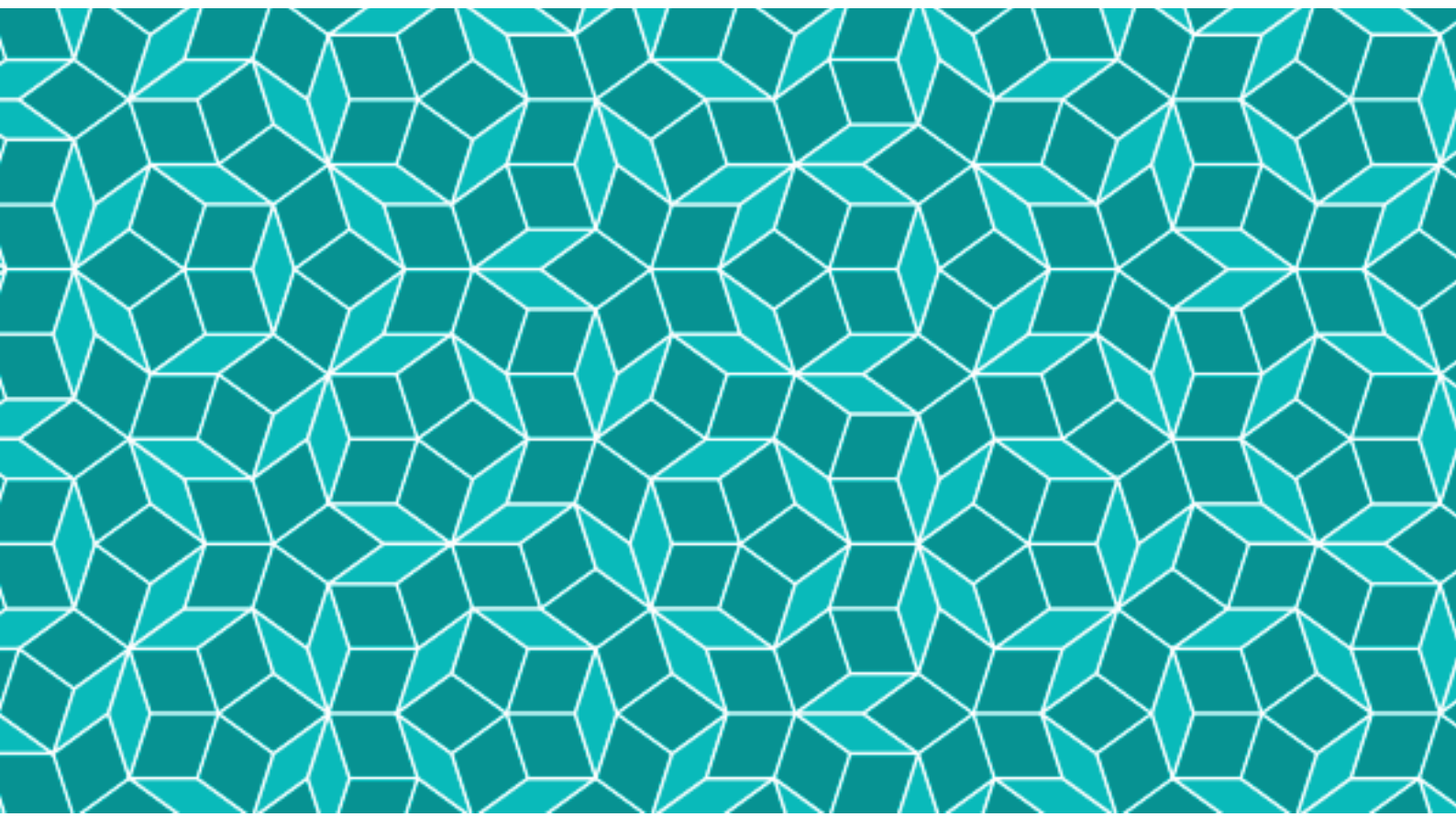# The Road to Mastery: Mathematics Olympiad

RYAN JOO RUI AN

The Road to Mastery: Mathematics Olympiad

Ryan Joo Rui An

Last updated: December 4, 2023

Preface

About the Author

Ryan Joo Rui An is a high school student currently completing his A Levels in Singapore. He has participated in numerous Mathematics Olympiad competitions and consistently achieved decent results, including the Singapore Mathematics Olympiad (SMO) and IMO National Selection Test (IMONST), which are the two selection tests for the prestigious International Mathematics Olympiad (IMO) by Singapore and Malaysia respectively.

About the Book

The motivation of the writer to write this book was to the author for Mathematics Olympiad competitions by summarising important topics in Mathematics Olympiad, with a focus on SMO and MAA-AMC, which feature rather challenging problems.

Do reach out to the author at `ryanjooruian18@gmail.com` if you wish to point out any (glaring) mistakes, or provide comments and suggestions regarding the content and/or formatting of the book.

Resources

Here are some notes and materials that you might find useful when learning Mathematics Olympiad:

- Unofficial syllabus for math olympiads, by Evan Chen
- Notes on proof-writing style
- AoPS Contest Collections
- Yufei Zhao's olympiad handouts
- Evan Chen's olympiad handouts
- Olympiad Problems and Solutions, by Evan Chen
- Canadian Mathematical Society Resources

- Mathematical Reflections

- 3Blue1Brown

Contents

Part I

Number Theory

1 **Divisibility**

- [Olympiad Number Theory Through Challenging Problems](#)

- [A Concise Introduction to Pure Mathematics, Fourth Edition](#)

- [NT notes](#)

§1.1 Division Algorithm

> **Theorem 1.1.1: Division Algorithm**
>
> For every integer pair a and b, there exists distinct integer **quotient** and **remainder**, denoted by q and r respectively, that satisfy
> $$a = bq + r, \quad \text{where } 0 \leq r < b$$

> **Definition 1.1.1: Divisible**
>
> An integer b is said to be **divisible** by an integer $a \neq 0$, denoted by $a \mid b$, if there exists some integer c such that $b = ac$.
> We write $a \nmid b$ to indicate that b is not divisible by a.

Remark. If a is a divisor of b, then b is also divisible by $-a$, so the divisors of an integer always occur in pairs. To find all the divisors of a given integer, it is sufficient to obtain the positive divisors and then adjoin them to the corresponding negative integers. For this reason, we usually limit ourselves to the consideration of the positive divisors.

Using the definition above, for integers a, b, c, the following properties hold:

(i) $a \mid 0$, $1 \mid a$, $a \mid a$

(ii) $a \mid 1$ if and only if $a = \pm 1$

(iii) If $a \mid b$ and $c \mid d$, then $ac \mid bd$

(iv) If $a \mid b$ and $b \mid c$, then $a \mid c$

(v) $a \mid b$ and $b \mid a$ if and only if $a = \pm b$

(vi) If $a \mid b$ and $b \neq 0$, then $a \leq b$

(vii) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers x and y.

Remark. Property (vii) extends by induction to sums of more than two terms. That is, if $a \mid bk$ for $k = 1, 2, \dots, n$, then

$$a \mid (b_1 x_1 + b_2 x_2 + \cdots + b_n x_n)$$

for all integers x_i.

§1.2   Greatest Common Divisor and Lowest Common Multiple

§1.2.1   Greatest Common Divisor (GCD)

Of special significance is the case in which the remainder in the Division Algorithm turns out to be zero.

Let a and b be two non-zero integers.

> **Definition 1.2.1: Greatest common divisor**
>
> The **greatest common divisor** of a and b, denoted by $\gcd(a,b)$, is the *largest* positive integer d where $d \mid a$ and $d \mid b$.

> **Definition 1.2.2: Coprime**
>
> a and b are said to be **coprime** (or relatively prime) when $\gcd(a,b) = 1$.

§1.2.2   Lowest Common Multiple (LCM)

> **Definition 1.2.3: Lowest common multiple**
>
> The **lowest common multiple** of a and b, denoted by $\operatorname{lcm}(a,b)$, is the *smallest* positive integer m where $a \mid m$ and $b \mid m$.

> **Theorem 1.2.1**
>
> For positive integers a and b,
>
> $$\gcd(a,b) \times \operatorname{lcm}(a,b) = ab.$$

§1.2.3   Primes

> **Definition 1.2.4: Prime and composite numbers**
>
> An integer $p > 1$ is **prime** if its only positive divisors are 1 and p.
> It is **composite** if it is not prime.

> ### Theorem 1.2.2: Prime Number Theorem
>
> The **Riemann Zeta Function** describes the distribution of prime numbers. For a positive real x, the function $\pi(x)$ denotes the number of primes less than or equal to x.
>
> Then the number of primes not exceeding x is asymptotic to $\dfrac{x}{\ln x}$; that is,
>
> $$\lim_{x \to \infty} \pi(x) = \frac{x}{\ln x}$$

Also, regarding prime numbers,

> ### Theorem 1.2.3: Euler
>
> There are infinitely many primes.

Proof. We prove this by contradiction. Suppose there is only a finite number m of primes, say $p_1 < p_2 < \cdots < p_m$. Consider the number $P = p_1 p_2 \cdots p_m + 1$.

Case 1: If P is prime, then $P > p_m$, contradicting the maximality of p_m.

Case 2: If P is composite, it has a prime divisor $p_k > 1$ which is one of $p_1, p_2, \ldots, p_m$. Then it follows that $p_k \mid p_1 p_2 \cdots p_m + 1$. But this means that $p_k \mid 1$, which is a contradiction. $\quad\square$

> ### Theorem 1.2.4: Fundamental Theorem of Arithmetic
>
> Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof. We prove this by strong induction. Consider some integer $n > 1$. Either it is prime or it is composite.

Case 1: If n is prime, we are done.

Case 2: If n is composite, then there exists an integer $d \mid n$ and $1 < d < n$. Among all such integers d, choose the smallest, say p_1. Then p_1 must be prime. Hence we can write $n = p_1 n_1$ for some integer n_1 satisfying $1 < n_1 < n$. This completes the induction. $\quad\square$

§1.3   Euclidean Algorithm

Before introducing the Euclidean Algorithm, we need to prove this fact:

Proposition 1.3.1. For integers a and b,

$$\gcd(a,b) = \gcd(a-b,b)$$

Proof.   □

The Euclidean Algorithm makes use of the following properties:

- $\gcd(a,0) = a$

- $\gcd(a,b) = \gcd(a-b,b)$

The Euclidean Algorithm may be described as follows: Let a and b be two integers whose greatest common divisor is desired. WLOG $a \geq b > 0$. The first step is to apply the Division Algorithm to a and b to obtain

$$a = q_1 b + r_1 \quad 0 \leq r_1 < b$$

In the case where $r_1 = 0$, then $b|a$ and $\gcd(a,b) = b$. When $r_1 \neq 0$, divide b by r_1 to obtain integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1$$

If $r_2 = 0$, we stop; otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \quad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears, say at the $(n+1)$-th step where r_{n+1} is divided by r_n Note that this process will stop eventually as the strictly decreasing sequence $b > r_1 > r_2 > \cdots > r_{n+1} > r_{n+2} = 0$ cannot contain more than b integers.

The result is the following sequence of equations (or operations):

$$
\begin{aligned}
a &= q_1 b + r_1 & 0 &\leq r_1 < b \\
b &= q_2 r_1 + r_2 & 0 &\leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 &\leq r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n & 0 &\leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}
$$

The claim is that the last nonzero remainder $r_n = \gcd(a,b)$.

> **Example 1.3.1**
>
> Find $\gcd(682, 264)$.

Solution.

$$682 = 3(264) - 110$$
$$264 = 2(110) + 44$$
$$110 = 2(44) + 22$$
$$44 = 2(22) + 0$$

Hence $\gcd(682, 264) = \boxed{22}$. $\square$

§1.4   Divisibility Rules

These divisibility rules help determine when positive integers are divisible by particular other integers. All of these rules apply for base-10 only – other bases have their own, different versions of these rules.

- 2 and powers of 2

  A number is divisible by 2^n if and only if the last n digits of the number are divisible by 2^n. Thus, in particular, a number is divisible by 2 if and only if its units digit is divisible by 2, i.e. if the number ends in 0, 2, 4, 6 or 8.

- 3 and 9

  A number is divisible by 3 or 9 if and only if the sum of its digits is divisible by 3 or 9, respectively. Note that this does not work for higher powers of 3. For instance, the sum of the digits of 1899 is divisible by 27, but 1899 is not itself divisible by 27.

- 5 and powers of 5 A number is divisible by 5^n if and only if the last n digits are divisible by that power of 5.

- 7

  Partition N into 3 digit numbers from the right $(d_3 d_2 d_1, d_6 d_5 d_4, \dots)$. The alternating sum $(d_3 d_2 d_1 - d_6 d_5 d_4 + d_9 d_8 d_7 - \dots)$ is divisible by 7 if and only if N is divisible by 7.

- 10 and powers of 10

  If a number is power of 10, define it as a power of 10. The exponent is the number of zeros that should be at the end of a number for it to be divisible by that power of 10.

  Example: A number needs to have 6 zeroes at the end of it to be divisible by 1,000,000 because $1,000,000 = 10^6$.

- 11

  A number is divisible by 11 if and only if the alternating sum of the digits is divisible by 11.

- 13

  Partition N into 3 digit numbers from the right $(d_3d_2d_1, d_6d_5d_4, \dots)$. The alternating sum $(d_3d_2d_1 - d_6d_5d_4 + d_9d_8d_7 - \dots)$ is divisible by 13 if and only if N is divisible by 13.

- 17

  Truncate the last digit, multiply it by 5 and subtract from the remaining leading number. The number is divisible if and only if the result is divisible. The process can be repeated for any number.

- 19

  Truncate the last digit, multiply it by 2 and add to the remaining leading number. The number is divisible if and only if the result is divisible. This can also be repeated for large numbers.

- 29

  Truncate the last digit, multiply it by 3 and add to the remaining leading number. The number is divisible if and only if the result is divisible. This can also be repeated for large numbers.

2 Modular Arithmetic

§2.1 Definition

> **Definition 2.1.1: Modulo**
>
> Given integers a, b, and n, with $n > 0$, we say that a is congruent to b modulo n, or $a \equiv b \pmod{n}$, if the difference $a - b$ is divisible by n.

§2.1.1 Modular operations

Consider four integers a, b, c, d and positive integer n such that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. In modular arithmetic, the following identities hold:

- Addition: $a + c \equiv b + d \pmod{n}$.

- Subtraction: $a - c \equiv b - d \pmod{n}$.

- Multiplication: $ac \equiv bd \pmod{n}$.

- Division: $\dfrac{a}{e} \equiv \dfrac{b}{e} \left(\bmod\ \dfrac{n}{\gcd(n,e)} \right)$, where e is a positive integer that divides a and b.

- Exponentiation: $a^e \equiv b^e \pmod{n}$ where e is a positive integer.

§2.1.2 Integers modulo n

The relation $a \equiv b \pmod{n}$ allows us to divide the set of integers into sets of equivalent elements. For example, if $n = 3$, then the integers are divided into the following sets:

$$\{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$\{\ldots, -5, -2, 1, 4, 7, \ldots\}$$

$$\{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

Notice that if we pick two numbers a and b from the same set, then a and b differ by a multiple of 3, and therefore $a \equiv b \pmod 3$.

We sometimes refer to one of the sets above by choosing an element from the set, and putting a bar over it. For example, the symbol $\bar{0}$ refers to the set containing 0; that is, the set of all integer multiples of 3. The symbol $\bar{1}$ refers to the second set listed above, and $\bar{2}$ the third. The symbol $\bar{3}$ refers to the same set as $\bar{0}$, and so on.

Instead of thinking of the objects $\bar{0}$, $\bar{1}$, and $\bar{2}$ as sets, we can treat them as algebraic objects – like numbers – with their own operations of addition and multiplication. Together, these objects form the integers modulo 3, or $\mathbb{Z}_3$. More generally, if n is a positive integer, then we can define

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\},$$

where for each k, $\bar{k}$ is defined by

$$\bar{k} = \{m \in \mathbb{Z} \text{ s.t. } m \equiv k \pmod n\}.$$

§2.1.3   Addition, Subtraction, and Multiplication mod n

We define addition, subtraction, and multiplication in $\mathbb{Z}_n$ according to the following rules:

- Addition: $\bar{a} + \bar{b} = \overline{a+b}$ for all $a, b \in \mathbb{Z}$.

- Subtraction: $\bar{a} - \bar{b} = \overline{a-b}$ for all $a, b \in \mathbb{Z}$.

- Multiplication: $\bar{a} \cdot \bar{b} = \overline{ab}$ for all $a, b \in \mathbb{Z}$.

§2.2 Modular inverse

For coprime a and n, there exists an inverse of $a \pmod{n}$. In other words, there exists b such that
$$ab \equiv 1 \pmod{n}$$

We can find the modular inverse using the extended Euclidean algorithm.

Example 2.2.1

Solve the following modular equation.

$$7x \equiv 1 \pmod{26}$$

Solution. Compute GCD and keep the tableau:

$$\gcd(26,7) = \gcd(7,5) = \gcd(5,2) = \gcd(2,1) = \gcd(1,0) = 1$$

Solve the equations for r in the tableau:

$$a = qb + r$$
$$26 = 3(7) + 5$$
$$7 = 1(5) + 2$$
$$5 = 2(2) + 1$$

Back substitute the equations for r:

$$1 = 5 - 2 \times (7 - 1 \times 5)$$
$$= (-2) \times 7 + 3 \times 5$$
$$= (-2) \times 7 + 3 \times (26 - 3 \times 7)$$
$$= 3 \times 26 + (-11) \times 7$$

Modular inverse of $7 \pmod{26}$ is $-11 \pmod{26} = 15$. Hence $x = 26k + 15$ for $k \in \mathbb{Z}$. $\qquad \square$

§2.3   Orders Modulo A Prime

https://web.evanchen.cc/handouts/ORPR/ORPR.pdf

§2.4   Theorems

For $n = p_1{}^{a_1} p_2{}^{a_2} \ldots p_k{}^{a_k}$,

- Number of factors:
$$\tau(n) = \prod_{i=1}^{k}(a_i + 1)$$

- Sum of factors:
$$d(n) = \prod_{i=1}^{k}\left(1 + p_i + \cdots + p_i{}^{a_i}\right)$$

- Number of positive integers less than n which are coprime to n:
$$\varphi(n) = n \prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

  This is known as the **totient function**.

Theorem 2.4.1: Fermat's Little Theorem

For prime p and $1 \leq a < p$,
$$a^p \equiv a \pmod{p} \tag{2.1}$$

Theorem 2.4.2: Euler's Totient Theorem

For coprime a and n,
$$a^{\varphi(n)} \equiv 1 \pmod{n} \tag{2.2}$$

Theorem 2.4.3: Wilson's Theorem

For odd prime p,
$$(p-1)! \equiv -1 \pmod{p} \tag{2.3}$$

Theorem 2.4.4: Chinese Remainder Theorem

Given pairwise coprime positive integers n_i and arbitrary integers a_i, the system of simultaneous congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_k \pmod{n_k}$$

has a unique solution modulo $n_1 n_2 \cdots n_k$.

> **Example 2.4.1**
>
> Find the set of values of n that satisfy the following system of modular equations.
> $$\begin{cases} n \equiv 4 \pmod 5 \\ n \equiv 5 \pmod 9 \\ n \equiv 3 \pmod{11} \end{cases}$$

Solution. From the first equation, let $n = 4+5x$. Substituting this into the second equation gives $4 + 5x \equiv 5 \pmod 9$, which reduces to $x \equiv 2 \pmod 9$.

Let $x = 2 + 9y$. Substituting this into the third equation gives $14 + 45y \equiv 3 \pmod 1 1$, which reduces to $y \equiv 0 \pmod 1 1$.

Let $y = 0 + 11z$. Substituting expressions for x and y into $n = 4 + 5x$ gives $n = 14 + 495z$. Hence the set of values are $\{z \in \mathbb{Z} \mid 14 + 495z\}$.

Remark. To check our answer, using the Chinese Remainder Theorem, we can see that there is indeed a unique solution modulo $5 \times 9 \times 11 = 495$.

$\square$

§2.5   Quadratic Residues

Definition 2.5.1: Quadratic residue

For prime p and integer a, a is a **quadratic residue** modulo p if there is a perfect square in the congruence class a $(\text{mod } p)$.

$$x^2 \equiv a \pmod{p}$$

Otherwise, a is a non-quadratic residue modulo p.

Some examples:

$$n^2 \equiv 0/1 \pmod{3}$$
$$n^2 \equiv 0/1 \pmod{4}$$
$$n^2 \equiv 0/1/4 \pmod{5}$$
$$n^2 \equiv 0/1/4 \pmod{8}$$

Notice that the numbers that are colored above are in the order of $\{1, 4, 9, 5, 3, 3, 5, 9, 4, 1\}$. That is, the first number and the last number are equal; the second number and the second last number are equal; the third number and the third last number are equal, and so on. This is because $x^2 \equiv (-x)^2 \pmod{p}$, so the squares of the first half of the nonzero numbers mod p give a complete list of the nonzero quadratic residues mod p. In general, we have the following fact:

Proposition 2.5.1. If p is an odd prime, the residue classes of $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are distinct and give a complete list of the quadratic residues modulo p. So there are $\frac{p-1}{2}$ residues and $\frac{p-1}{2}$ non-residues.

Proof. They give a complete list because x^2 and $(p-x)^2$ are congruent mod p. To see that they are distinct, note that

$$
\begin{aligned}
x^2 \equiv y^2 \pmod{p} &\iff p \mid x^2 - y^2 \\
&\iff p \mid (x+y)(x-y) \\
&\iff p \mid x+y \text{ or } p \mid x-y
\end{aligned}
$$

which is impossible if x and y are two different members of the set $\{0, 1, \ldots, \frac{p-1}{2}\}$. $\qquad \square$

Example 2.5.1: CANADA 1969

Show that there are no integers a, b, c for which

$$a^2 + b^2 - 8c = 6.$$

Proof. Using quadratic residues, all perfect squares are equivalent to $0, 1, 4 \pmod{8}$. Hence, the problem statement is equivalent to $a^2 + b^2 \equiv 6 \pmod{8}$. It is impossible to obtain a sum of 6 with two of $0, 1, 4$, so our proof is complete. $\qquad \square$

§2.5.1   Legendre symbol

Definition 2.5.2: Legendre symbol

For any integer a and prime p, we define

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ has solutions} \\ -1 & p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ has no solutions} \end{cases} \tag{2.4}$$

In other words, the Legendre symbol returns the following values:

- 0 if n is divisible by p;

- 1 if n is a non-zero quadratic residue modulo p; and

- -1 if a is a non-quadratic residue modulo p.

Properties of the Legendre Symbol:

1. Euler's Criterion

Theorem 2.5.1: Euler's Criterion

Let p be an odd prime and let a be an integer not divisible by p, then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \tag{2.5}$$

Proof. By Fermat's little theorem, $a^{(}p-1) \equiv 1 \pmod{p}$, so $\left(a^{\frac{p-1}{2}}\right)^2 - 1 \equiv 0 (mod p)$.

The LHS can be factorised, and one of them must be divisible by p due to the above.

If a is a non-zero quadratic residue modulo p, then $a \equiv x^2 \pmod{p}$ where $x \neq 0$; taking the $\frac{p-1}{2}$-th power on both sides give $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

We claim that for all non-quadratic residues a we have $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. This is sufficient as its contrapositive gives the following statement: if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, then a is a nonzero quadratic residue modulo p. So the iff case is derived automatically.

For this one we need the following fact from abstract algebra:

Lemma 2.5.1. Let $P(x)$ be a polynomial of degree n, then $P(x) \equiv 0 \pmod{p}$ has at most n roots modulo p.

Now consider the modular equation $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

As we've proven above, all non-zero quadratic residues modulo p are roots to the above equation.

However, we can actually show that there are at least $\frac{p-1}{2}$ quadratic residues by direct constructions: Consider the set of congruence classes modulo p denoted by

Now we consider $\{1^2, 2^2, \ldots, (p-1)^2\}$. If the congruence class $a \pmod p$ lies in the above set, then by construction we know that a is a quadratic residue modulo p. Conversely, if a is a quadratic residue modulo p, then some of the elements in $\{1^2, 2^2, \ldots, (p-1)^2\}$ correspond to a.

However, there are in fact at most two of them that are actually a. This is because the element must satisfy $x^2 \equiv a \pmod p$, and $x^2 - a$ is a polynomial of degree 2. So there are at most two roots, meaning at most two elements. In fact we know exactly which of the elements are the same: $x^2 \equiv (p-x)^2 \pmod p$. So the set of quadratic residues is precisely the set $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$.

And thus, there are at least $\frac{p-1}{2}$ quadratic residues modulo p (Note that at this point we still haven't proven the fact that $\{1^2, 2^2, \ldots, (\frac{p-1}{2})^2\}$ accounts for all quadratic residues; we're very close though)

The final step is to combine the two: 1. $x^{\frac{p-1}{2}} \equiv 1 \pmod p$ has at most $\frac{p-1}{2}$ roots 2. Since $x^2 \equiv a$ has at most 2 roots, there are at least $\frac{p-1}{2}$ quadratic residues, each satisfying $x^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Therefore, if a is a non-quadratic residue modulo p, the congruence class a (mod p) is distinct from all elements in $\{1^2, \ldots, (p-1)^2\}$ and thus together with the at least $\frac{p-1}{2}$ quadratic residues in $\{1^2, \ldots, (p-1)^2\}$, there will be more than (p-1)/2 distinct roots in $x^{\frac{p-1}{2}} \equiv 1 \pmod p$, a contradiction.

This finally proves that $a^{\frac{p-1}{2}} \equiv -1 \pmod p$, and everything falls into place due to this. $\qquad\square$

2. Multiplicity

   For prime p and integers a, b not divisible by p,

   $$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

   Proof. This follows from Euler's Criterion.

   1b) is a direct consequence of 1a), although there is in fact a way to prove this directly : The nontrivial deduction is that the product of two nonquadratic residues must be a quadratic residue : First note that the proof in 1a) actually provided a proof for 1c) : Now that I think about it, this feels strange because we are still referring to the proof of 1a) The thing is that, if we know 1c), then we can show 1b) $\qquad\square$

3. For odd prime p, then there are an equal number of non-zero quadratic residues and non-quadratic residues modulo p.

4. Gauss' Lemma

> **Theorem 2.5.2: Gauss' Lemma**
>
> For odd prime p and integer a where $p \nmid a$,
>
> $$\left(\frac{a}{p}\right) = (-1)^n$$
>
> where n is the number of integers $0 < k < \frac{p}{2}$ such that $k \cdot a$ belongs to the congruence class $m \pmod{p}$ where $\frac{p}{2} < m < p$.

5. Second Supplementary Law

> **Theorem 2.5.3: Second Supplementary Law**
>
> For odd prime p,
>
> $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

6. Eisenstein's Lemma

> **Theorem 2.5.4: Eisenstein's Lemma**
>
> For distinct odd primes p and q,
>
> $$\left(\frac{q}{p}\right) = (-1)^{\alpha} \tag{2.6}$$
>
> where
>
> $$\alpha = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$$

7. Law of Quadratic Reciprocity

> **Theorem 2.5.5: Law of Quadratic Reciprocity**
>
> For distinct odd primes p and q,
>
> $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \tag{2.7}$$

Proof. Evaluate the product $a \cdot 2a \cdots \frac{p-1}{2}a \pmod{p}$ in two different ways. By rearranging terms, we get

$$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

But the product can also be evaluated by noticing that each of the distinct integers in Gauss's lemma is either x or $p - x$ for $1 \leq x \leq \frac{p-1}{2}$, and showing that each of the x's is distinct. Multiplying them together modulo p gives $(\frac{p-1}{2})!$ multiplied by n minus signs due to the number of $p - x$ terms of which there are n, hence the sign is $(-1)^n$. The result follows by Euler's criterion and cancelling the $(\frac{p-1}{2})!$. $\qquad \square$

Special cases

- $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

- $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

- $\left(\dfrac{-3}{p}\right) = \begin{cases} 1 & p = 1 \pmod 6 \\ -1 & p = 5 \pmod 6 \end{cases}$

- $\left(\dfrac{5}{p}\right) = \begin{cases} 1 & p = 1, 9 \pmod{10} \\ -1 & p = 3, 7 \pmod{10} \end{cases}$

3 Diophantine Equations

§3.1 Linear diophantine equation

One famous problem is the McNugget Numbers. McNugget Numbers (Henri Picciotto, 1980s) I Original boxes had 6, 9, and 20 nuggets. I Worked out the largest non-McNugget number on a napkin. I g(6, 9, 20) = 43.

A Diophantine equation in the form $ax + by = c$ is known as a linear combination. There will always be an infinite number of solutions when $\gcd(a, b) = 1$ and $\gcd(a, b) \mid c$.

Theorem 3.1.1: Bezout's Lemma

For non-zero integers a and b, let $d = \gcd(a, b)$, there exists integers x and y that satisfy

$$ax + by = d.$$

An important case:
$$ax + by = 1, x, y \in \mathbb{Z} \iff a, b \text{ coprime}$$

Example 3.1.1

Find integers x and y that satisfy

$$102x + 38y = 2.$$

Solution. Apply the extended Euclidean algorithm on a and b to calculate $\gcd(a, b)$:

$$102 = 2 \times 38 + 26$$
$$38 = 1 \times 26 + 12$$
$$26 = 2 \times 12 + 2$$
$$12 = 6 \times 2 + 0$$
$$6 = 3 \times 2 + 0$$

Work backwards and substitute the numbers from above:

$$2 = 26 - 2 \times 12$$
$$= 3 \times 26 - 2 \times 38$$
$$= 3 \times 102 - 8 \times 38$$

Hence $x = 3$, $y = -8$. □

All solutions of linear diophantine equations:

Theorem 3.1.2

If (x_0, y_0) is a solution of $ax + by = n$, then all solutions are given by

$$\{(x, y) : x = x_0 + bt, y = y_0 - at, t \in \mathbb{Z}\}$$

For three variables in the equation $ax + by + cz = d$, this is the equation of a plane, instead of a line.

§3.2 Pythagorean Triples

Pythagorean triples are triplets (a, b, c), where a, b, c are positive integers, that satisfy $a^2 + b^2 = c^2$.

The smallest and best-known Pythagorean triple is $(a, b, c) = (3, 4, 5)$. The right triangle having these side lengths is sometimes called the $3, 4, 5$ triangle.

In fact, all Pythagorean triples can be expressed in the form of

$$a = k(m^2 - n^2) \quad b = k(2mn) \quad c = k(m^2 + n^2)$$

§3.3 Pell's Equation

Theorem 3.3.1: Pell's Equation

If $n > 0$ is not a perfect square, then the equation

$$x^2 - ny^2 = 1$$

has infinitely many solutions.

Note that $(x, y) = (1, 0)$ is a trivial solution.

Steps:

1. Find one non-trivial solution (x, y).

2. Let $\alpha^n = (x + y\sqrt{d})^n$ where $n = 2, 3, \ldots$. The coefficients of the integer and square root give us the values of x and y respectively.

> **Example 3.3.1**
>
> Find positive integers x and y that satisfy
>
> $$x^2 - 2y^2 = 1.$$

Solution. We first observe that $(x, y) = (3, 2)$ is a solution.

$$\alpha = (3 + 2\sqrt{2})$$
$$\alpha^n = (3 + 2\sqrt{2})^n$$

For $n = 2$,

$$\alpha^2 = (3 + 2\sqrt{2})^2$$
$$= 17 + 12\sqrt{2}$$

From this, we deduce that another solution is $(x, y) = (17, 12)$.

Simply repeat the above method to find further solutions. $\square$

> **Theorem 3.3.2: Frobenius coin problem**
>
> What is the largest number n such that $ax + by = n$ has no solutions for $x, y \geq 0$?
> Let the Frobenius Number be $n = g(a, b)$.
> The claim is
> $$g(a, b) = ab - a - b.$$

Proof. $\square$

> **Theorem 3.3.3: Fermat's Last Theorem**
>
> For $n > 2$, there are no non-zero solutions to
>
> $$a^n + b^n = c^n.$$

The proof is quite complicated and can be found here.

Part II

Algebra

4 Basic Algebra

§4.1   Elementary Manipulation

This book assumes the reader should be familiar with basic algebraic manipulation.

Factorisations:

- Difference of squares:
$$a^2 - b^2 = (a+b)(a-b)$$

- Sum of squares:
$$a^2 + b^2 = (a+b)^2 - 2ab$$

- Sum of cubes:
$$a^3 + b^3 = (a+b)(a^2 - ab + b^2)$$

- Difference of cubes:
$$a^3 - b^3 = (a-b)(a^2 + ab + b^2)$$

- Generalised formulae:
$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \quad \forall n \in \mathbb{N}$$

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}) \quad \forall \text{ odd } n \in \mathbb{N}$$

- Generalised expansion of square:
$$(a_1 + a_2 + \cdots + a_n)^2 = (a_1^2 + a_2^2 + \cdots + a_n^2) + (2a_1a_2 + \cdots + 2a_1a_n) + (2a_2a_3 + \cdots + 2a_2a_n) + \cdots + 2a_{n-1}a_n$$

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

Example 4.1.1

Evaluate the expression
$$(2+1)(2^2+1)(2^4+1)\cdots(2^{2^{10}}+1)+1.$$

29

Solution. By using the formula $(a - b)(a + b) = a^2 - b^2$ repeatedly, we have

$$
\begin{aligned}
&(2 + 1)(2^2 + 1)(2^4 + 1)\cdots(2^{2^{10}} + 1) + 1 \\
&= (2 - 1)(2 + 1)(2^2 + 1)(2^4 + 1)\cdots(2^{2^{10}} + 1) + 1 \\
&= ((2^{2^{10}})^2 - 1) + 1 = \boxed{2^{2048}}
\end{aligned}
$$

$\square$

Example 4.1.2

Given that the real numbers x, y and z satisfy the system of equations

$$
\begin{cases}
x + y + z = 6 \\
x^2 + y^2 + z^2 = 26 \\
x^3 + y^3 + z^3 = 90
\end{cases}
$$

Find the values of xyz and $x^4 + y^4 + z^4$.

Solution. $(x + y + z)^2 = (x^2 + y^2 + z^2) + 2(xy + yz + zx)$ implies that $xy + yz + zx = 5$.

Since $x^3 + y^3 + z^3 - 3xyz = (x + y + z)[(x^2 + y^2 + z^2) - (xy + yz + zx)]$, $xy + yz + zx = \boxed{-12}$.

Further, by completing squares,

$$
\begin{aligned}
x^4 + y^4 + z^4 &= (x^2 + y^2 + z^2)^2 - 2(x^2y^2 + y^2z^2 + z^2x^2) \\
&= (x^2 + y^2 + z^2)^2 - 2[(xy + yz + zx)^2 - 2(xy^2z + yz^2x + x^2yz)] \\
&= (x^2 + y^2 + z^2)^2 - 2[(xy + yz + zx)^2 - 2xyz(x + y + z)] = \boxed{338}
\end{aligned}
$$

$\square$

§4.2   Polynomials

A **polynomial**, in terms of the variable x, takes the form of

$$P(x) = a_n x^n + \cdots + a_1 x + a_0$$

where a_i are the *coefficients*, a_0 is the *constant term*, the highest power n is the *degree* of the polynomial denoted by $\deg P(x)$.

> **Theorem 4.2.1: Quadratic formula**
>
> For $a, b, c \in \mathbb{R}, a \neq 0$, the quadratic equation $ax^2 + bx + c = 0$ has solutions
>
> $$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{4.1}$$

Proof. The proof is quite simple; it can be done by completing the square. □

Let Δ denote the **discriminant**, then $\Delta = b^2 - 4ac$.

- For $\Delta < 0$, the 2 roots are complex and conjugates to each other.

- For $\Delta = 0$, the 2 roots are real and repeated.

- For $\Delta > 0$, the 2 roots are real and distinct.

> **Theorem 4.2.2: Vieta's relations**
>
> For polynomial $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with complex coefficients with roots $r_1, r_2, \ldots, r_n$,
>
> $$r_1 + r_2 + \cdots + r_n = -\frac{a_{n-1}}{a_n}$$
> $$r_1 r_2 + r_2 r_3 + \cdots + r_{n-1} r_n = \frac{a_{n-2}}{a_n}$$
> $$\vdots \tag{4.2}$$
> $$r_1 r_2 \cdots r_n = (-1)^n \frac{a_0}{a_n}$$

For a polynomial with integer coefficients a_i, $x = \frac{p}{q}$ is a rational root, where $p \mid a_0$ and $q \mid a_n$.

> **Theorem 4.2.3: Division Algorithm**
>
> If $f(x)$ and $d(x)$ are polynomials where $d(x) \neq 0$ and $\deg d(x) < \deg f(x)$, then
>
> $$f(x) = d(x)q(x) + r(x) \tag{4.3}$$

Theorem 4.2.4: Remainder Theorem

If the polynomial $f(x)$ is divided by $x - c$, then the remainder is $f(c)$.

Theorem 4.2.5: Factor Theorem

Let $f(x)$ be a polynomial. $f(c) = 0$ iff $x - c$ is a factor of $f(x)$.

Theorem 4.2.6: Linear Factorisation Theorem

If $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, where $n \geq 1, a_n \neq 0$, then

$$f(x) = a_n(x - c_1)(x - c_2) \ldots (x - c_n)$$

where $c_1, c_2, \ldots c_n$ are complex numbers.

A polynomial equation of degree n has n roots, counting multiple roots (multiplicities) separately.

Imaginary roots occur in conjugate pairs; if $a + bi$ is a root $(b \neq 0)$, then the imaginary number $a - bi$ is also a root.

Theorem 4.2.7: Fundamental Theorem of Algebra

A polynomial of degree $n > 0$, with real or complex coefficients, has at least one real or complex root.

§4.3   Absolute Value Equations

Common problem-solving techniques:

- Squaring both sides

- Casework: solve each case for x

- Sketching graph

Example 4.3.1

Find all real values of x such that

$$|x + 2| + |2x + 6| + |3x - 3| = 12.$$

Solution. The turning points of the three terms are $x = -2$, $x = -3$, $x = 1$ respectively. Hence, we just need to check the cases:

- $x \leq 3$

- $-3 < x \leq -2$

- $-2 < x \leq 1$

- $x > 1$

$\therefore \quad x = -\dfrac{5}{2}, \; x = \dfrac{7}{6}$ □

Example 4.3.2

How many real solutions x are there to the equation $x|x| + 1 = 3|x|$?

Solution. Two cases: either $x \geq 0$ and $x^2 + 1 = 3x$, or $x < 0$ and $-x^2 + 1 = -3x$. The first case has solutions $\dfrac{3 \pm \sqrt{5}}{2}$ which are both positive. The second case has solutions $\dfrac{3 \pm \sqrt{13}}{2}$ and only one of these is negative. So there are three solutions in total. □

Problems

Problem 4.3.1. Let a, b, c be distinct non-zero real numbers such that

$$a + \frac{1}{b} = b + \frac{1}{c} = c + \frac{1}{a}.$$

Prove that $|abc| = 1$.

Proof. From the given conditions it follows that

$$a - b = \frac{b - c}{bc} \quad b - c = \frac{c - a}{ca} \quad c - a = \frac{a - b}{ab}.$$

Multiplying the above equations gives $(abc)^2 = 1$, from which the desired result follows.
$\square$

Problem 4.3.2. Let $\alpha, \beta, \gamma, \delta$ be the roots of $x^4 - 8x^3 + 24x^2 - 42x + 16 = 0$. Given

$$\left(\frac{2}{\sqrt[4]{\alpha} + \sqrt[4]{\beta} + \sqrt[4]{\gamma}} + \frac{2}{\sqrt[4]{\beta} + \sqrt[4]{\gamma} + \sqrt[4]{\delta}} + \frac{2}{\sqrt[4]{\alpha} + \sqrt[4]{\beta} + \sqrt[4]{\delta}} + \frac{2}{\sqrt[4]{\delta} + \sqrt[4]{\gamma} + \sqrt[4]{\alpha}} \right)^2 = \frac{a\sqrt{b}}{c}$$

where a, b, c are pairwise coprime. Find the value of $a + b + c$.

Hint: Vieta's Relation

Solution. The given quartic equation is simply $(x - 2)^4 = 10x$. so we get the stuff as $\left(\sum_{\text{cyc}} \frac{2 \cdot \sqrt[4]{10}}{2 - \alpha} \right)^2$ this is just $4\sqrt{10} \cdot \left(\frac{f'(2)}{f(2)} \right)^2$, where $f(x)$ is the given polynomial and $\frac{f'(2)}{f(2)} = \frac{1}{2}$.

Hence our answer is $\boxed{\sqrt{10}}$. $\qquad \square$

Problem 4.3.3 (TRIPOS 1878). If $x + y + z = 0$, show that

$$\left(\frac{y-z}{x} + \frac{z-x}{y} + \frac{x-y}{z}\right)\left(\frac{x}{y-z} + \frac{y}{z-x} + \frac{z}{x-y}\right) = 9$$

Proof. We have

$$\left(\frac{y-z}{x} + \frac{z-x}{y} + \frac{x-y}{z}\right)\frac{x}{y-z} = 1 + \frac{x}{y}\cdot\frac{z-x}{y-z} + \frac{x}{z}\cdot\frac{x-y}{y-z}$$

$$= 1 + \frac{xz(z-x) + xy(x-y)}{yz(y-z)}$$

$$= 1 + \frac{x(z^2 - zx + xy - y^2)}{yz(y-z)}$$

$$= 1 + \frac{x}{yz}(x - y - z)$$

$$= 1 + \frac{2x^2}{yz} \quad \because y + z = -x$$

Therefore

$$\left(\frac{y-z}{x} + \frac{z-x}{y} + \frac{x-y}{z}\right)\left(\frac{x}{y-z} + \frac{y}{z-x} + \frac{z}{x-y}\right) = 3 + 2\frac{x^3 + y^3 + z^3}{xyz} = 3 + 6 = 9$$

for, since $x + y + z = 0$, $x^3 + y^3 + z^3 - 3xyz = 0$. □

Problem 4.3.4 (TRIPOS 1878)**.** Find the real roots of the equations:

$$
\begin{cases}
x^2 + z'^2 + y'^2 = a^2 \\
z'^2 + y^2 + x'^2 = b^2 \\
y'^2 + x'^2 + z^2 = c^2
\end{cases}
\qquad
\begin{cases}
y'z' + x'(y+z) = bc \\
z'x' + y'(z+x) = ca \\
x'y' + z'(x+y) = ab
\end{cases}
$$

Solution. We have

$$
b^2 c^2 = \left(z'^2 + y^2 + x'^2\right)\left(y'^2 + x'^2 + z^2\right) =
$$

$\square$

Problem 4.3.5 (SSSMO 2000)**.** For any real numbers a, b and c, find the smallest possible value that the following expression can take:

$$3a^2 + 27b^2 + 5c^2 - 18ab - 30c + 237$$

Proof. By completing squares, the above expression can be rewritten as

$$3(a - 3b)^2 + 5(c - 3)^2 + 192 \geq 192$$

The value 192 is obtainable when $a = 3b$, $c = 3$.

Hence the smallest possible value is $\boxed{192}$. $\square$

Remark. The technique of completing squares is an important tool in determining the extreme values of polynomials.

Problem 4.3.6 (GERMANY)**.** Given that $m^{15} + m^{16} + m^{17} = 0$, solve for m^{18}.

Solution. Factorising gives us

$$m^{15}(m^2 + m + 1) = 0$$

Case 1: $m^{15} = 0$

Then $m = 0$, thus $m^{18} = 0$.

Case 2: $m^2 + m + 1 = 0$

Multiplying $m - 1$ on both sides,

$$(m - 1)(m^2 + m + 1) = 0 \implies m^3 - 1 = 0 \implies m^3 = 1$$

Hence $m^{18} = (m^3)^6 = \boxed{1}$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ $\square$

Problem 4.3.7. Given that for positive real number a,

$$\left(\frac{5}{x}\right)^{\log_a 25} = \left(\frac{3}{x}\right)^{\log_a 9}$$

Solution. Taking log base a at both sides,

$$\log_a \left(\frac{5}{x}\right)^{\log_a 25} = \log_a \left(\frac{3}{x}\right)^{\log_a 9}$$

$$\log_a 25 \times \log_a \left(\frac{5}{x}\right) = \log_a 9 \times \log_a \left(\frac{3}{x}\right)$$

$$2\log_a 5 \times \left(\log_a 5 - \log_a x\right) = 2\log_a 3 \times \left(\log_a 3 - \log_a x\right)$$

Let $p = \log_a 5$, $q = \log_a 3$. The equation can be rewritten as

$$2(p - q)(p + q) = 2(p - q) \times \log_a x$$

Dividing $2(p - q)$ for both sides, $p + q = \log_a x \implies \boxed{x = 15}$. $\square$

Problem 4.3.8. Consider the following expression. Find all possible real roots.

$$\frac{1}{x^2 - 10x - 29} + \frac{1}{x^2 - 10x - 45} - \frac{2}{x^2 - 10x - 69} = 0$$

Solution. Since the given equation looks quite complicated to solve, we try the substitution method. Let $a = (x-5)^2$, then the equation can be rewritten as

$$\frac{1}{a - 54} + \frac{1}{a - 70} - \frac{2}{a - 94} = 0$$

Solving quadratically gives us $\boxed{x = 13}$ or $\boxed{x = -3}$. □

Problem 4.3.9 (DOKA)**.** Given that $f(x) = \dfrac{x}{x-3}$, $f^8(x) = \dfrac{x}{ax+b}$, where a and b are integers. Find a and b.

Solution. Observe that

$$f(x) = \frac{x}{x-p}$$

$$f^2(x) = \frac{x}{(1-p)x+p^2}$$

$$f^3(x) = \frac{x}{(1-p+p^2)x-p^3}$$

$$f^4(x) = \frac{x}{(1-p+p^2-p^3)x+p^4}$$

Suppose $f^n(x) = \dfrac{x}{a_n x - b_n}$,

$$a_n = (-3)^0 + (-3)^1 + \cdots + (-3)^{n-1}$$

$$b_n = (-3)^n$$

Hence $\boxed{a = -1640}$ and $\boxed{b = 6561}$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Problem 4.3.10 (Oxford MAT 2022)**.** Find the constant term of the expression

$$\left(x + 1 + \frac{1}{x}\right)^4$$

Solution. We calculate the square of $(x + 1 + x^{-1})$ first;

$$x^2 + 2x + 1 + 2x^{-1} + x^{-2}$$

Now if we were to square this expression, the constant term independent of x would be

$$2(x^2)(x^{-2}) + 2(2x)(2x^{-1}) + 32$$

Most of the terms have a factor of 2 because they occur in either order. This sum is $2 + 8 + 9 = \boxed{19}$. $\qquad\square$

Problem 4.3.11 (Oxford MAT)**.** How many real solutions x are there to the following equation?

$$\log_2(2x^3 + 7x^2 + 2x + 3) = 3\log_2(x+1) + 1$$

Solution. We can use laws of logarithms to write the right-hand side of the given equation as

$$\log_2(2x^3 + 6x^2 + 6x + 2).$$

Since $\log_2 x$ is an increasing function for $x > 0$, we can compare the arguments of the logarithms, provided that both are positive. This gives the polynomial equation

$$2x^3 + 7x^2 + 2x + 3 = 2x^3 + 6x^2 + 6x + 2$$

which rearranges to $x^2 - 4x + 1 = 0$, which has $\boxed{2}$ real solutions. We should check that $2x^3 + 7x^2 + 2x + 3$ is positive for these roots, but it definitely is because the roots of the quadratic are both positive and all the coefficients of the cubic are positive. $\square$

Problem 4.3.12 (CHINA 1979)**.** Given that $x^2 - x + 1 = 0$, find the value of $x^{2015} - x^{2014}$.

Solution. Multiplying both sides by $x + 1$,

$$(x^2 - x + 1)(x + 1) = 0 \implies x^3 + 1 = 0 \implies x^3 = -1$$

Substituting this into the given expression,

$$x^{2015} - x^{2014} = x^{2014}(x - 1) = x^{2014} \cdot x^2 = x^{2016} = (x^3)^{672} = (-1)^6 = \boxed{1}$$

$\square$

Problem 4.3.13 (DOKA)**.** For a positive integer n, we have the polynomial

$$\left(2 + \frac{x}{2}\right)\left(2 + \frac{2x}{2}\right)\left(2 + \frac{3x}{2}\right)\cdots\left(2 + \frac{nx}{2}\right) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where $a_0, \ldots, a_n$ are the coefficients of the polynomial. Find the smallest possible value of n if $2a_0 + 4a_1 + 8a_2 + \cdots + 2^{n+1}a_n - (n+1)!$ is divisible by 2020.

Solution. By comparing the coefficients of x^n,

$$\left(\frac{1}{2}\right)\left(\frac{2}{2}\right)\left(\frac{3}{2}\right)\cdots\left(\frac{n}{2}\right) = \frac{n!}{2^n} = a_n.$$

Now if we let $x = 2$, notice that

$$(2+1)(2+2)(2+3)\cdots(2+n) = a_0 + a_1(2) + a_2(2)^2 + a_3(2)^3 + \cdots + a_n(2)^n$$
$$(3)(4)(5)\cdots(n+2) = a_0 + 2a_1 + 4a_2 + 8a_3 + \cdots + 2^n a_n$$
$$\frac{(n+2)!}{2} = a_0 + 2a_1 + 4a_2 + 8a_3 + \cdots + 2^n a_n$$
$$(n+2)! = 2a_0 + 4a_1 + 8a_2 + \cdots + 2^{n+1}a_n$$

Therefore

$$2a_0 + 4a_1 + 8a_2 + \cdots + 2^{n+1}a_n - (n+1)! = (n+2)! - (n+1)! = (n+1)!(n+1)$$

which is divisible by 2020.

Smallest possible n is when $(n+1)!$ is divisible by 2020. Hence $n + 1 = 101$ gives $\boxed{n = 100}$.

$\square$

Problem 4.3.14. Consider the sequence of real numbers $\{a_n\}$ is defined by $a_1 = \dfrac{1}{1000}$ and $a_{n+1} = \dfrac{a_n}{na_n - 1}$ for $n \geq 1$. Find the value of $\dfrac{1}{a_{2020}}$.

Solution.

$$\frac{1}{a_{n+1}} = \frac{na_n - 1}{n} = n - \frac{1}{a_n}$$

Listing out terms,

$$\frac{1}{a_{2020}} = 2019 - \frac{1}{a_{2019}}$$
$$-\frac{1}{a_{2019}} = -2018 + \frac{1}{a_{2018}}$$
$$\frac{1}{a_{2018}} = 2017 - \frac{1}{a_{2017}}$$
$$\vdots$$
$$\frac{1}{a_4} = 3 - \frac{1}{a_3}$$
$$-\frac{1}{a_3} = -2 + \frac{1}{a_2}$$
$$\frac{1}{a_2} = 1 - \frac{1}{a_1} = 1 - 1000$$

Thus $\dfrac{1}{a_{2020}} = 2019 - 2018 + 2017 - 2016 + \cdots + 3 - 2 + 1 - 1000 = \boxed{10}$. $\qquad\square$

Problem 4.3.15. Let a, b, c be non-zero real numbers such that $a + b + c = 0$ and

$$28(a^4 + b^4 + c^4) = a^7 + b^7 + c^7.$$

Find $a^3 + b^3 + c^3$.

Proof. We use two lemmas.

Lemma 4.3.1. For $a + b + c = 0$,

$$2(a^4 + b^4 + c^4) = (a^2 + b^2 + c^2)^2 \tag{1}$$

Proof. We prove this by direct expansion.

$$
\begin{aligned}
2(a^4 + b^4 + c^4) &= 2[a^4 + b^4 + (a + b)^4] \\
&= 4(a^4 + 2a^3b + 3a^2b^2 + 2ab^3 + b^4) \\
&= 4(a^2 + ab + b^2)^2 \\
&= (a^2 + b^2 + c^2)^2
\end{aligned}
$$

$\square$

Lemma 4.3.2. For $a + b + c = 0$,

$$4(a^7 + b^7 + c^7) = 7abc(a^2 + b^2 + c^2)^2$$

Proof. This is a restatement of $(a + b)^7 - a^7 - b^7 = 7ab(a + b)(a^2 + ab + b^2)^2$. $\square$

Dividing (2) by (1) gives us

$$\frac{2(a^7 + b^7 + c^7)}{a^4 + b^4 + c^4} = 7abc \implies abc = 8$$

Hence $a^3 + b^3 + c^3 = 3abc = \boxed{24}$. $\square$

5 **Inequalities**

For Mathematics Olympiad competitions, you are only required to apply these inequalities; hence the proofs of the following inequalities will not be included in this book.

§5.1 AM–GM Inequality

The most well-known and frequently used inequality is the Arithmetic mean–Geometric mean inequality, also known as the AM–GM inequality. The inequality simply states that the arithmetic mean is greater than or equal to the geometric mean.

§5.1.1 General AM–GM Inequality

> **Theorem 5.1.1: AM–GM**
>
> For non-negative real $a_1, a_2, \ldots, a_n$,
> $$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n} \tag{5.1}$$
> Equality holds iff $a_1 = a_2 = \cdots = a_n$.

> **Example 5.1.1**
>
> For real numbers a, b, c prove that
> $$a^2 + b^2 + c^2 \geq ab + bc + ca.$$

Proof. By AM–GM inequality, we have

$$a^2 + b^2 \geq 2ab$$
$$b^2 + c^2 \geq 2bc$$
$$c^2 + a^2 \geq 2ca$$

Adding the three inequalities and then dividing by 2 we get the desired result. Equality holds if and only if $a = b = c$. $\qquad\square$

> **Example 5.1.2**
>
> Let $a_1, a_2, \ldots, a_n$ be positive real numbers such that $a_1 a_2 \cdots a_n = 1$. Prove that
> $$(1 + a_1)(1 + a_2)\cdots(1 + a_n) \geq 2^n.$$

Proof. By AM–GM,

$$1 + a_1 \geq 2\sqrt{a_1}$$
$$1 + a_2 \geq 2\sqrt{a_2}$$
$$\vdots$$
$$1 + a_n \geq 2\sqrt{a_n}$$

Multiplying the above inequalities and using the fact $a_1 a_2 \cdots a_n = 1$ we get our desired result. Equality holds if and only if $a_i = 1$ for $i = 1, 2, \ldots, n$. $\qquad\square$

> **Example 5.1.3**
>
> Let a, b, c be non-negative real numbers. Prove that
> $$(a + b)(b + c)(c + a) \geq 8abc.$$

Proof. By AM–GM,

$$a + b \geq 2\sqrt{ab}$$
$$b + c \geq 2\sqrt{bc}$$
$$c + a \geq 2\sqrt{ca}$$

Multiplying the above inequalities gives us our desired result. Equality holds if and only if $a = b = c$. $\qquad\square$

> **Example 5.1.4**
>
> Let $a, b, c > 0$. Prove that
> $$\frac{a^3}{bc} + \frac{b^3}{ca} + \frac{c^3}{ab} \geq a + b + c.$$

Proof. By AM–GM we deduce that

$$\frac{a^3}{bc} + b + c \geq 3a$$
$$\frac{b^3}{ca} + c + a \geq 3b$$
$$\frac{c^3}{ab} + a + b \geq 3c$$

Adding the three inequalities we get our desired result. $\qquad\square$

Example 5.1.5

Let a, b, c be positive real numbers. Prove that

$$ab(a + b) + bc(b + c) + ca(c + a) \geq \sum_{\text{cyc}} ab\sqrt{\frac{a}{b}(b + c)(c + a)}.$$

Proof. By AM–GM,

$$2ab(a + b) + 2ac(a + c) + 2bc(b + c)$$
$$= ab(a + b) + ac(a + c) + bc(b + c) + ab(a + b) + ac(a + c) + bc(b + c)$$
$$= a^2(b + c) + b^2(a + c) + c^2(a + b) + (a^2b + b^2c + ca^2) + (ab^2 + bc^2 + ca^2)$$
$$\geq a^2(b + c) + b^2(a + c) + c^2(a + b) + (a^2b + b^2c + c^2a) + 3abc$$
$$= a^2(b + c) + b^2(a + c) + c^2(a + b) + ab(a + c) + bc(a + b) + ac(b + c)$$
$$= \left(a^2(b + c) + ab(a + c)\right) + \left(b^2(a + c) + bc(a + b)\right) + \left(c^2(a + b) + ac(b + c)\right)$$
$$\geq 2\sqrt{a^3b(b + c)(c + a)} + 2\sqrt{b^3c(c + a)(a + b)} + 2\sqrt{c^3a(a + b)(b + c)}$$
$$= 2ab\sqrt{\frac{a}{b}(b + c)(c + a)} + 2bc\sqrt{\frac{b}{c}(c + a)(a + b)} + 2ca\sqrt{\frac{c}{a}(a + b)(b + c)}$$

Equality holds if and only if $a = b = c$. □

Example 5.1.6: Nesbitt's Inequality

For positive real numbers a, b, c prove that

$$\frac{a}{b + c} + \frac{b}{c + a} + \frac{c}{a + b} \geq \frac{3}{2}.$$

Proof. Our inequality is equivalent to

$$1 + \frac{a}{b + c} + 1 + \frac{b}{c + a} + 1 + \frac{c}{a + b} \geq \frac{9}{2}$$

or

$$(a + b + c)\left(\frac{1}{b + c} + \frac{1}{c + a} + \frac{1}{a + b}\right) \geq \frac{9}{2}$$

Using AM–GM, we have

$$\frac{(b + c) + (c + a) + (a + b)}{3} \geq \sqrt[3]{(b + c)(c + a)(a + b)}$$

and

$$\frac{\frac{1}{b+c} + \frac{1}{c+a} + \frac{1}{a+b}}{3} \geq \frac{1}{\sqrt[3]{(b + c)(c + a)(a + b)}}$$

□

> **Example 5.1.7**
>
> For positive real numbers p, q, r, find the minimum of
> $$\frac{p+q}{r} + \frac{q+r}{p} + \frac{r+p}{q}.$$

Solution. We split the expression up first into

$$\frac{p}{r} + \frac{q}{r} + \frac{r}{p} + \frac{q}{p} + \frac{p}{q} + \frac{r}{q}$$

Now we pair up terms as such:

$$\left(\frac{p}{r} + \frac{r}{p}\right) + \left(\frac{q}{r} + \frac{r}{q}\right) + \left(\frac{q}{p} + \frac{p}{q}\right)$$

Applying AM–GM to each pair, the result follows easily. $\qquad\square$

§5.1.2   Weighted AM–GM Inequality

The weighted version of the AM–GM inequality follows from the original AM–GM inequality.

> **Theorem 5.1.2: Weighted AM–GM**
>
> For positive real $a_1, a_2, \ldots, a_n$ and positive integers $\omega_1, \omega_2, \ldots, \omega_n$, by AM–GM,
>
> $$\frac{\omega_1 a_1 + \omega_2 a_2 + \cdots + \omega_n a_n}{\omega_1 + \omega_2 + \cdots + \omega_n} \geq \left(a_1^{\omega_1} + a_2^{\omega_2} + \cdots + a_n^{\omega_n}\right)^{\frac{1}{\omega_1 + \omega_2 + \cdots + \omega_n}} \qquad (5.2)$$

Or equivalently in symbols

$$\frac{\sum \omega_i a_i}{\sum \omega_i} \geq \left(\prod a_i^{\omega_i}\right)^{\frac{1}{\sum \omega_i}}$$

> **Example 5.1.8**
>
> Let a, b, c be positive real numbers such that $a + b + c = 3$. Show that
> $$a^b b^c c^a \leq 1$$

Proof. Notice that

$$1 = \frac{a+b+c}{3} \geq \frac{ab+bc+ca}{a+b+c} \geq \left(a^b b^c c^a\right)^{\frac{1}{a+b+c}}$$

which implies $a^b b^c c^a \leq 1$. $\qquad\square$

§5.1.3   Other mean quantities

For non-negative real $a_1, a_2, \ldots, a_n$, the **harmonic mean** is given by

$$\frac{1}{\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}}$$

For non-negative real $a_1, a_2, \ldots, a_n$, the **square mean** is given by

$$\frac{\sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}}{n}$$

Relating AM, GM, HM, and SM, we have the following inequality:

$$SM \geq AM \geq GM \geq HM$$

§5.2   Cauchy–Schwarz and Hölder's Inequalities

Theorem 5.2.1: Cauchy–Schwarz

For real $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$,

$$\left(a_1{}^2 + a_2{}^2 + \cdots + a_n{}^2\right)\left(b_1{}^2 + b_2{}^2 + \cdots + b_n{}^2\right) \geq \left(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n\right)^2 \qquad (5.3)$$

Equality holds iff $\dfrac{a_1}{b_1} = \dfrac{a_2}{b_2} = \cdots = \dfrac{a_n}{b_n}$.

Theorem 5.2.2: Titu

For positive real $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$,

$$\frac{a_1{}^2}{b_1} + \frac{a_2{}^2}{b_2} + \cdots + \frac{a_n{}^2}{b_n} \geq \frac{\left(a_1 + a_2 + \cdots + a_n\right)^2}{b_1 + b_2 + \cdots + b_n} \qquad (5.4)$$

Equality holds iff $\dfrac{a_1}{b_1} = \dfrac{a_2}{b_2} = \cdots = \dfrac{a_n}{b_n}$.

Example 5.2.1: IMO 1995

Let a, b, c be positive real numbers such that $abc = 1$. Prove that

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

Proof. Let $x = \frac{1}{a}, y = \frac{1}{b}, z = \frac{1}{c}$. Then by the given condition we obtain $xyz = 1$. Note that

$$\sum \frac{1}{a^3(b + c)} = \sum \frac{1}{\frac{1}{x^3}\left(\frac{1}{y} + \frac{1}{z}\right)} = \sum \frac{x^2}{y + z}$$

Now by Cauchy–Schwarz,

$$\sum \frac{x^2}{y+z} \geq \frac{(x+y+z)^2}{2(x+y+z)} = \frac{x+y+z}{2}$$

and by AM–GM,

$$\frac{1}{2}(x+y+z) \geq \frac{3}{2}\sqrt[3]{xyz} = \frac{3}{2}$$

Hence proven. □

Theorem 5.2.3: Hölder

For positive real $a_1, a_2, \ldots, a_n$ and $b_1, b_2, \ldots, b_n$, and positive real p, q that satisfy $\frac{1}{p} + \frac{1}{q} = 1$,

$$\left(\sum_{i=1}^{n} a_i{}^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{n} b_i{}^q\right)^{\frac{1}{q}} \geq \sum_{i=1}^{n} a_i b_i \tag{5.5}$$

Remark. Cauchy–Schwarz is a special case of Hölder, when $p = q = 2$.

§5.3 Rearrangement and Chebyshev's Inequalities

Theorem 5.3.1: Chybeshev

For real $a_1 \geq \cdots \geq a_n$ and $b_1 \geq \cdots \geq b_n$,

$$\frac{a_1 b_1 + \cdots + a_n b_n}{n} \geq \frac{a_1 + \cdots + a_n}{n} \frac{b_1 + \cdots + b_n}{n} \tag{5.6}$$

Theorem 5.3.2: Rearrangement

For real $a_1 \geq \cdots \geq a_n$ and $b_1 \geq \cdots \geq b_n$, for any permutation σ of $\{1, \ldots, n\}$,

$$\sum_{i=1}^{n} a_i b_i \geq \sum_{i=1}^{n} a_i b_{\sigma(i)} \geq \sum_{i=1}^{n} a_i b_{n+1-i} \tag{5.7}$$

§5.4 Other Useful Strategies

Theorem 5.4.1: Triangle inequality

For real $a_1, a_2, \ldots, a_n$,

$$|a_1| + |a_2| + \cdots + |a_n| \geq |a_1 + a_2 + \cdots + a_n| \tag{5.8}$$

Equality holds iff $a_1, a_2, \cdots, a_n$ are all non-negative.

Theorem 5.4.2: Schur

For non-negative real a, b, c and $n > 0$,

$$a^n(a-b)(a-c) + b^n(b-c)(b-a) + c^n(c-a)(c-b) \geq 0 \qquad (5.9)$$

Equality holds iff either $a = b = c$ or when two of a, b, c are equal and the third is 0.

Proof. WLOG, let $a \geq b \geq c$. Note that

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

Clearly, $a^n \geq b^n \geq 0$, and $a - c \geq b - c \geq 0$. Thus,

$$(a-b)(a^n(a-c) - b^n(b-c)) \geq 0 \implies a^n(a-b)(a-c) + b^n(b-a)(b-c) \geq 0$$

However, $c^n(c-a)(c-b) \geq 0$, and thus the proof is complete. $\qquad \square$

When $n = 1$, we have the well-known inequality:

$$a^3 + b^3 + c^3 + 3abc \geq a^2b + a^2c + b^2a + b^2c + c^2a + c^2b$$

When $n = 2$, an equivalent form is:

$$a^4 + b^4 + c^4 + abc(a+b+c) \geq a^3b + a^3c + b^3a + b^3c + c^3a + c^3b$$

Theorem 5.4.3: Minkowski

For positive real $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ and $p > 1$,

$$\left(\sum_{i=1}^{n} a_i{}^p \right)^{\frac{1}{p}} + \left(\sum_{i=1}^{n} b_i{}^p \right)^{\frac{1}{p}} \geq \left(\sum_{i=1}^{n} (a_i + b_i)^p \right)^{\frac{1}{p}} \qquad (5.10)$$

Theorem 5.4.4: Generalised Minkowski

Let $a_{ij} \geq 0$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ and let $p > 1$, then

$$\left[\sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij} \right) \right]^{\frac{1}{p}} \leq \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij}{}^p \right)^{\frac{1}{p}} \qquad (5.11)$$

Definition 5.4.1: Convex function

> ### Theorem 5.4.5: Jensen
>
> Let a real-valued function f be convex on the interval I. Let $x_1, \ldots, x_n \in I$ and $\omega_1, \ldots, \omega_n \geq 0$. Then we have
>
> $$\frac{\omega_1 f(x_1) + \omega_2 f(x_2) + \cdots + \omega_n f(x_n)}{\omega_1 + \omega_2 + \cdots + \omega_n} \geq f\left(\frac{\omega_1 x_1 + \omega_2 x_2 + \cdots + \omega_n x_n}{\omega_1 + \omega_2 + \cdots + \omega_n}\right) \qquad (5.12)$$
>
> If f is concave, the direction of the inequality is flipped.
> In particular, if we take the weights $\omega_1 = \omega_2 = \cdots = \omega_n = 1$, we get the inequality
>
> $$\frac{f(x_1) + f(x_2) + \cdots + f(x_n)}{n} \geq f\left(\frac{x_1 + x_2 + \cdots + x_n}{n}\right).$$

AM–GM inequality is one of the special cases of Jensen's inequality.

> ### Theorem 5.4.6: Bernoulli
>
> For $x > -1, x \neq 0$ and integer $n > 1$,
>
> $$(1+x)^n > 1 + nx \qquad (5.13)$$

Problems

Problem 5.4.1. Given that $a, b > 0$ and $ab(a + b) = 2000$, find the minimum value of

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{a + b}.$$

Solution. Using AM–GM,

$$a + b \geq 2\sqrt{ab}$$

$$\left(\frac{a + b}{2}\right)^2 \geq ab$$

$$\left(\frac{a + b}{2}\right)^2 (a + b) \geq ab(a + b)$$

$$\frac{(a + b)^3}{4} \geq 2000$$

$$a + b \geq 20$$

Using AM–GM,

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{a + b} = \frac{1}{2a} + \frac{1}{2a} + \frac{1}{2b} + \frac{1}{2b} + \frac{1}{a + b}$$

$$\geq 5\sqrt[5]{\frac{1}{16}\frac{a + b}{a^2 b^2 (a + b)^2}}$$

$$\geq 5\left(\frac{1}{20}\right) = \boxed{\frac{1}{4}}$$

Equality holds if and only if $\dfrac{1}{2a} = \dfrac{1}{2b} = \dfrac{1}{a + b}$, or $a = b = 10$. $\qquad\qquad\square$

Problem 5.4.2 (HCI 2020 Prelim Q7)**.** Given positive reals a, b, c, prove that

$$\frac{(a+1)^3}{b} + \frac{(b+1)^3}{c} + \frac{(c+1)^3}{a} \geq \frac{81}{4}$$

Proof. Applying AM-GM gives us

$$\frac{(a+1)^3}{b} + \frac{(b+1)^3}{c} + \frac{(c+1)^3}{a} \geq \frac{3(a+1)(b+1)(c+1)}{\sqrt[3]{abc}}$$

We note the denominator is a cube root and hence we want to get the numerator to be a product of cube roots containing a, b and c so that they cancel out. To do so, split each term in the bracket into three terms and apply AM-GM on the numerator:

$$\frac{3(a+1)(b+1)(c+1)}{\sqrt[3]{abc}} = \frac{3\left(a+\frac{1}{2}+\frac{1}{2}\right)\left(b+\frac{1}{2}+\frac{1}{2}\right)\left(c+\frac{1}{2}+\frac{1}{2}\right)}{\sqrt[3]{abc}}$$

$$\geq \frac{81\sqrt[3]{\frac{a}{4}}\sqrt[3]{\frac{b}{4}}\sqrt[3]{\frac{c}{4}}}{\sqrt[3]{abc}} = \frac{81}{4}$$

$\square$

Problem 5.4.3 (HCI 2020 Prelim Q7)**.** Given $x, y, z \geq 1$, $\dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = 2$, prove that

$$\sqrt{x + y + z} \geq \sqrt{x - 1} + \sqrt{y - 1} + \sqrt{z - 1}$$

Solution. The expression is certainly odd, as we would usually expect some squares in a Cauchy. We note that if we square both sides, we get something that better resembles a Cauchy inequality.

We construct the inequality

$$(x + y + z)\left(\frac{x - 1}{x} + \frac{y - 1}{y} + \frac{z - 1}{z}\right) \geq (\sqrt{x - 1} + \sqrt{y - 1} + \sqrt{z - 1})^2$$

where

$$\frac{x - 1}{x} + \frac{y - 1}{y} + \frac{z - 1}{z} = 3 - \left(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}\right) = 3 - 2 = 1$$

so applying Cauchy gives us the desired result. $\qquad \square$

Problem 5.4.4 (HCI 2020 Prelim Q7)**.** Given that $a+b+c+d = 3$ and $a^2+2b^2+3c^2+6d^2 = 5$, prove that $1 \le a \le 2$.

Solution. Since the desired result concerns the variable a, we naturally try to express the remaining variables in terms of a.

We hence yield

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

and

$$2b^2 + 3c^2 + 6d^2 = 5 - a^2$$

Note that since both the sum of variables and the sum of the squares of said variables are given, it is an indication that Cauchy is the way to go for this question.

Applying Cauchy,

$$(2b^2 + 3c^2 + 6d^2)(18 + 12 + 6) \ge (6b + 6c + 6d)^2$$

Substituting in the relevant expressions gives us $36(5 - a^2) \ge (18 - 6a)^2$ which is a fairly easy inequality to solve. $\qquad\square$

Problem 5.4.5. Prove that for all $n \in \mathbb{N}$,

$$\sqrt{1^2 + 1} + \sqrt{2^2 + 1} + \cdots + \sqrt{n^2 + 1} \geq \frac{n}{2}\sqrt{n^2 + 2n + 5}.$$

Proof. Define the function $f(x) = \sqrt{x^2 + 1}$. Observe that for $x \to \infty$, we have $f(x) \to |x|$, so the graph is convex.

Applying Jensen's inequality with reals $x_1 = 1, x_2 = 2, \ldots, x_n = n$,

$$\frac{f(x_1) + f(x_2) + \cdots + f(x_n)}{n} \geq f\left(\frac{x_1 + x_2 + \cdots + x_n}{n}\right)$$

$$\frac{f(1) + f(2) + \cdots + f(n)}{n} \geq f\left(\frac{1 + 2 + \cdots + n}{n}\right)$$

$$\frac{\sqrt{1^2 + 1} + \sqrt{2^2 + 1} + \cdots + \sqrt{n^2 + 1}}{n} \geq f\left(\frac{n(n+1)/2}{n}\right)$$

$$= f\left(\frac{n+1}{2}\right) = \frac{1}{2}\sqrt{n^2 + 2n + 5}$$

$\square$

Problem 5.4.6 (MACEDONIA 2016)**.** For $n \geq 3$, $a_1, a_2, \ldots, a_n \in \mathbb{R}^+$ satisfy

$$\frac{1}{1 + a_1{}^4} + \frac{1}{1 + a_2{}^4} + \cdots + \frac{1}{1 + a_n{}^4} = 1.$$

Prove that

$$a_1 a_2 \cdots a_n \geq (n-1)^{\frac{n}{4}}.$$

Proof. Let $b_i = a_i{}^4$ where $b_i \geq 0$. The given condition becomes

$$\frac{1}{1 + b_1} + \frac{1}{1 + b_2} + \cdots + \frac{1}{1 + b_n} = 1.$$

and we want to prove

$$b_1 b_2 \cdots b_n \geq (n-1)^n.$$

Let $t_i = \dfrac{1}{1 + b_i}$. Rewriting the given condition gives us

$$t_1 + t_2 + \cdots + t_n = 1.$$

and we want to prove

$$\frac{1 - t_1}{t_1} \frac{1 - t_2}{t_2} \cdots \frac{1 - t_n}{t_n} \geq (n-1)^n.$$

Using AM-GM, we have

$$\frac{1 - t_1}{t_1} \frac{1 - t_2}{t_2} \cdots \frac{1 - t_n}{t_n} = \frac{t_2 + t_3 + \cdots + t_n}{t_1} \frac{t_1 + t_3 + \cdots + t_n}{t_2} \cdots \frac{t_1 + t_2 + \cdots + t_{n-1}}{t_n}$$

$$\geq \frac{(n-1)(t_2 t_3 \cdots t_n)^{\frac{1}{n-1}}}{t_1} \frac{(n-1)(t_1 t_3 \cdots t_n)^{\frac{1}{n-1}}}{t_2} \cdots \frac{(n-1)(t_1 t_2 \cdots t_{n-1})^{\frac{1}{n-1}}}{t_n}$$

$$= (n-1)^n$$

$\square$

Problem 5.4.7 (USAMO 2012)**.** Find all integers $n \geq 3$ such that among any n positive real numbers $a_1, a_2, \ldots, a_n$ with

$$\max(a_1, a_2, \ldots, a_n) \leq n \cdot \min(a_1, a_2, \ldots, a_n),$$

there exist three that are the side lengths of an acute triangle.

Solution. We claim that $n \geq 13$ are all the satisfying positive integers.

WLOG, let $a_1 \leq a_2 \leq \cdots \leq a_n$. Three positive real numbers $a \leq b \leq c$ are the side lengths of an acute triangle iff $a^2 + b^2 > c^2$.

Thus, if our n positive real numbers contain no such triple, we must have $a_i^2 + a_j^2 \leq a_k^2$ for all $i < j < k$.

We have the following claim:

Lemma 5.4.1. Let $S = \{a_1, a_2, \cdots, a_n\}$ be a set of $n \geq 3$ positive real numbers, where $a_1 \leq a_2 \leq \cdots \leq a_n$. If S contains no three numbers that are side lengths of an acute triangle, we have $a_i \geq F_i \cdot a_1^2$ for all $1 \leq i \leq n$, where F_i is the i-th Fibonacci number.

Proof. If $n = 3$, we must have $a_1^2 + a_2^2 \leq a_3^2$. And since $a_1^2 \leq a_2^2$ and $a_3^2 \geq a_1^2 + a_2^2 \geq 2a_2^2$, the claim holds for $n = 3$.

Assume that the claim holds for all $t \leq n$. Consider a set S of $n + 1$ real numbers such that $a_1 \leq a_2 \leq \cdots \leq a_{n+1}$ and S contains no three numbers that are side lengths of an acute triangle. Then, we must have

$$a_1^2 + a_2^2 \leq a_3^2$$
$$a_2^2 + a_3^2 \leq a_4^2$$
$$\vdots$$
$$a_{n-1}^2 + a_n^2 \leq a_{n+1}^2.$$

Since the statement holds for all $t \leq n$, we have $a_i \geq F_i \cdot a_1^2$ for all $1 \leq i \leq n$. Thus, $a_{n+1}^2 \geq a_{n-1}^2 + a_n^2 \geq F_{n-1} \cdot a_1^2 + F_n \cdot a_1^2 = F_{n+1} \cdot a_1^2$. QED $\square$

Now, if $n \geq 13$, we have $a_n \geq F_n \cdot a_1^2$. However, since $\max(a_1, a_2, \ldots, a_n) \leq n \cdot \min(a_1, a_2, \ldots, a_n)$, we have $n \cdot a_1 \geq a_n$, or $a_n^2 \geq n^2 \cdot a_1^2$. But for all $n \geq 13$, we have $n^2 < F_n$, hence $a_n \geq F_n \cdot a_1^2 > n^2 a_1^2 \geq a_n$, which is absurd. Thus for all $n \geq 13$, we will always have three numbers that are side lengths of an acute triangle.

For $n \leq 12$, the set $S = \{\sqrt{F_i} t \mid 1 \leq i \leq n, t \in \mathbb{R}^+, F_i \text{ is the } i\text{-th Fibonacci number}\}$ satisfies that it contains no three numbers that are side lengths of an acute triangle. $\square$

Problem 5.4.8 (IMO 2000). Let a, b, c be positive real numbers so that $abc = 1$. Prove that

$$\left(a - 1 + \frac{1}{b}\right)\left(b - 1 + \frac{1}{c}\right)\left(c - 1 + \frac{1}{a}\right) \leq 1.$$

Proof. Let $a = \dfrac{x}{y}, b = \dfrac{y}{z}, c = \dfrac{z}{x}$, then

$$\prod_{cyc}(x - y + z) \leq xyz \iff (x^3 + y^3 + z^3) + 3xyz \geq \sum_{cyc} x^2 y + \sum_{cyc} x^2 z$$

This holds by Schur's inequality. $\qquad\square$

Problem 5.4.9. Show that

$$\sum_{k=1}^{n} a_k^2 \geq a_1 a_2 + a_2 a_3 + \cdots + a_{n-1} a_n + a_n a_1$$

Proof. Multiply both sides by 2,

$$2 \sum_{k=1}^{n} a_k^2 \geq 2\left(a_1 a_2 + a_2 a_3 + \cdots + a_{n-1} a_n + a_n a_1\right)$$

Subtracting each side by the RHS,

$$\left(a_1 - a_n\right)^2 + \left(a_2 - a_1\right)^2 + \left(a_3 - a_2\right)^2 + \cdots + \left(a_n - a_{n-1}\right)^2 \geq 0$$

which is always true. $\square$

Problem 5.4.10 (CANADA/1969)**.** Show that if $\dfrac{a_1}{b_1} = \dfrac{a_2}{b_2} = \dfrac{a_3}{b_3}$ and p_1, p_2, p_3 are not all zero, then

$$\left(\frac{a_1}{b_1}\right)^n = \frac{p_1 a_1{}^n + p_2 a_2{}^n + p_3 a_3{}^n}{p_1 b_1{}^n + p_2 b_2{}^n + p_3 b_3{}^n}$$

for every positive integer n.

Proof. Instead of proving the two expressions equal, we prove that their difference equals zero.

Subtracting the LHS from the RHS,

$$\frac{p_1 a_1{}^n + p_2 a_2{}^n + p_3 a_3{}^n}{p_1 b_1{}^n + p_2 b_2{}^n + p_3 b_3{}^n} - \frac{a_1{}^n}{b_1{}^n} = 0$$

Finding a common denominator, the numerator becomes

$$b_1{}^n \left(p_1 a_1{}^n + p_2 a_2{}^n + p_3 a_3{}^n\right) - a_1{}^n \left(p_1 b_1{}^n + p_2 b_2{}^n + p_3 b_3{}^n\right)$$
$$= p_2 \left(a_2{}^n b_1{}^n - a_1{}^n b_2{}^n\right) + p_3 \left(a_3{}^n b_1{}^n - a_1{}^n b_3{}^n\right) = 0$$

(The denominator is irrelevant since it never equals zero)

From $\dfrac{a_1}{b_1} = \dfrac{a_2}{b_2}$, we have

$$a_1{}^n b_2{}^n = a_2{}^n b_1{}^n$$

Similarly, from $\dfrac{a_1}{b_1} = \dfrac{a_3}{b_3}$, we have

$$a_1{}^n b_3{}^n = a_3{}^n b_1{}^n$$

Hence, $a_2{}^n b_1{}^n - a_1{}^n b_2{}^n = a_3{}^n b_1{}^n - a_1{}^n b_3{}^n = 0$ and our proof is complete. $\square$

6 Sequences and Series

§6.1 Summation

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \tag{6.1}$$

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \tag{6.2}$$

$$\sum_{i=1}^{n} i^3 = \left[\frac{n(n+1)}{2}\right]^2 \tag{6.3}$$

Proof. These can be proven using mathematical induction. $\qquad\square$

§6.2 Telescoping sums

A sum in which subsequent terms cancel each other, leaving only initial and final terms. For example,

$$\begin{aligned}
S &= \sum_{i=1}^{n-1}(a_i - a_{i+1}) \\
&= (a_1 - a_2) + (a_2 - a_3) + \ldots + (a_{n-2} - a_{n-1}) + (a_{n-1} - a_n) \\
&= a_1 - a_n
\end{aligned}$$

Example 6.2.1

Evaluate the following sum:

$$\frac{1}{\sqrt{1}+\sqrt{2}} + \frac{1}{\sqrt{2}+\sqrt{3}} + \cdots + \frac{1}{\sqrt{99}+\sqrt{100}}.$$

Solution.

$$\frac{1}{\sqrt{n+1}+\sqrt{n}} = \frac{\sqrt{n+1}-\sqrt{n}}{(\sqrt{n+1}+\sqrt{n})(\sqrt{n+1}-\sqrt{n})}$$
$$= \sqrt{n+1}-\sqrt{n}$$

Doing this for each fraction gives us

$$(\sqrt{2}-\sqrt{1}) + (\sqrt{3}-\sqrt{2}) + \cdots + (\sqrt{100}-\sqrt{99}) = \sqrt{100}-\sqrt{1} = 9$$

□

Example 6.2.2

Evaluate the following sum:
$$\sum_{n=1}^{2015} \frac{1}{n^2 + 3n + 2}.$$

Solution. A common method is to use partial fractions which will cancel each other out.

$$\frac{1}{n^2 + 3n + 2} = \frac{1}{n+1} - \frac{1}{n+2}$$

$$\sum_{n=1}^{2015} \left(\frac{1}{n+1} - \frac{1}{n+2}\right) = \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{2016} - \frac{1}{2017}\right)$$
$$= \frac{1}{2} - \frac{1}{2017} = \frac{2015}{4034}$$

□

§6.3   Power series

Theorem 6.3.1: Taylor Series

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n \tag{6.4}$$

Theorem 6.3.2: Maclaurin Series

This is a special case of Taylor Series, where $a = 0$.

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!}x^n \tag{6.5}$$

The power series below can be easily computed:

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots \tag{6.6}$$

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots \tag{6.7}$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots \tag{6.8}$$

$$\ln(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots \tag{6.9}$$

$$\frac{1}{1 - x} = 1 + x + x^2 + x^3 + \cdots \tag{6.10}$$

$$\frac{1}{(1 - x)^2} = 1 + 2x + 3x^2 + 4x^3 + \cdots \tag{6.11}$$

§6.4   Generating Functions

A generating function is just a different way of writing a sequence of numbers. Here we will be dealing mainly with sequences of numbers (a_n).

Definition 6.4.1

Let $(a_n)_{n \geq 0}$ be a sequence of numbers. The generating function associated with this sequence is the series

$$A(x) = \sum_{n \geq 0} a_n x^n.$$

7 Recurrence Relations

A **recurrence relation** for the sequence $\{a_n\}$ is an equation that expresses a_n in terms of one or more of the *previous terms* $a_0, a_1, \ldots, a_{n-1}$.

We will study more closely linear homogeneous recurrence relations of degree k with constant coefficients:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k},$$

where $c_1, c_2, \ldots, c_k$ are real numbers and $c_k \neq 0$.

Remark. linear = previous terms appear with exponent 1 (not squares, cubes, etc),

homogeneous = no term other than the multiples of a_i

degree k = expressed in terms of previous k terms

constant coefficients = coefficients in front of the terms are constants, instead of general functions.

Relevant examples:

- $a_{n+1} = a_n + k$
  Solution: $a_n = a_1 + (k-1)n$

- $a_{n+1} = a_n + n$
  Solution: $a_n = a_1 + 1 + 2 + \cdots + (n-1) = a_1 + \frac{n(n-1)}{2}$

- $a_{n+1} = a_n \cdot k$
  Solution: $a_n = a_1 k^{n-1}$

- $a_{n+1} = a_n \cdot n$
  Solution: $a_n = a_1 (n-1)!$

- Fibonacci sequence: $a_{n+1} = a_n + a_{n-1}$ (for $n \geq 2$), $a_1 = a_2 = 1$

- Cauchy equation: $f(x+y) = f(x) + f(y)$
  Solution: $f(x) = f(1)x$ for rational x

§7.1 First-order Recurrence Relations

The homogeneous case can be written in the following way:

$$x_n = rx^{n-1}, x_0 = A$$

Its general solution is

$$x_n = Ar^n$$

which is a geometric sequence with ratio r.

§7.2 Second-order Recurrence Relations

$$c_0 x_n + c_1 x_{n-1} + c_2 x_{n-2} = 0$$

We first look for solutions in the form of $x_n = cr^n$. Plugging in the equation, we get

$$c_0 cr^n + c_1 cr^{n-1} + c_2 cr^{n-2} = 0.$$

This simplifies to

$$c_0 r^2 + c_1 r + c_2 = 0$$

which is known as the *characteristic equation* of the recurrence. The roots r_1, r_2 of the above equation are known as the *characteristic roots*.

In the case of distinct real roots, the general solution is

$$x_n = c_1 r_1{}^n + c_2 r_2{}^n$$

where c_1 and c_2 are constants to be found.

> **Example 7.2.1: Fibonacci Equation**
>
> Let
> $$f(n+2) = f(n+1) + f(n)$$
> where $f(0) = 0, f(1) = 1$. Find a general formula for the sequence.

Solution. Consider the solution of the form

$$f(n) = \alpha^n$$

for some real number α. Then we have

$$\alpha^{n+2} = \alpha^{n+1} + \alpha^n$$

from which we conclude that $\alpha^2 - \alpha - 1$. Solving quadratically, we have

$$\alpha_1 = \frac{1 + \sqrt{5}}{2}, \alpha_2 = \frac{1 - \sqrt{5}}{2}.$$

Hence, a general solution of the sequence can be written as

$$f(n) = c_1 \left(\frac{1 + \sqrt{5}}{2} \right)^n + c_2 \left(\frac{1 - \sqrt{5}}{2} \right)^n$$

where c_1 and c_2 are coefficients to be determined using the initial values.

By the initial conditions, we have

$$c_1 + c_2 = 0$$
$$c_1 \left(\frac{1 + \sqrt{5}}{2} \right) + c_2 \left(\frac{1 - \sqrt{5}}{2} \right) = 1$$

Thus we have

$$c_1 = \frac{1}{\sqrt{5}}, \ c_2 = -\frac{1}{\sqrt{5}}.$$

Hence this gives us

$$\boxed{f(n) = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n}.$$

$\square$

8 Functional Equations

An equation containing an unknown function is called a **functional equation**. A typical functional equation problem will ask you to find all functions satisfying a certain property. For such problems, you must prove *both* directions.

Common problem-solving techniques:

- Guess the function.

- Substitute values such as 1, 0, −1, x, or −x.

- Spotting recurrence relations.

- Spotting cyclic functions.

- Cauchy's method.

> **Example 8.0.1**
>
> Let $a \neq 1$. Solve the equation
>
> $$af(x) + f\left(\frac{1}{x}\right) = ax$$
>
> where the domain of f is the set of all non-zero real numbers.

Solution. Replacing x by x^{-1}, we get

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

We therefore have

$$(a^2 - 1)f(x) = a^2 x - \frac{a}{x}$$

and hence

$$\boxed{f(x) = \frac{a^2 x - \frac{a}{x}}{a^2 - 1}.}$$

$\square$

> **Example 8.0.2: Cauchy's functional equation (rationals)**
>
> Find all functions $f : \mathbb{Q} \to \mathbb{Q}$ such that
>
> $$f(x + y) = f(x) + f(y)$$
>
> holds for each $x, y \in \mathbb{Q}$.

Solution. First put $y = 0$:

$$f(x + 0) = f(x) + f(0) \implies f(0) = 0$$

Then put $y = -x$:

$$f(x - x) = f(x) + f(-x) \implies f(-x) = -f(x) \quad \forall x \in \mathbb{Q}$$

Then, by repeated application of the original equation to expand the right side of $f(nx) = f(x + x + \cdots + x)$ we get

$$f(nx) = nf(x) \quad \forall x \in \mathbb{Q}, \forall n \in \mathbb{N}$$

By substituting $x = \frac{1}{n}$:

$$f\left(\frac{1}{n}\right) = \frac{1}{n}f(1) \quad \forall n \in \mathbb{N}$$

Combining the two equations above with $x = \frac{1}{m}$, we get:

$$f\left(\frac{n}{m}\right) = nf\left(\frac{1}{m}\right) = \frac{n}{m}f(1) \quad \forall m, n \in \mathbb{N}$$

Using $f(-x) = -f(x)$ and multiplying the equation above by -1, we get

$$-f\left(\frac{n}{m}\right) = -\frac{n}{m}f(1)$$
$$f\left(-\frac{n}{m}\right) = \left(-\frac{n}{m}\right)f(1) \quad \forall m, n \in \mathbb{N}$$
$$f(q) = qf(1) \quad \forall q \in \mathbb{Q}$$

Thus, we have found that $f(x) = cx \forall x \in \mathbb{Q}$ and some constant $c \in \mathbb{R}$. It is obvious that this family of functions is indeed a solution of $f(x + y) = f(x) + f(y)$ for rational x and y. More generally, it is easy to show that $\boxed{f(\alpha q) = qf(\alpha) \forall q \in \mathbb{Q}, \alpha \in \mathbb{R}}$. $\qquad\square$

Problems

Problem 8.0.1 (IMO 2019). Determine all functions $f : \mathbb{Z} \to \mathbb{Z}$ such that, for all integers a and b,
$$f(2a) + 2f(b) = f(f(a + b)).$$

Solution. First, we substitute $a = 0$ to get
$$f(0) + 2f(b) = f(f(b)).$$

It follows that
$$f(f(a + b)) = 2f(a + b) + f(0),$$

so we have
$$2f(a + b) + f(0) = f(2a) + 2f(b).$$

Substituting $a = 1$ (the motivation is that, since $f(x)$ takes the integers to the integers, it might be useful to relate $f(x + 1)$ with $f(x)$) yields
$$2f(b + 1) + f(0) = f(2) + 2f(b).$$

Rearranging this a little bit, we get
$$f(b + 1) - f(b) = \frac{f(2) - f(0)}{2}.$$

Clearly, $\frac{f(2) - f(0)}{2}$ is constant, so it follows that $f(x)$ is linear.

Now, we let $f(x) = gx + h$. Substituting this back, we find that either $g = h = 0$ or $g = 2$.

Hence, we have $\boxed{f(x) = 2x + h \text{ for some constant h}}$, or $\boxed{f \equiv 0}$. $\qquad\square$

Problem 8.0.2 (IMO 2015)**.** Determine all functions $f : \mathbb{R} \to \mathbb{R}$ that satisfy the equation

$$f(x + f(x + y)) + f(xy) = x + f(x + y) + yf(x)$$

for all real x and y.

Solution. Let $P(x, y)$ denote the assertion. Then, $P(0, y)$ gives $f(f(y)) + f(0) = f(y) + yf(0)$. Therefore, $y = 0$ gives $f(f(0)) = 0$ and $y = f(0)$ gives $2f(0) = f(0)^2$. This implies $f(0) = 0$ or $f(0) = 2$.

Case 1: $f(0) = 2$ Then, $f(2) = 0$ and $f(f(y)) = f(y) + 2y - 2$. This implies f is injective and $f(y) = y$ if and only if $y = 1$. Now, $P(x, 1)$ gives $f(x + f(x + 1)) = x + f(x + 1)$, so $f(x + 1) = 1 - x$. Therefore, $f(x) = 2 - x$. This works because both sides are equal to $y + 2 - xy$.

Case 2: $f(0) = 0$ Then, $f(f(y)) = f(y)$. Now, $P(f(k), k - f(k))$ gives

$$f(2f(k)) + f(f(k)(k - f(k))) = 2f(k) + (k - f(k))f(k)$$

and $P(f(k), 0)$ gives
$$f(2f(k)) = 2f(k).$$
This means that $f(f(k)(k - f(k))) = (k - f(k))f(k)$. Therefore, $P(k - f(k), f(k))$ gives

$$f(k) + f(f(k)(k - f(k))) = f(k) + (k - f(k))f(k) = k - f(k)f(k - f(k)),$$

so
$$(k - f(k))(f(k) - 1) = -f(k - f(k)).$$

Therefore, if $f(a) - a = f(b) - b \neq 0$, then $f(a) = f(b)$, so $a = b$. Since $P(1, -1)$ gives $f(1) + f(-1) = 1 - f(1)$ and $P(-1, 1)$ gives $f(-1) + f(-1) = -1 + f(-1)$, we get $f(-1) = -1$ and $f(1) = 1$. Now, $P(1, y)$ gives $f(1 + f(1 + y)) - (1 + f(1 + y)) + f(y) - y = 0$, so if $g(x) = f(x) - x$, then $g(y) = -g(1 + f(1 + y))$. If $g(y) \neq 0$, then $g(y) = -g(1 + f(1 + y)) = g(1 + f(1 + 1 + f(1 + y)))$, so $y - 1 = f(f(y + 1) + 2)$. Therefore, $f(y - 1) = y - 1$. If $f(y + 1) \neq y + 1$, then $f(y) = y$, contradiction. Therefore, $f(y + 1) = y + 1$, so $f(y + 3) = y - 1$, which implies $f(y + 2) = y + 2$. However, $P(1, y + 2)$ gives $f(y) - y + f(y + 2) - (y + 2) = 0$, contradiction since $f(y + 2) = y + 2$ but $f(y) \neq y$. Therefore, we must have $f(y) = y$ for all y, which works since both sides are equal to $2x + y + xy$.

Therefore, the only solutions are $\boxed{f(x) = x}$ and $\boxed{f(x) = 2 - x}$. $\square$

Problem 8.0.3 (CHINA 2016)**.** Find all functions $f : \mathbb{Z} \to \mathbb{Z}$, such that for $\forall m, n \in \mathbb{Z}$,

$$f(f(m + n)) = f(m) + f(n).$$

Solution. Let $a = f(0)$ and $c = f(1) - f(0)$ $f(m) + f(1) = f(f(m + 1)) = f(m + 1) + f(0)$ and so $f(m + 1) = f(m) + c$ and so $f(x) = cx + a$

Plugging this back into the original equation, we get $\boxed{\text{S1: } f(x) = 0 \quad \forall x \in \mathbb{Z}}$, which indeed fits

$\boxed{\text{S2: } f(x) = x + a \quad \forall x \in \mathbb{Z}}$, which indeed fits, whatever is $a \in \mathbb{Z}$ $\qquad \square$

Part III

Geometry

9 Synthetic Geometry

§9.1   Angles

The reader should be familiar with terms such as segment, endpoint, midpoint, ray, origin, line, collinear.

§9.1.1   Phantom Points

§9.2   Triangle

§9.2.1   Triangle Centers

Definitions

Let ABC be a triangle.

Triangle centers:

1. Centroid G: Intersection of medians.

2. Circumcenter O: Center of the circle which passes through vertices of the triangle.

3. Incenter I: Intersection of the internal angle bisectors, which is also the center of the unique circle inside the triangle tangent to all three sides.

4. Excenter J: Center of the circle which is tangent to sides of the triangle but lies outside the triangle.

5. Orthocenter H: Intersection of altitudes.

Associated inscribed triangles:

1. Intouch triangle: The triangle whose vertices are the contact points of the incircle with the sides of ABC.

2. **Medial triangle**: The triangle whose vertices are the midpoints of the sides of ABC.

3. **Orthic triangle**: The triangle whose vertices are the feet of the altitudes.

Properties

Centroid medians cut triangle into 6 parts of equal area G divides medians into segments of ratio 2:1

Circumcenter R = a/2sinA = b/2sinB = c/2sinC

Incenter r=area/s (s is semiperimeter)

Orthocenter cyclic quadrilaterals H,A,B,C are incenter/excenters of orthic triangle

Point where angle bisector of A meets perp bisector of BC lies on circumcircle of ABC. This point is also the center of circle passing through B, C, I, J_A

Properties of the orthocenter

§9.2.2   Right triangle

> **Theorem 9.2.1: Pythagoras' Theorem**
>
> For triangle $\triangle ABC$ where the right angle is at $\angle C$,
>
> $$a^2 + b^2 = c^2 \tag{9.1}$$

Using similar triangles, we can deduce

$$\frac{1}{h^2} = \frac{1}{a^2} + \frac{1}{b^2} \tag{9.2}$$

where h is the perpendicular distance from C to a.

§9.2.3   Congruency and Similarity

Triangle similarity

1. Two angles match.

2. Two sides have lengths in the same ratio, and the angle between those two sides matches.

3. Three sides have lengths in the same ratio.

4. The triangles are right-angled and the ratio between one side and hypotenuse is the same.

Triangle congruence Same conditions but check that one corresponding side matches.

§9.2.4 Viviani's Theorem

Theorem 9.2.2: Viviani's Theorem

The sum of the distances from any interior point to the sides of an equilateral triangle equals the length of the triangle's altitude.

Proof. □

Theorem 9.2.3

The sum of the distances from any point P inside a parallelogram is independent of the location of P.

The converse also holds: If the sum of the distances from a point in the interior of a quadrilateral to the sides is independent of the location of the point, then the quadrilateral is a parallelogram.

Theorem 9.2.4

Generalisation: In a 2k-sided polygon with opposite sides parallel, the sum of distances from an arbitrary point inside the polygon to its sides is constant and is independent of the point's position.


Regular polygons: Theorem 4. In every regular polygon, the sum of distances from an arbitrary point inside the polygon to its sides is constant and is independent of the point's position.

Theorem 5. The sum of distances from a point to the side lines of an equiangular polygon does not depend on the point and is that polygon's invariant.

Theorem 9.2.5: Carnot's Theorem

For a triangle ABC, P lies in the interior of the triangle. D, E, F denote the foots of perpendicular from P to sides BC, CA, AB respectively. The following equation holds:
$$AE^2 + BD^2 + CF^2 = AF^2 + BE^2 + CD^2 \tag{9.3}$$
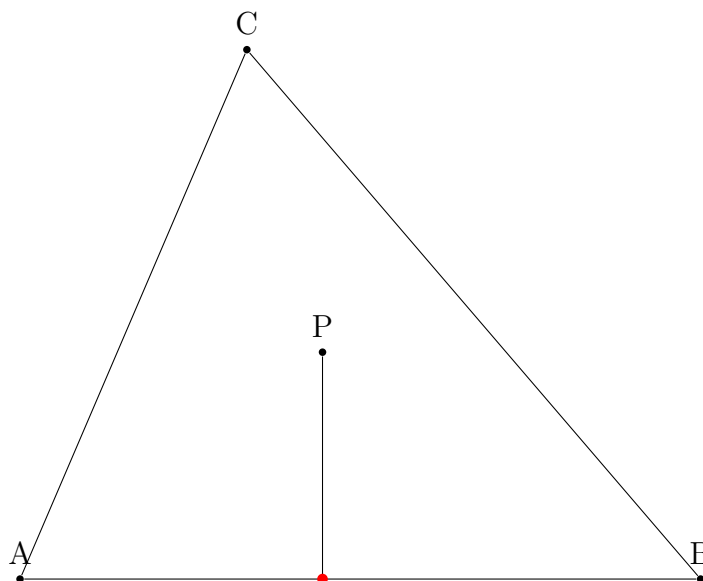
Proof. By Pythagoras' Theorem:

$$PC^2 - CF^2 = PF^2$$
$$PA^2 - AF^2 = PF^2$$

This gives us

$$PC^2 - PA^2 = CF^2 - AF^2 \tag{1}$$

Similarly, we have

$$PA^2 - PB^2 = AE^2 - BE^2 \tag{2}$$

$$PB^2 - PC^2 = BD^2 - CD^2 \tag{3}$$

Adding $(1) + (2) + (3)$ gives us our desired outcome. $\square$

Theorem 9.2.6: Pythagorean Inequality

A generalisation of the Pythagorean theorem, which states that in a right triangle with sides $a \leq b \leq c$ we have $a^2 + b^2 = c^2$. This inequality extends this to obtuse and acute triangles. The inequality states:
For an acute triangle with sides $a \leq b \leq c$,

$$a^2 + b^2 > c^2$$

For an obtuse triangle with sides $a \leq b \leq c$,

$$a^2 + b^2 < c^2$$

This inequality is a direct result of the Cosine Law.

§9.2.5   Area of triangle

Let $[ABC]$ denote the area of triangle $\triangle ABC$.

$$[ABC] = \frac{ah_a}{2} = \frac{1}{2}ab\sin C \tag{9.4}$$

$$[ABC] = \frac{abc}{4R} \tag{9.5}$$

This formula can derived from Sine Rule where $\sin C = \dfrac{c}{2R}$.

$$[ABC] = sr \tag{9.6}$$

where s denotes the semiperimeter, r denotes the radius of incircle.

Theorem 9.2.7: Heron's formula

$$[ABC] = \sqrt{s(s-a)(s-b)(s-c)} \tag{9.7}$$

where s denotes semiperimeter.
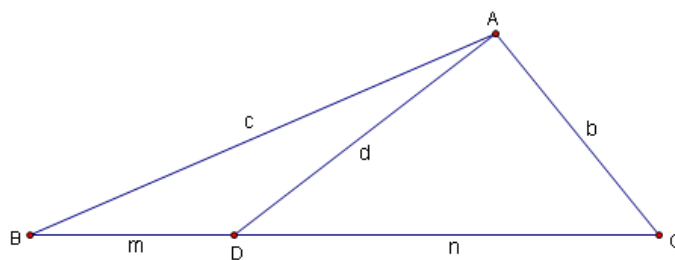

Theorem 9.2.8: Stewart's Theorem

Given a triangle $\triangle ABC$, if cevian AD is drawn so that $BD = m$, $CD = n$, $AD = d$, we have
$$b^2 m + c^2 n = amn + d^2 a.$$

Rewriting this,

$$man + dad = bmb + cnc. \tag{9.8}$$

This Theorem can be derived using Cosine Rule. You will usually use this Theorem to find the lengths of angle bisectors and medians.
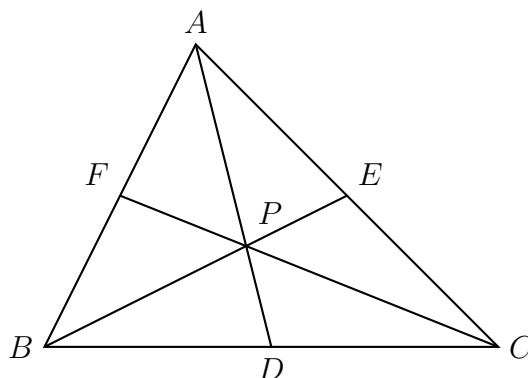
§9.2.6   Ceva and Menelaus

Theorem 9.2.9: Ceva's Theorem

Given a triangle ΔABC with a point P inside the triangle, continue lines AP, BP, CP to intersect BC, CA, AB at D, E, F respectively.
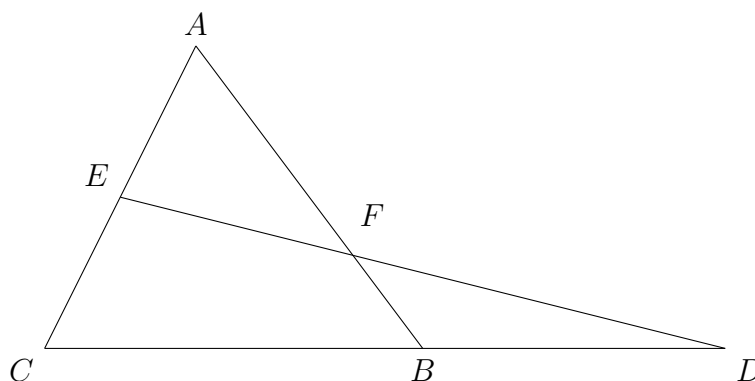
$$\frac{AF}{FB} \times \frac{BD}{DC} \times \frac{CE}{EA} = 1 \tag{9.9}$$

Theorem 9.2.10: Menelaus' Theorem

Given a triangle ΔABC, and a transversal that intersects BC, AC, AB at points D, E, F respectively.

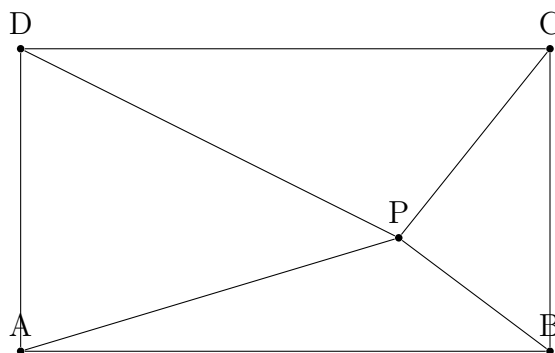$$\frac{AF}{FB} \times \frac{BD}{DC} \times \frac{CE}{EA} = 1 \tag{9.10}$$

§9.3   Quadrilaterals

> **Theorem 9.3.1: British Flag Theorem**
>
> If $ABCD$ is a rectangle and P is a point inside of it, then we have
>
> $$PA^2 + PC^2 = PB^2 + PD^2$$

Proof. This can be easily proven using Pythagoras' Theorem.   □

§9.4   Circle

The reader should be familiar with basic circle terminology, such as **center**, **radius**, **chord**, **diameter**, **tangent**, **secant**, **arc**, **sector**, **segment**, and **circumference**.

§9.4.1   Angles

Angle subtended at the centre of a circle by a chord is twice the angle subtended on the circumference.

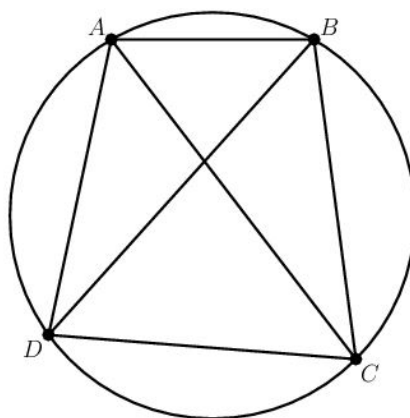All angles subtended by a fixed chord in the same segment of a circle are equal.

§9.4.2   Cyclic Quadrilaterals

Angle chasing and cyclic quadrilaterals

Theorem 9.4.1: Ptolemy's Theorem

Given a cyclic quadrilateral $ABCD$, the product of lengths of diagonals is equal to the sum of products of lengths of the pairs of the opposite sides:

$$AC \cdot BD = AB \cdot CD + AD \cdot BC \tag{9.11}$$

Theorem 9.4.2: Ptolemy's Inequality

For four points A, B, C, D in the plane,

$$AB \cdot CD + BC \cdot DA \geq AC \cdot BD \tag{9.12}$$

where equality holds if and only if $ABCD$ is a cyclic quadrilateral with diagonals AC and BD, or if A, B, C, D are collinear.

Proof. We construct a point P such that the triangles APB and DCB are similar and have the same orientation. This means that

$$BD = \frac{BA \cdot DC}{AP} \tag{1}$$

But since this is a spiral similarity, we also know that the triangles ABD and PBC are also similar, which implies that

$$BD = \frac{BC \cdot AD}{PC} \tag{2}$$

By the triangle inequality, we have $AP + PC \geq AC$. Multiplying both sides of the inequality by BD and using equations (1) and (2) gives us

$$BA \cdot DC + BC \cdot AD \geq AC \cdot BD$$

which is the desired inequality. Equality holds iff A, P, C are collinear. But since the triangles BAP and BDC are similar, this would imply that the angles BAC and BDC are congruent, i.e. that $ABCD$ is a cyclic quadrilateral. $\square$

Theorem 9.4.3: Brahmagupta's Formula

Given a cyclic quadrilateral $ABCD$,

$$[ABCD] = \sqrt{(s-a)(s-b)(s-c)(s-d)} \tag{9.13}$$
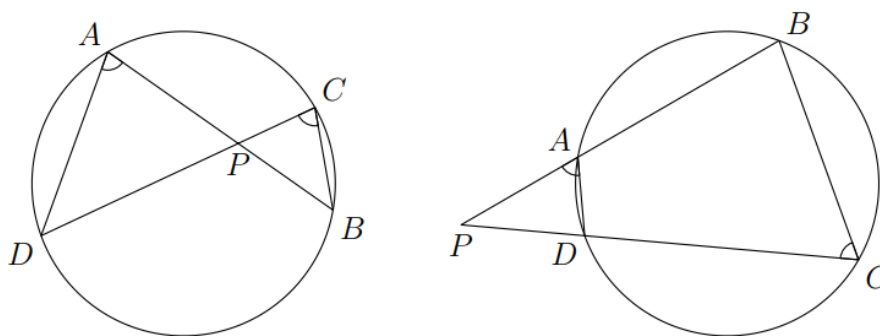
where s denotes the semiperimeter.

§9.4.3   Power of a Point

Power of a point is a frequently used tool in Olympiad geometry.

> **Theorem 9.4.4: Power of a point**
>
> Let Γ be a circle, and P be a point. Let a line through P meet Γ at points A and B, and another line through P meet Γ at points C and D. Then
>
> $$PA \cdot PB = PC \cdot PD \qquad\qquad (9.14)$$

Proof. There are two configurations to consider, depending on whether P lies inside the circle or outside the circle.

When P lies inside the circle, we have $\angle PAD = \angle PCB$ and $\angle APD = \angle CPB$, so triangles PAD and PCB are similar. Hence $\dfrac{PA}{PD} = \dfrac{PC}{PB}$. Rearranging, we get $PA \cdot PB = PC \cdot PD$.

When P lies outside the circle, we have $\angle PAD = \angle PCB$ and $\angle APD = \angle CPB$, so again triangles PAD and PCB are similar. We get the same result in this case. $\square$

As a special case, when P lies outside the circle and $C = D(PC$ is a tangent), we have

$$PA \cdot PB = PC^2 \qquad\qquad (9.15)$$
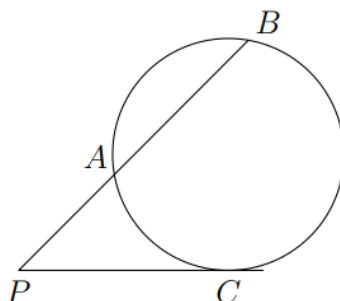
> ### Theorem 9.4.5: Converse to Power of a Point
>
> Let A, B, C, D be four distinct points. Let lines AB and CD intersect at P. Assume that either (1) P lies on both line segments AB and CD, or (2) P lies on neither line segments. Then A, B, C, D are concyclic if and only if $PA \cdot PB = PC \cdot PD$.

Proof. The expression $PA \cdot PB = PC \cdot PD$ can be rearranged as $\dfrac{PA}{PD} = \dfrac{PC}{PB}$. In both configurations described in the statement of the theorem, we have $\angle APD = \angle CPB$. It follows by angles and ratios that triangles APD and CPB are similar.

Thus $\angle PAD = \angle PCB$. In both cases this implies that A, B, C, D are concyclic. $\qquad \square$

Suppose that Γ has center O and radius r. We say that the **power** of point P with respect to Γ is

$$PO^2 - r^2$$

Let line PO meet Γ at points A and B, so that AB is a diameter. We will use *directed lengths*, meaning that for collinear points P, A, B, an expression such as $PA \cdot PB$ is assigned a positive value if PA and PB point in the same direction, and a negative value if they point in opposite directions. Then

$$PA \cdot PB = (PO + OA)(PO + OB) = (PO - r)(PO + r) = PO^2 - r^2,$$

which is the power of P. So the power of a point theorem says that this quantity equals to $PC \cdot PD$, where C and D are the intersections with Γ of any line through P.

By convention, the power of P is negative when P is inside the circle, and positive when P is outside the circle. When P is outside the circle, the power equals to the square of the length of the tangent from P to the circle.
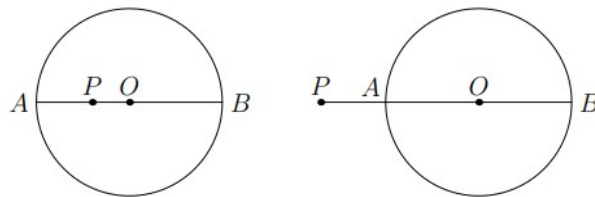
Let Γ_1 and Γ_2 be two circles with different centers O_1 and O_2, and radii r_1 and r_2 respectively.

The radical axis of Γ_1 and Γ_2 is the set of points with equal powers with respect to both circles.

$$PO_1{}^2 - r_1{}^2 = PO_2{}^2 - r_2{}^2$$

which can be represented as

$$pow(P, \Gamma_1) = pow(P, \Gamma_2).$$

The radical axis is a line perpendicular to the line connecting the circles' centers (line ℓ).

Proof.

Lemma 9.4.1. Let P be a point in the plane, and let P' be the foot of the perpendicular from P to O_1O_2. Then

$$pow(P, \Gamma_1) - pow(P, \Gamma_2) = pow(P', \Gamma_1) - pow(P', \Gamma_2).$$

The proof of the lemma is an easy application of the Pythagorean Theorem.

Lemma 9.4.2. There is a unique point P on line O_1O_2 such that $pow(P, O_1) = pow(P, O_2)$.

Proof: First show that P lies between O_1 and O_2 via proof by contradiction, by using a bit of inequality theory and the fact that $O_1O_2 > r_1 + r_2$. Then, use the fact that $O_1P + PO_2 = O_1O_2$ (a constant) to prove the lemma.

The first lemma shows that every point on the plane can be equivalently mapped to a line on O_1O_2. The second lemma shows that only one point in this mapping satisfies the given condition. Combining these two lemmas shows that the radical axis is a line perpendicular to ℓ, hence proved. $\qquad\square$

When Γ_1 and Γ_2 intersect, the intersection points A and B both have a power of 0 with respect to either circle, so A and B must lie on the radical axis. This shows that the radical axis *coincides with the common chord* when the circles intersect.

To show that some point lies on the radical axis or the common chord, we can show that the point has *equal powers with respect to the two circles*.
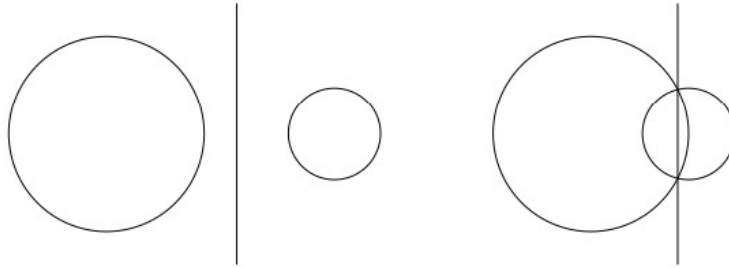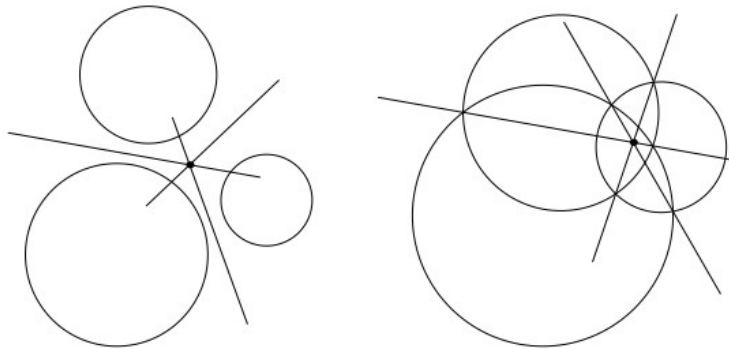

Figure 9.1: Radical axis

Figure 9.2: Radical center

> **Theorem 9.4.6: Radical Axis Theorem**
>
> Given three circles, no two concentric, the three pairwise radical axes (which are non-parallel) are concurrent, at a point known as the radical center.

Proof. Denote the three circles by $\Gamma_1, \Gamma_2, \Gamma_3$, and denote the radical axes of Γ_i and Γ_j by ℓ_{ij}.

Suppose that the radical axes are not all parallel. Let ℓ_{12} and ℓ_{13} meet at X. Since X lies on ℓ_{12}, it has equal powers with respect to Γ_1 and Γ_2. Since X lies on ℓ_{13}, it has equal powers with respect to Γ_1 and Γ_3. Therefore, X has equal powers with respect to all three circles, and hence it must lie on ℓ_{23} as well. $\qquad\square$

§9.4.4   Euler's Line and Nine-point Circle

> **Theorem 9.4.7: Hamilton's theorem**
>
> For $\triangle ABC$ with circumcenter O and orthocenter H,
> $$\overrightarrow{OH} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}$$

> **Theorem 9.4.8: Euler line**
>
> The circumcenter O, the centroid G and the orthocenter H are collinear.
> In fact, we have
> $$GH = 2OG$$
> and
> $$OI^2 = R^2 - 2Rr$$

> **Theorem 9.4.9: Nine-point circle**
>
> The midpoints of each side of the triangle, the feet of each altitude, and the midpoints of the line segments from each vertex to the orthocenter, all lie on a single circle.

The center of this circle lies on the Euler line, at the midpoint between the orthocenter and circumcenter.

The radius of this circle is half the circumradius of the triangle.

§9.4.5 Simson line

§9.4.6 Miquel's theorem

> **Theorem 9.4.10: Miquel's theorem**
>
> Let ABC be a triangle, and let X, Y, Z be points on lines BC, CA, AB respectively. Assume that the six points A, B, C, X, Y, Z are all distinct. Then the circumcircles of triangles AYZ, BZX, CXY pass through a common point.

Proof. The proof involves angle chasing. □

Problems

Problem 9.4.1 (Oxford MAT 2022). 100 circles all share the same centre, the n-th circle named as C_n. For each whole number n between 1 and 99 inclusive, a tangent to circle C_n intersects circle C_{n+1} at two points, separated by a distance of 2.

Given that C_1 has radius 1, what is the radius of C_{100}?

Solution. The relationship between circle C_n of radius r_n and circle C_{n+1} of radius r_{n+1} is shown below.
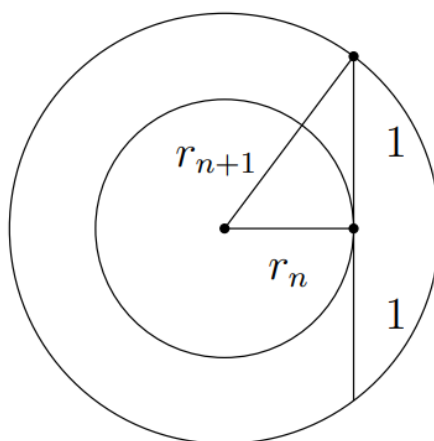
The tangent is at right angles to the radius, so there is a right-angled triangle with hypotenuse $r_n + 1$ and other sides r_n and 1. Pythagoras gives $r_{n+1}^2 = r_n^2 + 1$. Since $r_1^2 = 1$, we have $r_2^2 = 2$ and $r_3^2 = 3$ and so on, up to $r_{100}^2 = 100$, so the radius of C_100 is 10. $\square$

Problem 9.4.2. Prove that for angles $\alpha_1, \alpha_2, \ldots, \alpha_n$ which satisfy the condition $0° \leq a_i \leq 180°$ for $i = 1, 2, \ldots, n$ then

$$\sin\alpha_1 + \sin\alpha_2 + \cdots + \sin\alpha_n \leq n\sin\frac{\alpha_1 + \cdots + \alpha_n}{n}$$

with equality iff $\alpha_1 = \cdots = \alpha_n$.

Proof. For 2 angles,

$\square$

10 Trigonometry

Readings:

-

-

§10.1   Basic Definitions

Trigonometric functions describe how the ratio of lengths vary according to the angle between the lengths.

For a triangle $\triangle ABC$ with $\angle C = 90°$, we define **sine** as

$$\sin A = \frac{a}{c} \tag{10.1}$$

and **cosine** as

$$\cos A = \frac{b}{c}. \tag{10.2}$$

We define **tangent** as the ratio of sine and cosine; that is,

$$\tan A = \frac{\sin A}{\cos A} = \frac{a}{b}. \tag{10.3}$$

We also define the reciprocals of the above trigonometric functions: **cosecant**, **secant** and **cotangent** are the reciprocals of sine, cosine and tangent respectively.

$$\operatorname{cosec} A = \frac{1}{\sin A} \tag{10.4}$$

$$\sec A = \frac{1}{\cos A} \tag{10.5}$$

$$\cot A = \frac{1}{\tan A} \tag{10.6}$$

§10.2   Formulae

§10.2.1   Pythagorean identities

The following equation is known as the **Pythagorean identity**.

$$\sin^2 A + \cos^2 A = 1 \tag{10.7}$$

Proof.

$$\sin^2 A + \cos^2 A = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = \frac{a^2 + b^2}{c^2}$$

By Pythagoras' Theorem, for a right-angled triangle, $a^2 + b^2 = c^2$. Hence we have our desired result. $\square$

The following two equations are corollaries of eq. (10.7); they can be easily derived and shall be left as an exercise for the reader.

$$\tan^2 A + 1 = \sec^2 A$$

$$1 + \cot^2 A = \operatorname{cosec}^2 A$$

Example 10.2.1

Compute $\sin^2 5° + \sin^2 10° + \cdots + \sin^2 90°$.

Solution.

$$\begin{aligned}
&\sin^2 5° + \sin^2 10° + \cdots + \sin^2 90° \\
&= \left(\sin^2 5° + \sin^2 85°\right) + \cdots + \left(\sin^2 40° + \sin^2 50°\right) + \sin^2 45° + \sin^2 90° \\
&= \left(\sin^2 5° + \cos^2 5°\right) + \cdots + \left(\sin^2 40° + \cos^2 40°\right) + \frac{1}{2} + 1 \\
&= 8(1) + \frac{1}{2} + 1 \\
&= \boxed{9\frac{1}{2}}
\end{aligned}$$

$\square$

§10.2.2   Addition formulae

$$\sin(A \pm B) = \sin A \cos B \pm \cos A \sin B$$

$$\cos(A \pm B) = \cos A \cos B \mp \sin A \sin B$$

$$\tan(A \pm B) = \frac{\tan A \pm \tan B}{1 \mp \tan A \tan B}$$

Double-angle formulae

$$\sin 2A = 2 \sin A \cos A$$
$$\cos 2A = \cos^2 A - \sin^2 A$$
$$= 2 \cos^2 A - 2$$
$$= 2 - 2 \sin^2 A$$
$$\tan 2A = \frac{2 \tan A}{1 - \tan^2 A}$$

Triple-angle formulae

$$\sin 3A = 3 \sin A - 4 \sin^3 A$$
$$\cos 3A = 4 \cos^3 A - 3 \cos A$$
$$\tan 3A = \frac{3 \tan A - \tan^3 A}{1 - 3 \tan^2 A}$$

Half-angle formulae

The following formulae are corollaries of eq. (10.7).

$$\sin \frac{A}{2} = \pm \sqrt{\frac{1 - \cos A}{2}}$$

$$\cos \frac{A}{2} = \pm \sqrt{\frac{1 + \cos A}{2}}$$

Multiple-angle formulae

Multiple-angle formulas are given by

$$\sin nA = \sum_{k=0}^{n} \binom{n}{k} \cos^k A \sin^{n-k} A \sin \frac{n-k}{2} \pi$$

$$\cos nA = \sum_{k=0}^{n} \binom{n}{k} \cos^k A \sin^{n-k} A \cos \frac{n-k}{2} \pi$$

Sum to product

$$\sin A + \sin B = 2 \sin \frac{A+B}{2} \cos \frac{A-B}{2}$$
$$\sin A - \sin B = 2 \cos \frac{A+B}{2} \sin \frac{A-B}{2}$$
$$\cos A + \cos B = 2 \cos \frac{A+B}{2} \cos \frac{A-B}{2}$$
$$\cos A - \cos B = -2 \sin \frac{A+B}{2} \sin \frac{A-B}{2}$$

Product to sum

$$\sin A \cos B = \frac{1}{2}\left[\sin(A+B) + \sin(A-B)\right]$$

$$\cos A \cos B = \frac{1}{2}\left[\cos(A+B) + \cos(A-B)\right]$$

$$\sin A \sin B = -\frac{1}{2}\left[\cos(A+B) - \cos(A-B)\right]$$

§10.2.3   R-formula

$$a\sin\theta \pm b\cos\theta = \sin(\theta \pm \alpha)$$

$$a\cos\theta \mp b\cos\theta = \cos(\theta \pm \alpha)$$

where $R = \sqrt{a^2+b^2}$, $\alpha = \tan^{-1}\dfrac{b}{a}$ where $0 < \alpha < \frac{\pi}{4}$.

§10.3   Theorems

Theorem 10.3.1: Sine rule

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R \tag{10.8}$$

where R denotes radius of circumcircle of triangle ABC.

Theorem 10.3.2: Cosine rule

$$a^2 = b^2 + c^2 - 2bc\cos A \tag{10.9}$$

Theorem 10.3.3: Tangent law

$$\frac{a-b}{a+b} = \frac{\tan\frac{A-B}{2}}{\tan\frac{A+B}{2}} \tag{10.10}$$

Theorem 10.3.4: Cotangent law

$$\cot A = \frac{b^2 + c^2 - a^2}{4S} \tag{10.11}$$

§10.4   Hyperbolic Functions

The hyperbolic trigonometric functions extend the notion of the parametric equations for a unit circle ($x = \cos t$ and $y = \sin t$) to the parametric equations for a hyperbola, which yield the following two fundamental **hyperbolic equations**:

$$x = \cosh t = \frac{e^t + e^{-t}}{2} \quad \text{and} \quad y = \sinh t = \frac{e^t - e^{-t}}{2} \tag{10.12}$$

$$\sinh x + \cosh x = e^x \tag{10.13}$$

> **Theorem 10.4.1: Osborn's rule**
>
> Osborn's rule is a rule for converting a trigonometric identity into a corresponding hyperbolic one. The rule states that one replaces every occurrence of sine or cosine with the corresponding hyperbolic sine or cosine, and wherever one has a product of two sines, the product of the hyperbolic sines must be negated.

$$\cosh 2x = 1 + 2\sinh^2 x \tag{10.14}$$

$$\sinh 2A = 2\sinh A \cosh A \tag{10.15}$$

Problems

Problem 10.4.1. Angles of $\triangle ABC$ satisfies

$$\frac{\sin A + \sin B + \sin C}{\cos A + \cos B + \cos C} = \frac{12}{7}$$

and

$$\sin A \sin B \sin C = \frac{12}{15}.$$

Given that $\sin C$ takes on three possible values s_1, s_2, s_3, find the value of $s_1 s_2 s_3$.

Solution.

$$\sin A + \sin B + \sin C = 2 \sin \frac{A+B}{2} \cos \frac{A-B}{2} + \sin C$$

$$=$$

□

Problem 10.4.2. Let

$$A = \cos^2 10° + \cos^2 50° - \sin 40° \sin 80°.$$

Determine the value of A.

Solution. Let $B = \sin^2 10° + \sin^2 50° - \cos 40° \cos 80°$.

Then

$$A + B = 2 - \cos 40°$$
$$A - B = \left(\cos^2 10° - \sin 10°\right) + \left(\cos^2 50° - \sin^2 50°\right) + \left(\cos 40° \cos 80° - \sin 40° \sin 80°\right)$$
$$= \cos 20° + \cos 100° + \cos(40° + 80°)$$
$$= \cos 20° + \cos 100° + \cos 120°$$
$$= 2\cos 60° \cos 40° - \cos 60°$$
$$= \cos 40° - \frac{1}{2}$$

Adding up the two equations gives us $2A = \dfrac{3}{2}$. Hence $\boxed{A = \dfrac{3}{4}}$. $\qquad\square$

Problem 10.4.3 (SMO Open)**.** Find the value of

$$\frac{\tan 40° \tan 60° \tan 80°}{\tan 40° + \tan 60° + \tan 80°}.$$

Solution. We can show more generally, for acute $\triangle ABC$,

$$\frac{\tan A \tan B \tan C}{\tan A + \tan B + \tan C} = 1.$$

We see that

$$
\begin{aligned}
\tan A + \tan B + \tan &= \tan A + \tan B + \tan[180° - (A + B)] \\
&= \tan A + \tan B - \tan(A + B) \\
&= \tan A + \tan B - \frac{\tan A + \tan B}{1 - \tan A \tan B} \\
&= (\tan A + \tan B)\left(1 - \frac{1}{1 - \tan A \tan B}\right) \\
&= (\tan A + \tan B)\left(-\frac{\tan A \tan B}{1 - \tan A \tan B}\right) \\
&= \tan A \tan B\left(-\frac{\tan A + \tan B}{1 - \tan A \tan B}\right) \\
&= \tan A \tan B[-\tan(A + B)] \\
&= \tan A \tan B \tan[180° - (A + B)] \\
&= \tan A \tan B \tan C
\end{aligned}
$$

Hence proven. □

Problem 10.4.4 (Oxford MAT)**.** Evaluate

$$\sin^2 1° + \sin^2 2° + \cdots + \sin^2 89° + \sin^2 90°.$$

Solution. Recall the Pythagorean Identity $\sin^2 x + \cos^2 x = 1$.

Rewriting and pairing up terms gives us

$$\sin^2 1° + \sin^2 2° + \cdots + \cos^2 2° + \cos^2 1° + 1$$
$$= \left(\sin^2 1° + \cos^2 1°\right) + \cdots + \left(\sin^2 44° + \cos^2 44°\right) + \sin^2 45° + 1$$
$$= 44(1) + \frac{1}{2} + 1 = \boxed{45\frac{1}{2}}$$

□

11 Coordinate Systems

§11.1   Cartesian Coordinates

§11.1.1   Basics

The coordinate plane is determined by two **axes** – a horizontal x-axis and a vertical y-axis; both axes intersect at a point called the **origin**. Each point in the coordinate plane can be specified by an ordered pair of numbers (x, y).

The **gradient** of a line with points (x_1, y_1) and (x_2, y_2) is given by

$$m = \frac{y_2 - y_1}{x_2 - x_1} \tag{11.1}$$

Given gradient m and y-intercept c, a line can be represented in the point-slope form:

$$y = mx + c \tag{11.2}$$

Given gradient m and a point on the line (x_1, y_1), a line can be represented as

$$y - y_1 = m(x - x_1) \tag{11.3}$$

For two **parallel** lines, they have the same gradients.

For two **perpendicular** lines, the product of the gradients is −1.

The distance from a point (m, n) to the line $Ax + By + C = 0$ is given by

$$d = \frac{Am + Bn + C}{\sqrt{A^2 + B^2}}$$

The distance between two lines is given by

The area of polygon is given by

reflection of point, line about line

§11.1.2   Conic Sections

Definitions and basic properties of conic sections - refer to F maths

§11.2   Barycentric Coordinates

§11.2.1   Basics

The Coordinates

> **Definition 11.2.1**
>
> Each point in the plane is assigned an ordered triple of real numbers $P = (x, y, z)$ such that
> $$\vec{P} = x\vec{A} + y\vec{B} + z\vec{C} \quad \text{and} \quad x + y + z = 1$$

Lines

§11.3   Complex Numbers

12 Advanced Techniques

§12.1 Inversion in the plane

Definition and first properties Generalised lines and circles Inversion distance formula O Inversive geometry

§12.2 Projective geometry

Cross ratios Projective transformations O Projective geometry, e.g. cross ratios, harmonic bundles, poles and polars, Pascal's theorem, and so on

§12.2.1 Homothety

§12.3 Complete quadrilaterals

Spiral similarity Miquel point of a cyclic quadrilateral

Part IV

Combinatorics

13 **Combinatorics**

" Recursion and recurrence relations " Definition of sets and functions O Elementary probability O Expected value and linearity of expectation O Basic properties and definitions from graph theory, e.g. connectedness and degree of a vertex O Definition and existence of the convex hull of a finite set of points !! Nontrivial results from graph theory, such as Hall's marriage lemma or Turan's theorem

§13.1   Permutations and Combinations

A **permutation** is an arrangement of objects in a specific order. Number of ways to permute k of n items:

$$^{n}\mathrm{P}_k = \frac{n!}{(n-k)!}$$

A **combination** is a selection of objects without regard to the order. Number of ways to choose k ok n items:

$$^{n}\mathrm{C}_k = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Number of subsets of a set with n elements is 2^n.

Number of ways to choose k objects from n objects if repetition is allowed $= \binom{n+k-1}{k}$.

Number of paths from $(0,0)$ to (m,n) going 1 unit rightwards or upwards $= \binom{m+n}{n}$.

Number of k-tuples of positive integers which sum equals n is $\binom{n-1}{k-1}$.

Number of k-tuples of non-negative integers which sum equals n is $\binom{n+k-1}{k-1}$.

§13.1.1   Stars and Bars

The setup is the following: suppose there are three children c_1, c_2, c_3, and we distribute 10 identical candies among these three children. Each child can receive any number of candies, including 0. For example, one possible distribution is $(4,3,3)$: in this case, c_1 receives 4 candies, c_2 receives 3, and c_3 receives 3. How many ways can we distribute the candies?

The key observation is the following: we can distribute the candies by arranging them in a line, and then placing two "bars" somewhere along the line. For example, the $(4,3,3)$ described above can be modeled by the following:

$$* * * * \mid * * * \mid * * *$$

Each $*$ represents a candy, and the two location of the two bars determines the distribution of the candies. Notice that the following distribution is also possible:

$$\parallel * * * * * * * * * *$$

The above diagram corresponds to the distribution $(0,0,10)$. In general, c_1 receives the candies left of the first bar, c_2 receives the candies between the two bars, and c_3 receives the candies right of the second bar.

So we can see that distributing candies is identical to choosing the location of the two bars to place in $10 + 2 = 12$ empty slots, hence $\binom{12}{2}$ ways.

In general, if there are n candies and k children, then there are $n + k - 1$ slots, and we must place $k - 1$ bars. The remaining n candies, interspersed among the bars, represent a istribution. Thus, the number of distributions is

$$\binom{n + k - 1}{k - 1}.$$

§13.2   Combinatorial Identities

§13.2.1   Pascal's Triangle

We can observe that by means of expansion,

$$\binom{n}{k} = \binom{n}{n-k} \tag{13.1}$$

Each number in the Pascal's triangle is a binomial coefficient. Pascal's and hockey-stick identities:

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \tag{13.2}$$

$$\sum_{r=k}^{n} \binom{r}{k} = \binom{n+1}{k+1} \tag{13.3}$$

$$\sum_{r=0}^{n} \binom{k+r}{r} = \binom{n+k+1}{n} \tag{13.4}$$

We also have

$$\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m} \tag{13.5}$$

which can be easily proven via expansion.

> **Theorem 13.2.1: Vandermonde's Identity**
>
> $$\sum_{r=0}^{k} \binom{m}{r}\binom{n}{k-r} = \binom{m+n}{k} \tag{13.6}$$

§13.2.2   Binomial Theorem

> **Theorem 13.2.2: Binomial Theorem**
>
> For $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{R}$,
>
> $$\begin{aligned} (a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \\ &= \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n} b^n \end{aligned} \tag{13.7}$$

Proof. This can be proven using mathematical induction. □

Corollary 1. For all $n \in \mathbb{Z}^+$, the following equality holds:

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} \tag{13.8}$$

Remark. The above identity simply follows by $a = b = 1$.

We give an alternate proof below that relates this identity to the set of subsets of a set.

Proof. Let A be a set with n elements, and let A_k denote the subset of the power set 2_A containing the subsets of A of size k. Then the sets $A_0, A_1, \ldots, A_n$ partition 2^A, which means the following equalities hold:

$$2^n = |2^A| = |A_0| + |A_1| + \cdots + |A_n|$$
$$= \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k}$$

In other words, every subset of A has a size in $\{0, 1, \ldots, n\}$, so to count the number of subsets of A, we can count the number of subsets of each size over all possible sizes. $\square$

Sums:

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1} \qquad (13.9)$$

$$\sum_{k=0}^{n} k^2\binom{n}{k} = n(n+1)2^{n-2} \qquad (13.10)$$

§13.3 Cardinality Rules and Principles

In this section, we will see the formalization of counting strategies that we often take for granted: the product rule, the sum rule, and the pigeonhole principle.

§13.3.1 Product Rule

Examples of counting

Counting number of rectangles:

For a $m \times n$ grid, to form a rectangle, choose 2 points from the $m + 1$ points along the column, and choose 2 points from the $n + 1$ points along the row. Hence the number of rectangles we can form is

$$\binom{m+1}{2}\binom{n+1}{2}$$

Circle division: chords divide a circle number of chords = n choose 2 where there are n points number of intersection points = n choose 4 (any 4 points forms 2 chords, thus gives a unique intersection point)

§13.3.2 Principle of Inclusion-Exclusion

The **principle of inclusion and exclusion** is a counting technique that computes the number of elements that satisfy at least one of several properties while guaranteeing that elements satisfying more than one property are not counted twice.

The idea behind this principle is that summing the number of elements that satisfy at least one of two categories and subtracting the overlap prevents double counting.

For two sets,

$$|A \cup B| = |A| + |B| - |A \cap B|$$

where $|S|$ denotes the cardinality (i.e. number of elements) of set S.

For three sets,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$$

More generally, if A_i are finite sets, then

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i \le j \le n} |A_i \cap A_j| + \sum_{1 \le i \le j \le k \le n} |A_i \cap A_j \cap A_k| \tag{13.11}$$
$$- \cdots + (-1)^{n-1}|A_1 \cap \cdots \cap A_n|.$$

> **Example 13.3.1**
>
> Find the number of integers from the set $\{1, 2, \ldots, 1000\}$ which are divisible by 3 or 5.

Solution. Let

$$S = \{1, 2, \ldots, 1000\}$$
$$A = \{x \in S \mid x \text{ is divisible by 3}\}$$
$$B = \{x \in S \mid x \text{ is divisible by 5}\}$$

It follows that

$$A \cap B = \{x \in S \mid x \text{ is divisible by 15}\}$$

Observe that

for any two natural numbers n and k with $n \geq k$, the number of integers in the set $\{1, 2, \ldots, n\}$ which are divisible by k is $\left\lfloor \dfrac{n}{k} \right\rfloor$

Hence we have

$$\begin{aligned}
|A \cup B| &= |A| + |B| - |A \cap B| \\
&= \left\lfloor \frac{1000}{3} \right\rfloor + \left\lfloor \frac{1000}{5} \right\rfloor - \left\lfloor \frac{1000}{15} \right\rfloor \\
&= 333 + 200 - 66 = \boxed{467}
\end{aligned}$$

$\square$

§13.3.3 Pigeonhole Principle

> **Theorem 13.3.1: Pigeonhole Principle**
>
> If $k + 1$ objects are placed into k boxes, then at least one box contains two or more objects.

Proof. We use a proof by contraposition.

Suppose none of the k boxes has more than one object. Then the total number of objects would be at most k. This contradicts the statement that we have $k + 1$ objects. $\square$

> **Theorem 13.3.2: Generalised Pigeonhole Principle**
>
> If n objects are placed into k boxes, then there is at least one box containing at least $\left\lceil \frac{n}{k} \right\rceil$ objects.

Proof. We use a proof by contradiction.

Suppose that none of the boxes contains more than $\left\lceil \dfrac{n}{k} \right\rceil - 1$ objects.

Then the total number of objects is

$$k \left(\left\lceil \frac{n}{k} \right\rceil - 1 \right)$$

but

$$k\left(\left\lceil\frac{n}{k}\right\rceil - 1\right) < k\left[\left(\frac{n}{k} + 1\right) - 1\right] = n$$

where the inequality $\left\lceil\dfrac{n}{k}\right\rceil < \dfrac{n}{k} + 1$ was used.

This is a contradiction, because there are a total of n objects.   □

§13.4   Catalan Numbers

> **Theorem 13.4.1: Catalan numbers**
>
> The Catalan numbers are given by the formula
>
> $$C_n = \frac{1}{n+1}\binom{2n}{n} \tag{13.12}$$

§13.4.1   Dyck Paths and Acceptable Sequences

The number of valid parenthesis expressions that consist of n right parentheses and n left parentheses is equal to the n-th Catalan number.

For example, $C_3 = 5$ and there are 5 ways to create valid expressions with 3 sets of parenthesis:

- ( ) ( ) ( )
- (( )) ( )
- ( ) (( ))
- ((( )))
- (( ) ( ))

Considering right parenthesis to be +1s, and left −1s, we can write this more formally as follows:

The number of sequences $a_1, \ldots, a_n$ of $2n$ terms that can be formed using n copies of +1s and n copies of −1s whose partial sums satisfy

§13.4.2   Recurrence Relation; Generating Function

§13.5   Derangements

A derangement is a permutation with no fixed points. That is, a derangement of a set leaves no element in its original place. For example, the derangements of $\{1, 2, 3\}$ are $\{2, 3, 1\}$ and $\{3, 1, 2\}$, but $\{3, 2, 1\}$ is not a derangement of $\{1, 2, 3\}$ because 2 is a fixed point.

The number of derangements of an n-element set is denoted D_n. This number satisfies the recurrences

$$D_n = n \cdot D_{n-1} + (-1)^n$$

and

$$D_n = (n-1) \cdot (D_{n-1} + D_{n-2})$$

and is given by the formula

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

§13.6 Probability

Problems

Problem 13.6.1 (Langford's Problem $L(n)$)**.** Given the multiset[1] of positive integers:

$$\{1, 1, 2, 2, 3, 3, \ldots, n, n\},$$

can they be arranged in a sequence such that for $1 \le i \le n$ there are i numbers between the two occurrences of i?

Proof. □

---

[1]A multiset is like a set except that there may be more than one occurrence of an element.

Problem 13.6.2. Use a combinatorial proof to show that

$$\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}.$$

Proof. For combinatorial proofs, we begin with a story. Consider a group of $2n$ animals, where n are dogs and n are cats.

RHS: Number of ways to pick n animals from a group of $2n$ animals.

For LHS, we try to understand what's going on in the summation:

$$\sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} = \binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots$$

We see that each term looks like a case. For example, for the first term, pick 0 items from the first group, and pick n items from the second group. This shows that if we want to pick n animals, we can pick k dogs and $n-k$ cats.

LHS: Consider all cases where we pick k dogs and $n-k$ cats.

$\therefore$ LHS is the same as RHS as they both count the same number of things.   Hence proven. $\qquad\square$

Problem 13.6.3. Evaluate

$$S = \binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n}.$$

Solution. Writing the sum backwards yields

$$S = n\binom{n}{n} + (n-1)\binom{n}{n-1} + \cdots + \binom{n}{1}$$
$$= n\binom{n}{0} + (n-1)\binom{n}{1} + \cdots + \binom{n}{n-1}$$

Add this to the original series gives us

$$2S = n\left[\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}\right]$$
$$2S = n2^n$$
$$\boxed{S = n2^{n-1}}$$

$\square$

This is the proof of the sum

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$$

Problem 13.6.4 (USAMO 2005)**.** Legs L_1, L_2, L_3, L_4 of a square table each have length n, where n is a positive integer. For how many ordered 4-tuples (k_1, k_2, k_3, k_4) of non-negative integers can we cut a piece of length k_i from the end of leg L_i $(i = 1, 2, 3, 4)$ and still have a stable table?

(The table is stable if it can be placed so that all four of the leg ends touch the floor. Note that a cut leg of length 0 is permitted.)

Solution. The table is stable if $k_1 + k_3 = k_2 + k_4$. Let this common value be k such that that $k_1 + k_3 = k_2 + k_4 = k$. Let c_k be the number of ways to make the table stable for each value of k. We want to find $\sum_{k=0}^{2n} c_k$.

Note that each table leg is at least 0 and at most n, hence we'll break this into two sums so that it's easier to handle:

$$\sum_{k=0}^{n} c_k + \sum_{k=n+1}^{2n} c_k$$

Case 1: If $0 \leq k \leq n$, there are $k + 1$ ways to partition k_1 and k_3, and another $k + 1$ ways to partition k_2 and k_4. There are $(k + 1)^2$ ways to partition k_i in this interval. Hence

$$\sum_{k=0}^{n} (k + 1)^2$$

Case 2: If $n + 1 \leq k \leq 2n$, each of the k_i is at most n and at least 0. There are $(2n - k + 1)^2$ ways to partition the k_i in this interval. Hence

$$\sum_{k=n+1}^{2n} (2n - k + 1)^2$$

Evaluating the sum gives us $\boxed{\dfrac{(n + 1)(2n^2 + 4n + 3)}{3}}$. $\qquad\square$

14 Graph Theory

Readings:

- [Graph Theory Vol. 3](#)

basics of counting; the inclusion-exclusion principle; the pigeonhole principle; permutations and combinations; the binomial theorem; recurrence relations and linear recurrence relations;

graph concepts such as Shortest-, Euler-, Hamilton-Paths and Cycles, coloring, planarity, weighted graphs, and directed graphs.

Topics in graph theory, including: connectivity and matchings, Hall's theorem, Menger's theorem, network flows; paths and cycles, complete subgraphs and Turán's theorem, and the Erdös-Stone theorem; graph colouring and the four-colour theorem; Ramsey theory; probabilistic methods in graph theory; and the use of software to solve graph-theoretic problems.

§14.1   Basic Notions

§14.1.1   Graphs

- A **graph** G is a pair $G = (V, E)$ where V is a set of **vertices** and E is a (multi)set of unordered pairs of vertices. The elements of E are called **edges**. We write $V(G)$ for the set of vertices and $E(G)$ for the set of edges of a graph G. Also, $|G| = |V(G)|$ denotes the number of vertices and $e(G) = |E(G)|$ denotes the number of edges.

- A loop is an edge (v, v) for some $v \in V$. An edge $e = (u, v)$ is a multiple edge if it appears multiple times in E. A graph is **simple** if it has no loops or multiple edges.

  Unless explicitly stated otherwise, we will only consider simple graphs. General (potentially nonsimple) graphs are also called multigraphs.

- Vertices u, v are **adjacent** in G if $(u, v) \in E(G)$.

  An edge $e \in E(G)$ is **incident** to a vertex $v \in V(G)$ if $v \in e$.

  Edges e, e' are **incident** if $e \cap e' = \varnothing$.

If $(u,v) \in E$ then v is a **neighbour** of u.

- Given a vertex v, the **degree** of v is defined to be the number of edges containing v as an endpoint. If the degree of each vertex is the same, we can call that the degree of the graph.

- A **path** in a graph G is defined to be a finite sequence of distinct vertices $v_0, v_1, \ldots, v_t$ such that v_i is adjacent to v_{i+1}. (A graph itself can also be called a path.) The **length** of a path is defined to be the number of edges in the path.

- A **cycle** in a graph G is defined to be a finite sequence of distinct vertices $v_0, v_1, \ldots, v_t$ such that v_i is adjacent to v_{i+1} where the indices are taken modulo $t+1$. (A graph itself can also be called a cycle.) The **length** of a cycle is defined to be the number of vertices (or edges) in the path.

- A graph is said to be **connected** if for any pair of vertices, there exists a path joining the two vertices. Otherwise, a graph is said to be **disconnected**.

- The **distance** between two vertices u, v in a graph is defined to be the length of the shortest path joining u, v. (In the case the graph is disconnected, this may not be well-defined.)

- Let $G = (V, E)$ be a graph. The **complement** $\overline{G}$ of G is a graph with the same vertex set as G and $E(\overline{G}) = e \notin E(G)$, i.e. $\overline{G}$ has edges exactly where there are no edges in G.

- Let $G = (V, E)$ be a finite graph. A graph G is said to be **complete** if every pair of vertices in G is joined by an edge. A complete graph on n vertices is denoted by K_n.

- A graph G is said to be **bipartite** if $V(G)$ can be partitioned into two non-empty disjoint sets A, B such that no edge has both endpoints in the same set. A graph is said to be **complete bipartite** if G is bipartite and all possible edges between the two sets A, B are drawn. In the case where $|A| = m, |B| = n$, such a graph is denoted by $K_{m,n}$.

- Let $k \geq 2$. A graph G is said to be k-**partite** if $V(G)$ can be partitioned into k pairwise disjoint sets $A_1, \ldots, A_k$ such that no edge has both endpoints in the same set. A **complete k-partite** graph is defined similarly as a complete bipartite. In the case where $|A_i| = n_i$, such a graph is denoted by $K_{n_1, n_2, \ldots, n_k}$. (Note that a 2-partite graph is simply a bipartite graph.)

- A graph is said to be **planar** if it can be drawn such that a pair of edges can only cross at a vertex.

Trivial graph: one vertex

> **Theorem 14.1.1: Euler's Characteristic Formula**
>
> For any connected planar graph, the number of vertices V minus the number of edges E plus the number of regions R equals 2.
>
> $$V - E + R = 2 \qquad (14.1)$$

(or V-E+F=2 for 3 dimensional polyhedra) To prove this, for trivial graph, V=1, F=1, E=0 Adding one edge, we either introduce a new vertex or face (if edge is connected to preexisting vertex)

vertex/edge colouring and Ramsey Theory

nature and properties

Connected graph Regular graph Complete graph Bipartite graph Directed graph

§14.1.2 Graph isomorphism

> **Definition 14.1.1: Isomorphism**
>
> Let $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ be graphs. An isomorphism $\varphi : G_1 \to G_2$ is a bijection (a one-to-one correspondence) from V_1 to V_2 such that $(u, v) \in E_1$ if and only if $(\varphi(u), \varphi(v)) \in E_2$. We say G_1 is isomorphic to G_2 if there is an isomorphism between them.

§14.2 Trees and Balancing

A **tree** is defined to be a connected graph that does not contain any cycles.

A **cycle** in a graph means there is a path from an object back to itself.

Characterisation of trees: Let G be a connected graph with n vertices. The following statements are equivalent.

1. G does not contain any cycles

2. G contains exactly $n - 1$ edges

3. For any two vertices, there exists exactly one path joining the two vertices

4. The removal of any edge disconnects the graph

Problems

Problem 14.2.1 (Königsberg Bridge Problem)**.** Königsberg was a small town in Prussia. There is a river running through the town and there were seven bridges across the river. The inhabitants of Königsberg liked to walk around the town and cross all of the bridges:

Is it possible to walk around the town and cross every bridge, once and once only?

Solution. We replace every landmass by a vertex and every bridge by an edge to give the following graph.

$\square$

Problems can include tournament, matching, and scheduling problems.

Problem 14.2.2. (Moser's circle problem) Determine the number of regions into which a circle is divided if n points on its circumference are joined by chords with no three internally concurrent.

Solution. Consider the graph which has points on the circumference and intersection points between chords as its vertices.

Let V, E, F denote the number of vertices, edges, regions respectively.

To count the number of intersection points, note that 4 points on the circumference give one unique intersection point between the two non-parallel chords formed by connecting two pairs of points which intersect inside the circle. Hence, number of intersection points is $\binom{n}{4}$.

$$V = n + \binom{n}{4}$$

Total number of edges includes n circular arcs, number of original chords formed from connecting pairs of points on the circumference E = no. of original lines + 2 x no. of intersection points E = n choose 2 + 2 x n choose 4 + n since there are n circular arcs

Using Euler's Characteristic Formula, we have

$$F = E - V - 1$$

$$\boxed{F = 1 + \binom{n}{2} + \binom{n}{4}}$$

$\square$

Part V

Miscellaneous

15 Proofs

§15.1 Induction

> **Definition 15.1.1: Mathematical induction**
>
> Let $P(n)$ be a family of statements indexed by $n \in \mathbb{N}$.
> By **mathematical induction**, If $P(0)$ is true and $P(k)$ is true $\forall k \in \mathbb{N}$, then $P(n)$ is true $\forall n \in \mathbb{N}$.

Steps to write the proof:

1. **Base case.**

   Prove that $P(0)$ is true.

2. **Inductive step..**

   $P(k) \implies P(k+1)$

> **Example 15.1.1: P**
>
> ove that
> $$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$
> for all positive integers n.

Proof.
The statement is true for $n = 1$ (base case) because with $n = 1$, LHS = RHS = 1.

Assume that the statement is true for some $n = k$, where $k \in \mathbb{Z}^+$. By our induction hypothesis, we have $1 + 2 + 3 + \cdots + k = \dfrac{k(k+1)}{2}$.

To show that the statement is true for $k + 1$,

$$
\begin{aligned}
1 + 2 + 3 + \cdots + k + (k + 1) &= \frac{k(k + 1)}{2} + (k + 1) \\
&= \frac{(k + 1)(k + 2)}{2} \\
&= \frac{(k + 1)[(k + 1) + 1]}{2}
\end{aligned}
$$

$\because$ The statement holds true for $n = k$ and $n = k + 1$,

$\therefore$ The statement is true for all positive integers n. $\qquad \square$

Definition 15.1.2: Cauchy induction

Cauchy induction, also known as forward-backward induction, is a variant of mathematical induction.

To write the proof, there are a few steps:

1. **Base case.**

   Prove that $P(0)$ is true.

2. **Inductive step**.
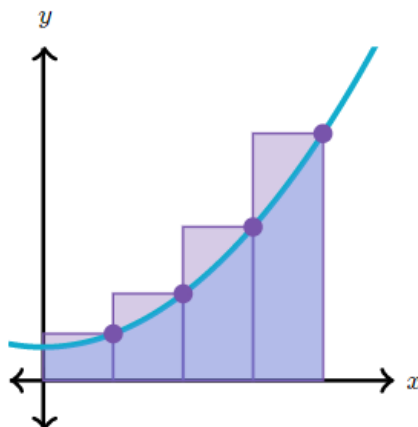
   $P(k) \implies P(2k)$

   $P(k) \implies P(k - 1)$

16 Calculus

§16.1 Riemann Sums

Given $y = f(x)$, we want to find the integral on the x-interval $[0, 1]$.

Split the interval $[0, 1]$ into n equal subintervals

$$\left[0, \frac{1}{n}\right], \left[\frac{1}{n}, \frac{2}{n}\right], \cdots, \left[\frac{n-1}{n}, 1\right].$$

Consider the height of the rectangles. We take the right value. Hence for the k-th subinterval $\left[\frac{k-1}{n}, \frac{k}{n}\right]$ where $k = 1, \ldots, n$, the height of rectangle is $f\left(\frac{k}{n}\right)$.

Area of kth rectangle is

$$\frac{1}{n} \cdot f\left(\frac{k}{n}\right).$$

Therefore, the integral is obtained by summing up the area of n rectangles, which gives us

$$\int_0^1 f(x)\,\mathrm{d}x = \lim_{n \to \infty} \sum_{k=1}^n \frac{1}{n} f\left(\frac{k}{n}\right) \tag{16.1}$$

where there are infinitely many rectangles, i.e. $n \to \infty$.

Problems

Problem 16.1.1 (SMO 2020 Open Q10)**.** Find the value of

$$S = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{\sqrt{n(n+k)}}$$

Solution.

$$S = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{n} \sqrt{\frac{1}{1+\frac{k}{n}}}$$

$$= \int_0^1 \frac{1}{\sqrt{1+x}} \, \mathrm{d}x$$

$$= 2\sqrt{2} - 2$$

$\square$

Problem 16.1.2 (SMO 2018 Open Q12)**.** Given that

$$S = \lim_{n\to\infty} \sum_{k=1}^{n} \frac{1}{n+k}$$

Find the value of S.

Solution. Using Riemann sums,

$$\lim_{n\to\infty} \sum_{k=1}^{n} f\left(\frac{k}{n}\right) = \int_0^1 f(x) \, \mathrm{d}x$$

Hence

$$S = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \frac{1}{1+\frac{k}{n}} = \int_0^1 \frac{1}{1+x} \, \mathrm{d}x = \boxed{\ln 2}$$

$\square$