



AIME HANDOUT

Polynomials in the AIME

Author:

NAMAN12

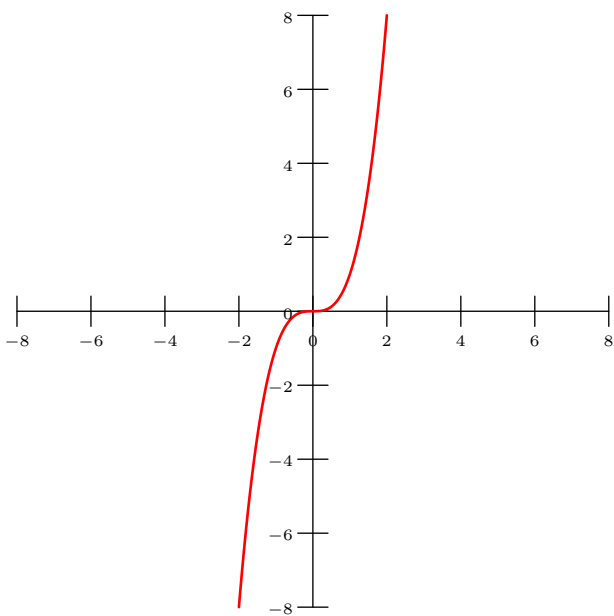
FREEMAN66

For:

AOPS

Date:

May 13, 2020



There will be a lot of this in the handout.

I had a polynomial once. My doctor removed it. - Michael Grant, "Gone"

Contents

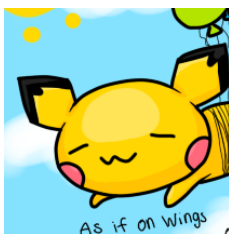
0	Acknowledgements	3
1	Introduction	4
2	Roots	4
3	Vietas	10
4	Symmetric Polynomials	13
5	Complex Numbers	16
5.1	Direct Applications to Polynomials	17
5.2	Polar Complex Numbers	19
6	A Small Bit Of Number Theory	23
7	Advanced Algebraic Manipulations	24
8	Worked Through Problems	28
9	Parting Words and Final Problems	32
10	Hints	36
A	Appendix A: Proof of Results	39
B	Appendix B: Polynomial Division	40
C	Appendix C: Real Roots	42
D	Appendix D: Lagrange Interpolation Formula	47
E	Appendix E: List of Theorems, Corollaries, and Definitions	49

§0 Acknowledgements

This was made for the Art of Problem Solving Community out there! We would like to thank Evan Chen for his `evan.sty` code. In addition, all problems in the handout were either copied from the Art of Problem Solving Wiki or made by ourselves. Finally, we would like to finally thank jsharmz for countless hours of proofreading and correcting us for all of our silly mistakes.



Art of Problem Solving Community - Specific shout out to members of **Professor-Mom's** Beginner AIME Forum and **FIREDRAGONMATH16's** Intermediate Algebra Forum



Evan Chen's Personal Sty File



Me! Say hi!



A friend of naman12's, who spent a lot of time to make sure we weren't making trivial mistakes.

And Evan says he would like this here for `evan.sty`:

Boost Software License - Version 1.0 - August 17th, 2003
 Copyright (c) 2020 Evan Chen [evan at evanchen.cc]
<https://web.evanchen.cc/> || github.com/vEnhance

He also helped us with the hint formatting. Evan is a \LaTeX god!
 And finally, please do not make any copies of this document without referencing this original one.

§1 Introduction

Problems in polynomials come in all different flavors. Approximately once a year (AIME I and AIME II), there is a polynomial problem. It's not like the problem is very trivial: here's the fish we are trying to chase:

Problem 1 (2016 AIME I Problem 11)

Let $P(x)$ be a nonzero polynomial such that $(x-1)P(x+1) = (x+2)P(x)$ for every real x , and $(P(2))^2 = P(3)$. Then $P(\frac{7}{2}) = \frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$.

This is definitely polynomial problem, and trying to solve it isn't exactly trivial, as seen after a few minutes of attempting this. Another problem is as follows:

Problem 2 (1984 AIME Problem 15)

Determine $w^2 + x^2 + y^2 + z^2$ if

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

Do you see a polynomial here? Well, technically yes, but not what we've normally seen. So how can we relate this to what we've seen before? We'll see in the following sections.

A word of advice for those who intend to follow this document: almost all problems are from the AIME; a few HMMT and USA(J)MO problems might be scattered in, but remember we go into a fair amount of depth here. The [Appendix A: Proof of Results](#) contains very technical results that are only included for completion, but don't need to be understood. [Appendix B: Polynomial Division](#) contains information on polynomial division that could be useful. [Appendix C: Real Roots](#) talks about some strategies used to find roots (not just rational)! Most of these start basic, but quickly jump to advanced techniques and uses.

And do you have questions, comments, concerns, issues, or suggestions? Here are two ways to contact me:

1. Send an email to realnaman12@gmail.com and I should get back to you (unless I am incorporating your suggestion into the document, when it might take a bit more time).
2. Send a private message to [naman12](#) by either clicking the button that says PM or by going [here](#) and clicking New Message and typing naman12.

Please include something related to **Polynomial AIME Handout** in the subject line so I know what you are talking about.

§2 Roots

We start this section with one of the most important theorems (arguably) in algebra:

Theorem 2.1 (Fundamental Theorem of Algebra)

Given a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ in $\mathbb{C}[x]$ (polynomials with complex number coefficients), there exists a root $r \in \mathbb{C}$ (aka $f(r) = 0$).

Remark 2.2. The proof is given at the end. Don't look at it unless you believe you can handle it!

Remark 2.3. n (the highest power x is raised to in $f(x)$) is called the degree of f and denoted as $\deg f$.

Exercise 2.4. Show that $\deg(f \cdot g) = \deg f + \deg g$ and $\deg(f + g) \leq \max(\deg f, \deg g)$. **This is an important exercise.** Hints: 27

Now, this looks pretty naive, but we can use polynomial division (see [Appendix B: Polynomial Division](#) for more details) repeatedly to get the following corollary:

Corollary 2.5 (Number of Roots Corollary)

Given a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ in $\mathbb{C}[x]$ (polynomials with complex number coefficients), there exists exactly n roots $r_1, r_2, \dots, r_n \in \mathbb{C}$ (aka $f(r_1) = f(r_2) = \cdots = f(r_n) = 0$).

Sketch of Proof. Induct on the degree of f , with $n = 1$ being trivial and use the [Fundamental Theorem of Algebra](#) to reduce it to the case of $n - 1$. □

Remark 2.6. Note that the roots need not be distinct. For example, the polynomial $x^2 - 2x + 1 = 0$ has roots 1, 1, which are the same.

This leads to the following corollary:

Corollary 2.7 (Zero Polynomial Corollary)

Given a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ in $\mathbb{C}[x]$ (polynomials with complex number coefficients), if there are $n + 1$ roots, then $f(x) = 0$.

Now, how does this help? It's really useful in the next problem.

Theorem 2.8 (Unique Factorization of Polynomials)

Any polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ can be expressed as $f(x) = a_n(x - r_1)(x - r_2) \cdots (x - r_n)$, where r_1, r_2, \dots, r_n are the roots of $f(x)$.

Proof. Assume that the roots of $f(x)$ were r_1, r_2, \dots, r_n (by [Number of Roots Corollary](#)), then we consider

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

Then, consider $f(x) - g(x)$. The terms of degree n cancel, so $\deg f - g$ is at most $n - 1$. However, r_1, r_2, \dots, r_n are roots of both f and g (the second because of the Zero Product Property). Thus, we get that $f - g$ has n roots, so by [Zero Polynomial Corollary](#), $f(x) - g(x) = 0$, so $f(x) = g(x)$. □

Remark 2.9. For those of you who know what a UFD is, this is proving that $\mathbb{C}[x]$ is a UFD. We haven't shown it is a domain yet, but the underlying idea is this.

Thus, we get that for all roots r of $f(x)$, $x - r$ is a factor of $f(x)$ by the unique factorization of polynomials. Thus, we get this useful theorem by using the fact $f(r) = 0$ for all roots:

Theorem 2.10 (Factor Theorem)

$x - r$ is a factor of $f(x)$ if and only if $f(r) = 0$.

This leads to the following generalization (proved in [Appendix B: Polynomial Division](#)):

Theorem 2.11 (Remainder Theorem)

$f(k)$ is the remainder when $f(x)$ is divided by $x - k$.

The factor theorem is a special case by taking r as a root, so $f(r) = 0$, and so as the remainder is 0, it is divisible by $x - r$. This doesn't exactly relate to roots, but is still helpful. Let's see an example in action:

Example 2.12 (AMC 12A 2017/23)

For certain real numbers a , b , and c , the polynomial

$$g(x) = x^3 + ax^2 + x + 10$$

has three distinct roots, and each root of $g(x)$ is also a root of the polynomial

$$f(x) = x^4 + x^3 + bx^2 + 100x + c.$$

What is $f(1)$?

Solution. Let's see how to approach this. We get by the [Factor Theorem](#), $g(x) = (x - a)(x - b)(x - c)$ (as there can not be any more roots by [Zero Polynomial Corollary](#)), and $f(x)$ is divisible by $x - a, x - b, x - c$. Thus, $f(x)$ is divisible by their product, and in particular,

$$f(x) = g(x)h(x)$$

for some other polynomial $h(x)$. So now, we need to find $f(1)$, which seems pretty daunting. However, we can try to extract more information from $h(x)$. What's the degree? Well, we have that if the degree of $h(x)$ is d , then $g(x)$ has 3 roots and $h(x)$ has d roots, so then $f(x)$ has $3 + d$ roots. But we know $f(x)$ has degree 4, so $3 + d = 4$! Thus, we can write $h(x) = x + r$ for some unknown root. Then, we get that

$$x^4 + x^3 + bx^2 + 100x + c = (x^3 + ax^2 + x + 10)(x + r)$$

Thus, we get that

$$x^4 + x^3 + bx^2 + 100x + c - (x^3 + ax^2 + x + 10)(x + r) = 0 \tag{*}$$

Looking at the coefficient of x^3 , we get

$$1 - (a + r) = 0$$

or $a + r = 1$. Now, looking at the coefficient of x in the expansion of (*), we get

$$100 - (10 + r) = 0$$

so $r = 90$. Then, we get that $a = -89$. Now, we know $g(x) = x^3 - 89x^2 + x + 10$. Do we use that to find roots? Well, we have no good way. Let's try our idea of computing coefficients in (*); the coefficient of x^2 is

$$b - (ar + 1) = 0$$

We know $ar + 1$...but isn't that a bit big?

Remark 2.13. When the problem gets too big, try to take a step back and look at it from a different perspective. Most of the time, if you have some substantial progress, start to work backwards.

We need to find $f(1)$. That's the same as $g(1)h(1)$. Do we know $g(1)$? Well, we get

$$g(1) = 1 + a + 1 + 10 = 1 - 89 + 1 + 10 = -77,$$

$$h(1) = 1 + r = 1 + 90 = 91,$$

so

$$f(1) = g(1)h(1) = -77 \cdot 91 = \boxed{-7007}.$$

□

Remark 2.14. A question that may arise: how did we know that $h(x)$ was in the form of $x + r$ and not $2(x + r)$? The answer is once again to use (*) and the fact that if the coefficient of x^4 (leading term) was k , then $1 - k = 0$, so $k = 1$. This is a small detail I glossed over; make sure you understand why this is valid.

Remark 2.15. So what if we didn't notice that $f(1) = g(1)h(1)$? We can still find b and c , right? We can compute

$$b = ar + 1 = -89 \cdot 90 + 1 = -8009$$

and similarly $c = 10r = 900$. Thus, we can plug it in to get

$$f(1) = 1 + 1 - 8009 + 100 + 900 = -7007$$

as well.

So our first remark showed us an important point - polynomials can have the exact same set of roots because of the leading coefficient can vary while the roots are the same - something I talked above in the first remark. For example, we can take $f(x) = (x - 1)(x - 2)$ and $g(x) = 2(x - 1)(x - 2)$, which are obviously not the same polynomial, but the roots of both are 1, 2. Make sure you don't forget this!

Our first problem - solved. And don't think it's easy - it is one of the harder problems on an AMC 12. I'll leave you with a few exercises:

Exercise 2.16 (2018 AIME I Problem 1). Let S be the number of ordered pairs of integers (a, b) with $1 \leq a \leq 100$ and $b \geq 0$ such that the polynomial $x^2 + ax + b$ can be factored into the product of two (not necessarily distinct) linear factors with integer coefficients. Find the remainder when S is divided by 1000.

Hints: 71

Exercise 2.17 (2007 AIME I Problem 8). The polynomial $P(x)$ is cubic. What is the largest value of k for which the polynomials $Q_1(x) = x^2 + (k - 29)x - k$ and $Q_2(x) = 2x^2 + (2k - 43)x + k$ are both factors of $P(x)$? Hints: 57

Exercise 2.18. Let N be the number of complex numbers^a z with the properties that $|z| = 1$ and $z^{6!} - z^{5!}$ is a real number. Find the remainder when N is divided by 1000. Hints: 50

^aSee [Complex Numbers](#) for more information. The only pieces of information you will need: z is a root if and only if \bar{z} is needed, and for $z\bar{z} = |z|^2$.

Now, let's look at a theorem that is very useful when dealing with polynomials:

Theorem 2.19 (Rational Root Theorem)

Given a polynomial $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ with integral coefficients, $a_n \neq 0$. The Rational Root Theorem states that if $P(x)$ has a rational^a root $r = \pm \frac{p}{q}$ with p, q relatively prime positive integers, p is a divisor of a_0 and q is a divisor of a_n .

^aA number that can be expressed as $\frac{p}{q}$ for integers p and q . Typically, we deal with rational numbers **in lowest terms**, which just means $\gcd(p, q) = 1$.

Sketch of Proof. Plug it in and multiply by q^n . Rearranging and factoring gives $-a_0 q^n = p(a_1 q^{n-1} + a_2 p q^{n-2} + \dots + a_n p^{n-1})$. The left hand side is an integer and so is the second part of the right hand side, so we get $p \mid a_0 q^n$. Because p and q are relatively prime, $p \mid a_0$. A similar result follows by isolating the term $-a_n p^n$ for $q \mid a_n$. \square

But what does this mean? Well, we can find all rational roots as follows¹: take the leading coefficient (say a) and take the constant term (or the last term) (say b). Then, we get that if $\frac{p}{q}$ is a root, p has to divide b and q has to divide a . This helps a lot as it gives an algorithm to give a (possibly long) list of solutions (that are rational). Let's look at this example:

Example 2.20 (naman12)

Find all rational roots of $6x^3 + x^2 - 19x + 6$.

Solution. [Walkthrough] I'll only explain a walkthrough on how to solve this:

- Write all factors of our leading coefficient (positive and negative).
- Write all factors of our constant term.
- Consider the following: do we need to write all negative factors for part (b)?
- Consider all roots. Try to find them.

\square

¹Keep a watch; not all roots are rational - they can also be irrational or complex. In addition, not all of these roots are definitely roots of the polynomial - they are all possible roots.

Doing the rational root theorem is pretty tedious, so we can use this with polynomial division in [Appendix B: Polynomial Division](#). For now, let us proceed with the following AIME problem:

Example 2.21 (AIME I 2011/9)

Suppose x is in the interval $[0, \pi/2]$ and $\log_{24 \sin x}(24 \cos x) = \frac{3}{2}$. Find $24 \cot^2 x$.

Solution. At first look, where are the polynomials? We'll need to manipulate our original condition. We can exponentiate to get

$$24 \cos x = (24 \sin x)^{3/2}$$

Squaring, we get

$$(24 \sin x)^3 = (24 \cos x)^2$$

Now what? Well, we know from trigonometry² $\sin^2 x + \cos^2 x = 1$, so we can substitute to get

$$(24 \sqrt{1 - \sin^2 x})^2 = (24 \sin x)^3$$

so expanding and dividing by 24^2 , we get

$$1 - \sin^2 x = 24 \sin^3 x$$

Now, take $y = \sin x$, then we get

$$1 - y^2 = 24y^3$$

Rearranging, we get

$$24y^3 + y^2 - 1 = 0$$

Here's where the [Rational Root Theorem](#) comes in handy: we use it and check that $y = \frac{1}{3}$ is a root. Now, this means that $y - \frac{1}{3}$ is a factor. However, this is not very nice - however we can multiply by 3 (see my earlier remark on leading coefficients) to rid of fraction to get $3y - 1$ divides our previous polynomial, so $\sin x$ satisfies

$$(3y - 1)(8y^2 + 3y + 1) = 24y^3 + y^2 - 1 = 0$$

But the quadratic factor has no real roots³! So $y = \sin x = \frac{1}{3}$. And then, we get because $\cos^2 x + \sin^2 x = 1$ (the standard Pythagorean identity) and $\cos x > 0$, $\cos x = \frac{2\sqrt{2}}{3}$. This gives $\cot x = \frac{\cos x}{\sin x} = \sqrt{8}$, so our answer is $24 \cot^2 x = 24 \cdot (\sqrt{8})^2 = 24 \cdot 8 = \boxed{192}$. □

Remark 2.22. Even if a problem doesn't have a polynomial, it's possible that it was intended to be a polynomial problem.

Let's cap it off with a few exercises:

Exercise 2.23 (2018 AIME II Problem 6). A real number a is chosen randomly and uniformly from the interval $[-20, 18]$. The probability that the roots of the polynomial $x^4 + 2ax^3 + (2a - 2)x^2 + (-4a + 3)x - 2$ are all real can be written in the form $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$.

Hints: 47

Exercise 2.24 (1988 Canadian Mathematical Olympiad Problem 1). For what real values of k do $1988x^2 + kx + 8891$ and $8891x^2 + kx + 1988$ have a common zero? **Hints:** 35

²See the trigonometry handout for more information.

³This can be checked by taking the discriminant of the quadratic. In general, for a quadratic $ax^2 + bx + c$, if it has (any) real roots, we can use the quadratic formula to get that the term $\sqrt{b^2 - 4ac}$ has to indeed be a real number, so $b^2 - 4ac \geq 0$ and $b^2 \geq 4ac$. In this problem, taking $a = 8$, $b = 3$, and $c = 1$. $3^2 = 9 \leq 32 = 4 \cdot 8$, so there are no real roots.

§3 Vietas

Vieta's Formulas are a set of formulas that relate the roots of a polynomial to the coefficients of the polynomial. Call the symmetric sum of the numbers k_1, k_2, \dots, k_m taking p at a time as⁴

$$\sigma_p = \sum_{1 \leq a_1 < a_2 < \dots < a_p \leq m} k_{a_1} k_{a_2} \dots k_{a_p}$$

Isn't this complicated?

Remark 3.1. Don't let fancy notation scare you! It normally is easier if you break the given equation down.

a_1, a_2, \dots, a_r , what do they mean? Well, as this is a handout, I have⁵ to include the formal definition of everything - which can get a bit tedious, and a bit of an eyesore. However, we can take a look at this.

Example 3.2

Find the symmetric sum of just one number k taking one at a time.

Solution. Isn't this just k ? Think about it. If we are choosing numbers $1 \leq a_1 \leq 1$, we **have** to have $a_1 = 1$. Easily, this means that $\sigma_1 = k$. \square

Looking at the footnote above, there isn't much else to do for one number. Let's take two numbers:

Example 3.3

Find the symmetric sum of just two numbers k_1, k_2 taking one and two at a time.

Solution. Well, let's first tackle taking them one at a time. Well, we get that $1 \leq a_1 \leq 2$, so we have two choices: $a_1 = 1$ or $a_2 = 2$. So $\sigma_1 = k_1 + k_2$.

Now, if we're taking two at a time, we get that $1 \leq a_1 < a_2 \leq 2$, so $a_1 = 1$ and $a_2 = 2$. Thus, $\sigma_2 = k_1 k_2$. \square

Exercise 3.4. Can you find what the symmetric sum of three numbers k_1, k_2, k_3 are taking one, two, and three at a time? **Hints:** 67

Exercise 3.5. Try expanding $(x - k_1)$, $(x - k_1)(x - k_2)$, and $(x - k_1)(x - k_2)(x - k_3)$. Do the results seem familiar? **Hints:** 26

Exercise 3.6. Can you generalize what σ_n is for n variables? **Hints:** 61

Now, we look at the following theorem that showcases the main idea of this section.

⁴Technically, we define alternative values for $p > m$ and $p \leq 0$. See [Newton's Formulas](#) (just the statement of the theorem) for more details.

⁵Well, not **have**, but **should**, at some point.

Theorem 3.7 (Vieta's Formulas)

Suppose that the roots to $f(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_0$ are r_1, r_2, \dots, r_n . Then, we get that if σ_k is the symmetric sum taking the r_i k at a time, then

$$\sigma_k = (-1)^k \frac{c_{n-k}}{c_n}$$

Sketch of Proof. Just take the expansion of $f(x)$ as $c_n(x - r_1)(x - r_2) \dots (x - r_n)$. We choose c_n so that the leading coefficients of $f(x)$ (in the expanded form and factored form) match. To find σ_k , look at the coefficient of x^{n-k} . On one hand, in the expanded form, it's obviously c_{n-k} . However, now consider how many x 's you will need from $(x - r_1)(x - r_2) \dots (x - r_n)$ in the factored form. Then, see how many $-r_j$'s you can choose, as these will be from the factors we didn't choose an x from. Show that this sum is just $(-1)^k c_0 \sigma_k$. \square

Now, how do these help? Let's look at an application:

Example 3.8 (AIME I 2001/3)

Find the sum of the roots, real and non-real, of the equation $x^{2001} + \left(\frac{1}{2} - x\right)^{2001} = 0$, given that there are no multiple roots.

Solution. Well, let's see what happens if we try to pseudo-expand it. But first we need the following well-known theorem:

Theorem 3.9 (Binomial Theorem)

$$(x + y)^n = x^n + \binom{n}{1} x^{n-1} y + \dots + \binom{n}{n-1} x y^{n-1} + y^n$$

Equipped with this, we get that

$$x^{2001} + \left(\frac{1}{2} - x\right)^{2001} = x^{2001} - x^{2001} + \binom{2001}{1} \cdot \frac{1}{2} x^{2000} - \binom{2001}{2} \left(\frac{1}{2}\right)^2 x^{1999} + \dots$$

What's important are the first and second nonzero terms - from these, we can use Vieta's ($k = 1$, which is also the sum of the roots) to get the sum of the roots is

$$\frac{\binom{2001}{2} \left(\frac{1}{2}\right)^2}{\binom{2001}{1} \cdot \frac{1}{2}} = \frac{2000}{4} = \boxed{500}.$$

\square

That's a simple answer. Is there another way to get this answer? Here is a hint: note that if x is a root, so is $\frac{1}{2} - x$. I leave the rest as an exercise:

Exercise 3.10 (AIME I 2001/3). Solve [AIME I 2001/3](#) with the above method. **Hints:** 16

Exercise 3.11. Prove [Binomial Theorem](#). **Hints:** 13

Exercise 3.12 (2014 AIME I Problem 5). Real numbers r and s are roots of $p(x) = x^3 + ax + b$, and $r + 4$ and $s - 3$ are roots of $q(x) = x^3 + ax + b + 240$. Find the sum of all possible values of $|b|$. **Hints:** 31

Let's see another example:

Example 3.13 (AIME 1996/5)

Suppose that the roots of $x^3 + 3x^2 + 4x - 11 = 0$ are a , b , and c , and that the roots of $x^3 + rx^2 + sx + t = 0$ are $a + b$, $b + c$, and $c + a$. Find t .

Solution. Now, at first, this looks daunting. But let's write down what we know and what we want to find. We have by Vieta's that

$$a + b + c = -3$$

$$ab + bc + ac = 4$$

$$abc = 11$$

and we want to find

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

That doesn't look too nice, right? In the next section, we'll see how to deal with this. However, we can try something else. Let's look at each of our terms in $(a + b)(b + c)(c + a)$. We know $a + b + c = -3$, so $a + b = -3 - c$. That's pretty nice. We can then rewrite t (after cancelling out negative signs) as:

$$t = (3 + c)(3 + b)(3 + a)$$

which expands to

$$t = 27 + 9(a + b + c) + 3(ab + bc + ac) + abc = \boxed{23}.$$

Now, that looks a lot like something we've seen before - 27, 9, 3, and 1. So let's see if there is a shorter way to get this solution. We get that

$$t = -(-3 - c)(-3 - b)(-3 - a)$$

Let's replace -3 with k , to make it look more symmetric. We get

$$t = -(k - a)(k - b)(k - c)$$

Wait. By [Factor Theorem](#), we have $k^3 + 3k^2 + 4k - 11 = f(k) = (k - a)(k - b)(k - c)$. That's interesting. We get

$$t = -f(k) = -f(-3) = \boxed{23}.$$

□

So there does exist a nice solution! This shows that there typically is a nice solution to most AIME Problems.

Exercise 3.14 (2005 AIME I Problem 8). The equation $2^{333x-2} + 2^{111x+2} = 2^{222x+1} + 1$ has three real roots. Given that their sum is $\frac{m}{n}$ where m and n are relatively prime positive integers, find $m + n$. **Hints:** [44](#)

Exercise 3.15 (1993 AIME Problem 5). Let $P_0(x) = x^3 + 313x^2 - 77x - 8$. For integers $n \geq 1$, define $P_n(x) = P_{n-1}(x - n)$. What is the coefficient of x in $P_{20}(x)$? **Hints:** [60](#)

Exercise 3.16 (2008 AIME II Problem 7). Let r , s , and t be the three roots of the equation

$$8x^3 + 1001x + 2008 = 0.$$

Find $(r + s)^3 + (s + t)^3 + (t + r)^3$. **Hints:** [17](#)

§4 Symmetric Polynomials

We actually are going to go expand something from last section. Remember [Vieta's Formulas](#)? Turns out, we are going to use the same notation for σ_k .

Definition 4.1 (Elementary Symmetric Polynomial) — An **elementary symmetric polynomial** is any multivariate (in more than one variable, like x_1, x_2, \dots) polynomial defined as taking the sum of x_1, x_2, \dots, x_n k at a time - basically σ_k .

Furthermore, we have the following definition

Definition 4.2 (k -Variable Symmetric Polynomial) — A **symmetric polynomial** in k variables is basically a polynomial when switching any two of the variables leaves the polynomial unchanged. For example, in $x + y + z - xyz$, switching any two of x, y, z don't change the polynomial. However, in $x + y + z - x^2z$, switching x and y changes the polynomial to $x + y + z - y^2z$.

Now, this leads to the following powerful theorem:

Theorem 4.3 (Fundamental Theorem of Symmetric Polynomials)

Any symmetric polynomial can be expressed as the sum/product of multiple (not necessarily different) symmetric polynomials.

For example, try this exercise:

Exercise 4.4. Show that $x_1^2 + x_2^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$. **Hints:** 40

Now, the proof is once again given in the appendix. But this doesn't tell us much - as an analogy, the theorem tells us there is another planet outside of Earth, but not how to find it⁶, where to find it, and anything about it. Now, that does make sense. There are basically infinitely many symmetric polynomials - we can't have all of them. But, there are quite a few that appear very frequently, and these are given in the following relation:

Theorem 4.5 (Newton's Formulas)

Let ρ_k be $x_1^k + x_2^k + \dots + x_n^k$. Then, we get

$$k\sigma_k + \sum_{j=1}^k (-1)^j \sigma_{k-j} \rho_j = 0$$

where we define for $j > n$ and $j < 0$ $\sigma_j = 0$ and for $j = 0$ $\sigma_j = 1$.

Proof. We can write this as the sum/product of a bunch of symmetric polynomials as guaranteed by the [Fundamental Theorem of Symmetric Polynomials](#). Suppose that x_1, x_2, \dots, x_n were the roots of $P(x)$. We use [Vieta's Formulas](#) to get

$$P(x) = \sum_{k=0}^n (-1)^k \sigma_k x^n$$

Now, We have the following claim:

⁶The clever Mr. Quines pointed out that the proof **does** give a greedy algorithm to find it, so more fun to the reader!

Claim 4.6 — [Newton's Formulas](#) is true for $n = k$.

Proof. Just add up all terms in the form

$$P(x_i) = \sum_{j=0}^n (-1)^j \sigma_{k-j} x_i^j = 0$$

which finishes off the proof. ■

For $k > n$, the result follows by considering the polynomial

$$P(x)x^{n-k}$$

and applying Claim 2.5 (as the zeroes contribute nothing). Now, to prove the other side, we just consider

$$g(x) = a_n x^k + a_{n-1} x^{k-1} + \cdots + a_{n-k}$$

where $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. From this, we can use the Claim on $g(x)$. □

This is the slickest proof I actually know. It's pretty short. Let's see if you got a hang of this:

Exercise 4.7. Find ρ_1, ρ_2, ρ_3 , only in terms of $\sigma_1, \sigma_2, \sigma_3$ (no ρ_1, ρ_2, ρ_3). Compare your answer for ρ_2 to your answer to [Exercise 4.4](#). **Hints:** 43

Where do these come up in the AIME? Correction: where do these not come up in the AIME? Let's look at the following example:

Example 4.8 (AIME 1983/5)

Suppose that the sum of the squares of two complex numbers x and y is 7 and the sum of the cubes is 10. What is the largest real value that $x + y$ can have?

Solution. Now, we will use the result of [Exercise 4.7](#). We get that

$$7 = \rho_2 = \sigma_1^2 - 2\sigma_2$$

$$10 = \rho_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = \sigma_1^3 - 3\sigma_1\sigma_2$$

Oh look! It wants us to find σ_1 ! We can get from the first equation

$$\sigma_2 = \frac{\sigma_1^2 - 7}{2}$$

so substituting this into the second equation, we get

$$10 = \sigma_1^3 - 3\sigma_1 \left(\frac{\sigma_1^2 - 7}{2} \right) = \frac{-\sigma_1^3 + 21\sigma_1^2}{2}$$

so $\sigma_1^3 - 21\sigma_1^2 + 20 = 0$. Using the [Rational Root Theorem](#), we get that the solutions are $\sigma_1 = 1, 4, -5$, so the maximum value is 4. □

Exercise 4.9. Find the values of σ_2 for each value of [AIME 1983/5](#). Are you glad we didn't find the values of x and y ? **Hints:** [39](#)

Exercise 4.10 (2019 AIME I Problem 8). Let x be a real number such that $\sin^{10} x + \cos^{10} x = \frac{11}{36}$. Then $\sin^{12} x + \cos^{12} x = \frac{m}{n}$ where m and n are relatively prime positive integers. Find $m + n$. **Hints:** [80](#)

Let's take a look at another example:

Example 4.11 (AIME II 2003/9)

Consider the polynomials $P(x) = x^6 - x^5 - x^3 - x^2 - x$ and $Q(x) = x^4 - x^3 - x^2 - 1$. Given that z_1, z_2, z_3 , and z_4 are the roots of $Q(x) = 0$, find $P(z_1) + P(z_2) + P(z_3) + P(z_4)$.

Solution. Although this is Newton's Sums, we don't bash. So, we note that we need to find

$$\rho_6 - \rho_5 - \rho_3 - \rho_2 - \rho_1$$

Now, we can use our knowledge of Newton's Sums. We get from [Newton's Formulas](#),

$$\rho_6 - \rho_5 - \rho_4 - \rho_2 = 0$$

so thus, we can reduce what we want to find (by subtracting the equations) to

$$\rho_4 - \rho_3 - \rho_1$$

Similarly from [Newton's Formulas](#), we get

$$\rho_4 - \rho_3 - \rho_2 - 4 = 0$$

so we need to find

$$\rho_2 - \rho_1 + 4$$

Now, we note that

$$\rho_1 = \sigma_1 = 1$$

and

$$\rho_2 = \sigma_1^2 - 2\sigma_2 = 1^2 - 2(-1) = 3$$

Thus, our desired answer is

$$\rho_2 - \rho_1 + 4 = \boxed{6}$$

So don't rip in blindly, make manipulations and then finish off the problem with little computation. □

Exercise 4.12 (2015 AIME II Problem 14). Let x and y be real numbers satisfying $x^4y^5 + y^4x^5 = 810$ and $x^3y^6 + y^3x^6 = 945$. Evaluate $2x^3 + (xy)^3 + 2y^3$. **Hints:** [10](#)

Exercise 4.13 (1973 USAMO Problem 4). Determine all the roots, real or complex, of the system of simultaneous equations

$$x + y + z = 3$$

$$x^2 + y^2 + z^2 = 3$$

$$x^3 + y^3 + z^3 = 3$$

Hints: [1](#)

I know the last one *is technically* a USAMO problem, but it's easier than the other AIME Problem. Finally, I would like to write down four commonly seen factorizations (last one due to AoPS user dchenmathcounts, and is known as the **Sophie Germain Identity**):

$$\begin{aligned}(a + b + c)(ab + bc + ac) - abc &= (a + b)(b + c)(a + c) \\ (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ac) &= a^3 + b^3 + c^3 - 3abc \\ (b^2 + b + 1)(b^2 - b + 1) &= b^4 + b^2 + 1 \\ a^4 + 4b^4 &= (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)\end{aligned}$$

§5 Complex Numbers

So, what happens if we try to do

$$\sqrt{-1}$$

We shall define the two solutions to this $\pm i$. We also note that⁷

$$x = \sqrt{-1} \iff x^2 = -1 \iff x^2 + 1 = 0$$

so thus we can “factor” by using difference of squares:

$$x^2 + 1 = (x - i)(x + i)$$

i is called the imaginary unit. What happens if we add a real number and an imaginary unit (like $5i$)? Well, this gets to

$$z = a + bi$$

But what do we call it? We call it the following:

Definition 5.1 (Complex Number) — A **complex number** $z = a + bi$ (for real a and b) is the sum of a real number and imaginary number.

Note that all real numbers and pure imaginary numbers are also complex. Now, what happens when we add? We consider

$$z = a + bi, w = c + di$$

Then, we get

$$z + w = (a + bi) + (c + di) = a + (c + di) + bi = (a + c) + (di + bi) = (a + c) + (b + d)i$$

where we used the associativity of addition (we add the imaginary and real numbers separately). What about multiplication? It's slightly different (using the distributive property):

$$(a + bi)(c + di) = a(c + di) + bi(c + di) = ac + adi + bci + bdi^2 = ac + adi + bci - bd = (ac - bd) + (ad + bc)i$$

Note we brought our answer in the form $x + yi$, which is pretty normal to do. Similarly, we can define division and subtraction. Now, we come to one of the most important definitions:

Definition 5.2 (Conjugate) — The **conjugate** of the complex number $z = a + bi$ is denoted as \bar{z} and has value $a - bi$.

Let's try the following:

⁷ \iff means that the first statement is true if and only if the second statement is true.

Example 5.3

Suppose $z = a + bi$. Find $z\bar{z}$.

Solution. We have that

$$(a + bi)(a - bi) = a^2 + abi - abi - b^2i^2 = a^2 + b^2$$

□

Note this gives a very easy way to divide. We get that as

$$(a + bi)(a - bi) = (a + bi)(\overline{a + bi}) = a^2 + b^2$$

we have

$$\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$$

Also try to verify the following:

Exercise 5.4 (Conjugate Addition). $\bar{z} + \bar{w} = \overline{z + w}$ **Hints:** 62

Exercise 5.5 (Conjugate Multiplication). $\bar{z} \cdot \bar{w} = \overline{z \cdot w}$ **Hints:** 28

Exercise 5.6. Prove that $\overline{z^n} = \bar{z}^n$. **Hints:** 54se [Conjugate Multiplication](#) (a.k.a the previous exercise).

Exercise 5.7. $\bar{\bar{z}} = z$. **Hints:** 33

Exercise 5.8. $f(\bar{z}) = \bar{z}$. **Hints:** 48

Now, what happens when we imagine plotting complex numbers on a plane? We can do that and indeed define this plane as the **Argand Plane**, while the one in which we plot (x, y) is the Cartesian Plane. These planes are essentially identical except for one key caveat - the Cartesian Plane plots x versus y while the Argand Plane plots $\text{Re}(z)$ versus $\text{Im}(z)$. We can define the following:

Definition 5.9 (Modulus/Magnitude) — The **modulus** or **magnitude** of a complex number z is denoted as $|z|$ and is the distance from z to the origin, which is 0, in the complex plane.

Remark 5.10. This can be seen (by the Pythagorean Theorem) as $\sqrt{a^2 + b^2}$, where z can be put in the Cartesian Plane as (a, b) .

We thus see that by [our last example](#), we get that $z\bar{z} = |z|^2$.

Exercise 5.11. Show that $|z||w| = |zw|$. **Hints:** 34

Exercise 5.12 (Real Number Conjugate). Consider a real number r . Then $r = \bar{r}$. **Hints:** 20

§5.1 Direct Applications to Polynomials

We have the following beautiful result:

Theorem 5.13 (Complex Conjugate Theorem)

z is a root of a polynomial with real coefficients if and only if \bar{z} is.

Proof. Take a polynomial $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ such that z is a root. Then, we get this means

$$0 = P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0$$

Now, what can we do? Well, one thing we can do is to take the conjugate. We get

$$0 = \bar{0} = \overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0}$$

Now, we can use [Conjugate Addition](#) to get

$$0 = \overline{a_n z^n} + \overline{a_{n-1} z^{n-1}} + \cdots + \overline{a_0}$$

Now, we can use [Conjugate Multiplication](#) to get

$$0 = \overline{a_n}(\bar{z})^n + \overline{a_{n-1}}(\bar{z})^{n-1} + \cdots + \overline{a_0}$$

Finally, as a_0, a_1, \dots, a_n are real numbers, we can use [Real Number Conjugate](#) to get

$$0 = a_n(\bar{z})^n + a_{n-1}(\bar{z})^{n-1} + \cdots + a_0 = P(\bar{z})$$

so \bar{z} is a root. The “if” part can be resolved as $\bar{\bar{z}} = z$. □

Let’s see an application:

Example 5.14 (AIME 1995/5)

For certain real values of a, b, c , and d , the equation $x^4 + ax^3 + bx^2 + cx + d = 0$ has four non-real roots. The product of two of these roots is $13 + i$ and the sum of the other two roots is $3 + 4i$, where $i = \sqrt{-1}$. Find b .

Solution. We call the roots $w = p + qi, \bar{w} = p - qi, z = r + si, \bar{z} = r - si$.

Remark 5.15. z and w are commonly used for complex numbers (as opposed to x and y , which are for real variables).

We note that

$$w + \bar{w} = 2p$$

is a real number, and so is $z + \bar{z}$. Thus, we get that either $w + z$ or $w + \bar{z} = 3 + 4i$. By symmetry, it doesn’t matter, so we assume $w + z = 3 + 4i$. Then, we get

$$\overline{w + z} = \bar{w} + \bar{z} = 3 - 4i.$$

In addition, we get

$$\bar{w} \cdot \bar{z} = 13 + i,$$

so thus it’s conjugate is

$$wz = w \cdot z = 13 - i.$$

Now, let’s look at what we want to find. By Vieta’s, we know that

$$b = zw + z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} + \bar{w}\bar{z} = 26 + (z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w})$$

But how to finish? We know $z + w$, so let’s see if we can factor the last term. Aha!

$$z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} = (z + w)(\bar{z} + \bar{w}) = (3 + 4i)(3 - 4i) = |3 + 4i|^2 = 3^2 + 4^2 = 25$$

So we finish by getting

$$b = 26 + 25 = \boxed{51}.$$

□

So the [Complex Conjugate Theorem](#) is actually pretty helpful.

Exercise 5.16 (2013 AIME I Problem 13). There are nonzero integers a , b , r , and s such that the complex number $r + si$ is a zero of the polynomial $P(x) = x^3 - ax^2 + bx - 65$. For each possible combination of a and b , let $p_{a,b}$ be the sum of the zeros of $P(x)$. Find the sum of the $p_{a,b}$'s for all possible combinations of a and b . **Hints:** 14

Exercise 5.17 (2013 AIME II Problem 12). Let S be the set of all polynomials of the form $z^3 + az^2 + bz + c$, where a , b , and c are integers. Find the number of polynomials in S such that each of its roots z satisfies either $|z| = 20$ or $|z| = 13$. **Hints:** 51

§5.2 Polar Complex Numbers

Imagine standing at the origin of the Cartesian Plane. If I gave you a direction and asked you to walk 5 steps, it might be difficult to write the point that I end up at without Trigonometry. Instead, we have made a system to do exactly this! It is called the Polar Coordinate system. Polar numbers (technically coordinates) are numbers in the form of (r, θ) , where r is a real number and θ is an angle (in radians). Typically, we try to use polar coordinates as an alternative to the standard rectangular coordinates (on the cartesian plane), and we can do the same thing here.

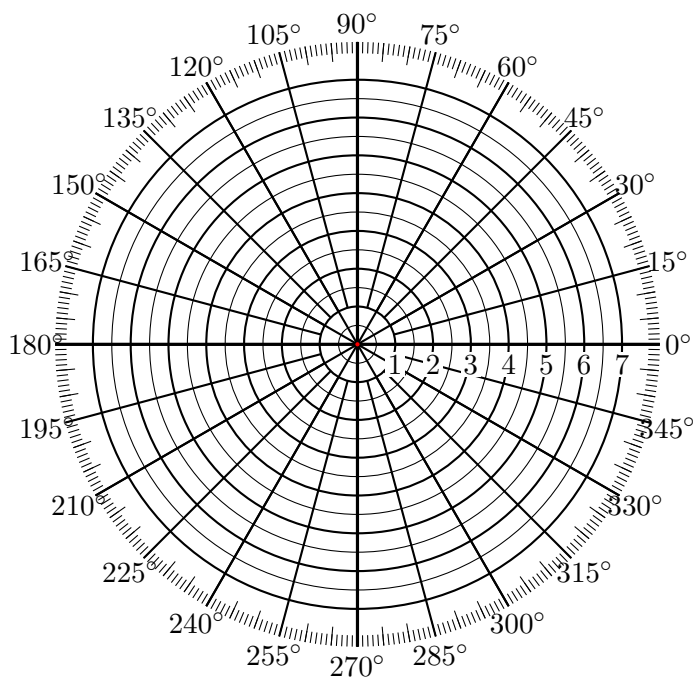


Figure 1: The Polar Coordinate Plane.

We note that we can scale a complex number to another complex number with magnitude 1 (by dividing by $|z|$). Then, we get that if

$$z = a + bi, a^2 + b^2 = 1,$$

we can substitute $(a, b) = (\cos \theta, \sin \theta)$. Thus,

$$\frac{z}{|z|} = \frac{z}{r} = \cos \theta + i \sin \theta$$

so we can scale up to get

$$z = r(\cos \theta + i \sin \theta)$$

This is the polar form of a complex numbers (while previously we had the rectangular form $a + bi$). From this eloquent form, we have the following formula:

Theorem 5.18 (De Moivre's Theorem)

$$\cos n\theta + i \sin n\theta = (\cos \theta + i \sin \theta)^n$$

Sketch of Proof. We can induct on n . When $n = 1$, the result is immediate. Otherwise, we have

$$\cos n\theta + i \sin n\theta = \cos((n-1)\theta + \theta) + i \sin((n-1)\theta + \theta)$$

Using our addition formulas⁸, we get $\cos n\theta + i \sin n\theta$ is equal to

$$\cos((n-1)\theta) \cos \theta - \sin((n-1)\theta) \sin \theta + i(\sin((n-1)\theta) \cos \theta + \cos((n-1)\theta) \sin \theta)$$

However, we also have

$$(\cos \theta + i \sin \theta)^n = (\cos \theta + i \sin \theta)^{n-1}(\cos \theta + i \sin \theta) = (\cos(n-1)\theta + i \sin(n-1)\theta)(\cos \theta + i \sin \theta)$$

Expanding and simplifying should give these are equal. □

Euler used this theorem to prove the following result:

Theorem 5.19 (Euler's Formula)

$$e^{i\theta} = \cos \theta + i \sin \theta$$

This is considered one of the most beautiful results in mathematics, especially when $\theta = \pi$.

Remark 5.20. Actually, we “define” $i = (1, \frac{\pi}{2})$ (as if we were plotting on a complex plane), but this is completely arbitrary, as we could have chosen $i = (1, \frac{3\pi}{2})$. This doesn't matter too much, but it is pretty important in the terms of complex numbers. It simplifies numbers a lot.

This theorem helps a lot. We can take another look at the proof of [De Moivre's Theorem](#) using [Euler's Formula](#):

Theorem 5.21 (De Moivre's Theorem)

$$\cos n\theta + i \sin n\theta = (\cos \theta + i \sin \theta)^n$$

Sketch of Proof. We use Euler's formula to get

$$\cos n\theta + i \sin n\theta = e^{in\theta} = (e^{i\theta})^n = (\cos \theta + i \sin \theta)^n$$

from [Euler's Formula](#). □

Now, try the following exercise:

⁸See the trigonometry handout.

Exercise 5.22. What is $e^{2\pi i}$? What about $e^{\pi i}$? **Hints:** 78

Exercise 5.23. What is $e^{i\theta}e^{i\gamma}$? **Hints:** 22

Now, let's consider the polynomial $z^n = 1$, for some complex number z . First, let's find $|z|$. We get that $|z|^n = 1$, so $|z| = 1$ (as $|z|$ is a distance, so it is nonnegative and real). Now, we can write

$$z = \cos \theta + i \sin \theta \quad (\beta)$$

We consider θ in the form (for integer k)

$$\theta = \frac{2k\pi}{n} \quad (\Gamma)$$

By [De Moivre's Theorem](#), we get that

$$z^n = (\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta = \cos 2\pi k + i \sin 2\pi k = 1$$

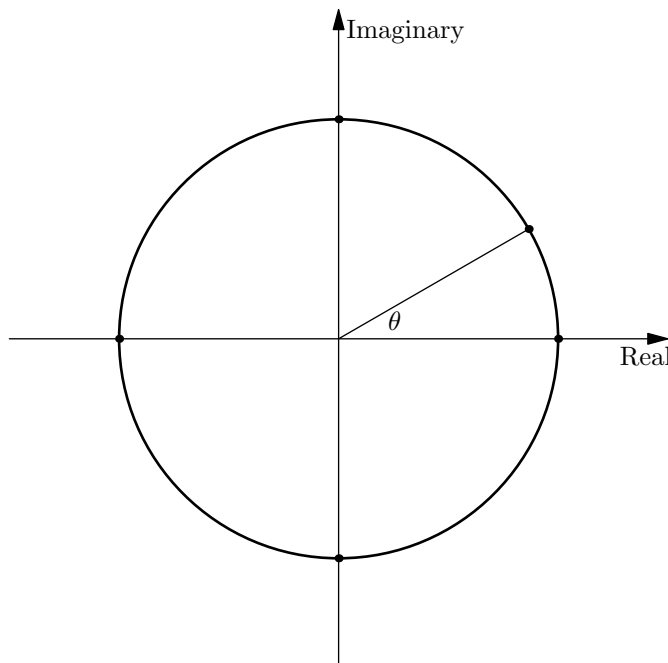
Thus, this means that as there are n distinct values of θ for $k = 0, 1, \dots, n-1$ (note that beyond this it repeats), we get by the [Fundamental Theorem of Algebra](#) that these are the only (distinct, remember that we can keep looping around the circle!) solutions. These are called the n th roots of unity:

Definition 5.24 (Roots of Unity) — The n th **roots of unity** are roots of $z^n = 1$.

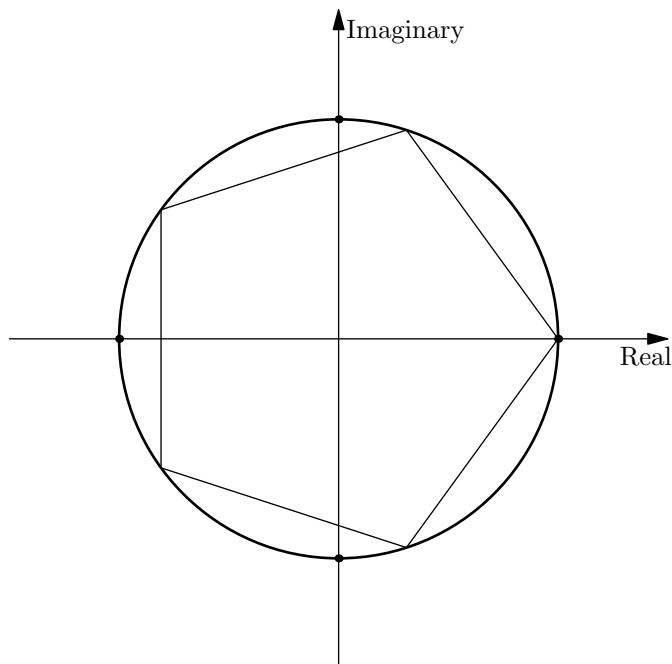
Exercise 5.25. Find the third and fourth roots of unity. **Hints:** 72

Exercise 5.26. Show that $31 \mid 5^{31} + 5^{17} + 1$ (or 31 divides $5^{31} + 5^{17} + 1$). 79

We can plot all of these roots of unity and also all other points z with $|z| = 1$. We get something like the following graph:



The roots of unity actually do something more than expected - they form a regular polygon:



That's an example with $n = 5$, or the fifth roots of unity!

Remark 5.27. Figuring out *why* exactly this is a regular pentagon is simple - because the idea is easy to see, I will leave this as an exercise. Think about the angles between the roots of unity - more accurately, how are they spaced?

Now, let's try the following problem:

Example 5.28 (AIME II 2011/8)

Let $z_1, z_2, z_3, \dots, z_{12}$ be the 12 zeroes of the polynomial $z^{12} - 2^{36}$. For each j , let w_j be one of z_j or iz_j . Then the maximum possible value of the real part of $\sum_{j=1}^{12} w_j$ can be written as $m + \sqrt{n}$ where m and n are positive integers. Find $m + n$.

Solution. We note that it's obvious that these (the z_j 's) aren't roots of unity - we have to divide z by 2^{36} to get one. Let $8x_k = z_k$ for each k ; we thus get that

$$x_k^{12} - 1 = 0,$$

so thus

$$x_k = \cos \frac{2\pi k}{12} + i \sin \frac{2\pi k}{12} = \cos \frac{\pi k}{6} + i \sin \frac{\pi k}{6}$$

Now, we note that multiplying by i adds $\frac{\pi}{2}$ to the imaginary part, so thus we get that

$$ix_k = \cos \frac{(3+k)\pi}{6} + i \sin \frac{(3+k)\pi}{6}$$

We don't care about the imaginary part, so let's drop it. Then, we get (by manually plugging in the numbers - I won't do it here) that the sum of our desired x_k has maximum value $2 + 2\sqrt{3}$. However, we still have to multiply by 8 to get our answer as

$$m + \sqrt{n} = 16 + 16\sqrt{3} = 16 + \sqrt{768} \implies m + n = 16 + 768 = \boxed{784}.$$



Why won't I do it? It turns out this is manual computation checking if

$$\cos \frac{(3+k)\pi}{6} \geq \frac{\pi k}{6}$$

and plugging in 12 values isn't exactly my strongest suit. You can check them if you want.

Exercise 5.29. Check that indeed what I claimed is correct.

Exercise 5.30 (2019 AIME II Problem 8). The polynomial $f(z) = az^{2018} + bz^{2017} + cz^{2016}$ has real coefficients not exceeding 2019, and $f\left(\frac{1+\sqrt{3}i}{2}\right) = 2015 + 2019\sqrt{3}i$. Find the remainder when $f(1)$ is divided by 1000. **Hints:** 24

Exercise 5.31 (1996 AIME Problem 11). Let P be the product of the roots of $z^6 + z^4 + z^3 + z^2 + 1 = 0$ that have a positive imaginary part, and suppose that $P = r(\cos \theta^\circ + i \sin \theta^\circ)$, where $0 < r$ and $0 \leq \theta < 360$. Find θ . **Hints:** 69

§6 A Small Bit Of Number Theory

The core of this section is the following result:

Theorem 6.1 (Difference of Polynomials)

Let $P(x)$ be a polynomial with integer coefficients. Then, we have that $a - b \mid P(a) - P(b)$.

Sketch of Proof. Try to expand $P(x) = c_n x^n + c_{n-1} x^{n-1} + \dots + c_0$. Then, substitute a and b , and use the factorization:

$$a^k - b^k = (a - b) \left(\sum_{i=0}^{k-1} a^i b^{k-i} \right) = (a - b)(a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1})$$



Looking at [Difference of Polynomials](#), we get that it isn't too deep - how will this help us? Well, let's take a look at this problem:

Example 6.2 (AIME II 2005/13)

Let $P(x)$ be a polynomial with integer coefficients that satisfies $P(17) = 10$ and $P(24) = 17$. Given that $P(n) = n + 3$ has two distinct integer solutions n_1 and n_2 , find the product $n_1 \cdot n_2$.

Remark 6.3. One non-rigorous way to prove this is that we take $P(x)$ as a quadratic. It isn't 100% rigorous though.

So, this is the number theory section. Let's try to see what we know - we do know that

$$P(n_1) = n_1 + 3$$

We'll only focus on n_1 , get two solutions, and then use one as n_1 and the other as n_2 . Well, the only thing I can think of to induce [Difference of Polynomials](#) is to take the difference:

$$n_1 - k \mid P(n_1) - P(k) = n_1 + 3 - P(k)$$

We only know 3 values of $P(k)$ (that are not n_1) - $k = n_2, 17, 24$. We can plug them all in

$$n_1 - n_2 \mid n_1 + 3 - (n_2 + 3) = n_1 - n_2$$

$$n_1 - 17 \mid n_1 + 3 - 10 = n_1 - 7$$

$$n_1 - 24 \mid n_1 + 3 - 17 = n_1 - 14$$

The first is useless. The second and third give the numbers

$$\frac{n_1 - 7}{n_1 - 17}, \frac{n_1 - 14}{n_1 - 24}$$

are integers. There's an n_1 in the numerator and denominator in each of them, so we can rewrite the fractions as

$$\begin{aligned} \frac{n_1 - 7}{n_1 - 17} &= \frac{n_1 - 7}{n_1 - 17} - \frac{n_1 - 17}{n_1 - 17} + 1 = \frac{10}{n_1 - 17} + 1 \\ \frac{n_1 - 14}{n_1 - 24} &= \frac{n_1 - 14}{n_1 - 24} - \frac{n_1 - 24}{n_1 - 24} + 1 = \frac{10}{n_1 - 24} + 1 \end{aligned}$$

Wow, so we get $n_1 - 17, n_1 - 24 \mid 10$. So we have two divisors of 10 that differ by $n_1 - 17 - (n_1 - 24) = 24 - 17 = 7$. We can list them out - there are only 8:

$$-10, -5, -2, -1, 1, 2, 5, 10$$

and easily find the only such ones are $\{2, -5\}, \{-2, 5\}$. Thus, we get that either $n_1 - 17 = 2$ or $n_1 - 17 = 5$, so $n_1 = 19, 22$. By what we mentioned above, it's easy to see that $n_2 = 19, 22$, so

$$n_1 \cdot n_2 = 19 \cdot 22 = \boxed{418}.$$

□

So this problem showed us that polynomial problems also can be solved with some Number Theory. For fun, however, solve the following parody of the AIME problem. Don't solve it with number theory - use [Zero Polynomial Corollary](#) to explicitly find $P(x)$ and then solve it:

Exercise 6.4 (Parody of 2005 AIME II Problem 13). Let $P(x)$ be a monic^a quadratic^b polynomial with integer coefficients that satisfies $P(17) = 10$ and $P(24) = 17$. Given that $P(n) = n + 3$ has two distinct integer solutions n_1 and n_2 , find the product $n_1 \cdot n_2$. **Hints:** [53](#)

The problem is that there aren't many problems on this topic. Here's a problem I made:

Exercise 6.5. Consider a polynomial $f(x)$ with integer coefficients such that for any integer $n > 0$, $f(n) - f(0)$ is a multiple of the sum of the first n positive integers. Find the minimum value of $f(2020) - f(0)$, given that $f(n + 1) > f(n)$ for all positive integers n . **Hints:** [45](#)

^aThis means the leading coefficient is 1.

^bThis means the degree is 2.

§7 Advanced Algebraic Manipulations

This section was only created due to suggestions from freeman66 and ab_xy123 on the AoPS Community.

Sometimes, when we are working with σ_k (see [Vieta's Formulas](#)) for small numbers, we will need to do a

bunch of manipulations. It isn't very easy to go back to [Newton's Formulas](#) every time, so here is a list for 3 variables (we get 2 variables is too easy, four variables is uncommon), due to freeman66. This list is not exhaustive, but it includes almost everything seen in an AIME setting. Also note that he uses the shorthand $u = \sigma_1, v = \sigma_2, w = \sigma_3$.

$$\text{Solution 1. } a^2 + b^2 + c^2 = u^2 - 2v$$

$$2. \ a^3 + b^3 + c^3 = u(u^2 - 3v) + 3w$$

$$3. \ a^2b^2 + b^2c^2 + c^2a^2 = v^2 - 2uw$$

$$4. \ a^4 + b^4 + c^4 = (u^2 - 2v)^2 - 2(v^2 - 2uw) = u^4 - 4u^2v + 2v^2 + 4uw$$

$$5. \ (a+b)(b+c)(c+a) = uv - w$$

$$6. \ \sum_{\text{cyc}} ab(a+b) = uv - 3w$$

$$7. \ (1+a)(1+b)(1+c) = 1 + u + v + w$$

$$8. \ \sum_{\text{cyc}} (1+a)(1+b) = 3 + 2u + v$$

$$9. \ \sum_{\text{cyc}} (1+a^2) = u^2 + v^2 + w^2 - 2uw - 2v + 1$$

I do suggest you go through these again to check that these are actually true. But let's see some uses of these manipulations. Most of them are AIME-like (suggested to me by ab_xy123) and require clever insights of different theorems to solve the problem:

Example 7.1 (PRMO 2019/2)

Let $f(x) = x^2 + ax + b$. If for all nonzero real x

$$f\left(x + \frac{1}{x}\right) = f(x) + f\left(\frac{1}{x}\right)$$

and the roots of $f(x) = 0$ are integers, what is the value of $a^2 + b^2$?

This problem looks pretty hard - how are we going to solve it? Well, what is something that makes

$$x, \frac{1}{x}, x + \frac{1}{x}$$

all look nice? I know that the only integer x such that $\frac{1}{x}$ is also an integer is ± 1 . We can try plugging in $x = 1$. We get

$$f(1+1) = f(1) + f(1)$$

We can use the polynomial to get

$$4 + 2a + b = f(2) = 2f(1) = 2(1 + a + b) = 2 + 2a + 2b$$

which gives $b = 2$. That's a good start, but how do we find a ? Well, let's look at the problem. It says all roots are integers. So what does this remind me of? Personally, I go back to the [Rational Root Theorem](#). So we get the roots are $\pm 1, \pm 2$. By [Vieta's Formulas](#), we also get the roots multiply to 2. So thus we get they are $(1, 2)$ or $(-1, -2)$.

We got two solutions! How is this possible! Well, it just boils down to how attentive you are. We need to find a^2 (because we already have b^2), and $a = 3, -3$ are our two values of a (we used [Vieta's Formulas](#)). So then, it's obvious - the sum is $a^2 + b^2 = \boxed{13}$ no matter what! So the problem was crafted in such a way it's impossible to find the roots - you must find a^2 .

Let's see another example in action - we will use some of [freeman66's tactics](#):

Example 7.2 (Modified from RMO 2013/2)

Let $f(x) = x^3 + ax^2 + bx + c$ and $g(x) = x^3 + bx^2 + cx + a$, where a, b, c are real numbers with $c \neq 0$. Suppose that the following conditions hold:

- $f(1) = 0$
- the roots of $g(x) = 0$ are the squares of the roots of $f(x) = 0$.

Find the value of $a^{2013} + b^{2013} + c^{2013}$.

Solution. Well, let's see what we know. We let the roots of f be r, s, t . By [Vieta's Formulas](#), we get

- $r + s + t = -a$
- $rs + rt + st = b$
- $rst = -c$

Now, the roots of $g(x)$ are r^2, s^2, t^2 , we get

- $r^2 + s^2 + t^2 = -b$
- $r^2s^2 + r^2t^2 + s^2t^2 = c$
- $r^2s^2t^2 = a$

Now, we can use some of [freeman66's properties](#). Specifically, using property 1, we get

$$a^2 - 2b = r^2 + s^2 + t^2 = -b$$

so $b = a^2$. Using property 3, we get

$$b^2 - 2ac = b^2 - 2(-a)(-c) = r^2s^2 + r^2t^2 + s^2t^2 = c$$

so

$$a^4 = b^2 = (2a + 1)c$$

This means that

$$c = \frac{a^4}{2a + 1} \tag{\Theta}$$

Finally, we get that

$$c^2 = r^2s^2t^2 = -a$$

so we get $(a, b, c) = (-c^2, c^4, c)$. But what about (Θ) ? Can we use it? Trying to use it, we get

$$c = \frac{c^8}{1 - 2c^2} \implies c^7 = 1 - 2c^2 \tag{\Pi}$$

Oh god! Not a degree 7 equation. But we can still use it to check solutions, in case. Let's see the other information that we got in the problem. We know $f(1) = 0$. We know

$$f(x) = x^3 - c^2x^2 + c^4x = c$$

so

$$0 = f(1) = 1 - c^2 + c + c^4 = (c + 1)(c^3 - c^2 + 1)$$

But the second factor isn't very nice, right? Let's see what we get from (II). We can factor it to get

$$0 = c^7 + 2c^2 - 1 = (c + 1)(c^6 - c^5 + c^4 - c^3 + c^2 + c + 1)$$

so obviously $c = -1$ is a root. If we assume that r is a root of the second factor, then $r^3 = r^2 - 1$. We can probably manipulate this, right? I mean, we must have that

$$r^6 - r^5 + r^4 - r^3 + r^2 + r + 1 = 0$$

Let's use our identity we found repeatedly. We get $r^6 = r^5 - r^3$, so plugging it in gives

$$r^4 - 2r^3 + r^2 + r + 1 = 0$$

Again! We get $r^4 = r^3 - r$, so thus plugging it in gives

$$-r^3 + r^2 + 1 = 0$$

One last time! $r^3 = r^2 - 1$, so

$$2r^2 = -2$$

which means $r = \pm i$. But it's easy to check that it isn't a root of $c^3 - c^2 + 1 = 0$! So we must have $c = -1$. Then, $a = -1$ and $b = 1$. Then, the problem becomes $-1 - 1 + 1 = \boxed{-1}$. \square

Remark 7.3. The problem only asked the question if a, b, c are integers. We proved they must be!

Here are some other exercises:

Exercise 7.4 (1991 INMO Problem 2). How many ordered triples (x, y, z) of real numbers satisfy the system of equations

$$x^2 + y^2 + z^2 = 9,$$

$$x^4 + y^4 + z^4 = 33,$$

$$xyz = -4?$$

Hints: [76](#)

Exercise 7.5 (AoPS Forums).

$$x + y + z = 1$$

$$x^2 + y^2 + z^2 = 2$$

$$x^3 + y^3 + z^3 = 3$$

Evaluate $x^4 + y^4 + z^4$. Hints: [18](#)

§8 Worked Through Problems

Remember the problems I promised you at the beginning? Let's look at them here:

Example 8.1 (AIME I 2016/11)

Let $P(x)$ be a nonzero polynomial such that $(x-1)P(x+1) = (x+2)P(x)$ for every real x , and $(P(2))^2 = P(3)$. Then $P(\frac{7}{2}) = \frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$.

Solution. Eh, this problem looks too mild. Let's spice it up! How about we find $P(x)$, and I leave plugging in $\frac{7}{2}$ for you?

First, let's try to scout for roots. We note that $x = -1$ and $x = -2$ give "easy" roots; here we get $P(1) = P(-1) = 0$ (do the work here, I may be lying). Now, plugging in $x = 0$ gives us $0 = -P(1) = 2P(0)$, so 0 is also a root.

So, what other roots are there, if any? Let's consider a root $r \neq 0, \pm 1$. Then, what can we get? We plug them into our only thing we know to get

$$(r-1)P(r+1) = (r+2)P(r) = 0$$

but as $r \neq 1$, we have $r+1 = 0$. Similarly, we get that $r+2$, is a root, and so on.

Or really? What if $r = -2$? Then we sort of hit a stopping point - we can't go forwards anymore, as we stop at 1. However, we only went forwards - we can do the same thing backwards to get

$$0 = (r-2)P(r) = (r+1)P(r-1)$$

so as $r \neq -1$, we are good as we go backwards. Obviously, no nonzero polynomial has ∞ roots, so the only roots are $0, \pm 1$. Thus, we almost have our polynomial - $P(x) = cx(x-1)(x+1)$. How to find c ? Well, there's a reason we have that second equation. That gives

$$P(2) = c \cdot 2 \cdot 1 \cdot 3 = 6c$$

$$P(3) = c \cdot 3 \cdot 2 \cdot 4 = 24c$$

so thus

$$36c^2 = P(2)^2 = P(3) = 24c$$

As c is nonzero, we divide by 0 to get $c = \frac{2}{3}$. Thus, $P(x) = \frac{2}{3}x(x-1)(x+1)$. I'll do a formal write-up in the following:

Formal Proof.

Call the assertion $Q(x)$ as $(x-1)P(x+1) = (x+2)P(x)$ ^a. Then, we get that $0, \pm 1$ are roots from $Q(1), Q(-2)$, and $Q(0)$.

Now, we shall prove that these are the only such roots. Assume that r is another root. If r is not a negative integer, we note that $Q(r)$ gives

$$(r-1)P(r+1) = (r+2)P(r) = 0$$

so as $r - 1 \neq 0$, we have that $r + 1$ is also a root. Now, we shall induct on k to show that $r + k$ is a root:

Base Case. $k = 1$ has been shown above.

Induction Hypothesis. Assume it is true for some k ; we will show it for $k + 1$.

Induction Step. We have that if r is not an integer, $r + k + 1$ can not be an integer, so it can not be $0, \pm 1$. If integer $r \geq 2$, then $r + k + 1 \geq 2$ and thus $r \neq 0, \pm 1$. Thus, we have that in this case $r + k + 1$ is an integer by applying our Base Case to $r + k$ instead of r .

For negative integers, by using $Q(r - 1)$, we get

$$0 = (r - 2)P(r) = (r + 1)P(r - 1)$$

so for negative integer roots r not -1 , we get $r - 1$ is also a root. Now, we shall induct on k to show that $r - k$ is a root:

Base Case. $k = 1$ has been shown above.

Induction Hypothesis. Assume it is true for some k ; we will show it for $k + 1$.

Base Case. As $r \leq -2$, then $r + k + 1 \leq -2$ and thus $r \neq 0, \pm 1$. Thus, we have that in this case $r - (k + 1)$ is an integer by applying our Base Case to $r - k$ instead of r .

Now, in either case we get infinitely many roots, so by [Zero Polynomial Corollary](#), we have that $P(x)$ is the zero polynomial, a contradiction. Thus, we get that $P(x) = cx(x - 1)(x + 1)$. Plugging in $x = 2, 3$, we have that $P(2) = 6c, P(3) = 24c$, so

$$36c^2 = P(2)^2 = P(3) = 24c$$

and as c is nonzero, $c = \frac{2}{3}$. Thus, we get that $P(x) = \frac{2}{3}x(x - 1)(x + 1)$ and in particular

$$\frac{m}{n} = P\left(\frac{7}{2}\right) = \frac{2}{3} \cdot \frac{7}{2} \cdot \frac{9}{2} \cdot \frac{5}{2} = \frac{105}{4}$$

which implies $m + n = \boxed{109}$.

^aThat's so I don't have to keep writing awkwardly our initial constraint

□

Example 8.2 (AIME 1984/15)

Determine $w^2 + x^2 + y^2 + z^2$ if

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

Solution. Ok, now this looks daunting. And in the wrong handout. Where's the polynomial? But that's the beauty of this problem - the polynomial comes when we see that trying to expand is *too tedious*. So, first, the

w^2, x^2, y^2, z^2 seems 150% unnecessary - like we could replace them with a, b, c, d . So let's do that:

$$\begin{aligned}\frac{a}{2^2-1} + \frac{b}{2^2-3^2} + \frac{c}{2^2-5^2} + \frac{d}{2^2-7^2} &= 1 \\ \frac{a}{4^2-1} + \frac{b}{4^2-3^2} + \frac{c}{4^2-5^2} + \frac{d}{4^2-7^2} &= 1 \\ \frac{a}{6^2-1} + \frac{b}{6^2-3^2} + \frac{c}{6^2-5^2} + \frac{d}{6^2-7^2} &= 1 \\ \frac{a}{8^2-1} + \frac{b}{8^2-3^2} + \frac{c}{8^2-5^2} + \frac{d}{8^2-7^2} &= 1\end{aligned}$$

It's already nicer. We just have to find $a + b + c + d$. Ok, now what else happens nicely? The denominators are always $t^2 - 1, t^2 - 9, t^2 - 25, t^2 - 49$ for $t = 2, 4, 6, 8$. Hmm...if we used this, we would get really big numbers, like degree 8 polynomials. What about $t - 1, t - 9, t - 25, t - 49$, where $t = 4, 16, 36, 64$.

Remark 8.3. It's more beneficial to spend time to step back and look at a problem from a different angle, especially when you have time and you realize the numbers you are getting are cancerous. Also, try to show any pattern you see holds.

Now, let's make that substitution, so we get

$$\frac{a}{t-1} + \frac{b}{t-9} + \frac{c}{t-25} + \frac{d}{t-49} = 1$$

for $t = 4, 16, 36, 64$. So what can we do? Well, we can't deal with these, but what if we made it a polynomial? Then, we would need a common denominator. Thus, we get

$$\frac{a(t-9)(t-25)(t-49) + b(t-1)(t-25)(t-49) + c(t-1)(t-9)(t-49) + d(t-1)(t-9)(t-25)}{(t-1)(t-9)(t-25)(t-49)} = 1$$

For the sake of allowing this to fit in the page, define

$$\tau_a = (t-9)(t-25)(t-49) = t^3 - 83t^2 + 1891t - 11025$$

$$\tau_b = (t-1)(t-25)(t-49) = t^3 - 75t^2 + 1299t - 1225$$

$$\tau_c = (t-1)(t-9)(t-49) = t^3 - 59t^2 + 499t - 441$$

$$\tau_d = (t-1)(t-9)(t-25) = t^3 - 35t^2 + 259t - 225$$

Remark 8.4. It is implied that these are polynomials. I should do a better job of this, but it's in the formal write-up.

Then, cross multiplying would give us

$$a\tau_a + b\tau_b + c\tau_c + d\tau_d = (t-1)(t-9)(t-25)(t-49)$$

for $t = 4, 16, 36, 64$. How can we manipulate this? Well, the equation has degree 4, and we have four roots, so we can use the [Unique Factorization of Polynomials](#) to say they are equal. But which one of $a\tau_a + b\tau_b + c\tau_c + d\tau_d$ and $(t-1)(t-9)(t-25)(t-49)$ do we choose?

What are we doing? We have to write $f(t) = 0$, so we want the polynomial of their difference,

$$a\tau_a + b\tau_b + c\tau_c + d\tau_d - (t-1)(t-9)(t-25)(t-49) = 0 \quad (\#)$$

and get that $t = 4, 16, 36, 64$ are roots. So then, we can take this equal to $(t - 4)(t - 16)(t - 36)(t - 64)$, right?

But what about the leading coefficients? Don't forget them! We see that $\tau_a, \tau_b, \tau_c, \tau_d$ are all degree 3 polynomials, so $(\#)$ has leading coefficient -1 . Thus, we actually get that $(\#) = -(t - 4)(t - 16)(t - 36)(t - 64)$, so

$$a\tau_a + b\tau_b + c\tau_c + d\tau_d - (t - 1)(t - 9)(t - 25)(t - 49) = -(t - 4)(t - 16)(t - 36)(t - 64)$$

Yeah, so we can look at what we want to find: $a + b + c + d$. As this has infinitely many roots, we have that by [Zero Polynomial Corollary](#), the coefficients on each side are equal. But, what can we do?

Looking at $\tau_a, \tau_b, \tau_c, \tau_d$, we get that as we move towards lower degree terms, the polynomial gets more "cancerous", shall we say? So thus, we start with the highest degree terms: 4. We get that the left hand side has leading coefficient -1 ($\tau_a, \tau_b, \tau_c, \tau_d$ all have degree 3), but the right hand side has coefficient -1 .

Oh well, let's go to degree 3. τ_a has the coefficient of degree 3 as 1, so $a\tau_a$ has coefficient a . Similarly, $b\tau_b, c\tau_c, d\tau_d$ all have coefficients of t^3 as b, c, d . Now, by [Vieta's Formulas](#), the coefficient of t^3 in $(t - 1)(t - 9)(t - 25)(t - 49)$ is $-(1 + 9 + 25 + 49) = -84$. However, once again by [Vieta's Formulas](#), the coefficient of t^3 in $-(t - 4)(t - 16)(t - 36)(t - 64)$ is $4 + 16 + 36 + 64 = 120$ (note the negative signs cancelled out). Thus, we get that

$$a + b + c + d - (-84) = 120 \implies a + b + c + d = 120 - 84 = \boxed{36}.$$

□

Once again, I'll provide a formal write-up:

Formal Proof.

Define $a = x^2, b = y^2, c = z^2, d = w^2$, then we get that the problem condition rewrites to

$$\begin{aligned} \frac{a}{2^2 - 1} + \frac{b}{2^2 - 3^2} + \frac{c}{2^2 - 5^2} + \frac{d}{2^2 - 7^2} &= 1 \\ \frac{a}{4^2 - 1} + \frac{b}{4^2 - 3^2} + \frac{c}{4^2 - 5^2} + \frac{d}{4^2 - 7^2} &= 1 \\ \frac{a}{6^2 - 1} + \frac{b}{6^2 - 3^2} + \frac{c}{6^2 - 5^2} + \frac{d}{6^2 - 7^2} &= 1 \\ \frac{a}{8^2 - 1} + \frac{b}{8^2 - 3^2} + \frac{c}{8^2 - 5^2} + \frac{d}{8^2 - 7^2} &= 1 \end{aligned}$$

and we need to find $w^2 + x^2 + y^2 + z^2 = a + b + c + d$. Notice that

$$\frac{a}{t - 1} + \frac{b}{t - 9} + \frac{c}{t - 25} + \frac{d}{t - 49} = 1 \tag{!}$$

holds for $t = 4, 16, 36$, and 64 as guaranteed by the problem statement. Thus, we define

$$\begin{aligned} \tau_a(t) &= (t - 9)(t - 25)(t - 49) \\ \tau_b(t) &= (t - 1)(t - 25)(t - 49) \\ \tau_c(t) &= (t - 1)(t - 9)(t - 49) \\ \tau_d(t) &= (t - 1)(t - 9)(t - 25) \\ \tau(t) &= (t - 1)(t - 9)(t - 25)(t - 49) \end{aligned}$$

Now, we get that

$$\frac{a}{t-1} = \frac{a(t-9)(t-25)(t-49)}{(t-1)(t-9)(t-25)(t-49)} = \frac{a\tau_a(t)}{\tau(t)}$$

Thus, by symmetry, we get that

$$\begin{aligned}\frac{b}{t-9} &= \frac{b\tau_b(t)}{\tau(t)} \\ \frac{c}{t-25} &= \frac{c\tau_c(t)}{\tau(t)} \\ \frac{d}{t-49} &= \frac{d\tau_d(t)}{\tau(t)}\end{aligned}$$

Thus, (!) asserts that

$$\frac{a\tau_a(t) + b\tau_b(t) + c\tau_c(t) + d\tau_d(t)}{\tau(t)} = 1 \implies a\tau_a(t) + b\tau_b(t) + c\tau_c(t) + d\tau_d(t) = \tau(t)$$

where $t = 4, 16, 36, 64$. Thus, we get that

$$\chi(t) = a\tau_a(t) + b\tau_b(t) + c\tau_c(t) + d\tau_d(t) - \tau(t) \quad (\Omega)$$

has zeroes at $t = 4, 16, 36, 64$. Furthermore, as $\tau_a, \tau_b, \tau_c, \tau_d$ have degree 3 and τ has degree 4, we have that χ has degree 4. Thus, we can write (by [Unique Factorization of Polynomials](#)):

$$\chi(t) = k(t-4)(t-16)(t-36)(t-64) \quad (\zeta)$$

for some (nonzero^a) real k . Now, we get that comparing the leading coefficients, by (Ω) , the leading coefficient of χ is the opposite of the leading coefficient of τ (as $\tau_a, \tau_b, \tau_c, \tau_d$ have degrees all less than τ). Thus, because the leading coefficient of τ is 1, the leading coefficient of χ is -1 , and thus so is k (by (ζ)). Now, we compare the coefficients of t^3 . The coefficient of t^3 in $\tau_a, \tau_b, \tau_c, \tau_d$ is 1. The coefficient of t^3 in τ is

$$-(1 + 9 + 25 + 49) = -84$$

so thus the coefficient of t^3 in χ is

$$a + b + c + d + 84$$

However, the coefficient of χ in $-(t-4)(t-16)(t-36)(t-64)$ is

$$-(4 + 16 + 36 + 64) = 120$$

These are equal, so

$$a + b + c + d + 84 = 120 \implies a + b + c + d = \boxed{36}$$

^aThis is as τ is the only polynomial with degree 4, so the x^4 term can not “cancel” out.

§9 Parting Words and Final Problems

So with this, you should be able to solve almost any AIME Problem on polynomials. I hope this document helped you learn a bit about how to use polynomials in all kinds of contexts, even ones that aren’t obviously apparent. Any suggestion would be extremely helpful, whether it would be problem suggestions, mistakes I made, or stuff I should explain better. Here’s a final problem set that should incorporate (almost) every AIME Problem which requires polynomials (that hasn’t been solved above). In addition, there are other problems, which are suggestions from one of twinbrian or ab_xy123:

Problem 9.1 (1983 AIME Problem 3). What is the product of the real roots of the equation $x^2 + 18x + 30 = 2\sqrt{x^2 + 18x + 45}$? **Hints:** 63

Problem 9.2 (2013 AIME I Problem 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 $a + b + c$. **Hints:** 64

Problem 9.3 (2010 AIME I Problem 6). 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 $P(16)$. **Hints:** 66

Problem 9.4 (2015 AIME II Problem 6). Steve says to Jon, “I am thinking of a polynomial whose roots are all positive integers. The polynomial has the form $P(x) = 2x^3 - 2ax^2 + (a^2 - 81)x - c$ for some positive integers a and c . Can you tell me the values of a and c ?”

After some calculations, Jon says, “There is more than one such polynomial.”

Steve says, “You’re right. Here is the value of a .” He writes down a positive integer and asks, “Can you tell me the value of c ?”

Jon says, “There are still two possible values of c .”

Find the sum of the two possible values of c . **Hints:** 49

Problem 9.5 (2016 AIME II Problem 6). For polynomial $P(x) = 1 - \frac{1}{3}x + \frac{1}{6}x^2$, define

$$Q(x) = P(x)P(x^3)P(x^5)P(x^7)P(x^9) = \sum_{i=0}^{50} a_i x^i.$$

Then $\sum_{i=0}^{50} |a_i| = \frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$. **Hints:** 8

Problem 9.6 (2004 AIME I Problem 7). Let C be the coefficient of x^2 in the expansion of the product $P(x) = (1 - x)(1 + 2x)(1 - 3x) \cdots (1 + 14x)(1 - 15x)$. Find $|C|$. **Hints:** 5 55

Problem 9.7 (2011 AIME I Problem 7). Find the number of positive integers m for which there exist nonnegative integers $x_0, x_1, \dots, x_{2011}$ such that

$$m^{x_0} = \sum_{k=1}^{2011} m^{x_k}.$$

Hints: 3

Problem 9.8 (1984 AIME Problem 8). The equation $z^6 + z^3 + 1 = 0$ has complex roots with argument θ between 90° and 180° in the complex plane. Determine the degree measure of θ . **Hints:** 12

Problem 9.9 (1989 AIME Problem 8). Assume that x_1, x_2, \dots, x_7 are real numbers such that

$$\begin{aligned} x_1 + 4x_2 + 9x_3 + 16x_4 + 25x_5 + 36x_6 + 49x_7 &= 1 \\ 4x_1 + 9x_2 + 16x_3 + 25x_4 + 36x_5 + 49x_6 + 64x_7 &= 12 \\ 9x_1 + 16x_2 + 25x_3 + 36x_4 + 49x_5 + 64x_6 + 81x_7 &= 123. \end{aligned}$$

Find the value of $16x_1 + 25x_2 + 36x_3 + 49x_4 + 64x_5 + 81x_6 + 100x_7$. **Hints:** 52

Problem 9.10 (2014 AIME I Problem 9). Let $x_1 < x_2 < x_3$ be the three real roots of the equation $\sqrt{2014}x^3 - 4029x^2 + 2 = 0$. Find $x_2(x_1 + x_3)$. **Hints:** 15

Problem 9.11 (2010 AIME II Problem 10). Find the number of second-degree polynomials $f(x)$ with integer coefficients and integer zeros for which $f(0) = 2010$. **Hints:** 6

Problem 9.12 (2015 AIME I Problem 10). Let $f(x)$ be a third-degree polynomial with real coefficients satisfying

$$|f(1)| = |f(2)| = |f(3)| = |f(5)| = |f(6)| = |f(7)| = 12.$$

Find $|f(0)|$. **Hints:** 73

Problem 9.13 (2019 AIME I Problem 10). For distinct complex numbers z_1, z_2, \dots, z_{673} , the polynomial

$$(x - z_1)^3(x - z_2)^3 \cdots (x - z_{673})^3$$

can be expressed as $x^{2019} + 20x^{2018} + 19x^{2017} + g(x)$, where $g(x)$ is a polynomial with complex coefficients and with degree at most 2016. The value of

$$\left| \sum_{1 \leq j < k \leq 673} z_j z_k \right|$$

can be expressed in the form $\frac{m}{n}$, where m and n are relatively prime positive integers. Find $m + n$. **Hints:** 32

Problem 9.14 (1986 AIME Problem 11). The polynomial $1 - x + x^2 - x^3 + \cdots + x^{16} - x^{17}$ may be written in the form $a_0 + a_1y + a_2y^2 + \cdots + a_{16}y^{16} + a_{17}y^{17}$, where $y = x + 1$ and the a_i 's are constants. Find the value of a_2 . **Hints:** 4

Problem 9.15 (1988 AIME Problem 13). Find a if a and b are integers such that $x^2 - x - 1$ is a factor of $ax^{17} + bx^{16} + 1$. **Hints:** 2

Problem 9.16 (2000 AIME Problem 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 $m + n + r$. **Hints:** 74 30

Problem 9.17 (2004 AIME I Problem 13). The polynomial $P(x) = (1 + x + x^2 + \cdots + x^{17})^2 - x^{17}$ has 34 complex roots of the form $z_k = r_k[\cos(2\pi a_k) + i \sin(2\pi a_k)]$, $k = 1, 2, 3, \dots, 34$, with $0 < a_1 \leq a_2 \leq a_3 \leq \cdots \leq a_{34} < 1$ and $r_k > 0$. Given that $a_1 + a_2 + a_3 + a_4 + a_5 = \frac{m}{n}$, where m and n are relatively prime positive integers, find $m + n$. **Hints:** 68

Problem 9.18 (2007 AIME II Problem 14). Let $f(x)$ be a polynomial with real coefficients such that $f(0) = 1$, $f(2) + f(3) = 125$, and for all x , $f(x)f(2x^2) = f(2x^3 + x)$. Find $f(5)$. **Hints:** 11 38 9

Problem 9.19 (2020 AIME I Problem 14). Let $P(x)$ be a quadratic polynomial with complex coefficients whose x^2 coefficient is 1. Suppose the equation $P(P(x)) = 0$ has four distinct solutions, $x = 3, 4, a, b$. Find the sum of all possible values of $(a + b)^2$. **Hints:** 37 58 19

Problem 9.20 (2011 AIME I Problem 15). For some integer m , the polynomial $x^3 - 2011x + m$ has the three integer roots a, b , and c . Find $|a| + |b| + |c|$. **Hints:** 36 77

Problem 9.21 (1984 USAMO Problem 1). In the polynomial $x^4 - 18x^3 + kx^2 + 200x - 1984 = 0$, the product of 2 of its roots is -32 . Find k . **Hints:** 70

Problem 9.22 (2017 RMO Problem 3). Let $P(x) = x^2 + \frac{x}{2} + b$ and $Q(x) = x^2 + cx + d$ be two polynomials with real coefficients such that $P(x)Q(x) = Q(P(x))$ for all real x . Find all real roots of $P(Q(x)) = 0$. **Hints:** 56 23

Problem 9.23 (2018 PRMO Problem 30). Let $P(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial in which a_i is non-negative integer for each $i \in 0, 1, 2, 3, \dots, n$. If $P(1) = 4$ and $P(5) = 136$, what is the value of $P(3)$? **Hints:** 7 75 59

Problem 9.24 (2020 February HMMT Algebra and Number Theory Problem 8). Let $P(x)$ be the unique polynomial of degree at most 2020 satisfying $P(k^2) = k$ for $k = 0, 1, 2, \dots, 2020$. Compute $P(2021^2)$. **Hints:** [42](#) [41](#) [46](#)

Problem 9.25 (Modified from 2016 PUMaC A7). Let S_P be the set of all polynomials P with complex coefficients, such that $P(x^2) = P(x)P(x-1)$ for all complex numbers x . **Hints:** [29](#) [65](#) [21](#) [25](#)

§10 Hints

1. Find $\sigma_1, \sigma_2, \sigma_3$. This should be a routine exercise, and then consider all roots of $x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 = 0$.
2. You could try to use recursions if you recognize $x^2 - x - 1$. Otherwise, try to use polynomial division with smaller sequences - and see if there is a pattern.
3. Doesn't seem like a polynomial problem? Think of a simple value of which you know x^k for all k - and find $P(x)$. Then, try to use polynomial division. The backwards of this, however, is purely number theory. I'm sure you can do it!
4. Try a geometric series as the value of the polynomial. It should make the rest very easy.
5. Well, considering the x^2 term isn't very good. How about the polynomial with roots $\frac{1}{r_1}, \frac{1}{r_2}, \dots$ (r_1, r_2, \dots are the roots of $P(x)$)? Is it simpler now?
6. Write it in factored form! Where can you go from there?
7. Can you bound n ? Remember, $5^3 = 125$!
8. This is more daunting than it looks - try to see what value of x satisfies $P(x)$ is the sum of the coefficients of $P(x)$. Can you generalize to $Q(x)$?
9. Consider the polynomial $g(x)$ with the roots found above, and write $f(x) = g(x)h(x)$. Does $h(x)$ satisfy the same constraints as $f(x)$? Use this to finish off the problem (after finding the form of $f(x)$).
10. Use Newton's Sums, but make sure to factor first! Make it as simple as possible! (In general, try to keep everything factored for as long as possible).
11. Try to find a root with $r > 1$. Can you find another? What is the magnitude of that? Greater, equal to, or less than r ? Can you keep going? Remember [Zero Polynomial Corollary](#) and use ∞ roots.
12. Let $x = z^3$. Does this look familiar (third roots of unity)? Use the polar form to get such a value of θ .
13. Use induction and the fact $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k}$.⁹
14. Use [Complex Conjugate Theorem](#) as well as the fact that every polynomial of odd degree has at least one real root. We can show the last statement as follows: graph $f(x)$, and note on one side, it goes to ∞ while on the other it goes to $-\infty$ so it must hit the x -axis in the middle.
15. Let $n = 2014$. Write $\sqrt{2014}$ and 4029 in terms of n . Now try to factor!
16. How many roots are there? Can you use a double counting method?
17. Can you use Vieta's to find an expression for t in terms of r and s ? Then try to expand!
18. Try to use manipulations 2 and 4 from freeman66's list. It's not 4!
19. For some of the cases, you may have to solve for a and b explicitly. There's nothing to do about that.
20. What's the imaginary part of r ?
21. What if $|r| < 1$? First, however, ignore $r = 0$.
22. Use the exponent laws - don't try to convert into complex numbers.
23. Expanding is good. We already should know one value, so there are only two "unknowns".
24. Rewrite $\frac{1+\sqrt{3}i}{2}$ as a root of unity. Can you simplify, for example, z^{2018} to a lower power?
25. Assume $|r| = 1$, and let $r = a + bi$. You'll get an equation in terms of a and b . Expand and solve!
26. The answer to "do the results seem familiar" should be yes. They should relate to the coefficients in the expansions.
27. Try to expand $f \cdot g$ and $f + g$!
28. Assume $z = a + bi, w = c + di$, and then expand both sides and then show they are equal.

⁹We use $\binom{n}{k}$ to mean the number of ways to choose an (unordered) set k elements from n elements.

29. What are the roots of $P(x^2)$ in terms of the roots of $P(x)$?
30. Only one of the two factors will have real roots. Use the [Discriminant of a Quadratic Polynomial](#) to help you determine this (if x^2 is not real, neither is x).
31. What's the third root? Also use [Factor Theorem](#); it can be helpful to reduce the amount of extra algebra done. But alas, the problem ends bashy.
32. It's a little more complicated than straightforward [Vieta's Formulas](#) - can you also use [Newton's Formulas](#) (or [freeman66's tactics](#))?
33. Assume $z = a + bi$, and then expand both sides and then show they are equal.
34. Assume $z = a + bi, w = c + di$, and then expand both sides and then show they are equal.
35. Use the [Rational Root Theorem](#) to find all possible roots of both polynomials.
36. Without loss of generality, let $|a| \leq |b| \leq |c|$. Consider what c is in terms of a and b . Also use [Newton's Formulas](#) to reduce your search.
37. Consider the roots of $P(x)$ as r_1, r_2 . How many cases do you really have here for $P(x) = r_1, P(x) = r_2$. Remember to exploit symmetry.
38. Repeat the same thing with $r < 1$. Can you find a root with $|r| = 1$?
39. Use the first equation to substitute.
40. Expand! No better hint for this problem.
41. Now, here's the magic (it's called finite differences). Consider $Q(x+1) - Q(x)$.
 - What's its degree?
 - List 4038 roots.
 - Can you find the value of the leading coefficient (what is $Q(1) - Q(-1)$)?
42. If you know Lagrange Interpolation, use it! Otherwise, can you find an **obvious root** of $P(x)$? Can you consider a polynomial $Q(x)$ (of degree 4039) with roots $k = 1, 2, \dots, 2020$ and manageable values for $k = -1, -2, \dots, -2020$?
43. Solve the exercise in the order given ρ_1, ρ_2, ρ_3 . You may need to substitute.
44. Try using $y = 2^{111x}$. Then, try to also work backwards as we did in the above problem to find a nice expression for the sum of all values for x in terms of all values of y .
45. Remember, 2020 also divides $f(2020) - f(0)$. Now, can you find a polynomial that satisfies $f(2020)$ as the value you had. I suggest looking at the formula for the sum of the first n numbers.
46. If you don't recognize some of the scary terms - think of binomial coefficients.
47. Can you experiment with some smaller roots? Maybe use [Rational Root Theorem](#)?
48. Look at [Complex Conjugate Theorem](#) for a weakened version. Follow the same proof.
49. Take that problem step by step. Also, [Vieta's Formulas](#) comes in handy here. And [Newton's Formulas](#) can help too. Alternatively, consider #1 from [freeman66's tactics](#).
50. This has a nice polynomial solution. Note a number is real if and only if it is equal to its conjugate. Use that to obtain a polynomial in z . How many roots does it have?
51. Use [Complex Conjugate Theorem](#) and the fact that every polynomial of odd degree has at least one real root.
52. Try to generalize (like we did in [AIME 1984/15](#))! Can you find a polynomial here? Can you find the coefficients?
53. Try to find a linear polynomial $Q(x)$ with $Q(17) = 10$ and $Q(24) = 17$. Then factor $P(x) - Q(x)$.
54. U
55. [Newton's Formulas](#) can help too. Alternatively, consider #1 from [freeman66's tactics](#).

56. Assume $P(x)$ has real roots (otherwise the problem is trivial). Consider any root r of $P(x)$. What's $P(r)Q(r)$? $Q(P(r))$?
57. How many roots are in common between $Q_1(x)$ and $Q_2(x)$?
58. Also remember that the polynomials $P(x) - r_1, P(x) - r_2$ have the same linear term. Some cases will be nearly trivial with [Vieta's Formulas](#). Others will be almost impossible without bashing.
59. The bounds should be easy to obtain for the rest except a_0, a_1 , where you will get two equations in two variables. Elimination works, and so does substitution, and any other method taught in Algebra I. Solve for $P(x)$.
60. How can you relate the roots of P_k and P_{k+1} . The rest should follow from Vieta's relationships.
61. It was k_1 for σ_1 , k_1k_2 for σ_2 , and $k_1k_2k_3$ for σ_3 . See a pattern?
62. Assume $z = a + bi, w = c + di$, and then expand both sides and then show they are equal.
63. Make the substitution $y = x^2 + 18x + 30$ and solve for y instead.
64. Do some of the terms look similar to those in $(x+1)^3$? What can you conclude (rearrange it to $(x+1)^3 = \text{something}$)?
65. Consider a root r . What can you tell me if $|r| > 1$ (specifically, what is the magnitude in relationship to r)? Remember [Zero Polynomial Corollary](#) with ∞ roots. Also use $m > \sqrt{m}$ if $m > 1$.
66. Suppose $Q(x) = x^2 - 2x + 2$ and $R(x) = 2x^2 - 4x + 3$. When $Q(x) = R(x)$, do we know the value of $P(x)$? Can you find the exact value of $P(x)$ from there?
67. Like in the above two problems, just break the \sum into less daunting sums and take casework.
68. Use a geometric series, and then expand! It won't disappoint if you try to factor.
69. Can you try to factor? Use the fifth roots of unity to help you.
70. The algebraic manipulation $ab + ac + ad + bc + bd + cd = (a + b)(c + d) + ab + cd$ comes in handy a lot.
71. Factor it! How many roots does it have?
72. Use [\(\$\beta\$ \)](#) and [\(\$\Gamma\$ \)](#).
73. This was built for [Vieta's Formulas](#). Find the roots of $P(x) + 12$ and $P(x) - 12$ (note the only change between the polynomials is the constant term).
74. You could try to factor this. Focus on the terms of even degree and odd degree separately.
75. Is it even possible that $a_m = 0$, where m is the maximum value of n ? Remember that the sum of the a_i is 4! Can it be more than 1?
76. Try to use manipulations 2 and 4 from freeman66's list.
77. Take cases on if $c > 0$ or $c < 0$. Bound c well, and do casework on the rest.
78. Use [Euler's Formula](#).
79. Try to rewrite $31 = 5^2 + 5 + 1$. Can you use roots of unity (you may have to factor $x^n - 1$)?
80. Let $\zeta = \sin^2 x$ and $\chi = \cos^2 x$. Do you have any information on ζ and χ that would allow you to solve for $\zeta\chi$?

§A Appendix A: Proof of Results

Let's prove some of the results here:

Theorem A.1 (Fundamental Theorem of Algebra)

Given a polynomial $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ in $\mathbb{C}[x]$ (polynomials with complex number coefficients), there exists a root $r \in \mathbb{C}$ (aka $f(r) = 0$).

Proof due to Matthew Steed, University of Chicago. We shall use [Liouville's Theorem](#), which is a powerful argument in complex analysis which states the following:

Theorem A.2 (Liouville's Theorem)

Every bounded holomorphic function must be constant.

That's it. It's pretty powerful, and for sake of completeness, I include a proof:

Proof. Note any holomorphic function f is analytic. Consider the Taylor Series about 0:

$$f(x) = \sum_{k=0}^{\infty} b_k x^k$$

Then, using Cauchy's Integral Formula, we get

$$b_k = \frac{f^{(k)}(0)}{k!} = \frac{1}{2\pi i} \oint_C \frac{f(\zeta)}{\zeta^{k+1}} d\zeta$$

where C is a circle radius r (arbitrary) centered at 0. Now, suppose f is bounded. Then, if $|f(x)| \leq M$, we get

$$|b_k| \leq \frac{1}{2\pi} \oint_C \frac{|f(\zeta)|}{|\zeta|^{k+1}} |d\zeta| \leq \oint_C \frac{M}{r^{k+1}} |d\zeta| = \frac{M 2\pi r}{2\pi r^{k+1}} = \frac{M}{r^k}$$

Taking $r \rightarrow \infty$, we accomplish our proof. □

Back to the proof of [Fundamental Theorem of Algebra](#). Consider a disk of radius R used in the previous proof. There exists some α on the disk such that $|f(\alpha)|$ is a minimum on the disk. We suppose again that $f(\alpha) \neq 0$. For any z such that $|z| \geq |R|$, $|f(z)| > |f(\alpha)|$, so $\left| \frac{1}{f(\alpha)} \right| > \left| \frac{1}{f(z)} \right|$. By Liouville's Theorem, this is bounded above, so $\left| \frac{1}{f} \right|$ is constant, so $|f|$ is constant, which is a contradiction. Thus, $f(\alpha) = 0$. □

Theorem A.3 (Fundamental Theorem of Symmetric Polynomials)

Any symmetric polynomial can be expressed as the sum/product of a bunch of different symmetric polynomials.

Proof. We will do an induction on the degree of the polynomial m :

Base Case.

$m = 1$ is obvious.

Induction Hypothesis.

Assume the statement is true for all $m - 1 \geq k \geq 1$. We shall prove it is true for m .

Induction Step.

Now, for the rest of the proof to work, we can break up our polynomial into a bunch of symmetric polynomials of the same degree. We shall thus focus only when the degree of each term is m . Now, let us order the terms of our symmetric polynomial, with $ax_1^{a_1}x_2^{a_2}\cdots$ coming before $bx_1^{b_1}x_2^{b_2}\cdots$ if and only if for the first k such that $b_k \neq a_k$, $a_k > b_k$. Now, consider any term of our symmetric polynomial $f = ax_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}$ (and $a_1 + a_2 + \cdots + a_n = m$). We can assume

$$a_1 \geq a_2 \geq \cdots \geq a_n$$

because every permutation of a_1, a_2, \dots, a_n is included. Thus, we consider

$$g = a\sigma_1^{a_1-a_2}\sigma_2^{a_2-a_3}\cdots\sigma_n^{a_n}$$

Then, this has the same leading term as f , so applying our induction hypothesis, we can write $f - g$ as the sum/product of a bunch of symmetric polynomials, so we can write f as a sum/product of a bunch of symmetric polynomials.

□

§B Appendix B: Polynomial Division

We introduce polynomial division and give a proof of the [Remainder Theorem](#). Consider two polynomials, $f(x)$ and $g(x)$. Then, we can write

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

where $\deg r < \deg g$. We can prove the existence of such by induction on $\deg f$:

Base Case.

When $\deg f = \deg g$, we consider $q(x)$ the constant defined as the ratio of the leading coefficients of f to g . Then, we get that $f(x) - q(x)g(x)$ has its terms of $\deg g$ cancel out, so thus we get our claim is valid in this case. Where $\deg f < \deg g$, we get that $r(x) = f(x)$ and $q(x) = 0$ works.

Induction Hypothesis.

We assume the result holds for all polynomials such that $\deg f \leq k$ for some k . We shall show the result holds for $k + 1$ as well.

Induction Step.

Consider p as the ratio of the leading coefficients of f to g . Then, we get that considering

$$f'(x) = f(x) - px^{\deg f - \deg g}g(x)$$

we get the leading term (of degree $\deg f$) cancel, so thus $\deg f' \leq k$. Thus, we get

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

from our induction hypothesis, and then

$$f(x) = g(x)(q(x) + px^{\deg f - \deg g}) + r(x)$$

completing the induction step.

Now, we can also show uniqueness. We suppose that

$$f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$$

Then, we have that

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x)$$

Now, we note that if $q_1 \neq q_2$, we get that the right hand side has at least $\deg g$ roots by the [Fundamental Theorem of Algebra](#), but the left hand side has less than $\deg g$ roots by the [Fundamental Theorem of Algebra](#) (as $\deg r_1, \deg r_2 < g$ by assumption). Thus, this is a contradiction, so thus $q_1 = q_2$ and $r_1 = r_2$, so the expressibility is unique.

But how do we do this? Remember normal division? We can use something like that. Let's recap:

$$\begin{array}{r} 949 \\ 13 \overline{)12345} \\ \underline{117} \\ 64 \\ \underline{52} \\ 125 \\ \underline{117} \\ 8 \end{array}$$

We can do something similar with polynomials:

$$\begin{array}{r} X^2 + 2X + 2 \\ X - 1 \overline{) X^3 + X^2 + 0X - 1} \\ \underline{-X^3 + X^2} \\ 2X^2 + 0X \\ \underline{-2X^2 + 2X} \\ 2X - 1 \\ \underline{-2X + 2} \\ 1 \end{array}$$

Let's go step by step. First, we take the smallest number of digits such that we can find a multiple of 13:

$$\begin{array}{r} 9 \\ 13 \overline{)12345} \\ \underline{117} \\ 6 \end{array}$$

Similarly, we do the same in polynomials long division:

$$\begin{array}{r} X^2 \\ X - 1 \overline{) X^3 + X^2 + 0X - 1} \\ \underline{-X^3 + X^2} \\ 2X^2 + 0X \\ \underline{-2X^2 + 2X} \\ 2X - 1 \\ \underline{-2X + 2} \\ 1 \end{array}$$

Now, we just reiterate the process:

$$\begin{array}{r}
 94 \\
 13 \overline{)12345} \\
 \underline{117} \\
 64 \\
 \underline{52} \\
 12
 \end{array}$$

$$\begin{array}{r}
 X^2 + 2X + 2 \\
 X - 1 \overline{) X^3 + X^2 + 0X - 1} \\
 \underline{-X^3 + X^2} \\
 2X^2 + 0X \\
 \underline{-2X^2 + 2X} \\
 2X - 1
 \end{array}$$

Until we get the quotient as described above. And for the sake of demonstration that it can be done with not only linear polynomials:

$$\begin{array}{r}
 X^2 + 2X + 1 \\
 X^2 + X - 1 \overline{) X^4 + 3X^3 + 2X^2 - 2X - 3} \\
 \underline{-X^4 - X^3 + X^2} \\
 2X^3 + 3X^2 - 2X \\
 \underline{-2X^3 - 2X^2 + 2X} \\
 X^2 + 0X - 3 \\
 \underline{-X^2 - X + 1} \\
 -X - 2
 \end{array}$$

But onto the proof of [Remainder Theorem](#). We have that we can divide a polynomial $f(x)$ by $x - r$ to get

$$f(x) = (x - r)g(x) + h(x)$$

However, we get plugging in $x = r$, we get

$$f(r) = (r - r)g(r) + h(r) = h(r)$$

However, we note that $\deg h < \deg(x - r) = 1$, so $\deg h = 0$, so $h(x)$ is constant. Thus, $h(x) = f(r)$, so the remainder is indeed $f(r)$.

§C Appendix C: Real Roots

This section is dedicated to how do we know where a real (possibly irrational) root is. The first theorem is called the intermediate value theorem and is also used a lot in calculus:

Theorem C.1 (Intermediate Value Theorem)

Consider a **continuous** function $f : I \rightarrow \mathbb{R}$ for some interval $I = [a, b]$ (with $a < b$). Then, for all $c \in (f(a), f(b))$, we can find some $a < k < b$ such that $f(k) = c$.

Remark C.2. It isn't necessary $I = [a, b]$. It can be $[a, b)$, $(a, b]$, (a, b) as well. That's just how we talk about the intermediate value theorem in normal context.

Proof. Consider the set $S = \{x \mid x \in I, f(x) \leq c\}$, or all elements x in I such that $f(x) \leq c$. Now, we note that as $\min(f(a), f(b)) < c$ (by our assumption), so thus we can talk about the supremum of S , say k . We shall show $f(k) = c$. Otherwise, by the definition of continuity, we can find for all $\epsilon > 0$ some $\delta > 0$ such that

$$|f(x) - f(k)| \leq \epsilon, |x - k| \leq \delta$$

Now, consider the interval $(k - \delta, k + \delta)$. By our assumption, we have

$$f(x) - \epsilon < f(k) < f(x) + \epsilon$$

As f is the supremum, we must have for $x \in (k - \delta)$, we get

$$f(k) < f(x) + \epsilon \geq c + \epsilon$$

and for $x \in (k, k + \delta)$, we get

$$f(k) > f(x) > \epsilon > c - \epsilon$$

so thus for arbitrary $\epsilon > 0$, we have

$$c - \epsilon < f(k) < c + \epsilon$$

Now, by the Squeeze Theorem (or taking $\lim_{\epsilon \rightarrow 0}$), we get

$$f(k) = c$$

which is the theorem statement. □

Now, how does [Intermediate Value Theorem](#) help? Let's take a look at [2005 AIME I Problem 8](#). In particular, how did they know there were 3 real roots? Well, we note the function

$$f(x) = 2^{333x-2} + 2^{111x+2} - 2^{222x+2} - 1$$

is definitely continuous (essentially almost all functions are continuous, these can be visualized as being smooth graphs). So we will try to find some values of $f(x)$. We can make the following table:

$f(-\infty)$	-1
$f(0)$	1
$f(1)$	Really Huge Number

so that won't really work. We found guarantee of a root, but not 3. Let's try the substitution that motivates the solution of the problem:

$$g(y) = \frac{1}{4}y^3 - 2y^2 + 4y - 1$$

If we can find three positive roots of this, we should be done, right (as for any solution y we can take $x = \frac{1}{111} \log_2 x$? Let's make a table (I'm only including even values so I get even:

$f(0)$	-1
$f(2)$	1
$f(4)$	-1
$f(6)$	5

so we have a real root y in each of $(0, 2)$, $(2, 4)$, $(4, 6)$, so we have three positive integer roots by [Intermediate Value Theorem](#). This is also very helpful when using the rational root theorem - sometimes it isn't easy to do the division - but it's better to use this to find integer values and then find where there are roots for sure. Now, let's talk about this following magnificent result due Descartes:

Theorem C.3 (Descartes' Rule of Signs)

Consider a polynomial (with $\deg f = n \geq 1$)

$$f(x) = a_n \epsilon_n x^n + a_{n-1} \epsilon_{n-1} x^{n-1} + \cdots + a_0 \epsilon_0$$

where $a_n > 0$ and $\epsilon_n \in \{-1, 0, 1\}$. Let m be the number of times $\epsilon_k \epsilon_{k-1} = -1$. Then, the number of positive roots (say p) (counting multiplicities, i.e. the roots of $(x-1)^2$ are 1, 1) is at most m , and furthermore leaves the same remainder as m when divided by 2.

Remark C.4. This following heuristic argument helped me understand the argument (due to Professor Stewart A. Levin) - as x goes towards 0, the constant term comes into play, and as we move to $+\infty$, the leading term comes into play. In the middle the other ones have a chance to dominate, but sometimes are still dominated by other terms.

Proof due to Xiaoshen Wang. Divide by $a_n \epsilon_n$ (as it doesn't affect the product $\epsilon_k \epsilon_{k-1}$ as it is divided by 1) so thus

$$f(x) = x^n + a_{n-1} \epsilon_{n-1} x^{n-1} + \cdots + a_0 \epsilon_0$$

Now, if $\epsilon_0 = 0$, then we can "remove" it as it doesn't affect the number of positive roots. Thus, we also assume $\epsilon_0 \neq 0$. We have the following lemma:

Lemma C.5 — If $\epsilon_0 = 1$, then p is even. Otherwise, p is odd.

Proof. We note that at any root r , if it has odd multiplicity, then the function crosses the x -axis, while if it has even multiplicity, then it does not cross the x -axis. We note that if $\epsilon_0 = 1$, then $f(0) > 0$ and $f(\infty) > 0$, so thus we must have an even number of roots (counting multiplicities). Similarly, if $\epsilon_0 = -1$, then $f(0) < 0$ and $f(\infty) > 0$, so thus we must have an odd number of roots. ■

We shall prove this by induction on $\deg f$:

Base Case.

$n = 1$ is fairly obvious. If $\epsilon_0 > 0$, then by our Lemma, there are no real roots, and $\epsilon_0 \epsilon_1 = 1$. If $\epsilon_0 < 0$, then by our Lemma, there is one real root (as it is odd and at most 1 by the [Fundamental Theorem of Algebra](#)), and $\epsilon_0 \epsilon_1 = -1$.

Induction Hypothesis.

Assume for some positive integer k , the lemma is true for all polynomials f such that $\deg f \leq k$. We shall show the statement for $\deg f = k + 1$.

Induction Step.

Now, we have two cases:

Case 1. $\epsilon_0 \epsilon_q = 1$, where q is the least positive integer such that $\epsilon_q \neq 0$.

Then, we have by [Rolle's Theorem](#) (I'm too lazy to prove it),

$$f'(x)$$

$p' \geq p - 1$ and $m' \equiv p' \pmod{2}$ and $m' \geq p'$ (by the inductive hypothesis assuming that m' and p' have the same definition with respect to $f'(x)$). By our lemma, we have that considering it with $f(x)$ and $f'(x)$,

$p \equiv p' \pmod{2}$ (as ϵ_0, ϵ_q have the same sign), but then we get that

$$p \equiv p' \equiv m' = m \pmod{2}$$

Now, we only need to show that $m \geq p$, which is apparent as

$$p \leq p' + 1 \leq m' + 1 = m + 1$$

Case 2. $\epsilon_0 \epsilon_q = -1$, where q is the least positive integer such that $\epsilon_q \neq 0$.

Then, we have by **Rolle's Theorem** (I'm too lazy to prove it),

$$f'(x)$$

$p' \geq p - 1$ and $m' \equiv p' \pmod{2}$ and $m' \geq p'$ (by the inductive hypothesis assuming that m' and p' have the same definition with respect to $f'(x)$). By our lemma, we have that considering it with $f(x)$ and $f'(x)$, $p \equiv 1 + p' \pmod{2}$ (as ϵ_0, ϵ_q have the opposite sign), but then we get that

$$p \equiv p' + 1 \equiv m' + 1 = m \pmod{2}$$

Now, we only need to show that $m \geq p$, which is apparent as

$$p \leq p' + 1 \leq m' + 1 \leq m$$

□

So what about negative roots? We have the following corollary:

Corollary C.6 (Descartes' Rule of Sign's Corollary)

The number of negative roots is when we just apply $f(-x)$ to [Descartes' Rule of Signs](#) instead.

Now, this can provide upper bounds on the number of roots. For example, consider the following:

Example C.7

Find the number of nonreal roots of $f(x) = x^3 + 1$.

Solution. By [Descartes' Rule of Signs](#), we see that there are at most 0 positive roots. By [Descartes' Rule of Sign's Corollary](#), we see there are an odd number of negative roots and at most 1 negative root. Thus there is exactly 1 negative root, so exactly 1 real root. Thus there are 2 nonreal roots. □

Now, there is something that is very useful, and described as the discriminant. We touched on it in our discussion of [AIME I 2011/9](#) but didn't actually use it much. We will introduce it here:

Theorem C.8 (Discriminant of a Polynomial)

Define the discriminant of a polynomial is

$$\text{Disc}(p(x)) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (r_i - r_j)^2$$

where the leading coefficient of $p(x)$ is a_n , the degree is n , and the roots are r_1, r_2, \dots, r_n .

Note that this immediately implies that the discriminant is 0 if and only if two roots are equal. In addition, all roots are real if and only if the discriminant is nonnegative (the if part is hard to prove and out of scope - the only if part is very easy to prove). But how does this help? Well, let's see an example:

Corollary C.9 (Discriminant of a Quadratic Polynomial)

The discriminant of a quadratic polynomial $ax^2 + bx + c$ is

$$b^2 - 4ac$$

Proof. You may have seen something like this when dealing with the quadratic formula. Let's talk about it here. Let the roots be r_1, r_2 . By [Vieta's Formulas](#), we have that

$$\sigma_1 = r_1 + r_2 = -\frac{b}{a}$$

$$\sigma_2 = r_1 r_2 = \frac{c}{a}$$

Then, we get that

$$\text{Disc}(p(x)) = a^2(r_1 - r_2)^2$$

Let's expand this:

$$\text{Disc}(p(x)) = a^2(r_1^2 + r_2^2 - 2r_1 r_2)$$

We note that by [Newton's Formulas](#) (or #1 of [freeman66's tactics](#)), we get

$$\text{Disc}(p(x)) = a^2(\sigma_1^2 - 2\sigma_2 - 2\sigma_2) = a^2(\sigma_1^2 - 4\sigma_2)$$

Substituting, we get

$$\text{Disc}(p(x)) = b^2 - 4ac$$

□

Now, how can we get the discriminant without actually using the roots? We need the following definition:

Definition C.10 (Matrix of Two Polynomials) — Consider two polynomials $f(x)$ and $g(x)$, with degrees m and n . The resultant is the discriminant of the $(m+n) \times (m+n)$ matrix formed by writing the coefficients of $f(x)$ n times and the coefficients of $g(x)$ m times.

That's hard to imagine. We need an example:

Example C.11

Find the resultant of the polynomials $x^2 + 2x + 1$ and $2x + 2$.

Solution. Well, the resultant is the discriminant of

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 2 & 0 \\ 0 & 2 & 2 \end{pmatrix}$$

I know the definition is hard to grasp, but with this example it should be a lot easier. Anyways, we can compute the resultant to indeed be 0. □

How does this relate to anything? The following theorem says it all:

Theorem C.12 (Discriminants from Resultants)

The discriminant of the polynomial $p(x)$ is equal to

$$\frac{(-1)^{\binom{n}{2}}}{a_n} R(p, p')$$

where $R(p, p')$ is the resultant of $p(x)$ and $p'(x)$, $n = \deg p$, and a_n is the leading coefficient of p .

This is way too out of scope for me to present. Google it up if you want to see it. However, we can indeed once again check [Discriminant of a Quadratic Polynomial](#):

Corollary C.13 (Discriminant of a Quadratic Polynomial)

The discriminant of a quadratic polynomial $ax^2 + bx + c$ is

$$b^2 - 4ac$$

Proof. We have that $p'(x) = 2ax + b$, so

$$\text{Disc}(p(x)) = \frac{-1}{a} \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = -\frac{1}{a} (ab^2 + 4a^2c - 2ab^2) = b^2 - 4ac$$

□

The only other case that would be helpful would be a cubic. I am stating the result, but you can use [Discriminants from Resultants](#) for matrix bashing. Have fun!

Theorem C.14 (Discriminant of a Cubic Polynomial)

The discriminant of a cubic is given by

$$18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2.$$

I can't really think of a good time this would be useful, except maybe as for what we did for [2005 AIME I Problem 8](#) in the beginning of the Appendix.

§D Appendix D: Lagrange Interpolation Formula

This is an **addendum** to the Polynomial handout, added because it is occasionally useful.

Theorem D.1 (Lagrange Interpolation Formula)

For any distinct complex numbers x_0, \dots, x_n and any complex numbers y_0, \dots, y_n , there exists a unique polynomial $P(x)$ of degree less than or equal to n such that for all integers $0 \leq i \leq n$, $P(x_i) = y_i$, and this polynomial is

$$P(x) = \sum_{i=0}^n y_i \frac{(x - x_0) \cdots (x - x_{i-1})(x - x_{i+1}) \cdots (x - x_n)}{(x_i - x_0) \cdots (x_i - x_{i-1})(x_i - x_{i+1}) \cdots (x_i - x_n)}.$$

Example D.2 (USAMO 1975/3)

If $P(x)$ denotes a polynomial of degree n such that

$$P(k) = \frac{k}{k+1}$$

for $k = 0, 1, 2, \dots, n$, determine $P(n+1)$.

Solution. It is fairly natural to use Lagrange's Interpolation Formula on this problem:

$$\begin{aligned} P(n+1) &= \sum_{k=0}^n \frac{k}{k+1} \prod_{j \neq k} \frac{n+1-j}{k-j} \\ &= \sum_{k=0}^n \frac{k}{k+1} \cdot \frac{\frac{(n+1)!}{n+1-k}}{k(k-1)(k-2) \dots 1 \cdot (-1)(-2) \dots (k-n)} \\ &= \sum_{k=0}^n \frac{k}{k+1} (-1)^{n-k} \cdot \frac{(n+1)!}{k!(n+1-k)!} \\ &= \sum_{k=0}^n (-1)^{n-k} \binom{n+1}{k} - \sum_{k=0}^n \frac{(n+1)!(-1)^{n-k}}{(k+1)!(n+1-k)!} \\ &= - \left(\sum_{k=0}^{n+1} (-1)^{n+1-k} \binom{n+1}{k} - 1 \right) + \frac{1}{n+2} \cdot \sum_{k=0}^n (-1)^{n+1-k} \binom{n+2}{k+1} \\ &= 1 + \frac{1}{n+2} \left(\sum_{k=-1}^{n+1} (-1)^{n+2-(k+1)} \binom{n+2}{k+1} - (-1)^{n+2} - 1 \right) \\ &= \boxed{1 - \frac{(-1)^n + 1}{n+2}}. \end{aligned}$$

□

Example D.3 (USAMO 1984/5)

$P(x)$ is a polynomial of degree $3n$ such that

$$\begin{aligned} P(0) = P(3) = \dots &= P(3n) = 2, \\ P(1) = P(4) = \dots &= P(3n-2) = 1, \\ P(2) = P(5) = \dots &= P(3n-1) = 0, \quad \text{and} \\ &P(3n+1) = 730. \end{aligned}$$

Determine n .

Solution. By Lagrange Interpolation Formula,

$$f(x) = 2 \sum_{p=0}^n \left(\prod_{0 \leq r \neq 3p \leq 3n} \frac{x-r}{3p-r} \right) + \sum_{p=1}^n \left(\prod_{0 \leq r \neq 3p-2 \leq 3n} \frac{x-r}{3p-2-r} \right),$$

and hence

$$f(3n+1) = 2 \sum_{p=0}^n \left(\prod_{0 \leq r \neq 3p \leq 3n} \frac{3n+1-r}{3p-r} \right) + \sum_{p=1}^n \left(\prod_{0 \leq r \neq 3p-2 \leq 3n} \frac{3n+1-r}{3p-2-r} \right).$$

After some calculations we get

$$f(3n+1) = \left(\binom{3n+1}{0} - \binom{3n+1}{3} + \binom{3n+1}{6} - \dots \right) (2 \cdot (-1)^{3n} - 1) + 1.$$

Given $f(3n+1) = 730$ so we have to find n such that

$$\left(\binom{3n+1}{0} - \binom{3n+1}{3} + \binom{3n+1}{6} - \dots \right) (2 \cdot (-1)^{3n} - 1) = 729.$$

Lemma. If p is even, then

$$\binom{p}{0} - \binom{p}{3} + \binom{p}{6} - \dots = \frac{2^{p+1} \sin^p \left(\frac{\pi}{3} \right) (i)^p \left(\cos \left(\frac{p\pi}{3} \right) \right)}{3},$$

and if p is odd,

$$\binom{p}{0} - \binom{p}{3} + \binom{p}{6} - \dots = \frac{-2^{p+1} \sin^p \left(\frac{\pi}{3} \right) (i)^{p+1} \left(\sin \left(\frac{p\pi}{3} \right) \right)}{3}.$$

(We will not discuss the proof of this lemma in this handout - the idea is **Roots of Unity Filter**.) Using the above lemma, we do not get any solutions when n is odd, but when n is even, $3n+1 = 13$ satisfies the required condition, implying $n = \boxed{4}$ is the only solution. \square

Exercise D.4 (USAMO 2002/3). Prove that any monic polynomial (a polynomial with leading coefficient 1) of degree n with real coefficients is the average of two monic polynomials of degree n with n real roots.

Exercise D.5 (AIME I 2015/10). Let $f(x)$ be a third-degree polynomial with real coefficients satisfying

$$|f(1)| = |f(2)| = |f(3)| = |f(5)| = |f(6)| = |f(7)| = 12.$$

Find $|f(0)|$.

Exercise D.6 (HMMT February Algebra and Number Theory 2017/6). A polynomial P of degree 2015 satisfies the equation $P(n) = \frac{1}{m^2}$ for $n = 1, 2, \dots, 2016$. Find $\lfloor 2017P(2017) \rfloor$.

§E Appendix E: List of Theorems, Corollaries, and Definitions

List of Theorems

2.1	Theorem - Fundamental Theorem of Algebra	5
2.8	Theorem - Unique Factorization of Polynomials	5
2.10	Theorem - Factor Theorem	6
2.11	Theorem - Remainder Theorem	6

2.19 Theorem - Rational Root Theorem	8
3.7 Theorem - Vieta's Formulas	11
3.9 Theorem - Binomial Theorem	11
4.3 Theorem - Fundamental Theorem of Symmetric Polynomials	13
4.5 Theorem - Newton's Formulas	13
5.13 Theorem - Complex Conjugate Theorem	18
5.18 Theorem - De Moivre's Theorem	20
5.19 Theorem - Euler's Formula	20
5.21 Theorem - De Moivre's Theorem	20
6.1 Theorem - Difference of Polynomials	23
A.1 Theorem - Fundamental Theorem of Algebra	39
A.2 Theorem - Liouville's Theorem	39
A.3 Theorem - Fundamental Theorem of Symmetric Polynomials	39
C.1 Theorem - Intermediate Value Theorem	42
C.3 Theorem - Descartes' Rule of Signs	44
C.8 Theorem - Discriminant of a Polynomial	45
C.12 Theorem - Discriminants from Resultants	47
C.14 Theorem - Discriminant of a Cubic Polynomial	47
D.1 Theorem - Lagrange Interpolation Formula	47

List of Corollaries

2.5 Corollary - Number of Roots Corollary	5
2.7 Corollary - Zero Polynomial Corollary	5
C.6 Corollary - Descartes' Rule of Sign's Corollary	45
C.9 Corollary - Discriminant of a Quadratic Polynomial	46
C.13 Corollary - Discriminant of a Quadratic Polynomial	47

List of Definitions

4.1	Definition - Elementary Symmetric Polynomial	13
4.2	Definition - k -Variable Symmetric Polynomial	13
5.1	Definition - Complex Number	16
5.2	Definition - Conjugate	16
5.9	Definition - Modulus/Magnitude	17
5.24	Definition - Roots of Unity	21
C.10	Definition - Matrix of Two Polynomials	46