

# **Mathematics Olympiad: A Guidebook**

Ryan Joo Rui An

*You don't have to be a mathematician to have a feel for numbers.*

— John Forbes Nash, Jr. (1928–2015)  
American mathematician

Copyright © 2024 by Ryan Joo Rui An. Text licensed under [CC-by-SA-4.0](#). Source files licensed under [GNU GPL v3](#).

This is (still!) an incomplete draft. Please send corrections and comments to [ryanjooruian18@gmail.com](mailto:ryanjooruian18@gmail.com), or pull-request at <https://github.com/Ryanjoo18/math-olympiad>.

Typeset using L<sup>A</sup>T<sub>E</sub>X.

Last updated September 1, 2024.

## About the Author

**Ryan Joo Rui An** is a dedicated and passionate high school student currently engaged in A Level studies in Singapore. With a strong foundation in mathematics, He has spent over 11 years honing his skills in various mathematics competitions. His journey began at an early age, where he developed a fascination with numbers while doing mental arithmetic. This early interest quickly blossomed into a deep commitment to mathematics, leading him to participate in numerous mathematics olympiads competitions.

The author's (not many) mathematics credentials include:

- Singapore Mathematics Olympiad 2022 – 2024: 3 Silver awards
- Singapore and Asian Schools Math Olympiad 2019 – 2023: 6 Gold awards, top in Singapore in 2022 – 2023, top in Malaysia in 2024
- Singapore International Mathematical and Computational Challenge 2024: Merit award
- Australian Mathematics Competition 2019 – 2023: 2 Prize awards, 2 High Distinction awards, best in school in 2023
- High School Mathematical Contest in Modeling 2023: Honourable mention
- Hua Lo Geng Secondary School Mathematics Competition 2019: 2nd place
- Chen Jingrun's Cup Secondary School Mathematics Competition 2019: 1st place

Outside of mathematics, the author has a keen interest in playing chess and programming.

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, which feature rather challenging problems.

Do reach out to the author at [ryanjoorui18@gmail.com](mailto:ryanjoorui18@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.

## Preface

This book is divided into the following sections.

The chapters in this book are structured in the following typical manner. Each chapter begins with a **theoretical portion**, which starts off with a couple of definitions, followed by theorems, lemmas and propositions built upon the definitions. Each chapter is ended by some **exercises** accompanied by solutions to them.

The reader is not assumed to have any mathematical prerequisites.

# Contents

<b>I</b>	<b>Number Theory</b>	<b>1</b>
<b>1</b>	<b>Modular Arithmetic</b>	<b>2</b>
1.1	Divisibility . . . . .	2
1.2	GCD and LCM . . . . .	4
1.3	Arithmetic Functions . . . . .	7
1.4	Congruence . . . . .	7
1.4.1	Some theorems . . . . .	8
1.5	Modular Inverse . . . . .	10
1.6	Orders Modulo A Prime . . . . .	13
1.6.1	Order . . . . .	13
1.6.2	Primitive Roots . . . . .	13
1.7	Quadratic Residues . . . . .	14
<b>2</b>	<b>Diophantine Equations</b>	<b>22</b>
2.1	Linear Diophantine Equations . . . . .	22
2.1.1	Homogeneous Linear Diophantine Equations . . . . .	22
2.1.2	Non-homogeneous Linear Diophantine Equations . . . . .	23
2.1.3	Chicken McNugget Theorem . . . . .	24
2.2	Pythagorean Triples . . . . .	25
2.3	Pell's Equation . . . . .	25
<b>II</b>	<b>Algebra</b>	<b>27</b>
<b>3</b>	<b>Basic Algebra</b>	<b>28</b>
3.1	Algebraic Manipulation . . . . .	28
3.2	Polynomials . . . . .	30
3.2.1	Finding Roots of Polynomials . . . . .	30
3.2.2	Coefficients and Roots . . . . .	32
3.2.3	Combinatorial Nullstellensatz . . . . .	32
3.2.4	Transforming Polynomials . . . . .	32
3.2.5	Newton's Sums . . . . .	32

3.3	Absolute Value Equations . . . . .	33
3.4	Logarithms . . . . .	34
<b>4</b>	<b>Inequalities</b>	<b>62</b>
4.1	AM–GM Inequality . . . . .	62
4.1.1	General AM–GM Inequality . . . . .	62
4.1.2	Weighted AM–GM Inequality . . . . .	65
4.1.3	Other mean quantities . . . . .	65
4.1.4	Murihead’s inequality . . . . .	66
4.2	Cauchy–Schwarz and Hölder’s Inequalities . . . . .	66
4.3	Rearrangement and Chebyshev’s Inequalities . . . . .	67
4.4	Other Useful Strategies . . . . .	67
4.4.1	Schur’s Inequality . . . . .	67
4.4.2	Jensen’s Inequality . . . . .	68
4.4.3	Minkowski’s Inequality . . . . .	69
4.4.4	Ravi Transformation . . . . .	69
4.4.5	Normalisation . . . . .	69
4.4.6	Homogenisation . . . . .	70
<b>5</b>	<b>Functional Equations</b>	<b>90</b>
5.1	Introduction . . . . .	90
5.2	Heuristics . . . . .	90
5.3	Cauchy’s Functional Equation Over $\mathbf{Q}$ . . . . .	92
5.4	Cauchy’s Functional Equation Over $\mathbf{R}$ . . . . .	93
<b>6</b>	<b>Sequences and Series</b>	<b>98</b>
6.1	Summation Series . . . . .	98
6.2	Arithmetic and Geometric Progressions . . . . .	98
6.2.1	Arithmetic Progression . . . . .	98
6.2.2	Geometric Progression . . . . .	98
6.3	Telescoping Sums . . . . .	99
6.4	Power Series . . . . .	99
<b>III</b>	<b>Geometry</b>	<b>101</b>
<b>7</b>	<b>Synthetic Geometry</b>	<b>102</b>
7.1	Angles . . . . .	102
7.1.1	Phantom Points . . . . .	102
7.2	Triangle . . . . .	103
7.2.1	Triangle centres . . . . .	103
7.2.2	Right triangle . . . . .	104
7.2.3	Congruency and Similarity . . . . .	104
7.2.4	Theorems . . . . .	105

7.2.5	Ceva and Menelaus . . . . .	106
7.2.6	Area of triangle . . . . .	108
7.3	Quadrilaterals . . . . .	109
7.4	Circle . . . . .	110
7.4.1	Angles . . . . .	110
7.4.2	Cyclic Quadrilaterals . . . . .	110
7.4.3	Power of a Point . . . . .	111
7.4.4	Theorems . . . . .	113
<b>8</b>	<b>Analytic Geometry</b>	<b>120</b>
8.1	Trigonometry . . . . .	120
8.1.1	Pythagorean identities . . . . .	120
8.1.2	Addition formulae . . . . .	121
8.1.3	R-formula . . . . .	122
8.1.4	Sine and Cosine Rules . . . . .	123
8.2	Hyperbolic Functions . . . . .	124
8.2.1	Basics . . . . .	124
8.2.2	Reciprocals and Inverses . . . . .	124
8.2.3	Identities . . . . .	124
8.3	Cartesian Geometry . . . . .	126
8.3.1	Basics . . . . .	126
8.3.2	Conic Sections . . . . .	126
8.3.3	Polar Coordinates . . . . .	129
8.4	Linear Algebra . . . . .	130
8.4.1	Determinant . . . . .	130
8.4.2	Transposes . . . . .	130
8.4.3	Matrix Product . . . . .	130
8.4.4	Vector spaces associated with a matrix . . . . .	130
8.4.5	Rank and nullity . . . . .	131
8.5	Complex Numbers . . . . .	132
8.6	Barycentric Coordinates . . . . .	133
8.6.1	The Basics . . . . .	133
8.6.2	Standard Strategies . . . . .	134
<b>9</b>	<b>Transformations</b>	<b>143</b>
9.1	Inversive Geometry . . . . .	143
9.1.1	Definition and First Properties . . . . .	143
9.1.2	Generalised Lines and Circles . . . . .	143
9.1.3	Inversion Distance Formula . . . . .	144
9.2	Projective Geometry . . . . .	145
9.2.1	Homothety . . . . .	145
9.3	Complete Quadrilaterals . . . . .	145

9.3.1	Spiral Similarity . . . . .	145
9.3.2	Miquel Point of Cyclic Quadrilateral . . . . .	145
<b>10</b>	<b>Miscellaneous</b>	<b>147</b>
10.1	Construction . . . . .	147
10.2	Locus . . . . .	148
10.3	3D Geometry . . . . .	148
10.4	Geometric Inequalities . . . . .	148
<b>IV</b>	<b>Combinatorics</b>	<b>150</b>
<b>11</b>	<b>Combinatorics</b>	<b>151</b>
11.1	Basic Identities . . . . .	151
11.1.1	Pascal's Triangle . . . . .	151
11.1.2	Binomial Theorem . . . . .	152
11.2	Counting Problems . . . . .	153
11.2.1	Addition and Multiplication Principles . . . . .	153
11.2.2	Some Techniques . . . . .	153
11.2.3	Bijection Principle . . . . .	153
11.2.4	Principle of Inclusion–Exclusion . . . . .	155
11.2.5	Pigeonhole Principle . . . . .	157
11.3	Distribution Problems . . . . .	159
11.3.1	Distinguishable objects into distinguishable boxes . . . . .	159
11.3.2	Indistinguishable objects into distinguishable boxes . . . . .	159
11.3.3	Distinguishable objects into indistinguishable boxes . . . . .	160
11.3.4	Indistinguishable objects into indistinguishable boxes . . . . .	162
11.4	Further Concepts . . . . .	163
11.4.1	Catalan Numbers . . . . .	163
11.4.2	Derangements . . . . .	163
11.5	Colouring Problems . . . . .	164
11.6	Probability . . . . .	165
11.6.1	Definitions and Notation . . . . .	165
11.6.2	Properties of Expected Value . . . . .	165
11.7	Generating Functions . . . . .	166
11.7.1	Properties of OGFs . . . . .	166
11.7.2	Properties of EGFs . . . . .	166
<b>12</b>	<b>Recurrence Relations</b>	<b>178</b>
12.1	Introduction . . . . .	178
12.1.1	Definition . . . . .	178
12.1.2	Identifying Recurrence Relations . . . . .	179
12.2	First-order Recurrence Relations . . . . .	181



---

12.3 Second-order Recurrence Relations . . . . .	181
<b>13 Graph Theory</b>	<b>187</b>
13.1 Introduction, Definitions and Notations . . . . .	187
13.2 Trees and Balancing . . . . .	188
13.3 Friends, Strangers and Cliques . . . . .	188
13.4 Directed Graphs, Lots of Arrows and Tournaments . . . . .	188
13.5 Matchings: Pair Them Up . . . . .	188
13.6 Hamiltonian and Eulerian Paths and Cycles . . . . .	188
<b>V Other Topics</b>	<b>191</b>
<b>14 Proofs</b>	<b>192</b>
14.1 Induction . . . . .	192
<b>15 Riemann Integrals</b>	<b>194</b>
15.1 Riemann Sums . . . . .	194
15.2 Double Integrals . . . . .	198
<b>16 Strategy Games</b>	<b>202</b>

# List of Theorems

1.5	Theorem (Division algorithm)	3
1.6	Theorem (Fundamental theorem of arithmetic)	3
1.7	Theorem (Euclid)	3
1.8	Theorem (Prime number theorem)	4
1.16	Theorem (Dirichlet's theorem)	7
1.21	Theorem (Fermat's little theorem)	8
1.22	Theorem (Euler's totient theorem)	9
1.24	Theorem (Wilson's theorem)	10
1.25	Theorem (Chinese remainder theorem)	11
1.28	Theorem (Fundamental theorem of orders)	13
1.33	Theorem (Euler's criterion)	14
1.36	Theorem (Gauss' lemma)	15
1.37	Theorem (Second supplementary law)	15
1.38	Theorem (Eisenstein's lemma)	15
1.39	Theorem (Law of quadratic reciprocity)	15
2.2	Theorem (Bezout's lemma)	23
2.4	Theorem (Chicken mcnugget theorem)	24
2.6	Theorem (Pell's equation)	25
2.7	Theorem (Fermat's last theorem)	26
3.1	Theorem (Quadratic formula)	30
3.2	Theorem (Division algorithm)	30
3.3	Theorem (Remainder theorem)	30
3.4	Theorem (Factor theorem)	30
3.5	Theorem (Linear factorisation theorem)	30
3.6	Theorem (Fundamental theorem of algebra)	31
3.7	Theorem (Rational root theorem)	31
3.8	Theorem (Descartes' rule of signs)	31
3.10	Theorem (Lagrange interpolation formula)	31
3.11	Theorem (Gauss's lemma)	31
3.12	Theorem (Vieta's relations)	32

4.1	Theorem (AM–GM inequality) . . . . .	62
4.2	Theorem (Weighted AM–GM inequality) . . . . .	65
4.3	Theorem (Muirhead’s inequality) . . . . .	66
4.4	Theorem (Cauchy–Schwarz’s inequality) . . . . .	66
4.5	Theorem (Titu’s lemma) . . . . .	66
4.6	Theorem (Hölder’s inequality) . . . . .	67
4.7	Theorem (Chebyshev’s inequality) . . . . .	67
4.8	Theorem (Rearrangement inequality) . . . . .	67
4.9	Theorem (Triangle inequality) . . . . .	67
4.10	Theorem (Schur’s inequality) . . . . .	67
4.11	Theorem (Jensen’s inequality) . . . . .	68
4.12	Theorem (Minkowski’s inequality) . . . . .	69
4.13	Theorem (Generalised Minkowski’s inequality) . . . . .	69
4.14	Theorem (Bernoulli’s inequality) . . . . .	69
7.9	Theorem (Pythagoras’ theorem) . . . . .	104
7.10	Theorem (Viviani’s Theorem) . . . . .	105
7.11	Theorem (Carnot’s theorem) . . . . .	105
7.12	Theorem (Angle bisector theorem) . . . . .	105
7.14	Theorem (Stewart’s theorem) . . . . .	106
7.16	Theorem (Ceva’s theorem) . . . . .	106
7.17	Theorem (Menelaus’ theorem) . . . . .	106
7.22	Theorem (Heron’s formula) . . . . .	108
7.23	Theorem (British flag theorem) . . . . .	109
7.24	Theorem (Ptolemy’s theorem) . . . . .	110
7.25	Theorem (Ptolemy’s inequality) . . . . .	110
7.26	Theorem (Brahmagupta’s formula) . . . . .	110
7.27	Theorem (Power of a point) . . . . .	111
7.28	Theorem (Converse to power of a point) . . . . .	112
7.34	Theorem (Radical axis theorem) . . . . .	113
7.35	Theorem (Hamilton’s theorem) . . . . .	113
7.36	Theorem (Euler line) . . . . .	113
7.37	Theorem (Nine-point circle) . . . . .	114
7.38	Theorem (Simson line) . . . . .	114
7.40	Theorem (Miquel’s theorem) . . . . .	114
8.1	Theorem (Sine rule) . . . . .	123
8.2	Theorem (Cosine rule) . . . . .	123
8.4	Theorem (Line) . . . . .	133
8.6	Theorem (Ceva’s theorem) . . . . .	133
10.1	Theorem (Triangle inequality) . . . . .	148
10.2	Theorem (Pythagorean inequality) . . . . .	148

10.3 Theorem (Isoperimetric inequality) . . . . .	148
10.4 Theorem (Euler's inequality) . . . . .	149
10.5 Theorem (Ptolemy's inequality) . . . . .	149
10.6 Theorem (Erdos–Mordell inequality) . . . . .	149
11.7 Theorem (Binomial Theorem) . . . . .	152
11.11 Theorem (Bijection Principle) . . . . .	153
11.12 Theorem (Principle of Inclusion–Exclusion) . . . . .	155
11.13 Theorem (Pigeonhole Principle) . . . . .	157
11.14 Theorem (Generalised Pigeonhole Principle) . . . . .	157
11.28 Theorem (Linearity of expectation) . . . . .	165
13.1 Theorem (Euler) . . . . .	188
13.3 Theorem (Hall's theorem) . . . . .	188
13.4 Theorem (Dirac's theorem) . . . . .	189
13.5 Theorem (Turan's theorem) . . . . .	189
13.6 Theorem (Four colour theorem) . . . . .	189
13.7 Theorem (Hall's marriage theorem) . . . . .	189
14.1 Theorem (Principle of Mathematical Induction (PMI)) . . . . .	192
14.2 Theorem (Strong Form of Induction) . . . . .	192
14.3 Theorem (Cauchy Induction) . . . . .	193



**Part I**

**Number Theory**

# 1 Modular Arithmetic

## §1.1 Divisibility

**Definition 1.1** (Divisibility). For integers  $a$  and  $b$ , we say that  $a$  *divides*  $b$ , or that  $a$  is a *divisor* (or *factor*) of  $b$ , or that  $b$  is a multiple of  $a$ , if there exists an integer  $c$  such that  $b = ca$ , and we denote this by  $a \mid b$ . Otherwise,  $a$  does not divide  $b$ , and we denote this by  $a \nmid b$ .

**Definition 1.2** (Prime). A positive integer  $p$  is a *prime* if the only divisors of  $p$  are 1 and  $p$ .

If  $p^k \mid a$  and  $p^{k+1} \nmid a$  where  $p$  is prime, i.e.  $p^k$  is the highest power of  $p$  dividing  $a$ , then we denote this by  $p^k \parallel a$ .

*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.

**Proposition 1.3.** 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  $a \mid b_1, \dots, a \mid b_n$ , then for any integers  $c_1, \dots, c_n$ ,

$$a \mid \sum_{i=1}^n b_i c_i.$$

### Exercise 1

Let  $a, b \in \mathbf{Z}$ . Prove that if  $a, b > 0$  and  $a \mid b$ , then  $a \leq b$ .

*Proof.* Suppose  $a, b > 0$  and  $a \mid b$ . Then there exists an integer  $k$  such that  $b = ak$ .

So  $k > 0$  as  $a$  and  $b$  are positive.

It follows that  $1 \leq k$ , as every positive integer  $\geq 1$ .

Then  $a \leq ak$ , as multiplying both sides of an inequality by a positive number preserves the inequality.

Hence  $a \leq b$ . □

The following **divisibility rules** help determine when positive integers are divisible by particular other integers.

**Lemma 1.4** (Divisibility rules).

- (i) A number is divisible by  $2^n$  if and only if its last  $n$  digits are divisible by  $2^n$ .
- (ii) A number is divisible by 3 if and only if the sum of its digits is divisible by 3; a number is divisible by 9 if and only if the sum of its digits is divisible by 9.
- (iii) A number is divisible by  $5^n$  if and only if its last  $n$  digits are divisible by  $5^n$ .
- (iv) A number is divisible by 7 if and only if partitioning it 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 7.
- (v) A number is divisible by  $10^n$  if and only if it has  $n$  trailing zeros.
- (vi) A number is divisible by 11 if and only if the alternating sum of the digits is divisible by 11.
- (vii) A number is divisible by 13 if and only if partitioning it 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.

**Theorem 1.5** (Division algorithm). For all integers  $n$  and  $d$  with  $d > 0$ , there exists unique integers  $q$  and  $r$ , known as *quotient* and *remainder* respectively, such that

$$n = dq + r, \quad 0 \leq r < d.$$

**Theorem 1.6** (Fundamental theorem of arithmetic). Every integer  $n > 1$  can be expressed as a product of primes in a unique way apart from the order of the prime factors; that is,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where  $p_i$  are prime numbers and  $a_i$  are positive integers.

*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.  $\square$

**Theorem 1.7** (Euclid). There are infinitely many primes.

*Proof.* We prove by contradiction. Suppose otherwise, that there are a finite number of primes, say  $p_1, p_2, \dots, p_n$ . Let  $N = p_1 p_2 \cdots p_n + 1$ . By the fundamental theorem of arithmetic,  $N$  is divisible by some prime  $p$ . This prime  $p$  must be among the  $p_i$ , since by assumption these are all the primes, but  $N$  is seen not to be divisible by any of the  $p_i$ , a contradiction.  $\square$

## Exercise 2

Find all positive integers  $d$  such that  $d$  divides both  $n^2 + 1$  and  $(n + 1)^2 + 1$  for some integer  $n$ .

**Solution.** Let  $d \mid (n^2 + 1)$  and  $d \mid [(n + 1)^2 + 1]$ , or  $d \mid (n^2 + 2n + 2)$ . Then

$$\begin{aligned} d &\mid [(n^2 + 2n + 2) - (n^2 + 1)] \\ d &\mid (2n + 1) \\ d &\mid (4n^2 + 4n + 1) \\ d &\mid [4(n^2 + 2n + 2) - (4n^2 + 4n + 1)] \\ d &\mid (4n + 7) \\ d &\mid [(4n + 7) - 2(2n + 1)] \\ d &\mid 5 \end{aligned}$$

so  $d$  can only be 1 or 5. Taking  $n = 2$  shows that both of these values are achieved.  $\square$



**Exercise 3** (IMO 1984 Shortlist)

Suppose that  $a_1, a_2, \dots, a_{2n}$  are distinct integers such that the equation

$$(x - a_1)(x - a_2) \cdots (x - a_{2n}) - (-1)^n (n!)^2 = 0$$

has an integer solution  $r$ . Show that

$$r = \frac{a_1 + a_2 + \cdots + a_{2n}}{2n}.$$

**Solution.** Clearly,  $r \neq a_i$  for all  $i$ , and the  $r - a_i$  are  $2n$  distinct integers, so

$$|(r - a_1)(r - a_2) \cdots (r - a_{2n})| \geq |(1)(2) \cdots (n)(-1)(-2) \cdots (-n)| = (n!)^2,$$

with equality if and only if

$$\{r - a_1, r - a_2, \dots, r - a_{2n}\} = \{1, 2, \dots, n, -1, -2, \dots, -n\}.$$

Therefore, this must be the case, so

$$\begin{aligned} & (r - a_1) + (r - a_2) + \cdots + (r - a_{2n}) \\ &= 2nr - (a_1 + a_2 + \cdots + a_{2n}) \\ &= 1 + 2 + \cdots + n + (-1) + (-2) + \cdots + (-n) = 0 \end{aligned}$$

and hence

$$r = \frac{a_1 + a_2 + \cdots + a_{2n}}{2n}.$$

□

**Exercise 4** (Putnam 1966)

Let  $0 < a_1 < a_2 < \cdots < a_{mn+1}$  be  $mn + 1$  integers. Prove that you can select either  $m + 1$  of them no one of which divides any other, or  $n + 1$  of them each dividing the following one.

**Solution.** For each  $i$ ,  $1 \leq i \leq mn + 1$ , let  $n_i$  be the length of the longest sequence starting with  $a_i$  and each dividing the following one, among the integers  $a_i, a_{i+1}, \dots, a_{mn+1}$ . If some  $n_i$  is greater than  $n$  we are done. Otherwise, by the pigeonhole principle, there are at least  $m + 1$  values of  $n_i$  that are equal. Then, the integers  $a_i$  corresponding to these  $n_i$  cannot divide each other. □

**Theorem 1.8** (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  $\frac{x}{\ln x}$ ; that is,

$$\pi(x) \sim \frac{x}{\ln x}.$$

## §1.2 GCD and LCM

**Definition 1.9.** Let  $a, b$  be integers, not both 0, and  $d \in \mathbf{Z}^+$ .  $d$  is the *greatest common divisor* of  $a$  and  $b$ , denoted by  $d = \gcd(a, b)$ , if and only if

- (i)  $d \mid a$  and  $d \mid b$
- (ii) for all  $k \in \mathbf{Z}^+$ , if  $k \mid a$  and  $k \mid b$  then  $k \leq d$ .

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

We say that  $a$  and  $b$  are *relatively prime* (or coprime) if  $\gcd(a, b) = 1$ .

Basic properties of GCD:

- $\gcd(a, b) > 0$ , whether  $a$  and  $b$  are positive or negative
- $\gcd(a, a) = |a|$
- $\gcd(a, 0) = |a|$
- $\gcd(a, b) = \gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b)$

**Lemma 1.10.** For positive integers  $a$  and  $b$ ,

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

**Proposition 1.11.** For positive integers  $a$ ,  $b$  and  $m$ ,

$$\gcd(ma, mb) = m \gcd(a, b), \quad \text{lcm}(ma, mb) = m \text{lcm}(a, b).$$

**Proposition 1.12.** If  $d \mid \gcd(a, b)$ , then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\gcd(a, b)}{d}.$$

In particular, if  $d = \gcd(a, b)$ , then  $\gcd(a/d, b/d) = 1$ ; that is,  $\frac{a}{d}$  and  $\frac{b}{d}$  are relatively prime.

**Lemma 1.13.** Let  $c$  and  $d$  be integers, not both 0. If  $q$  and  $r$  are integers such that  $c = dq + r$  then  $\gcd(c, d) = \gcd(d, r)$ .

*Proof.* Let  $m = \gcd(c, d)$  and  $n = \gcd(d, r)$ . To prove  $m = n$ , we will show  $m \leq n$  and  $n \leq m$ .

We first show  $n \leq m$ . Since  $n = \gcd(d, r)$  then  $n \mid d$  and  $n \mid r$ . There exists integers  $x$  and  $y$  such that  $d = nx$  and  $r = ny$ .

From  $c = dq + r$  we have

$$c = (nx)q + ny = n(xq + y)$$

Hence  $n \mid c$ . Since  $n$  is a common divisor of  $c$  and  $d$ ,  $n \leq \gcd(c, d)$  so  $n \leq m$ .

The proof of  $m \leq n$  is similar and shall be left as an exercise. □

Let  $a$  and  $b$  be two non-zero integers. Then  $a$  and  $b$  are said to be *relatively prime* (or coprime) if and only if  $\gcd(a, b) = 1$ .

**Lemma 1.14** (Euclid's Lemma). Let  $a, b, c$  be any integers. If  $a \mid bc$  and  $\gcd(a, b) = 1$  then  $a \mid c$ .

*Proof.* Since  $a \mid bc$ ,  $bc = ak$  for some  $k \in \mathbf{Z}$ .

Since  $\gcd(a, b) = 1$  then  $ax + by = 1$  for some  $x, y \in \mathbf{Z}$ .

$$\begin{aligned} cax + cby &= c \\ acx + akby &= c \\ acx + akby &= c \\ a(cx + ky) &= c \end{aligned}$$

Hence  $a \mid c$ . □

**Proposition 1.15** (Sieve of Eratosthenes). If  $p > 1$  is an integer and  $n \mid p$  for each integer  $n$  for which  $2 \leq n \leq \sqrt{p}$ , then  $p$  is prime.

*Proof.* Prove by contrapositive.

Suppose that  $p$  is not prime, so it factors as  $p = mn$  for  $1 < m, n < p$ .

Observe that it is not the case that both  $m > \sqrt{p}$  and  $n > \sqrt{p}$ , because if this were true the inequalities would multiply to give  $mn > \sqrt{p}\sqrt{p} = p$ , which contradicts  $p = mn$ .

Therefore  $m \leq \sqrt{p}$  or  $n \leq \sqrt{p}$ . Without loss of generality, say  $n \leq \sqrt{p}$ . Then the equation  $p = mn$  gives  $n \mid p$ , with  $1 < n \leq \sqrt{p}$ . Hence it is not true that  $n \nmid p$  for each integer  $n$  for which  $2 \leq n \leq \sqrt{p}$ . □

**Exercise 5**

Show that for any positive integer  $N$ , there exists a multiple of  $N$  that consists only of 1s and 0s. Furthermore, show that if  $N$  is relatively prime to 10, then there exists a multiple that consists only of 1s.

**Solution.** Consider the  $N + 1$  integers  $1, 11, 111, \dots, \underbrace{111\dots 1}_{N+1 \text{ 1s}}$ .

When divided by  $N$ , they leave  $N + 1$  remainders. By the pigeonhole principle, two of these remainders are equal, so the difference in the corresponding integers, an integer of the form  $111\dots 000$ , is divisible by  $N$ .

If  $N$  is relatively prime to 10, then we may divide out all powers of 10, to obtain an integer of the form  $111\dots 1$  that remains divisible by  $N$ .  $\square$

The *Euclidean Algorithm* is an efficient method to determine the gcd of two numbers. It makes use of the following properties:

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

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

$$a = q_1b + r_1 \quad 0 \leq r_1 < b$$

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

$$b = q_2r_1 + r_2 \quad 0 \leq r_2 < r_1$$

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

$$r_1 = q_3r_2 + r_3 \quad 0 \leq r_3 < r_2$$

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  $b > r_1 > r_2 > \dots > r_{n+1} > r_{n+2} = 0$  cannot contain more than  $b$  integers.

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

$$\begin{array}{ll} a = q_1b + r_1 & 0 \leq r_1 < b \\ b = q_2r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = q_3r_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \\ r_{n-2} = q_nr_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} = q_{n+1}r_n + 0 & \end{array}$$

Hence  $\gcd(a, b) = \gcd(b, r_1) = \dots = \gcd(r_n, 0) = r_n$ .

**Exercise 6**

Find  $\gcd(682, 264)$ .

**Solution.**

$$\begin{aligned} 682 &= 3 \times 264 - 110 \\ 264 &= 2 \times 110 + 44 \\ 110 &= 2 \times 44 + 22 \\ 44 &= 2 \times 22 + 0 \end{aligned}$$

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

### Exercise 7

Let  $n$  be a positive integer, and let  $S$  be a subset of  $n + 1$  elements of the set  $\{1, 2, \dots, 2n\}$ . Show that

- (a) There exist two elements of  $S$  that are relatively prime, and
- (b) There exist two elements of  $S$ , one of which divides the other.

**Solution.**

- (a) There must be two elements of  $S$  that are consecutive, and thus, relatively prime.
  - (b) Consider the greatest odd factor of each of the  $n + 1$  elements in  $S$ . Each is among the  $n$  odd integers  $1, 3, \dots, 2n - 1$ . By the pigeonhole principle, two must have the same greatest odd factor, so they differ (multiplication-wise) by a power of 2, and so one divides the other.
- 

### Exercise 8 (Russian Mathematics Olympiad 1951)

The positive integers  $a_1, a_2, \dots, a_n$  are such that each is less than 1000, and  $\text{lcm}(a_i, a_j) > 1000$  for all  $i, j, i \neq j$ . Show that

$$\sum_{i=1}^n \frac{1}{a_i} < 2.$$

**Solution.** □

**Theorem 1.16** (Dirichlet's theorem). If  $a$  and  $b$  are relatively prime positive integers, then the arithmetic sequence  $a, a + b, a + 2b, \dots$  contains infinitely many primes.

## §1.3 Arithmetic Functions

Let  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ .

**Lemma 1.17.** Number of factors of  $n$  is given by

$$\tau(n) = \prod_{i=1}^k (a_i + 1). \quad (1.1)$$

**Lemma 1.18.** Sum of factors of  $n$  is given by

$$d(n) = \prod_{i=1}^k (1 + p_i + \dots + p_i^{a_i}). \quad (1.2)$$

**Lemma 1.19.** Number of positive integers less than  $n$  which are coprime to  $n$  is given by

$$\phi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right), \quad (1.3)$$

where  $\phi(n)$  is known as the **totient function**.

## §1.4 Congruence

**Definition 1.20** (Congruence). Let  $a, b, n$  be integers with  $n > 0$ . Then we say  $a$  and  $b$  are *congruent modulo  $n$* , or  $a$  is congruent to  $b$  modulo  $n$ , denoted by  $a \equiv b \pmod{n}$ , if and only if  $n \mid a - b$  (or  $a = b + nk$  for some integer  $k$ ).

Properties of congruence<sup>1</sup>

- **Reflexive:** for every integer  $a$ ,  $a \equiv a \pmod{n}$ .
- **Symmetric:** for all integers  $a$  and  $b$ , if  $a \equiv b \pmod{n}$  then  $b \equiv a \pmod{n}$ .
- **Transitive:** for all integers  $a$ ,  $b$  and  $c$ , if  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$  then  $a \equiv c \pmod{n}$ .

For all integers  $a, b, c, d$  and  $n$ , with  $n > 1$ , if  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then

- $a + c \equiv b + d \pmod{n}$  (preserve addition)
- $ac \equiv bd \pmod{n}$  (preserve multiplication)
- $a + k \equiv b + k \pmod{n}$  for every  $k \in \mathbf{Z}$
- $ka \equiv kb \pmod{n}$  for every  $k \in \mathbf{Z}$
- $a^m \equiv b^m \pmod{n}$  for every  $m \in \mathbf{Z}^+$  (preserve power)

### Exercise 9

Prove that if  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then  $ac \equiv bd \pmod{n}$ .

*Proof.* Given  $a \equiv b \pmod{n}$ . So  $a = b + nk$  for some integer  $k$ .

Given  $c \equiv d \pmod{n}$ . So  $c = d + nh$  for some integer  $h$ .

Hence

$$ac = (b + nk)(d + nh) = bd + n(dk + bh + nkh)$$

Let  $q = dk + bh + nkh$ . Since  $ac = bd + nq$  for some integer  $q$ , hence  $ac \equiv bd \pmod{n}$ . □

## §1.4.1 Some theorems

**Theorem 1.21** (Fermat's little theorem). For prime  $p$  and  $p \nmid a$ ,

$$a^{p-1} \equiv 1 \pmod{p} \quad (1.4)$$

*Proof.* The idea is that if we write down the sequence of numbers

$$\{a, 2a, 3a, \dots, (p-1)a\}$$

and reduce each one modulo  $p$ , the resulting sequence turns out to be a rearrangement of

$$\{1, 2, 3, \dots, p-1\}.$$

To show this, we just need to show the elements in the first sequence are all different  $\pmod{p}$ : we want to show  $k_1 \not\equiv k_2 \pmod{p} \implies k_1a \not\equiv k_2a \pmod{p}$ .

We prove by contrapositive: suppose  $k_1a \equiv k_2a \pmod{p}$ . Since  $\gcd(a, p) = 1$ , we can do cancellation to give  $k_1 \equiv k_2 \pmod{p}$ . Hence proven.

Thus if we multiply together the numbers in each sequence, the results must be identical modulo  $p$ :

$$a \times 2a \times 3a \times \dots \times (p-1)a \equiv 1 \times 2 \times 3 \times \dots \times (p-1) \pmod{p}$$

Collecting together the  $a$  terms yields

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Since  $\gcd(p, (p-1)!) = 1$ , we can cancel  $(p-1)!$  on both sides to give  $a^{p-1} \equiv 1 \pmod{p}$ . □

<sup>1</sup>these properties can be proven during the definition of congruence.

**Exercise 10**

If  $n \in \mathbf{N}$  and  $\gcd(n, 35) = 1$ , prove that  $n^{12} \equiv 1 \pmod{35}$ .

*Proof.* By Fermat's Little Theorem,

$$n^4 \equiv 1 \pmod{5} \iff n^{12} \equiv 1 \pmod{5}$$

$$n^6 \equiv 1 \pmod{7} \iff n^{12} \equiv 1 \pmod{7}$$

Hence  $n^{12} \equiv 1 \pmod{35}$

□

The following theorem generalises Fermat's Little Theorem:

**Theorem 1.22** (Euler's totient theorem). For coprime  $a$  and  $n$ ,

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{1.5}$$

## §1.5 Modular Inverse

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

$$ab \equiv 1 \pmod{n}.$$

$b$  is known as the *inverse* of  $a$  modulo  $n$ .

*Proof.* Since  $\gcd(a, n) = 1$ , we have  $ab + nm = 1$  for some  $b, m \in \mathbf{Z}$ .

So  $ab + nm \equiv 1 \pmod{n}$ . Since  $nm \equiv 0 \pmod{n}$ , we get  $ab \equiv 1 \pmod{n}$ .  $\square$

We can find the modular inverse by reversing the Euclidean algorithm.

### Exercise 11

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:

$$26 = 3(7) + 5$$

$$7 = 1(5) + 2$$

$$5 = 2(2) + 1$$

Back substitute the equations:

$$\begin{aligned} 1 &= 5 - 2 \times (7 - 1 \times 5) \\ &= (-2) \times 7 + 3 \times 5 \\ &= (-2) \times 7 + 3 \times (26 - 3 \times 7) \\ &= 3 \times 26 + (-11) \times 7 \end{aligned}$$

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

**Lemma 1.23** (Uniqueness of modular inverse). The modular inverse is unique.

*Proof.* Assume  $x$  has two modular inverses  $b$  and  $c \pmod{n}$ . Then  $xb \equiv 1 \pmod{n}$  and  $xc \equiv 1 \pmod{n}$ .

Thus

$$b \equiv 1b \equiv (xc)b \equiv (xb)c \equiv 1c \equiv c \pmod{n}$$

$\square$

**Theorem 1.24** (Wilson's theorem). For odd prime  $p$ ,

$$(p-1)! \equiv -1 \pmod{p} \tag{1.6}$$

*Proof.* Each  $a \in \{1, 2, \dots, p-1\}$  has an inverse  $a' \in \{1, 2, \dots, p-1\}$  modulo  $p$ , that is  $aa' \equiv 1 \pmod{p}$ . This inverse is unique and it follows that  $(a')' = a$ .

If  $a = a'$  then  $1 \equiv aa' = a^2 \pmod{p}$ . We have seen that this necessitates  $a \equiv \pm 1 \pmod{p}$  and so  $a = 1$  or  $a = p-1$ . In the product  $(p-1)! = 1 \times 2 \times 3 \times \dots \times (p-2) \times (p-1)$  we pair off each term, save for 1 and  $p-1$  with its inverse modulo  $p$ . We thus get  $(p-1)! \equiv 1 \times (p-1) \equiv -1 \pmod{p}$ .  $\square$

**Theorem 1.25** (Chinese remainder theorem). Given  $k$  pairwise coprime positive integers  $n_i$  and arbitrary integers  $a_i$ , the system of simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

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

*Proof.* We first prove the case where  $k = 2$ . Let  $n_1 = p, n_2 = q$ .

Let  $p_1 \equiv p^{-1} \pmod{q}$  and  $q_1 \equiv q^{-1} \pmod{p}$ . These must exist since  $p$  and  $q$  are coprime.

We claim that if  $y$  is an integer such that

$$y \equiv aqq_1 + bpp_1 \pmod{pq}$$

then  $y$  satisfies

$$\begin{aligned} y &\equiv aqq_1 \pmod{p} \\ y &\equiv a \pmod{p} \end{aligned}$$

Similarly,

$$\begin{aligned} y &\equiv bpp_1 \pmod{q} \\ y &\equiv b \pmod{q} \end{aligned}$$

Since  $y \equiv a \pmod{p}$  and  $y \equiv b \pmod{q}$ , then  $y$  is a solution for  $x$ . QED.

To prove the general case, we define

$$b_i = \frac{N}{n_i}$$

where  $N = n_1 \cdots n_k$  and

$$b_i' \equiv b_i^{-1} \pmod{n_i}$$

By a similar argument as before,  $x = \sum_{i=1}^n a_i b_i b_i' \pmod{N}$  is a unique solution. □

### Exercise 12

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  $14 + 45y \equiv 3 \pmod{11}$ , which reduces to  $y \equiv 0 \pmod{11}$ .

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

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



**Exercise 13**

Solve the following linear system of congruences:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$$

**Solution.**  $N = 2 \times 3 \times 5 \times 7 = 210$ .

□

## §1.6 Orders Modulo A Prime

### §1.6.1 Order

**Definition 1.26.** Let  $p$  be a prime and take  $a \not\equiv 0 \pmod{p}$ . The *order* of  $a \pmod{p}$  is defined to be the smallest positive integer  $m$  such that

$$a^m \equiv 1 \pmod{p}.$$

*Remark.* This order is clearly finite because Fermat's Little Theorem tells us  $a^{p-1} \equiv 1 \pmod{p}$ , id est, the order of  $a$  is at most  $p-1$ .

**Example 1.27.** Here are some examples of each  $a \pmod{11}$  and  $a \pmod{13}$ .

$a$	mod 11	mod 13
1	1	1
2	10	12
3	5	3
4	5	6
5	5	4
6	10	12
7	10	12
8	10	4
9	5	3
10	2	6
11		12
12		2

One observation you might make about this is that it seems that the orders all divide  $p-1$ . Obviously if  $m \mid p-1$ , then  $a^{p-1} \equiv 1 \pmod{p}$  as well. The miracle of orders is that the converse of this statement is true in an even more general fashion.

**Theorem 1.28** (Fundamental theorem of orders). Suppose  $a^N \equiv 1 \pmod{p}$ . Then the order of  $a \pmod{p}$  divides  $N$ .

### §1.6.2 Primitive Roots

## §1.7 Quadratic Residues

**Definition 1.29** (Quadratic residue). Let positive integer  $m > 1$ , integer  $a$  relatively prime to  $m$ . If  $x^2 \equiv a \pmod{m}$  has a solution, then we say that  $a$  is a *quadratic residue* of  $m$ . Otherwise, we say that  $a$  is a quadratic non-residue.

**Proposition 1.30.**

- (i)  $n^2 \equiv 0/1 \pmod{3}$
- (ii)  $n^2 \equiv 0/1 \pmod{4}$
- (iii)  $n^2 \equiv 0/1/4 \pmod{5}$
- (iv)  $n^2 \equiv 0/1/4 \pmod{8}$

**Proposition 1.31.** If  $p$  is an odd prime, the residue classes of  $0^2, 1^2, \dots, (\frac{p-1}{2})^2$  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  $\{0, 1, \dots, \frac{p-1}{2}\}$ . □

We now introduce a convenient notation to indicate if  $a$  is a quadratic residue mod  $p$ .

**Definition 1.32** (Legendre symbol). For any integer  $a$  and odd prime  $p$ , we define the *Legendre symbol* as such:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p \mid a \\ 1 & a \text{ is a non-zero quadratic residue modulo } p \\ -1 & a \text{ is a non-quadratic residue modulo } p \end{cases}$$

**Theorem 1.33** (Euler's criterion). Let  $p$  be an odd prime, and integer  $a$  relatively prime to  $p$ . Then

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

*Proof.* If the congruence  $x^2 \equiv a \pmod{p}$  has a solution, then  $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ , by Fermat's Little Theorem.

If the congruence  $x^2 \equiv a \pmod{p}$  has no solution, then for each  $i$  ( $1 \leq i \leq p-1$ ), there is a unique  $j \neq i$  ( $1 \leq j \leq p-1$ ), such that  $ij \equiv a$ . Therefore, all the integers from 1 to  $p-1$  can be arranged into  $\frac{p-1}{2}$  such pairs. Taking their product,

$$a^{\frac{p-1}{2}} \equiv 1 \cdot 2 \cdots (p-1) \equiv (p-1)! \equiv -1 \pmod{p}$$

by Wilson's Theorem. □

**Proposition 1.34** (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) □

**Proposition 1.35.** For odd prime  $p$ , then there are an equal number of non-zero quadratic residues and non-quadratic residues modulo  $p$ .

**Theorem 1.36** (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  $\frac{p}{2} < m < p$ .

**Theorem 1.37** (Second supplementary law). For odd prime  $p$ ,

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

**Theorem 1.38** (Eisenstein's lemma). For distinct odd primes  $p$  and  $q$ ,

$$\left(\frac{q}{p}\right) = (-1)^\alpha \tag{1.7}$$

where

$$\alpha = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$$

**Theorem 1.39** (Law of quadratic reciprocity). For distinct odd primes  $p$  and  $q$ ,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \tag{1.8}$$

*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  $(\frac{p-1}{2})!$ .  $\square$

Special cases

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
- $\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{6} \\ -1 & p \equiv 5 \pmod{6} \end{cases}$
- $\left(\frac{5}{p}\right) = \begin{cases} 1 & p \equiv 1, 9 \pmod{10} \\ -1 & p \equiv 3, 7 \pmod{10} \end{cases}$

## Exercises

**Problem 1** (SMO Open 2018 Q18).

**Problem 2** (SMO Open 2018 Q21). Determine the largest value of the expression  $2^{k_1} + 2^{k_2} + \dots + 2^{k_{498}}$ , where for each  $i = 1, 2, \dots, 498$ ,  $k_i$  is an integer,  $1 \leq k_i \leq 507$ , and  $k + 1 + k_2 + \dots + k_{498} = 507$ .

**Solution.**

□

**Problem 3** (SMO Open 2017 Q23).

**Problem 4** (SMO Open 2016 Q18).

**Problem 5** (SMO Open 2016 Q19).

**Problem 6** (SMO Open 2013 Q15).

**Problem 7** (SMO Open 2013 Q17).

**Problem 8** (SMO Open 2006 Q18). Find the largest integer  $n$  such that  $n$  is a divisor of  $a^5 - a$  for all integers  $n$ .

**Solution.** Factorising,

$$a^5 - a = a(a - 1)(a + 1)(a^2 + 1).$$

It is clear that  $2 \mid a^5 - a$  and  $3 \mid a^5 - a$ . We can show that  $5 \mid a^5 - a$  by considering the five cases of  $a \equiv i \pmod{5}$ ,  $i = 0, 1, 2, 3, 4$ . Thus  $30 \mid a^5 - a$ . When  $a = 2$ , we have  $a^5 - a = 30$ . Thus the maximum  $n$  is 30. □

**Problem 9** (SMO Open 2005 Q1). Find the last three digits of  $9^{100} - 1$ .

**Solution.**

$$9^{100} - 1 = (1 - 10)^{100} - 1 = 1 - \binom{100}{1}10^1 + \dots + \binom{100}{100}10^{100} - 1 = 1000k$$

for some integer  $k$ . Thus the last three digits are 000.  $\square$

**Problem 10** (IMO 2023 P1). Determine all composite integers  $n > 1$  that satisfy the following property: if  $d_1, d_2, \dots, d_k$  are all the positive divisors of  $n$  with  $1 = d_1 < d_2 < \dots < d_k = n$ , then  $d_i$  divides  $d_{i+1} + d_{i+2}$  for every  $1 \leq i \leq k - 2$ .

**Solution.** If  $n$  has at least 2 prime divisors, WLOG let  $p < q$  be the smallest two of these primes. Then the ordered tuple of divisors is of the form  $(1, p, p^2, \dots, p^a, q, \dots, n)$  for some integer  $a \geq 1$ .

To prove this claim, note that  $p$  is the smallest prime that divides  $n$ , so it is the smallest divisor not equal to 1, meaning the first 2 divisors are 1 and  $p$ . Furthermore, the smallest divisor of  $n$  that is not equal to a power of  $p$  (i.e. not equal to  $(1, p, p^2, \dots)$ ) is equal to  $q$ . This is because all other divisors either include a prime  $z$  different from both  $q$  and  $p$ , which is larger than  $q$  (since  $q$  and  $p$  are the smallest two prime divisors of  $n$ ), or don't include a different prime  $z$ . In the first case, since  $z > q$ , the divisor is larger than  $q$ . In the second case, all divisors divisible by  $q^2$  are also larger than  $q$ , and otherwise are of the form  $p^x \cdot q^1$  or  $p^x$  for some non-negative integer  $x$ . If the divisor is of the form  $p^x$ , then it is a power of  $p$ . If it is of the form  $p^x \cdot q^1$ , the smallest of these factors is  $p^0 \cdot q^1 = q$ . Therefore, (in the case where 2 or more primes divide  $n$ ) the ordered tuple of divisors is of the form  $(1, p, p^2, \dots, p^a, q, \dots, n)$  for some integer  $a \geq 1$ , since after each divisor  $p^x$ , the next smallest divisor is either  $p^{x+1}$  or simply  $q$ .

If  $a \geq 2$ , the condition fails. This is because  $p^{a-1} \nmid p^a + q$ , since  $p^a$  is divisible by  $p^{a-1}$ , but  $q$  is not since it is a prime different from  $p$ . If  $a = 1$ , then  $p^{a-1} = p^0 = 1$ , which does divide  $q$ . Therefore  $a$  must equal 1 for the condition to be satisfied in this case. However, we know that the ordered list of divisors satisfies  $d_i \cdot d_{k+1-i} = n$ , meaning since the first 3 divisors are  $(1, p, q)$ , then the last 3 divisors are  $(\frac{n}{q}, \frac{n}{p}, n)$ , so  $(\frac{n}{q})$  must divide  $(\frac{n}{p} + n)$ . The fraction  $\frac{(\frac{n}{p} + n)}{(\frac{n}{q})} = \frac{(\frac{1}{p} + 1)}{(\frac{1}{q})} = (\frac{q}{p}) + q$  which is clearly not an integer since  $q$  is an integer, but  $\frac{q}{p}$  is not an integer, so  $(\frac{q}{p}) + q$  is not an integer. Therefore the condition fails specifically for the final 3 divisors in the list in this case, meaning  $n$  can never have 2 or more prime divisors.

When  $n = p^x$ , it is easy to verify this works for all primes  $p$  and all  $x \geq 2$ , since  $p^y \mid (p^{y+1} + p^{y+2})$ , and the divisors are ordered as  $1, p, p^2, \dots, p^x$ .  $\square$

**Problem 11** (Australia 2020 Q2). Amy and Ben play the following game. Initially, there are three piles, each containing 2020 stones. The players take turns to make a move, with Amy going first. Each move consists of choosing one of the piles available, removing the unchosen pile(s) from the game, and then dividing the chosen pile into 2 or 3 non-empty piles. A player loses the game if they are unable to make a move.

Prove that Ben can always win the game, no matter how Amy plays.

**Solution.** Call a pile *perilous* if the number of stones in it is one more than a multiple of three, and *safe* otherwise. Ben has a winning strategy by ensuring that he only leaves Amy perilous piles. Ben wins because the number of stones is strictly decreasing, and eventually Amy will be left with two or three piles each with just one stone.

To see that this is a winning strategy, we prove that Ben can always leave Amy with only perilous piles, and that under such circumstances, Amy must always leave Ben with at least one safe pile.

On Amy's turn, whenever all piles are perilous it is impossible to choose one such perilous pile and divide it into two or three perilous piles by virtue of the fact that  $1 + 1 \not\equiv 1 \pmod{3}$  and  $1 + 1 + 1 \not\equiv 1 \pmod{3}$ . Thus Amy must leave Ben with at least one safe pile.

On Ben's turn, whenever one of the piles is safe, he can divide it into two or three piles, each of which are safe, by virtue of the fact that  $2 \equiv 1 + 1 \pmod{3}$  and  $0 \equiv 1 + 1 + 1 \pmod{3}$ .  $\square$

**Problem 12** (Canada 1969 P7). Show that there are no integers  $a, b, c$  for which

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

**Solution.** 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.  $\square$

**Problem 13** (Italy 2011). Given that  $p$  is a prime number, find integer solutions to

$$n^3 = p^2 - p - 1.$$

**Solution.** It is easy to see that  $n < p$ .

$$\begin{aligned} p^2 - p &= n^3 + 1 \\ p(p-1) &= (n+1)(n^2 - n + 1) \end{aligned}$$

Since  $p$  is prime,  $p \mid n+1$  or  $p \mid n^2 - n + 1$ .

**Case 1:**  $p \mid n+1$

Since  $n < p$ , thus  $n+1 \leq p$ . Hence,  $n+1 = p$ . Substituting this into the original equation gives us

$$\begin{aligned} n^3 &= n^2 + n - 1 \\ (n-1)^2(n+1) &= 0 \\ n &= 1 \end{aligned}$$

$\therefore (n, p) = (1, 2)$ .

**Case 2:**  $p \mid n^2 - n + 1$

Let  $n^2 - n + 1 = kp$  where  $k$  is a positive integer. Then

$$\begin{aligned} p(p-1) &= (n+1)(n^2 - n + 1) \\ &= kp(n+1) \\ p-1 &= k(n+1) \\ p &= kn + k + 1 \\ n^2 - n + 1 &= k(kn + k + 1) \\ n^2 - n(1+k^2) - (k^2 + k - 1) &= 0 \end{aligned}$$

Taking discriminant,

$$\Delta = (1+k^2)^2 + 4(k^2 + k - 1) = k^4 + 6k^2 + 4k - 3$$

which is a perfect square.

Let  $f(k) = k^4 + 6k^2 + 4k - 3$ .

We find that  $k = 3$  via trial and error, then  $n = 11$ ,  $p = 37$ .

For  $k \geq 4$ , we can prove that  $f(k)$  is not a perfect square; in fact,  $f(k)$  lies between two consecutive perfect squares, as shown below:

$$(k^2 + 3)^2 < f(k) < (k^2 + 4)^2$$

which can be easily shown by expanding the terms.

$\therefore (n, p) = (11, 37)$   $\square$

**Problem 14** (USAMO 2003). Prove that for every positive integer  $n$  there exists an  $n$ -digit number divisible by  $5^n$  all of whose digits are odd.

**Solution.** This is immediate by induction on  $n$ . For  $n = 1$  we take 5; moving forward if  $M$  is a working  $n$ -digit number then exactly one of

$$\begin{aligned} N_1 &= 10^n + M \\ N_3 &= 3 \cdot 10^n + M \\ N_5 &= 5 \cdot 10^n + M \\ N_7 &= 7 \cdot 10^n + M \\ N_9 &= 9 \cdot 10^n + M \end{aligned}$$

is divisible by  $5^{n+1}$ ; as they are all divisible by  $5^n$  and  $\frac{N_k}{5^n}$  are all distinct.  $\square$

**Problem 15** (Albania 2009). Find all the natural numbers  $m, n$  such that  $1 + 5 \cdot 2^m = n^2$ .

**Solution.** We have  $5 \cdot 2^m = (n-1)(n+1) \implies n-1 = 2^k$  or  $n+1 = 2^k$

**Case 1:**  $n-1 = 2^k$

This implies  $n+1 = 2^k + 2$

But  $5 \mid 2^k + 2$ ,  $2^k + 2 = 2^t \cdot 5 \implies t = 1, k = 3 \implies n = 9, m = 4$

**Case 2:**  $n+1 = 2^k$

This implies  $n-1 = 2^k - 2$ . But  $5 \mid 2^k - 2$ ,  $2^k - 2 = 2^t \cdot 5 \implies t = 1, 2^k = 12$  which has no integer solution for  $k$ .

$\therefore (m, n) = (4, 9)$  is a unique solution. □

**Problem 16** (NJC H3M 2019 Prelim Q4). Let  $p$  be a prime number. Show that

$$\binom{2p}{p} \equiv 2 \pmod{p}$$

**Solution.** We first express  $\binom{2p}{p}$  as

$$\binom{2p}{p} = \frac{(2p)!}{p!p!} = \frac{(2p)(2p-1)(2p-2)\cdots(p+1)}{(p)(p-1)(p-2)\cdots 1}$$

Note that  $2p$  and  $p$  will cancel each other out to give 2. We hence need to prove the remaining thing is congruent to 1 (mod  $p$ ).

$$\frac{(2p-1)(2p-2)\cdots(p+1)}{(p-1)(p-2)\cdots 1} = \binom{2p-1}{p-1}$$

which is an integer, so

$$(p-1)! \mid (2p-1)(2p-2)\cdots(p+1).$$

We can hence write

$$(2p-1)(2p-2)\cdots(p+1) = k(p-1)! \quad k \in \mathbf{Z}^+$$

Note that since  $p$  is prime,

$$(p+1)(p+2)\cdots(2p-1) \equiv (1)(2)\cdots(p-1) = (p-1)! \pmod{p}$$

Hence,

$$p \mid (2p-1)(2p-2)\cdots(p+1) - (p-1)! \implies p \mid k(p-1)! - (p-1)! = (k-1)(p-1)!$$

Since  $p$  is prime,  $\gcd(p, (p-1)!) = 1$  which implies  $p \mid k-1$  or  $k \equiv 1 \pmod{p}$ .

The rest follows easily. □

**Problem 17** (IMO 1988 P6). Let  $a$  and  $b$  be positive integers such that  $ab+1$  divides  $a^2+b^2$ . Show that  $\frac{a^2+b^2}{ab+1}$  is the square of an integer.

**Solution.** We proceed by way of contradiction, using a method known as **Vieta Jumping**.

WLOG, let  $a \geq b$  and fix  $c$  to be the nonsquare positive integer such that  $\frac{a^2+b^2}{ab+1} = c$ , or  $a^2+b^2 = c(ab+1)$ . Choose a pair  $(a, b)$  out of all valid pairs such that  $a+b$  is minimized. Expanding and rearranging,

$$P(a) = a^2 + a(-bc) + b^2 - c = 0.$$

This quadratic has two roots,  $r_1$  and  $r_2$ , such that

$$(a-r_1)(a-r_2) = P(a) = 0.$$

WLOG, let  $r_1 = a$ . By Vieta's, **(1)**  $r_2 = bc - a$ , and **(2)**  $r_2 = \frac{b^2-c}{a}$ . From **(1)**,  $r_2$  is an integer, because both  $b$  and  $c$  are integers.

From **(2)**,  $r_2$  is nonzero since  $c$  is not square, from our assumption.



We can plug in  $r_2$  for  $a$  in the original expression, because  $P(r_2) = P(a) = 0$ , yielding  $c = \frac{r_2^2 + b^2}{r_2b + 1}$ . If  $c > 0$ , then  $r_2b + 1 > 0$ , and  $r_2b + 1 \neq 0$ , and because  $b > 0$ ,  $r_2$  is a positive integer.

We construct the following inequalities:  $r_2 = \frac{b^2 - c}{a} < a$ , since  $c$  is positive. Adding  $b$ ,  $r_2 + b < a + b$ , contradicting the minimality of  $a + b$ .  $\square$

**Problem 18** (ARML 2019 P7). Compute the least positive integer  $n$  such that the sum of the digits of  $n$  is five times the sum of the digits of  $n + 2019$ .

**Solution.** Let  $S(n)$  denote the sum of the digits of  $n$ , so that solving the problem is equivalent to solving  $S(n) = 5S(n + 2019)$ .

Using the fact that  $S(n) \equiv n \pmod{9}$  for all  $n$ , it follows that

$$\begin{aligned} n &\equiv 5(n + 2019) \equiv 5(n + 3) \pmod{9} \\ 4n &\equiv -15 \pmod{9} \\ n &\equiv 3 \pmod{9}. \end{aligned}$$

Then  $S(n + 2019) \equiv 6 \pmod{9}$ . In particular,  $S(n + 2019) \geq 6$  and  $S(n) \geq 5 \cdot 6 = 30$ . The latter inequality implies  $n \geq 3999$ , which then gives  $n + 2019 \geq 6018$ . Thus if  $n + 2019$  were a four-digit number, then  $S(n + 2019) \geq 7$ . Moreover,  $S(n + 2019)$  can only be 7, because otherwise,  $S(n) = 5S(n + 2019) \geq 40$ , which is impossible (if  $n$  has four digits, then  $S(n)$  can be no greater than 36). So if  $n + 2019$  were a four-digit number, then  $S(n + 2019) = 7$  and  $S(n) = 35$ . But this would imply that the digits of  $n$  are 8, 9, 9, 9 in some order, contradicting the assumption that  $n + 2019$  is a four-digit number. On the other hand, if  $n + 2019$  were a five-digit number such that  $S(n + 2019) \geq 6$ , then the least such value of  $n + 2019$  is 10005, and indeed, this works because it corresponds to  $\boxed{n = 7986}$ , the least possible value of  $n$ .  $\square$

**Problem 19.** Let  $a, b$  be integers, not both 0. Prove that  $\gcd(a + b, a - b) \leq \gcd(2a, 2b)$ .

*Proof.* Direct proof.

Let  $e = \gcd(a + b, a - b)$ . Then  $e \mid (a + b)$  and  $e \mid (a - b)$ . So

$$e \mid (a + b) + (a - b) \implies e \mid 2a$$

and

$$e \mid (a + b) - (a - b) \implies e \mid 2b$$

This implies  $e$  is a common divisor of  $2a$  and  $2b$ . So  $e \leq \gcd(2a, 2b)$ .  $\square$

**Problem 20** (Division Algorithm). Let  $c$  and  $d$  be integers, not both 0. If  $q$  and  $r$  are integers such as  $c = dq + r$ , then  $\gcd(c, d) = \gcd(d, r)$ .

*Proof.* Let  $m = \gcd(c, d)$  and  $n = \gcd(d, r)$ . To prove  $m = n$ , we will show  $m \leq n$  and  $n \leq m$ .

(i) Show  $n \leq m$

Since  $n = \gcd(d, r)$ ,  $n \mid d$  and  $n \mid r$ . There exists integers  $x$  and  $y$  such that  $d = nx$  and  $r = ny$ .

From  $c = dq + r$ , we have  $c = (nx)q + ny = n(xq + y)$  thus  $n \mid c$ .  $n$  is a common divisor of  $c$  and  $d$ , so  $n \leq \gcd(c, d)$ . Hence  $n \leq m$ .

(ii) Show  $m \leq n$

This is left as an exercise.  $\square$

**Problem 21** (Euclid's Lemma). Let  $a, b, c$  be any integers. If  $a \mid bc$  and  $\gcd(a, b) = 1$ , then  $a \mid c$ .

*Proof.* Since  $a \mid bc$ ,  $bc = ak$  for some  $k \in \mathbf{Z}$ .

Since  $\gcd(a, b) = 1$ ,

$$\begin{aligned} ax + by &= 1 \quad \text{for some } x, y \in \mathbf{Z} \\ cax + cby &= c \\ acx + akby &= c \\ a(cx + ky) &= c \end{aligned}$$

thus  $a \mid c$ . □

**Problem 22.** Let  $a$  and  $b$  be integers, not both 0. Show that  $\gcd(a, b)$  is the smallest possible positive linear combination of  $a$  and  $b$ . (i.e. There is no positive integer  $c < \gcd(a, b)$  such that  $c = ax + by$  for some integers  $x$  and  $y$ .)

*Proof.* Prove by contradiction.

Suppose there is a positive integer  $c < \gcd(a, b)$  such that  $c = ax + by$  for some integers  $x$  and  $y$ .

Let  $d = \gcd(a, b)$ . Then  $d \mid a$  and  $d \mid b$ , and hence  $d \mid ax + by$ . This means  $d \mid c$ .

Since  $c$  is positive, this implies  $\gcd(a, b) = d \leq c$ . This contradicts  $c < \gcd(a, b)$ .

Hence we conclude that there is no positive integer  $c < \gcd(a, b)$  such that  $c = ax + by$  for some integers  $x$  and  $y$ . □

# 2 Diophantine Equations

**Definition 2.1.** A *Diophantine equation* is a polynomial equation with 2 or more integer unknowns.

## §2.1 Linear Diophantine Equations

A *linear Diophantine equation* is an equation with 2 or more integer unknowns and the integer unknowns are each to at most degree of 1. Linear Diophantine equation in two variables takes the form of

$$ax + by = c$$

where  $x, y \in \mathbf{Z}$  and  $a, b, c$  are integer constants.  $x$  and  $y$  are unknown variables.

Such equations can be solved completely, and the first known solution was constructed by Brahmagupta, which makes use of the Euclidean algorithm, as we will see later.

### §2.1.1 Homogeneous Linear Diophantine Equations

A special case of linear Diophantine equations is *homogeneous linear Diophantine equations*, i.e. when  $c = 0$ , which take the form

$$ax + by = 0$$

where  $x, y \in \mathbf{Z}$ . Note that  $(x, y) = (0, 0)$  is a solution, known as the *trivial solution* for this equation.

Homogeneous linear Diophantine equations can be easily solved: If  $d = \gcd(a, b)$ , then the complete family of solutions to the above equation is

$$x = \frac{b}{d}k, \quad y = -\frac{a}{d}k$$

for  $k \in \mathbf{Z}$ .

#### Exercise 14

Solve the homogeneous linear Diophantine equation

$$6x + 9y = 0$$

where  $x, y \in \mathbf{Z}$ .

**Solution.** Note that  $\gcd(6, 9) = 3$ . Hence the solutions are

$$x = \frac{9k}{3} = 3k \quad \text{and} \quad y = -\frac{6k}{3} = -2k$$

with  $k \in \mathbf{Z}$ . □

### §2.1.2 Non-homogeneous Linear Diophantine Equations

We can use the following steps to solve non-homogeneous linear Diophantine equations (of the form  $ax + by = c$ ,  $x, y \in \mathbf{Z}$ ).

1. Determine  $\gcd(a, b)$ .  
Let  $d = \gcd(a, b)$ . For smaller  $a, b$  you can simply determine  $d$  by manually checking factors of  $a$  and  $b$ ; for larger  $a, b$  use the Euclidean algorithm to determine  $d$ .
2. Check that  $d \mid c$ .  
If YES, continue on. If NO, stop as there are no solutions.
3. Find a particular solution to  $ax + by = c$ .  
by first finding  $x_0$  and  $y_0$  such that  $ax + by = d$ . Suppose  $x = cd x_0$  and  $y = cd y_0$ .
4. Use a change of variables.  
Let  $u = x - cd x_0$  and  $v = y - cd y_0$ , then we will see that  $au + bv = 0$  (important to check your results).
5. Solve  $au + bv = 0$ .  
That is:  $u = -\frac{b}{d}m$  and  $v = \frac{a}{d}m$ ,  $m \in \mathbf{Z}$ .
6. Substitute for  $u$  and  $v$ .  
Thus the general solutions are  $x - cd x_0 = -bdm$  and  $y - cd y_0 = adm$ , or  $(x, y) = (cd x_0 - bdm, cd y_0 + adm)$ ,  $m \in \mathbf{Z}$ .

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 2.2** (Bezout's lemma). For non-zero integers  $a$  and  $b$ , let  $d = \gcd(a, b)$ . Then there exists integers  $s$  and  $t$  that satisfy

$$sa + tb = d.$$

An important case of Bezout's Lemma is when  $a, b$  are coprime:

$$ax + by = 1, x, y \in \mathbf{Z} \iff a, b \text{ coprime}$$

#### Exercise 15

Find integers  $x$  and  $y$  that satisfy

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

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

$$\begin{aligned} 102 &= 2 \times 38 + 26 \\ 38 &= 1 \times 26 + 12 \\ 26 &= 2 \times 12 + 2 \\ 12 &= 6 \times 2 + 0 \\ 6 &= 3 \times 2 + 0 \end{aligned}$$

Work backwards and substitute the numbers from above:

$$\begin{aligned} 2 &= 26 - 2 \times 12 \\ &= 3 \times 26 - 2 \times 38 \\ &= 3 \times 102 - 8 \times 38 \end{aligned}$$

Hence  $x = 3$ ,  $y = -8$ . □

All solutions of linear Diophantine equations:

**Theorem 2.3.** If  $(x_0, y_0)$  is a solution of  $ax + by = n$ , then all solutions are given by

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

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

### §2.1.3 Chicken McNugget Theorem

**Theorem 2.4** (Chicken McNugget theorem). For coprime  $m$  and  $n$ , the largest impossible sum of  $m$  and  $n$  (i.e. largest number not expressible in the form  $mx + ny$  for non-negative integer  $x$  and  $y$ ) is  $mn - m - n$ .

*Proof.* Because the equation is symmetric, WLOG assume that  $n \geq m$ .

Assume that  $mn - m - n = mx + ny$ . Taking  $\pmod{m}$ , we arrive at

$$ny \equiv -n \pmod{m} \implies y \equiv -1 \pmod{m}$$

This implies that  $y \geq m - 1$ , however, this gives

$$mx + ny \geq mx + mn - m > mn - m - n$$

which is a contradiction. Now, we prove that

$$mn - m - n + k = mx + ny, \quad k \in \{1, 2, 3, \dots, m\}.$$

The reason for this is that for  $k = k_1 > m$ , then we can repeatedly add  $m$  to the reduced value of  $k_1 \pmod{m}$  until we reach  $k_1$ . Our goal is to prove that for every  $k$ , there exists an  $x$  such that

- $x$  is an integer.
- $x$  is a non-negative integer.

Taking the equation  $\pmod{m}$  brings us to

$$n(y + 1) \equiv k \pmod{m} \implies y \equiv kn^{-1} - 1 \pmod{m}$$

Using this value of  $y$  produces the first desired outcome. For the second, we must have  $mn - m - n + k - ny \geq 0$ . For  $y = m - y_0$  and  $m \geq y_0 \geq 2$ , we get

$$mn - m - n + k - ny = (y_0 - 1)n - m + k > 0.$$

For  $y_0 = 1$ , we have

$$y \equiv -1 \pmod{m} \implies kn^{-1} - 1 \equiv -1 \pmod{m} \implies k \equiv 0 \pmod{m}$$

Therefore,  $k = m$ , and we get

$$mn - m - n + k - ny = mn - m - n + m - n(m - 1) = 0 \implies x = 0$$

Therefore, we have proven our desired statement, and we are done.  $\square$

## §2.2 Pythagorean Triples

**Definition 2.5** (Pythagorean triple). A *Pythagorean triple* is a triplet  $(a, b, c)$ , 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

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

### Exercise 16

Prove that there is one and only one Pythagorean triple  $(a, b, c)$  such that  $a, b, c$  are consecutive integers.

**Solution.** We need to prove two parts: existence (“one”) and uniqueness (“only one”).

**Existence:**

Take  $(a, b, c) = (3, 4, 5)$ , which indeed satisfies  $a^2 + b^2 = c^2$ .

**Uniqueness:**

Suppose  $a, b, c$  are consecutive. Then  $b = a + 1$  and  $c = a + 2$ . By Pythagoras’ theorem we have

$$a^2 + (a + 1)^2 = (a + 2)^2$$

which simplifies down to  $(a - 3)(a + 1) = 0$ , so  $a = 3$  or  $a = -1$ . Since Pythagorean triple consists of positive integers,  $a$  can only be 3.  $\square$

### Exercise 17

Prove that there are infinitely many Pythagorean triples.

**Solution.** This is an existential statement. We prove this by construction.

Suppose  $(a, b, c)$  is a Pythagorean triple (Pythagorean triples exist, one example being  $(a, b, c) = (3, 4, 5)$  as shown earlier). Then  $a^2 + b^2 = c^2$ .

Let  $k$  be any positive integer. Note that

$$(ka)^2 + (kb)^2 = k^2a^2 + k^2b^2 = k^2(a^2 + b^2) = k^2c^2 = (kc)^2.$$

Thus  $(ka, kb, kc)$  is also a Pythagorean triple.

Since there are infinitely many  $k$ , we have infinitely many Pythagorean triples  $(ka, kb, kc)$ .  $\square$

## §2.3 Pell’s Equation

**Theorem 2.6** (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  $n = 2, 3, \dots$ . The coefficients of the integer and square root give us the values of  $x$  and  $y$  respectively.

**Exercise 18**

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  $n = 2$ ,

$$\begin{aligned}\alpha^2 &= (3 + 2\sqrt{2})^2 \\ &= 17 + 12\sqrt{2}\end{aligned}$$

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

Simply repeat the above method to find further solutions. □

**Theorem 2.7** (Fermat's last theorem). For  $n > 2$ , there are no non-zero solutions to

$$a^n + b^n = c^n.$$

*Proof.* Refer to Andrew Wiles's proof. □

# Part II

# Algebra



# 3 Basic Algebra

## §3.1 Algebraic Manipulation

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

Some common **factorisation** techniques include

- 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:

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) \quad \forall n \in \mathbf{N}$$

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

- Generalised expansion of square:

$$(a_1 + a_2 + \dots + a_n)^2 = (a_1^2 + a_2^2 + \dots + a_n^2) + (2a_1a_2 + \dots + 2a_1a_n) + (2a_2a_3 + \dots + 2a_2a_n) + \dots + 2a_{n-1}a_n$$

or, written succinctly,

$$\left( \sum_{i=1}^n a_i \right)^2 = \sum_{i=1}^n a_i^2 + 2 \sum_{i < j} a_i a_j$$

- Useful ones:

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

### Exercise 19

Evaluate the expression

$$(2 + 1)(2^2 + 1)(2^4 + 1) \dots (2^{2^{10}} + 1) + 1.$$

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

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

Note the trick here: to multiply the expression by  $(2 - 1)$

□

**Exercise 20**

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,

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

□

Sometimes it is useful to look out for terms or expressions that are always positive or negative.

**Exercise 21 (Vietnam 1962)**

Prove that

$$\frac{1}{\frac{1}{a} + \frac{1}{b}} + \frac{1}{\frac{1}{c} + \frac{1}{d}} \leq \frac{1}{\frac{1}{a+c} + \frac{1}{b+d}},$$

for all positive real numbers  $a, b, c, d$ .

**Solution.** We prove that

$$\frac{1}{\frac{1}{a+c} + \frac{1}{b+d}} - \left( \frac{1}{\frac{1}{a} + \frac{1}{b}} + \frac{1}{\frac{1}{c} + \frac{1}{d}} \right) \geq 0.$$

A straightforward summing up and simplification show that this is equivalent to

$$\frac{a^2d^2 - 2abcd + b^2c^2}{(a+b+c+d)(a+b)(c+d)} \geq 0,$$

which is always true, as the denominator is positive, and the numerator is  $(ad - bc)^2 \geq 0$ .

The equality occurs if and only if  $ad = bc$ .

□

Since  $(a - b)^2 \geq 0$ , we have  $a^2 + b^2 \geq 2ab$ . Adding  $a^2 + b^2$  to both sides gives us

$$2(a^2 + b^2) \geq (a + b)^2 \quad (3.1)$$

Expanding this to three and four variables,

$$3(a + b + c)^2 \geq (a + b + c)^2 \quad (3.2)$$

and

$$4(a^2 + b^2 + c^2 + d^2) \geq (a + b + c + d)^2 \quad (3.3)$$

*Remark.* This can be easily seen by applying Titu's Lemma.

The above equations are useful in finding the minimum value of  $a^2 + b^2$  given  $a + b$ , or finding the maximum value of  $a + b$  given  $a^2 + b^2$ .

## §3.2 Polynomials

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

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

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

### §3.2.1 Finding Roots of Polynomials

Suppose we are given the polynomial  $f(x)$  and asked to find the solutions to  $f(x) = 0$ . We call these solutions **roots** of the polynomials.

**Theorem 3.1** (Quadratic formula). For  $a, b, c \in \mathbf{R}$ ,  $a \neq 0$ , the quadratic equation  $ax^2 + bx + c = 0$  has solutions

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad (3.4)$$

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

Let  $\Delta$  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.

Unfortunately, no quick and easy method like the quadratic formula exists to solve general polynomials. We do have some helpful hints to do.

**Theorem 3.2** (Division algorithm). If  $f(x)$  and  $D(x)$  are polynomials where  $Q(x) \neq 0$  and  $\deg D(x) < \deg f(x)$ , then

$$f(x) = D(x)Q(x) + R(x).$$

**Theorem 3.3** (Remainder theorem). If the polynomial  $f(x)$  is divided by  $x - c$ , then the remainder is  $f(c)$ .

**Theorem 3.4** (Factor theorem). Let  $f(x)$  be a polynomial.  $f(c) = 0$  if and only if  $x - c$  is a factor of  $f(x)$ .

We can generalise the above:

**Theorem 3.5** (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

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

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

#### Exercise 22 (MA0 1990)

$P(x)$  is a polynomial with real coefficients. When  $P(x)$  is divided by  $x - 1$ , the remainder is 3. When  $P(x)$  is divided by  $x - 2$ , the remainder is 5. Find the remainder when  $P(x)$  is divided by  $x^2 - 3x + 2$ .

**Solution.** We write

$$P(x) = (x^2 - 3x + 2)q(x) + r(x),$$

where  $r(x)$  is the desired remainder.

Since  $\deg r(x) < \deg(x^2 - 3x + 2)$ , we can write  $r(x) = ax + b$  for some constants  $a$  and  $b$ . From the given information, we know  $P(1) = 3$  and  $P(2) = 5$ . Since  $x^2 - 3x + 2 = 0$  for  $x = 2$  and  $x = 1$ , we put these values in our equation for  $P(x)$ , yielding

$$\begin{aligned} 0 \cdot q(1) + r(1) &= a + b = P(1) = 3 \\ 0 \cdot q(2) + r(2) &= 2a + b = P(2) = 5. \end{aligned}$$

Solving this system, we find  $(a, b) = (2, 1)$ , so the remainder is  $2x + 1$ .  $\square$

**Theorem 3.6** (Fundamental theorem of algebra). A polynomial of degree  $n > 0$ , with real or complex coefficients, has  $n$  complex roots (some may be repeated).

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.

For the *rational* roots of a polynomial, there is a method we can use to narrow the search.

**Theorem 3.7** (Rational root theorem). For any polynomial  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$  with integer coefficients, all rational roots are of the form  $\frac{p}{q}$ , where  $p \mid a_0$  and  $q \mid a_n$ .

*Proof.* Let  $\frac{p}{q}$  be a rational roots of the polynomial  $f(x)$ , where  $p$  and  $q$  are relatively prime positive integers. Since  $\frac{p}{q}$  is a root, we have

$$f\left(\frac{p}{q}\right) = a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \cdots + a_0 = 0.$$

Multiplying by  $q^n$  gives

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n = 0.$$

Now look at this equation modulo  $p$ . The first  $n$  terms on the left will become 0 since they are multiples of  $p$ , so we have

$$a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n \equiv a_0 q^n \pmod{p} \equiv 0 \pmod{p}$$

Thus  $a_0 q^n \equiv 0 \pmod{p}$ , so  $p \mid a_0 q^n$ . Since  $p$  and  $q$  are relatively prime, it follows that  $p \mid a_0$ .

By the same argument, we can evaluate the sum mod  $q$  to show that  $q \mid a_n p^n$ . Thus  $q \mid a_n$  and our proof is complete.  $\square$

There are a few more guides to tell us where to look for roots. The first is Descartes' Rule of Signs.

**Theorem 3.8** (Descartes' rule of signs). To count how many positive and negative roots there are, we count sign changes.

The number of sign changes in the coefficients of  $f(x)$  (meaning we list the coefficients from first to last and count how many times they change from positive to negative) tells us the maximum number of positive roots the polynomial has, and the number of sign changes in the coefficients of  $f(-x)$  gives us the maximum number of negative roots the polynomial has.

**Example 3.9.** For

$$f(x) = 3x^5 + 2x^4 - 3x^2 + 2x - 1,$$

there are at most 3 positive roots and at most 2 negative roots (since  $f(x) = -3x^5 + 2x^4 - 3x^2 - 2x - 1$ ).

**Theorem 3.10** (Lagrange interpolation formula). The polynomial  $Q$  that solves  $Q(a_0) = 1, Q(a_1) = 0, Q(a_2) = 0, \dots, Q(a_n) = 0$  is

$$\frac{(x - a_1)(x - a_2) \cdots (x - a_n)}{(a_0 - a_1)(a_0 - a_2) \cdots (a_0 - a_n)}.$$

We can take a linear combination of these types of polynomials to create a polynomial where  $f(a_0) = b_0, f(a_1) = b_1, \dots, f(a_n) = b_n$ .

**Theorem 3.11** (Gauss's lemma). If a polynomial with integer coefficients can be factored with rational coefficients, then it can also be factored with integer coefficients.

### §3.2.2 Coefficients and Roots

The coefficients of a polynomial are directly related to the sum and product of the roots.

**Theorem 3.12** (Vieta's relations). For polynomial  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$  with complex coefficients with roots  $r_1, r_2, \dots, r_n$ ,

$$\begin{aligned} r_1 + r_2 + \cdots + r_n &= -\frac{a_{n-1}}{a_n} \\ r_1 r_2 + r_2 r_3 + \cdots + r_{n-1} r_n &= \frac{a_{n-2}}{a_n} \\ &\vdots \\ r_1 r_2 \cdots r_n &= (-1)^n \frac{a_0}{a_n} \end{aligned} \tag{3.5}$$

### §3.2.3 Combinatorial Nullstellensatz

Let

$$f(x) = cx^d + \cdots$$

be a polynomial with degree  $d$ . For any set  $S$  such that  $|S| > d$ , there will be an element  $a \in S$  such that

$$f(a) \neq 0.$$

More generally, let

$$f(x_1, x_2, \dots, x_k) = cx_1^{d_1} x_2^{d_2} \cdots x_k^{d_k} + \cdots$$

where  $c$  is non-zero be a polynomial with total degree  $d_1 + d_2 + \cdots + d_k$ . Then for any sets  $S_1, \dots, S_k$  such that  $|S_1| > d_1, \dots, |S_k| > d_k$ , there exists  $a_1 \in S_1, \dots, a_k \in S_k$  such that

$$f(a_1, \dots, a_k) \neq 0.$$

### §3.2.4 Transforming Polynomials

AOPS Volume 2 pg62

### §3.2.5 Newton's Sums

Newton sums give us a clever and efficient way of finding the sums of roots of a polynomial raised to a power.

Consider a polynomial  $f(x)$  of degree  $n$ ,

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

Let  $f(x) = 0$  have roots  $x_1, x_2, \dots, x_n$ . Let  $S_k$  be the sum of the  $k$ -th powers of the roots of  $f(x)$ ; that is,

$$S_k = x_1^k + x_2^k + \cdots + x_n^k.$$

**Newton's sums** tell us that

$$\begin{aligned} a_n S_1 + a_{n-1} &= 0 \\ a_n S_2 + a_{n-1} S_1 + 2a_{n-2} &= 0 \\ a_n S_3 + a_{n-1} S_2 + a_{n-2} S_1 + 3a_{n-3} &= 0 \\ &\vdots \\ a_n S_k + a_{n-1} S_{k-1} + \cdots + a_{n-k+1} S_1 + k \cdot a_{n-k} &= 0 \end{aligned}$$

(Define  $a_j = 0$  for  $j < 0$ .)

### §3.3 Absolute Value Equations

Common problem-solving techniques:

- Squaring both sides
- Casework: solve each case for  $x$
- Sketching graph

#### Exercise 23

Find all real values of  $x$  such that

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

**Solution.** The three turning points are at  $x = -2$ ,  $x = -3$  and  $x = 1$ . Hence we just need to check the following cases:

- $x \leq -3$
- $-3 < x \leq -2$
- $-2 < x \leq 1$
- $x > 1$

Solving all the cases gives us  $x = -\frac{5}{2}, x = \frac{7}{6}$

□

#### Exercise 24

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  $\frac{3 \pm \sqrt{5}}{2}$  which are both positive. The second case has solutions  $\frac{3 \pm \sqrt{13}}{2}$  and only one of these is negative. So there are  $\boxed{3}$  solutions in total. □

### §3.4 Logarithms

Properties of logarithms

1.  $\log_a b^n = n \log_a b$
2.  $\log_a b + \log_a c = \log_a bc$
3.  $\log_a b - \log_a c = \log_a \frac{b}{c}$
4.  $\frac{\log_a b}{\log_a c} = \log_c b$
5.  $\log_{a^n} b^n = \log_a b$

One useful identity is the chain rule for logarithms:

$$(\log_a b)(\log_b c) = \log_c a$$

which can be easily proven by changing of base.

#### Exercise 25

Find the sum

$$\log \frac{1}{2} + \log \frac{2}{3} + \log \frac{3}{4} + \cdots + \frac{99}{100}.$$

**Solution.** Using the sum of logarithms,

$$S = \log \left( \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdots \frac{99}{100} \right) = \log \frac{1}{100} = \log 10^{-2} = \boxed{-2}$$

□

Another useful property is

$$x^{\log_x y} = y$$

## Exercises

**Problem 23.** Solve the equation

$$x^5 + (x+1)^5 + (x+2)^5 + \cdots + (x+1998)^5 = 0.$$

**Solution.** Let  $u = x + 999$  to get  $(u-999)^5 + (u-998)^5 + \cdots + (u+998)^5 + (u+999)^5$ . Note that when  $(u-a)^5 + (u+a)^5 = 10a^4u + 20a^2u^3 + 2u^5$  for all  $a$ , but when  $u = 0$  this expression is always equal to 0. We can apply this for all  $a = 0$  to  $a = 999$  to make all the terms 0, thus  $u = 0$  and  $x = -999$ .  $\square$

**Problem 24.** 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 25** (SMO 2014 (Junior) Q16). If  $m$  and  $n$  are positive real numbers satisfying the equation  $m + 4\sqrt{mn} - 2\sqrt{m} - 4\sqrt{n} + 4n = 3$ , find the value of  $\frac{\sqrt{m} + 2\sqrt{n} + 2014}{4 - \sqrt{m} - 2\sqrt{n}}$ .

**Solution.** Grouping the expression as  $m + 4\sqrt{mn} + 4n - 2(\sqrt{m} + 2\sqrt{n}) - 3 = 0$  becomes

$$(\sqrt{m} + 2\sqrt{n})^2 - 2(\sqrt{m} + 2\sqrt{n}) - 3 = 0$$

which is factorised as  $(\sqrt{m} + 2\sqrt{n} - 3)(\sqrt{m} + 2\sqrt{n} + 1) = 0$  which gives  $\sqrt{m} + 2\sqrt{n} = 3$  or  $-1$  (rejected). Hence  $\sqrt{m} + 2\sqrt{n} = 3$ .

Substituting this into the given expression gives  $\boxed{2017}$ .

□

**Problem 26** (SMO Open 2005 Q19). Let  $x$  and  $y$  be positive integers such that

$$\frac{100}{151} < \frac{y}{x} < \frac{200}{251}.$$

What is the minimum value of  $x$ ?

**Solution.** The inequality can be transformed to

$$\frac{302}{200}y > x > \frac{251}{200}y.$$

The minimum  $y$  such that  $\left(\frac{251}{200}y, \frac{302}{200}y\right)$  contains an integer is  $y = 2$  and when  $y = 2$ , the only integer it contains is 3. Hence the answer is 3.  $\square$

**Problem 27** (SMO Open 2006 Q2). Given that  $p$  and  $q$  are integers that satisfy the equation

$$36x^2 - 4(p^2 + 11)x + 135(p + q) + 576 = 0,$$

find the value of  $p + q$ .

**Solution.** By Vieta's, we have

$$p + q = \frac{p^2 + 11}{9} \quad \text{and} \quad pq = \frac{135(p + q) + 576}{36}.$$

Solving simultaneously gives  $p = 13$  and  $p + q = 20$ . □

**Problem 28** (Australia 2020 Q1). Determine all pairs  $(a, b)$  of non-negative integers such that

$$\frac{a+b}{2} - \sqrt{ab} = 1.$$

**Solution.** Reorganising the equation we get

$$2\sqrt{ab} = a + b - 2$$

thus after squaring:

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

Hence

$$0 = a^2 + b^2 + 4 - 2ab - 4a - 4b = (a - b)^2 + 4(1 - a - b),$$

so 4 divides  $(a - b)^2$ . It follows that  $a - b$  is even and hence  $1 - a - b$  is odd. Thus  $a - b = 4k + 2$  for some  $k$ . Then  $(2k + 1)^2 = a + b - 1 = 2b + 4k + 1$ , and so  $b = 2k^2$  and  $a = 2k^2 + 4k + 2 = 2(k + 1)^2$ .  $\square$

**Problem 29.** 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  $\boxed{\sqrt{10}}$ .

□

**Problem 30** (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

$$\begin{aligned} \left( \frac{y-z}{x} + \frac{z-x}{y} + \frac{x-y}{z} \right) \frac{x}{y-z} &= 1 + \frac{x}{y} \cdot \frac{z-x}{y-z} + \frac{x}{z} \cdot \frac{x-y}{y-z} \\ &= 1 + \frac{xz(z-x) + xy(x-y)}{yz(y-z)} \\ &= 1 + \frac{x(z^2 - zx + xy - y^2)}{yz(y-z)} \\ &= 1 + \frac{x}{yz}(x - y - z) \\ &= 1 + \frac{2x^2}{yz} \quad \because y + z = -x \end{aligned}$$

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 31** (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  $\boxed{192}$ . □

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

**Problem 32** (GERMANY). Given that  $m^{15} + m^{16} + m^{17} = 0$ , solve for  $m^{18}$ .

**Solution.** Factorising gives us

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

Either  $m^{15} = 0$  which implies  $m = 0$  so  $m^{18} = 0$ , or  $m^2 + m + 1 = 0$  where multiplying  $m - 1$  on both sides gives  $(m - 1)(m^2 + m + 1) = 0 \implies m^3 - 1 = 0 \implies m^3 = 1$ .

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

□



**Problem 33.** 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,

$$\begin{aligned}\log_a \left(\frac{5}{x}\right)^{\log_a 25} &= \log_a \left(\frac{3}{x}\right)^{\log_a 9} \\ \log_a 25 \times \log_a \left(\frac{5}{x}\right) &= \log_a 9 \times \log_a \left(\frac{3}{x}\right) \\ 2 \log_a 5 \times (\log_a 5 - \log_a x) &= 2 \log_a 3 \times (\log_a 3 - \log_a x)\end{aligned}$$

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,  $p + q = \log_a x \implies \boxed{x = 15}$ . □

**Problem 34.** 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 35** (DOKA). Given that  $f(x) = \frac{x}{x-3}$ ,  $f^8(x) = \frac{x}{ax+b}$ , where  $a$  and  $b$  are integers. Find  $a$  and  $b$ .

**Solution.** Observe that

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

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

$$\begin{aligned} a_n &= (-3)^0 + (-3)^1 + \cdots + (-3)^{n-1} \\ b_n &= (-3)^n \end{aligned}$$

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

□

**Problem 36** (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  $2 + 8 + 9 = \boxed{19}$ .  $\square$

**Problem 37** (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 38** (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,

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

□

**Problem 39** (DOKA). For a positive integer  $n$ , we have the polynomial

$$\left(2 + \frac{x}{2}\right)\left(2 + \frac{2x}{2}\right)\left(2 + \frac{3x}{2}\right)\cdots\left(2 + \frac{nx}{2}\right) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

where  $a_0, \dots, a_n$  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

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

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  $\boxed{n = 100}$ . □

**Problem 40.** Consider the sequence of real numbers  $\{a_n\}$  is defined by  $a_1 = \frac{1}{1000}$  and  $a_{n+1} = \frac{a_n}{na_n - 1}$  for  $n \geq 1$ . Find the value of  $\frac{1}{a_{2020}}$ .

**Solution.**

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

Listing out terms,

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

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

□



**Problem 41** (SMO 2014 (Senior) Q2). Find, with justification, all positive real numbers  $a, b, c$  satisfying the system of equations

$$a\sqrt{b} = a + c, \quad b\sqrt{c} = b + a, \quad c\sqrt{a} = c + b.$$

**Solution.** Adding the three equations, we have

$$a\sqrt{b} + b\sqrt{c} + c\sqrt{a} = 2a + 2b + 2c$$

and factorising yields

$$a(\sqrt{b} - 2) + b(\sqrt{c} - 2) + c(\sqrt{a} - 2) = 0.$$

Thus  $a = b = c = 0$  (rejected) or  $\sqrt{b} - 2 = \sqrt{c} - 2 = \sqrt{a} - 2$  which gives  $\boxed{a = b = c = 4}$ .  $\square$

**Problem 42.** Let  $x, y, z$  be positive real numbers, such that  $x + y + z = 1$  and  $xy + yz + zx = \frac{1}{3}$ . Find the value of

$$\frac{4x}{y+1} + \frac{16y}{z+1} + \frac{64z}{x+1}.$$

**Solution.** Dividing the two equations, we have

$$\frac{x+y+z}{xy+yz+zx} = \frac{1}{\frac{1}{3}}$$

and after cross multiplication

$$3xy + 3yz + 3zx = x + y + z.$$

Upon factorising

$$x(3y - 1) + y(3z - 1) + z(3x - 1) = 0.$$

We arrive at  $x = y = z = \frac{1}{3}$ . Substituting these values into the above expression gives  $\boxed{21}$ .  $\square$

**Problem 43** (SMO Open 2018 Q11). Find the shortest distance from the point  $(22, 21)$  to the graph with equation  $x^3 + 1 = y(3x - y^3)$ .

**Solution.** The equation can be expanded as  $x^3 + 1 - 3xy + y^3 = 0$  which by observation is “symmetric”. Substituting  $x = y$  we have  $x^3 + 1 - 3x^2 + x^3 = 0$  which upon solving gives  $(x, y) = (1, 1)$  or  $\left(-\frac{1}{2}, \frac{1}{2}\right)$ .

Since  $(1, 1)$  is nearer to  $(22, 21)$  than  $\left(-\frac{1}{2}, \frac{1}{2}\right)$ , the shortest distance is

$$\sqrt{(22-1)^2 + (21-1)^2} = \boxed{29}.$$

$\square$

**Problem 44.** 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 3.13.** For  $a + b + c = 0$ ,

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

*Proof.* We prove this by direct expansion.

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

□

**Lemma 3.14.** For  $a + b + c = 0$ ,

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

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

□

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

□

**Problem 45.** Find all the real solution pairs  $(x, y)$  that satisfy the system

$$\frac{1}{\sqrt{x}} + \frac{1}{2\sqrt{y}} = (x + 3y)(3x + y) \quad (1)$$

$$\frac{1}{\sqrt{x}} - \frac{1}{2\sqrt{y}} = 2(y^2 - x^2) \quad (2)$$

**Solution.** Let  $a = \sqrt{x}$  and  $b = \sqrt{y}$ . The two equations become

$$\frac{1}{a} + \frac{1}{2b} = (a^2 + 3b^2)(3a^2 + b^2) \quad (3)$$

$$\frac{1}{a} - \frac{1}{2b} = 2(b^4 - a^4) \quad (4)$$

Adding the two equations above, we obtain

$$\frac{2}{a} = (3a^4 + 10a^2b^2 + 3b^4) + (2b^4 - 2a^4).$$

Thus we get

$$1 = 5a^4b + 10a^2b^3 + b^5. \quad (5)$$

By adding (5) and (6), we obtain  $3 = (a+b)^5$ . Similarly, by subtracting (6) from (5), we obtain  $1 = (a-b)^5$ . It is now easy to deduce that

$$a = \frac{1 + \sqrt[5]{3}}{2} \text{ and } b = \frac{\sqrt[5]{3} - 1}{2}.$$

Consequently, we obtain

$$x = \left( \frac{1 + \sqrt[5]{3}}{2} \right)^2 \text{ and } y = \left( \frac{\sqrt[5]{3} - 1}{2} \right)^2.$$

□

**Problem 46.** Find all pairs of integers  $(x, y)$  such that

$$x^3 + y^3 = (x + y)^2.$$

**Solution.** Since  $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ , all pairs of integers  $(n, -n)$  where  $n \in \mathbf{Z}$  are solutions. Suppose that  $x + y \neq 0$ . Then the equation becomes

$$x^2 - xy + y^2 = x + y,$$

i.e.

$$x^2 - (y + 1)x + y^2 - y = 0.$$

Considering the above as a quadratic equation in  $x$ , we calculate the discriminant

$$\Delta = y^2 + 2y + 1 - 4y^2 + 4y = -3y^2 + 6y + 1.$$

Solving for  $\Delta \geq 0$  yields

$$\frac{3 - 2\sqrt{3}}{3} \leq y \leq \frac{3 + 2\sqrt{3}}{3}.$$

Thus the possible values for  $y$  are 0, 1, and 2, which lead to the solutions  $(1, 0)$ ,  $(0, 1)$ ,  $(1, 2)$ ,  $(2, 1)$ , and  $(2, 2)$ .

Therefore the integer solutions of the equation are  $(x, y) = (1, 0), (0, 1), (1, 2), (2, 1), (2, 2), (n, -n)$  for all  $n \in \mathbf{Z}$ .  $\square$

**Problem 47.** Find all pairs of integers  $(a, b)$  such that the polynomial  $ax^{17} + bx^{16} + 1$  is divisible by  $x^2 - x - 1$ .

**Solution.** Let  $p$  and  $q$  be the roots of  $x^2 - x - 1 = 0$ . By Vieta's theorem,  $p + q = 1$  and  $pq = -1$ . Note that  $p$  and  $q$  must also be the roots of  $ax^{17} + bx^{16} + 1$ . Thus

$$ap^{17} + bp^{16} = -1 \quad \text{and} \quad aq^{17} + bq^{16} = -1.$$

Multiplying the first of these equations by  $q^{16}$  and the second one by  $p^{16}$ , and using the fact that  $pq = -1$ , we find

$$ap + b = -q^{16} \quad \text{and} \quad aq + b = -p^{16}. \quad (1)$$

Thus

$$a = \frac{p^{16} - q^{16}}{p - q} = (p^8 + q^8)(p^4 + q^4)(p^2 + q^2)(p + q).$$

Since

$$\begin{aligned} p + q &= 1, \\ p^2 + q^2 &= (p + q)^2 - 2pq = 1 + 2 = 3, \\ p^4 + q^4 &= (p^2 + q^2)^2 - 2p^2q^2 = 9 - 2 = 7, \\ p^8 + q^8 &= (p^4 + q^4)^2 - 2p^4q^4 = 49 - 2 = 47, \end{aligned}$$

It follows that  $a = 1 \cdot 3 \cdot 7 \cdot 47 = 987$ .

Likewise, eliminating  $a$  in (1) gives

$$\begin{aligned} -b &= \frac{p^{17} - q^{17}}{p - q} \\ &= p^{16} + p^{15}q + p^{14}q^2 + \cdots + q^{16} \\ &= (p^{16} + q^{16}) + pq(p^{14} + q^{14}) + p^2q^2(p^{12} + q^{12}) + \cdots + p^7q^7(p^2 + q^2) + p^8q^8 \\ &= (p^{16} + q^{16}) - (p^{14} + q^{14}) + \cdots - (p^2 + q^2) + 1. \end{aligned}$$

For  $n \geq 1$ , let  $k_{2n} = p^{2n} + q^{2n}$ . Then  $k_2 = 3$  and  $k_4 = 7$ , and

$$\begin{aligned} k_{2n+4} &= p^{2n+4} + q^{2n+4} \\ &= (p^{2n+2} + q^{2n+2})(p^2 + q^2) - p^2q^2(p^{2n} + q^{2n}) \\ &= 3k_{2n+2} - k_{2n} \end{aligned}$$

for  $n \geq 3$ . Then  $k_6 = 18$ ,  $k_8 = 47$ ,  $k_{10} = 123$ ,  $k_{12} = 322$ ,  $k_{14} = 843$ ,  $k_{16} = 2207$ .

Hence

$$-b = 2207 - 843 + 322 - 123 + 47 - 18 + 7 - 3 + 1 = 1597$$

or

$$(a, b) = (987, -1597).$$

□

**Problem 48.** Let  $x, y, z$  be complex numbers such that  $x + y + z = 2$ ,  $x^2 + y^2 + z^2 = 3$ , and  $xyz = 4$ . Evaluate

$$\frac{1}{xy + z - 1} + \frac{1}{yz + x - 1} + \frac{1}{zx + y - 1}.$$

**Solution.** Let  $S$  be the desired value. Note that

$$xy + z - 1 = xy + 1 - x - y = (x - 1)(y - 1).$$

Likewise,

$$yz + x - 1 = (y - 1)(x - 1)$$

and

$$zx + y - 1 = (z - 1)(x - 1).$$

Hence

$$\begin{aligned} S &= \frac{1}{(x-1)(y-1)} + \frac{1}{(y-1)(z-1)} + \frac{1}{(z-1)(x-1)} \\ &= \frac{x + y + z - 3}{(x-1)(y-1)(z-1)} = \frac{-1}{(x-1)(y-1)(z-1)} \\ &= \frac{-1}{xyz - (xy + yz + zx) + x + y + z - 1} \\ &= \frac{-1}{5 - (xy + yz + zx)}. \end{aligned}$$

But

$$2(xy + yz + zx) = (x + y + z)^2 - (x^2 + y^2 + z^2) = 1.$$

Therefore  $\boxed{S = -\frac{2}{9}}$ .

□

**Problem 49** (USAMO 1978). Given that the real numbers  $a, b, c, d, e$  satisfy simultaneously the relations

$$a + b + c + d + e = 8 \quad \text{and} \quad a^2 + b^2 + c^2 + d^2 + e^2 = 16,$$

determine the maximum and the minimum value of  $a$ .

**Solution.** Since the total of  $b, c, d, e$  is  $8 - a$ , their average is  $x = \frac{8-a}{4}$ . Let

$$b = x + b_1, \quad c = x + c_1, \quad d = x + d_1, \quad e = x + e_1.$$

Then  $b_1 + c_1 + d_1 + e_1 = 0$  and

$$16 = a^2 + 4x^2 + b_1^2 + c_1^2 + d_1^2 + e_1^2 \geq a^2 + 4x^2 = a^2 + \frac{(8-a)^2}{4}$$

or

$$0 \geq 5a^2 - 16a = a(5a - 16).$$

Therefore  $0 \leq a \leq \frac{16}{5}$ , where  $a = 0$  if and only if  $b = c = d = e = 2$  and  $a = \frac{16}{5}$ , and  $a = \frac{16}{5}$  if and only if  $b = c = d = e = \frac{6}{5}$ . □

**Problem 50.** Let  $a$  and  $b$  be given real numbers. Solve the system of equations

$$\frac{x - y\sqrt{x^2 - y^2}}{\sqrt{1 - x^2 + y^2}} = a$$

$$\frac{y - x\sqrt{x^2 - y^2}}{\sqrt{1 - x^2 + y^2}} = b$$

for real numbers  $x$  and  $y$ .

**Solution.** Let  $u = x + y$  and  $v = x - y$ . Then

$$0 < x^2 - y^2 = uv < 1, \quad x = \frac{u + v}{2}, \quad y = \frac{u - v}{2}.$$

Adding the two equations and subtracting the two equations in the original system yields the new system

$$u - u\sqrt{uv} = (a + b)\sqrt{1 - uv}$$

$$v + v\sqrt{uv} = (a - b)\sqrt{1 - uv}$$

Multiplying the above two equations yields

$$uv(1 - uv) = (a^2 - b^2)(1 - uv),$$

hence  $uv = a^2 - b^2$ . It follows that

$$u = \frac{(a + b)\sqrt{1 - a^2 + b^2}}{1 - \sqrt{a^2 - b^2}} \quad \text{and} \quad v = \frac{(a - b)\sqrt{1 - a^2 + b^2}}{1 + \sqrt{a^2 - b^2}},$$

which in turn implies that

$$(x, y) = \left( \frac{a + b\sqrt{a^2 - b^2}}{\sqrt{1 - a^2 + b^2}}, \frac{b + a\sqrt{a^2 - b^2}}{\sqrt{1 - a^2 + b^2}} \right),$$

whenever  $0 < a^2 - b^2 < 1$ . □



**Problem 51.** Find all real numbers  $x$  for which

$$10^x + 11^x + 12^x = 13^x + 14^x.$$

**Solution.** It is easy to check that  $x = 2$  is a solution. We claim that it is the only one. In fact, dividing by  $13^x$  on both sides gives

$$\left(\frac{10}{13}\right)^x + \left(\frac{11}{13}\right)^x + \left(\frac{12}{13}\right)^x = 1 + \left(\frac{14}{13}\right)^x.$$

The LHS is a decreasing function of  $x$  and the RHS is an increasing function of  $x$ .

Therefore their graphs can have at most one point of intersection. □

*Remark.* More generally,

$$a^2 + (a+1)^2 + \cdots + (a+k)^2 = (a+k+1)^2 + (a+k+2)^2 + \cdots + (a+2k)^2$$

for  $a = k(2k+1)$ ,  $k \in \mathbf{N}$ .

**Problem 52** (Korean Mathematics Competition 2000). Find all real numbers  $x$  satisfying the equation

$$2^x + 3^x - 4^x + 6^x - 9^x = 1.$$

**Solution.** Setting  $2^x = a$  and  $3^x = b$ , the equation becomes

$$1 + a^2 + b^2 - a - b - ab = 0.$$

Multiplying both sides of the equation by 2 and completing the square gives

$$(1 - a)^2 + (a - b)^2 + (b - 1)^2 = 0.$$

Therefore  $1 = 2^x = 3^x$ , and  $x = 0$  is the only solution. □

# 4 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.

## §4.1 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.

### §4.1.1 General AM–GM Inequality

The **arithmetic mean** (AM) of  $n$  non-negative real variables is given by

$$A(n) = \frac{a_1 + a_2 + \cdots + a_n}{n}.$$

The **geometric mean** (GM) of  $n$  non-negative real variables is given by

$$G(n) = \sqrt[n]{a_1 a_2 \cdots a_n}.$$

**Theorem 4.1** (AM–GM inequality).

$$A(n) \geq G(n),$$

or

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}. \quad (4.1)$$

Equality holds iff  $a_1 = a_2 = \cdots = a_n$ .

#### Exercise 26

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  $a = b = c$ .  $\square$

**Exercise 27**

Let  $a_1, a_2, \dots, a_n$  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,

$$\begin{aligned} 1 + a_1 &\geq 2\sqrt{a_1} \\ 1 + a_2 &\geq 2\sqrt{a_2} \\ &\vdots \\ 1 + a_n &\geq 2\sqrt{a_n} \end{aligned}$$

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  $i = 1, 2, \dots, n$ .  $\square$

**Exercise 28**

Let  $a, b, c$  be non-negative real numbers. Prove that

$$(a + b)(b + c)(c + a) \geq 8abc.$$

*Proof.* By AM–GM,

$$\begin{aligned} a + b &\geq 2\sqrt{ab} \\ b + c &\geq 2\sqrt{bc} \\ c + a &\geq 2\sqrt{ca} \end{aligned}$$

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

**Exercise 29**

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

$$\begin{aligned} \frac{a^3}{bc} + b + c &\geq 3a \\ \frac{b^3}{ca} + c + a &\geq 3b \\ \frac{c^3}{ab} + a + b &\geq 3c \end{aligned}$$

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

**Exercise 30**

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,

$$\begin{aligned}
 & 2ab(a+b) + 2ac(a+c) + 2bc(b+c) \\
 &= ab(a+b) + ac(a+c) + bc(b+c) + ab(a+b) + ac(a+c) + bc(b+c) \\
 &= a^2(b+c) + b^2(a+c) + c^2(a+b) + (a^2b + b^2c + ca^2) + (ab^2 + bc^2 + ca^2) \\
 &\geq a^2(b+c) + b^2(a+c) + c^2(a+b) + (a^2b + b^2c + c^2a) + 3abc \\
 &= a^2(b+c) + b^2(a+c) + c^2(a+b) + ab(a+c) + bc(a+b) + ac(b+c) \\
 &= (a^2(b+c) + ab(a+c)) + (b^2(a+c) + bc(a+b)) + (c^2(a+b) + ac(b+c)) \\
 &\geq 2\sqrt{a^3b(b+c)(c+a)} + 2\sqrt{b^3c(c+a)(a+b)} + 2\sqrt{c^3a(a+b)(b+c)} \\
 &= 2ab\sqrt{\frac{a}{b}(b+c)(c+a)} + 2bc\sqrt{\frac{b}{c}(c+a)(a+b)} + 2ca\sqrt{\frac{c}{a}(a+b)(b+c)}
 \end{aligned}$$

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

### Exercise 31 (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

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

□

### Exercise 32

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. □

**Exercise 33**

Show that  $A$ , the maximum area of a triangle  $XYZ$  with a fixed perimeter  $P$ , happens when the triangle is equilateral. You may use the Heron's formula which states that  $A$ , the area of a triangle is

$$A = \sqrt{\frac{P}{2} \left( \frac{P}{2} - x \right) \left( \frac{P}{2} - y \right) \left( \frac{P}{2} - z \right)}$$

where  $x, y, z$  are the lengths of the sides of the triangle.

*Proof.* Using the AM–GM inequality,

$$\left( \frac{P}{2} - x \right) \left( \frac{P}{2} - y \right) \left( \frac{P}{2} - z \right) \leq \left( \frac{\frac{P}{2} - x + \frac{P}{2} - y + \frac{P}{2} - z}{3} \right)^3 = \left( \frac{P}{6} \right)^3.$$

Hence the maximum area is  $A = \sqrt{\frac{P}{2} \left( \frac{P}{6} \right)^3} = \frac{P^2}{12\sqrt{3}}$  and occurs when  $\frac{P}{2} - x = \frac{P}{2} - y = \frac{P}{2} - z$ , i.e.  $x = y = z$  which means that the triangle is equilateral.  $\square$

**§4.1.2 Weighted AM–GM Inequality**

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

**Theorem 4.2** (Weighted AM–GM inequality). For positive real  $a_1, a_2, \dots, a_n$  and positive integers  $\omega_1, \omega_2, \dots, \omega_n$ , by AM–GM,

$$\frac{\omega_1 a_1 + \omega_2 a_2 + \dots + \omega_n a_n}{\omega_1 + \omega_2 + \dots + \omega_n} \geq \left( a_1^{\omega_1} a_2^{\omega_2} \dots a_n^{\omega_n} \right)^{\frac{1}{\omega_1 + \omega_2 + \dots + \omega_n}} \quad (4.2)$$

Or equivalently in symbols

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

**Exercise 34**

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

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

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

**§4.1.3 Other mean quantities**

For non-negative real  $a_1, a_2, \dots, a_n$ , the **harmonic mean** (HM) is given by

$$H(n) = \frac{1}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}}$$

For non-negative real  $a_1, a_2, \dots, a_n$ , the **quadratic mean** (QM) is given by

$$Q(n) = \frac{\sqrt{a_1^2 + a_2^2 + \dots + a_n^2}}{n}$$

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

$$Q(n) \geq A(n) \geq G(n) \geq H(n)$$

### §4.1.4 Murihead's inequality

Suppose we have two sequences  $x_1 \geq x_2 \geq \dots \geq x_n$  and  $y_1 \geq y_2 \geq \dots \geq y_n$  such that

$$x_1 + x_2 + \dots + x_n = y_1 + y_2 + \dots + y_n,$$

and for  $k = 1, 2, \dots, n-1$ ,

$$x_1 + x_2 + \dots + x_k \geq y_1 + y_2 + \dots + y_k,$$

Then we say that  $(x_n)$  *majorises*  $(y_n)$ , written  $(x_n) > (y_n)$ .

Using the above, we have the following theorem.

**Theorem 4.3** (Muirhead's inequality). For positive real  $a_1, a_2, \dots, a_n$ , and  $(x_n)$  majorises  $(y_n)$ ,

$$\sum_{\text{sym}} a_1^{x_1} \dots a_n^{x_n} \geq \sum_{\text{sym}} a_1^{y_1} \dots a_n^{y_n} \quad (4.3)$$

## §4.2 Cauchy–Schwarz and Hölder's Inequalities

**Theorem 4.4** (Cauchy–Schwarz's inequality). For real  $a_1, a_2, \dots, a_n$  and  $b_1, b_2, \dots, b_n$ ,

$$(a_1^2 + a_2^2 + \dots + a_n^2)(b_1^2 + b_2^2 + \dots + b_n^2) \geq (a_1 b_1 + a_2 b_2 + \dots + a_n b_n)^2 \quad (4.4)$$

Written compactly,

$$\left( \sum_{i=1}^n a_i b_i \right)^2 \leq \left( \sum_{i=1}^n a_i^2 \right) \left( \sum_{i=1}^n b_i^2 \right)$$

Equality holds iff  $\frac{a_1}{b_1} = \frac{a_2}{b_2} = \dots = \frac{a_n}{b_n}$ .

*Proof.* Let  $\mathbf{v} = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$  and  $\mathbf{u} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$  for real  $a_1, a_2, \dots, a_n$  and  $b_1, b_2, \dots, b_n$ . Note that the inequality holds

trivially for  $\mathbf{v} = \mathbf{0}$ .

Let  $\lambda \in \mathbf{R}$ . Since  $|\mathbf{u} - \lambda \mathbf{v}| \geq 0$ ,

$$\begin{aligned} (\mathbf{u} - \lambda \mathbf{v}) \cdot (\mathbf{u} - \lambda \mathbf{v}) &\geq 0 \\ \mathbf{u} \cdot \mathbf{u} - \lambda \mathbf{v} \cdot \mathbf{u} - \lambda \mathbf{u} \cdot \mathbf{v} + \lambda^2 \mathbf{v} \cdot \mathbf{v} &\geq 0 \\ (\mathbf{v} \cdot \mathbf{v}) \lambda^2 - (2\mathbf{u} \cdot \mathbf{v}) \lambda + (\mathbf{u} \cdot \mathbf{u}) &\geq 0 \end{aligned}$$

This is a quadratic function in  $\lambda \in \mathbf{R}$ , hence the discriminant must be less than or equal to zero. Thus

$$\begin{aligned} (2\mathbf{u} \cdot \mathbf{v})^2 - 4(\mathbf{v} \cdot \mathbf{v})(\mathbf{u} \cdot \mathbf{u}) &\leq 0 \\ (\mathbf{u} \cdot \mathbf{v})^2 &\leq |\mathbf{u}|^2 |\mathbf{v}|^2 \\ \left( \sum_{k=1}^n a_k b_k \right)^2 &\leq \left( \sum_{k=1}^n a_k^2 \right) \left( \sum_{k=1}^n b_k^2 \right) \end{aligned}$$

□

**Theorem 4.5** (Titu's lemma). For positive real  $a_1, a_2, \dots, a_n$  and  $b_1, b_2, \dots, b_n$ ,

$$\frac{a_1^2}{b_1} + \frac{a_2^2}{b_2} + \dots + \frac{a_n^2}{b_n} \geq \frac{(a_1 + a_2 + \dots + a_n)^2}{b_1 + b_2 + \dots + b_n} \quad (4.5)$$

Equality holds iff  $\frac{a_1}{b_1} = \frac{a_2}{b_2} = \dots = \frac{a_n}{b_n}$ .

*Proof.* Substitute  $a_i = \frac{x_i}{\sqrt{y_i}}$  and  $b_i = \sqrt{y_i}$ . □

Generalising Cauchy–Schwarz to integrals,

$$\left( \int_a^b f(t)g(t) dt \right)^2 \leq \left( \int_a^b [f(t)]^2 dt \right) \left( \int_a^b [g(t)]^2 dt \right) \quad (4.6)$$

*Proof.* For all  $x \in \mathbf{R}$ ,

$$(xf(t) + g(t))^2 \geq 0$$

□

**Theorem 4.6** (Hölder’s inequality). For positive real  $a_1, a_2, \dots, a_n$  and  $b_1, b_2, \dots, b_n$ , and positive real  $p, q$  that satisfy  $\frac{1}{p} + \frac{1}{q} = 1$ ,

$$\left( \sum_{i=1}^n a_i^p \right)^{\frac{1}{p}} \left( \sum_{i=1}^n b_i^q \right)^{\frac{1}{q}} \geq \sum_{i=1}^n a_i b_i \quad (4.7)$$

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

### §4.3 Rearrangement and Chebyshev’s Inequalities

**Theorem 4.7** (Chebyshev’s inequality). For real  $a_1 \geq \dots \geq a_n$  and  $b_1 \geq \dots \geq b_n$ ,

$$\frac{a_1 b_1 + \dots + a_n b_n}{n} \geq \frac{a_1 + \dots + a_n}{n} \frac{b_1 + \dots + b_n}{n} \geq \frac{a_1 b_n + \dots + a_n b_1}{n} \quad (4.8)$$

**Theorem 4.8** (Rearrangement inequality). For real  $a_1 \geq \dots \geq a_n$  and  $b_1 \geq \dots \geq b_n$ , for any permutation  $\sigma$  of  $\{1, \dots, n\}$ ,

$$\sum_{i=1}^n a_i b_i \geq \sum_{i=1}^n a_i b_{\sigma(i)} \geq \sum_{i=1}^n a_i b_{n+1-i} \quad (4.9)$$

### §4.4 Other Useful Strategies

**Theorem 4.9** (Triangle inequality). For real  $a_1, a_2, \dots, a_n$ ,

$$|a_1| + |a_2| + \dots + |a_n| \geq |a_1 + a_2 + \dots + a_n| \quad (4.10)$$

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

#### §4.4.1 Schur’s Inequality

**Theorem 4.10** (Schur’s inequality). For non-negative real  $a, b, c$  and  $n > 0$ ,

$$a^n(a-b)(a-c) + b^n(b-c)(b-a) + c^n(c-a)(c-b) \geq 0 \quad (4.11)$$

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. □



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:

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

#### §4.4.2 Jensen's Inequality

A real function defined on  $(a, b)$  is said to be **convex** if for all  $x, y \in (a, b)$ ,

$$f\left(\frac{x+y}{2}\right) \leq f(x) + f(y).$$

If the opposite inequality holds, then  $f$  is said to be **concave**.

Properties

- If  $f(x)$  and  $g(x)$  are convex functions on  $(a, b)$ , then so are  $h(x) = f(x) + g(x)$  and  $M(x) = \max\{f(x), g(x)\}$ .
- If  $f(x)$  and  $g(x)$  are convex functions on  $(a, b)$  and if  $g(x)$  is non-decreasing on  $(a, b)$ , then  $h(x) = g(f(x))$  is convex on  $(a, b)$ .

**Theorem 4.11** (Jensen's inequality). Let a real-valued function  $f$  be convex on the interval  $I$ . Let  $x_1, \dots, x_n \in I$  and  $\omega_1, \dots, \omega_n \geq 0$ . Then we have

$$\frac{\omega_1 f(x_1) + \omega_2 f(x_2) + \dots + \omega_n f(x_n)}{\omega_1 + \omega_2 + \dots + \omega_n} \geq f\left(\frac{\omega_1 x_1 + \omega_2 x_2 + \dots + \omega_n x_n}{\omega_1 + \omega_2 + \dots + \omega_n}\right) \quad (4.12)$$

If  $f$  is concave, the direction of the inequality is flipped.

In particular, if we take the weights  $\omega_1 = \omega_2 = \dots = \omega_n = 1$ , we get the inequality

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

If  $f$  is concave, the inequality is reversed.

##### Exercise 35

Let  $a, b, c > 0$ . Prove that

$$a^a b^b c^c \geq \left(\frac{a+b+c}{3}\right)^{a+b+c}.$$

*Proof.* Consider the function  $f(x) = x \ln x$ . Verify that  $f''(x) = \frac{1}{x} > 0$  for all  $x \in \mathbf{R}^+$ . Thus  $f$  is convex in  $\mathbf{R}^+$  and by Jensen's inequality we conclude that

$$f(a) + f(b) + f(c) \geq 3f\left(\frac{a+b+c}{3}\right) \iff \ln a^a + \ln b^b + \ln c^c \geq 3 \ln \left(\frac{a+b+c}{3}\right)^{a+b+c},$$

which is equivalent to

$$\ln(a^a b^b c^c) \geq \ln \left(\frac{a+b+c}{3}\right)^{a+b+c}$$

as desired. □

### §4.4.3 Minkowski's Inequality

**Theorem 4.12** (Minkowski's inequality). For positive real  $a_1, \dots, a_n$  and  $b_1, \dots, b_n$  and  $p > 1$ ,

$$\left( \sum_{i=1}^n a_i^p \right)^{\frac{1}{p}} + \left( \sum_{i=1}^n b_i^p \right)^{\frac{1}{p}} \geq \left( \sum_{i=1}^n (a_i + b_i)^p \right)^{\frac{1}{p}} \quad (4.13)$$

**Theorem 4.13** (Generalised Minkowski's inequality). Let  $a_{ij} \geq 0$  for  $i = 1, \dots, n$  and  $j = 1, \dots, m$  and let  $p > 1$ , then

$$\left[ \sum_{i=1}^n \left( \sum_{j=1}^m a_{ij} \right)^p \right]^{\frac{1}{p}} \leq \sum_{j=1}^m \left( \sum_{i=1}^n a_{ij}^p \right)^{\frac{1}{p}} \quad (4.14)$$

**Theorem 4.14** (Bernoulli's inequality). For  $x > -1, x \neq 0$  and integer  $n > 1$ ,

$$(1 + x)^n > 1 + nx \quad (4.15)$$

### §4.4.4 Ravi Transformation

Suppose that  $a, b, c$  are the side lengths of a triangle. Then positive real numbers  $x, y, z$  exist such that  $a = x + y, b = y + z$  and  $c = z + x$ .

To verify this, let  $s$  be the semi-perimeter. Then denote  $z = s - a, x = s - b, y = s - c$  and the conclusion is obvious since  $s - a = \frac{b + c - a}{2} > 0$  and similarly for the others.

#### Exercise 36

Let  $a, b, c$  be the lengths of the sides of a triangle. Prove that

$$\sqrt{3(\sqrt{ab} + \sqrt{bc} + \sqrt{ca})} \geq \sqrt{a + b - c} + \sqrt{b + c - a} + \sqrt{c + a - b}.$$

*Proof.* Let  $x, y, z > 0$  such that  $a = x + y, b = y + z, c = z + x$ . Then the above inequality is equivalent to

$$3 \sum_{\text{cyc}} \sqrt{(x+y)(x+z)} \geq 2 \left( \sum_{\text{cyc}} \sqrt{x} \right)^2.$$

From Cauchy,

$$\begin{aligned} 3 \sum_{\text{cyc}} \sqrt{(x+y)(x+z)} &\geq 3 \sum_{\text{cyc}} (y + \sqrt{zx}) \\ &\geq 2 \sum_{\text{cyc}} y + 4 \sum_{\text{cyc}} \sqrt{zx} \\ &= 2 \left( \sum_{\text{cyc}} \sqrt{x} \right)^2 \end{aligned}$$

□

### §4.4.5 Normalisation

Homogeneous inequalities can be **normalised** e.g. applied restrictions with homogeneous expressions in the variables

For example, to show that  $a^3 + b^3 + c^3 - 3abc \geq 0$ , assume that, WLOG,  $abc = 1$  or  $a + b + c = 1$  etc. The reason is explained below.

Suppose that  $abc = k^3$ . Let  $a = ka', b = kb', c = kc'$ . This implies  $a'b'c' = 1$ , and our inequality becomes  $a'^3 + b'^3 + c'^3 - 3a'b'c' \geq 0$ , which is the same as before. Therefore the restriction  $abc = 1$  doesn't change anything of the inequality. Similarly one might also assume  $a + b + c = 1$ .

### §4.4.6 Homogenisation

**Homogenisation** is the opposite of normalisation. It is often useful to substitute  $a = \frac{x}{y}$ ,  $b = \frac{y}{z}$ ,  $c = \frac{z}{x}$ , when the condition  $abc = 1$  is given. Similarly when  $a+b+c = 1$  we can substitute  $a = \frac{x}{x+y+z}$ ,  $b = \frac{y}{x+y+z}$ ,  $c = \frac{z}{x+y+z}$  to homogenise the inequality.

#### Exercise 37

If  $a, b, c > 0$  and  $a + b + c = 1$ , prove that  $a^2 + b^2 + c^2 + 1 \geq 4(ab + bc + ca)$ .

*Proof.* So all the terms except for the 1 are of the second degree. We substitute  $a + b + c$  for 1. The inequality still gives a non-homogeneous inequality. So instead we square the condition to make it second degree and get

$$a^2 + b^2 + c^2 + 2(ab + bc + ca) = 1$$

Now plugging this for 1 in the inequality and simplifying gives  $a^2 + b^2 + c^2 \geq ab + bc + ca$ , which is well-known by the Rearrangement Inequality.  $\square$

## Exercises

**Problem 53** (H3M 2018 Q3). A triangle has sides of length  $a, b, c$  units. In each of the following cases, prove that there is a triangle having sides of the given lengths.

- (a)  $\frac{a}{1+a}, \frac{b}{1+b}$  and  $\frac{c}{1+c}$  units.
- (b)  $\sqrt{a}, \sqrt{b}$  and  $\sqrt{c}$  units.
- (c)  $\sqrt{a(b+c-a)}, \sqrt{b(c+a-b)}$  and  $\sqrt{c(a+b-c)}$  units.

**Solution.** To prove that there is a triangle having sides of the given lengths, prove that the sum of lengths of any two sides is greater than length of third side.

- (a) WLOG, assume that  $a \leq b \leq c$ . By monotonicity of the function  $y = \frac{x}{1+x}$ ,  $x > 0$ , we have
- $$\frac{a}{1+a} \leq \frac{b}{1+b} \leq \frac{c}{1+c}.$$

It remains to be shown that  $\frac{a}{1+a} + \frac{b}{1+b} > \frac{c}{1+c}$ , as the remaining other triangle inequalities are trivially true.

$$\begin{aligned} \frac{a}{1+a} + \frac{b}{1+b} &\geq \frac{a}{1+b} + \frac{b}{1+b} \\ &= \frac{a+b}{1+b} \\ &> \frac{c}{1+b} \quad [\text{using triangle inequality on triangle with sides } a, b, c] \\ &\geq \frac{c}{1+c} \end{aligned}$$

- (b) WLOG, assume that  $a \leq b \leq c$ . By monotonicity of the function  $y = \sqrt{x}$ ,  $x > 0$ , we have  $\sqrt{a} \leq \sqrt{b} \leq \sqrt{c}$ .

It remains to be shown that  $\sqrt{a} + \sqrt{b} > \sqrt{c}$ , as the remaining other triangle inequalities are trivially true.

$$\begin{aligned} (\sqrt{a} + \sqrt{b})^2 &= a + b + 2\sqrt{ab} \\ &> c + 2\sqrt{ab} \quad [\text{using triangle inequality on triangle with sides } a, b, c] \\ &> c + 0 = c \end{aligned}$$

- (c) WLOG, we only need to show that  $\sqrt{a(b+c-a)} + \sqrt{b(c+a-b)} > \sqrt{c(a+b-c)}$  due to the symmetricity of the terms involved.

$$\begin{aligned} &a(b+c-a) + b(c+a-b) > c(a+b-c) \\ \iff &ab + ac - a^2 + bc + ab - b^2 > ac + bc - c^2 \\ \iff &c^2 - a^2 + 2ab - b^2 > 0 \\ \iff &c^2 - (a-b)^2 > 0 \\ \iff &(c+a-b)(c-a+b) > 0 \end{aligned}$$

By triangle inequality,  $c+a-b > 0$  and  $c-a+b > 0$ .

□

**Problem 54** (H3M 2016 Q3).

- (i) For some positive integer
- $n$
- , let
- $x_1 \leq x_2 \leq \dots \leq x_n$
- and
- $y_1 \leq y_2 \leq \dots \leq y_n$
- be real numbers.

By considering the sum of all  $n^2$  terms of the form  $(x_i - x_j)(y_i - y_j)$ , prove that

$$\sum_{i=1}^n x_i y_i \geq \frac{1}{n} \left( \sum_{i=1}^n x_i \right) \left( \sum_{i=1}^n y_i \right).$$

[5]

- (ii) Let a triangle have angles
- $A, B, C$
- and let the lengths of the opposite sides be
- $a, b$
- and
- $c$
- .

By applying the result of part (i), prove that

$$aA + bB + cC \geq \frac{1}{3}\pi(a + b + c).$$

[4]

- (iii) Let
- $a, b, c$
- be three positive numbers such that
- $a^2 + b^2 + c^2 = 1$
- . By applying the result of part (i)

with  $\{x_i\} = \left\{ \frac{a+b}{c}, \frac{c+a}{b}, \frac{b+c}{a} \right\}$ , find the minimum possible value of

$$\frac{(a+b)(a^2+b^2)}{c} + \frac{(c+a)(c^2+a^2)}{b} + \frac{(b+c)(b^2+c^2)}{a}.$$

[7]

**Solution.**

- (i) We have

$$\begin{aligned} & \sum_{i=1}^n \sum_{j=1}^n (x_i - x_j)(y_i - y_j) \\ &= \sum_{i=1}^n \sum_{j=1}^n (x_i y_i - x_j y_i - x_i y_j + x_j y_j) \\ &= \sum_{i=1}^n \left( n x_i y_i - y_i \sum_{j=1}^n x_j - x_i \sum_{j=1}^n y_j + \sum_{j=1}^n x_j y_j \right) \\ &= 2n \sum_{i=1}^n x_i y_i - 2 \sum_{i=1}^n x_i \sum_{i=1}^n y_i \end{aligned}$$

Also,

$$\begin{aligned} \sum_{i=1}^n \sum_{j=1}^n (x_i - x_j)(y_i - y_j) &= \sum_{i=j} (x_i - x_j)(y_i - y_j) + \sum_{i \neq j} (x_i - x_j)(y_i - y_j) \\ &= 0 + \sum_{i < j} (x_i - x_j)(y_i - y_j) + \sum_{i > j} (x_i - x_j)(y_i - y_j) \\ &= 0 + \sum (\leq 0)(\leq 0) + \sum (\geq 0)(\geq 0) \\ &\geq 0 \end{aligned}$$

Combining both results,

$$2n \sum_{i=1}^n x_i y_i - 2 \sum_{i=1}^n x_i \sum_{i=1}^n y_i - 2 \sum_{i=1}^n x_i \sum_{i=1}^n y_i \geq 0$$

$$2n \sum_{i=1}^n x_i y_i \geq 2 \sum_{i=1}^n x_i \sum_{i=1}^n y_i$$

$$\sum_{i=1}^n x_i y_i \geq \frac{1}{n} \sum_{i=1}^n x_i \sum_{i=1}^n y_i$$

- (ii) Let  $x_1 = a, x_2 = b, x_3 = c$ , and  $y_1 = A, y_2 = B, y_3 = C$ , and without loss of generality let  $a \leq b \leq c$ .

Otherwise or in short we assign the  $x$ 's in ascending length order, the objective is to show that (i) can be applied and apply it to show the result in (ii).

**Case 1:**

- (iii)

□

**Problem 55** (H3M). If  $a, b, c$  are sides of a triangle, show that

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

**Solution.** Let  $x = a + b - c$ ,  $y = a + c - b$ ,  $z = b + c - a$ , which are all positive by triangle inequality.

Thus we have  $a = \frac{x+y}{2}$ ,  $b = \frac{x+z}{2}$ ,  $c = \frac{y+z}{2}$ .

Substituting these in gives us

$$\begin{aligned} \frac{a}{b+c-a} + \frac{b}{a+c-b} + \frac{c}{a+b-c} &= \frac{x+y}{2z} + \frac{x+z}{2y} + \frac{y+z}{2x} \\ &= \frac{1}{2} \left( \frac{x}{z} + \frac{y}{z} + \frac{x}{y} + \frac{z}{y} + \frac{y}{x} + \frac{z}{x} \right) \\ &\geq \frac{1}{2} \cdot 6\sqrt[6]{1} = 3 \end{aligned}$$

□

**Problem 56** (HCI H3M Prelim 2020 Q7).

(a) Given positive reals  $a, b, c$ , prove that

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

(b) Given  $x, y, z \geq 1$ ,  $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 2$ , prove that

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

(c) Given that  $a+b+c+d=3$  and  $a^2+2b^2+3c^2+6d^2=5$ , prove that  $1 \leq a \leq 2$ .

**Solution.**

(a) 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:

$$\begin{aligned} \frac{3(a+1)(b+1)(c+1)}{\sqrt[3]{abc}} &= \frac{3(a+\frac{1}{2}+\frac{1}{2})(b+\frac{1}{2}+\frac{1}{2})(c+\frac{1}{2}+\frac{1}{2})}{\sqrt[3]{abc}} \\ &\geq \frac{81\sqrt[3]{\frac{a}{4}}\sqrt[3]{\frac{b}{4}}\sqrt[3]{\frac{c}{4}}}{\sqrt[3]{abc}} = \frac{81}{4} \end{aligned}$$

(b) 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.

(c) 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,

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

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

□



**Problem 57** (SMO Open 2020 Q24). Let  $x, y, z$  and  $w$  be real numbers such that  $x + y + z + w = 5$ . Find the minimum value of  $(x + 5)^2 + (y + 10)^2 + (z + 20)^2 + (w + 40)^2$ .

**Solution.** By Cauchy–Schwarz,

$$4(a^2 + b^2 + c^2 + d^2) \geq (a + b + c + d)^2.$$

Substituting  $a = x + 5$ ,  $b = y + 10$ ,  $c = z + 20$ ,  $d = w + 40$  gives us

$$4\left((x + 5)^2 + (y + 10)^2 + (z + 20)^2 + (w + 40)^2\right) \geq (x + 5 + y + 10 + z + 20 + w + 40)^2$$

from which we can work out the answer of  $\boxed{1600}$ .

□

**Problem 58** (IMO 1995). Let  $a, b, c$  be positive real numbers such that  $abc = 1$ . Prove that

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

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

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

Now by Cauchy–Schwarz,

$$\sum_{\text{cyc}} \frac{x^2}{y+z} \geq \frac{(x+y+z)^2}{2(x+y+z)} = \frac{x+y+z}{2}$$

and by AM–GM,

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

Hence proven. □

**Problem 59.** Prove that for all  $n \in \mathbf{N}$ ,

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

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

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

$$\begin{aligned} \frac{f(x_1) + f(x_2) + \cdots + f(x_n)}{n} &\geq f\left(\frac{x_1 + x_2 + \cdots + x_n}{n}\right) \\ \frac{f(1) + f(2) + \cdots + f(n)}{n} &\geq f\left(\frac{1 + 2 + \cdots + n}{n}\right) \\ \frac{\sqrt{1^2+1} + \sqrt{2^2+1} + \cdots + \sqrt{n^2+1}}{n} &\geq f\left(\frac{n(n+1)/2}{n}\right) \\ &= f\left(\frac{n+1}{2}\right) = \frac{1}{2}\sqrt{n^2+2n+5} \end{aligned}$$

□

**Problem 60.** 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,

$$\begin{aligned} a + b &\geq 2\sqrt{ab} \\ \left(\frac{a + b}{2}\right)^2 &\geq ab \\ \left(\frac{a + b}{2}\right)^2 (a + b) &\geq ab(a + b) \\ \frac{(a + b)^3}{4} &\geq 2000 \\ a + b &\geq 20 \end{aligned}$$

Using AM–GM,

$$\begin{aligned} \frac{1}{a} + \frac{1}{b} + \frac{1}{a + b} &= \frac{1}{2a} + \frac{1}{2a} + \frac{1}{2b} + \frac{1}{2b} + \frac{1}{a + b} \\ &\geq 5 \sqrt[5]{\frac{1}{16} \frac{a + b}{a^2 b^2 (a + b)^2}} \\ &\geq 5 \left(\frac{1}{20}\right) = \boxed{\frac{1}{4}} \end{aligned}$$

Equality holds if and only if  $\frac{1}{2a} = \frac{1}{2b} = \frac{1}{a + b}$ , or  $a = b = 10$ . □

**Problem 61** (USAMO 2012). Find all integers  $n \geq 3$  such that among any  $n$  positive real numbers  $a_1, a_2, \dots, a_n$  with

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

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  $a_1 \leq a_2 \leq \dots \leq a_n$ . 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 4.15.** Let  $S = \{a_1, a_2, \dots, a_n\}$  be a set of  $n \geq 3$  positive real numbers, where  $a_1 \leq a_2 \leq \dots \leq a_n$ . 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  $a_1 \leq a_2 \leq \dots \leq a_{n+1}$  and  $S$  contains no three numbers that are side lengths of an acute triangle. Then, we must have

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

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  $\max(a_1, a_2, \dots, a_n) \leq n \cdot \min(a_1, a_2, \dots, a_n)$ , 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  $S = \{\sqrt{F_i}t \mid 1 \leq i \leq n, t \in \mathbf{R}^+, F_i \text{ is the } i\text{-th Fibonacci number}\}$  satisfies that it contains no three numbers that are side lengths of an acute triangle.  $\square$

**Problem 62** (IMO 2000). Let  $a, b, c$  be positive real numbers so that  $abc = 1$ . Prove that

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

**Solution.** Let  $a = \frac{x}{y}, b = \frac{y}{z}, c = \frac{z}{x}$ , 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. □

**Problem 63** (IMO 1964). Let  $a, b, c$  be the side lengths of a triangle. Prove that

$$a^2(b+c-a) + b^2(c+a-b) + c^2(a+b-c) \leq 3abc.$$

**Solution.** The inequality can be written as

$$(a+b-c)(b+c-a)(c+a-b) \leq abc.$$

Let  $a = x + y$ ,  $b = y + z$  and  $c = z + x$ . Then the above inequality becomes  $8xyz \leq (x+y)(y+z)(z+x)$  which is obvious by AM–GM.  $\square$

**Problem 64** (China 2007 Q1). Given complex numbers  $a, b, c$ , let  $|a + b| = m$ ,  $|a - b| = n$ , and suppose  $mn \neq 0$ . Prove that

$$\max\{|ac + b|, |a + bc|\} \geq \frac{mn}{\sqrt{m^2 + n^2}}.$$

**Solution.** We have

$$\begin{aligned} \max\{|ac + b|, |a + bc|\} &\geq \frac{|b||ac + b| + |a||a + bc|}{|b| + |a|} \\ &\geq \frac{|b(ac + b) - a(a + bc)|}{|a| + |b|} \\ &= \frac{|b^2 - a^2|}{|a| + |b|} \\ &\geq \frac{|b + a||b - a|}{\sqrt{2(|a|^2 + |b|^2)}}. \end{aligned}$$

Since

$$m^2 + n^2 = |a - b|^2 + |a + b|^2 = 2(|a|^2 + |b|^2),$$

we get

$$\max\{|ac + b|, |a + bc|\} \geq \frac{mn}{\sqrt{m^2 + n^2}}$$

as desired. □



**Problem 65.** Show that

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

**Solution.** Multiply both sides by 2,

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

Subtracting each side by the RHS,

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

which is always true. □

**Problem 66** (MACEDONIA 2016). For  $n \geq 3$ ,  $a_1, a_2, \dots, a_n \in \mathbb{R}^+$  satisfy

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

Prove that

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

**Solution.** Let  $b_i = a_i^4$  where  $b_i \geq 0$ . The given condition becomes

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

and we want to prove

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

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

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

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

$$\begin{aligned} \frac{1-t_1}{t_1} \frac{1-t_2}{t_2} \cdots \frac{1-t_n}{t_n} &= \frac{t_2+t_3+\dots+t_n}{t_1} \frac{t_1+t_3+\dots+t_n}{t_2} \cdots \frac{t_1+t_2+\dots+t_{n-1}}{t_n} \\ &\geq \frac{(n-1)(t_2 t_3 \cdots t_n)^{\frac{1}{n-1}}}{t_1} \frac{(n-1)(t_1 t_3 \cdots t_n)^{\frac{1}{n-1}}}{t_2} \cdots \frac{(n-1)(t_1 t_2 \cdots t_{n-1})^{\frac{1}{n-1}}}{t_n} \\ &= (n-1)^n \end{aligned}$$

□

**Problem 67** (Canada 1969). Show that if  $\frac{a_1}{b_1} = \frac{a_2}{b_2} = \frac{a_3}{b_3}$  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  $n$ .

**Solution.** 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

$$\begin{aligned} & b_1^n(p_1 a_1^n + p_2 a_2^n + p_3 a_3^n) - a_1^n(p_1 b_1^n + p_2 b_2^n + p_3 b_3^n) \\ &= p_2(a_2^n b_1^n - a_1^n b_2^n) + p_3(a_3^n b_1^n - a_1^n b_3^n) = 0 \end{aligned}$$

(The denominator is irrelevant since it never equals zero)

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

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

Similarly, from  $\frac{a_1}{b_1} = \frac{a_3}{b_3}$ , 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.  $\square$

**Problem 68** (ARML 1987). If  $a, b, c$  are positive and  $a + b + c = 6$ , show that

$$\left(a + \frac{1}{b}\right)^2 + \left(b + \frac{1}{c}\right)^2 + \left(c + \frac{1}{a}\right)^2 \geq \frac{75}{4}.$$

**Solution.**

□

**Problem 69** (Jensen's inequality). Let  $f$  be a convex function over an interval  $I$ . Given  $x_i \in I$  and real values  $t_i \geq 0$  with  $\sum_{i=1}^n t_i = 1$ , for  $1, 2, \dots, n$ , show that

$$f\left(\sum_{i=1}^n t_i x_i\right) \leq \sum_{i=1}^n t_i f(x_i).$$

**Solution.** Prove by induction. Let  $P(n)$  be the statement that  $f\left(\sum_{i=1}^n t_i x_i\right) \leq \sum_{i=1}^n t_i f(x_i)$  with the given conditions supplied by the question.

Base cases:  $P(1)$  is trivial with  $f(x_1) \leq f(x_1)$ , and  $P(2)$  is true by the definition of convexity for  $f$  [recall that  $f$  being convex is defined as  $f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)f(x_2)$ ].

Assume the relation holds for  $n = k$  for some positive integer  $k$ . Then we have

$$\begin{aligned} f\left(\sum_{i=1}^{k+1} t_i x_i\right) &= f\left(t_{k+1} x_{k+1} + \sum_{i=1}^k t_i x_i\right) \\ &= f\left(t_{k+1} x_{k+1} + (1-t_{k+1}) \frac{1}{1-t_{k+1}} \sum_{i=1}^k t_i x_i\right) \\ &\leq t_{k+1} f(x_{k+1}) + (1-t_{k+1}) f\left(\frac{1}{1-t_{k+1}} \sum_{i=1}^k t_i x_i\right) \quad [\text{use result for } n=2] \\ &= t_{k+1} f(x_{k+1}) + (1-t_{k+1}) f\left(\sum_{i=1}^k \frac{t_i}{1-t_{k+1}} x_i\right) \\ &\leq t_{k+1} f(x_{k+1}) + (1-t_{k+1}) \sum_{i=1}^k \frac{t_i}{1-t_{k+1}} f(x_i) \quad [\text{use induction hypothesis}] \\ &= t_{k+1} f(x_{k+1}) + \sum_{i=1}^k t_i f(x_i) = \sum_{i=1}^{k+1} t_i f(x_i) \end{aligned}$$

□

**Problem 70.** Prove that

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} < \frac{1}{\sqrt{3n}}$$

for all positive integers  $n$ .

**Solution.** We prove a stronger statement:

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n-1}}.$$

We use induction.

For  $n = 1$ , the result is evident.

Suppose the statement is true for some positive integer  $k$ , i.e.

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2k-1}{2k} < \frac{1}{\sqrt{3k-1}}.$$

Then

$$\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2k-1}{2k} \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{3k+1}} \cdot \frac{2k+1}{2k+2}.$$

In order for the induction step to pass it suffices to prove that

$$\frac{1}{\sqrt{3k+1}} \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{3k+4}}.$$

This reduces to

$$\left( \frac{2k+1}{2k+2} \right)^2 < \frac{3k+1}{3k+4},$$

i.e.

$$(4k^2 + 4k + 1)(3k + 4) < (4k^2 + 8k + 4)(3k + 1),$$

i.e.

$$0 < k,$$

which is evident. Our proof is complete. □

# 5 Functional Equations

## §5.1 Introduction

**Definition 5.1** (Function). Let  $X$  and  $Y$  be sets. A **function**  $f : X \rightarrow Y$  is an assignment of a value in  $Y$  for each  $x \in X$ ; we denote this value  $f(x) \in Y$ .

Let  $f : X \rightarrow Y$  be a function. The set  $X$  is called the **domain**, and  $Y$  the **codomain**. A couple definitions which will be useful:

**Definition 5.2** (Injectivity). A function  $f : X \rightarrow Y$  is **injective** if  $f(x) = f(y) \iff x = y$ . (Sometimes also called *one-to-one*.)

**Definition 5.3** (Surjectivity). A function  $f : X \rightarrow Y$  is surjective if for all  $y \in Y$ , there is some  $x \in X$  such that  $f(x) = y$ . (Sometimes also called *onto*.)

**Definition 5.4** (Bijectivity). A function is **bijective** if it is both injective and surjective.

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. In fact, I recommend structuring the opening lines of your solution as follows:

**Solution.** The answer is  $f(x) = kx, k \in \mathbf{R}$ . It's easy to see that these functions satisfy the given equation.

We now show these are the only solutions ... □

## §5.2 Heuristics

At the beginning of a problem:

- Figure out what the answer is. For many problems, plug in  $f(x) = kx + c$  and find which  $k$  and  $c$  work. It may also be worth trying general polynomial functions.
- Make obvious optimisations (like scaling or shifting).
- Plug in  $x = y = 0$ ,  $x = 0$  into the givens, et cetera. See what the most simple substitutions give first.

Once you have done these obvious steps, some other things to try:

- The battle cry “DURR WE WANT STUFF TO CANCEL”. Plug in things that make lots of terms cancel or that make lots of terms vanish (think  $x = y = 0$ ).
- Watch for opportunities to prove injectivity or surjectivity, for example using isolated parts.
- Watch for bumps in symmetry and involutions.

- For equations over  $\mathbf{N}$ ,  $\mathbf{Z}$ , or  $\mathbf{Q}$ , induction is often helpful. It can also be helpful over  $\mathbf{R}$  as well. The triggers for induction are the same as any other olympiad problem: you can pin down new values to previous ones.
- It may help to rewrite the function in terms of other functions.

Here are three more tricks that are frequently useful.

- Tripling an involution.

If you know something about  $f(f(x))$ , try applying it  $f(f(f(x)))$  in different ways. For example, if we know that  $f(f(x)) = x + 2$ , then we obtain  $f^3(x) = f(x + 2) = f(x) + 2$ .

- Isolated parts.

When trying to obtain injective or surjective, watch for “isolated” variables or parts of the equation. For example, suppose you have a condition like

$$f(x + 2xf(y)^2) = yf(x) + f(f(y) + 1)$$

(I made that up). Noting that  $f \equiv 0$  works, assume  $f$  is not zero everywhere. Then by taking  $x_0$  with  $f(x_0) \neq 0$ , one obtains  $f$  is injective. (Try putting in  $y_1$  and  $y_2$ .)

Proving surjectivity can often be done in similar spirit. For example, suppose

$$f(f(y) + xf(x)) = y + f(x)^2.$$

By varying  $y$  with  $x$  fixed we get that  $f$  is surjective, and thus we can pick  $x_0$  so that  $f(x_0) = 0$  and go from there. Surjectivity can be especially nice if every  $y$  is wrapped in an  $f$ , say; then each  $f(y)$  just becomes replace by an arbitrary real.

- Exploiting “bumps” in symmetry.

If some parts of an equation are symmetric and others are not, swapping  $x$  and  $y$  can often be helpful. For example, suppose you have a condition like

$$f(x + f(y)) + f(xy) = f(x + 1)f(y + 1) - 1$$

(again I made that up). This equation is “almost symmetric”, except for a “bump” on the far left where  $f(x + f(y))$  is asymmetric. So if we take the equation with  $x$  and  $y$  flipped and then eliminate the common terms, we manage to obtain

$$f(x + f(y)) = f(y + f(x)).$$

If we have shown  $f$  is injective, we are even done! So often these “bumps” are what let you solve a problem. (In particular, don’t get rid of the bumps!)

Some other small tricks I should mention:

- Often, you’ll get something like  $f(x)^2 = x^2$ . When this happens, make sure you do not automatically assume  $f(x) = x$  for each  $x$ ; this type of equality holds only for each individual  $x$ .
- Check the solutions work! Don’t get a 6 unnecessarily after solving the problem just because you forget this trivial step.

### Exercise 38

If  $f(x^2 f(y)) = x^2 y$ , find  $f(2000)$ .

**Solution.** We guess  $f(x) = x$ , which in fact works. Hence  $f(2000) = \boxed{2000}$ . □



**Exercise 39**

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

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

and hence

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

□

**§5.3 Cauchy's Functional Equation Over  $\mathbf{Q}$** 

For this section, all functions are  $f : \mathbf{Q} \rightarrow \mathbf{Q}$ .

**Exercise 40 (Cauchy's functional equation)**

Find all functions  $f : \mathbf{Q} \rightarrow \mathbf{Q}$  such that

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

holds for each  $x, y \in \mathbf{Q}$ .

**Solution.** First put  $y = 0$ :

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

Then put  $y = -x$ :

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

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

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

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

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

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

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

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

$$\begin{aligned} -f\left(\frac{n}{m}\right) &= -\frac{n}{m}f(1) \\ f\left(-\frac{n}{m}\right) &= \left(-\frac{n}{m}\right)f(1) \quad \forall m, n \in \mathbf{N} \\ f(q) &= qf(1) \quad \forall q \in \mathbf{Q} \end{aligned}$$

Thus, we have found that  $f(x) = cx \forall x \in \mathbf{Q}$  and some constant  $c \in \mathbf{R}$ . 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  $f(\alpha q) = qf(\alpha) \forall q \in \mathbf{Q}, \alpha \in \mathbf{R}$ . □

## **§5.4** Cauchy's Functional Equation Over $\mathbb{R}$

## Exercises

**Problem 71** (SMO Open 2005 Q9). The function  $f(n)$  is defined for all positive integer  $n$  and take on non-negative integer values such that  $f(2) = 0$ ,  $f(3) > 0$  and  $f(9999) = 3333$ . Also, for all  $m$  and  $n$ ,

$$f(m+n) - f(m) - f(n) = 0 \text{ or } 1.$$

Determine  $f(2005)$ .

**Solution.** The given relation implies that

$$f(m+n) \geq f(m) + f(n).$$

Putting  $m = n = 1$  we obtain  $0 = f(2) \geq 2f(1) \geq 0$ . Thus  $f(1) = 0$ . Next,

$$f(3) = f(2+1) = f(2) + f(1) + x = x, \quad \text{where } x = 0 \text{ or } 1.$$

Since  $f(3) > 0$ , it follows that  $f(3) = 1$ . Since

$$f((3(m+1))) \geq f(3m) + f(3),$$

it follows, by induction, that  $f(3n) \geq n$  for all  $n$ . Also, it follows that  $f(3k) > k$  for some  $k$ , then  $f(3m) > m$  for all  $m \geq k$ .

So since  $f(3 \times 3333) = f(9999) = 3333$ , it follows that  $f(3n) = n$  for  $n \leq 3333$ . In particular  $f(3 \times 2005) = 2005$ . Consequently,

$$2005 = f(3 \times 2005) \geq f(2 \times 2005) + f(2005) \geq 3f(2005)$$

and so  $f(2005) \leq \frac{2005}{3} < 669$ . On the other hand,

$$f(2005) \geq f(2004) + f(1) = f(3 \times 668) = 668.$$

Therefore  $f(2005) = 668$ . □

**Problem 72** (SMO Open 2005 Q12). A function  $f: \mathbf{N} \rightarrow \mathbf{N}$  satisfies

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

for all  $m, n \in \mathbf{N}$ , and  $f(6) = 2$ . Also, no two of the values  $f(6)$ ,  $f(9)$ ,  $f(12)$  and  $f(15)$  coincide. How many three-digit positive integers  $n$  satisfy  $f(n) = f(2005)$ ?

**Solution.** Since

$$f(6+n) = f(f(6) + n) = f(2+n) \quad \text{for all } n,$$

the function  $f$  is periodic with period 4 starting from 3 onwards.

Now  $f(6), f(5), f(4), f(3)$  are four distinct values. Thus in every group of 4 consecutive positive integers greater than 3, there is exactly one that is mapped by  $f$  to  $f(2005)$ .

Since the collection of three-digit positive integers can be divided into exactly 225 groups of 4 consecutive integers each, there are 225 three-digit positive integer  $n$  that satisfies  $f(n) = f(2005)$ . □

**Problem 73** (SMO Open 2005 Q13). Let  $f$  be a real-valued function so that

$$f(x, y) = f(x, z) - 2f(y, z) - 2z$$

for all real numbers  $x, y$  and  $z$ . Find  $f(2005, 1000)$ .

**Solution.** Setting  $x = y = z$ , we see that

$$f(x, x) = f(x, x) - 2f(x, x) - 2x \implies f(x, x) = -x \quad \forall x.$$

Setting  $y = x$  gives

$$f(x, x) = f(x, z) - 2f(x, z) - 2z \implies f(x, z) = x - 2z \quad \forall x, z.$$

Therefore,  $f(2005, 1000) = 5$ . □

**Problem 74** (SMO Open 2006 Q3). A function  $f$  is such that  $f : \mathbf{R} \rightarrow \mathbf{R}$  where

$$f(xy + 1) = f(x)f(y) - f(y) - x + 2$$

for all  $x, y \in \mathbf{R}$ . Find  $10f(2006) + f(0)$ .

**Solution.** By interchanging  $x$  and  $y$ , we have

$$f(yx + 1) = f(y)f(x) - y + 2 \implies f(x) = y = f(y) + x.$$

Let  $y = 0$ . Then  $f(x) = f(0) + x$ . Putting  $x = y = 0$ , we get

$$f(0) + 1 = f(1) = f(0)f(0) - f(0) + 2 \implies (f(0) - 1)^2 = 0 \implies f(0) = 1.$$

Thus  $100f(2006) + f(0) = 20071$ . □

**Problem 75** (SMO Open 2006 Q9). Suppose  $f$  is a function satisfying  $f(x + x^{-1}) = x^6 + x^{-6}$ , for all  $x \neq 0$ . Determine  $f(3)$ .

**Solution.** Let  $y = x + x^{-1}$ . Factoring the RHS,

$$\begin{aligned} f(y) &= x^6 + \frac{1}{x^6} \\ &= \left(x^2 + \frac{1}{x^2}\right)\left(x^4 - 1 + \frac{1}{x^4}\right) \\ &= \left(\left(x + \frac{1}{x}\right)^2 - 2\right)\left(\left(x^2 + \frac{1}{x^2}\right)^2 - 3\right) \\ &= \left(\left(x + \frac{1}{x}\right)^2 - 2\right)\left(\left(\left(x + \frac{1}{x}\right)^2 - 2\right)^2 - 3\right) \\ &= (y^2 - 2)((y^2 - 2)^2 - 3) \end{aligned}$$

Therefore  $f(3) = 322$ . □

**Problem 76** (SMO Open 2020 Q7). Given that  $f : \mathbf{R} \rightarrow \mathbf{R}$  such that

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

For all numbers  $a$  and  $b$  and that  $f(1) = \frac{1}{101}$ . Find the value of  $\sum_{k=1}^{100} f(k)$ .

**Solution.** Our first guess is  $f(x)$ , since  $a^2 - b^2 = (a - b)(a + b)$ . But upon looking at  $f(1) = \frac{1}{101}$ , we have  $f(x) = \frac{x}{101}$ .

Hence we evaluate

$$\sum_{k=1}^{100} f(k) = \frac{1}{101} + \frac{2}{101} + \cdots + \frac{100}{101} = \frac{1}{101} \left( \frac{100 \times 101}{2} \right) = \boxed{50}.$$

□

**Problem 77** (SMO Open 2021 Q6). Consider all the polynomials  $P(x, y)$  in two variables such that  $P(0, 0) = 2020$  and for all  $x$  and  $y$ ,  $P(x, y) = P(x + y, y - x)$ . Find the largest possible value of  $P(1, 1)$ .

**Solution.** Starting with  $P(x, y) = P(x + y, y - x)$ ,  $P(0, 1) = P(1, 1)$ .

Then  $P(0, 1) = P\left(-\frac{1}{2}, \frac{1}{2}\right)$  and  $P\left(-\frac{1}{2}, \frac{1}{2}\right) = P\left(-\frac{1}{2}, 0\right)$  and  $P\left(-\frac{1}{2}, 0\right) = P\left(-\frac{1}{4}, -\frac{1}{4}\right)$ .

Then  $P\left(-\frac{1}{4}, -\frac{1}{4}\right) = P\left(-\frac{1}{4}, 0\right)$  and  $P\left(-\frac{1}{4}, 0\right) = P\left(-\frac{1}{8}, -\frac{1}{8}\right)$  and it will converge to  $P(0, 0)$ . Thus  $P(1, 1) = P(0, 0) = \boxed{2020}$ . □

**Problem 78** (IMO 2019 Shortlist A1). Determine all functions  $f : \mathbf{Z} \rightarrow \mathbf{Z}$  such that, for all integers  $a$  and  $b$ ,

$$f(2a) + 2f(b) = f(f(a+b)).$$

Most solutions to this problem first prove that  $f$  must be linear, before determining all linear functions satisfying the above equation.

**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  $\boxed{f(x) = 2x + h, h \in \mathbf{Z}}$ , or  $\boxed{f \equiv 0}$ . □

**Problem 79** (IMO 2015). Solve the functional equation

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

for  $f : \mathbf{R} \rightarrow \mathbf{R}$ .

**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 80** (China 2016). Find all functions  $f : \mathbf{Z} \rightarrow \mathbf{Z}$ , such that for  $\forall m, n \in \mathbf{Z}$ ,

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

**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  $\boxed{\text{S1: } f(x) = 0 \quad \forall x \in \mathbf{Z}}$ , which indeed fits

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

**Problem 81** (Vietnam 2006 B). Find all real continuous functions  $f(x)$  satisfying

$$f(x-y)f(y-z)f(z-x) + 8 = 0,$$

for all real  $x, y, z$ .

**Solution.** Let  $P(x, y, z) : f(x-y)f(y-z)f(z-x) + 8 = 0$ .

$$P\left(\frac{t}{2}, -\frac{t}{2}, 0\right) : f(t) \cdot f\left(-\frac{t}{2}\right)^2 + 8 = 0$$

shows that  $f(t) < 0$  for all  $t$ . Then we can write  $f(x) = -2^{g(x)}$ , where  $g(x)$  is a function we have to find.

Now the given equation becomes

$$g(x-y) + g(y-z) + g(z-x) = 3. \tag{1}$$

Put  $u = x - y$ ,  $v = y - z$ , then  $z - x = -(u + v)$ . Also denoting  $h(x) = g(x) - 1$  we get

$$h(u) + h(v) = -h(-u - v). \tag{2}$$

Note that for  $u = v = 0$  and  $u = x, v = 0$  we have  $h(0) = 0$  and  $h(-x) = -h(x)$ , respectively, and hence (2) can be written as

$$h(u) + h(v) = h(u + v)$$

which is the Cauchy equation, which has all solutions  $h(t) = Ct$  with  $C \in \mathbf{R}$ . Then  $g(x) = Ct + 1$  and  $f(x) = -2^{Cx+1}$ .

Conversely, by direct verification we see that the obtained functions satisfy the requirement of the problem. Thus the solutions are

$$f(x) = -2^{Cx+1},$$

where  $C$  is an arbitrary real constant.  $\square$

# 6 Sequences and Series

## §6.1 Summation Series

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

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

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

*Proof.* These can be proven using mathematical induction. □

## §6.2 Arithmetic and Geometric Progressions

### §6.2.1 Arithmetic Progression

An **arithmetic progression** (AP) is a sequence where the next term is a constant addition/subtraction of the previous term.

For a particular term,

$$a_n = a + (n-1)d$$

where  $a$  is the first term,  $d$  is the common difference.

The series is given by

$$S_n = \frac{[a + a + (n-1)d]n}{2} = \frac{n}{2}[2a + (n-1)d].$$

### §6.2.2 Geometric Progression

A **geometric progression** (GP) is a sequence where the next term is a constant product of the previous term.

For a particular term,

$$a_n = ar^{n-1}$$

where  $a$  is the first term,  $r$  is the common ratio.

The series is given by

$$S_n = \frac{a(1-r^n)}{1-r} \quad \text{or} \quad \frac{a(r^n-1)}{r-1}$$

where the former formula is preferred for  $|r| < 1$ , and the latter for  $|r| > 1$ .

If the sequence is convergent with  $|r| < 1$ , then the sum to infinity exists, given by

$$S_{\infty} = \frac{a}{1-r}.$$

## §6.3 Telescoping Sums

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

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

### Exercise 41

Evaluate the following sum:

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

**Solution.**

$$\begin{aligned} \frac{1}{\sqrt{n+1} + \sqrt{n}} &= \frac{\sqrt{n+1} - \sqrt{n}}{(\sqrt{n+1} + \sqrt{n})(\sqrt{n+1} - \sqrt{n})} \\ &= \sqrt{n+1} - \sqrt{n} \end{aligned}$$

Doing this for each fraction gives us

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

□

### Exercise 42

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.

$$\begin{aligned} \frac{1}{n^2 + 3n + 2} &= \frac{1}{n+1} - \frac{1}{n+2} \\ \sum_{n=1}^{2015} \left( \frac{1}{n+1} - \frac{1}{n+2} \right) &= \left( \frac{1}{2} - \frac{1}{3} \right) + \left( \frac{1}{3} - \frac{1}{4} \right) + \dots + \left( \frac{1}{2016} - \frac{1}{2017} \right) \\ &= \frac{1}{2} - \frac{1}{2017} = \frac{2015}{4034} \end{aligned}$$

□

## §6.4 Power Series

The **Taylor series** is given by

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



The **Maclaurin series** is a special case of Taylor Series, where  $a = 0$ ; that is,

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

The power series below can be easily computed:

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

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

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

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

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots \quad (6.10)$$

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

## Exercises

**Problem 82** (SMO Open 2013 Q1). Evaluate the sum

$$\frac{1}{1 \times 2 \times 3} + \frac{1}{2 \times 3 \times 4} + \cdots + \frac{1}{100 \times 101 \times 102}.$$

**Solution.**

□

SMO Open 2011 Q25

**Part III**

**Geometry**

# 7 Synthetic Geometry

Otherwise mentioned, let  $\triangle ABC$  denote a triangle,  $[ABCD]$  denote area of polygon  $ABCD$ .

## §7.1 Angles

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

### §7.1.1 Phantom Points

## §7.2 Triangle

### §7.2.1 Triangle centres

Although there are many triangle centres, we will only be concerned with the following more important ones.

1. **Centroid**  $G$ : intersection of medians
2. **circumcentre**  $O$ : centre of the circle which passes through vertices of the triangle
3. **Incentre**  $I$ : intersection of the internal angle bisectors, which is also the centre of the unique circle inside the triangle tangent to all three sides
4. **Excentre**  $J$ : centre of the circle which is tangent to sides of the triangle but lies outside the triangle
5. **Orthocentre**  $H$ : intersection of altitudes

[to include figures]

Along with triangle centres, there are some 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

[to include figures]

We shall outline some important properties of triangle centres.

**Proposition 7.1.** Medians cut triangle into 6 parts of equal area.

**Proposition 7.2.** Centroid  $G$  divides medians into segments of ratio 2 : 1.

**Proposition 7.3.** Circumcentre Extended sine rule

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

**Proposition 7.4.** Excentres, excircles

**Proposition 7.5.** If  $\triangle ABC$  is acute, then the incentre of the orthic triangle of  $\triangle ABC$  is the orthocentre  $H$ .

*to include figure.* Let  $\theta = \angle EAH$ . Since  $\angle ADC = 90^\circ$ , we have that  $\theta = 90^\circ - \angle C$ . The quadrilateral  $EA FH$  is cyclic and, in fact  $E$  and  $F$  lie on the circle with diameter  $AH$ . Since  $EH$  subtends  $\theta$  as well as  $\angle EFH$  on this circle, so  $\angle EFH = \theta = 90^\circ - \angle C$ . The same argument (with  $A$  instead of  $B$ ) shows that  $\angle DFH = 90^\circ - \angle C$ . Hence  $\angle EFH = \angle DFH$ , i.e. the line  $HF$  bisects  $\angle EFD$ . By the same reasoning  $HD$  bisects  $\angle EDF$  and  $HE$  bisects  $\angle FED$ .  $\square$

If  $\triangle ABC$  is obtuse, then the incentre of the orthic triangle of  $\triangle ABC$  is the obtuse vertex.

**Proposition 7.6.** For any acute  $\triangle ABC$  and any  $\triangle DEF$ ,  $\triangle DEF$  is the orthic triangle of  $\triangle ABC$  if and only if  $A$ ,  $B$ , and  $C$  are the excentres of  $\triangle DEF$ .

*Proof.* First, we show that the orthic triangle leads to the excentres. Let  $D$ ,  $E$ , and  $F$  be on  $\overline{AB}$ ,  $\overline{BC}$ , and  $\overline{CA}$ , respectively. Because  $ADEB$  is cyclic,  $\angle EDC = \angle A$ . Likewise,  $\angle BDF = \angle A$  as well. Then because  $\angle BDF + \angle D + \angle EDC = 180^\circ$ ,  $\angle A + \angle D + \angle A = 180^\circ$  and so  $\angle D = 180^\circ - 2\angle A$ .

Thus, the exterior angle of  $\angle D$  is  $2\angle A$ . But  $\angle BDF = \angle EDC = \angle A$ , so  $\overline{BC}$  bisects the exterior angle of  $\angle D$ . Similarly,  $\overline{CA}$  and  $\overline{AB}$  bisect the exterior angles of  $\angle E$  and  $\angle F$  respectively. Thus, the intersections of  $\overline{AB}$ ,  $\overline{BC}$ , and  $\overline{CA}$  (namely  $A$ ,  $B$ , and  $C$ ) are the excentres of  $\triangle DEF$ , and we are halfway finished.

Next, we show that the excentres lead to the orthic triangle. Let  $A$ ,  $B$ , and  $C$  be the  $D$ -excentre,  $E$ -excentre, and  $F$ -excentre of  $\triangle DEF$ , and let  $H$  be the incentre of  $\triangle DEF$ .  $A$  is equidistant from  $\overline{DE}$  and  $\overline{FE}$ , so  $A$  is on  $\overline{DH}$ ; as a result,  $\overline{AH}$  is an internal angle bisector of  $\angle D$ .

We know that  $\angle ADE = \frac{1}{2}\angle D$  and because  $C$  is an  $F$ -excentre of  $\triangle DEF$ ,  $\angle EDC = 90^\circ - \frac{1}{2}\angle D$ . Thus,  $\angle ADC = 90^\circ$ , and because  $D$  is on  $\overline{BC}$ ,  $D$  is the foot of the altitude from  $A$  of  $\triangle ABC$ . Similarly,  $E$  and  $F$  are feet of the altitudes from  $B$  and  $C$ , respectively. Then  $\triangle DEF$  is the orthic triangle of  $\triangle ABC$ , and we are done.  $\square$

In the obtuse case, the two vertices with acute angles and the orthocentre of  $\triangle ABC$  are the excentres.

*Remark.* This lemma makes frequent appearances in olympiad geometry. Problems written in either excentres or the orthic triangle can often be solved by shifting perspective to the other, via the medium of this lemma. Also, note the converse works as well.

**Proposition 7.7.** Point where angle bisector of  $A$  meets perp bisector of  $BC$  lies on circumcircle of  $ABC$ . This point is also the centre of circle passing through  $B, C, I, J_A$ .

**Proposition 7.8** (Incentre–excentre lemma). Given any  $\triangle ABC$  with incenter  $I$  and  $A$ -excenter  $I_A$ , let  $L$  be the midpoint of arc  $BC$  on the triangle's circumcenter. Then, the theorem states that  $L$  is the center of a circle through  $I, B, I_A$ , and  $C$ .

*Proof.* Let  $A = \angle BAC$ ,  $B = \angle CBA$ ,  $C = \angle ACB$ , and note that  $A, I, L$  are collinear (as  $L$  is on the angle bisector). We are going to show that  $LB = LI$ , the other cases being similar. First, notice that

$$\angle LBI = \angle LBC + \angle CBI = \angle LAC + \angle CBI = \angle IAC + \angle CBI = \frac{1}{2}A + \frac{1}{2}B.$$

However,

$$\angle BIL = \angle BAI + \angle ABI = \frac{1}{2}A + \frac{1}{2}B.$$

Hence,  $\triangle BIL$  is isosceles, so  $LB = LI$ . The rest of the proof proceeds along these lines.  $\square$

*Remark.* The incentre/excenter lemma makes frequent appearances in olympiad geometry. Along with the larger lemma, two smaller results follow: first,  $A, I, L$ , and  $I_A$  are collinear, and second,  $I_A$  is the reflection of  $I$  across  $L$ . Both of these follow easily from the main proof.

### §7.2.2 Right triangle

**Theorem 7.9** (Pythagoras' theorem). Given  $\triangle ABC$  where the right angle is at  $C$ ,

$$a^2 + b^2 = c^2 \tag{7.1}$$

Using similar triangles, we can deduce

$$\frac{1}{h^2} = \frac{1}{a^2} + \frac{1}{b^2} \tag{7.2}$$

where  $h$  is the perpendicular distance from  $C$  to  $a$ .

### §7.2.3 Congruency and Similarity

Triangle similarity - AA, SAS, SSS, RHS

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 - SSS, ASA, SAS, SAA

Same conditions but check that one corresponding side matches.

### §7.2.4 Theorems

**Theorem 7.10** (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.* The core idea of the proof is to find the relationship between the area and the height of the triangle. Given  $\triangle ABC$  is an equilateral triangle with height  $h$  and side length  $a$ . Let  $P$  denote an arbitrary point within the triangle.

Let  $s$ ,  $t$  and  $u$  be the distances from  $P$  to  $BC$ ,  $CA$  and  $AB$  respectively. □

**Theorem 7.11** (Carnot's theorem). Given  $\triangle ABC$ .  $P$  lies in the interior of the triangle.  $D$ ,  $E$  and  $F$  denote the foots of perpendicular from  $P$  to sides  $BC$ ,  $CA$  and  $AB$  respectively. Then we have

$$AE^2 + BD^2 + CF^2 = AF^2 + BE^2 + CD^2 \quad (7.3)$$

*Proof.* By Pythagoras' Theorem, we have

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

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

This gives us

$$PC^2 - PA^2 = CF^2 - AF^2 \quad (1)$$

Similarly, we have

$$PA^2 - PB^2 = AE^2 - BE^2 \quad (2)$$

$$PB^2 - PC^2 = BD^2 - CD^2 \quad (3)$$

Adding (1), (2) and (3) gives us our desired outcome. □

**Theorem 7.12** (Angle bisector theorem). Given  $\triangle ABC$ . Let the angle bisector of  $\angle A$  intersect  $BC$  at point  $D$ . Then we have

$$\frac{BD}{CD} = \frac{AB}{AC} \quad (7.4)$$

**Definition 7.13.** A **Fermat point** is a point in a triangle (with no angle greater than  $120^\circ$ ) such that the sum of the distances from the vertices to the point is minimal.

One of the methods to construct the Fermat point – which is provided by Fermat – is as follows:

- Draw an equilateral triangle on any of the 2 sides of the triangle.
- For each new vertex of the equilateral triangles draw a line from the new vertex joining to the original triangles opposite vertex.
- The points intersect at the Fermat point.

**Theorem 7.14** (Stewart's theorem). Given  $\triangle ABC$ . If cevian  $AD$  with length  $d$  divides  $BC$  into segments of lengths  $m$  and  $n$ , we have

$$cnc + bmb = dad + man. \quad (7.5)$$

You will usually use this theorem to find the lengths of angle bisectors and medians.

*Proof.* Since  $\cos \angle ADB = -\cos \angle ADC$  (because the angles are supplementary), we can relate all the given lengths using cosine rule:

$$\cos \angle ADB = \frac{c^2 - d^2 - m^2}{-2dm} = -\frac{b^2 - d^2 - n^2}{-2dn} = -\cos \angle ADC$$

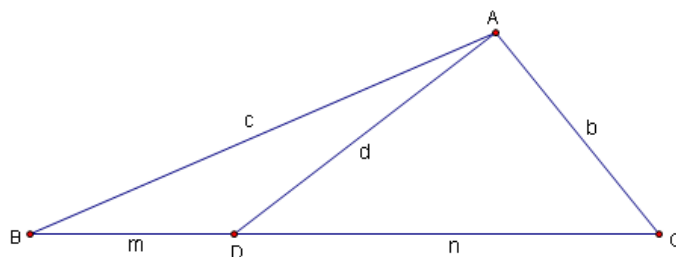
Multiplying both sides by  $-2mnd$ ,

$$c^2n - d^2n - nm^2 = -b^2m + d^2m + n^2m.$$

Rearranging this, we have

$$c^2n + b^2m = d^2(m + n) + mn(m + n)$$

and notice that  $m + n = BC = a$ . □



**Corollary 7.15** (Apollonius's Theorem (Pappus's Median Theorem)). Given  $\triangle ABC$ .  $AD$  is median from  $A$  to  $BC$ . Then

$$AD^2 = \frac{2b^2 + 2c^2 - a^2}{4}.$$

### §7.2.5 Ceva and Menelaus

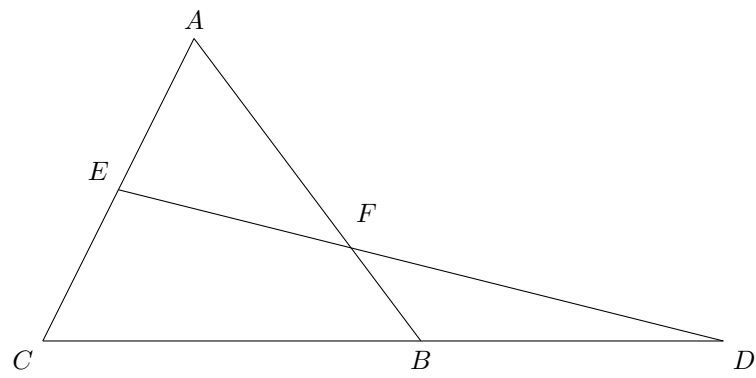
We will specifically look at these two theorems because they are of utmost importance in olympiad.

**Theorem 7.16** (Ceva's theorem). Given  $\triangle ABC$ . Point  $P$  inside the triangle. Continue lines  $AP$ ,  $BP$  and  $CP$  to intersect  $BC$ ,  $CA$  and  $AB$  at  $D$ ,  $E$  and  $F$  respectively. Then

$$\frac{AF}{FB} \times \frac{BD}{DC} \times \frac{CE}{EA} = 1. \quad (7.6)$$

**Theorem 7.17** (Menelaus' theorem). Given  $\triangle ABC$ . A transversal intersects  $BC$ ,  $AC$  and  $AB$  at points  $D$ ,  $E$  and  $F$  respectively. Then we have

$$\frac{AF}{FB} \times \frac{BD}{DC} \times \frac{CE}{EA} = 1 \quad (7.7)$$





### §7.2.6 Area of triangle

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

**Proposition 7.18.**

$$[ABC] = \frac{ah_a}{2} \quad (7.8)$$

**Proposition 7.19.**

$$[ABC] = \frac{1}{2}ab \sin C \quad (7.9)$$

*Proof.* Observe that using trigonometry, we have  $h_a = b \sin C$ . □

**Proposition 7.20.**

$$[ABC] = \frac{abc}{4R} \quad (7.10)$$

*Proof.* From sine rule, we have  $\sin C = \frac{c}{2R}$ . Substituting this into the above equation. □

**Proposition 7.21.**

$$[ABC] = sr \quad (7.11)$$

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

**Theorem 7.22** (Heron's formula). Given  $\triangle ABC$ ,

$$[ABC] = \sqrt{s(s-a)(s-b)(s-c)} \quad (7.12)$$

where  $s$  denotes the semiperimeter.

*Proof.* Our objective is to find the area of a triangle from just its three sides.

Since we know how to relate the angles of a triangle to the sides, we use  $[ABC] = \frac{1}{2}ab \sin C$ . Since  $\sin C = \sqrt{1 - \cos^2 C}$ , we have

$$\begin{aligned} [ABC] &= \frac{ab}{2} \sqrt{1 - \cos^2 C} \\ &= \frac{ab}{2} \sqrt{1 - \frac{(c^2 - a^2 - b^2)^2}{4a^2b^2}} \quad \text{by cosine rule} \\ &= \sqrt{\frac{4a^2b^2 - (c^2 - a^2 - b^2)^2}{16}} \\ &= \sqrt{\frac{(2ab - c^2 + a^2 + b^2)(2ab + c^2 - a^2 - b^2)}{16}} \\ &= \sqrt{\frac{[(a+b)^2 - c^2][c^2 - (a-b)^2]}{16}} \\ &= \sqrt{\frac{(a+b-c)(a+b+c)(a-b+c)(-a+b+c)}{16}} \\ &= \sqrt{s(s-a)(s-b)(s-c)} \end{aligned}$$

□

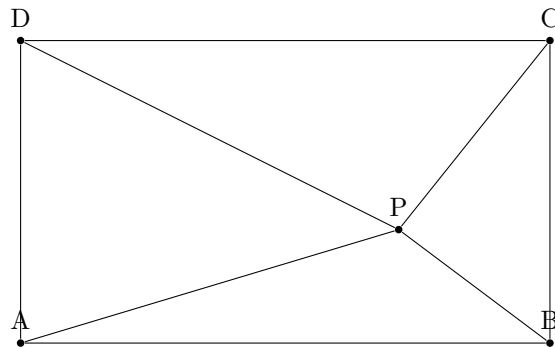
$$[ABC] = 2R^2 \sin A \sin B \sin C \quad (7.13)$$

*Proof.* □

### §7.3 Quadrilaterals

**Theorem 7.23** (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.

□

## §7.4 Circle

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

### §7.4.1 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.

### §7.4.2 Cyclic Quadrilaterals

Unlike triangles, not all quadrilaterals can be inscribed in a circle. Those which can be are known as **cyclic quadrilaterals**. Such quadrilaterals have the following special properties:

- Sum of opposite angles in a cyclic quadrilaterals is always  $180^\circ$ .
- When we draw the diagonals of a cyclic quadrilaterals, we form four pairs of equal inscribed angles.

Angle chasing and cyclic quadrilaterals

**Theorem 7.24** (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:

$$AC \cdot BD = AB \cdot CD + AD \cdot BC \quad (7.14)$$

**Theorem 7.25** (Ptolemy's inequality). For four points  $A, B, C, D$  in the plane,

$$AB \cdot CD + BC \cdot DA \geq AC \cdot BD \quad (7.15)$$

where equality holds if and only if  $ABCD$  is a cyclic quadrilateral with diagonals  $AC$  and  $BD$  (or a trivial case where  $A, B, C$  and  $D$  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

$$BD = \frac{BA \cdot DC}{AP} \quad (1)$$

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

$$BD = \frac{BC \cdot AD}{PC} \quad (2)$$

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 7.26** (Brahmagupta's formula). Given a cyclic quadrilateral  $ABCD$ ,

$$[ABCD] = \sqrt{(s-a)(s-b)(s-c)(s-d)} \quad (7.16)$$

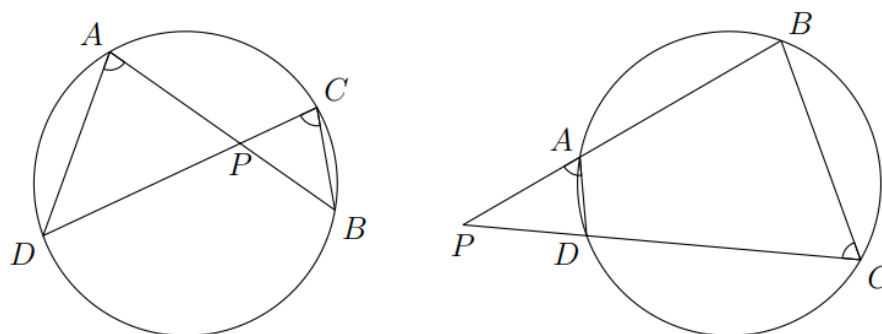
where  $s$  denotes the semiperimeter.

### §7.4.3 Power of a Point

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

**Theorem 7.27** (Power of a point). Let  $\Gamma$  be a circle, and  $P$  be a point. Let a line through  $P$  meet  $\Gamma$  at points  $A$  and  $B$ , and another line through  $P$  meet  $\Gamma$  at points  $C$  and  $D$ . Then

$$PA \cdot PB = PC \cdot PD \quad (7.17)$$



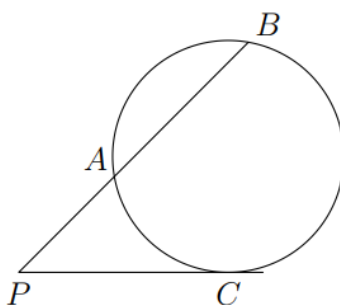
*Proof.* There are two configurations to consider, depending on whether  $P$  lies inside the circle or outside the circle.

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  $\frac{PA}{PD} = \frac{PC}{PB}$ . 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

$$PA \cdot PB = PC^2 \quad (7.18)$$



**Theorem 7.28** (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  $\frac{PA}{PD} = \frac{PC}{PB}$ . 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  $A, B, C$  and  $D$  are concyclic.  $\square$

**Definition 7.29.** Suppose that  $\Gamma$  has centre  $O$  and radius  $r$ . We say that the **power** of point  $P$  with respect to  $\Gamma$  is

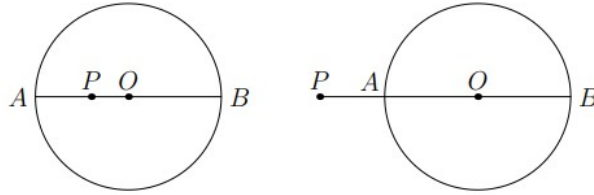
$$OP^2 - r^2.$$

Let line  $PO$  meet  $\Gamma$  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  $\Gamma$  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  $\Gamma_1$  and  $\Gamma_2$  be two circles with different centres  $O_1$  and  $O_2$ , and radii  $r_1$  and  $r_2$  respectively.

**Definition 7.30.** The **radical axis** of  $\Gamma_1$  and  $\Gamma_2$  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

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

**Lemma 7.31.** The radical axis is a line perpendicular to the line connecting the circles' centres.

*Proof.* We first prove two lemmas.

**Lemma 7.32.** 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 7.33.** There is a unique point  $P$  on line  $O_1O_2$  such that  $pow(P, \Gamma_1) = pow(P, \Gamma_2)$ .

*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  $\ell$ , hence proved.  $\square$

When  $\Gamma_1$  and  $\Gamma_2$  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*.

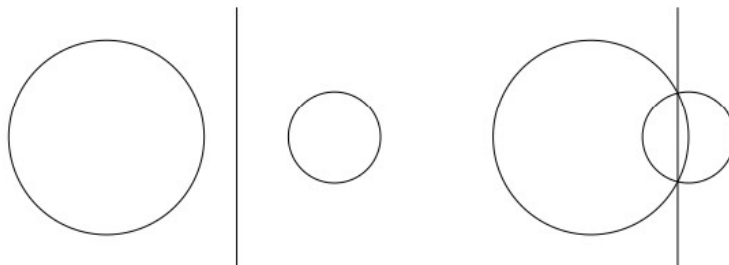


Figure 7.1: Radical axis

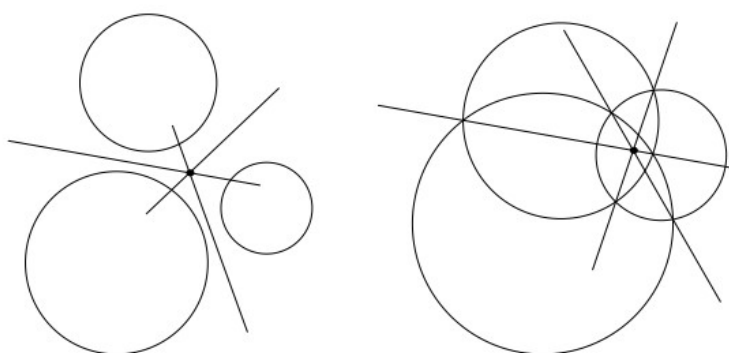


Figure 7.2: Radical centre

**Theorem 7.34** (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 centre.

*Proof.* Denote the three circles by  $\Gamma_1, \Gamma_2, \Gamma_3$ , and denote the radical axes of  $\Gamma_i$  and  $\Gamma_j$  by  $\ell_{ij}$ .

Suppose that the radical axes are not all parallel. Let  $\ell_{12}$  and  $\ell_{13}$  meet at  $X$ . Since  $X$  lies on  $\ell_{12}$ , it has equal powers with respect to  $\Gamma_1$  and  $\Gamma_2$ . Since  $X$  lies on  $\ell_{13}$ , it has equal powers with respect to  $\Gamma_1$  and  $\Gamma_3$ . Therefore,  $X$  has equal powers with respect to all three circles, and hence it must lie on  $\ell_{23}$  as well.  $\square$

#### §7.4.4 Theorems

**Theorem 7.35** (Hamilton's theorem). For  $\triangle ABC$  with circumcentre  $O$  and orthocentre  $H$ ,

$$\overrightarrow{OH} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}$$

**Theorem 7.36** (Euler line). Circumcentre  $O$ , the centroid  $G$  and the orthocentre  $H$  are collinear. We also have

$$GH = 2OG$$

and

$$OI^2 = R^2 - 2Rr.$$

**Theorem 7.37** (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 orthocentre, all lie on a single circle.

The centre of this circle lies on the Euler line, at the midpoint between the orthocentre and circumcentre.

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

**Theorem 7.38** (Simson line). Let  $P$  be a point on the circumcircle of  $\triangle ABC$ . Points  $D, E, F$  are the feet of the perpendicular bisectors from  $P$  to sides (or the extensions of)  $AB, AC, BC$  respectively. Then  $D, E, F$  are collinear.

*Proof.* Proof of existence: It suffices to show that  $\angle NMP + \angle PML = 180^\circ$ .

$PCAB$  is a cyclic quadrilateral, so  $\angle PBA + \angle ACP = \angle PBN + \angle ACP = 180^\circ$ .  $PMNB$  is a cyclic quadrilateral (since  $\angle PMB = \angle PNB = 90^\circ$ ), so  $\angle PBN + \angle NMP = 180^\circ$ . Hence  $\angle NMP = \angle ACP$ . Now  $PLCM$  is cyclic, so  $\angle PML = \angle PCL = 180^\circ - \angle ACP$ .

Therefore  $\angle NMP + \angle PML = \angle ACP + (180^\circ - \angle ACP) = 180^\circ$ .  $\square$

We now prove some properties regarding the Simson line.

The Simson line of a vertex of the triangle is the altitude of the triangle dropped from that vertex, and the Simson line of the point diametrically opposite to the vertex is the side of the triangle opposite to that vertex. If  $P$  and  $Q$  are points on the circumcircle, then the angle between the Simson lines of  $P$  and  $Q$  is half the angle of the arc  $PQ$ . In particular, if the points are diametrically opposite, their Simson lines are perpendicular and in this case the intersection of the lines lies on the nine-point circle.

**Lemma 7.39.** Let  $ABC$  be a triangle with orthocentre  $H$  and circumcircle  $\odot(ABC)$ . Suppose  $P \in \odot(ABC)$ . Let  $\gamma$  be Simson's line of  $P$  wrt  $ABC$ .

Prove that  $\gamma$  bisects  $PH$ .

*Proof.* Let  $PA, PB, PC$  be the projections of  $P$  on the sides  $BC, AC, AB$ ; let  $Q$  be the intersection between  $AH$  and the Simson's line of  $P$ . We want to show that  $HQ = PP_A$ . If we call  $H_A$  the symmetric of  $H$  with respect to the  $BC$  side, we have that  $HA$  lies on the circumcircle of  $ABC$ , so, in order to prove that  $HQ = PP_A$ , it is sufficient to show that  $PP_AQH_A$  is an isosceles trapezoid. Let  $\theta = \widehat{P_C P_A B} = \widehat{P_B P_A C}$ . Since  $PP_A P_C B$  and  $PP_A C P_B$  are cyclic quadrilaterals, we have  $\theta = \widehat{P_C P B} = \widehat{P_B P C}$ , too.

Now:

$$\widehat{P_A Q H_A} = \frac{\pi}{2} - \theta,$$

and:

$$\widehat{P H_A Q} = \widehat{P H_A A} = \widehat{P B A} = \widehat{P B P_C} = \frac{\pi}{2} - \theta.$$

Since  $PP_A$  and  $QH_A$  are both orthogonal to  $BC$ ,  $PP_AQH_A$  is an isosceles trapezoid and we have  $PP_A = QH$ .  $\square$

Given two triangles with the same circumcircle, the angle between the Simson lines of a point  $P$  on the circumcircle for both triangles does not depend of  $P$ .

**Theorem 7.40** (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.  $\square$

Generalising, the circumcircles of the four triangles in a cyclic quadrilateral are concurrent.

## Exercises

**Problem 83** (SMO Open 2005 Q2). Circles  $C_1$  and  $C_2$  have radii 3 and 7 respectively. The circles intersect at distinct points  $A$  and  $B$ . A point  $P$  outside  $C_2$  lies on the line determined by  $A$  and  $B$  at a distance of 5 from the center of  $C_1$ . Point  $Q$  is chosen on  $C_2$  so that  $PQ$  is tangent to  $C_2$  at  $Q$ . Find the length of the segment  $PQ$ .

**Solution.** The point  $P$  lies on the radical axis of  $C_1$  and  $C_2$ , namely  $AB$ , and hence has equal power with respect to both circles. Thus  $PQ^2 = 5^2 - 3^2 = 16$ .  $\square$



**Problem 84** (SMO Open 2005 Q10). It is known that the three sides of a triangle are consecutive positive integers and the largest angle is twice the smallest angle. Find the perimeter of this triangle.

**Solution.** Let  $\angle C = 2\angle A$  and  $CD$  the bisector of  $\angle C$ . Let  $BC = x - 1$ ,  $CA = x$ ,  $AB = x + 1$ . Then  $\triangle ABC \sim \triangle CBD$ , which implied

$$\frac{BD}{BC} = \frac{BC}{AB} \implies BD = \frac{(x-1)^2}{x+1}$$

and

$$\frac{CD}{AC} = \frac{CB}{AB} \implies AD = CD = \frac{x(x-1)}{x+1}.$$

Since  $AB = AD + BD$ , we have

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

The only positive solution to this equation is  $x = 5$ . Hence the perimeter is 15. □

**Problem 85** (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 perpendicular to the radius, so there is a right-angled triangle with hypotenuse  $r_{n+1}$  and other sides  $r_n$  and 1. By Pythagoras, we have

$$r_{n+1}^2 = r_n^2 + 1.$$

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 86** (USA TSTST P5). Let  $ABC$  be a triangle with incentre  $I$ . Let  $D$  be a point on side  $BC$  and let  $\omega_B$  and  $\omega_C$  be the incircles of  $\triangle ABD$  and  $\triangle ACD$ , respectively. Suppose that  $\omega_B$  and  $\omega_C$  are tangent to segment  $BC$  at points  $E$  and  $F$ , respectively. Let  $P$  be the intersection of segment  $AD$  with the line joining the centers of  $\omega_B$  and  $\omega_C$ . Let  $X$  be the intersection point of lines  $BI$  and  $CP$  and let  $Y$  be the intersection point of lines  $CI$  and  $BP$ . Prove that lines  $EX$  and  $FY$  meet on the incircle of  $\triangle ABC$ .

**Solution.** (homothety): Let  $Z$  be the diametrically opposite point on the incircle. We claim this is the desired intersection.

Note that:  $P$  is the insimilicenter of  $\omega_B$  and  $\omega_C$ .  $C$  is the exsimilicenter of  $\omega$  and  $\omega_C$ . Thus by Monge theorem, the insimilicenter of  $\omega_B$  and  $\omega$  lies on line  $CP$ .

This insimilicenter should also lie on the line joining the centers of  $\omega$  and  $\omega_B$ , which is  $\overline{BI}$ , hence it coincides with the point  $X$ . So  $X \in \overline{EZ}$  as desired.  $\square$

**Solution.** (harmonic): Let  $T = \overline{I_B I_C} \cap \overline{BC}$ , and  $W$  the foot from  $I$  to  $\overline{BC}$ . Define  $Z = \overline{FY} \cap \overline{IW}$ . Because  $\angle I_B D I_C = 90^\circ$ , we have

$$-1 = (I_B I_C; PT) \stackrel{B}{=} (II_C; YC) \stackrel{F}{=} (I\infty; ZW)$$

So  $I$  is the midpoint of  $\overline{ZW}$  as desired.  $\square$

**Solution.** (outline, barycentric, Andrew Gu): Let  $AD = t$ ,  $BD = x$ ,  $CD = y$  (so with Stewart). We then have  $D = (0 : y : x)$  and so

$$\overline{AI_B} \cap \overline{BC} = \left( 0 : y + \frac{tx}{c+t} : \frac{cx}{c+t} \right)$$

hence intersection with  $BI$  gives  $I_B = (ax : cy + at : cx)$ . Similarly,  $I_C = (ay : by : bx + at)$ .

Then, we can compute

$$P = (2axy : y(at + bx + cy) : x(at + bx + cy))$$

since  $P \in \overline{I_B I_C}$ , and clearly  $P \in \overline{AD}$ . Intersection now gives

$$\begin{aligned} X &= (2ax : at + bx + cy : 2cx) \\ Y &= (2ay : 2by : at + bx + cy). \end{aligned}$$

From here one can check that the antipode

$$Q = (4a^2 : -a^2 + 2ab - b^2 + c^2 : -a^2 + 2ac - c^2 + b^2)$$

lies on each of lines  $EX$  and  $FY$  (using Stewart's Theorem).  $\square$

**Problem 87** (Australia 2024 P2). Let  $ABCD$  be a cyclic quadrilateral. Point  $P$  is on line  $CB$  such that  $CP = CA$  and  $B$  lies between  $C$  and  $P$ . Point  $Q$  is on line  $CD$  such that  $CQ = CA$  and  $D$  lies between  $C$  and  $Q$ . Prove that the incentre of triangle  $ABD$  lies on line  $PQ$ .

*Proof.* Let  $PQ$  intersect the angle bisector of  $\angle BAC$  at  $I'$ .  $APBI'$  is cyclic since  $\angle BPI' = \frac{\angle A}{2} = \angle PAI'$ . Then,  $\angle I'BA = \angle I'PA = \frac{\angle QCA}{2} = \frac{\angle B}{2}$  so  $I' = I$  and we are done.  $\square$

# 8 Analytic Geometry

## §8.1 Trigonometry

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

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

$$\sin A = \frac{a}{c} \quad (8.1)$$

and **cosine** as

$$\cos A = \frac{b}{c}. \quad (8.2)$$

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

$$\tan A = \frac{\sin A}{\cos A} = \frac{a}{b}. \quad (8.3)$$

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

$$\operatorname{cosec} A = \frac{1}{\sin A} \quad (8.4)$$

$$\sec A = \frac{1}{\cos A} \quad (8.5)$$

$$\cot A = \frac{1}{\tan A} \quad (8.6)$$

### §8.1.1 Pythagorean identities

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

$$\sin^2 A + \cos^2 A = 1 \quad (8.7)$$

*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. (8.7); they can be easily derived and shall be left as an exercise for the reader.

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

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

**Exercise 43**

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

**Solution.**

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

□

**Exercise 44**

Evaluate

$$\tan 10^\circ \tan 20^\circ \tan 30^\circ \cdots \tan 80^\circ.$$

**Solution.** Writing this in terms of sines and cosines, we have

$$\frac{\sin 10^\circ \sin 20^\circ \sin 30^\circ \cdots \sin 80^\circ}{\cos 10^\circ \cos 20^\circ \cos 30^\circ \cdots \cos 80^\circ}.$$

Applying  $\sin x = \cos(90^\circ - x)$  to each term in the numerator, we get

$$\frac{\cos 80^\circ \cos 70^\circ \cos 60^\circ \cdots \cos 10^\circ}{\cos 10^\circ \cos 20^\circ \cos 30^\circ \cdots \cos 80^\circ} = \boxed{1}$$

□

**§8.1.2 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 the double angle formulae:

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

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

### Multiple-angle formulae

To generalise, multiple-angle formulae 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

The sum-to-product formulae can be derived from the addition formulae.

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

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

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

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

### Product to sum

The product-to-sum formulae can be, in turn, simply observed from the sum-to-product formulae.

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

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

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

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

### §8.1.3 R-formula

It is rather difficult to immediately the amplitude of some function of a combination of trigonometric functions, given by  $f(x) = a \sin \theta + b \cos \theta$ . To do so, we combine the two trigonometric functions using the **R-formula**.

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

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

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

### §8.1.4 Sine and Cosine Rules

**Theorem 8.1** (Sine rule). Given  $\triangle ABC$ ,

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R \quad (8.8)$$

where  $R$  denotes the circumradius of  $\triangle ABC$ .

**Theorem 8.2** (Cosine rule). Given  $\triangle ABC$ ,

$$c^2 = a^2 + b^2 - 2ab \cos C \quad (8.9)$$

#### Exercise 45 (Pythagorean inequality)

Use the law of cosines to justify the statement that if  $a$ ,  $b$  and  $c$  are the sides of triangle  $\triangle ABC$  and  $a \leq b \leq c$ , then  $\triangle ABC$  is acute if  $a^2 + b^2 > c^2$  and obtuse if  $a^2 + b^2 < c^2$ .

*Proof.* From the law of cosines,

$$\cos C = \frac{c^2 - a^2 - b^2}{-2ab}.$$

If  $c^2 < a^2 + b^2$ , then the numerator of RHS is negative, so  $\cos C$  is positive and  $\angle C$  is acute. Similarly, if  $c^2 > a^2 + b^2$ ,  $\cos C$  is negative and  $\angle C$  is obtuse.  $\square$



## §8.2 Hyperbolic Functions

### §8.2.1 Basics

The three main hyperbolic functions are:

$$\sinh x = \frac{e^x - e^{-x}}{2} \quad (8.10)$$

$$\cosh x = \frac{e^x + e^{-x}}{2} \quad (8.11)$$

$$\tanh x = \frac{e^x - e^{-x}}{e^x + e^{-x}} = \frac{e^{2x} - 1}{e^{2x} + 1} \quad (8.12)$$

It is easy to see that

$$\sinh x + \cosh x = e^x$$

### §8.2.2 Reciprocals and Inverses

Again these functions all have their inverse functions:

$$\sinh^{-1} x = \operatorname{arsinh} x = \ln(x + \sqrt{x^2 + 1}) \quad (8.13)$$

$\operatorname{arsinh} x$  has domain  $x \geq 1$ .

$$\cosh^{-1} x = \operatorname{arcosh} x = \ln(x + \sqrt{x^2 - 1}) \quad (8.14)$$

$\operatorname{arcosh} x$  has domain  $x \geq 1$ .

$$\tanh^{-1} x = \operatorname{artanh} x = \frac{1}{2} \ln(1 + x) - \frac{1}{2} \ln(1 - x) \quad (8.15)$$

$\operatorname{artanh} x$  has domain  $-1 < x < 1$ .

As well as their reciprocal functions:

$$\operatorname{cosech} x = \frac{1}{\sinh x} \quad (8.16)$$

$$\operatorname{sech} x = \frac{1}{\cosh x} \quad (8.17)$$

$$\operatorname{coth} x = \frac{1}{\tanh x} \quad (8.18)$$

### §8.2.3 Identities

Hyperbolic function identities have very similar forms to the trigonometric identities.

However there is one key difference outlined in **Osborn's rule**: all the identities for the hyperbolic functions are exactly the same as the trigonometric identities, except whenever a product of two  $\sinh$  functions is present we put a minus sign in front. For example if a trigonometric formula involved a  $\sin^2 x$ , then the corresponding hyperbolic formula would contain a  $-\sinh^2 x$  instead.

Trigonometric	Hyperbolic
$\cos^2 \theta + \sin^2 \theta = 1$	$\cosh^2 x - \sinh^2 x = 1$
$\sin(A \pm B) = \sin A \cos B \pm \cos A \sin B$	$\sinh(A \pm B) = \sinh A \cosh B \pm \cosh A \sinh B$
$\cos(A \pm B) = \cos A \cos B \mp \sin A \sin B$	$\cosh(A \pm B) = \cosh A \cosh B \mp \sinh A \sinh B$
$\cos 2\theta = \cos^2 \theta - \sin^2 \theta$	$\cosh 2\theta = \cosh^2 \theta + \sinh^2 \theta$
$\sin 2\theta = 2 \sin \theta \cos \theta$	$\sinh 2\theta = 2 \sinh \theta \cosh \theta$
$1 + \tan^2 \theta = \sec^2 \theta$	$1 - \tanh^2 \theta = \operatorname{sech}^2 \theta$
$1 + \cot^2 \theta = \operatorname{cosec}^2 \theta$	$1 - \coth^2 \theta = -\operatorname{cosech}^2 \theta$

## §8.3 Cartesian Geometry

### §8.3.1 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

$$m = \frac{y_2 - y_1}{x_2 - x_1} \quad (8.19)$$

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

$$y = mx + c \quad (8.20)$$

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

$$y - y_1 = m(x - x_1) \quad (8.21)$$

For two parallel lines, they have the same gradients.

For two perpendicular lines, the product of the gradients is  $-1$ .

Distance between two points  $(x_1, y_1)$  and  $(x_2, y_2)$  is given by

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (8.22)$$

which follows easily from Pythagoras' Theorem.

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 parallel lines  $Ax + By + C_1 = 0$  and  $Ax + By + C_2 = 0$  is given by

$$d = \frac{|C_2 - C_1|}{\sqrt{A^2 + B^2}}$$

Using the **shoelace formula**, the area of a polygon is given by

The reflection of point/line about line

### §8.3.2 Conic Sections

**Conic sections** are the family of curves obtained by intersecting a cone with a plane. This intersection can take different forms according to the angle the intersecting plane makes with the side of the cone.

The standard conic sections are<sup>1</sup>

1. **circle**
2. **parabola**
3. **ellipse**
4. **hyperbola**

---

<sup>1</sup>There are also special cases, such as a point or a line, however these are trivial (sometimes called degenerate) so we shall not cover them.

Conic	Cartesian equation	Parametric equation
Circle	$x^2 + y^2 = a^2$	$x = \cos t, y = \sin t$
Parabola	$x = 4ay^2$	$x = 4at^2, y = t$
Ellipse	$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$	$x = a \cos t, y = b \sin t$
Hyperbola	$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$	$x = b \tan t, y = a \sec t$

*Remark.* The circle is a special case of the ellipse, where  $a = b$ .

## Parabolas

Given a line  $l$  and a point  $P$  in a plane, a **parabola** is defined as the set of points  $S$  in the plane such that the length  $SP$  equals the distance from  $S$  to  $l$ . The point  $P$  is known as the **focus**, and the line  $l$  is known as the **directrix**.

[figure]

The minimum point on the curve is known as the **vertex**, denoted by  $X(h, k)$ .

If we let the distance from  $X$  to  $P$  be  $a$ , we have  $P(h, k + a)$ . Similarly,  $l$  is  $a$  below  $X$  (since  $X$  is equidistant from  $P$  and  $l$ ) and thus can be described by  $y = k - a$ . (Remember,  $l$  is a horizontal line.) If we choose any point  $S = (x, y)$  on the parabola, we have  $SP = \sqrt{(x - h)^2 + (y - k - a)^2}$  and the distance from  $S$  to  $l$  is simply  $y - (k - a)$ , or  $y - k + a$ . Hence from our definition of a parabola we have

$$\sqrt{(x - h)^2 + (y - k - a)^2} = y - k - a.$$

Through some algebraic manipulation we have

$$y - k = \frac{1}{4a}(x - h)^2 \quad (8.23)$$

which is the general form of a parabola with a horizontal directrix.

Similarly, if the directrix is vertical, the equation is

$$x - h = \frac{1}{4a}(y - k)^2$$

The **axis of symmetry** is the line through the focus and the vertex.

## Ellipses

The general equation for a circle with radius  $R$  is

$$(x - h)^2 + (y - k)^2 = R^2 \quad (8.24)$$

Dividing both sides by  $R^2$ , we can write this as

$$\frac{(x - h)^2}{R^2} + \frac{(y - k)^2}{R^2} = 1.$$

Notice that we can “stretch” a circle to form an ellipse. Let  $a$  denote the “radius” in the  $x$ -direction and  $b$  denote the “radius” in the  $y$ -direction. Then the equation of an ellipse is given by

$$\frac{(x - h)^2}{a^2} + \frac{(y - k)^2}{b^2} = 1 \quad (8.25)$$

Notice we have two different “diameters” in the  $x$  and  $y$  directions. These are known as the **major axis** and **minor axis**, where the major axis is the longer of the two.

Taking two points  $F_1$  and  $F_2$ , known as **foci**, we can define an **ellipse** as the set of points  $Z$  such that  $ZF_1 + ZF_2$  is constant.

We measure the amount an ellipse is stretched away from a circle by its **eccentricity**  $e$ . Let  $c$  denote distance from centre of ellipse to either focus.

$$e = \frac{c}{a} \quad (8.26)$$

The area enclosed in an ellipse is  $ab\pi$ .

## Hyperbolas

The general form of the equation for a hyperbola is

$$\frac{(x-h)^2}{a^2} - \frac{(y-k)^2}{b^2} = 1 \quad (8.27)$$

With each hyperbola we can associate a pair of **foci**  $F_1$  and  $F_2$  so that the hyperbola is the set of all points  $S$  where  $|SF_1 - SF_2|$  is constant.

### §8.3.3 Polar Coordinates

You will already be familiar with coordinates in the form  $(x, y)$  meaning that we move  $x$  units in the  $x$ -direction (along the  $x$ -axis) and  $y$  in the  $y$ -direction (along the  $y$ -axis). These are Cartesian coordinates on the  $xy$ -plane. Although Cartesian coordinates are very useful, there are sometimes situations where it is much easier to use another coordinate system called **polar coordinates**. These are coordinates in the form  $(r, \theta)$  where  $r$  is the distance to the point from the origin and  $\theta$  is the angle in radians between the positive  $x$ -axis and the line formed by  $r$ .

From trigonometry and Pythagoras' theorem there are the following relationships:

$$x = r \cos \theta \quad y = r \sin \theta \quad r = \sqrt{x^2 + y^2}$$

We can use the formulae above to allow us to convert between polar and Cartesian coordinates.

Polar Coordinates, Parametric Equations and Vector Functions: polar coordinate system. Parametric equations are introduced. Derivatives and integrals of polar, parametric and vector functions will also be taught.

## §8.4 Linear Algebra

A matrix over a field  $F$  is a function from  $A \times B$  to  $F$ , where  $A$  and  $B$  are the sets  $A = \{1, 2, \dots, m\}$  and  $B = \{1, 2, \dots, n\}$ . A matrix is usually represented as a rectangular array of scalars from the field, such that each column belongs to the vector space  $F^m$ , where  $m$  is the number of rows. If a matrix  $A$  has  $m$  rows and  $n$  columns, its order is said to be  $m \times n$ , and it is written as  $A_{m \times n}$ .

The element in the  $i^{th}$  row and  $j^{th}$  column of  $A$  is written as  $(A)_{ij}$ . It is more often written as  $a_{ij}$ , in which case  $A$  can be written as  $[a_{ij}]$ .

### §8.4.1 Determinant

If  $A_{m \times n}$  is a matrix over  $F$  with  $m = n$ , a Determinant assigns  $A_{m \times n}$  to a member of  $F$  and is denoted

$$\text{by } |A| \text{ or } \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

It is defined recursively.

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \doteq a_{11}a_{22} - a_{21}a_{12} \quad \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \doteq \sum_{k=1}^n (-1)^{k+1} a_{1k} |A'_{1k}| \text{ where } A'_{cd} \text{ is the matrix } A \text{ with}$$

the  $c^{th}$  row and  $d^{th}$  column removed.

### §8.4.2 Transposes

Let  $A$  be  $[a_{ij}]$ . Then  $[a_{ji}]$  is said to be the transpose of  $A$ , written as  $A^T$  or simply  $A'$ . If  $A$  is over the complex field, replacing each element of  $A^T$  by its complex conjugate gives us the conjugate transpose  $A^*$  of  $A$ . In other words,  $A^* = [\overline{a_{ji}}]$

$A$  is said to be symmetric if and only if  $A = A^T$ .  $A$  is said to be hermitian if and only if  $A = A^*$ .  $A$  is said to be skew symmetric if and only if  $A = -A^T$ .  $A$  is said to be skew hermitian if and only if  $A = -A^*$ .

### §8.4.3 Matrix Product

Let  $A$  be a matrix of order  $m_1 \times m_2$  and  $B$  a matrix of order  $n_1 \times n_2$ . Then the product  $AB$  exists if and only if  $m_2 = n_1$  and in that case we define the product  $C = AB$  as the matrix of order  $m_1 \times n_2$  for which

$$(C)_{ij} = \sum_{k=1}^{n_1} (A)_{ik} (B)_{kj}$$

for all  $i$  and  $j$  such that  $1 \leq i \leq m_1$  and  $1 \leq j \leq n_2$ .

### §8.4.4 Vector spaces associated with a matrix

As already stated before, the columns of  $A$  form a subset of  $F^m$ . The subspace of  $F^m$  generated by these columns is said to be the column space of  $A$ , written as  $C(A)$ . Similarly, the transposes of the rows form a subset of the vector space  $F^n$ . The subspace of  $F^n$  generated by these is known as the row space of  $A$ , written as  $R(A)$ .

$y \in C(A)$  implies  $\exists x$  such that  $y_{m \times 1} = A_{m \times n} x_{n \times 1}$

Similarly,  $y \in R(A)$  implies  $\exists x$  such that  $y_{n \times 1} = A_{n \times m}^T x_{m \times 1}$

The set  $\{x : A_{m \times n} x_{n \times 1} = \phi\}$  forms a subspace of  $F^n$ , known as the null space  $N(A)$  of  $A$ .

### §8.4.5 Rank and nullity

The dimension of  $C(A)$  is known as the column rank of  $A$ . The dimension of  $R(A)$  is known as the row rank of  $A$ . These two ranks are found to be equal, and the common value is known as the rank  $r(A)$  of  $A$ .

The dimension of  $N(A)$  is known as the nullity  $\eta(A)$  of  $A$ .

If  $A$  is a square matrix of order  $n \times n$ , then  $r(A) + \eta(A) = n$ .



## **§8.5** Complex Numbers

## §8.6 Barycentric Coordinates

### §8.6.1 The Basics

$\triangle ABC$  is a fixed non-degenerate reference triangle with vertices in counterclockwise order. The lengths will be abbreviated  $a = BC$ ,  $b = CA$ ,  $c = AB$ . These correspond with points in the vector plane  $\vec{A}, \vec{B}, \vec{C}$ .

For arbitrary points  $P$ ,  $Q$  and  $R$ ,  $[PQR]$  denotes the signed area of  $\triangle PQR$ .

#### The Coordinates

**Definition 8.3.** Each point in the plane is assigned an ordered triple of real numbers  $P = (x, y, z)$  such that

$$\vec{P} = x\vec{A} + y\vec{B} + z\vec{C} \quad \text{and} \quad x + y + z = 1.$$

These are called the **barycentric coordinates** of the point.

These are sometimes called areal coordinates because if  $P = (x, y, z)$ , then the signed area  $[CPB]$  is equal to  $x[ABC]$ , and so on. In other words, these coordinates can be viewed as

$$P = \frac{1}{[ABC]} ([PBC], [PCA], [PAB]).$$

Of course, notice that  $A = (1, 0, 0)$ ,  $B = (0, 1, 0)$  and  $C = (0, 0, 1)$ ! This is why barycentric coordinates are substantially more suited for standard triangle geometry problems.

#### Lines

**Theorem 8.4** (Line). The equation of a line is

$$ux + vy + wz = 0$$

where  $u, v, w$  are reals.

In particular, if a line  $\ell$  passes through a vertex, say  $A$ , then

$$u(1) + v(0) + w(0) = 0 \implies u = 0.$$

So we rearrange to obtain

**Corollary 8.5** (Line through a vertex). The equation of a line passing through  $A$  is simply of the form  $y = kz$  for some constant  $k$ .

In particular, the equation for the line  $AB$  is simply  $z = 0$ , by substituting  $(1, 0, 0)$  and  $(0, 1, 0)$  into  $ux + vy + wz = 0$ .

In fact, the above techniques are already sufficient to prove both Ceva's and Menelaus's Theorem:

**Theorem 8.6** (Ceva's theorem). Let  $AD$ ,  $BE$  and  $CF$  be cevians of  $\triangle ABC$ . Then the cevians concur if and only if

$$\frac{BD}{DC} \frac{CE}{EA} \frac{AF}{FB} = 1.$$

*Proof.* Since  $D$  lies on  $BC$ , the point  $D$  has the form  $D = (0, d, 1 - d)$ . So the equation of line  $AD$  is simply

$$z = \frac{1 - d}{d}y.$$

Similarly, if we let  $E = (1 - e, 0, e)$  and  $F = (f, 1 - f, 0)$  then the lines  $BE$  and  $CF$  have equations  $x = \frac{1 - e}{e}z$  and  $y = \frac{1 - f}{f}x$  respectively.

Notice that this system of three equations is homogeneous, so we may ignore the condition that  $x+y+z = 1$  temporarily. Then it is easy to see that this equation has solutions if and only if

$$\frac{(1-d)(1-e)(1-f)}{def} = 1.$$

□

Menelaus's Theorem

### Special points

Here we give explicit forms for several special points in barycentric coordinates. It will be understood that  $(u : v : w)$  refers to the point  $\frac{1}{u+v+w}(u, v, w)$ ; that is, we are not normalizing the coordinates such that they sum to 1.

Again, the coordinates here are not homogenised!

Point	Coordinates
Centroid	$G = (1 : 1 : 1)$
Incentre	$I = (a : b : c)$
Symmedian point	$K : (a^2 : b^2 : c^2)$
Excentre	$I_a = (-a : b : c)$ , etc.
Orthocentre	$H = (\tan A : \tan B : \tan C)$
Circumcentre	$O = (\sin 2A : \sin 2B : \sin 2C)$

## §8.6.2 Standard Strategies

### Perpendicular lines

## Exercises

**Problem 88** (SMO Open 2023 Q11). Let  $ABC$  be a triangle satisfying the following conditions that  $\angle A + \angle C = 2\angle B$  and  $\frac{1}{\cos A} + \frac{1}{\cos C} = \frac{-\sqrt{2}}{\cos B}$ . Determine the value of  $\cos \frac{A-C}{2}$ .

**Solution.** Given that  $\angle A + \angle C = 2\angle B$ , we can easily see that  $\angle B = 60^\circ \implies \cos B = \frac{1}{2}$  and  $\angle A + \angle C = 120^\circ$ .

$$\begin{aligned}\frac{1}{\cos A} + \frac{1}{\cos C} &= -2\sqrt{2} \\ \cos A + \cos C &= -2\sqrt{2} \cos A \cos C\end{aligned}$$

Applying sum-to-product to the LHS and product-to-sum to the RHS gives

$$2 \cos \frac{A+C}{2} \cos \frac{A-C}{2} = -\sqrt{2} [\cos(A+C) + \cos(A-C)]$$

Let  $x = \cos \frac{A-C}{2}$ . Then since  $A+C = 120^\circ$ ,

$$\begin{aligned}x &= -\sqrt{2} \left( -\frac{1}{2} + 2x^2 - 1 \right) \\ 2\sqrt{2}x^2 + x - \frac{3}{2}\sqrt{2} &= 0 \\ x &= -\frac{3}{\sqrt{2}} \text{ (rej.)} \quad \text{or} \quad x = \frac{1}{\sqrt{2}}\end{aligned}$$

□

**Problem 89** (SMO Open 2023 Q19). Let  $ABC$  be a triangle with  $AB = c$ ,  $AC = b$  and  $BC = a$ , and satisfies the conditions  $\tan C = \frac{\sin A + \sin B}{\cos A + \cos B}$ ,  $\sin(B-A) = \cos C$  and area of triangle  $ABC$  is  $3 + \sqrt{3}$ . Determine the value of  $a^2 + c^2$ .

**Solution.**

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

Since  $A+B = 180^\circ - C$ , we then have  $C = 60^\circ$ .

$$\sin(B-A) = \cos C = \cos(180^\circ - A-B) = \sin(A+B-90^\circ)$$

which implies that  $B-A = A+B-90^\circ$ . Thus  $A = 45^\circ, B = 75^\circ$ .

Given the area of the triangle,

$$\begin{aligned}3 + \sqrt{3} &= \frac{1}{2} ac \sin B \\ &= \frac{1}{2} ac \sin(45^\circ + 30^\circ) \\ &= \frac{1}{2} ac (\sin 45^\circ \cos 30^\circ + \cos 45^\circ \sin 30^\circ) \\ &= \frac{1}{2} ac \left( \frac{1 + \sqrt{3}}{2\sqrt{2}} \right)\end{aligned}$$

Hence

$$ac = \frac{4\sqrt{2}(3 + \sqrt{3})}{1 + \sqrt{3}} = 4\sqrt{6}.$$

By Sine Rule, we have  $\frac{a}{\sin A} = \frac{c}{\sin C}$ , giving us  $\frac{a}{\sqrt{2}} = \frac{c}{\sqrt{3}}$ . Hence

$$a \left( \frac{\sqrt{3}a}{\sqrt{2}} \right) = 4\sqrt{6} \implies a^2 = 8 \quad \text{and} \quad \left( \frac{\sqrt{2}c}{\sqrt{3}} \right) = 4\sqrt{6} \implies c^2 = 12.$$

This gives us  $a^2 + c^2 = 20$ . □

**Problem 90** (SMO Open 2021 Q1). Given that  $\frac{\pi}{2} < \beta < \alpha < \frac{3\pi}{4}$ ,  $\cos(\alpha - \beta) = \frac{12}{13}$  and  $\sin(\alpha + \beta) = -\frac{3}{5}$ . Find  $\sin 2\alpha$ .

**Solution.** Note that  $\alpha - \beta$  is in the first quadrant and  $\alpha + \beta$  is in the third quadrant.

$$\begin{aligned} \sin 2\alpha &= \sin[(\alpha + \beta) + (\alpha - \beta)] \\ &= \sin(\alpha + \beta) \cos(\alpha - \beta) + \cos(\alpha + \beta) \sin(\alpha - \beta) \\ &= \left(-\frac{3}{5}\right) \left(\frac{12}{13}\right) + \left(-\frac{4}{5}\right) \left(\frac{5}{13}\right) = \boxed{-\frac{56}{65}} \end{aligned}$$

□

**Problem 91** (SMO Open 2018 Q13). Let  $\triangle ABC$  be a triangle with  $a = BC$ ,  $b = AC$  and  $c = AB$ . Given that  $a + c = 2b$ ,  $\angle A - \angle C = \frac{\pi}{3}$ , find  $\sin B$ .

**Solution.** From Sine rule,

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C}.$$

Since  $a + c = 2b$ , we have

$$2 \sin B = \sin A + \sin C$$

or

$$2 \left( 2 \sin \frac{B}{2} \cos \frac{B}{2} \right) = 2 \sin \frac{A+C}{2} \cos \frac{A-C}{2}.$$

Since  $A + B + C = \pi$ ,

$$2 \sin \frac{A+C}{2} \cos \frac{A-C}{2} = 2 \sin \frac{\pi-B}{2} \cos \frac{\pi}{3} = 2 \cos \frac{B}{2} \frac{\sqrt{3}}{2}.$$

Hence we have  $\sin \frac{B}{2} = \frac{\sqrt{3}}{4}$  and thus  $\cos \frac{B}{2} = \frac{\sqrt{13}}{4}$ . Therefore

$$\sin B = 2 \sin \frac{B}{2} \cos \frac{B}{2} = \boxed{\frac{\sqrt{39}}{8}}.$$

□

**Problem 92** (SMO Open 2013 Q9). Let  $A = \cos^2 10^\circ + \cos^2 50^\circ - \sin 40^\circ \sin 80^\circ$ . Determine the value of  $A$ .

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

Then

$$A + B = 2 - \cos 40^\circ$$

$$\begin{aligned} A - B &= (\cos^2 10^\circ - \sin 10^\circ) + (\cos^2 50^\circ - \sin^2 50^\circ) + (\cos 40^\circ \cos 80^\circ - \sin 40^\circ \sin 80^\circ) \\ &= \cos 20^\circ + \cos 100^\circ + \cos(40^\circ + 80^\circ) \\ &= \cos 20^\circ + \cos 100^\circ + \cos 120^\circ \\ &= 2 \cos 60^\circ \cos 40^\circ - \cos 60^\circ \\ &= \cos 40^\circ - \frac{1}{2} \end{aligned}$$

Adding up the two equations gives us  $2A = \frac{3}{2}$ . Hence  $A = \boxed{\frac{3}{4}}$ . □

**Problem 93** (SMO Open 2011 Q16). Determine the value of  $\frac{3}{\sin^2 20^\circ} - \frac{1}{\cos^2 20^\circ} + 64 \sin^2 20^\circ$ .

**Solution.**

$$\begin{aligned}
 & \frac{3}{\sin^2 20^\circ} - \frac{1}{\cos^2 20^\circ} + 64 \sin^2 20^\circ \\
 &= \frac{6}{1 - \cos 40^\circ} - \frac{2}{1 + \cos 40^\circ} + 32(1 - \cos 40^\circ) \quad [\text{double angle formula}] \\
 &= \frac{6(1 + \cos 40^\circ)}{1 - \cos^2 40^\circ} - \frac{2(1 - \cos 40^\circ)}{1 - \cos^2 40^\circ} - 32 \cos 40^\circ + 32 \\
 &= \frac{4(1 - 6 \cos 40^\circ + 8 \cos^3 40^\circ)}{1 - \cos^2 40^\circ} + 32 \\
 &= \frac{4(1 + 2(4 \cos^3 40^\circ - 3 \cos 40^\circ))}{1 - \cos^2 40^\circ} + 32 \\
 &= \frac{4(1 + 2 \cos 3(40^\circ))}{1 - \cos^2 40^\circ} + 32 \quad [\text{triple angle formula}] \\
 &= \frac{4\left(1 - 2\left(\frac{1}{2}\right)\right)}{1 - \cos^2 40^\circ} = \boxed{32}
 \end{aligned}$$

□

**Problem 94** (SMO Open 2009 Q1). Evaluate the expression  $\sin 10^\circ \cos 20^\circ \cos 30^\circ \cos 40^\circ$ .

**Solution.**

□

**Problem 95** (SMO Open 2009 Q6). Find the value of  $\frac{\sin 80^\circ}{\sin 20^\circ} - \frac{\sqrt{3}}{2 \sin 80^\circ}$ .

**Solution.**

□

**Problem 96** (SMO Open 2009 Q22). Evaluate  $\sum_{k=0}^{\infty} \frac{2}{\pi} \tan^{-1} \frac{2}{(2k+1)^2}$ .

**Solution.** We can rewrite the fraction as

$$\frac{2}{(2k+1)^2} = \frac{2}{4k^2 + 4k + 1} = \frac{2k+2-2k}{1+2k(2k+2)}$$

which is in the same form as  $\tan(A-B) = \frac{\tan A - \tan B}{1 + \tan A \tan B}$ . Thus

$$\tan(\tan^{-1}(2k+2) - \tan^{-1}(2k)) = \frac{2k+2-2k}{1+2k(2k+2)}.$$

Therefore

$$\begin{aligned}
 \sum_{k=0}^{\infty} \frac{2}{\pi} \tan^{-1} \frac{2}{(2k+1)^2} &= \frac{2}{\pi} \sum_{k=0}^{\infty} \tan^{-1} \tan(\tan^{-1}(2k+2) - \tan^{-1}(2k)) \\
 &= \frac{2}{\pi} \sum_{k=0}^{\infty} (\tan^{-1}(2k+2) - \tan^{-1}(2k)) \\
 &= \frac{2}{\pi} \lim_{n \rightarrow \infty} \sum_{k=0}^n (\tan^{-1}(2k+2) - \tan^{-1}(2k)) \\
 &= \frac{2}{\pi} \lim_{n \rightarrow \infty} (-\tan^{-1} 0 + \tan^{-1}(2n+2)) \quad [\text{telescoping sum}] \\
 &= \frac{2}{\pi} \lim_{n \rightarrow \infty} \tan^{-1}(2n+2) \\
 &= \frac{2}{\pi} \left(\frac{\pi}{2}\right) = \boxed{1}
 \end{aligned}$$

□

**Problem 97** (SMO Open 2006 Q16). Find the value of

$$\frac{400(\cos^5 15^\circ + \sin^5 15^\circ)}{\cos 15^\circ + \sin 15^\circ}.$$

**Solution.**

$$\begin{aligned} & \frac{400(\cos^5 15^\circ + \sin^5 15^\circ)}{\cos 15^\circ + \sin 15^\circ} \\ &= 400(\cos^4 15^\circ - \cos^3 15^\circ \sin 15^\circ + \cos^2 15^\circ \sin^2 15^\circ - \cos 15^\circ \sin^3 15^\circ + \sin^4 15^\circ) \\ &= 400(\cos^4 15^\circ + \sin^4 15^\circ - \cos 15^\circ \sin 15^\circ + \cos^2 15^\circ \sin^2 15^\circ) \\ &= 400((\cos^2 15^\circ + \sin^2 15^\circ)^2 - \cos^2 15^\circ \sin^2 15^\circ - \cos 15^\circ \sin 15^\circ) \\ &= 400\left[1 - \left(\frac{1}{2} \sin 30^\circ\right)^2 - \left(\frac{1}{2} \sin 30^\circ\right)\right] = \boxed{275} \end{aligned}$$

□

**Problem 98** (SMO Open 2018). Find the value of

$$\frac{\tan 40^\circ \tan 60^\circ \tan 80^\circ}{\tan 40^\circ + \tan 60^\circ + \tan 80^\circ}.$$

**Solution.** We can show, more generally, that an acute  $\triangle ABC$ ,

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

We see that

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

Hence proven.

□

**Problem 99.** 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.**

$$\begin{aligned} \sin A + \sin B + \sin C &= 2 \sin \frac{A+B}{2} \cos \frac{A-B}{2} + \sin C \\ &= 2 \sin \left( 90^\circ - \frac{C}{2} \right) \cos \frac{A-B}{2} + 2 \sin \frac{C}{2} \cos \frac{C}{2} \\ &= 2 \cos \frac{C}{2} \cos \frac{A-B}{2} + 2 \sin \frac{C}{2} \cos \frac{C}{2} \\ &= 2 \cos \frac{C}{2} \left( \cos \frac{A-B}{2} + \cos \frac{A+B}{2} \right) \\ &= 2 \cos \frac{C}{2} \left( 2 \cos \frac{A}{2} \cos \frac{B}{2} \right) = 4 \cos \frac{A}{2} \cos \frac{B}{2} \cos \frac{C}{2} \end{aligned}$$

and

$$\begin{aligned} \cos A + \cos B + \cos C &= 2 \cos \frac{A+B}{2} \cos \frac{A-B}{2} + \cos C \\ &= 2 \cos \left( 90^\circ - \frac{C}{2} \right) \cos \frac{A-B}{2} + \cos 2 \left( \frac{C}{2} \right) \\ &= 2 \sin \frac{C}{2} \cos \frac{A-B}{2} + \left( 1 - 2 \sin^2 \frac{C}{2} \right) \\ &= 1 + 2 \sin \frac{C}{2} \left( \cos \frac{A-B}{2} - \sin \frac{C}{2} \right) \\ &= 1 + 2 \sin \frac{C}{2} \left( \cos \frac{A-B}{2} - \sin \left( 90^\circ - \frac{A+B}{2} \right) \right) \\ &= 1 + 2 \sin \frac{C}{2} \left( \cos \frac{A-B}{2} - \cos \frac{A+B}{2} \right) \\ &= 1 + 2 \sin \frac{C}{2} \left( 2 \sin \frac{A}{2} \sin \frac{B}{2} \right) = 1 + 4 \sin \frac{A}{2} \sin \frac{B}{2} \sin \frac{C}{2} \end{aligned}$$

This gives us the following simultaneous equations.

$$\begin{cases} \frac{\sin A + \sin B + \sin C}{\cos A + \cos B + \cos C} = \frac{4 \cos \frac{A}{2} \cos \frac{B}{2} \cos \frac{C}{2}}{1 + 4 \sin \frac{A}{2} \sin \frac{B}{2} \sin \frac{C}{2}} = \frac{12}{7} \\ \sin A \sin B \sin C = 8 \left( \sin \frac{A}{2} \sin \frac{B}{2} \sin \frac{C}{2} \right) \left( \cos \frac{A}{2} \cos \frac{B}{2} \cos \frac{C}{2} \right) = \frac{12}{15} \end{cases}$$

Solving, we get

$$\begin{cases} \sin \frac{A}{2} \sin \frac{B}{2} \sin \frac{C}{2} = \frac{1}{10} \\ \cos \frac{A}{2} \cos \frac{B}{2} \cos \frac{C}{2} = \frac{3}{5} \end{cases}$$

We see that

$$\begin{aligned} \sin \frac{C}{2} &= \cos \frac{A+B}{2} = \cos \frac{A}{2} \cos \frac{B}{2} - \sin \frac{A}{2} \sin \frac{B}{2} \\ \sin^2 \frac{C}{2} \cos \frac{C}{2} &= \frac{3}{5} \sin \frac{C}{2} - \frac{1}{10} \cos \frac{C}{2} \end{aligned}$$



Let  $t = \cos \frac{C}{2}$ . Then we get a quadratic equation. Solving it gives us

$$t = \sqrt{\frac{1}{2}}, \quad t = \sqrt{\frac{4}{5}}, \quad t = \sqrt{\frac{3}{10}}.$$

Hence  $\boxed{s_1 = 1, s_2 = \frac{4}{5}, s_3 = \frac{3}{5}}.$

□

**Problem 100** (MAT). Evaluate

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

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

Rewriting and pairing up terms gives us

$$\begin{aligned} & \sin^2 1^\circ + \sin^2 2^\circ + \cdots + \cos^2 2^\circ + \cos^2 1^\circ + 1 \\ &= (\sin^2 1^\circ + \cos^2 1^\circ) + \cdots + (\sin^2 44^\circ + \cos^2 44^\circ) + \sin^2 45^\circ + 1 \\ &= 44(1) + \frac{1}{2} + 1 = \boxed{45\frac{1}{2}} \end{aligned}$$

□

**Problem 101.** Evaluate  $\sin 10^\circ \sin 30^\circ \sin 50^\circ \sin 70^\circ$ .

**Solution.**

$$\begin{aligned} \sin 10^\circ \sin 30^\circ \sin 50^\circ \sin 70^\circ &= \frac{1}{4} \sin 10^\circ (2 \sin 70^\circ \sin 50^\circ) \\ &= \frac{1}{4} \sin 10^\circ (\cos 20^\circ - \cos 120^\circ) \\ &= \frac{1}{4} \sin 10^\circ \left( \cos 20^\circ + \frac{1}{2} \right) \\ &= \frac{1}{8} (2 \sin 10^\circ \cos 20^\circ) + \frac{1}{8} \sin 10^\circ \\ &= \frac{1}{8} (\sin 30^\circ - \sin 10^\circ) + \frac{1}{8} \sin 10^\circ \\ &= \frac{1}{16} \end{aligned}$$

□

**Problem 102.** Let  $A, B, C$  be angles of a triangle. Determine the maximum value of  $\sin A + \sin B + \sin C$ .

**Solution.** WLOG, assume  $A \leq B \leq C$ , then  $A \leq 60^\circ$ .  $\sin 3A \geq 0$ ,  $\sin 3B \geq -1$ ,  $\sin 3C \geq -1$  thus

$$\sin 3A + \sin 3B + \sin 3C \geq -2.$$

Let  $B = C$ , then  $B = C = 90^\circ - \frac{A}{2}$ . If  $A$  is very small,  $B$  and  $C$  are close to  $90^\circ$ , thus  $\sin 3A + \sin 3B + \sin 3C$  is close to  $-2$ .

Now we want to find an upper bound. When  $A = 20^\circ, B = 20^\circ, C = 140^\circ$ . Let  $X = 3A, Y = 3B, Z = 3(C - 120^\circ)$ , then  $X + Y + Z = 180^\circ$  and

$$\sin 3A + \sin 3B + \sin 3C = \sin X + \sin Y + \sin Z.$$

Suppose that  $X, Y, Z$  satisfy the condition that  $X + Y + Z = 180^\circ$  such that  $\sin X + \sin Y + \sin Z$  has max value. We can then show that  $X = Y = Z$ .

Assume that  $X \leq Y \leq Z$ . If  $X \leq Z$ , then

$$\sin X + \sin Z = 2 \sin \frac{X+Z}{2} \cos \frac{X-Z}{2} < 2 \sin \frac{X+Z}{2}$$

implying that

$$\sin X + \sin Y + \sin Z < \sin \frac{X+Z}{2} + \sin Y + \sin \frac{X+Z}{2}$$

which contradicts the assumption that  $\sin X + \sin Y + \sin Z$  has max value.

Hence  $X = Y = Z = 60^\circ$ ,  $A = 20^\circ, B = 20^\circ, C = 140^\circ$ . Thus  $\sin 3A + \sin 3B + \sin 3C = \frac{3\sqrt{3}}{2}$ . □

# 9 Transformations

Homothety Rotation and Reflection Circular inversion Projective geometry - Brocard's Theorem, Pascal's Theorem Spiral similarity

## §9.1 Inversive Geometry

In what follows, we consider the usual Euclidean plane  $\mathbf{R}^2$  with an additional “point at infinity”, which we denote as  $\infty$ . We consider every line to pass through this point  $\infty$ .

### §9.1.1 Definition and First Properties

**Definition 9.1.** For a circle  $\Gamma$  with center  $O$  and radius  $r > 0$ , an **inversion** around  $\Gamma$  is a map that sends each point  $P$  to be a point  $P^*$  as follows:

- If  $P = \infty$ , then  $P^* = O$ .
- If  $P = O$ , then  $P^* = \infty$ .
- For any other point  $P$ , we choose  $P^*$  to be the unique point satisfying

$$OP \cdot OP^* = r^2.$$

We immediately identify some properties of the inversion.

**Proposition 9.2.** Inversion is an involution:  $(P^*)^* = P$ .

**Proposition 9.3.** The point  $P$  lies on  $\Gamma$  if and only if  $\Gamma$  lies on  $\Gamma$ .

In the case where  $P$  lies outside the circle, there is also a geometric interpretation.

**Theorem 9.4.** Let  $P$  be a point outside  $\Gamma$  and suppose  $PA, PB$  are tangents to the circle. Then  $P^*$  coincides with the midpoint of  $AB$ .

### §9.1.2 Generalised Lines and Circles

We continue to fix a circle  $\Gamma$  with center  $O$  and radius  $r$ , through which we will perform inversions.

If  $\ell$  is a line, by its inverse  $\ell^*$  we mean the set

$$\ell^* = \{P^* \mid P \in \ell\}.$$

Similarly for a circle  $\gamma$  its inverse is the set

$$\gamma^* = \{P^* \mid P \in \gamma\}.$$

The main result of this section is that inverses of lines and circles are themselves lines and circles. We check this using the following propositions.

### §9.1.3 Inversion Distance Formula

## §9.2 Projective Geometry

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

### §9.2.1 Homothety

One way to capture at once a lot of information that normally would form a similar triangles argument is through the notion of homothety.

**Definition 9.5.** A **homothety**  $h$  is a transformation defined by a center  $O$  and a nonzero real number  $k$  (not necessarily positive). It sends a point  $P$  to another point  $h(P)$ , multiplying the distance from  $O$  by  $k$ .

*Remark.*  $k$  can be negative; in that case,  $O$  will lie between  $P$  and  $h(P)$ .

It is easy to see that homothety preserves similarity. Homothety also preserves many things, including but not limited to tangency, angles (both vanilla and directed), circles, and so on. They do not preserve length, but they work well enough: the lengths are simply all multiplied by  $k$ .

**Proposition 9.6.** Given non-congruent parallel segments  $AB$  and  $XY$ , there is a unique homothety sending  $A$  to  $X$  and  $B$  to  $Y$ .

*Proof.* Since  $AB \neq XY$ , the quadrilateral  $ABYX$  is not a parallelogram, and we may take  $O$  to be the intersection of lines  $AX$  and  $BY$ . Then  $\triangle OAB \sim \triangle OXY$ .

The common scale factor is then the signed quotient  $\frac{OX}{OA} = \frac{OY}{OB}$ . □

This is often used with triangles. A consequence of this is the following useful lemma.

**Corollary 9.7.** Let  $ABC$  and  $XYZ$  be non-congruent triangles such that  $AB \parallel XY$ ,  $BC \parallel YZ$ , and  $CA \parallel ZX$ . Then lines  $AX$ ,  $BY$ ,  $CZ$  concur at some point  $O$ , and  $O$  is a center of a homothety mapping  $\triangle ABC$  to  $\triangle XYZ$ .

## §9.3 Complete Quadrilaterals

### §9.3.1 Spiral Similarity

### §9.3.2 Miquel Point of Cyclic Quadrilateral

## Exercises

# 10 Miscellaneous

## §10.1 Construction

**Constructions** with straight edge and compass (i.e. the ability to mark off segments, draw circles and arcs, and draw straight lines) are a branch of geometry that rely on the use of basic geometrical axioms to create various figures in the Euclidean plane.

A **compass** is a tool that can draw circles and arcs of circles.

A **straightedge** is an unmarked ruler that can draw line segments.

No other tools are allowed in a construction. However, the two basic tools alone can allow one to:

1. Duplicate a line segment.
2. Copy an angle. Hence, construct a parallel line to line  $l$  through point  $A$  not on  $l$ .
3. Construct an angle bisector.
4. Construct a perpendicular bisector.
5. Construct a perpendicular from a point to a line.
6. Construct a triangle with side lengths  $a$ ,  $b$ , and  $c$ .
7. Partition a line segment into  $n$  different parts.
8. Construct length  $ab$  given lengths  $a$  and  $b$  and unit segment 1.
9. Construct  $a/b$  and  $\sqrt{ab}$ . Hence, construct  $\sqrt{a}$  given unit segment 1.
10. Construct a tangent to a circle.
11. Construct common tangents to two circles.
12. Construct a parallelogram with side lengths  $a$  and  $b$ . Hence, construct a square with side length  $a$ .

These basic constructions should be easy to accomplish. Now, try these:

13. Construct a line passing through a point  $P$  parallel to line  $l$ .
14. Construct a square circumscribed on a circle.
15. Construct a regular hexagon inside a given circle.
16. Construct the inverse of a point  $P$  with respect to circle  $C$ . In other words, construct the unique point  $P'$  on ray  $CP$  such that  $CP * CP'$  equals the square of the radius of  $C$ . Hence or otherwise, construct the inverse of a point  $P$  using compasses only.
17. Construct a square, all of whose vertices are on a given triangle.
18. Construct a regular pentagon.
19. Construct the radical axis of two circles.
20. Given two chords of a circle intersecting in the interior of the circle, construct another circle tangent to the chords and internally tangent to the original circle.



21. Construct  $\sin C, \cos C, \tan C$  given unit segment 1 and acute angle  $C$ .
22. Construct a right triangle with the given lengths of a hypotenuse and altitude to the hypotenuse.
23. Construct  $15^\circ, 30^\circ, 45^\circ, 60^\circ, 75^\circ$  angles. Hence or otherwise, construct a right triangle whose median to the hypotenuse is equal to the geometric mean of the legs. (Source: IMO)

## §10.2 Locus

**Locus** is a set of points satisfying a certain geometric condition.

Examples

A circle can be defined as the locus of all points that are a certain distance from a given center.

If we have a line  $l$  and a point  $P$ , a parabola is the locus of all points  $S$  such that  $SP =$  the distance from  $S$  to  $l$ .

If we have two points  $A$  and  $B$ , an ellipse is the locus of all points  $S$  such that  $SA + SB$  is equal to a given constant.

Given two points  $A$  and  $B$  and a constant  $k$ , the locus of all points  $P$  that satisfy  $\frac{PA}{PB} = k$  is a circle (sometimes called an Apollonius circle).

## §10.3 3D Geometry

A very common technique for approaching 3D Geometry problems is to make it 2D. We can do this by looking at certain cross-section(s) of the diagram one at a time.

## §10.4 Geometric Inequalities

A geometric inequality is an inequality involving various measures (angles, lengths, areas, etc.) in geometry.

**Theorem 10.1** (Triangle inequality). The sum of the lengths of any two sides of a nondegenerate triangle is greater than the length of the third side.

This inequality is particularly useful and shows up frequently on Intermediate level geometry problems. It also provides the basis for the definition of a metric space in analysis.

**Theorem 10.2** (Pythagorean inequality). For an acute triangle with sides of length  $a \leq b \leq c$ ,  $a^2 + b^2 > c^2$ . 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 Law of Cosines, although it is also possible to prove without using trigonometry.

**Theorem 10.3** (Isoperimetric inequality). If a figure in the plane has area  $A$  and perimeter  $P$ , then  $\frac{4\pi A}{P^2} \leq 1$ . This means that given a perimeter  $P$  for a plane figure, the circle has the largest area. Conversely, of all plane figures with area  $A$ , the circle has the least perimeter.

**Trigonometric Inequalities** In  $\triangle ABC$ ,  $\sin A + \sin B + \sin C \leq \frac{3\sqrt{3}}{2}$ . Proof:  $\sin$  is a concave function from  $0 \leq \theta \leq \pi$ . Therefore we may use Jensen's inequality:  $\frac{\sin A + \sin B + \sin C}{3} \leq \sin\left(\frac{A+B+C}{3}\right) = \frac{\sqrt{3}}{2}$

Alternatively, we may use a method that can be called "perturbation". If we let all the angles  $A, B, C$  be equal, we prove that if we make one angle greater and the other one smaller, we will decrease the total value of the expression. To prove this, all we need to show is if  $0 < A, B < 180$ , then  $\sin(A+B) + \sin(A-B) < 2\sin A$ . This inequality reduces to  $2\sin A \cos B < 2\sin A$ , which is equivalent to  $\cos B < 1$ . Since this is always true for  $0 < B < 180$ , this inequality is true. Therefore, the maximum value of this expression is when  $A = B = C = 60$ , which gives us the value  $\sin A + \sin B + \sin C = \frac{3\sqrt{3}}{2}$ .

Similarly, in  $\triangle ABC$ ,  $\cos A + \cos B + \cos C \leq \frac{3}{2}$ .

**Theorem 10.4** (Euler's inequality).  $R \geq 2r$  with equality when  $\triangle ABC$  is equilateral, where  $R$  and  $r$  denote the circumradius and inradius of triangle  $ABC$ , respectively.

Proof: The distance  $d$  from the circumcenter and incenter of a triangle can be expressed as  $d^2 = R(R-2r)$ , meaning  $R-2r \geq 0$  or equivalently  $R \geq 2r$  with equality if and only if the incenter equals the circumcenter, namely the triangle is equilateral.

**Theorem 10.5** (Ptolemy's inequality). Ptolemy's inequality states that for any quadrilateral  $ABCD$ ,  $AB \cdot CD + BC \cdot DA \geq AC \cdot BD$  with equality when quadrilateral  $ABCD$  is cyclic.

First Proof: Let  $P$  be the point such that  $\triangle ABC \sim \triangle ADP$ . By SAS we also have that  $\triangle ABD \sim \triangle ACP$ . By the triangle inequality,  $PD + DC \geq PC$ . calculating the lengths, we obtain an equivalent statement:  $BC \frac{DA}{AB} + CD \geq BD \frac{AC}{AB}$ . Multiplying by  $AB$  we get the desired result with equality when  $P$  is on  $DC$ . This happens when  $\angle ADP + \angle ADC = 180^\circ$ . But  $\angle ABC \cong \angle ADP$  so  $\angle ABC + \angle ADC = 180^\circ$ , or quadrilateral  $ABCD$  is cyclic.

Second Proof (using inversion): Let the inversion  $\psi(A, 1)$  map  $B, C$  and  $D$  to  $B', C'$  and  $D'$  respectively. We then have

$$\begin{aligned} B'C' &= \frac{BC}{AB \cdot AC} \\ C'D' &= \frac{CD}{AC \cdot AD} \\ B'D' &= \frac{BD}{AB \cdot AD}. \end{aligned}$$

By the triangle inequality, we have

$$B'C' + C'D' \geq B'D' \implies \frac{BC}{AB \cdot AC} + \frac{CD}{AC \cdot AD} \geq \frac{BD}{AB \cdot AD}.$$

By multiplying  $AB \cdot AC \cdot AD$  on both sides we get the desired result with equality when  $B'C'D'$  is collinear, implying either  $ABCD$  is cyclic or collinear.

**Theorem 10.6** (Erdős–Mordell inequality). If  $P$  lies in  $ABC$  then  $PA + PB + PC \geq 2(PD + PE + PF)$  where  $D, E, F$  are the foot of the altitudes from  $P$  to  $AB, BC$ , and  $AC$ .

Proof: First, we prove a lemma.

Mordell's Lemma:  $PA \sin A \geq PE \sin C + PF \sin B$

Proof of Lemma: Let  $M$  and  $N$  be the projections of  $E$  and  $F$  onto line  $PD$ .

Note that  $AFPE$  is cyclic with diameter  $AP$ . By ELOS,  $\frac{EF}{\sin A} = 2R = AP \implies EF = AP \sin A$ . Since  $BDPF$  is cyclic, we have that  $B$  and  $\angle FPD$  are supplementary. Since  $MPD$  is a line,  $B = \angle FPM$ . This means that  $\sin B = \sin FPN = \frac{FN}{FP} \implies FN = PF \sin B$ . Similarly,  $EM = PE \sin C$ . So the problem is reduced to proving that  $EF \geq FN + EM$  but this is obvious by the Pythagorean Theorem. ■

Now the rest of the problem is straightforward. We know that

$$\begin{aligned} PA &\geq PE \frac{\sin C}{\sin A} + PF \frac{\sin B}{\sin A} \\ PB &\geq PF \frac{\sin A}{\sin B} + PD \frac{\sin C}{\sin B} \\ PC &\geq PD \frac{\sin B}{\sin C} + PE \frac{\sin A}{\sin C}. \end{aligned}$$

Adding these cyclically implies

$$PA + PB + PC \geq PD \left( \frac{\sin B}{\sin C} + \frac{\sin C}{\sin B} \right) + PE \left( \frac{\sin C}{\sin A} + \frac{\sin A}{\sin C} \right) + PF \left( \frac{\sin A}{\sin B} + \frac{\sin B}{\sin A} \right).$$

By AM-GM,  $PA + PB + PC \geq 2(PD + PE + PF)$  with equality when  $ABC$  is equilateral and  $P$  is the center of it.

Part IV

**Combinatorics**

# 11 Combinatorics

## §11.1 Basic Identities

**Definition 11.1.** A **permutation** is an arrangement of objects in a specific order. The number of ways to permute  $k$  of  $n$  distinct items is given by

$${}^n P_k = \frac{n!}{(n-k)!}. \quad (11.1)$$

**Definition 11.2.** A **combination** is a selection of objects without regard to the order. The number of ways to choose  $k$  of  $n$  distinct items is given by

$${}^n C_k = \binom{n}{k} = \frac{n!}{k!(n-k)!}. \quad (11.2)$$

### §11.1.1 Pascal's Triangle

**Proposition 11.3.**

$$\binom{n}{k} = \binom{n}{n-k} \quad (11.3)$$

*Proof.* This is evident by means of expansion. □

Each number in the Pascal's triangle is a binomial coefficient.

**Proposition 11.4** (Pascal's and hockey-stick identities).

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1} \quad (11.4)$$

$$\sum_{r=k}^n \binom{r}{k} = \binom{n+1}{k+1} \quad (11.5)$$

$$\sum_{r=0}^n \binom{k+r}{r} = \binom{n+k+1}{n} \quad (11.6)$$

*Proof.* These can be easily proven through observation of Pascal's triangle. □

**Proposition 11.5.**

$$\binom{n}{k} \binom{k}{m} = \binom{n}{m} \binom{n-m}{k-m} \quad (11.7)$$

*Proof.* This can be easily proven via expansion. □

**Lemma 11.6** (Vandermonde's Identity).

$$\sum_{r=0}^k \binom{m}{r} \binom{n}{k-r} = \binom{m+n}{k} \quad (11.8)$$

### §11.1.2 Binomial Theorem

**Theorem 11.7** (Binomial Theorem). For  $n \in \mathbf{Z}^+$  and  $a, b \in \mathbf{R}$ ,

$$\begin{aligned} (a+b)^n &= \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \\ &= \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n} b^n \end{aligned} \quad (11.9)$$

*Proof.* This can be proven using mathematical induction.  $\square$

**Corollary 11.8.** For all  $n \in \mathbf{Z}^+$ , the following equality holds:

$$2^n = \sum_{k=0}^n \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} \quad (11.10)$$

*Proof.* The above identity simply follows by  $a = b = 1$ .  $\square$

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  $A_0, A_1, \dots, A_n$  partition  $2^A$ , which means the following equalities hold:

$$\begin{aligned} 2^n &= |2^A| = |A_0| + |A_1| + \cdots + |A_n| \\ &= \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = \sum_{k=0}^n \binom{n}{k} \end{aligned}$$

In other words, every subset of  $A$  has a size in  $\{0, 1, \dots, n\}$ , so to count the number of subsets of  $A$ , we can count the number of subsets of each size over all possible sizes.  $\square$

**Proposition 11.9.**

$$\sum_{k=0}^n k \binom{n}{k} = n 2^{n-1} \quad (11.11)$$

*Proof.* Writing the sum backwards yields

$$S = n \binom{n}{n} + (n-1) \binom{n}{n-1} + (n-2) \binom{n}{n-2} + \cdots + \binom{n}{1},$$

which after applying the identity  $\binom{n}{k} = \binom{n}{n-k}$  to each term in the sum becomes

$$S = n \binom{n}{0} + (n-1) \binom{n}{1} + (n-2) \binom{n}{2} + \cdots + \binom{n}{n-1}.$$

We add this to the original series to get

$$2S = n \binom{n}{0} + n \binom{n}{1} + n \binom{n}{2} + \cdots + n \binom{n}{n-1} + n \binom{n}{n} = n 2^n.$$

Thus  $S = n 2^{n-1}$ .  $\square$

$$\sum_{k=0}^n k^2 \binom{n}{k} = n(n+1) 2^{n-2} \quad (11.12)$$

## §11.2 Counting Problems

### §11.2.1 Addition and Multiplication Principles

**Example 11.10.**

- 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  $\binom{m+1}{2}\binom{n+1}{2}$ .
- 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, is  $\binom{n+k-1}{k}$ .
- Number of paths from  $(0,0)$  to  $(m,n)$  going 1 unit rightwards or upwards is  $\binom{m+n}{n}$ .
- 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  $\binom{n+k-1}{k-1}$ .

### §11.2.2 Some Techniques

**Complementary counting:** count what you don't want, then subtract that from the total number of possibilities.

If  $B$  is a subset of  $A$ ,

$$|B| = |A| - |B^c|$$

where  $B^c$  is the complement of  $B$ .

**Constructive counting:** count the total possibilities of each case/step, then assemble there to enumerate the full set

### §11.2.3 Bijection Principle

A mapping  $f$  from  $A$  to  $B$ , denoted by  $f : A \rightarrow B$ , is a rule which assigns each element  $a \in A$  to a unique element  $f(a) \in B$ .  $f(a)$  is called the image of  $a$ ;  $a$  is the preimage of  $f(a)$ .

*Remark.* The codomain  $B$  need not be the range of  $f$ ; in fact the range is a subset of  $B$ .

We say that a mapping is injective (or one to one) if

$$\forall x, y \in A, \quad f(x) = f(y) \implies x = y$$

where each element in  $A$  corresponds to a distinct image in  $B$ .

We say that a mapping is surjective (or onto) if

$$\forall b \in B, \exists a \in A \text{ s.t. } f(a) = b$$

where all elements in the codomain have a pre-image.

Let  $A$  and  $B$  be finite sets. Note that if there exists an injective mapping from  $A$  to  $B$ , clearly  $|A| \leq |B|$ ; if there exists a surjective mapping from  $A$  to  $B$ , then  $|A| \geq |B|$ .

A bijective mapping is both injective and surjective. Thus we have

**Theorem 11.11** (Bijection Principle). Let  $A$  and  $B$  be finite sets. If there exists a bijection  $f : A \rightarrow B$  then

$$|A| = |B|.$$

By establishing a bijection, we can enumerate  $B$  (easier to count) in order to enumerate  $A$  (difficult to count).

Employing the Bijection Principle:

1. State two sets  $A$  and  $B$ , one of which should be the set that you are trying to enumerate in original problem.
2. Define a mapping from  $A$  to  $B$ , i.e. describe how a general element in  $A$  is mapped to an element in  $B$ .
3. Show that the mapping defined is bijective.
4. Apply the Bijection Principle, i.e.  $|A| = |B|$ .

#### Exercise 46

In a  $5 \times 3$  grid, points  $P$  and  $Q$  are located at the bottom left corner and top right corner respectively. An ant wants to crawl from  $P$  to  $Q$ . If it can only crawl along the segments of the grid, how many shortest routes does it have to get from  $P$  to  $Q$ ?

**Solution.** Let  $A$  be the set of all possible shortest  $P - Q$  routes and  $B$  be the set of all 8-digit binary sequences with three 1's. We define a mapping  $f : A \rightarrow B$  as follows:

for each shortest  $P - Q$  route  $\alpha \in A$ ,

$$f(\alpha) = a_1 a_2 \cdots a_8$$

where

$$a_i = \begin{cases} 0 & \text{if } i\text{-th step is rightward} \\ 1 & \text{if } i\text{-th step is upward} \end{cases}.$$

Since  $f : A \rightarrow B$  is a bijection, thus by the Bijection Principle,

$$\text{number of shortest } P - Q \text{ routes} = |A| = |B| = \binom{8}{3} = 56.$$

Also note that

- since each distinct shortest  $P - Q$  is mapped by  $f$  to a distinct 8-digit binary sequence with three 1's,  $f$  is injective;
- for each 8-digit binary sequence with three 1's, there is a corresponding shortest  $P - Q$  route so  $f$  is surjective.

□

#### Exercise 47

Find the number of divisors of 12600.

**Solution.** To solve this problem of counting, we make use of the Fundamental Theorem of Arithmetic:

Every natural number  $n \geq 2$  can be factorised as  $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$  for some  $p_1, p_2, \dots, p_k$  and for some natural numbers  $m_1, m_2, \dots, m_k$ . Such a factorisation is unique if the order of primes is disregarded.

Prime decomposition of 12600 gives  $12600 = 2^3 \times 3^2 \times 5^2 \times 7^1$ .

Thus a number  $d$  divides 12600 if and only if it can be expressed as

$$d = 2^p \times 3^q \times 5^r \times 7^s$$

where  $p, q, r, s$  are positive integers such that  $0 \leq p \leq 3, 0 \leq q \leq 2, 0 \leq r \leq 2, 0 \leq s \leq 1$ .

Let  $A = \{\text{divisors of } 12600\}$  and  $B = \{(p, q, r, s) \mid 0 \leq p \leq 3, 0 \leq q \leq 2, 0 \leq r \leq 2, 0 \leq s \leq 1\}$ . We define a mapping  $f : A \rightarrow B$  as follows:  $\forall d \in A, d = 2^p \times 3^q \times 5^r \times 7^s$ ,

$$f(d) = (p, q, r, s).$$

Since  $f : A \rightarrow B$  is a bijection, thus by the Bijection Principle,

$$|A| = |B| = 4 \times 3 \times 3 \times 2 = 72.$$

□

#### Exercise 48

Consider 5 distinct points lying on the circumference of a circle, where any three chords formed by connecting two points are not concurrent.

How many points of intersections of chords are there within the circle?

**Solution.** Let  $C$  be the set of such points of intersection,  $D$  be the set of 4-element subsets of  $\{1, 2, 3, 4, 5\}$ .

For each point  $\beta \in C$ , define  $g(\beta) = \{p, q, r, s\}$ , where  $p, q, r, s$  are points on the circumference such that they are the endpoints of the two chords that intersect to give  $\beta$ . Hence  $g$  is a mapping from  $C$  to  $D$ .

Every pair of chords, with endpoints  $p, q, r, s$ , that intersect will result in one point of intersection, thus  $g$  is surjective. Also, 2 distinct points of intersection will not have the same pair of chords, so  $g$  is injective. Hence  $g : C \rightarrow D$  is a bijection.

Once we have done that, we know  $|C| = |D|$ . Hence  $|C| = |D| = \binom{5}{4} = 5$ .

□

### §11.2.4 Principle of Inclusion–Exclusion

The **Principle of Inclusion–Exclusion** (PIE) 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

**Theorem 11.12** (Principle of Inclusion–Exclusion).

$$\begin{aligned} \left| \bigcup_{i=1}^n A_i \right| = & \sum_{i=1}^n |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ & - \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|. \end{aligned} \quad (11.13)$$

#### Exercise 49

Find the number of integers from the set  $\{1, 2, \dots, 1000\}$  which are divisible by 3 or 5.



**Solution.** Let

$$\begin{aligned} S &= \{1, 2, \dots, 1000\} \\ A &= \{x \in S \mid x \text{ is divisible by } 3\} \\ B &= \{x \in S \mid x \text{ is divisible by } 5\} \end{aligned}$$

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  $\{1, 2, \dots, n\}$  which are divisible by  $k$  is  $\left\lfloor \frac{n}{k} \right\rfloor$ .

Hence we have

$$\begin{aligned} |A \cup B| &= |A| + |B| - |A \cap B| \\ &= \left\lfloor \frac{1000}{3} \right\rfloor + \left\lfloor \frac{1000}{5} \right\rfloor - \left\lfloor \frac{1000}{15} \right\rfloor \\ &= 333 + 200 - 66 = \boxed{467} \end{aligned}$$

□

### Exercise 50

By using the Principle of Inclusion and Exclusion, show that the number of ways to distribute  $r$  distinct objects into  $n$  distinct boxes, where  $r \geq n$ , where no boxes are empty, is given by

$$\sum_{i=0}^n (-1)^i \binom{n}{i} (n-i)^r.$$

**Solution.**

□

### Exercise 51

Using the Principle of Inclusion and Exclusion, show that the number of non-surjective mappings from  $\mathbf{N}_n$  to  $\mathbf{N}_m$  where  $n \geq m \geq 2$  is given by

$$\sum_{k=p}^q (-1)^{k+1} \binom{m}{k} (m-k)^n$$

for some constants  $p$  and  $q$  to be determined, where  $\mathbf{N}_k = \{1, 2, \dots, k\}$ .

A quaternary sequence is a sequence containing only the digits '0', '1', '2' and '3'. Hence use the Bijection Principle to find the number of six-digit quaternary sequences that do not contain at least one of the digits '0', '1', '2' and '3'.

**Solution.** Let  $A_i$  be the set of mappings from  $\mathbf{N}_n$  to  $\mathbf{N}_m \setminus \{i\}$ .

We want to find  $\left| \bigcup_{i=1}^m A_i \right|$ .

Note that

$$\sum_{i=1}^m |A_i| = \binom{m}{1} (m-1)^n, \quad \sum_{i < j} |A_i \cap A_j| = \binom{m}{2} (m-2)^n, \quad \dots$$

In general,

$$\sum_{i_1 < i_2 < \dots < i_k} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| = \binom{m}{k} (m-k)^n.$$

Hence

$$\begin{aligned}
 \left| \bigcup_{i=1}^m A_i \right| &= \sum_{i=1}^m |A_i| - \sum_{i < j} |A_i \cap A_j| + \cdots + (-1)^{k+1} \sum_{i_1 < i_2 < \cdots < i_k} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}| + \cdots \\
 &= \binom{m}{1}(m-1)^n - \binom{m}{2}(m-2)^n + \cdots + (-1)^{k+1} \binom{m}{k}(m-k)^n + \cdots \\
 &= \sum_{k=1}^{m-1} (-1)^{k+1} \binom{m}{k} (m-k)^n.
 \end{aligned}$$

Let  $A$  be the set of all non-surjective mappings from  $\mathbf{N}_6$  to  $\mathbf{N}_4$ .

Let  $B$  be the set of all 6-digit quarternary sequences that do not contain at least one of the digits '0', '1', '2' and '3'.

We define a mapping  $f : A \rightarrow B$  as follows: for each non-surjective mapping  $\alpha \in A$ ,

$$f(\alpha) = a_1 a_2 a_3 a_4 a_5 a_6, \quad \text{where } a_i = \alpha(i) - 1.$$

Proof of injectivity: Since each **distinct** non-surjective mapping from  $\mathbf{N}_6$  to  $\mathbf{N}_4$  is mapped to a **distinct** 6-digit quarternary sequence that does not contain at least one of the digits '0', '1', '2' and '3',  $f$  is injective.

Proof of surjectivity: **For each quarternary sequence** that does not contain at least one of the digits '0', '1', '2' and '3', there is a **corresponding non-surjective mapping**  $\mathbf{N}_6$  to  $\mathbf{N}_4$  mapped to it under  $f$ , hence  $f$  is surjective.

Therefore  $f$  is bijective. By the Bijection Principle,

$$\begin{aligned}
 &\text{number of 6-digit quarternary sequences that do not contain at least one of the digits} \\
 &\text{'0', '1', '2' and '3'} \\
 &= |B| = |A| \\
 &= \sum_{k=1}^3 (-1)^{k+1} \binom{4}{k} (4-k)^6 \\
 &= \binom{4}{1} 3^6 - \binom{4}{2} 2^6 + \binom{4}{3} 1^6 \\
 &= \boxed{2536}
 \end{aligned}$$

□

### §11.2.5 Pigeonhole Principle

**Theorem 11.13** (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. □

**Theorem 11.14** (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  $\left\lceil \frac{n}{k} \right\rceil - 1$  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  $\left\lceil \frac{n}{k} \right\rceil < \frac{n}{k} + 1$  was used.

This is a contradiction, because there are a total of  $n$  objects. □

## §11.3 Distribution Problems

In this section, we are going to study a common class of combinatorial problems: **distribution problems**, which deal with the counting of ways of distributing  $r$  objects into  $n$  boxes.

In distribution problems, objects can be distinguishable or indistinguishable, and boxes can be distinguishable or indistinguishable.

### §11.3.1 Distinguishable objects into distinguishable boxes

### §11.3.2 Indistinguishable objects into distinguishable boxes

This type of problem is also known as “Stars and Bars”.

The setup is the following: distribute 10 indistinguishable balls into 3 distinguishable boxes. For example, one possible distribution is  $(4, 3, 3)$ , where there are 4 balls in box 1, 3 balls in box 2, and 3 balls in box 3.

The key observation is the following: we can distribute the balls by arranging them in a line, and then placing two “vertical bars” to partition the balls. For example, the  $(4, 3, 3)$  described above can be modeled by the following:

\* \* \* \* | \* \* \* | \* \* \*

where each  $*$  represents a ball, and the two location of the two bars determines the distribution of the candies. In general, box 1 contains balls left of the first bar, box 2 contains balls between the two bars, and box 3 contains balls 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, we have

**Theorem 11.15.** The number of ways to distribute  $r$  indistinguishable balls into  $n$  distinguishable boxes is given by

$$\binom{n+r-1}{r-1}. \quad (11.14)$$

#### Exercise 52

The owner of a newly set-up bird shop made 20 huge bird cages numbered 1 to 20 and imported 15 indistinguishable parrot dummies. Find the number of ways for him to distribute these dummies into the bird cages in each of the following cases:

- (a) Cage 8 must hold at least 3 dummies. [2]
- (b) the total number of dummies in Cage 2 and Cage 3 is 5. [3]

Suppose now that the bird shop owner tagged 5 of the dummies with a different serial number each, how many ways are there for him to distribute these 5 dummies into indistinguishable box(es) such that each box must contain at least 1 dummy? [2]

**Solution.**

- (a) Distribution problem:

3 dummies into cage 8, leaving  $15 - 3 = 12$  remaining identical dummies to be distributed into 20 distinct boxes.

$$\text{Number of different selections} = \binom{12+20-1}{20-1} = \binom{31}{12} = \boxed{141120525}$$

- (b) Equivalent problem:

$$(i) \quad x_2 + x_3 = 5$$

$$\text{Number of ways} = \binom{5+2-1}{1} = 6$$

$$(ii) \quad \sum_{i=1}^{20} x_i = 10, i \neq 2, 3$$

$$\text{Number of ways} = \binom{10+18-1}{18-1} = \binom{27}{17}$$

$$\text{By multiplication principle, total number of ways} = 6\binom{27}{17} = \boxed{50617710}$$

$$\text{Total number of ways} = S(5, 1) + S(5, 2) + S(5, 3) + S(5, 4) + S(5, 5) = 1 + 15 + 25 + 10 + 1 = \boxed{52} \quad \square$$

In general, the number of ways of distributing  $r$  indistinguishable balls into  $n$  distinct boxes, where  $r \geq n$ , such that *no box is empty* can be found by the following steps:

First, put one ball in each box. As the balls are indistinguishable, this can be done in one way. Then distribute the remaining  $r - n$  balls in the  $n$  boxes freely. The number of ways to perform the second step is

$$\binom{(r-n) + (n-1)}{n-1} = \binom{r-1}{n-1}.$$

Thus by MP we arrive at the following result:

**Theorem 11.16.** The number of ways of distributing  $r$  indistinguishable balls into  $n$  distinguishable boxes, where  $r \geq n$ , such that no box is empty is given by

$$\binom{r-1}{n-1}. \quad (11.15)$$

*Remark.* Alternatively, you can think of this as picking  $n - 1$  of the  $r - 1$  gaps between the  $r$  balls to place partitions.

### §11.3.3 Distinguishable objects into indistinguishable boxes

**Definition 11.17** (Stirling number of second kind). **Stirling number of the second kind**, denoted by  $S(r, n)$ , is the number of ways of distributing  $r$  distinguishable objects into  $n$  indistinguishable boxes such that *no box is empty*.

**Lemma 11.18.**

$$S(n, 1) = 1. \quad (11.16)$$

*Proof.* Since we only want one subset that has all of the elements, that subset must be the set itself. Since there is only one way to do this, the amount of ways to partition  $n$  numbers into 1 subset is one.  $\square$

**Lemma 11.19.**

$$S(n, 2) = 2^{n-1} - 1. \quad (11.17)$$

*Proof.* To see this, first note that there are  $2n$  ordered pairs of complementary subsets  $A$  and  $B$ . In one case,  $A$  is empty, and in another  $B$  is empty, so  $2n - 2$  ordered pairs of subsets remain. Finally, since we want unordered pairs rather than ordered pairs we divide this last number by 2, giving the result above.  $\square$

**Lemma 11.20.**

$$S(n, n-1) = \binom{n}{2}. \quad (11.18)$$

*Proof.* This is because dividing  $n$  elements into  $n - 1$  sets necessarily means dividing it into one set of size 2 and  $n - 2$  sets of size 1, by Pigeonhole Principle. Therefore we need only pick those two elements.  $\square$

We can establish the following recurrence relation:

$$S(r, n) = S(r-1, n-1) + nS(r-1, n) \quad (11.19)$$

*Proof.* Consider a single object to be fixed, and then consider where the remaining objects go. There are two cases:

- **Case 1:** The fixed object is in its own box.

There are  $r - 1$  remaining objects to be distributed into  $n - 1$  boxes; by definition, there are  $S(r - 1, n - 1)$  ways to do so.

- **Case 2:** The fixed object is in a box with other objects.

The remaining  $r - 1$  objects are distributed into  $n$  boxes; there are  $S(r - 1, n)$  ways to do so. For each of these distributions, there are  $n$  ways to group the fixed object with the other object. Thus, there are  $nS(r - 1, n)$  ways to do so.

Summing both cases together yields

$$S(r, n) = S(r - 1, n - 1) + nS(r - 1, n).$$

□

### Exercise 53 (The Ice Cream Problem)

Imagine that you are going to serve  $n$  kids ice cream cones, one cone per kid, and there are  $k$  different flavours available. Assuming that no flavours get mixed, show that the number of ways we can give out the cones using all  $k$  flavours.

**Solution.** Arrange the  $n$  kids in a line. There are  $S(n, k)$  ways to partition the  $n$  kids into  $k$  subsets according to the flavours that they will be receiving. After partitioning the kids, there are  $k!$  ways of assigning the flavours to this partition. Hence, the of ways we can give out the cones using all  $k$  flavours is  $k!S(n, k)$ . □

This is an answer to the ice cream problem, but it is unsatisfying to us, because we still don't know how to solve for  $S(n, k)$ . In order to find a formula for Stirling numbers of the second kind, we have to solve the ice cream problem without Stirling numbers, then equate them and isolate  $S(n, k)$ .

First of all, ignoring the fact that we must use all of the flavours, there would be  $k^n$  ways to distribute the ice cream: each kid has  $k$  choices, so we just multiply  $k$  by itself  $n$  times. Now we have overcounted, so we have to subtract the cases where we didn't use at least one flavour. The number of ways we could have done this is

$$\binom{k}{1}(k - 1)^n$$

because we choose one flavour out of the total  $k$  to exclude, and then we distribute the other  $k - 1$  flavours.

Now we have subtracted the cases where we have excluded at least two cases at least twice. We have to add back the cases where we've excluded at least two cases, which is  $\binom{k}{2}(k - 2)^n$  because we choose two flavours to exclude and distribute the other  $k - 2$  flavours to the kids. Now we have

$$k^n - \binom{k}{1}(k - 1)^n + \binom{k}{2}(k - 2)^n.$$

However, now we've overcounted again. This pattern repeats as we overcount and undercount, following the Property of Inclusion–Exclusion where the sets are the cases where we exclude each of the flavours.

Our resulting expression for the number of ways to distribute the ice cream is

$$k^n - \binom{k}{1}(k - 1)^n + \binom{k}{2}(k - 2)^n - \dots + (-1)^k \binom{k}{k}(k - k)^n$$

which we can rewrite as

$$\sum_{i=0}^k (-1)^i \binom{k}{i} (k - i)^n.$$

Now that we have two solutions to this problem, one using Stirling numbers of the second kind, and another without them, we can set them equal to each other, giving us

$$S(n, k) = \frac{1}{k!} \sum_{i=0}^k (-1)^i \binom{k}{i} (k - i)^n. \quad (11.20)$$

**Definition 11.21** (Bell numbers). Bell number, denoted by  $B_n$ , is the number of ways to arrange  $n$  distinct objects into up to  $n$  identical boxes.

Hence, Bell numbers are computed as a sum of Stirling numbers:

$$B_n = \sum_{k=1}^n S(n, k).$$

The Bell numbers have their own recurrence relation:

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k. \quad (11.21)$$

*Proof.* We present a combinatorial argument.

Consider how the  $(n+1)$ -th element is partitioned. Suppose that there are  $k$  elements which are not in its box, then there are  $\binom{n}{k}$  ways to pick these  $k$  elements, and thereafter there are  $B_k$  ways to arrange these  $k$  elements into identical boxes. Hence, there are  $\binom{n}{k} B_k$  such arrangements. The resulting Bell number is the sum of all these arrangements across all possible values of  $k$ .  $\square$

It is interesting to note that the exponential generating function of the Bell numbers is

$$B(x) = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n = e^{e^x - 1}.$$

*Proof.* The simplest way to prove this is to show that the previous recurrence relation explains why  $B'(x) = e^x B(x)$ , from which the result follows by solving the differential equation and evaluating at  $x = 0$ .  $\square$

### §11.3.4 Indistinguishable objects into indistinguishable boxes

**Definition 11.22.** We define a **partition**  $P(r, n)$  of a positive integer  $r$  into  $n$  parts to be a set of  $n$  positive integers whose sum is  $r$ .

*Remark.* The ordering of the integers in the collection does not matter.

We can establish the following recurrence relation:

$$P(r, n) = P(r-1, n-1) + P(r-n, n) \quad (11.22)$$

where  $1 < n \leq r$ .

*Proof.*

$\square$

## §11.4 Further Concepts

### §11.4.1 Catalan Numbers

Let's look at the **Bracket Problem**. How many ways can you put  $n$  pairs of brackets (a pair of a left and a right bracket) in an expression so that pairs of brackets match up? Note that we can't legally have the situation  $(( ))($ , so the number of left brackets appearing at any stage never exceeds the number of right brackets.

The numbers that we have been looking here are known as the **Catalan numbers**, denoted by  $C_n$ . The  $n$ -th Catalan number is given by the formula

$$C_n = \frac{(2n)!}{(n+1)!n!} \quad (11.23)$$

for  $n \geq 0$ .

It can be written in other ways too:

$$C_n = \frac{1}{n+1} \binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1} = \frac{1}{n+1} \sum_{i=0}^n \binom{n}{i}^2$$

The Catalan numbers also satisfy the recurrence relationships:

$$C_{n+1} = \frac{2(2n+1)}{n+2} C_n, \quad C_0 = 1$$

and

$$C_{n+1} = \sum_{i=0}^n C_i C_{n-i}, \quad C_0 = 1.$$

### §11.4.2 Derangements

A **derangement** is a permutation with no fixed points. That is, a derangement of a set leaves no element in its original place.

**Example 11.23.** 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.

We denote the number of derangements of an  $n$ -element set by  $D_n$ . This number satisfies the recurrence relationships

$$D_n = n \cdot D_{n-1} + (-1)^n$$

and

$$D_n = (n-1) \cdot (D_{n-1} + D_{n-2})$$

and is given by the formula

$$D_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$



## §11.5 Colouring Problems

Colouring is a technique in combinatorics that can be used to solve board-tiling problems, specifically to prove certain tilings are impossible. Generally, we assign a specific colour or label to each square on a board and shows that the tiles cannot satisfy constraints set by the colouring.

## §11.6 Probability

Elementary probability ○ Expected value and linearity of expectation

### §11.6.1 Definitions and Notation

A **random variable** is just a quantity that we take to vary randomly.

**Example 11.24.** The outcome of a standard six-sided dice roll, say  $D_6$ , is a random variable.

We can now discuss the **probability** of certain events, denoted by  $\mathbf{P}(\cdot)$ .

**Example 11.25.** We can write

$$\mathbf{P}(D_6 = 1) = \mathbf{P}(D_6 = 2) = \cdots = \mathbf{P}(D_6 = 6) = \frac{1}{6},$$

or  $\mathbf{P}(D_6 = 0) = 0$  and  $\mathbf{P}(D_6 \geq 4) = \frac{1}{2}$ .

We can also discuss the **expected value** of a random variable  $X$ , which is the “average” value. The formal definition is

$$\mathbf{E}[X] := \sum_x \mathbf{P}(X = x) \cdot x. \quad (11.24)$$

**Example 11.26.**

$$\mathbf{E}[D_6] = \frac{1}{6} \cdot 1 + \frac{1}{6} \cdot 2 + \cdots + \frac{1}{6} \cdot 6 = 3.5.$$

In natural language, we just add up all the outcomes weighted by probability they appear.

### §11.6.2 Properties of Expected Value

**Example 11.27.** At MOP, there are  $n$  people, each of who has a name tag. We shuffle the name tags and randomly give each person one of the name tags. Let  $S$  be the number of people who receive their own name tag. Prove that the expected value of  $S$  is 1.

**Solution.** This result might seem surprising, as one might intuitively expect  $\mathbf{E}[S]$  to depend on the choice of  $n$ .

Call a person a *fixed point* if they receive their own name tag. Thus  $S$  is the number of fixed points, and we wish to show that  $\mathbf{E}[S] = 1$ . If we are interested in the expected value, then according to our definition we should go through all  $n!$  permutations, count up the total number of fixed points, and then divide by  $n!$  to get the average. Since we want  $\mathbf{E}[S] = 1$ , we expect to see a total of  $n!$  fixed points.

Note that if we have  $n$  letters, then each letter appears as a fixed point  $(n-1)!$  times.

Thus the expected value is

$$\mathbf{E}[S] = \frac{1}{n!} \left( \underbrace{(n-1)! + (n-1)! + \cdots + (n-1)!}_{n \text{ times}} \right) = \frac{1}{n!} \cdot n \cdot (n-1)! = 1.$$

□

**Theorem 11.28** (Linearity of expectation). Given any random variables  $X_1, X_2, \dots, X_n$ , we always have

$$\mathbf{E}[X_1 + X_2 + \cdots + X_n] = \mathbf{E}[X_1] + \mathbf{E}[X_2] + \cdots + \mathbf{E}[X_n]. \quad (11.25)$$

This theorem is obvious if  $X_1, X_2, \dots, X_n$  are independent of each other. The wonderful thing is that this holds even if the variables are not independent.

## §11.7 Generating Functions

AOPS Volume 2 pg200

Let  $\{a_n\}$  be an infinite sequence of numbers.

The **ordinary generating function** (OGF) of the sequence is defined by the formal series

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots \quad (11.26)$$

The **exponential generating function** (EGF) of the sequence is defined by the formal series

$$f(x) = a_0 + a_1 \frac{x}{1!} + a_2 \frac{x^2}{2!} + \cdots + a_n \frac{x^n}{n!} + \cdots \quad (11.27)$$

We are never required to consider the convergence of these functions. In fact, we can always substitute such a formal series with functions whose Taylor series is equal to the formal series.

### §11.7.1 Properties of OGFs

**Proposition 11.29.** If  $f(x)$  is the OGF of  $\{a_n\}$ , then the OGF of  $\{a_{n+1}\}$  is

$$\frac{f(x) - a_0}{x}.$$

In general, the OGF of  $\{a_{n+k}\}$  is given by

$$\frac{f(x) - a_0 - a_1x - \cdots - a_{k-1}x^{k-1}}{x^k}.$$

*Proof.* If we let  $g(x)$  to be the OGF of  $\{a_{n+1}\}$  then

$$g(x) = a_1 + a_2x + a_3x^2 + \cdots$$

Thus

$$f(x) = a_0 + x(a_1 + a_2x + \cdots) = a_0 + xg(x).$$

□

**Proposition 11.30.** If  $f(x)$  is the OGF of  $\{a_n\}$ , then the OGF of  $\{na_n\}$  is  $x\mathcal{D}f = xf'(x)$  where  $\mathcal{D}$  is the differential operator  $\frac{d}{dx}$ . In general, the OGF of  $\{n^k a_n\}$  is given by  $(x\mathcal{D})^n f$ . More generally, if  $P$  is a polynomial, then the OGF of  $\{P(n)a_n\}$  is  $P(x\mathcal{D})f$ .

**Proposition 11.31.** If  $f(x)$  and  $g(x)$  are the OGFs of  $\{a_n\}$  and  $\{b_n\}$  respectively, then  $f(x)g(x)$  is the OGF of

$$\left\{ \sum_{k=0}^n a_k b_{n-k} \right\}.$$

### §11.7.2 Properties of EGFs

## Exercises

**Problem 103** (SMO Open 2005 Q6). From the first 2005 natural numbers,  $k$  of them are arbitrarily chosen. What is the least value of  $k$  to ensure that there is at least one pair of numbers such that one of them is divisible by the other?

**Solution.** Take any set  $A$  of 1004 numbers. Write each number in the form

$$2^{a_i} b_i, \quad \text{where } a_i \geq 0 \text{ and } b_i \text{ is odd.}$$

Thus there are 1004 odd numbers  $b_1, \dots, b_{1004}$ . Since there are 1003 odd numbers among the first 2005 positive integers, at least two of these odd numbers are equal, say  $b_i = b_j$ . Then  $2^{a_i} b_i \mid 2^{a_j} b_j$  if  $2^{a_i} b_i < 2^{a_j} b_j$ . So the answer is 1004.  $\square$

**Problem 104** (SMO Open 2006 Q1). How many integers are there between 0 and  $10^5$  having the digit sum equal to 8?

**Solution.** Each integer can be written as  $\overline{x_1 x_2 x_3 x_4 x_5}$  where each  $x_i = 0, 1, \dots, 9$  and  $x_1 + \dots + x_5 = 8$ . The number of non-negative integer solutions to the above equation is  $\binom{8+4}{4} = 495$ . So there are 495 such integers.  $\square$

**Problem 105** (SMO Open 2006 Q15). Let  $X = \{1, 2, 3, \dots, 17\}$ . Find the number of subsets  $Y$  of  $X$  with odd cardinalities.

**Solution.** We have  $|A|$  odd if and only if  $|A^c|$  is even. Thus the number of subsets of odd cardinality is the same as the number of subsets with even cardinality. Hence the answer is  $\frac{1}{2} \times 2^{17} = 2^{16} = 65536$ .  $\square$

**Problem 106** (SMO Open 2006 Q19). Given two sets  $A = \{1, 2, 3, \dots, 15\}$  and  $B = \{0, 1\}$ , find the number of mappings  $f: A \rightarrow B$  with 1 being the image of at least two elements of  $A$ .

**Solution.** There are  $2^{15}$  mappings from  $A$  to  $B$ . There is only one where  $f(x) \neq 1$  for all  $x$  and 15 where  $f(x) = 1$  for exactly one  $x$ . Thus the answer is  $2^{15} - 16 = \boxed{32752}$ .  $\square$

**Problem 107** (SMO Open 2006 Q21). Let  $P$  be a 30-sided polygon inscribed in a circle. Find the number of triangles whose vertices are the vertices of  $P$  such that any two vertices of each triangle are separated by at least three other vertices of  $P$ .

**Solution.** Consider a vertex of such a triangle together with its three neighbouring vertices on the left as a block. We first count all such triangles that contain  $A$  as one of its vertices. After taking away the block counting  $A$ , we are left with 18 vertices and 2 blocks. Thus the number of triangles containing  $A$  is the number of ways to arrange these 20 objects and this can be done in  $\binom{20}{2} = 190$  ways. Hence there are  $30 \cdot 190/3 = \boxed{1900}$  such triangles.  $\square$

**Problem 108** (SMO Open 2006 Q25). Let

$$S = \sum_{r=0}^n \binom{3n+r}{r}.$$

Evaluate  $\frac{S}{23 \times 38 \times 41 \times 43 \times 47}$  when  $n = 12$ .

**Solution.** By using the fact that  $\binom{n}{r-1} + \binom{n}{r} = \binom{n+1}{r}$ , and writing  $\binom{3n}{0}$  as  $\binom{3n+1}{0}$ , we have

$$\begin{aligned} S &= \left[ \binom{3n+1}{0} + \binom{3n+1}{1} \right] + \binom{3n+2}{2} + \dots + \binom{3n+n}{n} \\ &= \binom{3n+2}{1} + \binom{3n+2}{2} + \dots + \binom{3n+n}{n} \\ &= \dots \\ &= \binom{3n+n}{n-1} + \binom{3n+n}{n} = \binom{4n+1}{n} \end{aligned}$$

Thus when  $n = 12$ ,

$$\frac{S}{23 \times 38 \times 41 \times 43 \times 47} = 1274.$$

□

**Problem 109** (SMO Open 2007 Q2). Determine the number of those 0-1 binary sequences of ten 0's and ten 1's which do not contain three 0's together.

**Solution.** In such a binary sequence, 0's either appear singly or in blocks of two. If the sequence has exactly  $m$  blocks of double 0's, then there are  $10 - 2m$  single 0's. The number of such binary sequences is  $\binom{11}{m} \times \binom{11-m}{10-2m}$ . Thus the answer is

$$\sum_{m=0}^5 \binom{11}{m} \times \binom{11-m}{10-2m} = 24068.$$

□

**Problem 110** (SMO Open 2018 Q5). A rectangular table has two chairs on each of the longer sides and one chair on each of the shorter sides. In how many ways can six people be seated?

(Note: Any two arrangements are the same up to 'rotation' of the rectangular table.)

**Solution.** Fix one person, say  $P$ . Note that there are three positions to consider:

1.  $P$  is seated on the shorter side;
2.  $P$  is seated on the left seat of the longer side;
3.  $P$  is seated on the right seat of the longer side.

In each case there are  $5! = 120$  ways, so in total there are 360 ways.

□

**Problem 111** (Putnam 1992 A6). Four points are chosen independently and at random on the surface of a sphere (using the uniform distribution). What is the probability that the center of the sphere lies inside the resulting tetrahedron?

**Solution.** Having placed 3 points  $A$ ,  $B$  and  $C$ , the fourth point  $D$  will enclose the center in the tetrahedron iff it lies in the spherical triangle  $A'B'C'$ , where  $P'$  is directly opposite to  $P$  (so that the center lies on  $PP'$ ).

The probability of this is the area of  $ABC$  divided by the area of the sphere. So taking the area of the sphere as 1, we want to find the expected area of  $ABC$ . But the 8 triangles  $ABC$ ,  $A'BC$ ,  $AB'C$ ,  $ABC'$ ,  $A'B'C$ ,  $AB'C'$ ,  $A'BC'$ ,  $A'B'C'$  are all equally likely and between them partition the surface of the sphere. So the expected area of  $ABC$ , and hence the required probability, is just  $\boxed{\frac{1}{8}}$ .  $\square$

**Problem 112** (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.** 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)

The lemma asserts that the number of regions is maximal if all "inner" intersections of chords are simple (exactly two chords pass through each point of intersection in the interior). This will be the case if the points on the circle are chosen "in general position". Under this assumption of "generic intersection", the number of regions can also be determined in a non-inductive way, using the formula for the Euler characteristic of a connected planar graph (viewed here as a graph embedded in the 2-sphere  $S^2$ ).

A planar graph determines a cell decomposition of the plane with  $F$  faces (2-dimensional cells),  $E$  edges (1-dimensional cells) and  $V$  vertices (0-dimensional cells). As the graph is connected, the Euler relation for the 2-dimensional sphere  $S^2$

$$V - E + F = 2$$

holds. View the diagram (the circle together with all the chords) above as a planar graph. If the general formulas for  $V$  and  $E$  can both be found, the formula for  $F$  can also be derived, which will solve the problem.

Its vertices include the  $n$  points on the circle, referred to as the exterior vertices, as well as the interior vertices, the intersections of distinct chords in the interior of the circle. The "generic intersection" assumption made above guarantees that each interior vertex is the intersection of no more than two chords.

Thus the main task in determining  $V$  is finding the number of interior vertices. As a consequence of the lemma, any two intersecting chords will uniquely determine an interior vertex. These chords are in turn uniquely determined by the four corresponding endpoints of the chords, which are all exterior vertices. Any four exterior vertices determine a cyclic quadrilateral, and all cyclic quadrilaterals are convex quadrilaterals, so each set of four exterior vertices have exactly one point of intersection formed by their diagonals (chords). Further, by definition all interior vertices are formed by intersecting chords.

Therefore, each interior vertex is uniquely determined by a combination of four exterior vertices, where the number of interior vertices is given by

$$V_{\text{interior}} = \binom{n}{4},$$

and so

$$V = V_{\text{exterior}} + V_{\text{interior}} = n + \binom{n}{4}.$$

The edges include the  $n$  circular arcs connecting pairs of adjacent exterior vertices, as well as the chordal line segments (described below) created inside the circle by the collection of chords. Since there are two groups of vertices: exterior and interior, the chordal line segments can be further categorized into three groups:

1. Edges directly (not cut by other chords) connecting two exterior vertices. These are chords between adjacent exterior vertices, and form the perimeter of the polygon. There are  $n$  such edges.
2. Edges connecting two interior vertices.
3. Edges connecting an interior and exterior vertex.

To find the number of edges in groups 2 and 3, consider each interior vertex, which is connected to exactly four edges. This yields

$$4 \binom{n}{4}$$

edges. Since each edge is defined by two endpoint vertices, only the interior vertices were enumerated, group 2 edges are counted twice while group 3 edges are counted once only.

Every chord that is cut by another (i.e., chords not in group 1) must contain two group 3 edges, its beginning and ending chordal segments. As chords are uniquely determined by two exterior vertices, there are altogether

$$2 \left( \binom{n}{2} - n \right)$$

group 3 edges. This is twice the total number of chords that are not themselves members of group 1.

The sum of these results divided by two gives the combined number of edges in groups 2 and 3. Adding the  $n$  edges from group 1, and the  $n$  circular arc edges brings the total to

$$E = \frac{4\binom{n}{4} + 2\left(\binom{n}{2} - n\right)}{2} + n + n = 2\binom{n}{4} + \binom{n}{2} + n.$$

Substituting  $V$  and  $E$  into the Euler relation solved for  $F$ ,  $F = E - V + 2$ , we then obtain

$$F = \binom{n}{4} + \binom{n}{2} + 2.$$

Since one of these faces is the exterior of the circle, the number of regions  $r_G$  inside the circle is  $F - 1$ , or

$$r_G = \binom{n}{4} + \binom{n}{2} + 1.$$

□



**Problem 113** (Langford's Problem  $L(n)$ ). Given the multiset<sup>1</sup> of positive integers:

$$\{1, 1, 2, 2, 3, 3, \dots, n, n\},$$

can they be arranged in a sequence such that for  $1 \leq i \leq n$  there are  $i$  numbers between the two occurrences of  $i$ ?

*Proof.*

□

---

<sup>1</sup>A multiset is like a set except that there may be more than one occurrence of an element.

**Problem 114.** 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:

$$\sum_{k=0}^n \binom{n}{k} \binom{n}{n-k} = \binom{n}{0} \binom{n}{n} + \binom{n}{1} \binom{n}{n-1} + \dots$$

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.  $\square$

**Problem 115.** Evaluate

$$S = \binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n}.$$

**Solution.** Writing the sum backwards yields

$$\begin{aligned} S &= n\binom{n}{n} + (n-1)\binom{n}{n-1} + \cdots + \binom{n}{1} \\ &= n\binom{n}{0} + (n-1)\binom{n}{1} + \cdots + \binom{n}{n-1} \end{aligned}$$

Add this to the original series gives us

$$2S = n \left[ \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} \right]$$

$$2S = n2^n$$

$$\boxed{S = n2^{n-1}}$$

□ This is the proof of the sum

$$\sum_{k=0}^n k \binom{n}{k} = n2^{n-1}$$

**Problem 116** (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  $k_1 + k_3 = k_2 + k_4 = k$ . 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  $\boxed{\frac{(n+1)(2n^2+4n+3)}{3}}$ . □

**Problem 117** (ROMANIA 1990). Find the least positive integer  $m$  such that

$$\binom{2n}{n}^{\frac{1}{n}} < m$$

for all positive integers  $n$ .

**Solution.** Note that

$$\binom{2n}{n} < \binom{2n}{0} + \binom{2n}{1} + \cdots + \binom{2n}{2n} = (1+1)^{2n} = 4^n$$

and for  $n = 5$ ,

$$\binom{10}{5} = 252 > 3^5.$$

Thus  $m = 4$ .

□

**Problem 118.** Evaluate

$$\sum_{k=0}^n \frac{1}{(n-k)!(n_k)!}.$$

**Solution.** Let  $S_n$  denote the desired sum. Then

$$\begin{aligned} S_n &= \frac{1}{(2n)!} \sum_{k=0}^n \frac{(2n)!}{(n-k)!(n+k)!} \\ &= \frac{1}{(2n)!} \sum_{k=0}^n \binom{2n}{n-k} \\ &= \frac{1}{(2n)!} \binom{2n}{n} \\ &= \frac{1}{(2n)!} \cdot \frac{1}{2} \left[ \sum_{k=0}^{2n} \binom{2n}{k} + \binom{2n}{n} \right] \\ &= \frac{1}{(2n)!} \cdot \frac{1}{2} \left[ 2^{2n} + \binom{2n}{n} \right] \\ &= \frac{2^{2n-1}}{(2n)!} + \frac{1}{2(n!)^2} \end{aligned}$$

□

# 12 Recurrence Relations

## §12.1 Introduction

### §12.1.1 Definition

**Definition 12.1.** 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*  $a_0, a_1, \dots, a_{n-1}$ , for all integers  $n \geq n_0$ .

The **initial conditions** for a sequence specify the terms before  $n_0$  (before the recurrence relation takes effect). The recurrence relations together with the initial conditions uniquely determines the sequence.

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

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

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

By **linear**, we mean the previous terms appear with exponent 1 (not squares, cubes, etc); by **homogeneous**, we mean there is no term other than the multiples of  $a_i$ ; by **degree** of  $k$ , we mean the current term can be expressed in terms of previous  $k$  terms.

Relevant examples:

- $a_{n+1} = a_n + k$

**Solution:**  $a_n = a_1 + (k-1)n$

- $a_{n+1} = a_n + n$

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

- $a_{n+1} = a_n \cdot k$

**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  $x$

Some useful heuristics for problem-solving:

- Try from small numbers, look for patterns
- Consider first/last things, split into cases

### §12.1.2 Identifying Recurrence Relations

We shall discuss some counting problems.

**Example 12.2** (Staircase problem). A boy wishes to climb a staircase of  $n$  steps. Each time, the boy either climbs up one step or two steps. How many ways are there for him to climb the staircase?

**Solution.** Consider two cases as follows:

- **Case 1:** The first move covers 1 step.  
Then there are  $n - 1$  steps left, thus  $a_{n-1}$  ways to climb these remaining steps.
- **Case 2:** The first move covers 2 steps.  
Then there are  $n - 2$  steps left, thus  $a_{n-2}$  ways to climb these remaining steps.

Combining the results of these two cases by applying Addition Principle, we conclude that

$$a_n = a_{n-1} + a_{n-2}$$

for  $n \geq 3$ , where  $a_1 = 1$ ,  $a_2 = 2$ . □

**Example 12.3** (Tower of Hanoi). A tower of  $n$  circular discs of different sizes is stacked on one of the three given pegs in decreasing size from the bottom. The task is to transfer the entire tower to another peg by a sequence of moves under the following conditions:

- (i) each move carries exactly one disc, and
- (ii) no disc can be placed on top of a smaller one.

What is the minimum number of moves required to accomplish the task?

**Solution.** The task of transferring the entire tower of  $n$  discs to another peg can be done via the following steps:

1. Transfer the top  $n - 1$  discs to another peg.
2. Move the largest disc from the original peg to the only empty peg.
3. Transfer the entire tower of  $n - 1$  smaller discs to the peg that the largest disc is currently placed.

The minimum number of moves for step 1, 2 and 3 are  $b_{n-1}$ , 1 and  $b_{n-1}$  respectively. Hence the minimum number of moves for the whole task is  $2b_{n-1} + 1$ .

By the definition of  $b_n$ , we have

$$b_n = 2b_{n-1} + 1$$

for  $n \geq 2$ , where  $b_1 = 1$ .

*Remark.* The closed formula is given by

$$b_n = 2^n - 1.$$
□

**Example 12.4** (Fibonacci's rabbits). Beginning with a pair of new-born rabbits, and assuming that each pair is immortal and gives birth to a new pair each month starting from the second month of its life, how many pairs will there be after  $n$  months?

**Solution.** Let  $F_n$  denote the number of pairs of rabbits at the end of the  $n$ -th month.

Note that  $F_n$  is the sum of number of pairs of rabbits in the previous month, and number of pairs of newborn rabbits that were born from rabbits two months ago. Thus

$$F_n = F_{n-1} + F_{n-2}$$

for  $n \geq 3$ , where  $F_1 = 1$ ,  $F_2 = 1$ . □



**Example 12.5** (Derangement). A permutation of  $a_1, a_2, \dots, a_n$  is called a derangement (nothing is in its right place) if  $a_i \neq i$  for each  $i = 1, 2, \dots, n$ . Denoting the number of derangements by  $D_n$ , show that

$$D_n = (n-1)(D_{n-1} + D_{n-2}).$$

**Solution.** The first digit cannot be '1', so there are  $n-1$  choices for the first digit.

Suppose the first digit is '2'.

- **Case 1:** If '1' is placed in the second position, the number of ways to arrange the remaining  $n-2$  digits such that none is in its right place is given by  $D_{n-2}$ .
- **Case 2:** If '1' is not placed in the second position, then the number of ways to arrange  $1, 3, 4, \dots, n$  such that none is in its right place is given by  $D_{n-1}$ .

Total number of derangements if the first digit is '2' =  $D_{n-1} + D_{n-2}$ .

A similar argument holds for the other  $n-2$  cases. Hence by Multiplication Principle,

$$D_n = (n-1)(D_{n-1} + D_{n-2})$$

for  $n \geq 3$ , where  $D_1 = 0$ ,  $D_2 = 1$ . □

## §12.2 First-order Recurrence Relations

- solution of (i) first order linear (homogeneous and nonhomogeneous) recurrence relations with constant coefficients

The homogeneous case can be written in the following way:

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

The general solution is

$$x_n = Ar^n$$

which is a geometric sequence with common ratio  $r$ .

## §12.3 Second-order Recurrence Relations

A second order linear homogeneous recurrence relation with constant coefficients can be written in the following way:

$$c_0x_n + c_1x_{n-1} + c_2x_{n-2} = 0.$$

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

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

which simplifies to

$$c_0r^2 + c_1r + c_2 = 0,$$

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

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

$$x_n = \alpha_1 r_1^n + \alpha_2 r_2^n$$

where  $\alpha_1$  and  $\alpha_2$  are constants to be found.

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

$$x_n = (\alpha_1 + \alpha_2 n) r_1^n$$

where  $\alpha_1$  and  $\alpha_2$  are constants to be found.

### Exercise 54

Solve the recurrence relation  $a_n = 3a_{n-1} - 2a_{n-2}$ , with initial conditions  $a_1 = 1$ ,  $a_2 = 2$ .

**Solution.** The characteristic equation  $x^2 = 3x - 2$  has two roots 1 and 2. Thus

$$a_n = K \cdot 1^n + L \cdot 2^n$$

where  $K$  and  $L$  are constants to be determined from initial conditions:

$$n = 1, \quad a_1 = K + 2L = 1$$

$$n = 2, \quad a_2 = K + 4L = 2$$

Solving these equations, we get  $K = 0$  and  $L = \frac{1}{2}$ . Therefore

$$a_n = 0 \cdot 1^n + \frac{1}{2} \cdot 2^n = 2^{n-1}.$$

□

**Exercise 55**

Solve the recurrence relation  $a_n = 6a_{n-1} - 9a_{n-2}$ , with initial conditions  $a_0 = 1$ ,  $a_1 = 6$ .

**Solution.**  $r^2 - 6r + 9 = 0$  has only 3 as a root. So the format of the solution is  $a_n = \alpha_1 3^n + \alpha_2 n 3^n$ . Need to determine  $\alpha_1$  and  $\alpha_2$  from initial conditions:

$$\begin{aligned} a_0 &= 1 = \alpha_1 \\ a_1 &= 6 = \alpha_1 \cdot 3 + \alpha_2 \cdot 3 \end{aligned}$$

Solving these equations we get  $\alpha_1 = 1$  and  $\alpha_2 = 1$ . Therefore

$$a_n = 3^n + n 3^n.$$

□

**Exercise 56**

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  $\alpha$ . Then we have

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

from which we conclude that  $\alpha^2 - \alpha - 1 = 0$ . 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

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

Thus we have

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

Hence this gives us

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

□

Generalising this, we have the following theorem.

**Theorem 12.6.** Let  $c_1, c_2, \dots, c_k$  be real numbers. Suppose that the characteristic equation  $r^k - c_1 r^{k-1} - \dots - c_k = 0$  has  $k$  distinct roots  $r_1, r_2, \dots, r_k$ . Then, a sequence  $\{a_n\}$  is a solution of the recurrence relation

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

if and only if  $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \dots + \alpha_k r_k^n$  for  $n = 0, 1, 2, \dots$ , where  $\alpha_1, \alpha_2, \dots, \alpha_k$  are constants.

## Exercises

**Problem 119** (SMO Open 2018 Q19). Assume that  $a_1 < 2$ , and for any integer  $n \geq 2$ ,  $a_n = 1 + a_{n-1}(a_{n-1} - 1)$ . If

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_m} = 1$$

for some integer  $m$ , and that  $16a_1 - a_{m+1} \leq N$  for some integer  $N$ , what is the least possible value of  $N$ ? (Note that  $N$  may not be attainable.)

**Solution.** For  $n \geq 2$ , as  $a_n = 1 + a_{n-1}(a_{n-1} - 1)$ , we have

$$\frac{1}{a_n - 1} = \frac{1}{(a_{n-1} - 1)(a_{n-1})} = \frac{1}{a_{n-1} - 1} - \frac{1}{a_{n-1}},$$

i.e.,

$$\frac{1}{a_{n-1}} = \frac{1}{a_{n-1} - 1} - \frac{1}{a_n - 1}.$$

Thus

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_m} = \frac{1}{a_1 - 1} - \frac{1}{a_{m+1} - 1}.$$

By the given condition,

$$\frac{1}{a_1 - 1} - \frac{1}{a_{m+1} - 1} = 1.$$

Solving this gives  $a_{m+1} = -\frac{1}{a_1 - 2}$ . Thus

$$\begin{aligned} 16a_1 - a_{m+1} &= 16a_1 + \frac{1}{a_1 - 2} \\ &= 16(a_1 - 2) + 32 + \frac{1}{a_1 - 2} \\ &= 32 - \left[ 16(2 - a_1) + \frac{1}{2 - a_1} \right] \\ &\leq 32 - 2\sqrt{16} \quad \text{by AM-GM} \\ &= 24. \end{aligned}$$

Equality is attained when  $16(2 - a_1) = \frac{1}{2 - a_1}$ , i.e.,  $a_1 = \frac{7}{4}$ . Note however that in this problem the maximum value is not attainable.  $\square$

**Problem 120** (SMO Open 2018 Q17). Let  $f_0(x) = \frac{x}{3x + 2}$  and for any integer  $n \geq 1$ ,  $f_n(x) = f_0(f_{n-1}(x))$ . Find  $f_{2018}(x)$ .

**Solution.** Observe that for  $n \geq 1$ ,

$$\frac{1}{f_n(x)} = \frac{3f_{n-1}(x) + 2}{f_{n-1}(x)} = \frac{2}{f_{n-1}(x)} + 3 = 2\left(\frac{1}{f_{n-1}(x)} + 3\right) - 3,$$

i.e.

$$\frac{1}{f_n(x)} + 3 = 2\left(\frac{1}{f_{n-1}(x)} + 3\right).$$

Thus

$$\frac{1}{f_n(x)} + 3 = 2^n \left( \frac{1}{f_0(x)} + 3 \right) = 2^n \left( \frac{3x + 2}{x} + 3 \right),$$

implying that

$$\frac{1}{f_n(x)} = 2^n \left( \frac{3x + 2}{x} + 3 \right) - 3 = \frac{3(2^{n+1} - 1)x + 2^{n+1}}{x}.$$

So

$$f_n(x) = \frac{x}{3(2^{n+1} - 1)x + 2^{n+1}}.$$

□

SMO Open 2017 Q24

SMO Open 2015 Q3

SMO Open 2012 Q21

**Problem 121** (SMO Open 2006 Q20). Let  $a_1, a_2, \dots$  be a sequence satisfying the condition that

$$a_1 = 1 \quad \text{and} \quad a_n = 10a_{n-1} - 1 \quad \text{for all } n \geq 2.$$

Find the minimum  $n$  such that  $a_n > 10^{100}$ .**Solution.** Note that  $a_n - \frac{1}{9} = 10(a_{n-1} - \frac{1}{9})$  for all  $n \geq 2$ . Let  $b_n = a_n - \frac{1}{9}$ . Then

$$b_n = 10b_{n-1} = \dots = 10^{n-1}b_1 = \frac{8 \cdot 10^{n-1}}{9}.$$

Therefore  $a_n = \frac{1 + 8 \cdot 10^{n-1}}{9}$ . For  $n \geq 2$ ,  $8 \cdot 10^{n-2} < a_n < 10^{n-1}$ . Thus  $a_{101} < 10^{101} < a_{102}$  and the answer is 102. □**Problem 122** (SMO Open 2005 Q14). Let  $a_1 = 2006$ , and for  $n \geq 2$ ,  $a_1 + a_2 + \dots + a_n = n^2 a_n$ . What is the value of  $2005a_{2005}$ ?**Solution.**

$$a_n = \sum_{i=1}^n a_i - \sum_{i=1}^{n-1} a_i = n^2 a_n - (n-1)^2 a_{n-1}.$$

This gives  $a_n = \frac{n-1}{n+1} a_{n-1}$ . Thus

$$a_{2005} = \frac{2004}{2006} a_{2004} = \dots = \frac{2004 \times 2003 \times \dots \times 1}{2006 \times 2005 \times \dots \times 3} a_1 = \frac{2}{2005}.$$

□

**Problem 123** (Vietnam 1977). Into how many regions do  $n$  circles divide the plane, if each pair of circles intersects at two points and no point lies on three circles?**Solution.** Denote by  $P(n)$ , the number of regions divided by  $n$  circles. We have  $P(1) = 2, P(2) = 4, P(3) = 8, P(4) = 14, \dots$  and from this we notice that

$$\begin{aligned} P(1) &= 2 \\ P(2) &= P(1) + 2 \\ P(3) &= P(2) + 4 \\ P(4) &= P(3) + 6 \\ &\vdots \\ P(n) &= P(n-1) + 2(n-1). \end{aligned}$$

Summing up these equations we obtain

$$P(n) = 2 + n(n-1).$$

We now prove this formula by induction.

For  $n = 1$  it is obviously true.Suppose the formula is true for  $n = k$ ,  $k \in \mathbf{Z}^+, k \geq 1$ ; that is,  $P(k) = 2 + k(k-1)$ . Consider  $k+1$  circles, the  $(k+1)$ -th circle intersects  $k$  other circles at  $2k$  points, which means that this circle is divided into  $2k$  arcs, each of which divides the region it passes into two sub-regions. Therefore, we have in addition  $2k$  regions, and so

$$\begin{aligned} P(k+1) &= P(k) + 2k \\ &= 2 + k(k-1) + 2k \\ &= 2 + k(k+1). \end{aligned}$$

□

**Problem 124** (Australia 2020 Q4). Define the sequence  $A_1, A_2, A_3, \dots$  by  $A_1 = 1$  and for  $n = 1, 2, 3, \dots$

$$A_{n+1} = \frac{A_{n+2}}{A_n + 1}.$$

Define the sequence  $B_1, B_2, B_3, \dots$  by  $B_1 = 1$  and for  $n = 1, 2, 3, \dots$

$$B_{n+1} = \frac{B_n^2 + 2}{2B_n}.$$

Prove that  $B_{n+1} = A_{2^n}$  for all non-negative integers  $n$ .

**Solution.**

□

**Problem 125.** The sequence given by  $x_0 = a$ ,  $x_1 = b$ , and

$$x_{n+1} = \frac{1}{2} \left( x_{n-1} + \frac{1}{x_n} \right)$$

is periodic.

Prove that  $ab = 1$ .

**Solution.** Multiplying by  $2x_n$  on both sides of the given recursive relation yields

$$2x_n x_{n+1} = x_{n-1} x_n + 1$$

or

$$2(x_n x_{n+1} - 1) = x_{n-1} x_n - 1.$$

Let  $y_n = x_{n-1} x_n - 1$  for  $n \in \mathbf{N}$ . Since  $y_{n+1} = \frac{y_n}{2}$ ,  $\{y_n\}$  is a geometric sequence. If  $x_n$  is periodic, then so is  $y_n$ , which implies that  $y_n = 0$  for all  $n \in \mathbf{N}$ . Therefore

$$ab = x_0 x_1 = y_1 + 1 = 1.$$

□

# 13 Graph Theory

Basic properties and definitions from graph theory, e.g. connectedness and degree of a vertex  
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 Introduction, Definitions and Notations

- A **graph** is a pair of sets  $G = (V, E)$  where  $V$  is a set of vertices and  $E$  is a collection of edges whose endpoints are in  $V$ . It is possible that a graph can have infinitely many vertices and edges. Unless stated otherwise, we assume that all graphs are simple.<sup>1</sup>
- Two vertices  $v, w$  are said to be **adjacent** if there is an edge joining  $v$  and  $w$ . An edge and a vertex are said to be **incident** if the vertex is an endpoint of the edge.
- Given a vertex  $v$ , the **degree** of  $v$  is defined to be the number of edges containing  $v$  as an endpoint.
- A **path** in a graph  $G$  is defined to be a finite sequence of distinct vertices  $v_0, v_1, \dots, v_t$  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  $v_0, v_1, \dots, v_t$  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  $u$  and  $v$ . (In the case the graph is disconnected, this may not be well-defined.)
- Let  $G = (V, E)$  be a graph. The **complement**  $\bar{G}$  of  $G$  is a graph with the same vertex set as  $G$  and  $E(\bar{G}) = \{e \notin E(G)\}$ . i.e.  $\bar{G}$  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  $A_1, \dots, A_k$  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  $K_{n_1, n_2, \dots, n_k}$ . (Note that a 2-partite graph is simply a bipartite graph.)

<sup>1</sup>An edge whose endpoints are the same is called a **loop**. A graph where there is more than one edge joining a pair of vertices is called a **multigraph**. A graph without loops and is not a multigraph is said to be **simple**.



**Theorem 13.1** (Euler). For a connected planar graph with  $V$  vertices,  $E$  edges and  $F$  faces,

$$V - E + F = 2. \quad (13.1)$$

## §13.2 Trees and Balancing

A **tree** is defined to be a connected graph that does not contain any cycles. We will first give characterisations to such graphs.

**Lemma 13.2** (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.

## §13.3 Friends, Strangers and Cliques

Given a graph  $G$ , a **clique** in  $G$  is a subset of vertices of  $G$  where every pair of vertices in the subset is joined by an edge. This becomes important in certain math olympiad problems involving friends and strangers.

## §13.4 Directed Graphs, Lots of Arrows and Tournaments

A **direct graph** is a graph where each edge is oriented with an arrow pointing in exactly one direction. A **directed path** is a path in the graph that moves along with the orientation of the arrow. A **directed cycle** is defined similarly. A **tournament** is defined to be a complete directed graph.

## §13.5 Matchings: Pair Them Up

Given a graph  $G$ , a **matching**  $M$  is a set of edges in  $G$  such that no two edges in  $M$  touch. A matching is said to be **perfect** if every vertex in  $G$  is incident to an edge in  $M$ . A vertex is said to be  **$M$ -exposed** if it is not covered by an edge in  $M$ . Clearly,  $M$  is a perfect matching if and only if there are no  $M$ -exposed vertices.

We will now state two important properties regarding matchings.

**Theorem 13.3** (Hall's theorem). Let  $G = A \cup B$  where  $A \cap B = \emptyset$  be a bipartite graph. For  $\emptyset \neq S \subseteq A$ , let  $\Gamma(S)$  be the vertices in  $B$  which is adjacent to a vertex in  $A$ . Then there is a matching that covers every vertex in  $A$  if and only if for all  $S \subseteq A$ ,

$$|\Gamma(S)| \geq |S|.$$

The latter condition is called **Hall's Condition**. In the special case where  $|A| = |B|$ , then  $G$  has a perfect matching if and only if  $G$  satisfies Hall's Condition.

## §13.6 Hamiltonian and Eulerian Paths and Cycles

Given a graph  $G$ , an **Eulerian walk** is defined to be a sequence of successive adjacent vertices that encounter every edge in the graph exactly once. An **Eulerian cycle** is a sequence of successive adjacent vertices that begin and ends at the same vertex, that encounter every edge in the graph exactly once.

**Eulerian Walk and Cycle Characterization:** A connected graph has an Eulerian walk if and only if the number of vertices with odd degree is 0 or 2. A connected graph has an Eulerian cycle if and only if every vertex has even degree.

A **Hamiltonian path** is a path that encounters every vertex in the graph. A **Hamiltonian cycle** is a cycle that encounters every vertex in the graph. A graph containing a Hamiltonian cycle is said to be **Hamiltonian**. It is in general difficult to determine whether these paths and cycles exist. The only real useful tool at our disposal is Dirac's Theorem.

**Theorem 13.4** (Dirac's theorem). Let  $n \geq 3$ . Suppose a graph  $G$  has  $n$  vertices and the degree of each vertex is at least  $\lceil \frac{n}{2} \rceil$ . Then  $G$  has a Hamiltonian cycle.

In a graph with  $E$  edges, the sum of degrees of each vertex is  $2E$ .

A Eulerian path is a path that visits each edge exactly once. For a connected path, a Eulerian path exists if and only if the number of vertices with odd degree is 0 or 2. If there are no vertices with odd degree, the path will return to the start forming a circuit.

**Theorem 13.5** (Turan's theorem). Let  $G$  be a graph with  $V$  vertices and  $E$  edges and let  $2 \leq r \leq V$ . If there are no  $r$ -cliques,

$$E \leq \frac{V^2}{2} \left( 1 - \frac{1}{r-1} \right).$$

**Berge's lemma:** An augmenting path is a path that starts and ends on unmatched vertices, and alternates between edges in and not in the matching. A matching is maximum if and only if there is no augmenting path.

**Theorem 13.6** (Four colour theorem). A map can be coloured with 4 colours such that adjacent regions have different colours.

**Theorem 13.7** (Hall's marriage theorem). In a bipartite graph with bipartitions  $X$  and  $Y$ , we wish to match each vertex in  $X$  to a different vertex in  $Y$ .

For a subset  $W$  of  $X$ , let  $N(W)$  be the neighbourhood of  $W$  (the set of all vertices in  $Y$  which are connected to some vertex in  $W$ ).

There is a perfect matching for  $X$  if and only if for every subset  $W$  of  $X$ ,  $|N(W)| \geq |W|$ .

Konig's theorem Max-flow min-cut theorem Dilworth's theorem

## Exercises

**Problem 126** (Vietnam 1969). A graph  $G$  has  $n + k$  vertices. Let  $A$  be a subset of  $n$  vertices of the graph  $G$ , and  $B$  be a subset of other  $k$  vertices. Each vertex of  $A$  is joined to at least  $k - p$  vertices of  $B$ . Prove that if  $np < k$  then there is a vertex in  $B$  that can be joined to all vertices of  $A$ .

**Solution.** Denote the number of edges between vertices of  $A$  and  $B$  by  $s$ . We prove by contradiction. Assume otherwise, that there is no vertex of  $B$  that can be joined to all vertices of  $A$ . Then  $s \leq k(n - 1)$ . On the other hand, since each vertex of  $A$  can be joined to at least  $k - p$  vertices of  $B$ ,  $s \geq n(k - p)$ . Moreover, by the hypothesis,  $np < k$ . This inequality gives  $n(k - p) = nk - np > nk - k = k(n - 1)$ . Thus  $s \leq k(n - 1) < n(k - p) \leq s$ , which is impossible.  $\square$

**Problem 127** (USA TSTST 2023 P4). Let  $n \geq 3$  be an integer and let  $K_n$  be the complete graph on  $n$  vertices. Each edge of  $K_n$  is colored either red, green, or blue. Let  $A$  denote the number of triangles in  $K_n$  with all edges of the same color, and let  $B$  denote the number of triangles in  $K_n$  with all edges of different colors. Prove

$$B \leq 2A + \frac{n(n-1)}{3}.$$

(The complete graph on  $n$  vertices is the graph on  $n$  vertices with  $\binom{n}{2}$  edges, with exactly one edge joining every pair of vertices. A triangle consists of the set of  $\binom{3}{2} = 3$  edges between 3 of these  $n$  vertices.)

**Solution.** Let  $C$  denote the number of triangles in  $K_n$  with two edges the same color and the third edge a different color. Let  $r_i, g_i, b_i$  be the number of red, green, and blue edges (respectively) emanating from vertex  $i$ . Let  $c_i$  and  $a_i$  denote the number of  $C$  triangles and  $A$  triangles vertex  $i$  is a part of (respectively). Notice that

$$c_i + a_i = \binom{r_i}{2} + \binom{g_i}{2} + \binom{b_i}{2}$$

Summing over  $i$ ,

$$\sum_i (c_i + a_i) = C + 3A = \sum_i \left( \binom{r_i}{2} + \binom{g_i}{2} + \binom{b_i}{2} \right)$$

Because each  $C$  triangle is counted only by the vertex connecting the two edges with the same color, and each  $A$  triangle is counted by each vertex. Now by Jensen,

$$C + 3A \geq 3n \binom{\frac{2\binom{n}{2}}{3n}}{2} = \binom{n}{3} - \frac{n(n-1)}{3}$$

Because  $\sum_i (r_i + b_i + g_i)$  is just twice the number of edges in  $K_n$ . Noting  $A + B + C = \binom{n}{3}$  finishes the problem.  $\square$

**Part V**

**Other Topics**

# 14 Proofs

## §14.1 Induction

**Theorem 14.1** (Principle of Mathematical Induction (PMI)). Let  $P(n)$  be a family of statements indexed by  $\mathbf{Z}^+$ . Suppose that

- (i) (**base case**)  $P(1)$  is true and
- (ii) (**inductive step**) for all  $k \in \mathbf{Z}^+$ ,  $P(k) \implies P(k+1)$ .

Then  $P(n)$  is true for all  $n \in \mathbf{Z}^+$ .

### Exercise 57

Prove that for all positive integers  $n$ ,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

*Proof.* The statement is true for  $n = 1$  (base case) because with  $n = 1$ ,  $\text{LHS} = \text{RHS} = 1$ .

Assume that the statement is true for some  $n = k$ , where  $k \in \mathbf{Z}^+$ . By our induction hypothesis, we have  $1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}$ .

To show that the statement is true for  $k+1$ ,

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(k+1)[(k+1)+1]}{2} \end{aligned}$$

Since  $P(1)$  is true and  $P(k) \implies P(k+1)$ , by mathematical induction,  $P(n)$  is true for all positive integers  $n$ .  $\square$

Another variant on induction is when the inductive step relies on some earlier case(s) but not necessarily the immediately previous case. This is known as *strong induction*:

**Theorem 14.2** (Strong Form of Induction). Let  $P(n)$  be a family of statements indexed by the natural numbers. Suppose that

- (i) (**base case**)  $P(1)$  is true and
- (ii) (**inductive step**) for all  $m \in \mathbf{Z}^+$ , if for integers  $k$  with  $1 \leq k \leq m$ ,  $P(k)$  is true then  $P(m+1)$  is true.

Then  $P(n)$  is true for all  $n \in \mathbf{N}$ .

**Theorem 14.3** (Cauchy Induction). Let  $P(n)$  be a family of statements indexed by  $\mathbf{Z}_{\geq 2}^+$ . Suppose that

- (i) (**base case**)  $P(2)$  is true and
- (ii) (**inductive step**) for all  $k \in \mathbf{Z}^+$ ,  $P(k) \implies P(2k)$  and  $P(k) \implies (k-1)$ .

Then  $P(n)$  is true for all  $n \in \mathbf{Z}_{\geq 2}^+$ .

# 15 Riemann Integrals

## §15.1 Riemann Sums

**Riemann sums** are an infinite sequence of sums that converges to an integral.

Given  $y = f(x)$ , we want to find the integral on the  $x$ -interval  $[0, 1]$ .

We first split the interval  $[0, 1]$  into  $n$  equal subintervals

$$\left[0, \frac{1}{n}\right], \left[\frac{1}{n}, \frac{2}{n}\right], \dots, \left[\frac{n-1}{n}, 1\right]$$

as shown in the figure below.

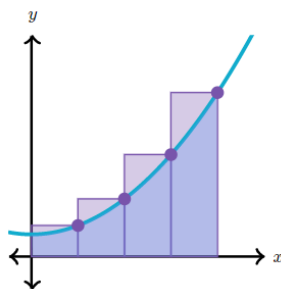


Figure 15.1: Riemann sum

Considering the height of the rectangles, there is not much difference between choosing the left and right values, but the right value is usually chosen because it's simpler for calculation. Hence for the  $k$ -th subinterval  $\left[\frac{k-1}{n}, \frac{k}{n}\right]$  where  $k = 1, \dots, n$ , the height of rectangle is  $f\left(\frac{k}{n}\right)$ . Thus the area of the  $k$ -th rectangle is given by

$$\frac{1}{n} f\left(\frac{k}{n}\right).$$

Therefore, the integral is obtained by summing up the area of  $n$  rectangles; that is,

$$\int_0^1 f(x) \, dx = \lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{n} f\left(\frac{k}{n}\right). \quad (15.1)$$

**Exercise 58**

Find the values of the following expressions:

- (a)  $\lim_{n \rightarrow \infty} \left( \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \right)$
- (b)  $\lim_{n \rightarrow \infty} \frac{1}{n} \left( e^{\frac{1}{n}} + e^{\frac{2}{n}} + \cdots + e^1 \right)$
- (c)  $\lim_{n \rightarrow \infty} \frac{\sqrt{n+1} + \sqrt{n+2} + \cdots + \sqrt{2n}}{n\sqrt{n}}$
- (d)  $\lim_{n \rightarrow \infty} \left( \frac{1}{\sqrt{n(n+1)}} + \frac{1}{\sqrt{n(n+2)}} + \cdots + \frac{1}{\sqrt{n(4n)}} \right)$
- (e)  $\lim_{n \rightarrow \infty} \frac{1}{n} \left( \frac{1}{\sqrt{n^2}} + \frac{1}{\sqrt{n^2+1}} + \cdots + \frac{1}{\sqrt{2n^2}} \right)$

**Solution.**

(a)

$$\begin{aligned}
 & \lim_{n \rightarrow \infty} \left( \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \right) \\
 &= \lim_{n \rightarrow \infty} \frac{1}{n} \left( \frac{1}{1 + \frac{1}{n}} + \frac{1}{1 + \frac{2}{n}} + \cdots + \frac{1}{1 + \frac{n}{n}} \right) \\
 &= \int_0^1 \frac{1}{1+x} dx = [\ln(1+x)]_0^1 = \boxed{\ln 2}
 \end{aligned}$$

Note that in this case  $f(x) = \frac{1}{1+x}$ .

(b)

$$\begin{aligned}
 & \lim_{n \rightarrow \infty} \frac{1}{n} \left( e^{\frac{1}{n}} + e^{\frac{2}{n}} + \cdots + e^1 \right) \\
 &= \int_0^1 e^x dx = [e^x]_0^1 = \boxed{e-1}
 \end{aligned}$$

Note that in this case  $f(x) = e^x$ .

(c)

$$\begin{aligned}
 & \lim_{n \rightarrow \infty} \frac{\sqrt{n+1} + \sqrt{n+2} + \cdots + \sqrt{2n}}{n\sqrt{n}} \\
 &= \lim_{n \rightarrow \infty} \frac{1}{n} \left( \sqrt{1 + \frac{1}{n}} + \sqrt{1 + \frac{2}{n}} + \cdots + \sqrt{1 + \frac{n}{n}} \right) \\
 &= \int_0^1 \sqrt{1+x} dx = \left[ \frac{2}{3} (1+x)^{\frac{3}{2}} \right]_0^1 = \boxed{\frac{2}{3} (2\sqrt{2} - 1)}
 \end{aligned}$$

Note that in this case  $f(x) = \sqrt{1+x}$ .



(d)

$$\begin{aligned}
& \lim_{n \rightarrow \infty} \left( \frac{1}{\sqrt{n(n+1)}} + \frac{1}{\sqrt{n(n+2)}} + \cdots + \frac{1}{\sqrt{n(4n)}} \right) \\
&= \lim_{n \rightarrow \infty} \sum_{k=1}^{3n} \frac{1}{n} \left( \frac{1}{\sqrt{1 + \frac{k}{n}}} \right) \\
&= \int_0^3 \frac{1}{\sqrt{1+x}} dx = \left[ 2\sqrt{1+x} \right]_0^3 = \boxed{2}
\end{aligned}$$

Note that the sum itself is the sum of  $3n$  rectangles, with their heights determined by  $f(x)$  from  $x = 0$  to  $x = 3$ .

(e)

$$\begin{aligned}
& \lim_{n \rightarrow \infty} \frac{1}{n} \left( \frac{1}{\sqrt{n^2}} + \frac{1}{\sqrt{n^2+1}} + \cdots + \frac{1}{\sqrt{2n^2}} \right) \\
&= \lim_{n \rightarrow \infty} \frac{1}{n^2} \left( \frac{1}{\sqrt{1 + \frac{1}{n^2}}} + \frac{1}{\sqrt{1 + \frac{2}{n^2}}} + \cdots + \frac{1}{\sqrt{1 + \frac{n^2}{n^2}}} \right) \\
&= \int_0^1 \frac{1}{\sqrt{1+x}} dx = \left[ 2\sqrt{1+x} \right]_0^1 = \boxed{2(\sqrt{2}-1)}
\end{aligned}$$

Note that the interval  $[0, 1]$  is divided into  $n^2$  subintervals.

□

**Exercise 59**

(a) Prove that for any positive integer  $n \geq 2$ ,

$$2\sqrt{n} - 2 < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n} - 1.$$

(b) Compare the sizes between  $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}}$  and  $2\sqrt{n} - \frac{3}{2}$ .

(c) Find the integer part of  $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{2023}}$ .

**Solution.**

(a) The sum  $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}}$  is relevant area under the graph  $y = \frac{1}{x}$ , in the interval  $[1, n]$ . By integration, this area is  $2\sqrt{n} - 2$ .

On the other hand, consider the area to be approximated by rectangles under the graph, then this approximation is  $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}}$ . Because all these rectangles are under the graph, we have

$$\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n} - 2$$

or

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n} - 1.$$

Consider these rectangles to cover the area under the graph. The same area can be covered if we consider the slightly higher rectangles which use the  $f$ -value of each of the left endpoints. So we have  $1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n-1}} > 2\sqrt{n} - 2$ .

(b) Consider the sum of trapeziums instead of just rectangles.

For each interval  $[k, k+1]$ , we use  $f(k)$  and  $f(k+1)$  for the two heights of the trapezium. Thus the area of one such trapezium is  $\frac{1}{2} \left( \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}} \right)$ . Hence the total area over the interval  $[1, n]$  is

$$\frac{1}{2} \cdot 1 + \left( \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n-1}} \right) + \frac{1}{2} \cdot \frac{1}{\sqrt{n}}.$$

Since the graph  $y = \frac{1}{\sqrt{x}}$  is convex, the trapeziums do in fact cover the area under its graph. Thus

$$\frac{1}{2} \cdot 1 + \left( \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n-1}} \right) + \frac{1}{2} \cdot \frac{1}{\sqrt{n}} > 2\sqrt{n} - 2$$

or

$$1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n-1}} + \frac{1}{2} \cdot \frac{1}{\sqrt{n}} > 2\sqrt{n} - \frac{3}{2}.$$

(c) From (b) we have

$$2\sqrt{n} - \frac{3}{2} < 1 + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n} - 1.$$

Substituting  $n = 2025$  gives

$$\begin{aligned} 1 + \cdots + \frac{1}{\sqrt{2023}} &< 1 + \cdots + \frac{1}{\sqrt{2025}} < 2(45) - 1 = 89 \\ 1 + \cdots + \frac{1}{\sqrt{2023}} &= 1 + \cdots + \frac{1}{\sqrt{2025}} - \frac{1}{\sqrt{2024}} - \frac{1}{\sqrt{2025}} \\ &> 2(45) - \frac{3}{2} - \frac{1}{\sqrt{2024}} - \frac{1}{\sqrt{2025}} \end{aligned}$$

The only thing left to do is to show that  $\frac{1}{\sqrt{2024}} + \frac{1}{\sqrt{2025}} < \frac{1}{2}$ , which is obviously true.

Hence  $1 + \cdots + \frac{1}{\sqrt{2023}} > 2(45) - 2 = 88$  so the integer part is 88.

□

## §15.2 Double Integrals

### Exercise 60

Find the value of the sum

$$\lim_{n \rightarrow \infty} \sum_{k,l=1}^n \frac{1}{n^2 + kl}.$$

**Solution.** Consider the double integral

$$\iint_{[0,1] \times [0,1]} f(x, y) \, dx \, dy.$$

We approximate using cuboids under the graph; split this region up by slicing horizontally and vertically into  $n$  slices each. Each cuboid has side length  $\frac{1}{n}$ ,  $n^2$  cuboids in total.

Hence

$$\begin{aligned} & \iint_{[0,1] \times [0,1]} f(x, y) \, dx \, dy \\ &= \lim_{n \rightarrow \infty} \frac{1}{n^2} \sum_{k,l=1}^n \frac{1}{1 + \frac{k}{n} \frac{l}{n}} \\ &= \iint_{[0,1] \times [0,1]} \frac{1}{1 + xy} \, dx \, dy \\ &= \iint_{[0,1] \times [0,1]} (1 - xy + x^2y^2 - x^3y^3 + \dots) \, dx \, dy \end{aligned}$$

Note that

$$\iint_{[0,1] \times [0,1]} x^k y^k \, dx \, dy = \int_{[0,1]} x^k \, dx \int_{[0,1]} y^k \, dy = \frac{1}{(k+1)^2}.$$

Hence

$$\begin{aligned} & \iint_{[0,1] \times [0,1]} (1 - xy + x^2y^2 - x^3y^3 + \dots) \, dx \, dy \\ &= 1 - \frac{1}{2^2} + \frac{1}{3^2} - \frac{1}{4^2} + \dots \\ &= \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots\right) - 2\left(\frac{1}{2^2} + \frac{1}{4^2} + \dots\right) \\ &= \frac{\pi^2}{6} - 2 \cdot \frac{1}{2^2} \cdot \frac{\pi^2}{6} = \boxed{\frac{\pi^2}{12}} \end{aligned}$$

where we have applied the solution for Basel's problem. □

Double integrals are usually calculated by integrating the terms one by one.

### Exercise 61

Find the value of the following integral:

$$\iint_{[-2,2] \times [-1,1]} x^2 |y|^3 \, dx \, dy$$

**Solution.**

$$\begin{aligned}
 & \iint_{[-2,2] \times [-1,1]} x^2 |y|^3 \, dx \, dy \\
 &= \int_{[-2,2]} \left( \int_{[-1,1]} x^2 |y|^3 \, dy \right) dx \\
 &= \int_{[-2,2]} dx \int_{[-1,1]} x^2 |y|^3 \, dy \\
 &= 4 \int_0^2 dx \int_0^1 x^2 y^3 \, dy \quad x^2 |y|^3 \text{ is even wrt to both } x \text{ and } y \\
 &= 4 \int_0^2 \left[ \frac{x^2 y^4}{4} \right]_0^1 dx \\
 &= \int_0^2 x^2 \, dx = \left[ \frac{x^3}{3} \right]_0^2 = \frac{8}{3}
 \end{aligned}$$

□

One other simplification method:  $x^2 |y|^3$  is separable because it is an expression in the form  $f(x)g(y)$ , and the region of integration is a product set  $A \times B$ , then

$$\iint_{A \times B} f(x)g(y) \, dx \, dy = \int_A f(x) \, dx \cdot \int_B g(y) \, dy$$

*Proof.*

$$\begin{aligned}
 & \iint_{A \times B} f(x)g(y) \, dx \, dy \\
 &= \int_A \left( \int_B f(x)g(y) \, dy \right) dx \\
 &= \int_A \left( f(x) \int_B g(y) \, dy \right) dx \\
 &= \int_A k f(x) \, dx \quad \text{where } k = \int_B g(y) \, dy \text{ is constant wrt } x \\
 &= k \int_A f(x) \, dx \\
 &= \int_A f(x) \, dx \cdot \int_B g(y) \, dy
 \end{aligned}$$

□

### Exercise 62

Find the values of the following integrals:

- (a)  $\int_0^{\sqrt{3}} dx \int_0^1 \frac{8x}{(x^2 + y^2 + 1)^2} dy$
- (b)  $\iint_D (x + y) \, dx \, dy$ , where  $D$  is the region enclosed by  $y = e^x$ ,  $y = 1$ ,  $x = 0$  and  $x = 1$ .
- (c)  $\iint_D x^2 y^2 \, dx \, dy$ , where  $D$  is the region enclosed by  $x^2 + y^2 = 1$ .

### Exercise 63

Find the volume of the region enclosed by the surfaces  $z = x^2 + y^2$  and  $z = 2x - y + 2$ .

### Exercise 64

Two numbers  $a$  and  $b$  are chosen randomly from the interval  $[0, 2]$ . Find the expected value of their product.

**Exercise 65**

Two points  $P$  and  $Q$  are chosen randomly on the line segment  $AB$ . Find the expected value of the volume of a cuboid of side lengths  $AP$ ,  $PQ$  and  $QB$ .

## Exercises

**Problem 128** (SMO (Open) 2020 Q10). Find the value of

$$S = \lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{\sqrt{n(n+k)}}$$

**Solution.**

$$S = \lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{n} \sqrt{\frac{1}{1 + \frac{k}{n}}} = \int_0^1 \frac{1}{\sqrt{1+x}} dx = \boxed{2\sqrt{2} - 2}$$

□

**Problem 129** (SMO (Open) 2018 Q12). Given that

$$S = \lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{n+k}$$

Find the value of  $S$ .

**Solution.**

$$S = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \frac{1}{1 + \frac{k}{n}} = \int_0^1 \frac{1}{1+x} dx = \boxed{\ln 2}$$

□

**Problem 130** (SMO (Open) 2018 Q10). Find the smallest integer  $r$  such that

$$1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{4}} + \cdots + \frac{1}{\sqrt{2018}} \leq r\sqrt{2018}.$$

**Solution.** Consider Riemann sum of  $y = \frac{1}{\sqrt{x}}$ . Then

$$\begin{aligned} & 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{4}} + \cdots + \frac{1}{\sqrt{2018}} \\ & < \int_0^{2018} \frac{1}{\sqrt{x}} dx \\ & = \left[ \frac{x^{\frac{1}{2}}}{\frac{1}{2}} \right]_0^{2018} \\ & = 2\sqrt{2018}. \end{aligned}$$

□

# 16 Strategy Games

## Exercises

**Problem 131** (Princess Problem). On the top floor of a castle lives a princess. The floor has 17 bedrooms arranged in a row. Each bedroom has doors connecting to the adjoining bedrooms as well as to the outside corridor. The princess sleeps in a different bedroom each night by opening the door to an adjoining bedroom and spending the night and the next day in that room.

One day a prince arrives at the castle and is desirous of marrying the princess. The guardian angel at the castle tells him of the princess' sleeping patterns and informs him that each morning he may knock on one of the outside doors. If the princess happens to be behind that door, she will open it and consent to marry him. The prince also has a return ticket to his kingdom in 30 days, so he can make at most 30 attempts. Can the prince win the hand of the princess, and if so, what is his strategy?

**Solution.** The main idea is that the princess switches parity every day.

The strategy is the Prince should knock on the second door from one of the ends of the corridor (call it door #2), and knock on the next adjacent door each successive day until he reaches the second door from the opposite end of the corridor (door #16). The day after that, he should begin the same process in reverse order (meaning he will knock on the 16th door two days in a row). By the time he reaches his starting point (door #2 on the 30th day), he will have found the princess.

Number the doors 1 thru 17. If the princess occupies an even numbered room on the day the prince first knocks on a door (#2), then she will either occupy the same room he knocks on or she will be an even number of rooms away. Since both move to an adjacent room each day, this will hold true so she will never be in a room adjacent to the one he knocks on, and thus never be in a position to move past him the next day. She will have nowhere else to go by the time he reaches the 16th door, and will have by then been located. If she, on the other hand, was in an odd numbered room when he began, then she will be in an even numbered room when the prince starts the process again on day 16 (when he knocks on door #16 the second time).

To visualise this, the pink squares are rooms where the princess could be on the given day, the blue squares are where the prince knocks that day, and the black squares are rooms in which she logically cannot be. On day 30 all rooms but room 2 have been eliminated, meaning that if the prince has not found the princess already, he will find her there on day 30.

		Room:																
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Day:	1																	
	2																	
	3																	
	4																	
	5																	
	6																	
	7																	
	8																	
	9																	
	10																	
	11																	
	12																	
	13																	
	14																	
	15																	
	16																	
	17																	
	18																	
	19																	
	20																	
	21																	
	22																	
	23																	
	24																	
	25																	
	26																	
	27																	
	28																	
	29																	
	30																	

□