Polynomials II - Divisibility and Irreducibles

Yan Tao

Febuary 13, 2022

1 Divisibility of Polynomials

Definition 1 *Let p and q be polynomials in the complex numbers $\mathbb{C}$. We say that p* ***is divisble by*** *q over $\mathbb{C}$ if there exists a polynomial r such that $p(z) = q(z)r(z)$.*

Problem 1 *By long division (which we learned how to do last week), answer the following:*

- Is $x^3 - 2x^2 + x - 2$ divisible by $x - 2$ over $\mathbb{C}$?

  Solution: Yes

- Is $x^2 - 4x + 3$ divisible by $x + 1$ over $\mathbb{C}$?

  Solution: No

- Is $x^4 + 1$ divisible by $x^2 + i$ over $\mathbb{C}$?

  Solution: Yes

There are some tricks to see divisibility more quickly than by long division, so let's establish a couple useful ones.

Problem 2

- *Show that if p is divisible by the linear (degree 1) polynomial $x - a$ over $\mathbb{C}$ if and only if a is a root of p.*

  Solution: Suppose p is divisible by $x-a$. Then there exists a polynomial q such that $p(x) = (x-a)q(x)$. Plugging in a, we get zero.

  Conersely, suppose that a is a root of p. Then performing long division of p by $x - a$, we get a quotient and a remainder $p(x) = (x - a)q(x) + r$. Plugging in a, we must get zero, so $r = 0$ and therefore p is divisible by $x - a$.

- *Show that if the coefficients of p add up to 0, then p is divisible by $x - 1$ over $\mathbb{C}$.*

  Solution: Plugging in 1, we get the sum of the coefficients of p, so 1 is a root of p.

For polynomials over the real numbers, we make a similar (but not quite the same) definition:

Definition 2 *Let p and q be polynomials in the real numbers $\mathbb{R}$. We say that p* ***is divisble by*** *q over $\mathbb{R}$ if there exists a polynomial r such that $p(z) = q(z)r(z)$.*

Divisibility over $\mathbb{C}$ and over $\mathbb{R}$ is similar. Because all real numbers are also complex numbers, if p is divisible by q over $\mathbb{R}$ it is also divisible by q over $\mathbb{C}$. The reverse is not true, however - in Problem 1 we see that x^4+1 is divisible by x^2+i over $\mathbb{C}$. But we cannot say that x^4+1 is divisible by x^2+i over $\mathbb{R}$ - because i is not a real number, x^2+i *doesn't exist* over $\mathbb{R}$.

Problem 3 *Show that the tricks proven in Problem 2 still work if we replace $\mathbb{C}$ with $\mathbb{R}$.*

Solution: The exact same logic applies over $\mathbb{R}$

2 Reducibility and Splitting

Definition 3 *Let p be a* ***non-constant*** *polynomial with coefficients in $\mathbb{C}$ (respectively, $\mathbb{R}$)*

- *p is* ***reducible over*** *$\mathbb{C}$ (respectively, over $\mathbb{R}$) if it is divisible by a polynomial q over $\mathbb{C}$ (respectively, over $\mathbb{R}$), where q is not constant and also has smaller degree than p.*
- *p is* ***irreducible over*** *$\mathbb{C}$ (respectively, over $\mathbb{R}$) if it is not reducible over $\mathbb{C}$ (respectively, over $\mathbb{R}$).*
- *p* ***splits over*** *$\mathbb{C}$ (respectively, over $\mathbb{R}$) if it factors into linear factors over $\mathbb{C}$ (respectively, over $\mathbb{R}$); i.e. if there exist $r_1, ..., r_n$ all in $\mathbb{C}$ (respectively, $\mathbb{R}$) such that $p(x) = (x-r_1)...(x-r_n)$.*

Problem 4 *Show that if p is a polynomial of degree at least 2 which splits over $\mathbb{C}$ (respectively, over $\mathbb{R}$), then p is reducible over $\mathbb{C}$ (respectively, over $\mathbb{R}$).*

Solution: Suppose p splits; then in particular it is divisible by a linear factor $x-a$, which is not constant and also has degree 1 which is smaller than the degree of p.

It's natural to ask whether the converse is true - does every reducible polynomial split? Let us see one example on the next page.

Problem 5 *Let* $p(x) = x^4 + 3x^2 + 2$.

- *Show that* p *is reducible over* $\mathbb{R}$. *(Hint: To find a factor, it might help to make a substitution.)*

  Solution: Making the substitution $y = x^2$ *and factoring (using the quadratic formula if neccessary) we get* $(y + 1)(y + 2)$, *so that* $p(x) = (x^2 + 1)(x^2 + 2)$, *so* p *is reducible.*

- *Show that* p *does not split over* $\mathbb{R}$. *(Hint: If a polynomial splits, its roots should be very easy to find. But does* p *have real roots?)*

  Solution: If p *split over* $\mathbb{R}$, *then it would have to have* 4 *real roots (one from each linear factor. But its roots are* $\pm i$ *and* $\pm\sqrt{2}i$, *none of which are real.*

Just like with integers, we can factor polynomials into irreducibles. Therefore, it helps a lot to know what the irreducibles are over $\mathbb{C}$ and over $\mathbb{R}$. The following very famous theorem, which we will not prove this time (maybe in the future!), helps us understand polynomials in complex coefficients.

Theorem 1 *(Fundamental Theorem of Algebra) Every polynomial splits over* $\mathbb{C}$.

Problem 6 *Describe all irreducible polynomials over* $\mathbb{C}$.

Solution: By the Fundamental Theorem of Algebra and by Problem 4, every polynomial of degree greater than 1 is reducible. Conversely, every linear polynomial is irreducible because there are no nonconstant polynomials of lower degree. Therefore all the irreducible polynomials over $\mathbb{C}$ are the linear polynomials.

Over $\mathbb{R}$, the task is a little harder, but not by much. Since this isn't too important, feel free to skip this page if you want.

Problem 7 *(Challenge) Show that every cubic polynomial is reducible over $\mathbb{R}$. (Hint: Consider the cubic formula from last week. Can you show that one of the three roots is real?)*

Solution: Recall the cubic formula. If $q^2/4 - p^3/27$ is nonnegative, then both u and v are real, so the root $x = u + v$ is real. If it is negative, then u^3 and v^3 are complex conjugates, so u and v are also complex conjugates, and therefore $x = u + v$ is, again, real.

Problem 8 *(Challenge) Describe all irreducible polynomials over $\mathbb{R}$. (Hint: For any polynomial in real coefficients, we know that it splits over $\mathbb{C}$. Using the fact that it has real coefficients, group the complex roots in a certain way, then factor the polynomial using that grouping as much as you can.)*

Solution: Given a polynomial p in real coefficients, it splits over $\mathbb{C}$ as $p = (x - r_1)...(x - r_n)$. If r_j is real, then it is a real root so p has $x - r_j$ as a factor over $\mathbb{R}$ by Problem 2. If r_j is not real, then $0 = \overline{p(r_j)} = p(\overline{r_j}$ so its complex conjugate is also a root; in that case, $(x - r_j)(x - \overline{r_j}) = x^2 - 2\mathrm{Re}(r_j) + |r_j|^2$ is a quadratic with real coefficients. Therefore we can group all non-real roots with their conjugate pairs, which results in quadratic factors, so all irreducibles over the reals are either linear or quadratics with no real roots.

3 Polynomials with Rational Coefficients

As we've just seen, finding the irreducible polynomials in the complex and real numbers is simple and not very interesting. The task is much harder (but much more interesting!) over the rational numbers $\mathbb{Q}$. We define the same things we did before, just replacing the number system with $\mathbb{Q}$. So now, for instance, $x^2 - 2$ is not divisible by $x - \sqrt{2}$ over $\mathbb{Q}$, since $x - \sqrt{2}$ doesn't exist over $\mathbb{Q}$.

Problem 9 *Show that $x^2 - 2$ is irreducible over $\mathbb{Q}$. (Hint: Suppose it were reducible. What would the degrees of the factors have to be, and what does that mean?)*

Solution: If it were reducible, then there would exist polynomials q and r such that $x^2 - 2 = q(x)r(x)$ where q is not constant and not quadratic. But then q would have to be linear, so q would give a rational root of $x^2 - 2$, which has no rational roots, so we get a contradiction.

Problem 10 *Show that $x^3 - 2$ is irreducible over $\mathbb{Q}$. (Hint: This is similar to Problem 9.)*

Solution: If it were reducible, then there would exist polynomials q and r such that $x^3 - 2 = q(x)r(x)$ where q is not constant and not cubic. But then either q is linear, or q is quadratic in which case r is linear; in either case q or r would give a rational root of $x^3 - 2$, which has no rational roots, so we get a contradiction.

In general, it is very hard to detect irreducibility. For instance, let us try

Problem 11 *(Challenge) Let $p(x) = x^4 + 6x^2 + 25$.*

- *Find all the roots of p. Are any of them rational?*

  Solution: Via the substitution $y = x^2$ (or otherwise) we get the roots $x = 1 \pm 2i$ and $x = -1 \pm 2i$. None of these are rational.

- *Show that p is not irreducible. (Hint: Finding a factor is really hard, but we can narrow it down a bit using the answer to the previous part.)*

  Solution: $x^4 + 6x^2 + 25 = (x^2 + 5)^2 - (2x)^2 = (x^2 + 2x + 5)(x^2 - 2x + 5)$

Fortunately, there are some easier ways for us to show whether or not a polynomial is reducible over $\mathbb{Q}$.

4 Testing for Irreducibility

Note that if a polynomial has rational coefficients, we can multiply everything by the common demoninator, so it suffices to consider polynomials with integer coefficients.

Theorem 2 *(Rational Root Theorem) Suppose that p/q is a root of $a_n x^n + ... + a_0$ where p and q are relatively prime integers. Then p divides a_0 and q divides a_n.*

Problem 12 *Let us prove the Rational Root Theorem.*

- *Suppose that p/q is a root of $a_n x^n + ... a_0$. Plug it in to find an equation in terms of $p, q,$ and $a_0, ..., a_n$.*

  Solution: $a_n p^n/q^n + ... + a_1 p/q + a_0 = 0$

- *We want an equation in integers so we can test for divisibility. How do we make everything integers? Write down the new equation.*

  Solution: We can clear the denominator by multiplying everything by q^n: $a_n p^n + a_{n-1} p^{n-1} q + ... + a_1 p q^{n-1} + a_0 q^n = 0$

- *Factor your equation and use the fact that p and q are relatively prime to finish the proof.*

  Solution: All but one term has a p, so we have

  $$p(a_n p^{n-1} + a_{n-1} p^{n-2} q + ... + a_1 q^{n-1}) + a_0 q^n = 0$$

  so that, in particular, $a_0 q^n$ is divisible by p. Since p and q are relatively prime, this means a_0 is divisible by p. Similarly, we can factor all the terms with a q:

  $$a_n p^n + q(a_{n-1} p^{n-1} + ... + a_1 p q^{n-2} + a_0 q^{n-1}) = 0$$

  so that $a_n p^n$ is divisible by q so a_n is divisible by q.

Problem 13 *Show that $3x^3 - 5x^2 + 5x - 2$ is reducible over $\mathbb{Q}$.*

Solution: The Rational Root Theorem helps us find the root $x = 2/3$.

Problem 14 *Can the Rational Root Theorem show if a polynomial is **irreducible**?*

Solution: No. As seen in Problem 11, having no roots does not imply irreducibility.

There is a stronger test available which can show irreducibility.

Theorem 3 *(Eisenstein's Criterion) Suppose that* $q(x) = a_n x^n + ... + a_0$ *is a polynomial, and that there exists a prime number* p *such that:*

- p *divides* $a_0, a_1, ..., a_{n-1}$.
- p *does not divide* a_n.
- p^2 *does not divide* a_0.

Then q *is irreducible over* $\mathbb{Q}$.

We'll come back and prove this later.

Problem 15 *Show that the following polynomials are irreducible over* $\mathbb{Q}$.

- $3x^4 + 15x^2 + 10$

- $x^2 - 2$

- $x^3 - 2$

- $x^7 + 15x^5 - 3x^4 + 6x^3 + 9x^2 - 330x + 420$

Solution: The correct primes are 5, 2, 2, and 3, respectively.

Problem 16 *For any positive integer* n*, find an irreducible (over* $\mathbb{Q}$*) polynomial of degree* n.

Solution: If $n = 1$, then any linear polynomial is irreducible (see Problem 6). If $n > 1$, then for any prime number p, $p^{1/n}$ is irrational, so $x^n - p$ is irreducible by Eisenstein's Criterion.

Eisenstein's criterion can also be used on some polynomials where it doesn't seem useful at first glance.

Problem 17 *Let a be any rational number and $q(x) = a_n x^n + ... + a_0$ be a polynomial with rational coefficients. Show that if $q(x + a)$ (the polynomial obtained by substituting $x + a$ in for x) is irreducible, so is $q(x)$. (Hint: Suppose $q(x)$ were reducible. Find a way to reduce $q(x + a)$.)*

Solution: Suppose q were reducible, so that it could be written as $q(x) = r_1(x)r_2(x)$ where r_1 is not constant and has lower degree than q. Then $q(x+a) = r_1(x+a)r_2(x+a)$, and both $r_1(x+a)$ and $r_2(x+a)$ have the same degrees as $r_1(x)$ and $r_2(x)$, respectively, so $q(x+a)$ (which has the same degree as $q(x)$) is reducible, which is a contradiction.

Problem 18 *Show that $x^2 + x + 2$ is irreducible over $\mathbb{Q}$. (Hint: Substitute $x + 3$ for x.)*

Solution: Substituting $x + 3$ we obtain $x^2 + 7 + 14$, which is irreducible by Eisenstein's Criterion ($p = 7$).

Problem 19 *(Challenge) Let p be a prime number. Show that $x^{p-1} + ... + x + 1$ is irreducible over $\mathbb{Q}$. (Hint: Find the right substitution.)*

Solution: First notice that

$$x^{p-1} + ... + x + 1 = \frac{x^p - 1}{x - 1}$$

and substitute $x + 1$ for x, so we get $((x + 1)^p - 1)/x$. Expanding this out with the Binomial Theorem gives

$$x^{p-1} + \binom{p}{p-1}x^{p-2} + ... + \binom{p}{2}x + \binom{p}{1}$$

Since p is prime, $\binom{p}{1}, \binom{p}{2}, ..., \binom{p}{p-1}$ are all divisible by p, and $\binom{p}{1} = p$ is not divisible by p^2, so this is irreducible by Eisenstein's Criterion.

Problem 20 *(Challenge) Let's prove Eisenstein's Criterion. Fix*

$$q(x) = a_n x^n + ... + a_0$$

satisfying the hypotheses. As with most irreducibility proofs we've seen so far, the best course of action will be contradiction, so let's suppose q is reducible, and write its factors as

$$r(x) = b_l x^l + ... + b_0$$
$$s(x) = c_m x^m + ... + c_0$$

Since these have to multiply to q, we must have $l + m = n$.

- *Since p does not divide a_n, what can we say about b_l and c_m?*

  Solution: p divides neither b_l nor c_m.

- *Since p divides a_0 but p^2 doesn't, what can we say about b_0 and c_0? If your statement contains an either or, assume one of them without loss of generality.*

  Solution: Since p divides $a_0 = b_0 c_0$, it must divide one of them. But since p^2 doesn't divide a_0, it can't divide both of them. Therefore, without loss of generality, let us say that p divides b_0 but not c_0.

- *Write out $a_1, a_2, ...,$ etc. in terms of b's and c's, until you see a pattern. (They will get longer and longer, but there's a nice pattern.)*

  Solution: Writing out a few terms

$$a_1 = b_0 c_1 + b_1 c_0$$
$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$$
$$a_3 = b_0 c_3 + b_1 c_2 + b_2 c_1 + b_3 c_0$$

- *Using what you've proven about b_0 or c_0, show something about b_1 or c_1. Then show something about b_2 or c_2. Notice a pattern? Complete the proof by showing something about b_l or c_m that contradicts what you found in the first part. (Hint: This is a proof by induction.)*

  Solution: All the b_j are in fact divisible by p. To prove this, let us induct on j. The base case $j = 0$ has already been established, so suppose there is some j such that b_k is divisible by p for all $k < j$. Then using the pattern we've seen above,

$$a_j = (b_0 c_j + b_1 c_{j-1} + ... + b_{j-1} c_1) + b_j c_0 \Rightarrow b_j c_0 = a_j - (b_0 c_j + b_1 c_{j-1} + ... + b_{j-1} c_1)$$

  By assumption, every term in the parenthesis on the right-hand side is divisible by p, and since $j \leq l < n$, a_j is also divisible by p. But since c_0 is not divisible by p, b_j must then be divisible by p, which completes the induction. But then b_l is divisible by p, which is a contradiction.