Factoring a Polynomial

Dennis Chen

AQU

We discuss how to factor multivariable polynomials by finding its roots and thinking about symmetry, list some common factorizations, and discuss the Remainder Theorem. The only prerequisites are a solid understanding of basic factorization and being able to solve single-variable polynomials: this includes knowing the Rational Root Theorem.

§ 1 Multivariable Polynomials

We first define a factor of a polynomial rigorously, because we're going to be making use of it often.

> **Definition 1 (Factor of a Polynomial)** Denote a polynomial in terms of $a_1, a_2, \ldots, a_n$ as $P(a_1, a_2, \ldots, a_n)$. Then $Q(a_1, a_2, \ldots, a_n)$ is a factor of P if and only if it satisfies both of the following conditions:
>
> ✦ $\deg P \geq \deg Q$.
>
> ✦ If $Q(a_1, a_2, \ldots, a_n) = 0$ then $P(a_1, a_2, \ldots, a_n) = 0$.

This means that if $Q(x) = 0$ when x satisfies a condition, then $P(x) = 0$ for this condition as well. One of the most common examples is that if $P(a, b) = 0$ when $a + b = 0$, then $a + b$ is a factor.

Also remember that if a polynomial is cyclic, its factors will be cyclic, and if it is symmetric, its factors will be symmetric.

> **Example 1** Factorize $a^3 + b^3 + c^3 - 3abc$.

Solution: Note that a cubic is either unfactorable, factored into linears, or factored into a linear and a quadratic. We start by noting the only possible linear root is $a + b + c$ because of the symmetry and the fact $a^3 + b^3 + c^3 - 3abc$ is monic. We check that $a + b + c$ is a root, as when $a + b + c = 0$, we also have $a^3 + b^3 + c^3 - 3abc = 0$.

Then note the quadratic root must also be symmetric.[1] Knowing this, we know the quadratic factor is of the form $x(a^2 + b^2 + c^2) + y(ab + bc + ca)$. Since $a^3 + b^3 + c^3 - 3abc$ is monic, $x = 1$ and we also know that the coefficient of abc is $3y = -3$, so $y = -1$. So $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$.

Now finish by noting that $a + b + c = 0$ does not imply $a^2 + b^2 + c^2 - ab - bc - ca = 0$, so we cannot further factorize.

This is a solution that goes into a fair amount of rigor to highlight the thought processes. You don't need to do this; just guess factors that seem like they'll work and hope they do. (The only "proof" you need for a factorization is "we can easily check it works," since this is true.)

For good measure, let's try a harder problem – one that can't just be killed by abusing symmetry.

---

[1] Perhaps the quadratic root can be factored too. We must check that it cannot be.

Example 2 (Dennis Chen) Factor out

$$a^4 - 3a^3b + 3a^2b^2 - 3ab^3 + 2b^4.$$

Solution 1: Notice that a convenient grouping of these terms seems like

$$(a^4 + 3a^2b^2 + 2b^4) - 3ab(a^2 + b^2),$$

which is equivalent to

$$(a^2 + b^2)(a^2 + 2b^2) - 3ab(a^2 + b^2) =$$
$$(a^2 + b^2)(a^2 - 3ab + 2b^2).$$

At this point the rest of the problem is pretty straightforward – from experience factoring single-variable quadratics, we should be able to easily guess that $(a^2 - 3ab + 2b^2) = (a - 2b)(a - b)$. Thus the entire factorization is

$$(a^2 + b^2)(a - 2b)(a - b).$$

We provide an alternative solution that abuses the following fact: **proving a factorization is a lot easier than finding one**, so we may abuse "illegitimate" strategies. This also abuses the fact that the entire function is homogenous and thus can be scaled. This way, we can turn a two-variable factorization problem into a one-variable factorization problem, which essentially is the same as solving a polynomial.

Solution 2: Note that the degree of each term is 4; this means that if (a, b) is a root, then so is $(\frac{a}{c}, \frac{b}{c})$. We abuse this by setting $c = b$; now we solve for the roots of a single-variable polynomial, which should be more familiar. So we set $b = 1$ and scale up later.

Our polynomial becomes $f(a) = a^4 - 3a^3 + 3a^2 - 3a + 2$. Rational Root Theorem[2] makes one of the roots easily guessable; plugging in $a = 1$ gives $f(a) = 0$. So then we divide out $(a - 1)$ to get

$$f(a) = (a - 1)(a^3 - 2a^2 + a - 2).$$

Either factoring by grouping or Rational Root Theorem will finish the job; in either case, our final factorization of $f(a)$ is

$$f(a) = (a - 1)(a - 2)(a^2 + 1).$$

Thus the roots are $a = 1, a = 2, a = i, a = -i$, and scaling up gives roots of $a = b, a = 2b, a = ib, a = -ib$, so the answer is

$$(a - b)(a - 2b)(a - ib)(a + ib) = (a - b)(a - 2b)(a^2 + b^2).$$

§ 1.1 Common Factorizations

Here's a list of common (but non-obvious) factorizations you should know well.

Fact 1 (Common Factorizations)

✦ $a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$

✦ Sophie Germain's: $a^4 + 4b^4 = (a^2 + 2b^2 - 2ab)(a^2 + 2b^2 + 2ab)$

✦ $b^4 + b^2 + 1 = (b^2 - b + 1)(b^2 + b + 1)$

---

[2]If you don't know what the Rational Root Theorem is, you can heuristically think of it as "guessing plausible nice-looking numbers as roots."

§ 2 Remainder Theorem

The polynomial remainder theorem provides an easy and systematic method to find the remainder of a polynomial $f(x)$ when divided by a linear equation $x - r$. Though the result itself is rather low-power and obscure, the idea behind it (and the more powerful Generalized Remainder Theorem) are very important tools when solving certain classes of algebra problems.

Theorem 1 (Remainder Theorem) The Remainder Theorem states that for polynomial $f(x)$, the remainder of $f(x)$ divided by $x - r$ is $f(r)$.

Proof: Let $f(x) = (x - r)p(x) + q$. Clearly q is the remainder. Then notice $f(r) = (r - r)p(x) + q = q$, as desired. ∎

Of course, the method here can be generalized.

Theorem 2 (Generalized Remainder Theorem) The Generalized Remainder Theorem states that for polynomial $f(x)$, the remainder of $f(x)$ when divided by nth degree polynomial $g(x)$ with roots $r_1, r_2 \ldots r_n$ is the $(n - 1)th$ degree polynomial $p(x)$ that satisfies $f(r_i) = p(r_i)$ for all $1 \leq i \leq n$.

Proof: Let $f(x) = g(x)p(x) + r(x)$. Then notice that for any r_i, $f(r_i) = g(r_i)p(r_i) + r(r_i) = r(r_i)$. (Notice that $g(r_i) = 0$ as r_i is defined to be a root of g.) ∎

Here's an example of a generic remainder theorem problem.

Example 3 (Roots of Unity) Prove that $a - 1 | a^n - 1$.

Solution: The remainder of $f(n) = a^n - 1$ when divided by $a - 1$ is $f(-(-1)) = f(1) = 1^n - 1 = 0$.

§ 3 Assorted Techniques

§ 3.1 Roots of Unity Substitution

When we divide a polynomial $P(x)$ by something like $\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + 1$, we can subtract copies of $x^n - 1$ because the remainder is still the same, and we can still easily keep track of the quotient.

Example 4 Find the remainder of $x^{28} + 1$ when divided by $x^4 + x^3 + x^2 + x + 1$.

Solution: Note that the remainder of $x^{28} + 1$ when divided by $x^4 + x^3 + x^2 + x + 1$ is the same as the remainder of $x^{28} + 1 - P(x)(x^5 - 1)$, since $x^4 + x^3 + x^2 + x + 1 \mid x^5 - 1$. Now note that the remainder of $x^{28} + 1$ divided by $x^5 - 1$ is $x^3 + 1$. Since this is a third degree polynomial, we're done.

This solution is predicated on the idea that you can subtract multiples of the divisor from the dividend and still get the same remainder. It just happens that we don't get a fourth degree polynomial in this case – you have to make sure the degree is correct when using this trick in general.

Now for a harder example, which is taken from the modular arithmetic handout.

MAST

Example 5 (NQU-Mod) Prove that $31 \mid 5^{31} + 5^{17} + 1$.

Solution: Note that $31 = 5^2 + 5 + 1$, which motivates the substitution $x = 5$. Now note we want to prove

$$x^2 + x + 1 \mid x^{31} + x^{17} + 1.$$

But note that the roots of the divisor are the third roots of unity, and also note that the third roots of unity are roots of $x^{31} + x^{17} + 1$, as

$$x^{31} + x^{17} + 1 = x + x^2 + 1 = 0$$

if x is a third root of unity.

   This solution is predicated on the idea that for $P(x) \mid Q(x)$, all of the roots of $P(x)$ must be roots of $Q(x)$.

§ 3.2   Factorizations as Identities

Before we relate factorizations and identities, we should first define an identity.

> **Definition 2 (Identity)** We say that $f = g$ is an identity for expressions f and g if it is true for all inputs that go into f, g.

   So, for example, $x^2 - y^2 = (x-y)(x+y)$ is an identity because it is true for all pairs (x, y), while $x - y = 0$ is not an identity because $2 - 1 = 0$, among other counterexamples.

   It is important to realize that **a factorization is really an identity**; that is, we are trying to show that $f(x) = g(x)$ where f is a polynomial and g is the factorization. The following intuitive observation will be stated explicitly.

> **Theorem 3 (Degrees of Identities)** If $f = g$, then the degree of f must be the same as the degree of g as defined about any variable where f, g take inputs. Also, f and g must nontrivially take the same inputs.[a]
>
> ---
> [a]If f non-trivially takes a variable x as an input, that means there exist two values x_1 and x_2 such that $f(x_1) \neq f(x_2)$. So $f = a + b + c - c$ does not take c as an input, because the value of c does not change the output of f.

   You can prove this theorem with some size argument; I do not care enough to do so because it should be intuitively obvious.

> **Exercise 1** Why can't $x^{101} + y^{100}x + (x^2 + xy - y^3)(x + xy + y^9) = (x + y)^{100}$ be an identity?

   This degree idea is very important, **because the degree of a polynomial limits the number of roots it can have.** This means that if $\deg f = \deg g = n$, and you show $f = g$ for $n + 1$ different inputs, then you're done. Alternatively, if you show $f = g$ for n different inputs and show that they have the same constant factor (generally an easy task for explicitly given identities), you are also done. The easiest n values to show $f = g$ for are usually the roots.

   This really comes into play in the next section: polynomial interpolation.

§ 3.3   Polynomial Interpolation

Occasionally you'll see problems that ask you to prove $p(x) = q(x)$, where $p(x)$ and $q(x)$ are some **rational functions**.[3] The trick here is that you can use polynomial interpolation – if you can clear common divisors to make it equivalent to $P(x) = Q(x)$ for polynomials P, Q, and then you show that this identity is true, the original problem is done as well.

   We provide an example to concretely show what this means.

---
[3]A rational function is one that can be expressed as the quotient of two polynomials.

Example 6 (AMC 10A 2019/24) Let p, q, and r be the distinct roots of the polynomial $x^3 - 22x^2 + 80x - 67$. It is given that there exist real numbers A, B, and C such that

$$\frac{1}{s^3 - 22s^2 + 80s - 67} = \frac{A}{s-p} + \frac{B}{s-q} + \frac{C}{s-r}$$

for all $s \notin \{p, q, r\}$. What is $\frac{1}{A} + \frac{1}{B} + \frac{1}{C}$?

Solution: Note that by the polynomial interpolation method discussed above, this is the same as solving for A, B, C such that

$$1 = A(s-q)(s-r) + B(s-r)(s-p) + C(s-p)(s-q).$$

Here's where polynomial interpolation helps us: **we are now allowed to set $s = p, q, r$.** With this in mind, the solution becomes much more straightforward.

Note that

$$1 = A(p-q)(p-r)$$
$$1 = B(q-r)(q-p)$$
$$1 = C(r-p)(r-q),$$

which we get from substituting $s = p, q, r$, respectively. This then implies

$$\frac{1}{A} = (p-q)(q-r)$$
$$\frac{1}{B} = (q-r)(q-p)$$
$$\frac{1}{C} = (r-p)(r-q).$$

At this point we can just finish with Vieta's Formulas. Note that

$$\frac{1}{A} + \frac{1}{B} + \frac{1}{C} = (p-q)(p-r) + (q-r)(q-p) + (r-p)(r-q) =$$

$$p^2 - pq - pr + qr + q^2 - qr - qp + rp + r^2 - rp - rq + pq =$$

$$(p+q+r)^2 - 3(pq + qr + rp) = 22^2 - 3 \cdot 80 = 244.$$

If you've done calculus before, this technique will be very familiar to you.

Here's a related theorem that should be intuitive.

Fact 2 (Infinite Roots) If a "degree n" polynomial has more than n roots, it must have infinite roots. Furthermore, the function must be 0.[a]

---
[a]"Degree n" is in quotations because it is not actually a degree n polynomial, but you would think of something like $a^2 - b^2 - (a+b)(a-b)$ as "degree 2" before simplifying to 0.

MAST

§4 Problems

Minimum is [40✐]. Problems with the ⬙ symbol are required.

> "Daru is like the universe—constantly expanding."
>
> Steins;Gate

[1✐] **Problem 1** (MATHCOUNTS 2020) What is the value of $\sqrt{111,111,111 \cdot 1,000,000,011 + 4}$?

[2✐] **Problem 2** Find $\frac{1999^3 - 1000^3 - 999^3}{1999 \cdot 1000 \cdot 999}$.

[2✐] **Problem 3** (PAMO 2003/3) Does there exists a base in which the numbers of the form:

$$10101, 101010101, 1010101010101, \cdots$$

are all prime numbers?

[2✐] **Problem 4** Find all constants r such that $a - r \mid ar^2 + ar - 17a + 15$.

[2✐] **Problem 5** (AIME 1985/3) Find c if a, b, and c are positive integers which satisfy $c = (a + bi)^3 - 107i$, where $i^2 = -1$.

[2⬙] **Problem 6 (AMC 10B 2020/22)** What is the remainder when $2^{202} + 202$ is divided by $2^{101} + 2^{51} + 1$?

[2✐] **Problem 7** (AHSME 1969/34) Find the remainder when x^{100} is divided by $x^2 - 3x + 2$.

[3✐] **Problem 8** (e-dchen Mock MATHCOUNTS) For any ordered pair of integers (a, b) such that $a, b \notin \{1, 2 \ldots 8\}$, $a \neq b$, and the remainder of

$$f(x) = (x - 1)(x - 2)(x - 3) \ldots (x - 8)$$

when divided by $x - a$ and $x - b$ are the same, find $a + b$.

[3✐] **Problem 9** (AIME 1991/1) Find $x^2 + y^2$ if x and y are positive integers such that

$$xy + x + y = 71$$

$$x^2 y + xy^2 = 880.$$

[3✐] **Problem 10** (AIME II 2011/5) The sum of the first 2011 terms of a geometric sequence is 200. The sum of the first 4022 terms is 380. Find the sum of the first 6033 terms.

[4✐] **Problem 11** (AIME I 2015/3) There is a prime number p such that $16p + 1$ is the cube of a positive integer. Find p.

[4✐] **Problem 12** (AIME 1987/14) Compute

$$\frac{(10^4 + 324)(22^4 + 324)(34^4 + 324)(46^4 + 324)(58^4 + 324)}{(4^4 + 324)(16^4 + 324)(28^4 + 324)(40^4 + 324)(52^4 + 324)}.$$

[4✐] **Problem 13** Consider cubic $p(x)$ such that $p(1) = 1, p(2) = 2, p(3) = 3, p(4) = 0$. Find $p(5)$.

[6⬙] **Problem 14 (JMC 10 2020/22)** What is the remainder of $17^7 + 17^2 + 1$ when divided by 307^2?

MAST

[9✎] **Problem 15** (AIME I 2013/5) The real root of the equation $8x^3 - 3x^2 - 3x - 1 = 0$ can be written in the form $\frac{\sqrt[3]{a} + \sqrt[3]{b} + 1}{c}$, where a, b, and c are positive integers. Find $a + b + c$.

[13✎] **Problem 16** (AIME 1988/13) Find a if a and b are integers such that $x^2 - x - 1$ is a factor of $ax^{17} + bx^{16} + 1$.

[13✎] **Problem 17** (AIME II 2000/13) The equation $2000x^6 + 100x^5 + 10x^3 + x - 2 = 0$ has exactly two real roots, one of which is $\frac{m + \sqrt{n}}{r}$, where m, n and r are integers, m and r are relatively prime, and $r > 0$. Find $m + n + r$.

MAST