As it turns out, there's more to algebra than pure uninspiring symbol pushing. In this chapter we look at some structures and concepts in elementary algebra.

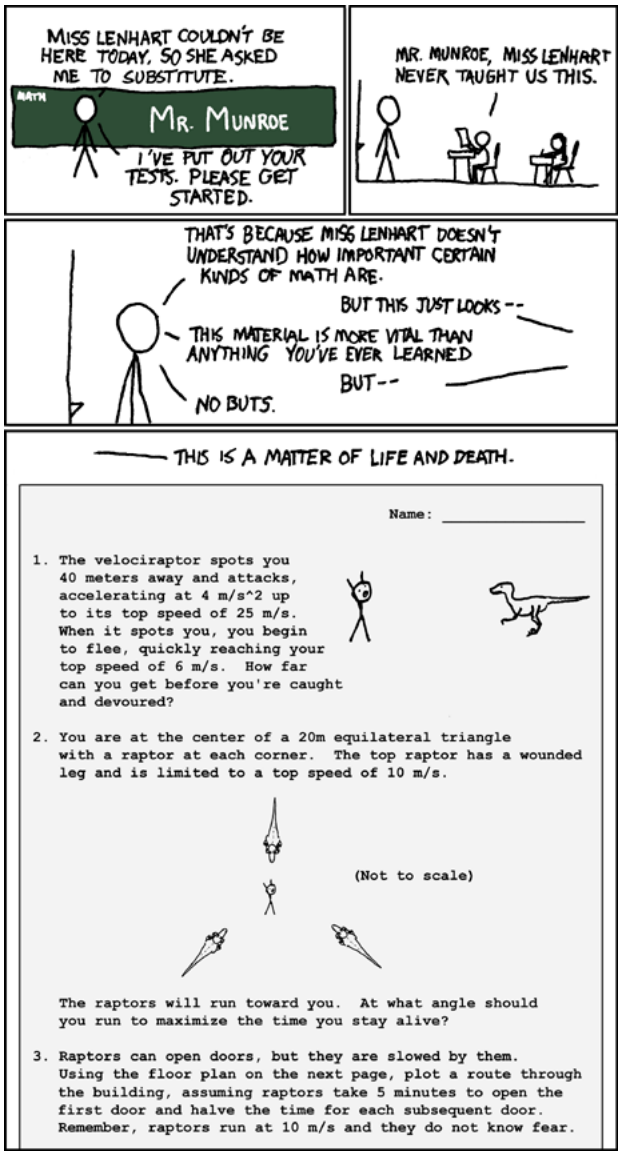

Figure 1: Comic from https://xkcd.wtf/135/

0.1 Proving and Thinking

0.1.1 Proof by Contradiction

Our first question showcases the powerful *proof by contradiction*. It is mostly used when a direct proof is less feasible, and so is an indirect approach to a problem.

The main idea is to begin with an (absurd) assumption and working towards deriving a contradiction. In other words, we are establishing the truth of a claim by assuming that the claim is false, and then showing that this leads to a contradiction. Also known as *reductio ad absurdum*.

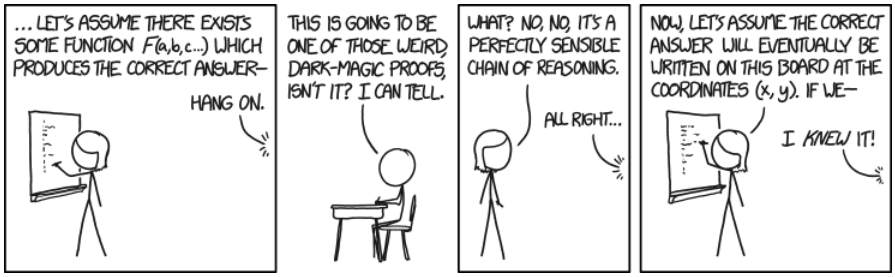

Figure 2: Comic from https://xkcd.wtf/1724/

Example 0.1 (Classic)
Let a, b be integers. We say that an integer is *tasty* if it is expressible in the form $a^2 + ab + b^2$. Prove that 2 is not tasty.

Classically, $a^2 + ab + b^2$ is a so-called quadratic form. This suggests a direct proof is not feasible: enter the realm of contradictions.

Proof. We first suppose for the sake of contradiction that 2 is expressible in this form. Then we have, for some a, b:

$$a^2 + ab + b^2 = 2 \implies (2a + b)^2 + 3b^2 = 8.$$

Now, the problem falls to simple casework: neither $b^2 = 0$, $b^2 = 1$ nor $b^2 = 4$ is possible, but we assumed initially that 2 is tasty! Since a wrong assumption resulted in an absurd conclusion, this means that our initial assumption must be wrong. In other words, 2 is not tasty. □

Another classical example is on the irrationality of $\sqrt{2}$.

Example 0.2 (Classic)
Prove that $\sqrt{2}$ is irrational.

Proof. As again, we suppose on the contrary that $\sqrt{2}$ is rational, so $\sqrt{2} = \frac{m}{n}$ where $\gcd(m, n) = 1$ (this just means that $\sqrt{2}$ can be expressed as a fraction in simplest terms).

Squaring,

$$2 = \frac{m^2}{n^2} \implies 2n^2 = m^2.$$

Hence, $2|m \implies 4|m^2$ and so $2|n^2$. However, this is a contradiction because we initially defined $\gcd(m, n) = 1$!

This means that our initial assumption that $\sqrt{2}$ is rational was wrong. In other words, $\sqrt{2}$ is irrational. □

0.1.2 Induction

Formally, for a proposition $P(n)$, $n \in \mathbb{Z}^+$, if $P(1)$ is true and $P(k)$ is true $\implies$ $P(k + 1)$ is true for some $k \in \mathbb{Z}^+$, then $P(n)$ is true $\forall\ n \in \mathbb{Z}^+$.

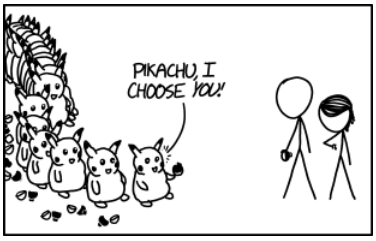

Figure 3: Comic from https://xkcd.wtf/1516 - Win by Induction

Intuitively, this can be think of as a chain effect in a dominoes setup: if an arbitrary proposition being true implies the succeeding tile proposition is true, then the corresponding tile topples its succeeding tile, which in turn topples the next tile, and so on - except we have infinitely many domino tiles.

All of these toppling, however, is subject to a condition: the base case must be true. That is, the first tile must be knocked over for this chain effect of tiles toppling over each other to start. This is the so-called *base case*.

Suppose we wish to prove that the proposition $P(n)$ is true for all $n \in \mathbb{Z}^+$, then the corresponding inductive proof follows a structure.

1. Base case: Establish that $P(1)$ is true.
2. Inductive hypothesis/assumption: Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{Z}^+$.
3. Inductive step: Prove that $P(k)$ being true implies $P(k+1)$ is true.
4. Conclude: Since $P(1)$ is true and $P(k)$ being true implies $P(k+1)$ is true, then $P(n)$ is true for all n (this is called the Principle of Mathematical Induction).

This structure holds for most cases, although care must be taken in establishing the base case. If the given proposition holds over a different domain, say $n \geq 2$ instead of $n \geq 1$, then the base case will be $P(2)$ instead of $P(1)$.

Let us now showcase some applications of the induction technique. In general, most textbook proofs by induction do not follow this strict structure and merely outline the inductive step. For starters, we shall follow closely the structure given above.

Example 0.3 (Classic)
Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{Z}^+$.

Proof. Let $P(n)$ denote the proposition that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for $n \in \mathbb{Z}^+$.

1. Base case: LHS of $P(1)$=1 and RHS of $P(1) = \frac{1(1+1)}{2} = 1$, so $P(1)$ is true.
2. Inductive hypothesis: Suppose that $P(k)$ is true for some $k \geq 0$. That is, assume that $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$.
3. Inductive step: To prove $P(k+1)$ is true, we begin with the LHS. This is because we can easily make use of the inductive hypothesis (keep an eye out for whenever you can use it!)

$$\begin{aligned} 1 + 2 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) && \text{by inductive hypothesis} \\ &= \frac{(k+1)(k+2)}{2} = \text{RHS of } P(k+1). \end{aligned}$$

□

Example 0.4 (Classic)
Prove that, for all integers $n \geq 0$ and real x, $|\sin nx| \leq n|\sin x|$.

Proof. Let $P(n)$ denote the proposition that $|\sin nx| \leq n|\sin x|$ for integers $n \geq 0$. Note that now, the base case is $n = 0$ instead of $n = 1$!

1. Base case: LHS of $P(0)$=0 and RHS of $P(0) = 0 \sin 0 \cdot x$=0, so $P(1)$ is true.
2. Inductive hypothesis: Suppose that $P(k)$ is true for some $k \geq 0$. That is, assume that $|\sin kx| \leq k|\sin x|$
3. Inductive step: To prove $P(k+1)$ is true, we again begin with the LHS.

$$\begin{aligned}
|\sin(k+1)x| &= |\sin kx \cos x + \cos kx \sin x| \\
&\leq |\sin kx \cos x| + |\cos kx \sin x| && \text{by triangle inequality} \\
&= |\sin kx||\cos x| + |\cos kx||\sin x| \\
&\leq k|\sin x||\cos x| + |\cos kx||\sin x| && \text{by inductive hypothesis} \\
&\leq k|\sin x| + |\sin x| \\
&= (k+1)|\sin x| = \text{RHS of } P(k+1)
\end{aligned}$$

□

To end off the section on induction, we show an unorthodox way to finish the inductive step. It's not always the case that we can simply move from LHS to RHS!

Example 0.5 (2021 H2 Further Math P1 Q4)
For real x and any positive integer n, the function F_n is defined by

$$F_n(x) = \frac{x(x+1)(x+2)\cdots(x+n-1)}{n!}.$$

Prove by induction that, for all positive integers n, $F_n\left(\frac{1}{2}\right) < \frac{1}{\sqrt{2n+1}}$.

The base case is simple, so we focus on the inductive assumption first. For the moment, write $x = \frac{1}{2}$ and assume that $F_k(x) < \frac{1}{\sqrt{2k+1}}$ (this is our inductive hypothesis!).

We have

$$\begin{aligned}
F_{k+1}(x) &= \frac{x(x+1)(x+2)\cdots(x+k-1)}{k!} \cdot \frac{x+k}{k+1} && \text{by inductive hypothesis} \\
&< \frac{1}{\sqrt{2k+1}} \cdot \frac{2k+1}{2(k+1)} \\
&= \frac{2k+1}{2(k+1)\sqrt{2k+1}}
\end{aligned}$$

How do we proceed? To start, we know that $\frac{2k+1}{2(k+1)} < 1$, but that gives $F_{k+1}(x) < \frac{1}{\sqrt{2k+1}}$, no good. On the other hand, our required form is $F_{k+1}(x) < \frac{1}{\sqrt{2k+3}}$, so the naive student may attempt to claim $\frac{1}{\sqrt{2k+1}} < \frac{1}{\sqrt{2k+3}}$, but this is not true!!

To this end, we try the most obvious thing possible: we want $F_{k+1}(x) < \frac{1}{\sqrt{2k+3}}$, so it would be great if we have $\frac{2k+1}{2(k+1)\sqrt{2k+1}} < \frac{1}{\sqrt{2k+3}}$. Trying our luck:

$$\begin{aligned}\frac{2k+1}{2(k+1)\sqrt{2k+1}} < \frac{1}{\sqrt{2k+3}} &\iff (2k+1)\sqrt{2k+3} < 2(k+1)\sqrt{2k+1} \\ &\iff (4k^2+4k+1)(2k+3) < (4k^2+8k+4)(2k+1) \\ &\iff 3(4k^2)+4k(2k+3)+(2k+3) < 4k^2+8k(2k+1)+4(2k+1) \\ &\iff 14k+3 < 16k+4 \iff k > \frac{1}{2}\end{aligned}$$

Miraculously, our high power terms cancel off! The astute reader will realise that we used "left-right" arrows instead of the usual "right" arrow. This "left-right" arrow indicates that the preceding line implies the next line, and the next line implies the preceding line. This means that our steps are **reversible**, so we can simply retrace our steps from the last line all the way back to the first line. This completes our induction proof, since the domain of our proposition is $k > 1$.

The reader is encouraged to furnish a cleaned induction proof, unlike the one we have just shown. It is, however, the case that most induction proofs are found in this form, where only the inductive step is shown.

Tangent: Central Binomial Coefficient We should probably be suspicious about why the cubic and quadratic terms in our inequalities cancel. Although, we should be equally suspicious about the choice of $x = \frac{1}{2}$. The function is defined for all real x, so why this specific rational number?

We start by expanding

$$F_n\left(\frac{1}{2}\right) = \frac{\frac{1}{2}\frac{3}{2}\frac{5}{2}\cdots\frac{2(n-1)+1}{2}}{n!} = \frac{1\cdot 3\cdot 5\cdots(2n-1)}{2^n n!}.$$

Moreover, the product of the even integers: $2\cdot 4\cdots 2n = \frac{(2n)!}{2^n}$, so

$$F_n\left(\frac{1}{2}\right) = \frac{1}{2^{2n}}\frac{(2n)!}{n!n!} = \frac{1}{2^{2n}}\binom{2n}{n}.$$

As it turns out, $\binom{2n}{n}$ is the so-called **central binomial coefficient** (why?).

The bound in the question asserts that $\binom{2n}{n} < \frac{4^n}{\sqrt{2n+1}}$, however Erdos argues that the best (asymptotic) bound is $\binom{2n}{n} < \frac{4^n}{\sqrt{\pi n}}$, as we will derive.

The binomial coefficient arises in binomial expansions, so we shall consider a suitable one. For this, we look to the related binomial expansion for cosine. In particular, letting $z = e^{it}$, we have $\cos t = \frac{1}{2}\left(z + \frac{1}{z}\right)$, and

$$\begin{aligned}\cos^{2n} t &= \frac{1}{2^{2n}}\sum_{k=0}^{2n}\binom{2n}{k} z^{2n-2k} \\ &= \frac{1}{2^{2n}}\sum_{k=0}^{2n}\binom{2n}{k}\cos(2n-2k)t + \frac{i}{2^{2n}}\sum_{k=0}^{2} n\binom{2n}{k}\sin(2n-2k)t\end{aligned}$$

Note that since $\cos^{2n} t$ is real, the imaginary part vanishes. Moreover,

$$\binom{2n}{k}\cos(2n-2k)t + \binom{2n}{2n-k}\cos(2k-2n)t = 2\binom{2n}{k}\cos(2n-2k)t \text{ by symmetry.}$$

Hence,

$$\begin{aligned}
\cos^{2n} t &= \frac{1}{2^{2n}} \sum_{k=0}^{2n} \binom{2n}{k} z^{2n-2k} \\
&= \frac{1}{2^{2n}} \sum_{k=0}^{2n} \binom{2n}{k} \cos{(2n-2k)t} + \frac{i}{2^{2n}} \sum_{k=0}^{2n} \binom{2n}{k} \sin{(2n-2k)t} \qquad \text{by de Moivre's theorem} \\
&= \frac{1}{2^{2n}} \sum_{k=0}^{2n} \binom{2n}{k} \cos{(2n-2k)t} \\
&= \frac{1}{2^{2n}} \left(\binom{2n}{n} + 2 \sum_{k=1}^{n-1} \binom{2n}{k} \cos{(2n-2k)t} \right)
\end{aligned}$$

The substitution $j = n - k$ gives

$$\cos^{2n} t = \frac{1}{2^{2n}} \left(\binom{2n}{n} + 2 \sum_{j=1}^{n} \binom{2n}{n-j} \cos 2jt \right) \implies \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^{2n} t \, dt = \frac{\pi}{2^{2n}} \binom{2n}{n}.$$

Thus, we have the chain of bounds:

$$\begin{aligned}
\binom{2n}{n} &= \frac{4^n}{\pi} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^{2n} x \, dx < \frac{4^n}{\pi} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} e^{-nx^2} \, dx \qquad (1) \\
&< \frac{4^n}{\pi} \int_{-\infty}^{\infty} e^{-nx^2} \, dx = \frac{4^n}{\sqrt{\pi n}} \qquad (2)
\end{aligned}$$

0.2 Polynomials

Outside of quadratic polynomials, there are also cubics, quartics, quintics, sextics..., that most students assume are extinct. However, they can be found in a select number of natural hideouts!

0.2.1 Quadratics

In this section, we will revisit the common quadratic polynomials. The techniques for quadratics aren't many. The usual few are the discriminant and completing the square, none of which are totally unexpected or inspiring. However, they are still useful-ish in extracting information from a given problem. We hope it suffices!

Example 0.6 (2010-2011 Mandelbrot)
Let $P(x) = x^3 + ax^2 + bx + c$ be a polynomial with three distinct roots. The polynomial P(Q(x)), where $Q(x) = x^2 + x + 2001$, has no real roots. Prove that $P(2001) > \frac{1}{64}$.

This is a strange idea: given the number of roots of a polynomial, what can we deduce about it's value?

Proof. For starters, let p, q, r be the three distinct roots of P, then $P(x) = (x-p)(x-q)(x-r)$ and let z be a complex root of $P(Q(x))$ so that $P(Q(z)) = 0$.

Hence, $Q(z) = p$ or q or r. Without loss of generality,

$$Q(z) = p \implies z^2 + z + (2001 - p) = 0.$$

However, there are no real values of z that satisfy this condition! This next step would be glaring: by considering the discriminant,

$$\Delta = 1 - 4(2001 - p) < 0 \implies p < \frac{8003}{4}.$$

Since we initially assumed without loss of generality that $Q(z) = p$, this conclusion should also hold for q, r, that is $p, q, r < \frac{8003}{4}$.

Finally,

$$\begin{aligned} P(2001) = (2001 - p)(2001 - q)(2001 - r) &> \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{1}{4} \\ &= \frac{1}{64} \end{aligned}$$

□

Next, we consider a quadratic with coefficients that form an arithmetic progression. As it turns out, if the quadratic has a unique root, then we can uniquely determine this root!

Example 0.7 (2013 AMC 10B P19)

Let c, b, a be real numbers form an arithmetic progression with $a \geq b \geq c \geq 0$. The quadratic $ax^2 + bx + c = 0$ has exactly one root. Find this root.

First step! The discriminant: $\Delta = b^2 - 4ac = 0$, implying that the only root is $x = \frac{-b}{2a}$ by considering the quadratic formula.

Proof. Since c, b, a have common differences with b being the median element, we may write $c = b + (b - a) = 2b - a$ so that

$$b^2 - 4ac = b^2 - 4a(2b - a) = b^2 - 8ab + 4a^2 = 0 \implies b = 4a \pm 2a\sqrt{3}.$$

Yet, we are given that $a \geq b$, so surely $b = 4a - 2a\sqrt{3}$, giving $x = -\frac{b}{2a} = \boxed{-2 + \sqrt{3}}$. □

0.2.2 The Rare Types

Contrary to popular belief, there are higher degree polynomials in the wild. We first consider some identities associated with the coefficients of a general polynomial.

Consider a general polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

with real coefficients $\{a_n\}$. Then, the

1. constant term is $P(0)$,
2. sum of coefficients is $P(1)$,
3. sum of *odd-power* coefficients is $\frac{P(1) - P(-1)}{2}$,
4. sum of *even-power* coefficients is $\frac{P(1) + P(-1)}{2}$.

The reader is strongly encouraged to derive the four properties above!

For the other coefficients, there are other higher-powered techniques (pun fully intended) to deal with them, but we will not introduce them here (for the interested, see the roots of unity filter).

We are guessing the student is familiar with the so-called "sum and product of roots" for a quadratic, and here, we introduce a generalisation - we have similar relations for higher-degree polynomials! This is given by Vieta's Theorem.

Proposition 0.8 (Vieta's Theorem)

A general polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with real coefficients $\{a_n\}$ and real and complex roots $r_1, r_2, \cdots r_n$ has the following relations:

$$r_1 + r_2 + \cdots + r_n = -\frac{a_{n-1}}{a_n}$$
$$(r_1r_2 + r_1r_3 + \cdots + r_1r_n) + (r_2r_3 + r_2r_4 + \cdots + r_2r_n) + \cdots + r_{n-1}r_n = \frac{a_{n-2}}{a_n}$$
$$r_1r_2\cdots r_n = (-1)^n \frac{a_0}{a_n}$$

In general, the *sum of roots taken k at a time* is given by $(-1)^k \frac{a_{n-k}}{a_n}$. Each of these sums are also known as *elementary symmetric polynomials*.

Let us show some examples of Vieta's theorem in action.

Example 0.9 (2001 All-Russian Olympiad)

The equation $(x - \sqrt[3]{13})(x - \sqrt[3]{53})(x - \sqrt[3]{103}) = \frac{1}{3}$ has three distinct roots r, s, t. Find the value of $r^3 + s^3 + t^3$.

First of all... yikes! Cube roots and cubes. However, it seems that the three cube roots look arbitrary: while the answer depends on their values, we can find an expression for $r^3 + s^3 + t^3$ in terms of these cube roots without caring about their values just yet.

Proof. We make the substitution $\alpha = \sqrt[3]{13}$, $\beta = \sqrt[3]{53}$, $\gamma = \sqrt[3]{103}$.

Now our equation is transformed into $(x - \alpha)(x - \beta)(x - \gamma) - \frac{1}{3} = 0$. By Vieta's theorem,

$$r + s + t = a + b + c$$
$$rs + st + rt = ab + bc + ca$$
$$rst = abc - \frac{1}{3}.$$

Now, how do we use this to our advantage to find $r^3 + s^3 + t^3$? For starters, we may expand

$$(r + s + t)^3 = r^3 + s^3 + t^3 + 3r^2s + 3r^2t + 3rs^2 + 3rt^2 + 3s^2t + 3st^2 + 6rst.$$

We're close to finding something substantial - if we can simplify the sum of the terms in the form m^2n. A natural way to do this is to expand

$$(r + s + t)(rs + st + rt) = r^2s + r^2t + rs^2 + rt^2 + s^2t + st^2 + 3rst.$$

Aha! Now our expression simplifies nicely:

$$(r + s + t)^3 = r^3 + s^3 + t^3 + 3(r + s + t)(rs + st + rt) - 3rst,$$

whence upon arranging, we have

$$\begin{aligned} r^3+s^3+t^3 &= (\alpha+\beta+\gamma)^3-3(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha)+3(\alpha+\beta+\gamma+\frac{1}{3}) \\ &= (\alpha+\beta+\gamma)^3-3(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha)+3(\alpha+\beta+\gamma)+1 \\ &= \alpha^3+\beta^3+\gamma^3+1 \\ &= \boxed{170} \end{aligned}$$

□

Example 0.10 (2019 AIME I P10)

For complex numbers $z_1, z_2, \cdots z_{673}$, 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 polynomials and of degree *at most* 2016. Find the value of

$$\sum_{1\le j\le k\le 673} z_j z_k.$$

The sum requested of us is an elementary symmetric polynomial, so we would expect to use Vieta's theorem in some way.

Let S, P denote the sum of roots one and twice at a time respectively and let $Q(x)$ denote the given polynomial. Note that the required sum is P. Since it's weird that the given polynomial is cubed throughout, we shall consider

$$p(x) = (x-z_1)(x-z_2)\cdots(x-z_{673}) = x^{673}-Sx^{672}+Px^{671}+\cdots$$

Thus, $Q(x)=[p(x)]^3$. To find S and P, we shall expand this to find the coefficients of x^{2018} and x^{2017}. To do this quickly, we consider how terms in 3 products can be multiplied together to give the relevant terms.

To wit,

1. x^{2019} can only be formed by multiplying all three x^{673}, and there is only 1 way to do this.
2. x^{2018} can be formed by multiplying two x^{673} and one Sx^{672}, and there are $\binom{3}{1}=3$ ways to do this.
3. x^{2017} can be formed by multiplying two x^{673} and one Px^{671}, and there are $\binom{3}{1}=3$ ways to do this. It can also be formed by multiplying one x^{673} and two Sx^{672}, giving 3 ways as well.

Proof. We now have,

$$\begin{aligned} Q(x)=[p(x)]^3 &= (x^{673}-Sx^{672}+Px^{671}+\cdots)(x^{673}-Sx^{672}+Px^{671}+\cdots)(x^{673}-Sx^{672}+Px^{671}+\cdots) \\ &= x^{2019}-3Sx^{2018}+3(P+S^2)x^{2017}+g(x), \end{aligned}$$

and thus

$$\begin{cases} -3S=20 \\ 3(P+S^2)=19 \end{cases} \Rightarrow \begin{cases} S=-\frac{20}{3} \\ P=-\frac{343}{9} \end{cases}.$$

Hence, $\boxed{P=-\frac{343}{9}}$. □

At this point, it's only complete if we also derive some common algebraic identities and factorisations.

Proposition 0.11 (Classic)

In what follows, assume the summation run over $x_1, x_2, \cdots, x_n$.

1. For the bivariate $x^2+y^2=(x+y)^2-2xy$, we also have the three-variable relation
$$x^2+y^2+z^2=(x+y+z)^2-2(xy+yz+zx).$$
In general,
$$\left(\sum x_i\right)^2=\sum x_i^2-2\left(\sum_{1\le i\le q\le n} x_ix_j\right).$$
2. $x^3+y^3+z^3-3xyz=\frac{1}{2}(x+y+z)[(x-y)^2+(y-z)^2+(z-x)^2]$.
3. Sophie-Germain Identity: $a^4+4b^4=(a^2+2b^2+2ab)(a^2+2b^2-2ab)$.
4. Lagrange's Identity: $(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2=(ac+bd)^2+(ad-bc)^2$
5. $(a+b)^3-(a^3+b^3)=3ab(a+b)$.
6. $(a+b)^5-(a^5+b^5)=5ab(a+b)(a^2+ab+b^2)$.
7. $(a+b)^7-(a^7+b^7)=7ab(a+b)(a^2+ab+b^2)^2$.
8. My personal favourite: $\frac{(a^2+bc)(b^2+ac)}{(a+c)(b+c)}+\frac{(a^2+bc)(c^2+ab)}{(a+b)(b+c)}+\frac{(b^2+ac)(c^2+ab)}{(a+b)(a+c)}=a^2+b^2+c^2$

For the final problem of this chapter, we shall prove identity 7.

Example 0.12 (Classic)

Factorise $(a+b)^7-(a^7+b^7)$.

Proof. Certainly we need some observations to reduce this problem into a more tractable form. We note that $a=0$ or $b=0$ make the expression vanish, so ab is a factor of the expression. Moreover, since the degrees on a,b are odd, $a=-b$ also causes the expression to vanish. Thus, $a+b$ is also a factor.

Thus, the expression is a polynomial that readily decomposes into the factor $ab(a+b)$ of degree 3 and another factor of degree 4 (or possibly more factors).

Let a,b,c be roots of the cubic with $c=-(a+b)$ such that

$$\begin{cases} A &= a+b+c=0 \\ B &= ab+bc+ca=-(a^2+b^2+ab) \\ C &= abc=-ab(a+b) \end{cases},$$

whence the cubic is

$$x^3+Bx-C=(x-a)(x-b)(x-c).$$

This gives $a^2+b^2+c^2=(a+b+c)^2-2(ab+bc+ca)=-2B$ We now "lift" the power up to x^7. Suppose t is one of a,b,c. Thus, we have

$$t^7=t(C-Bt)^2=B^2t^3-2BCt^2+C^2t \tag{3}$$

$$= B^2(C - Bt) - 2BCt^2 + C^2t \tag{4}$$
$$= -2BCt^2 + (C^2 - B^3)t + B^2C \tag{5}$$

Summing (5) over $t = a, b, c$,

$$\begin{aligned} a^7 + b^7 - (a+b)^7 &= -2BC(-2B) + 3B^2C \\ &= 7B^2C = -7ab(a+b)(a^2+ab+b^2)^2 \end{aligned}$$

whence

$$(a+b)^7 - (a^7 + b^7) = 7ab(a+b)(a^2+ab+b^2)^2.$$

□

Sometimes a polynomial is also hard to factorise, but the Rational Root Theorem is extremely useful to help us discover any potential linear factors and rational roots.

Proposition 0.13 (Rational Root Theorem)
For a polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with real coefficients $\{a_n\} = 0$, if $P(x)$ *has a rational root* $x = \frac{p}{q}$ where $\gcd(p, q) = 1$, then

- p is an integer factor of the constant term a_0, and
- q is an integer factor of the leading coefficient a_n.

It is important to point out that this **does not** guarantee that $P(x)$ has a rational root. It merely proposes that there are candidates.

0.3 Some Solving

Many questions will demand you to "find all X satisfying condition Y", the keyword being **find all**. These problems come in solving equations, functional equations, inequalities, etc. This implies that there are two parts to the problem:

1. Find the solutions and show that no other solutions exist.
2. Prove that your solutions satisfy the condition (this is part of the problem!).

It will be more instructive for us to work through a problem.

Example 0.14 (2021 SMO(O) P10)
Find all real roots to the equation

$$\sqrt[9]{x^7 + 30x^5} = \sqrt[7]{x^9 - 30x^5}.$$

As a first scout, we see that $x = 0$ is a solution. Moreover, if $x = k$ is a solution, then so is $x = -k$, so we may consider only $x > 0$.

Proof. Let $a = \sqrt[9]{x^7 + 30x^5}$, $b = \sqrt[7]{x^9 - 30x^5}$ so that

$$\begin{cases} a - b = 0 \\ a^9 + b^7 = x^{16} \end{cases} \implies a^{16} = x^{16} \implies a = \pm x.$$

If $a = x$, then $a^9 = a^7 + 30a^5$.

Aha! This gives our first solution $a = 0$, corresponding to $x = 0$. In what follows, we assume $x \neq 0 \implies a \neq 0$.

Thus, $a^4 = a^2 + 30 \implies (a^2 - 6)(a^2 - 5) = 0 \implies a = \pm\sqrt{5}, a = \pm\sqrt{6}$.

Now, are all of these valid solutions? We should verify so. Suppose $a = x = \sqrt{5}$ (since we have $x > 0$), then

$$a^9 = 625\sqrt{5} = 125\sqrt{5} + 750\sqrt{5} = 875\sqrt{5},$$

which is a contradiction. Thus $x \neq \sqrt{5}$.

Remark 0.15. Notice the use of proof by contradiction here! We assumed that $x = \sqrt{5}$ is a solution, and then derived the absurd statement that $625\sqrt{5} = 875\sqrt{5}$.

Similarly, suppose $a = x = \sqrt{6}$, then $a^9 = 1296\sqrt{6} = 216\sqrt{6} + 1080\sqrt{6}$, which is consistent. Hence, $a = \sqrt{6}$ is the solution we're after. Having exhausted all cases, and verified that our solution was correct, we can now confidently say that the only solutions to the original equation are

$$\boxed{x = 0,\ \sqrt{6} \text{ and } -\sqrt{6}}.$$

□

Example 0.16 (2021 SMO(S) P22)

Find all real solutions (x, y) to the system

$$x^3 + y^3 + y^2 = 0 \tag{6}$$
$$x^2 + x^2y + xy^2 = 0 \tag{7}$$

This is a tough system: both equations are cubic in nature. As an initial scout, it's wise to guess a few solutions: since x is the "lone variable" in equation 2, letting $x = 0$ gives $y = 0, -1$. We also see that $x = y$ is another solution. In particular, if $x = y$, we have

$$2y^3 + y^2 = 0 \implies y = 0, -\frac{1}{2}.$$

Thus, we immediately have the solutions $(0, 0)$, $(0, -1)$ and $(0, -\frac{1}{2})$, and we know these are (likely) all the solutions because the system has degree 3 (we still need to verify whether there are other nontrivial classes of solution).

Proof. To start, we see that (7) is a quadratic in x, so $x^2(1 + y) + xy^2 = 0$. If $x = 0$, then we get the three solutions as above. If $y = -1$ in (6), we have $x = 0$, as above. So, suppose $x \neq 0, y \neq -1$, then

$$x(1 + y) + y^2 = 0 \implies x = -\frac{y^2}{1 + y}.$$

Putting this into (6),

$$-\frac{y^6}{(1 + y)^3} + y^2(1 + y) = 0 \implies \frac{-y^6 + y^2(1 + y)^3}{(1 + y)^4} = 0 \implies 4y^3 + 6y^2 + 4y + 1 = 0.$$

To factorise this, we use the rational root theorem. The potential roots are thus $y = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}$, and from our scouting, we know $y = -\frac{1}{2}$ is a root. Thus,

$$4y^3 + 6y^2 + 4y + 1 = 0 = (2y + 1)(2y^2 + 2y + 1) = 0,$$

where the quadratic factor has no real solutions to it. Thus, having exhausted all cases, we have recovered the solutions

$$\boxed{(x,y) = (0,0), (0,-1), (0,-\frac{1}{2})}.$$

□

Example 0.17 (USAMO 2015 P1, JMO P2)
Solve in integers the equation

$$x^2 + xy + y^2 = \left(\frac{x+y}{3} + 1\right)^3.$$

To start off, we know LHS is an integer and so RHS must also be an integer. This means $\frac{x+y}{3}$ is also an integer, so we are motivated to write $x + y = 3k$ for some integer k.

On the other hand, LHS contains a pesky xy term. Here comes the *trick*: to kill off this nasty term, we rely on the symmetry of x and y.

Proof. Consider $a = x + y, b = x - y$:

$$xy = \frac{(a+b)(a-b)}{4} \quad \text{and} \quad x^2 + y^2 = \frac{(a+b)^2 + (a-b)^2}{4}$$

and the equation becomes

$$\frac{1}{4}\left((a+b)^2 + (a+b)(a-b) + (a-b)^2\right) = \left(\frac{a}{3} + 1\right)^3 \implies 3a^2 + b^2 = 4\left(\frac{a}{3} + 1\right)^3.$$

Letting $a = 3k$, $27k^2 + b^2 = 4(k+1)^3 \implies b^2 = 4k^3 - 15k^2 + 12k + 4$. At this point, surely the cubic must factor. Indeed, we miraculously see

$$b^2 = (k-2)^2(4k+1) \implies 4k + 1 = m^2,$$

for odd m (see the problem above for a similar reasoning).

Now, we are done, since by backsubstituting, we have:

$$a = 3k = \frac{3}{4}(m^2 - 1), \quad b^2 = (k-2)^2(4k+1) = \left(\frac{m^2-9}{4}\right)^2 m^2 \implies b = \pm\frac{m^3 - 9m}{4}.$$

Hence,

$$x = \frac{1}{8}\left(3(m^2-1) \pm (m^3 - 9m)\right) \quad \text{and} \quad y = \frac{1}{8}\left(3(m^2-1) \mp (m^3 - 9m)\right).$$

Is that all? Not quite! Don't forget that we are told to solve the given equation over the integers, so we should show also that our solutions are indeed all integers. Fortunately, since m is odd, we may let $m = 2n+1$ so that

$$\boxed{x = n^3 + 3n^2 - 1 \quad \text{and} \quad y = -n^3 + 3n + 1},$$

and permutations (note that the equation is symmetric in x and y!). □

Example 0.18 (2018 SMO(S) P25)

Suppose R is a real number such that

$$\left\lfloor R-\frac{1}{200}\right\rfloor+\left\lfloor R-\frac{2}{200}\right\rfloor+\cdots+\left\lfloor R-\frac{99}{200}\right\rfloor=2018.$$

Find $\lfloor 20R\rfloor$.

Proof. By definition of the floor function,

$$\left\lfloor R-\frac{k}{200}\right\rfloor\leq R-\frac{k}{200}<\left(R-\frac{k}{200}\right)+1.$$

Thus, $\left\lfloor R-\frac{1}{200}\right\rfloor$ and $\left\lfloor R-\frac{99}{200}\right\rfloor$ differ by at most 1. Define $M=\min_{1\leq k\leq 99}\left\lfloor R-\frac{k}{200}\right\rfloor$, then I claim that $M\geq 20$.

Suppose otherwise, then $M<20$. Thus,

$$\left\lfloor R-\frac{1}{200}\right\rfloor+\left\lfloor R-\frac{2}{200}\right\rfloor+\cdots+\left\lfloor R-\frac{99}{200}\right\rfloor<99\cdot 20=1980<2018,$$

a contradiction.

Thus, $M\geq 20$. Let a,b denote the number of $\left\lfloor R-\frac{k}{200}\right\rfloor$ attaining the values 20 and 21 respectively such that

$$\begin{cases}a+b=99\\20a+21b=2018\end{cases}\implies a=61,b=38.$$

Hence, we seek

$$\begin{cases}R-\frac{38}{200}\geq 21\\R-\frac{39}{200}\leq 21\end{cases}\implies 21.19\leq R\leq 21.195\implies \boxed{\lfloor 20R\rfloor=438}$$

. □

0.4 A Buffet Spread

This question is really a test of fundamentals: in essence, the number theory starter leads to an algebra finish.

Example 0.19 (2021 H3 Math P1 Q4)

Let a,b,c,d be positive integers such that

$$(ad-bc)^2=(a+b)(c+d) \tag{8}$$

Show that there exists coprime positive x,y and a positive integer z such that

$$a+b=x^2z,c+d=y^2z.$$

Here, we say that two integers r,s are **coprime** (or **relatively prime**) *if and only if* $\gcd(r,s)=1$, meaning that their greatest common factor is 1. The readers more familiar with number theory will quickly recall that the problem implies that $\gcd(a+b,c+d)=z$.

Indeed, we may claim as such, since the problem only asks of us to prove the existence of a positive integer z. We begin by defining $z = \gcd(a+b, c+d)$, whence $a+b = mz$, $c+d = nz$ for some coprime m, n. Our goal is now to show that m and n are both perfect squares.

From (8), $(ad-bc)^2 = mnz^2$, so mn is a perfect square. Now, consider the prime decompositions:

$$m = \prod {p_i}^{e_i},\ n = \prod {q_j}^{f_j}$$

Since m and n are coprime, no p_i and q_j are equal. Moreover,

$$mn = {p_1}^{e_1} \cdot {p_2}^{e_2} \cdots {q_1}^{f_1} \cdot {q_2}^{f_2} \cdots .$$

Since mn is a perfect square, all e_i and f_j are even, which implies that m and n are both perfect squares.

Now, we may write $m = x^2$, $n = y^2$ for some coprime x, y since m, n are coprime. Plugging this back into our original definition, we have $a+b = x^2 z, c+d = y^2 z$, as required.

Example 0.20 (cont.)
Find a quadratic equation that $\frac{y}{x}$ satisfies, and hence prove that $4ac+1$ is a perfect square.

We have

$$\frac{y^2}{x^2} = \frac{c+d}{a+b}.$$

Square-rooting this term is slightly obstructive, so we should find another way to express $\frac{y}{x}$. Since we have not used (8), this might be the time. Dividing across by $(a+b)^2$ (since it is non-zero), we have

$$\frac{(ad-bc)^2}{(a+b)^2} = \frac{c+d}{a+b} = \frac{y^2}{x^2} \implies \frac{ad-bc}{a+b} = \frac{y}{x}$$

since $\frac{y}{x}$ is positive.

Our quadratic is

$$\begin{aligned} &\frac{py^2}{x^2} + \frac{qy}{x} + r = \frac{p(c+d)}{a+b} + \frac{q(ad-bc)}{a+b} + r = 0 \\ \iff &p(c+d) + q(ad-bc) + r(a+b) = 0 \end{aligned}$$

This means we should make a choice for p, q and r. Let us investigate this observation: if we choose $p = a, r = -c$,

$$\begin{aligned} a(c+d) + q(ad-bc) - c(a+b) &= ac + ad + q(ad-bc) - ac - bc \\ &= ad + q(ad-bc) - bc = 0, \end{aligned}$$

almost as if it's forcing $q = -1$! Thus, a possible quadratic equation is $au^2 - u - c = 0$ with $u = \frac{y}{x}$.

Now, if x is a rational root, then we realise that Δ needs to be a rational square, that is the square of a rational number, and that this condition also implies that x is a rational root. We say that this bi-directional relationship is a **necessary and sufficient** condition. In this problem, $\frac{y}{x}$ is a rational root to our quadratic, so $4ac+1$ is a rational square. However, $4ac+1$ is also a positive integer, and so it must be a perfect square!

As again, proofs should be written in the forwards direction, and we present so succinctly.

Proof. I claim that the quadratic equation is $au^2 - u - c = 0$ if $ad - bc > 0$ and $au^2 + u - c = 0$ if $ad - bc < 0$.

We have

$$\frac{y^2}{x^2} = \frac{c+d}{a+b} \quad \text{and} \quad \frac{y}{x} = \frac{ad-bc}{a+b},$$

Thus,

$$\frac{a(c+d)}{a+b} - \frac{ad-bc}{a+b} - c = \frac{a(c+d) - (ad-bc) - c(a+b)}{a+b} = 0.$$

The discriminant is $\Delta = 4ac+1$. Since $\frac{y}{x}$ is a rational root, Δ is a rational square. Moreover, $4ac+1$ is a positive integer, and so it is a perfect square. □

The main challenge was discovering the quadratic equation, but we are motivated by the term $4ac+1$, which reminded us of the quadratic discriminant. Finally, the treatment of Δ required us to recall the definition of the discriminant and to argue that it must be a rational square, which implied that it is also a perfect square given that a, b, c, d are all integers.

0.5 Complex Numbers

To start off the section, we showcase a trick on evaluating (suspiciously convenient) trigonometric sums through the lenses of the **roots of unity**.

Example 0.21 (2021 H2 Further Math P1/9)
Let $\omega = \cos\frac{2\pi}{11} + \sin\frac{2\pi}{11}$. Show that

$$\sum_{j=1}^{10} \omega^j = -1.$$

Simple enough, ω is an 11th roots of unity, and so it satisfies the polynomial $z^{11} - 1 = 0$. Moreover, the required sum is a geometric progression, so

$$\sum_{j=1}^{10} \omega^j = \frac{\omega^{11} - 1}{\omega - 1} - 1 = -1.$$

Example 0.22 (cont.)
The complex numbers α and β are such that

$$\alpha = w + w^3 + w^4 + w^5 + w^9 \text{ and } \beta = w^{-1} + w^{-3} + w^{-4} + w^{-5} + w^{-9}.$$

Find in its simplest form, the quadratic equation whose roots are α and β.

Most jarringly, the exponents for α don't come in order: it jumps from 1 to 3, then 5 to 9 and β mirrors this behaviour, except with negative exponents. Fortunately, we see that $w^9 = e^{\frac{18\pi i}{11}} = e^{\frac{-4\pi i}{11}} = w^{-2}$ and that $\Re(w^{-2}) = \Re(w^2)$ (why doesn't the problem use w^2 and w^{-2} instead?). We also make a mental note that $\alpha = \beta^*$. Maybe this will come in handy later.

For now, we have

$$\begin{aligned}\alpha + \beta &= (w + w^{-1}) + (w^3 + w^{-3}) + (w^4 + w^{-4}) + (w^5 + w^{-5}) + (w^9 + w^{-9}) \\ &= 2\Re(w + w^3 + w^4 + w^5 + w^9) = 2\Re(w + w^2 + w^3 + w^4 + w^5) \\ &= 2\left(\cos\frac{2\pi}{11} + \cos\frac{4\pi}{11} + \cos\frac{6\pi}{11} + \cos\frac{8\pi}{11} + \cos\frac{10\pi}{11}\right)\end{aligned}$$

This is usually a tough sum to evaluate, but the values here just line up way too nicely for us to ignore... With that, here comes the *trick:*

$$S = \cos\frac{2\pi}{11} + \cos\frac{4\pi}{11} + \cos\frac{6\pi}{11} + \cos\frac{8\pi}{11} + \cos\frac{10\pi}{11}.$$

We consider

$$\begin{aligned}\frac{S \cdot 2\sin\frac{2\pi}{11}}{2\sin\frac{2\pi}{11}} &= \frac{2\sin\frac{2\pi}{11}\cos\frac{2\pi}{11} + 2\sin\frac{2\pi}{11}\cos\frac{4\pi}{11} + \cdots + 2\sin\frac{2\pi}{11}\cos\frac{10\pi}{11}}{2\sin\frac{2\pi}{11}} \\ &= \frac{\sin\frac{10\pi}{11} + \sin\frac{12\pi}{11} - \sin\frac{2\pi}{11}}{2\sin\frac{2\pi}{11}} \qquad \text{using the product-to-sum formula} \\ &= -\frac{1}{2}\end{aligned}$$

Remark 0.23. This doesn't work if we have one fewer term though. For instance if we exclude $\cos\frac{10\pi}{11}$, then the sum doesn't come out nice anymore. Hmm...

Hence, $\alpha+\beta=-1$. Furthermore, we have $w^{-i}=w^{-11+i}$ and $w^i=w^{11-i}$, so that

$$\begin{aligned}\alpha\beta &= (w+w^3+w^4+w^5+w^9)(w^{-1}+w^{-3}+w^{-4}+w^{-5}+w^{-9})\\ &= 5+w^{-8}+w^{-6}+w^{-5}+2w^{-4}+w^{-3}+2w^{-2}+2w^{-1}+2w+2w^2+w^3+2w^4+w^5+w^6+w^8\\ &= 5+(w^{-10}+w^{-9}+\cdots+w^{-1})+(w+w^2+\cdots+w^{10})\\ &= 5+\sum_{j=1}^{10}\omega^j+\left(\sum_{j=1}^{10}\omega^j\right)^* = 3\end{aligned}$$

where the final sum holds because

$$\left(\sum_{j=1}^{10}\omega^j\right)\left(\sum_{j=1}^{10}\omega^j\right)^* = \left|\left(\sum_{j=1}^{10}\omega^j\right)\right|^2 = 1$$

Hence, a possible quadratic equation is $x^2-x+3=0$.

Example 0.24 (cont..)
Prove that $|\alpha|=\sqrt{3}$

Aha! Here's where the property that $\alpha=\beta^*$ comes in handy.

$$|\alpha|^2=\alpha\cdot\alpha^*=\alpha\beta=3$$

and the result follows.

Example 0.25 (cont...)
Prove that

$$\sin\frac{2\pi}{11}+\sin\frac{6\pi}{11}+\sin\frac{8\pi}{11}+\sin\frac{10\pi}{11}+\sin\frac{18\pi}{11}=\frac{\sqrt{11}}{2}.$$

Observe that this is simply the imaginary part of α. In addition,

$$\begin{aligned}\Im(\alpha) &= \sin\frac{2\pi}{11}+\sin\frac{6\pi}{11}+\sin\frac{8\pi}{11}+\sin\frac{10\pi}{11}+\sin\frac{18\pi}{11}\\ &= \sin\frac{2\pi}{11}+\sin\frac{6\pi}{11}+\left(\sin\frac{8\pi}{11}-\sin\frac{7\pi}{11}\right)+\sin\frac{10\pi}{11}\\ &> 0\end{aligned}$$

since each term is positive. Thus,

$$\begin{aligned}\Im(\alpha) &= \frac{1}{2}\cdot 2\Im(\alpha)) = \frac{1}{2}(\alpha-\alpha^*)\\ &= \frac{1}{2}(\alpha-\beta)\\ &= \frac{1}{2}\Im\left(\sqrt{(\alpha+\beta)^2-4\alpha\beta}\right)\\ &= \frac{\sqrt{11}}{2}\end{aligned}$$

by taking the positive square root because $\alpha-\beta=2\Im(\alpha)>0$.

Tangent: Gaussian Periods So why didn't the question use w^{-2} and w^2? The set $(1, 3, 4, 5, 9)$ feels too specific anyways. As it turns out, this is the set of **quadratic residues** modulo 11 (prove this!), and the sums α and β are the so-called quadratic Gauss sums:

Definition 0.26 (Quadratic Gauss Sum)**.**

$$g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$$

where $\left(\frac{t}{p}\right)$ is the Legendre's symbol

Definition 0.27 (Legendre's symbol)**.** $\left(\frac{t}{p}\right) = \begin{cases} 1 & \text{if } t \text{ is a quadratic residue,} \\ -1 & \text{if } t \text{ is a quadratic non-residue,} \\ 0 & \text{if } p|t. \end{cases}$

In what follows, we showcase a technique of *summing in two ways* that reduces this problem to a sum of roots of unity.

Proposition 0.28 (Expressing g_a in terms of g_1)

$$g_a = \left(\frac{a}{p}\right) g_1.$$

Proof. Firstly if $p|a$, then $g_a = 0$ (why?).

Henceforth, suppose p does not divide a. Then,

$$\left(\frac{a}{p}\right) g_a = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{x} = g_1.$$

The first equality follows because $a \nmid p \implies at \nmid p$, so that as t runs over the set of residues (mod p), then so does at. Since at runs over the set of residues, then we may simply let the sum run over all x in the set of residues (mod p).

Now observe by definition that $\left(\frac{a}{p}\right)^2 = 1$, and we are done. □

What follows is the *coup de grace*:

Proposition 0.29 (Summing in two ways)

$$g_1^2 = (-1)^{\frac{p-1}{2}} p.$$

For convenience, write $g = g_1$. According to Ireland-Rosen, the main idea is to consider the sum $\sum_{a=0}^{p-1} g_a g_{-a}$ in two ways. Again, we consider only the case when $p \nmid a$.

On one hand, we have

$$g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2,$$

whence it follows that

$$\sum_{a=1}^{p-1} g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1) g^2.$$

On the other hand, we have

$$g_a g_{-a} = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)},$$

and summing both sides over a,

$$\begin{aligned}\sum_{a=0}^{p-1} g_a g_{-a} &= \sum_{a=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\zeta^{a(x-y)} \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)\sum_{a=0}^{p-1}\zeta^{a(x-y)} \\ &= \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)s(x,y)p \\ &= p(p-1)\end{aligned}$$

where we have $p^{-1}\sum_{t=0}^{p-1}\zeta^{at} = s(x,y) = \begin{cases}1 & \text{if } p \mid t \\ 0 & \text{otherwise.}\end{cases}$. Putting both parts together, the result follows.

0.6 A Splurge of Inequalities

We start off this chapter with a powerful technique for proving inequalities.

Example 0.30 (Schur's Inequality)
Let a, b, c, r be positive real numbers. Prove that

$$a^r(a-b)(a-c) + b^r(b-c)(b-a) + c^r(c-a)(c-b) \geq 0.$$

Let $f(a,b,c) = a^r(a-b)(a-c) + b^r(b-c)(b-a) + c^r(c-a)(c-b)$. In general, we say that f is symmetric if $f(a,b,c) = f(b,a,c) = f(c,b,a) = \cdots$. This means that the function remains constant even if we interchange the variables a, b and c.

Simple enough, if we interchange a and b, we have:

$$\begin{aligned}f(b,a,c) &= b^r(b-a)(b-c) + a^r(a-c)(a-b) + c^r(c-b)(c-a) \\ &= a^r(a-b)(a-c) + b^r(b-c)(b-a) + c^r(c-a)(c-b) \\ &= f(a,b,c)\end{aligned}$$

If you are paranoid, you can manually verify this for the $3! = 6$ possible "interchanges". I'll leave that to you.

With that, we say that the function, and hence Schur's Inequality, is **symmetric** in a, b, c. So what's the big deal?

Since the value of $f(a,b,c)$ remains constant even as we interchange variables, we may impose restrictions on a, b, c that we normally cannot. In particular, we may assume **without loss of generality** that $a \geq b \geq c$ (convince yourself!). This is very useful, especially for this inequality, because we have terms in $a-b, a-c\cdots$, and the ordering of a, b, c tells us whether these terms are positive or negative.

In fact, a cursory glance tells us that if $a \geq b \geq c$, then only $b^r(b-c)(b-a)$ is negative. Hence, this motivates an enlightening rearrangement of $f(a,b,c)$:

$$f(a,b,c) = a^r(a-b)(a-c) + b^r(b-c)(b-a) + c^r(c-a)(c-b)$$

$$= (a-b)[a^r(a-c) - b^r(b-c)] + c^r(a-c)(b-c)$$

And we are done!

This technique, ironically, is known as "breaking symmetry". The inequality is essentially proven after we impose a specific ordering on the variables, but before that, the inequality may look almost intractible!

0.7 Selected Problems

Problem 0.31. Prove by contradiction that $\sqrt{2}$ is irrational.

Problem 0.32. * Prove by contradiction that $x^2 + y^2 = 3z^2$ has no positive integer solutions.

Problem 0.33. Explain why lines (1) and (2) hold in Tangent: Central Binomial Coefficient. (Hint: You may want to consider the density function of the normal distribution.)

Problem 0.34. By referring to Schur's Inequality, prove that

- $a^3 + b^3 + c^3 \geq a^2(b+c) + b^2(c+a) + c^2(a+b)$,
- $$\frac{1}{a^5} + \frac{1}{b^5} + \frac{1}{c^5} + \frac{a+b+c}{a^2b^2c^2} \geq \frac{b^2+c^2}{a^3b^2c^2} + \frac{c^2+a^2}{b^3c^2a^2} + \frac{a^2+b^2}{c^3a^2b^2}.$$

Problem 0.35. (2017 USAJMO P2) Consider the equation

$$(3x^3 + xy^2)(x^2y + 3y^3) = (x-y)^7.$$

- Prove that there are infinitely many pairs of positive integers (x, y) satisfying the equation.
- Describe all pairs of positive integers (x, y) satisfying the equation.