. Why do this? Now $Q(1) = Q(2) = Q(3) = 0$; we've found the zeroes of Q! Since we know $Q(x)$ at four values and since $Q(x)$ is degree 3, the Fundamental Theorem tells us that

$$Q(x) = a(x-b)(x-c)(x-d) = a(x-1)(x-2)(x-3).$$

Using the fact that $Q(5) = P(5) - 2 = -2$ gives us

$$Q(5) = a(5-1)(5-2)(5-3) = -2 \implies 24a = -2 \implies a = -\frac{1}{12}.$$

Hence, we can find $Q(x)$ by plugging a into our form from above. All that is left to do now is to undo our translation so that we get $P(x)$, but fortunately this is easy to do. Thus, we see that

$$P(x) = Q(x) + 2 = -\frac{1}{12}(x-1)(x-2)(x-3) + 2 \implies P(0) = -\frac{1}{12}(0-1)(0-2)(0-3) + 2 = \boxed{\frac{5}{2}}.$$

□

2.2 Algebraic Nonsense

We begin by introducing some standard problems that seem rather difficult at first glance, but are quite straightforward using the ideas we introduced before.

Example 2.3: Suppose that $P(x)$ is a cubic polynomial such that $P(k) = \frac{k^2}{k+1}$ for $k = 1, 2, 3, 4$. Find $P(5)$.

Solution. One obvious but computationally heavy solution is to simply calculate what $P(k)$ is for $k = 1, 2, 3, 4$ and solve a system of linear equations, but we aim to find a better way.

Instead, we consider the polynomial

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

We are purposely setting up $Q(x)$ so that $Q(k) = 0$ for $k = 1, 2, 3, 4$. Also, since $P(x)$ is degree 3, $Q(x)$ is degree 4. Since we know all four roots of $Q(x)$, we have that

$$Q(x) = a(x-1)(x-2)(x-3)(x-4) = (x+1)P(x) - x^2.$$

However, we still haven't determined $Q(x)$ uniquely yet since only have four values. To make matters worse, we don't know any other values of $P(x)$ either! To deal with this, we'll pick a convenient value of x that eliminates $P(x)$ in the above equation [1]: -1 makes $x+1$ zero, so plugging this in gives

$$Q(-1) = a(-1-1)(-1-2)(-1-3)(-1-4) = a \cdot 5! = -(-1)^2 \implies a = -\frac{1}{5!}.$$

[1] This same tactic is employed in partial fraction decomposition

Now we can find $P(5)$, since

$$Q(5) = -\frac{1}{5!}(5-1)(5-2)(5-3)(5-4) = (5+1)P(5) - 5^2 \implies -\frac{1}{5} = 6P(5) - 25 \implies \boxed{P(5) = \frac{62}{15}}.$$

□

2.3 Roots of Unity

There is an important application of this concept that involved the roots of unity, which I will briefly introduce below.

Definition 6 (Roots of Unity)**.** If $\omega^n = 1$ where ω is a complex number, then ω is called an n^{th} *root of unity.*

Example 2.4: For $n = 2$, the second roots of unity are $1, -1$ since $\omega^2 = 1 \implies \omega = \pm 1$. For $n = 4$, the fourth roots of unity are $1, -1, i, -i$. In fact, if we were to plot each of the n^{th} roots of unity on the complex plane, they would look like this:

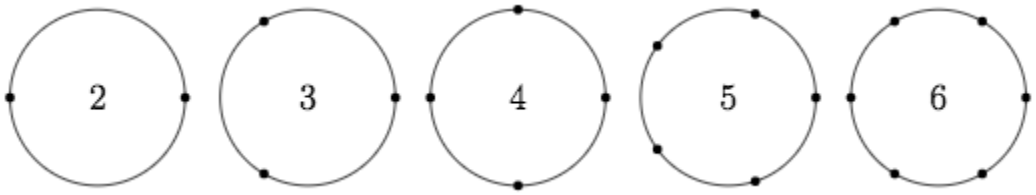

Figure 1: The Roots of Unity form the vertices of equilateral polygons. Source: EC

Now for our prize...

Example 2.5: If $\omega^{2013} = 1$ and $\omega \neq 1$, find $(2-\omega)(2-\omega^2)\dots(2-\omega^{2012})$. [2]

Solution. Let ω be as given, and consider the polynomial $z^{2013} - 1$. We know that 1 is a root of this polynomial since $1^{2013} - 1 = 0$. Also, ω is a root of this polynomial since $\omega^{2013} - 1 = 0$. Continuing in this fashion, ω^2 is also a root since $(\omega^2)^{2013} - 1 = (\omega^{2013})^2 - 1 = 1^2 - 1 = 0$, and so on. Hence, we know that $1, \omega, \omega^2, \dots, \omega^{2012}, \omega^{2013} = 1, \dots$ are all roots of $z^{2013} - 1$. The only distinct roots however are $1, \omega, \omega^2, \dots, \omega^{2012}$, so we can factor it as

$$z^{2013} - 1 = (z-1)(z-\omega)(z-\omega^2)\dots(z-\omega^{2012}).$$

Plugging in $z = 2$ tells us that $(2-\omega)(2-\omega^2)\cdots(2-\omega^{2012}) = \boxed{2^{2013} - 1}$. □

In general, we have proved the following lemma:

Lemma 7. *If $\omega^n = 1$, then we have that $z^n - 1 = (z-1)(z-\omega)(z-\omega^2)\cdots(z-\omega^{n-1})$.*

The heart of this idea is that the two degree n polynomials on the left and the right vanish on n distinct values and have the same leading coefficient. Therefore, they must be the same polynomial.

[2] Technically ω needs to be a primitive root of unity but alas...

2.4 Wilson's Theorem

Yet another application of the above technique is used to prove Wilson's Theorem. First we will need to recall a classic number theoretic fact.

Theorem 8 (Fermat's Little Theorem)**.** *For any integer a and prime p for which* $\gcd(a,p)=1$, $a^{p-1}\equiv 1 \pmod{p}$.

Proof. If we multiply the set of all non-zero numbers mod p by a, we get the set

$$\{1,2,\ldots,p-1\}\mapsto\{1\cdot a, 2\cdot a,\ldots,(p-1)\cdot a\}.$$

I claim that the sets are equal. This means that upon simplifying, the second set has the same numbers as the first set. This happens if no two numbers are equal to each other. We can check that this never happens because if $m\cdot a\equiv n\cdot a \pmod{p}$ where $1\le m<n<p$, then

$$m\cdot a\equiv n\cdot a \iff m\equiv n \pmod{p}$$

where dividing by zero is a non-issue. But this is a contradiction since $1\le m<n<p$. Thus, the product of the two sets must be equal. This gives

$$p!\equiv a^{p-1}\cdot p! \iff 1\equiv a^{p-1} \pmod{p},$$

proving the theorem. □

We can, in fact, prove Wilson's Theorem using the above techniques.

Theorem 9 (Wilson's Theorem)**.** *If p is a prime, then* $(p-1)!\equiv -1 \pmod{p}$.

Proof. Consider the polynomials $g(x)=(x-1)(x-2)\cdots(x-(p-1))$ and $h(x)=x^{p-1}-1$. Show that $g(x)\equiv h(x) \pmod{p}$ by root hunting (exercise). Comparing constant terms gives us that $(p-1)!\equiv -1 \pmod{p}$ which is what we want. □

2.5 Exercises

Exercise 2.6: Prove that $g(x)\equiv h(x) \pmod{p}$ as defined in the proof of Wilson's Theorem (Theorem 9) by root hunting.

Exercise 2.7: A third degree polynomial $f(x)$ satisfies the following: $f(1)=3, f(2)=5, f(3)=7, f(4)=15$. What is the value of $f(5)$?

Exercise 2.8 (USAMO 1975)**:** If $P(x)$ denotes a polynomial of degree n such that $P(k)=\frac{k}{k+1}$ for $k=0,1,2,\cdots,n$, determine $P(n+1)$ in terms of n.

Exercise 2.9: Suppose that $P(x)$ is a polynomial of degree 6 and $P(k)=\frac{k^2+10k-1}{k^2+k}$ for $k=1,2,3,\cdots,7$. Find $P(8)$.

Exercise 2.10 (SMT 2011)**:** Let $P(x)$ be a polynomial of degree 2011 such that $P(2^n)=n$ for $n=0,1,2,\ldots,2011$. Find the coefficient of x in $P(x)$.

3 Lagrange Interpolation [3]

We revisit the problem of determining a polynomial $P(x)$ of degree *at most* n when we are given $n+1$ points,[4] but this time we attack it in a general, systematic matter that leads to Lagrange's beautiful interpolation formula.

Example 3.1: Let $P(x)$ be a cubic polynomial where $P(0) = 5$, $P(1) = 2$, $P(3) = 0$, and $P(4) = 6$. Find $P(2)$.

Solution. Instead of solving $ax^3 + bx^2 + cx + d = 0$ for a, b, c, d, we do something smarter.

Let's tackle the easier question of solving for a polynomial $p_1(x)$ such that $p_1(0) = 1$, $p_1(1) = 0, p_1(3) = 0$, and $p_1(4) = 0$. By the Factor Theorem, we know that $(x-1)(x-3)(x-4)$ divides $p_1(x)$. We simple need to multiply this by some constant c so that $p_1(0) = 1$. Hence,

$$p_1(x) = c(x-1)(x-3)(x-4) \implies 1 = c(0-1)(0-3)(0-4) \implies c = \frac{1}{(0-1)(0-3)(0-4)},$$

and so

$$p_1(x) = \frac{(x-1)(x-3)(x-4)}{(0-1)(0-3)(0-4)}.$$

Similarly, to find a polynomial $p_2(x)$ such that $p_2(0) = 0, p_2(1) = 1, p_2(3) = 0, p_2(4) = 0$, we can take

$$p_2(x) = \frac{(x-0)(x-3)(x-4)}{(1-0)(1-3)(1-4)}.$$

In the same way, let

$$p_3(x) = \frac{(x-0)(x-1)(x-4)}{(3-0)(3-1)(3-4)},$$
$$p_4(x) = \frac{(x-0)(x-1)(x-3)}{(4-0)(4-1)(4-3)}.$$

Using a combination of these four polynomials, we can match any values at $x = 0, 1, 3$, and 4. For example, if we set

$$P(x) = y_1 p_1(x) + y_2 p_2(x) + y_3 p_3(x) + y_4 p_4(x),$$

then

$$\begin{aligned} P(0) &= y_1 p_1(0) + y_2 p_2(0) + y_3 p_3(0) + y_4 p_4(0) \\ &= y_1 \cdot 1 + y_2 \cdot 0 + y_3 \cdot 0 + y_4 \cdot 0 \\ &= y_1 \end{aligned}$$

Similarly, $P(1) = y_2$, $P(3) = y_3$, and $P(4) = y_4$. All we have to do now is set our y_i to the given values to solve the problem. This gives us

$$\begin{aligned} P(x) = 5 \cdot \frac{(x-1)(x-3)(x-4)}{(0-1)(0-3)(0-4)} + 2 \cdot \frac{(x-0)(x-3)(x-4)}{(1-0)(1-3)(1-4)} \\ 0 \cdot \frac{(x-0)(x-1)(x-4)}{(3-0)(3-1)(3-4)} + 6 \cdot \frac{(x-0)(x-1)(x-3)}{(4-0)(4-1)(4-3)} \\ = \frac{5x^3 - 12x^2 - 29x + 60}{12} \end{aligned}$$

□

[3] This section is adapted from the WOOT 2012-13 Polynomials C Handout.

[4] Why at most?

We can now write down the general formula.

Theorem 10 (Lagrange Interpolation Formula)**.** *Let* $(x_1, y_1), (x_2, y_2), \ldots, (x_{n+1}, y_{n+1})$ *be* $n+1$ *distinct points. Then the polynomial defined by*

$$P(x) = \sum_{i=1}^{n+1} y_i \frac{(x-x_1)(x-x_2)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)(x-x_{n+1})}{(x_i-x_1)(x_i-x_2)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)(x_i-x_{n+1})}$$

satisfies $P(x_i) = y_i$ *for* $i = 1, \ldots, n+1$.

Note that this interpolation is not entirely unique! If we had $P(1) = 1, P(3) = 9, P(6) = 36, P(7) = 49$, then obviously $P(x) = x^2$ works. But so does

$$P(x) = x^2 + (x-1)(x-3)(x-6)(x-7)(\pi x^4 + ex^3 - \sqrt{5}x + 1).$$

In fact, any polynomial of the form

$$P(x) = x^2 + (x-1)(x-3)(x-6)(x-7)q(x)$$

works, where $q(x)$ is a polynomial. Our intuition tells us that $P(x) = x^2$ should be the "best" solution to the interpolation; how do we make this precise?

Note that if $q(x)$ is a nonzero polynomial, then $P(x)$ becomes a polynomial of degree at least 4. Hence, $P(x) = x^2$ is the unique solution that has degree at most 3 (remember, $n+1$ points means degree n). So the Interpolation Formula does give us a unique solution; it is simply up to degree n.

3.1 Exercises

Exercise 3.2: Find the fourth degree polynomial $f(x)$ such that $f(-2) = 29$, $f(0) = 3$, $f(1) = 17$, $f(3) = -21$.

Exercise 3.3 (AIME 1984)**:** Determine $w^2 + x^2 + y^2 + z^2$ if

$$\begin{aligned}
\frac{x^2}{2^2-1} + \frac{y^2}{2^2-3^2} + \frac{z^2}{2^2-5^2} + \frac{w^2}{2^2-7^2} &= 1,\\
\frac{x^2}{4^2-1} + \frac{y^2}{4^2-3^2} + \frac{z^2}{4^2-5^2} + \frac{w^2}{4^2-7^2} &= 1,\\
\frac{x^2}{6^2-1} + \frac{y^2}{6^2-3^2} + \frac{z^2}{6^2-5^2} + \frac{w^2}{6^2-7^2} &= 1,\\
\frac{x^2}{8^2-1} + \frac{y^2}{8^2-3^2} + \frac{z^2}{8^2-5^2} + \frac{w^2}{8^2-7^2} &= 1.
\end{aligned}$$

4 Hints

Here are some hints with some answers.

1.1 We have that $f(x) = (x-a)g(x) + r(x)$ where $r(x)$ is either constant or zero. What happens when we plug in a?

1.2 By Division Algorithm, $H(x) = (x-1)(x-2)(x-3)q(x)+r(x)$. Note that $r(x)$ is the remainder. What is its degree?

2.6 What are the roots of $g(x)$? $h(x)$? How about their leading coefficients?

2.7 Note that $f(k) = 2k+1$ for $k = 1, 2, 3$. The answer is 1022_3.

2.8 Let $Q(x) = (x+1)P(x) - x$. What is the degree of Q and what are its roots?

2.9 $P(k) = 1 + \frac{9k-1}{k^2+k}$, so $(k^2+k)(P(k)-1) - 9k + 1 = 0$ for $k = 1, 2, \ldots, 7$. What happens when $k = 0$ and -1? Answer is $1101_3 - 1022_3$.

2.10 Consider $Q(x) = P(2x) - P(x) - 1$.

3.2 Use Lagrange's Interpolation Formula. Answer is $f(x) = -3x^4 + 2x^3 + 20x^2 - 5x + 3$.

3.3 Consider the expression

$$1 - \frac{x^2}{t-1} - \frac{y^2}{t-9} - \frac{z^2}{t-25} - \frac{w^2}{t-49}.$$

Analyze it upon multiplying by $(t-1)(t-9)(t-25)(t-49)$.