The Fundamental Theorem of Algebra

Yan Tao

Advanced 1

1 Polynomial Division

Definition 1 *A **polynomial** (over the real numbers) is an expression of the form $a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$, where $a_n, ..., a_0$, called the **coefficients**, are real numbers.*

Note that the term *polynomial* refers only to this expression, not an equation involving it. We can also define polynomials over other number systems (such as the rational numbers, or the complex numbers), where the coefficients are those kinds of numbers, in the same way. Finally, we'll make one crucial assumption:

Problem 1 *Explain why we can assume that, for a nonzero polynomial, the first coefficient $a_n \neq 0$. (The term a_nx^n is called the **leading term** of the polynomial.)*

Solution: If the first term is zero, we can remove it from the expression and replace n with $n-1$, and so on, until it's not zero.

With that assumption, we define

Definition 2 *The **degree** of a nonzero polynomial is the power of x in its leading term.*

We'll often write $f(x)$ (or just f) as shorthand for a polynomial in the variable x, and the degree of f can be abbreviated $\deg(f)$. So, for example, if $f(x) = 3x^5 + 15x^2 - 20$, then $\deg(f) = 5$. (The degree of the zero polynomial is undefined, but it can also be convenient to think of it as $-\infty$. Try to think about why as you work through these next problems!)

In general, the degree of a polynomial gives us a rough idea of how big it is, the same way that the absolute value of an integer does (for example). So, just like in the case of integers, we can divide polynomials:

Theorem 1 *For any polynomials f, g where g is nonzero, there exist unique polynomials q and r such that*

$$f = qg + r$$

*and $deg(r) < deg(g)$. q is called the **quotient** of the division, and r is the **remainder**.*

To prove Theorem 1, we use the *division algorithm* for polynomials. (Theorem 1 is itself called the polynomial division algorithm, even though it's not an algorithm, but we'll use these terms interchangeably.) The algorithm works similarly to long division for integers: as an example, let's see how we would divide $x^3 + 3x^2 + 5x - 4$ by $x - 1$. Similarly to usual long division, we multiply the *divisor* by the most simple thing (a *monomial* in this case) such that when we subtract the result, the leading terms of the polynomial cancel. We then repeat until we get a quotient and a remainder, as illustrated below:

$$
\begin{array}{rrrrr}
 & & x^2 & +4x & +9 \\ \cline{2-5}
x-1 \big) & x^3 & +3x^2 & +5x & -4 \\
 & -x^3 & +x^2 & & \\ \cline{2-3}
 & & 4x^2 & +5x & \\
 & & -4x^2 & +4x & \\ \cline{3-4}
 & & & 9x & -4 \\
 & & & -9x & +9 \\ \cline{4-5}
 & & & & 5
\end{array}
$$

In this case, we obtain a quotient of $x^2 + 4x + 9$ and a remainder of 5.

Problem 2 *Perform the following divisions of polynomials over the real numbers. What is the quotient and remainder of each?*

- Divide $x^2 + 1$ by $x - 1$

  Solution:
$$
\begin{array}{rrrr}
 & & x & +1 \\ \cline{2-4}
x-1 \big) & x^2 & & +1 \\
 & -x^2 & +x & \\ \cline{2-3}
 & & x & +1 \\
 & & -x & +1 \\ \cline{3-4}
 & & & 2
\end{array}
$$

- Divide $x^3 - 5x - 2$ by $x + 2$.

  Solution:
$$
\begin{array}{rrrrr}
 & & x^2 & -2x & -1 \\ \cline{2-5}
x+2 \big) & x^3 & & -5x & -2 \\
 & -x^3 & -2x^2 & & \\ \cline{2-3}
 & & -2x^2 & -5x & \\
 & & 2x^2 & +4x & \\ \cline{3-4}
 & & & -x & -2 \\
 & & & x & +2 \\ \cline{4-5}
 & & & & 0
\end{array}
$$

- Divide $x^4 + 3x^3 - 10x^2 + 4x - 8$ by $x^2 - x + 1$.

  Solution:
$$
\begin{array}{rrrrrr}
 & & & x^2 & +4x & -7 \\ \cline{2-6}
x^2-x+1 \big) & x^4 & +3x^3 & -10x^2 & +4x & -8 \\
 & -x^4 & +x^3 & -x^2 & & \\ \cline{2-4}
 & & 4x^3 & -11x^2 & +4x & \\
 & & -4x^3 & +4x^2 & -4x & \\ \cline{3-5}
 & & & -7x^2 & & -8 \\
 & & & 7x^2 & -7x & +7 \\ \cline{4-6}
 & & & & -7x & -1
\end{array}
$$

Problem 3 *Explain why this algorithm "works" as a proof of Theorem* 1 *(for real polynomials, let's say) - that is, why is* $deg(r) < deg(g)$ *and why are* q *and* r *unique?*

Solution: By definition the algorithm only stops once the remaining term has a smaller degree than the divisor, and q and r are unique because the monomials we get at each step have to be equal to one particular thing - the leading term of the remaining polynomial divided by the leading term of the divisor.

Problem 4 *(Bonus) Does your answer to the previous problem also work for other number systems, like the rationals and complex numbers? Think about which feature of the reals we've been using.*

Solution: The same proof works over the rationals and complexes, and indeed any number systems where numbers can be divided.

2 Roots of Polynomials

Definition 3 *A (rational, real, complex) root of a polynomial* f *is a (rational, real, complex, respectively) number* a *that satisfies the equation* $f(a) = 0$.

In general, the coefficients and root of a polynomial should be in the same number field for this to make sense (of course, these examples are all complex numbers). For now, let's examine some real roots.

Problem 5 *Show that* a *is a root of* f *if and only if* f *is* ***divisible*** *by* $x - a$ *(that is, that the remainder when* f *is divided by* $x - a$ *is zero).*

Solution: If f is divisible by $x - a$, then it can be written as $f = (x - a)q$, and plugging a into both sides gives zero on the right-hand side. Conversely, if a is a root of f, we apply the division algorithm to write $f = (x - a)q + r$, and plugging a into both sides gives $r = 0$, so f is divisible by $x - a$.

Problem 6 *Find the roots of the following polynomials.*

- $(x - 1)(x + 2)$

  Solution: 1 and -2.

- $(x + 5)^2(x - 18)^6$

  Solution: 18 and -5.

- $x^3(x + 1)(x - 1)^2$

  Solution: 0, 1, and -1.

Roots are easiest to find in factored polynomials - factoring is hard in general, so we will only handle factored forms for now. For the factored form of a polynomial, we define

Definition 4 *If a is a root of f, its* ***multiplicity*** *is the number of times the factor $(x - a)$ appears in the factored form of f.*

For example, in the polynomial $(x - 1)^2$, the root 1 has multiplicity 2. So even though it has one root, it will be useful to count the root 1 twice. In general, when we count roots a number of times equal to their multiplicity, we say the roots are *counted up to multiplicity.*

Problem 7 *For each example given in Problem 6, find the degree of the polynomial and the number of its roots, counted up to multiplicity.*

Solution: For the first example, 2 and 2. For the second example, 8 and 8. For the third example, 6 and 6. (To find the degrees, note that the leading term must use an x from each term when multiplied out.)

Unfortunately, for the case of polynomials in real numbers, some break the trend exhibited by these examples.

Problem 8 *What is the degree of $x^2 + 1$? How many real roots does it have, counted up to multiplicity? How many complex roots does it have, counted up to multiplicity?*

Solution: It's degree 2, and has no real roots. To prove the latter, we just set it equal to zero, so we get the impossible $-1 = x^2 \geq 0$. It has two complex roots, namely $\pm i$.

In the complex numbers, the trend we've seen so far does in fact hold for all polynomials; this is the content of the famous Fundamental Theorem of Algebra:

Theorem 2 *(Fundamental Theorem of Algebra) Every nonzero polynomial f in the complex numbers has exactly deg(f) roots, counted up to multiplicity.*

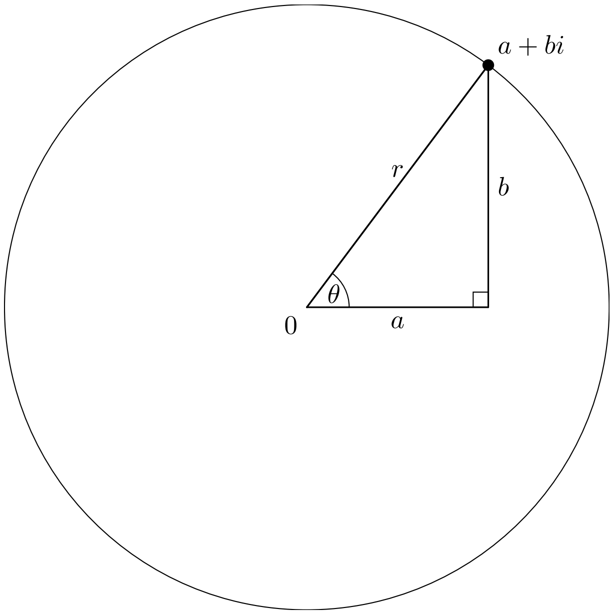
To prove this, we'll first reduce it to a (slightly) simpler statement:

Problem 9 *Show that the Fundamental Theorem of Algebra is equivalent to the statement that every non-constant (degree at least 1) polynomial has a complex root. (Hint: One direction is trivial. For the other direction, use Problem 4 - what is the degree of the quotient?)*

Solution: Clearly FTA implies this statement, so suppose we have this statement. Then by Problem 4 f is divisible by some $x - a$, so write $f = (x - a)q$. The leading term of f must come from the x multiplied by the leading term of q, so $\deg(q) = \deg(f) - 1$. FTA follows by induction on $\deg(f)$ (since nonzero constant polynomials have no roots).

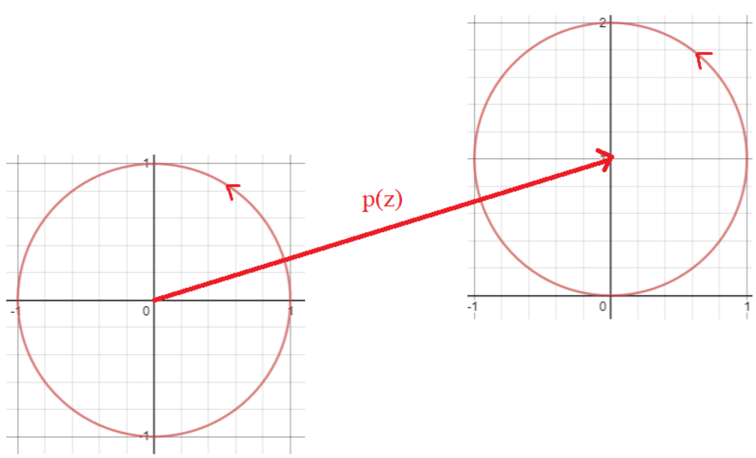
3 Finding a Complex Root

To finish the proof, it's convenient to recall two different forms of complex numbers: the *rectangular form* $a+bi$ and the *polar form* $re^{i\theta}$, which are related by the following diagram. (As a reminder, θ is the angle of the complex number from the positive real axis of the complex plane.) r is in particular called the *magnitude* of the complex number - if r is the magnitude of a complex number z, we denote that $r = |z|$.



We'll look at the *graph* of a polynomial. In the real case, this is easier because the domain and range are both 1-dimensional, but in the complex case they are 2-dimensional, so drawing the whole graph is impossible. Instead, we'll draw simple shapes, such as a circle, and look at the *images* of these shapes.

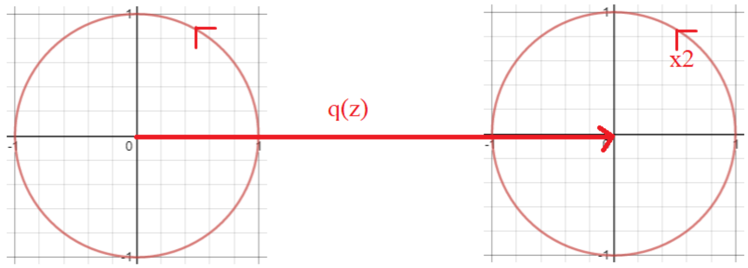
For example, consider the polynomial $f(z) = z + i$. When drawing the image of the unit circle, we first trace the unit circle. Generally, we'll do so counterclockwise. As we can see from the diagram above, points on the unit circle are of the form $e^{i\theta}$ (since $r = 1$) and tracing counterclockwise means we take θ to go up from 0 to 2π (since there are 2π radians in a circle). Plugging that in, we get $f(z) = i + e^{i\theta}$, still traced from 0 to 2π, so the image is still a counterclockwise circle, but is now centered at i instead of the origin. So graphing $f(z) = z + i$ can look like the following:



Problem 10 *Similarly graph the following polynomials:*

- $f(z) = z^2$, $f(z) = z^3$, $f(z) = z^4$, and so on. Do you see a pattern? How about $f(z) = z^n$?

  Solution: In general, z^n winds around the origin n times counterclockwise, as in the following diagram.

- $f(z) = 2z$, $f(z) = 3z$, $f(z) = 1/2z$. In general, how about is $f(z) = cz$, for some positive real number c?

  Solution: It winds around the origin once with radius c.

- $f(z) = -z$.

  Solution: It winds around the origin once with radius 1, but starts at a different point on the circle (at -1 instead of 1).

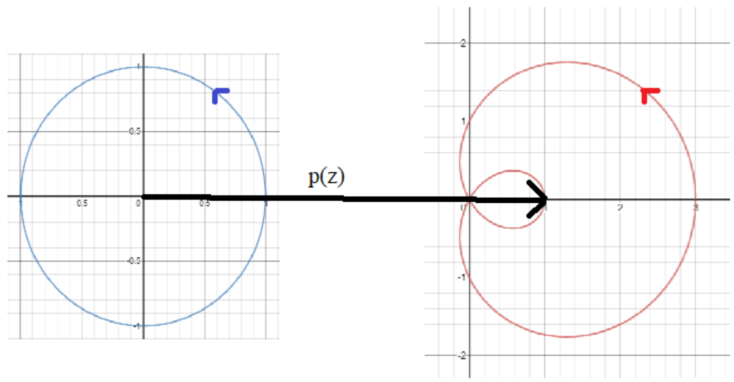
- $f(z) = z + z_0$, where z_0 is any complex number.

  Solution: This is a translated circle of radius 1.

Problem 11 *Now let's consider the slightly more complicated case* $f(z) = z^2 - z + 1$.

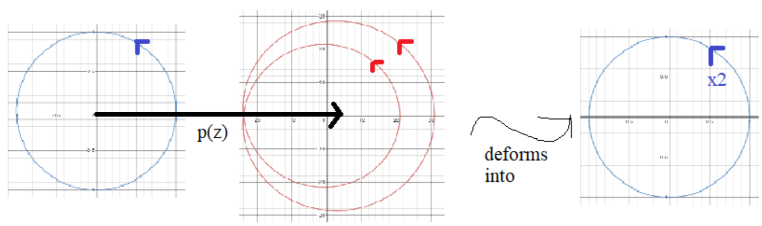
- Sketch a graph similarly to Problem 10. (Hint: To do this by hand, try graphing z^2 and $-z$ separately and adding the corresponding points together. It may also be helpful to use a tool like Desmos.)

  Solution:



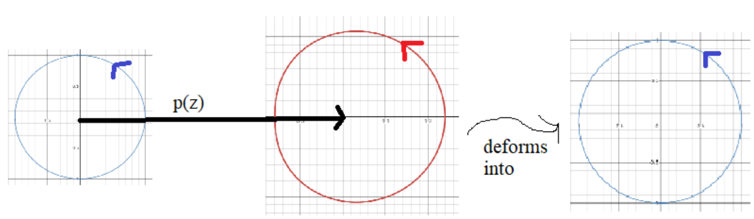
- Now consider a circle of radius $R = 5$. How about $R = 10$? $R = 100$? Is there any pattern for large R? (Hint: The image can be deformed into a picture we've seen before.)

  Solution: It looks more like the graph of $z^2 + 1$.



- Now consider a circle of radius $R = 0.2$, or $R = 0.1$, or $R = 0.000000001$. Do the same as above - what's the pattern here?

  Solution: It looks more like the graph of $-z + 1$.



Problem 12 *For a general polynomial $f(z) = a_n z^n + ... + a_0$, make your best guess as to what (approximately) the image of a circle of very large radius is. How about a very small radius?(Challenge: Prove your guesses.)*

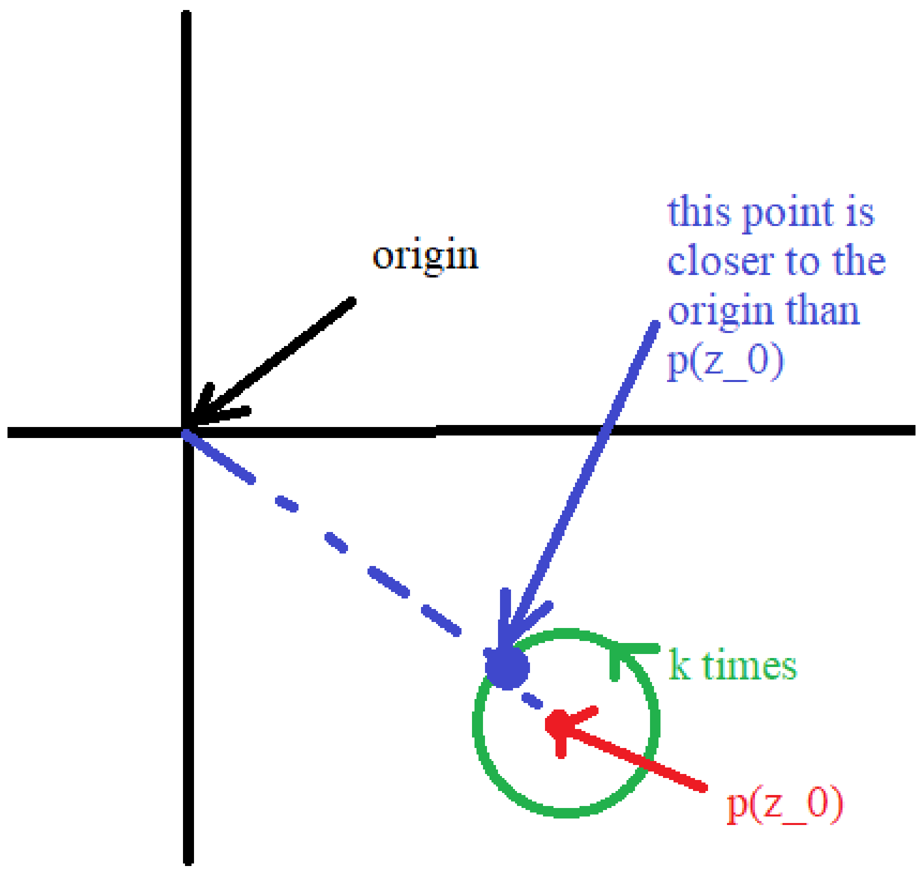
Solution: Large circles look like the image of z^n, while small circles look like the image of z^k for the smallest nonzero nonconstant term $a_k x^k$.

We need one last result to prove the Fundamental Theorem of Algebra, which we won't prove this week.

Theorem 3 *For every polynomial f, there is a point z_0 in the complex plane that minimizes $|f(z)|$.*

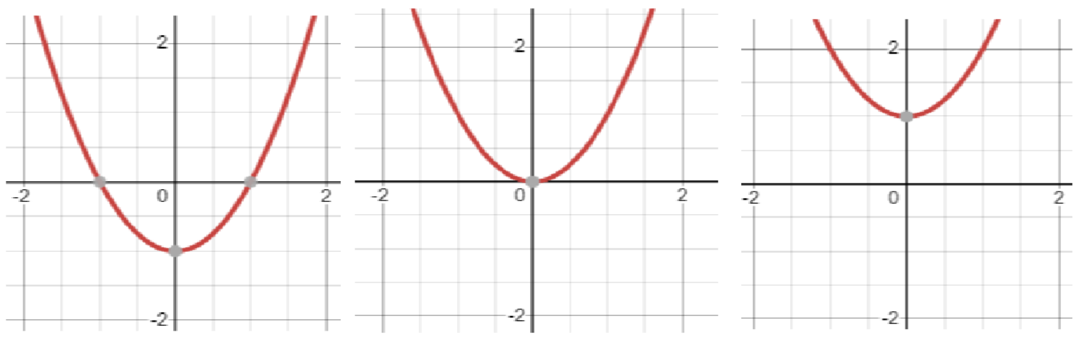
Problem 13 *Finish the proof of the Fundamental Theorem of Algebra, by showing that every nonconstant polynomial has a complex root. (Hint: By making the right substitution, first show that we can assume the point z_0 from Theorem 3 is just the origin. Then look at the image of some particular circles, and use the fact that $|w|$ is the distance from w to the origin in the complex plane.)*

Solution: First make the substitution $z \mapsto (z - z_0)$, so that we can assume z_0 is the origin. Then taking sufficiently small circles, we can see by Problem 12 that the image winds k times counterclockwise around $f(0)$, with a very small radius, for some $k > 0$. If f didn't have a root, then $f(0)$ would have to be nonzero, so a very small circle around it doesn't contain the origin, and we find a point closer to the origin, as in the diagram below, which is a contradiction, so f must have a root.



4 Bonus Section: Geometric Meaning of Multiplicity

Let's return to our discussion of real roots. Viewing a polynomial in the real numbers as a function from the reals to the reals, we can draw the entire graph in the plane, as we learned from algebra class. The following graphs are of the functions $x^2 - 1$, x^2, and $x^2 + 1$, respectively.



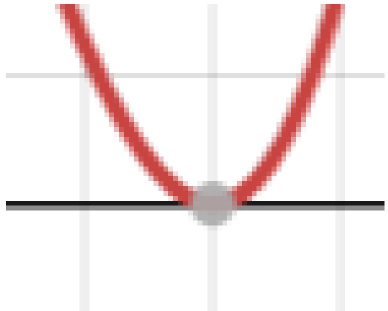
Problem 14 *How many real roots does each polynomial have, and how many do they have counted up to multiplicity? How can you tell the multiplicity of the roots just from the graph?*

Solution: The first has two real roots (two up to multiplicity), the second one (two up to multiplicity), and the third none. The first roots have multiplicity 1 because the graph passes through the x-axis, while the second polynomial's root has multiplicity at least 2 because it's tangent (and by FTA, exactly 2).

Problem 15 *Show that the graph near a root of multiplicity n looks like the graph near the root 0 of some ax^n if zoomed in close enough. (This can be seen on a website like Desmos.)*

Solution: If the root is at a, make the substitution $x \mapsto x - a$ so that it's at zero. For values sufficiently close to zero, the other factors $(x - b)$ are approximately constant at $-b$, so the function is approximately x^n (times some constants) since the root must correspond to n factors of x.

Problem 16 *Given that the following graph comes from a cubic (degree 3) polynomial, find the multiplicity of this root.*



Solution: 2, because it looks like an even power of x and its multiplicity must be less than 3 by FTA.

Problem 17 *Would the previous problem be answerable if we did not know the function was a cubic?*

Solution: Yes or no - the even powers (similarly, the odd powers) do look different from each other, but it is not easy to differentiate between them, unlike between an even power and an odd power.

Finally, we'd like to apply a similar notion of multiplicity not just to graphs of functions, but to more general geometric shapes. For instance, a circle is not the graph of any function (to see this, just see that it fails the vertical line test), but it is still related to a polynomial - the unit circle in the plane is given by $x^2 + y^2 = 1$, which is a polynomial (in two variables). We won't formally study these this week, but our intuition from graphs of polynomials does carry over.

Problem 18 *In the following pictures including circles, try to guess at what the "multiplicity" of each intersection point would be.*