# Theorems and lemmas in mathematics

Leen Jun Khye

# Theorems and lemmas in mathematics

Leen Jun Khye

# Preface

In recent years, the culture of mathematical competitions has been growing rapidly in Malaysia. More and more secondary-school and high-school mathematics enthusiasts are eager to test their skills on contest problems. I have had the honor of serving as a member of the Malaysian National Training Team for the International Mathematical Olympiad (BIMO). As I approach the end of my competitive career, I wish to consolidate the mathematics I' ve learned over these years, and thus this book was born.

This book is a compendium of theorems and results that frequently appear in mathematical Olympiads. Its purpose is to present each topic clearly, eliminate information gaps, and serve as a "mathematical dictionary." Beginners will find concise statements of the key ideas in each area, while seasoned competitors can review known theorems and proofs—or discover new results.

Proofs in this book are given primarily to justify why a result is true; they are intended as references rather than detailed expositions of proof strategies. This book is aimed at all scholars: secondary-school students, undergraduates, IMO trainees, graduate students, teachers, and coaches alike.

I have endeavored to collect as many elementary theorems and corollaries as possible. Personally, writing this book will motivate me to continue learning after I retire from competition, and future editions will naturally introduce more advanced material.

Because this book is authored solely by me, I apologize in advance for any typos or inaccuracies in the statements or proofs. Corrections and feedback are warmly welcomed; please contact me at +60 11-5854 4151. Thank you in advance for your understanding.

Because of my own limitations, many more general forms of theorems (for example, Minkowski' s inequality in $L^p$ spaces) are not included here, but the material should more than suffice for high-school–level competitions.

At present I am preparing for A-levels, so many chapters are still incomplete: the sections on number theory, geometry, and advanced topics do not yet have their illustrations, and several well-known theorems (such as Lagrange’ s theorem in the theory of orders and primitive roots, and various trigonometric identities) have not been included. Therefore, this edition is titled “Version 0.” The first complete edition is planned for release in February next year.

Should you wish to submit any results not yet included, please contact the author; your contribution will broaden the mathematical horizons of many.

**This book is not for profit, but provided purely for sharing.**

# Acknowledgments

First, I thank the Malaysian IMO Training Team for giving countless Malaysian mathematics enthusiasts the opportunity to learn so much, free of charge. I also thank our dedicated coaches who, without any funding, have organized BIMO so effectively—especially head coach Ivan Chan, the coaching staff, and senior squad members—including Wong Jer Ren, Kwong Weng, Sean Sze Khai and all other squad members—for their selfless sharing of mathematical knowledge and excellent references. Many thanks to Tristan Chaang for answering my questions about writing this book. I am grateful to all my friends, both within and outside BIMO, for their support and companionship, and to my parents—my first math teachers and the pillars of my family. Finally, I acknowledge the Art of Problem Solving community and the “数之谜” platform for providing outstanding venues for mathematics enthusiasts to exchange ideas. Theorems collected in this book are mainly referenced from AoPS, Wikipedia, “数之谜,” and various papers (in particular, those in the chapters on polynomials and integer-coefficient polynomials). The front-of-chapter illustration for the Algebra section references the cover of the Capybara Go mobile game.

（PS: the original statement is written in Chinese, then translated into English, if there’s any confusion, pls refer to the Chinese version.）

# 前言

近年来数学竞赛的风气在马来西亚日益增长，越来越多初高中数学爱好者跃跃欲试。笔者 (本人) 是马来西亚数学奥林匹克国家集训队（BIMO）的队员，随着年岁的增长，现已接近退役年龄，希望能把这几年学习的数学知识整合在一起，便萌生撰写此书的想法。

本书汇集了奥林匹克数学竞赛中常见的一些定理和结论，旨在使大纲脉络清晰，消除信息差，可作为“数学词典”使用，让初学者可以快速了解各领域的核心知识点，也可以让备赛多年的老将温习定理内容及其证明，甚至学习到新的结论。

本书中的证明多作为参考，以说明结论为何成立，而非详尽剖析证明思路。读者对象涵盖所有学者，无论是中学生、大学生、正在备赛的竞赛生，亦或是研究生，以及数学教师和竞赛教练都适用。

笔者会尽可能汇总初等数学中尽可能多的定理及结论；从个人角度来说，这也会促使我在退役之后依然继续学习新的数学知识，理所当然的也会在后续版本逐步引入一些高等内容。

因本书由本人独立撰写，若有错别字或定理、证明错误，敬请包涵，并欢迎拨打 +60 11-5854 4151 予以反馈指正，在此先行致谢。

由于笔者水平有限，许多定理的更一般形式（如在 $L^p$ 空间的 Minkowski 不等式）并不会囊括在此书当中，但应足以应对高中数学竞赛。

目前笔者正备考 A Level，本书诸多章节尚未完善，甚至数论、几何及高等章节的插画都还没画，一些熟知定理也尚未收录（如阶和原根中的 Lagrange 定理及三角恒等式等），故本版本命名为“第 0 版”。正式第一版预计将在明年二月发布。

如有意投稿未录入的结论，亦请联系笔者，您的分享将拓宽更多人的数学视野。

**本书无任何盈利，仅为纯粹分享。**

# 致谢

首先感谢马来西亚 IMO 集训队，让无数数学爱好者免费学习到海量数学知识；感谢教练组在没有任何拨款下仍有序管理 BIMO，尤其感谢国家队主教练 Ivan Chan 及教练组成员与集训队学长们；特别感谢 Wong Jer Ren、Kwong Weng、Sean Sze Khai 以及所有 squad 成员无私分享数学知识与优秀书籍；感谢 Tristan Chaang 解答我对写书的疑问；感谢 BIMO 及非 BIMO 的朋友们一路以来的陪伴；感谢我的数学启蒙人——我的父亲，以及家庭的后盾——我的母亲；最后感谢 AoPS 和“数之谜”平台，为数学爱好者提供优秀的交流平台。本书中定理的收集主要参考 AoPS、维基百科、“数之谜”及相关论文（多项式和整系数多项式章节内容尤多参考“数之谜”）。代数章节前插画形象参考 Capybara Go 手游封面。

17/7/2024

# Contents

$\forall P \in \mathbb{C}[x]$ , $\exists z$ s.t $P(z) = 0$
$\vec{a} \cdot \vec{b} = |\vec{a}||\vec{b}| \cos\theta$
$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
$e^{i\pi} + 1 = 0$
?
ALGEBRA

# Chapter 1

# Algebra

## 1.1 Inequality

### Theorem 1 *QM-AM-GM-HM Inequality*

**Statement:**

For $x_1, x_2, ..., x_n \in \mathbb{R}_{>0}, n \geq 1$, defined

$$\text{Quadratic mean}: Q_n = \sqrt{\frac{1}{n}\sum_{i=1}^{n} {x_i}^2},$$

$$\text{Arithmetic mean}: A_n = \frac{1}{n}\sum_{i=1}^{n} x_i,$$

$$\text{Geometric mean}: G_n = \sqrt[n]{\prod_{i=1}^{n} x_i},$$

$$\text{Harmonic mean}: H_n = \frac{n}{\displaystyle\sum_{i=1}^{n} \frac{1}{x_i}}.$$

Then $Q_n \geq A_n \geq G_n \geq H_n$. The equalities hold if and only if $x_1 = x_2 = ... = x_n$.

*2-variable form:*

$$\sqrt{\frac{a^2+b^2}{2}} \geq \frac{a+b}{2} \geq \sqrt{ab} \geq \frac{2}{\frac{1}{a}+\frac{1}{b}}.$$

**Proof:**
*QM-AM inequality*

*Method 1:* (*prove by vector*)
Consider $\vec{a} = (x_1, x_2, ..., x_n), \vec{b} = (1, 1, ..., 1)$, then

$$\sum_{i=1}^{n} x_i = \vec{a} \cdot \vec{b} = |\vec{a}| \cdot |\vec{b}| \cos\theta \leq |\vec{a}| \cdot |\vec{b}| = \sqrt{n\sum_{i=1}^{n} {x_i}^2}.$$

Multiply both side by $\dfrac{1}{n}$ and we are done. ■

*Method 2:* (*probabilistic method*)
Consider random variable $\boldsymbol{X} = \{x_1, x_2, ..., x_n\}$ , then

$$\operatorname{Var}(\boldsymbol{X}) = \frac{1}{n}\sum_{i=1}^{n} {x_i}^2 - \left(\frac{1}{n}\sum_{i=1}^{n} x_i\right)^2.$$

The result is followed by the fact that variance is non-negative. ■

*AM-GM inequality*

*Method 1:* (*backward induction*)
We first prove that $2^n$ works for $\forall n \in \mathbb{Z}_{\geq 0}$: The case $n = 0$ is trivial, suppose that AM-GM Inequality is true for some $2^k$, then for $n = 2^{k+1}$

$$\sum_{i=1}^{2^{k+1}} x_i = \sum_{i=1}^{2^k} x_i + \sum_{i=2^k+1}^{2^{k+1}} x_i \geq 2^k \cdot \sqrt[2^k]{\prod_{i=1}^{2^k} x_i} + 2^k \cdot \sqrt[2^k]{\prod_{i=2^k+1}^{2^{k+1}} x_i} \geq 2^k\left(2 \cdot \sqrt[2^{k+1}]{\prod_{i=1}^{2^{k+1}} x_i}\right) = 2^{k+1} \cdot \prod_{i=1}^{2^{k+1}} x_i.$$

Now we prove that if $n = k$ works, then $n = k + 1$ works too: Consider $x_1, x_2, ..., x_{k-1}, x_k$ where we choose $x_k = \frac{1}{k-1}\sum_{i=1}^{k-1} x_i$ then since

$$\frac{1}{k}\sum_{i=1}^{k} x_i \geq \sqrt[k]{\prod_{i=1}^{k} x_i}$$

is true, we substitute the value of $x_k$ inside the inequality obtain

$$\frac{1}{k}\sum_{i=1}^{k} x_i = \frac{(k-1)\sum_{i=1}^{k-1} x_i + \sum_{i=1}^{k-1} x_i}{k(k-1)} = \frac{1}{k-1}\sum_{i=1}^{k-1} x_i \geq \sqrt[k]{\prod_{i=1}^{k} x_i} = \sqrt[k]{\frac{1}{k-1}\sum_{i=1}^{k-1} x_i \cdot \prod_{i=1}^{k-1} x_i}.$$

which give us

$$\left(\frac{1}{k-1}\sum_{i=1}^{k-1} x_i\right)^{k-1} \geq \prod_{i=1}^{k-1} x_i.$$

■

*Method 2:* (*direct induction*)
The case $n = 0$ is obvious, suppose that AM-GM Inequality holds true for some $n = k$, then for $n = k + 1$,

$$A_{k+1} = \frac{1}{2k}[(k+1)A_{k+1} + (k-1)A_{k+1}] = \frac{1}{2k}\left[(k-1)A_{k+1} + \sum_{i=1}^{k+1} x_i\right] \geq \frac{1}{2k}\left(k\sqrt[k]{x_{k+1}A_{k+1}^{k-1}} + k\sqrt[k]{\prod_{i=1}^{k} x_i}\right)$$

$$\geq \sqrt[2k]{A_{k+1}^{k-1}\prod_{i=1}^{k+1} x_i} \Rightarrow A_{k+1} \geq G_{k+1}.$$

■

*GM-HM inequality*

By **AM-GM Inequality**,

$$\sqrt[n]{\prod_{i=1}^{n} \frac{1}{x_i}} \leq \frac{1}{n}\sum_{i=1}^{n} \frac{1}{x_i} \Leftrightarrow \sqrt[n]{\prod_{i=1}^{n} x_i} \geq \frac{n}{\sum_{i=1}^{n} \frac{1}{x_i}}$$

■

**Theorem 2** *Cauchy-Schwarz Inequality*

Statement:

For $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in \mathbb{R}$,

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

The equality holds if and only if $a_i = 0$ or $b_i = 0$ for $1 \leq i \leq n$ or $\dfrac{a_i}{b_i} = \dfrac{a_j}{b_j}$ for $1 \leq i \neq j \leq n$.

**Proof:**
*Method 1:* (*prove by algebraic identity*)
We compute

$$\left(\sum_{i=1}^{n} {a_i}^2\right)\left(\sum_{i=1}^{n} {b_i}^2\right)-\left(\sum_{i=1}^{n} a_ib_i\right)^2 = \sum_{1\leq i,j\leq n} {a_i}^2{b_j}^2 - \sum_{1\leq i,j\leq n} a_ib_ia_jb_j = \frac{1}{2}\sum_{1\leq i,j\leq n} {a_i}^2{b_j}^2+{a_j}^2{b_i}^2-2a_ib_ia_jb_j$$

$$= \frac{1}{2}\sum_{1\leq i,j\leq n}(a_ib_j - a_jb_i)^2 \geq 0.$$

■

*Method 2:* (*prove by vector*)
Consider vector $\vec{a} = (a_1, a_2, ..., a_n), \vec{b} = (b_1, b_2, ..., b_n)$, then the dot product

$$\sum_{i=1}^{n} a_ib_i = \vec{a}\cdot\vec{b} = |\vec{a}|\cdot|\vec{b}|\cos\theta \leq |\vec{a}|\cdot|\vec{b}| = \sqrt{\left(\sum_{i=1}^{n} {a_i}^2\right)\left(\sum_{i=1}^{n} {b_i}^2\right)}.$$

■

*Method 3:* (*prove by determinant*)

$$S = \left(\sum_{i=1}^{n} {a_i}^2\right)\left(\sum_{i=1}^{n} {b_i}^2\right) - \left(\sum_{i=1}^{n} a_ib_i\right)^2 = \begin{vmatrix} \sum_{i=1}^{n} {a_i}^2 & \sum_{i=1}^{n} a_ib_i \\ \sum_{i=1}^{n} a_ib_i & \sum_{i=1}^{n} {b_i}^2 \end{vmatrix} = \sum_{i=1}^{n} \begin{vmatrix} \sum_{i=1}^{n} {a_i}^2 & a_ib_i \\ \sum_{i=1}^{n} a_ib_i & {b_i}^2 \end{vmatrix}$$

$$= \sum_{i=1}^{n}\sum_{j=1}^{n} \begin{vmatrix} {a_j}^2 & a_ib_i \\ a_jb_j & {b_i}^2 \end{vmatrix} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_jb_i \begin{vmatrix} a_j & a_i \\ b_j & b_i \end{vmatrix}.$$

Similarly,

$$S = \sum_{i=1}^{n}\sum_{j=1}^{n} a_ib_j \begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} = -\sum_{i=1}^{n}\sum_{j=1}^{n} a_ib_j \begin{vmatrix} a_j & a_i \\ b_j & b_i \end{vmatrix}.$$

Thus,

$$2S = \sum_{i=1}^{n}\sum_{j=1}^{n}(a_jb_i - a_ib_j) \begin{vmatrix} a_j & a_i \\ b_j & b_i \end{vmatrix}. = \sum_{i=1}^{n}\sum_{j=1}^{n}(a_jb_i - a_ib_j)^2 \geq 0.$$

■

## Theorem 3 *Hölder's Inequality*

**Statement:**

*Form 1*:
For $p, q > 0, a_1, a_2, ..., a_n, b_1, b_2, ..., b_n > 0$,

$$\left(\sum_{i=1}^{n} a_i\right)^p \left(\sum_{i=1}^{n} b_i\right)^q \geq \left(\sum_{i=1}^{n} \sqrt[p+q]{{a_i}^p {b_i}^q}\right)^{p+q}.$$

*Form 2:*
For $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \geq 0$, if $p, q > 1$ s.t $\frac{1}{p} + \frac{1}{q} = 1$ then

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

Equality holds when $a_i = 0$ or $b_i = 0, \forall 1 \leq i \leq n$, or $\frac{{a_i}^p}{{b_i}^q} = \frac{{a_j}^p}{{b_j}^q}$, $\forall\ 1 \leq i, j \leq n$.

**Proof:**
One can easily check that *Form 1* and *Form 2* is equivalent, now we prove *Form 1.* Since the inequality is homogeneous, WLOG let $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i = 1$, then by **AM-GM Inequality**,

$$\sum_{i=1}^{n} \sqrt[p+q]{{a_i}^p {b_i}^q} \leq \sum_{i=1}^{n} \frac{pa_i + qb_i}{p+q} = 1.$$

■

***Remark:*** $p = q = 1$ in *Form 1* and $p = q = 2$ in *Form 2* is actually Cauchy-Schwarz Inequality.

## Theorem 4 *Titu's Lemma*

**Statement:**

For $m \geq 0, a_1, a_2, ..., a_n \geq 0, b_1, b_2, ..., b_n > 0$,

$$\sum_{i=1}^{n} \frac{{a_i}^{m+1}}{{b_i}^m} \geq \frac{\left(\sum_{i=1}^{n} a_i\right)^{m+1}}{\left(\sum_{i=1}^{n} b_i\right)^m};$$

Equality holds when $m = 0$ or $a_i = 0, \forall\ 1 \leq i \leq$ or $\frac{a_i}{b_i} = \frac{a_j}{b_j}$, $\forall\ 1 \leq i \neq j \leq n$ for $m \notin${-1,0}.

**Proof:** By **Hölder's Inequality**,

$$\left(\sum_{i=1}^{n} b_i\right)^m \left(\sum_{i=1}^{n} \frac{{a_i}^{m+1}}{{b_i}^m}\right) \geq \left(\sum_{i=1}^{n} a_i\right)^{m+1}.$$

■

## Theorem 5 *Schur's Inequality*

**Statement:**

*Form 1:*
For $a, b, c \geq 0$, $r \geq 0$,

$$\sum_{cyc} a^r(a-b)(a-c) \geq 0.$$

*Form 2:*
For $a, b, c \geq 0$, $r \geq 0$,

$$\sum_{cyc} a^r(a^2+bc) \geq \sum_{cyc} a^{r+1}(b+c).$$

*Form 3:* $(r=1)$
For $a, b, c \geq 0$,

$$a^3+b^3+c^3+3abc \geq \sum_{sym} a^2 b.$$

Equality holds if and only if $a=b=c$ or $a=b, c=0$.

**Proof:** Only need to prove *Form 1*. WLOG let $a \geq b \geq c$, then

$$\sum_{cyc} a^r(a-b)(a-c) = (a-b)[a^r(a-c)-b^r(b-c)] + c^r(c-a)(c-b) \geq 0.$$

The last step is because $a \geq b$ and $c \geq 0$. ■

## Theorem 6 *Power Mean Inequality*

**Statement:**

For $a_1, a_2, ..., a_n > 0, \alpha, \beta \neq 0$, if $\alpha \geq \beta$, then

$$\left(\frac{1}{n}\sum_{i=1}^{n} {a_i}^{\alpha}\right)^{\frac{1}{\alpha}} \geq \left(\frac{1}{n}\sum_{i=1}^{n} {a_i}^{\beta}\right)^{\frac{1}{\beta}}.$$

Equality holds if and only if $a_1 = a_2 = ... = a_n$.

**Proof:** Let $f(x) = x^{\frac{\alpha}{\beta}}, x > 0$, since $\alpha \geq \beta$, then $f''(x) > 0$ which means $f$ convex.
By **Jensen's Inequality**,

$$\frac{1}{n}\sum_{i=1}^{n} f({a_i}^{\beta}) \geq f\left(\frac{1}{n}\sum_{i=1}^{n} {a_i}^{\beta}\right) \Leftrightarrow \frac{1}{n}\sum_{i=1}^{n} ({a_i}^{\beta})^{\frac{\alpha}{\beta}} \geq \left(\frac{1}{n}\sum_{i=1}^{n} {a_i}^{\beta}\right)^{\frac{\alpha}{\beta}} \Leftrightarrow \left(\frac{1}{n}\sum_{i=1}^{n} {a_i}^{\alpha}\right)^{\frac{1}{\alpha}} \geq \left(\frac{1}{n}\sum_{i=1}^{n} {a_i}^{\beta}\right)^{\frac{1}{\beta}}.$$

■

***Remark:*** If denote

$$M(\alpha) = \left(\frac{1}{n}\sum_{i=1}^{n} {a_i}^{\alpha}\right)^{\frac{1}{\alpha}},$$

then

$$M(2) = Q_n, M(1) = A_n, \lim_{\alpha \to 0} M(\alpha) = G_n, M(-1) = H_n,$$
$$\lim_{\alpha \to -\infty} M(\alpha) = \min\{a_1, a_2, ..., a_n\}, \lim_{\alpha \to +\infty} M(\alpha) = \max\{a_1, a_2, ..., a_n\}.$$

## Theorem 7 *Triangle Inequality*

**Statement:**

For $z_i \in \mathbb{C}, 1 \le i \le n$,

$$\left|\sum_{i=1}^{n} z_i\right| \le \sum_{i=1}^{n} |z_i|.$$

**Proof**: We only prove the base case since the inductive step is trivial: Let $z_1, z_2 \in \mathbb{C}$ correspond to the vectors $\overrightarrow{OA}$ and $\overrightarrow{OB}$, respectively. Construct the parallelogram $OACB$, so that $z_1 + z_2$ corresponds to $\overrightarrow{OC}$. In $\triangle OAC$ we have

$$|\overrightarrow{OC}| \;\le\; |\overrightarrow{OA}| \;+\; |\overrightarrow{AC}|.$$

■

## Theorem 8 *Jensen's Inequality*

**Statement:**

Let $f : \mathrm{dom}(f) \to \mathbb{R}$ be a convex function. For any $n \in \mathbb{N}$ and any $\lambda_1, \lambda_2, \ldots, \lambda_n \in (0,1)$ with

$$\sum_{i=1}^{n} \lambda_i = 1,$$

and any $x_1, x_2, \ldots, x_n \in \mathrm{dom}(f)$, we have

$$f\left(\sum_{i=1}^{n} \lambda_i\, x_i\right) \;\le\; \sum_{i=1}^{n} \lambda_i\, f(x_i).$$

**Proof:**

We proceed by induction on $n$. For $n = 1$ the result is trivial. Assume the inequality holds for $n = k$. Consider $\lambda_1, \ldots, \lambda_{k+1} \in (0,1)$ and $x_1, \ldots, x_{k+1} \in \mathrm{dom}(f)$, and set

$$y = \frac{\sum_{i=1}^{k} \lambda_i\, x_i}{1 - \lambda_{k+1}},$$

so that $\displaystyle\sum_{i=1}^{k} \lambda_i = 1 - \lambda_{k+1}$ and

$$\sum_{i=1}^{k+1} \lambda_i\, x_i = (1 - \lambda_{k+1})\, y + \lambda_{k+1}\, x_{k+1}.$$

By convexity,

$$f\left(\sum_{i=1}^{k+1} \lambda_i\, x_i\right) \;\le\; (1 - \lambda_{k+1})\, f(y) + \lambda_{k+1}\, f(x_{k+1}).$$

The inductive hypothesis applied to $y$ gives

$$f(y) \;\le\; \sum_{i=1}^{k} \frac{\lambda_i}{1 - \lambda_{k+1}}\, f(x_i).$$

Combining these yields

$$f\Bigl(\sum_{i=1}^{k+1} \lambda_i\, x_i\Bigr) \;\le\; \sum_{i=1}^{k+1} \lambda_i\, f(x_i),$$

completing the induction. ■

## Definition 1 *Majorizes*

**Description:**

If $x_1 \geq x_2 \geq ... \geq x_n, y_1 \geq y_2 \geq ... \geq y_n,\ s.t$

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

$$\sum_{i=1}^{k} x_i \geq \sum_{i=1}^{k} y_i, \quad \forall\, 1 \leq k \leq n-1,$$

then we said that $(x_1, x_2, ..., x_n)$ **majorizes** $(y_1, y_2, ..., y_n)$, denoted as $(x_1, x_2, ..., x_n) \succ (y_1, y_2, ..., y_n)$.

## Theorem 9 *Karamata's Inequality*

**Statement:**

Let $f : \mathrm{dom}(f) \to \mathbb{R}$ be convex, if $(x_i) \succ (y_i)$, then

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

The reverse inequality holds when $f$ concave.

**Proof:**
*lemma:* if $f$ is convex over interval $(a, b)$, then for $\forall\ a \leq x_1 \leq x_2 \leq b$, we have

$$\frac{f(x) - f(x_1)}{x - x_1} \leq \frac{f(x) - f(x_2)}{x - x_2}.$$

*proof of lemma:* Just do casework on $x \notin \{x_1, x_2\}$.

□

Back to the problem, defined

$$c_i = \frac{f(a_i) - f(b_i)}{a_i - b_i}, \quad A_i = \sum_{j=1}^{i} a_j, A_0 = 0 \quad \text{and} \quad B_i = \sum_{j=1}^{i} b_j, B_0 = 0.$$

Since $a_i \geq a_{i+1}$ and $b_i \geq b_{i+1}$, we get that $c_i \geq c_{i+1}$. Now we can compute

$$\sum_{i=1}^{n} f(a_i) - f(b_i) = \sum_{i=1}^{n} c_i(a_i - b_i) = \sum_{i=1}^{n} c_i(A_i - A_{i-1} - B_i + B_{i-1}) = \sum_{i=1}^{n} c_i(A_i - B_i) - \sum_{i=0}^{n-1} c_{i+1}(A_i - B_i) = (*)$$

and since $A_n = B_n$,

$$(*) = \sum_{i=1}^{n-1} c_i(A_i - B_i) - \sum_{i=0}^{n-1} c_{i+1}(A_i - B_i) = \sum_{i=1}^{n} (c_i - c_{i+1})(A_i - B_i) \geq 0.$$

■

### Theorem 10 *Muirhead's Inequality*

**Statement:**

For $a_1, a_2, ..., a_n \geq 0$, if $(x_1, x_2, ..., x_n) \succ (y_1, y_2, ..., y_n)$, then

$$\sum_{sym} \prod_{i=1}^{n} a_i^{x_i} \geq \sum_{sym} \prod_{i=1}^{n} a_i^{y_i}.$$

*some useful result from Muirhead's Inequality:*
$(2,0,0) \succ (1,1,0)$,

$$(a+b+c)^2 \geq \frac{3}{2} \sum_{cyc} a(b+c).$$

$(2,1,0) \succ (1,1,1)$,

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

$(a,b) \succ (k,t)$ *for some* $k < a, k+t = a+b$, *e.g* $(5,1) \succ (4,2)$,

$$x^5y + xy^5 \geq x^4y^2 + x^2y^4.$$

**Proof:** (*by Lau Chi Hin*)
Let $(p_i) \succ (q_i)$, $1 \leq i \leq n$, then there $\exists j, k,\ j < k,\ s.t\ \ p_j > q_j, p_k < q_k$ and hence $p_j > q_j > q_k > p_k$. Let $b = \frac{p_j+p_k}{2}, d = \frac{p_j-p_k}{2}$ then $[b-d, b+d] = [p_k, p_j] \supset [q_k, q_j]$. Let $c = \max\{|q_j - b|, |q_k - b|\}$ then $c < d$ because if $c = q_l - b$ for $l \in \{j,k\}$ since $q_l < b+d$, then $q_l - b < c$ and if $c = b - q_l$ then since $q_l > b - d$, we also obtain $b - q_l < d$. Consider $(r_i)$ $s.t\ \ r_i = p_i$ except $r_j = b+c, r_k = b-c$, then either $r_j = q_j, r_k = 2b - q_j = p_j + p_k - q_j$ or $r_k = q_k, r_j = p_j + p_k - q_k$ because if $|q_j - b| > |q_k - b|$ then $q_j - b$ can only be non-negative since $q_j > q_k$ and if $|q_j - b| < |q_k - b|$ then $q_k - b$ can only be non-negative, then substitute the value of $c$ into $r_j, r_k$ and get what we want. Thus, we have $(p_i) \succ (r_i) \succ (q_i)$. Now

$$\sum_{sym} \prod_{i=1}^{n} a_i^{p_i} - \sum_{sym} \prod_{i=1}^{n} a_i^{r_i} = \sum_{sym} {a_j}^{p_j} {a_k}^{p_k} - {a_j}^{r_j} {a_k}^{r_k} = \sum_{sym} {a_j}^{b+d} {a_k}^{b-d} - {a_j}^{b+c} {a_k}^{b-c}.$$

For each permutation $\sigma$, $\exists$ permutation $\rho$ $s.t$ $\sigma(i) = \rho(i),\ \forall\ i \notin \{j,k\}$ and $\sigma(j) = \rho(k), \sigma(k) = \rho(j)$. We pair the terms for $\sigma$ and $\rho$ and observe that

$$({a_j}^{b+d}{a_k}^{b-d} - {a_j}^{b+c}{a_k}^{b-c}) - ({a_k}^{b+d}{a_j}^{b-d} - {a_k}^{b+c}{a_j}^{b-c}) = {a_j}^{b-d}{a_k}^{b-d}({a_j}^{d+c} - {a_k}^{d+c})({a_j}^{d-c} - {a_k}^{d-c}) \geq 0.$$

Then the sum

$$\sum_{sym} \prod_{i=1}^{n} a_i^{p_i} - \sum_{sym} \prod_{i=1}^{n} a_i^{r_i} \geq 0.$$

We notice that the number of identical terms between $(r_i)$ and $(q_i)$ is exactly one more than the number of identical terms between $(p_i)$ and $(q_i)$, repeat this process until $(r_i) = (q_i)$ then we are done
. $\blacksquare$

***Remark:*** It is a really hard proof and let me explain what's going on at the last step: We now replace $(p_i)$ with $(r_i)$, do the same thing to get $(r'_i)$ which is originally the $(r_i)$, then we have

$$\sum_{sym} \prod_{i=1}^{n} a_i^{r_i} - \sum_{sym} \prod_{i=1}^{n} a_i^{r'_i} \geq 0.$$

which imply

$$\sum_{sym} \prod_{i=1}^{n} a_i^{p_i} - \sum_{sym} \prod_{i=1}^{n} a_i^{r'_i} = \sum_{sym} \prod_{i=1}^{n} a_i^{p_i} - \sum_{sym} \prod_{i=1}^{n} a_i^{r_i} + \sum_{sym} \prod_{i=1}^{n} a_i^{r_i} - \sum_{sym} \prod_{i=1}^{n} a_i^{r'_i} \geq 0.$$

## Theorem 11 *Rearrangement Inequality*

**Statement:**

For $a_1 \leq a_2 \leq ... \leq a_n$, and $b_1 \leq b_2 \leq ... \leq b_n$, let $b_{\sigma(1)}, b_{\sigma(2)}, ..., b_{\sigma(n)}$ be the permutation of $b_1, b_2, ..., b_n$, then

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

**Proof:**
Let

$$(c_1, c_2, ..., c_n) = \underset{(b_{\sigma(1)}, b_{\sigma(2)}, ..., b_{\sigma(n)})}{\text{argmax}} \left\{ \sum_{i=1}^{n} a_i b_{\sigma(i)} \right\},$$

then $c_1 \leq c_2 \leq ... \leq c_n$, otherwise $\exists\ i\ s.t\ c_i > c_{i+1}$ but then $(a_{i+1} - a_i)(c_i - c_{i+1}) > 0$ gives $a_i c_{i+1} + a_{i+1} c_i > a_i c_i + a_{i+1} c_{i+1}$, contradiction. Hence $(c_i) = (b_i)$.

On the other hand, let

$$(d_1, d_2, ..., d_n) = \underset{(b_{\sigma(1)}, b_{\sigma(2)}, ..., b_{\sigma(n)})}{\text{argmin}} \left\{ \sum_{i=1}^{n} a_i b_{\sigma(i)} \right\},$$

Similarly $d_1 \geq d_2 \geq ... \geq d_n$, otherwise $\exists\ i\ s.t\ d_i < d_{i+1}$ but then $(a_{i+1} - a_i)(d_i - d_{i+1}) < 0$ gives $a_i d_{i+1} + a_{i+1} d_i < a_i d_i + a_{i+1} d_{i+1}$, contradiction. Thus $(d_i) = (b_{n+1-i})$. ■

## Theorem 12 *Chebyshev's Inequality*

**Statement:**

Let $a_1 \geq a_2 \geq ... \geq a_n, b_1 \geq b_2 \geq .. \geq b_n$ be reals, then

$$n \sum_{i=1}^{n} a_i b_i \geq \left( \sum_{i=1}^{n} a_i \right) \left( \sum_{i=1}^{n} b_i \right) \geq n \sum_{i=1}^{n} a_i b_{n+1-i}.$$

Both equalites hold at the same time when $a_i = a_j$ or $b_i = b_j$ for $1 \leq i, j \leq n$.

***Remark:*** Chebyshev's Inequality is also true when $a_1 \leq a_2 \leq ... \leq a_n, b_1 \leq b_2 \leq .. \leq b_n$ (just let $c_i = a_{n+1-i}, d_i = b_{n+1-i}$ then apply Chebyshev's Theorem as usual) and the reverse inequality holds when $a_1 \geq a_2 \geq ... \geq a_n, b_1 \leq b_2 \leq .. \leq b_n$ which is actually the second inequality

**Proof:**
For $\forall\ 1 \leq i, j \leq n$, $(a_i - a_j)(b_i - b_j) \geq 0 \Leftrightarrow a_i b_i + a_j + b_j \geq a_i b_j + a_j b_i$. Then

$$\left( \sum_{i=1}^{n} a_i \right) \left( \sum_{i=1}^{n} b_i \right) = \sum_{1 \leq i,j \leq n} a_i b_j = \frac{1}{2} \sum_{1 \leq i,j \leq n} a_i b_j + a_j b_i \leq \frac{1}{2} \sum_{1 \leq i,j \leq n} a_i b_i + a_j b_j = n \sum_{i=1}^{n} a_i b_i.$$

The second inequality is because $(a_i - a_j)(b_i - b_j) \leq 0$. ■

### Theorem 13 *Surányi's Inequality*

**Statement:**

For $x_1, x_2, ..., x_n > 0$,

$$(n-1)\sum_{i=1}^{n} {x_i}^n + n\prod_{i=1}^{n} x_i \geq \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} {x_i}^{n-1}\right).$$

**Proof:** (*by Mihály Bencze*)
Apply induction: The case $n = 2$ is trivial, suppose Surányi Inequality is true for some $n \geq 2$ and we prove for $n+1$. Since this inequality is symmetric and homogeneous, WLOG let
$x_1 \geq x_2 \geq ... \geq x_{n+1}, \sum_{i=1}^{n+1} x_i = x_{n+1} + 1$ *i.e* $\sum_{i=1}^{n} x_i = 1$. Now what we want to prove is

$$n\sum_{i=1}^{n+1} {x_i}^{n+1} + (n+1)\prod_{i=1}^{n+1} x_i \geq \left(\sum_{i=1}^{n+1} x_i\right)\left(\sum_{i=1}^{n+1} {x_i}^{n}\right),$$

which is equivalent to prove

$$n\sum_{i=1}^{n} {x_i}^{n+1} + nx_{n+1}^{n+1} + nx_{n+1}\prod_{i=1}^{n} x_i + x_{n+1}\prod_{i=1}^{n} x_i - (1+x_{n+1})\left(\sum_{i=1}^{n} {x_i}^{n} + x_{n+1}^{n}\right) \geq 0.$$

by inductive hypothesis,

$$nx_{n+1}\prod_{i=1}^{n} x_i \geq x_{n+1}\sum_{i=1}^{n} {x_i}^{n-1} - (n-1)x_{n+1}\sum_{i=1}^{n} {x_i}^{n}.$$

only need to prove

$$n\sum_{i=1}^{n} {x_i}^{n+1} - \sum_{i=1}^{n} {x_i}^{n} - x_{n+1}\left(n\sum_{i=1}^{n} {x_i}^{n} - \sum_{i=1}^{n} {x_i}^{n-1}\right) + x_{n+1}\left(\prod_{i=1}^{n} x_i + (n-1)x_{n+1}^{n} - x_{n+1}^{n-1}\right) \geq 0,$$

Consider

$$n\sum_{i=1}^{n} {x_i}^{n} - \sum_{i=1}^{n} {x_k}^{n-1} = n\sum_{i=1}^{n} {x_i}^{n} - \left(\sum_{i=1}^{n} {x_k}^{n-1}\right)\left(\sum_{i=1}^{n} x_i\right) \geq 0,$$

which is true by **Chebyshev's Inequality** and also

$$n{x_i}^{n+1} + \frac{1}{n}{x_i}^{n-1} \geq 2{x_i}^{n},$$

which is also true by **AM-GM Inequality**, then sum through $1 \leq i \leq n$ we have

$$n\sum_{i=1}^{n} {x_i}^{n+1} - \sum_{i=1}^{n} {x_i}^{n} \geq \frac{1}{n}\left(n\sum_{i=1}^{n} {x_i}^{n} - \sum_{i=1}^{n} {x_k}^{n-1}\right),$$

which means

$$n\sum_{i=1}^{n} {x_i}^{n+1} - \sum_{i=1}^{n} {x_i}^{n} - x_{n+1}\left(n\sum_{i=1}^{n} {x_i}^{n} - \sum_{i=1}^{n} {x_i}^{n-1}\right) \geq 0,$$

because $x_{n+1} \leq \frac{1}{n}\sum_{i=1}^{n} x_i = \frac{1}{n}$, remains to compute

$$\prod_{i=1}^{n} x_i + (n-1){x_{n+1}}^{n} - x_{n+1}^{n-1} = \prod_{i=1}^{n}(x_i - x_{n+1} + x_{n+1}) + (n-1){x_{n+1}}^{n} - x_{n+1}^{n-1}$$

$$\geq {x_{n+1}}^{n} - x_{n+1}^{n-1}\sum_{i=1}^{n}(x_i - x_{n+1}) + (n-1){x_{n+1}}^{n} - x_{n+1}^{n-1} = 0.$$

■

## **Theorem 14** *Bernoulli's Inequality*

**Statement:**

*Form 1:*
Let $0 \neq x > -1$. If $\alpha \notin [0,1]$, then

$$(1+x)^\alpha > 1 + \alpha x;$$

if $\alpha \in (0,1)$, then

$$(1+x)^\alpha < 1 + \alpha x.$$

*Form 2:*
Let $x_1, x_2, \ldots, x_n > -1$ and all $x_i$ are either non-negative or non-positive. Then

$$\prod_{i=1}^{n}(1+x_i) \ \geq \ 1 + \sum_{i=1}^{n} x_i,$$

with equality iff at least $n-1$ of the $x_i$ are zero.

**Proof:**
Proof of *Form 1*
Define

$$f(x) = (1+x)^\alpha - 1 - \alpha x,$$

so

$$f'(x) = \alpha(1+x)^{\alpha-1} - \alpha = \alpha\big((1+x)^{\alpha-1} - 1\big).$$

When $\alpha \notin [0,1]$, $(1+x)^{\alpha-1} > 1$ iff $x > 0$, hence $f'(x) > 0$ for $x > 0$ and $f(0) = 0$, giving $(1+x)^\alpha > 1 + \alpha x$. Similarly, if $0 < \alpha < 1$, then $(1+x)^{\alpha-1} > 1$ iff $x < 0$, so $f'(x) > 0$ for $x < 0$ and again $f(0) = 0$, yielding $(1+x)^\alpha < 1 + \alpha x$. ■

Proof of *Form 2*
We prove the generalized form by induction on $n$.
Base case $n = 2$:

$$(1+x_1)(1+x_2) = 1 + x_1 + x_2 + x_1x_2 \geq 1 + x_1 + x_2.$$

Assume for $n-1$ that

$$\prod_{i=1}^{n-1}(1+x_i) \geq 1 + \sum_{i=1}^{n-1} x_i.$$

Then

$$\prod_{i=1}^{n}(1+x_i) = \left(\prod_{i=1}^{n-1}(1+x_i)\right)(1+x_n) \geq \left(1 + \sum_{i=1}^{n-1} x_i\right)(1+x_n) = 1 + \sum_{i=1}^{n} x_i + \sum_{i=1}^{n-1} x_i\, x_n \geq 1 + \sum_{i=1}^{n} x_i.$$

This completes the induction. ■

## Theorem 15 *Minkowski's Inequality*

**Statement:**

For $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n > 0$ and $p \geq 1$,

$$\left(\sum_{i=1}^{n}(a_i + b_i)^p\right)^{\frac{1}{p}} \leq \left(\sum_{i=1}^{n} {a_i}^p\right)^{\frac{1}{p}} + \left(\sum_{i=1}^{n} {b_i}^p\right)^{\frac{1}{p}}.$$

Equality holds if and only if $\dfrac{{a_i}^p}{{b_i}^p} = \dfrac{{a_j}^p}{{b_j}^p}, \forall 1 \leq i, j \leq n$.

When $0 \neq p < 1$, the inequality change sign.

**Proof:**

When $p \geq 1$, by **Hölder's inequality**,

$$\sum_{i=1}^{n} a_i \left(a_i + b_i\right)^{p-1} \;\leq\; \left(\sum_{i=1}^{n} a_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{n}\left((a_i + b_i)^{p-1}\right)^{\frac{p}{p-1}}\right)^{1-\frac{1}{p}} \;=\; \left(\sum_{i=1}^{n} a_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{n}(a_i + b_i)^p\right)^{1-\frac{1}{p}}.$$

Similarly,

$$\sum_{i=1}^{n} b_i \left(a_i + b_i\right)^{p-1} \;\leq\; \left(\sum_{i=1}^{n} b_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{n}(a_i + b_i)^p\right)^{1-\frac{1}{p}}.$$

Adding these two inequalities yields

$$\sum_{i=1}^{n}(a_i + b_i)^p \;\leq\; \left[\left(\sum_{i=1}^{n} a_i^p\right)^{\frac{1}{p}} + \left(\sum_{i=1}^{n} b_i^p\right)^{\frac{1}{p}}\right]\left(\sum_{i=1}^{n}(a_i + b_i)^p\right)^{1-\frac{1}{p}},$$

and hence

$$\left(\sum_{i=1}^{n}(a_i + b_i)^p\right)^{\frac{1}{p}} \;\leq\; \left(\sum_{i=1}^{n} a_i^p\right)^{\frac{1}{p}} + \left(\sum_{i=1}^{n} b_i^p\right)^{\frac{1}{p}}.$$

The case $0 \neq p < 1$ is similar. ■

## Theorem 16 *Nesbitt's Inequality*

**Statement:**

For $a, b, c > 0$,

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

Equality holds when $a = b = c$.

**Proof:**

By **Cauchy-Schwarz Inequality**,

$$\left(\sum_{cyc} \frac{a}{b+c}\right)\left(\sum_{cyc} a(b+c)\right) \geq \left(\sum_{cyc} a\right)^2 = (a+b+c)^2 \geq \frac{3}{2}\sum_{cyc} a(b+c).$$

The last step is by **Muirhead's Inequality** when consider $(2,1,0) \succ (1,1,1)$. ■

## Theorem 17 *Hermite–Hadamard Inequality*

**Statement:**

For any convex function $f : \mathrm{dom}(f) \to \mathbb{R}$ if $a, b \in \mathrm{dom}(f),\ a < b$, then

$$f\Big(\frac{a+b}{2}\Big) \le \frac{1}{b-a}\int_a^b f(x)\,dx \le \frac{f(a)+f(b)}{2}.$$

If $f$ is concave, then both inequalities reverse.

**Proof:**
Set $x = t\,a + (1-t)\,b$, so $dx = (b-a)\,dt$ and

$$\int_a^b f(x)\,dx = (b-a)\int_0^1 f\big(t\,a + (1-t)\,b\big)\,dt.$$

Since $f$ is convex, for each $t \in [0,1]$,

$$f\big(t\,a + (1-t)\,b\big) \le t\,f(a) + (1-t)\,f(b).$$

Integrating over $[0,1]$ gives

$$\frac{1}{b-a}\int_a^b f(x)\,dx \le \int_0^1 \big(t\,f(a) + (1-t)\,f(b)\big)\,dt = \frac{f(a)+f(b)}{2}.$$

On the other hand, by **Jensen' s inequality**,

$$f\Big(\frac{a+b}{2}\Big) = f\Big(\int_0^1 (t\,a + (1-t)\,b)\,dt\Big) \le \int_0^1 f\big(t\,a + (1-t)\,b\big)\,dt = \frac{1}{b-a}\int_a^b f(x)\,dx.$$

Combining these yields the desired result. ■

## Lemma 1

**Statement:**

For $n, k \in \mathbb{Z}_{>0}$,

$$\binom{n}{k} < \frac{1}{e}\Big(\frac{en}{k}\Big)^k.$$

**Proof:** It is obvious that $\dfrac{n!}{(n-k)!} < n^k$, divide both side by $k!$ gives $\dbinom{n}{k} < \dfrac{n^k}{k!}$, only need to prove $k! \ge e(\frac{k}{e})^k$, we finish the proof after noticing

$$\sum_{i=1}^{k} \ln i \ge \int_1^k \ln x\ dx = k\ln k - k + 1.$$

■

## 1.2 Algebraic Identity

### Theorem 18 *Nicomachus' Theorem*

**Statement:**

For $n \in \mathbb{Z}_{>0}$,

$$\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2 = \left[\frac{n(n+1)}{2}\right]^2.$$

**Proof:**
We use induction on $n$. For $n = 1$ the identity reads $1^3 = 1^2$, which holds. Assume

$$\sum_{k=1}^{n} k^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

Then

$$\sum_{k=1}^{n+1} k^3 = \sum_{k=1}^{n} k^3 + (n+1)^3 = \left[\frac{n(n+1)}{2}\right]^2. + (n+1)^3 = (n+1)^2\left(\frac{n^2}{4} + n + 1\right) = \left[\frac{(n+1)(n+2)}{2}\right]^2,$$

completing the induction. ■

### Lemma 2

**Statement:**

For $x, y \in \mathbb{C}$ and $n \in \mathbb{Z}_{>0}$,
*Form 1:*

$$x^n - y^n = (x-y)\sum_{k=0}^{n-1} x^{\,n-1-k}\, y^k.$$

*Form 2:* For $2 \nmid n$,

$$x^n + y^n = (x+y)\sum_{k=0}^{n-1} (-1)^k\, x^{\,n-1-k}\, y^k.$$

**Proof:**
For the difference, observe the telescoping sum

$$x^n - y^n = \sum_{k=0}^{n-1}\left(x^{n-k}y^k - x^{n-k-1}y^{k+1}\right) = (x-y)\sum_{k=0}^{n-1} x^{n-1-k}y^k.$$

When $n$ is odd, set $y' = -y$. Then

$$x^n + y^n = x^n - (y')^n = (x-y')\sum_{k=0}^{n-1} x^{\,n-1-k}(y')^k = (x+y)\sum_{k=0}^{n-1}(-1)^k\, x^{\,n-1-k}y^k,$$

since $(y')^k = (-y)^k = (-1)^k y^k$. ■

## Theorem 19 *Lagrange's Identity*

**Statement:**

For $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in \mathbb{R}$,

$$\left(\sum_{i=1}^{n} {a_i}^2\right)\left(\sum_{i=1}^{n} {b_i}^2\right) - \left(\sum_{i=1}^{n} a_i b_i\right)^2 = \frac{1}{2}\sum_{1\le i,j\le n}(a_i b_j - a_j b_i)^2 = \sum_{1\le i<j\le n}(a_i b_j - a_j b_i)^2.$$

*vector form:* $|\vec{a}\times\vec{b}|^2 + (\vec{a}\cdot\vec{b})^2 = |\vec{a}|^2|\vec{b}|^2$.

**Proof:** Directly obtain from *Method 1* and *Method 3* in Cauchy-Schwarz Inequality section. ∎

## Theorem 20 *Abel's Transformation*

**Statement:**

For $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n \in \mathbb{C}$, defined $S_k = \sum_{i=1}^{k} b_i$, then

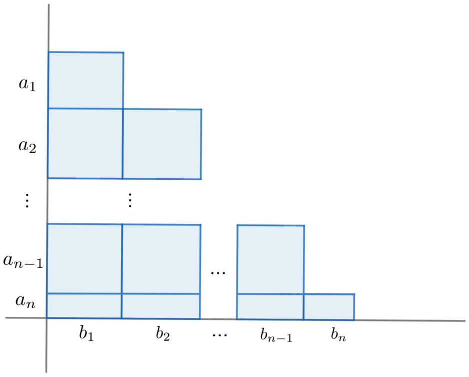
$$\sum_{i=1}^{n} a_i b_i = S_n a_n + \sum_{i=1}^{n-1} S_i(a_i - a_{i+1}).$$

**Proof:**
*Method 1*: (*algebraic method*)

$$\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n} a_i(S_i - S_{i-1}) = \sum_{i=1}^{n} a_i S_i - \sum_{i=1}^{n} a_i s_{i-1} = \sum_{i=1}^{n} a_i S_i - \sum_{i=0}^{n-1} a_{i+1} S_i$$
$$= a_n S_n - a_1 S_0 + \sum_{i=1}^{n-1} a_i S_i - \sum_{i=1}^{n-1} a_{i+1} S_i = S_n a_n + \sum_{i=1}^{n-1} S_i(a_i - a_{i+1}).$$

∎

*Method 2:* (*combinatoric method*)



Apply double counting: we compute the area of these rectangles horizontally and get $\sum_{i=1}^{n} a_i b_i$. On the other hand, we compute vertically obtain $S_n a_n + \sum_{i=1}^{n-1} S_i(a_i - a_{i+1})$. ∎

### Definition 2 *Pochhammer symbol*

**Description:**

For $x \in \mathbb{C}, n \in \mathbb{Z}_{\geq 0}, n \leq x$, the **Pochhammer symbol** define as

$$(x)_n := \prod_{i=0}^{n-1} (x - i).$$

where $(x)_1 = x$ and when $x \in \mathbb{Z}_{>0}$, $(x)_x = x!$.

### Theorem 21 *Binomial Theorem*

**Statement:**

*Form 1:*
For $a, b \in \mathbb{C}, n \in \mathbb{Z}_{>0}$,

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}.$$

*Form 2:* (Generalize)
For $x, y \in \mathbb{C}, |x| < |y|, r \in \mathbb{C}$,

$$(x + y)^r = \sum_{i \geq 0} \binom{r}{i} x^i y^{r-i}.$$

**Proof:**
*Form 1:*
Apply induction on $n$: The case $n = 1$ is trivial, suppose the identity holds for $n$, then for $n + 1$,

$$(a + b)^{n+1} = (a + b)(a + b)^n = (a + b) \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} = \sum_{i=0}^{n+1} \binom{n}{i} a^i b^{n+1-i} + \sum_{i=0}^{n+1} \binom{n}{i-1} a^i b^{n+1-i},$$

By **Pascal's Identity**,

$$\sum_{i=0}^{n+1} a^i b^{n+1-i} \left( \binom{n}{i} + \binom{n}{i-1} \right) = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}.$$

■

*Form 2:*
Consider $f(a) = (1 + a)^r, |a| < 1$ for $\forall i \in \mathbb{Z}_{\geq 0}$, we have

$$f^{(i)}(a) = (r)_i (1 + a)^{r-i},$$

so

$$\frac{f^{(n)}(0)}{i!} = \binom{r}{i}.$$

Therefore by **Taylor series** of $f(a)$,

$$(1 + a)^r = \sum_{i \geq 0} \binom{r}{i} a^i$$

take $a = \dfrac{x}{y}$, multiply both side by $y^r$ and we are done. ■

## Theorem 22 *Multinomial Theorem*

**Statement:**

For $k \in \mathbb{Z}_{>0}$, $n \in \mathbb{Z}_{\geq 0}$, and any commutative ring or field,

$$\Big(\sum_{i=1}^{k} x_i\Big)^n = \sum_{\substack{n_1,\ldots,n_k \geq 0 \\ n_1+\cdots+n_k=n}} \binom{n}{n_1, n_2, \cdots, n_k} \prod_{i=1}^{k} x_i^{n_i}.$$

**Proof:**
Consider the expansion of

$$(x_1 + x_2 + \cdots + x_k)^n$$

as the product of $n$ identical factors $(x_1 + \cdots + x_k)$. Expanding without simplification yields terms of the form

$$x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}, \quad n_1 + \cdots + n_k = n.$$

For each fixed tuple $(n_1, \ldots, n_k)$, there are $\frac{n!}{n_1!\, n_2! \cdots n_k!}$ ways to choose which factors contribute each $x_i$. Hence

$$(x_1 + \cdots + x_k)^n = \sum_{n_1+\cdots+n_k=n} \frac{n!}{n_1! \cdots n_k!} x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}.$$

■

## Theorem 23 *Hermite's Identity*

**Statement:**

For $x \in \mathbb{R}, n \in \mathbb{Z}_{>0}$

$$\sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \lfloor n\, x \rfloor .$$

**Proof:**
Define

$$f(x) = \sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor - \lfloor n\, x \rfloor .$$

Then

$$f(x + \frac{1}{n}) = \sum_{k=0}^{n-1} \left\lfloor x + \frac{k+1}{n} \right\rfloor - \lfloor n\, x + 1 \rfloor = \Big(\sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor + 1\Big) - \big(\lfloor n\, x \rfloor + 1\big) = f(x).$$

Hence $f$ is periodic of period $\dfrac{1}{m}$. For $x \in \Big[0, \dfrac{1}{m}\Big)$ each term $\left\lfloor x + \dfrac{k}{m} \right\rfloor = 0$ and $\lfloor m\, x \rfloor = 0$, so $f(x) = 0$. Therefore $f \equiv 0$, as required. ■

## Theorem 24 *Landau's identity*

**Statement:**

$m, n > 1$ are coprime odd integers, then

$$\sum_{k=1}^{\frac{m-1}{2}} \left\lfloor \frac{kn}{m} \right\rfloor + \sum_{k=1}^{\frac{n-1}{2}} \left\lfloor \frac{km}{n} \right\rfloor = \frac{(m-1)(n-1)}{4}.$$

**Proof:**
Consider the set

$$A = \left\{ xm - yn : 1 \le x \le \frac{n-1}{2},\ 1 \le y \le \frac{m-1}{2} \right\}.$$

First, if

$$xm - yn = x'm - y'n$$

then $(x - x')m = (y - y')n$. Since $\gcd(m, n) = 1$ and $1 \le x, x' \le \frac{n-1}{2} < n$, we deduce $x = x'$ and hence $y = y'$. Thus all elements of $A$ are distinct, giving

$$|A| = \frac{(m-1)(n-1)}{4}.$$

On the other hand, $xm - yn \ge 0$ iff $y \le \frac{xm}{n}$. For each integer $x \in \left\{1, \ldots, \frac{n-1}{2}\right\}$, there are $\left\lfloor \frac{xm}{n} \right\rfloor$ choices of $y$, so exactly

$$\sum_{x=1}^{\frac{n-1}{2}} \left\lfloor \frac{xm}{n} \right\rfloor$$

nonnegative elements in $A$, a similar count shows there are

$$\sum_{y=1}^{\frac{m-1}{2}} \left\lfloor \frac{yn}{m} \right\rfloor$$

nonpositive elements. Since $0 \notin A$, every element of $A$ is either positive or negative, and is counted exactly once. Hence

$$|A| = \sum_{x=1}^{\frac{n-1}{2}} \left\lfloor \frac{xm}{n} \right\rfloor + \sum_{y=1}^{\frac{m-1}{2}} \left\lfloor \frac{yn}{m} \right\rfloor.$$

Combining the two expressions for $|A|$ yields the identity. ■

## Lemma 3

**Statement:**

For $a, b \in \mathbb{R}$,

$$|a - b| = a + b - 2\min\{a, b\}.$$

**Proof:**
WLOG $a \ge b$ then $|a - b| = a - b = a + b - 2b = a + b - 2\min\{a, b\}$. ■

## Lemma 4

**Statement:**

For $a, b \in \mathbb{R}$,

$$|a+b| - |a-b| = 2\operatorname{sgn}(a)\operatorname{sgn}(b)\min\{|a|, |b|\}.$$

**Proof:**
WLOG let $|a| \geq |b|$, there are two cases:
1. $a, b$ same sign: $\operatorname{sgn}(a)\operatorname{sgn}(b) = 1$. Then

$$|a+b| = |a| + |b|, \quad |a-b| = \big|\,|a| - |b|\big| = |a| - |b|.$$

Hence

$$|a+b| - |a-b| = (|a| + |b|) - (|a| - |b|) = 2|b| = 2\operatorname{sgn}(a)\operatorname{sgn}(b)\min\{|a|, |b|\}.$$

2. $a, b$ opposite sign: $\operatorname{sgn}(a)\operatorname{sgn}(b) = -1$. Then

$$|a+b| = \big|\,|a| - |b|\,\big| = |a| - |b|, \quad |a-b| = |a| + |b|.$$

Thus

$$|a+b| - |a-b| = (|a| - |b|) - (|a| + |b|) = -2|b| = 2\operatorname{sgn}(a)\operatorname{sgn}(b)\min\{|a|, |b|\}.$$

■

## Theorem 25 *Binet–Cauchy Identity*

**Statement:**

Let $a_i, b_i, c_i, d_i \in \mathbb{C}$ for $1 \leq i \leq n$. Then

$$\Big(\sum_{i=1}^{n} a_i c_i\Big)\Big(\sum_{i=1}^{n} b_i d_i\Big) = \Big(\sum_{i=1}^{n} a_i d_i\Big)\Big(\sum_{i=1}^{n} b_i c_i\Big) + \sum_{1\leq i<j\leq n} (a_i b_j - a_j b_i)(c_i d_j - c_j d_i).$$

**Proof:**
Expand the last sum:

$$\sum_{1\leq i<j\leq n} (a_i b_j - a_j b_i)(c_i d_j - c_j d_i) = \sum_{1\leq i<j\leq n} \big(a_i c_i\, b_j d_j + a_j c_j\, b_i d_i - a_i c_j\, b_j d_i - a_j c_i\, b_i d_j\big).$$

Observe that

$$\sum_{1\leq i<j\leq n} \big(a_i c_i\, b_j d_j + a_j c_j\, b_i d_i\big) = \sum_{i\neq j} a_i c_i\, b_j d_j = \sum_{i=1}^{n} a_i c_i \sum_{j=1}^{n} b_j d_j - \sum_{i=1}^{n} a_i c_i\, b_i d_i,$$

and likewise

$$\sum_{1\leq i<j\leq n} \big(a_i c_j\, b_j d_i + a_j c_i\, b_i d_j\big) = \sum_{i=1}^{n} a_i d_i \sum_{j=1}^{n} b_j c_j - \sum_{i=1}^{n} a_i d_i\, b_i c_i.$$

Since $\sum_i a_i c_i\, b_i d_i = \sum_i a_i d_i\, b_i c_i$, taking the difference yields

$$\sum_{i=1}^{n} a_i c_i \sum_{j=1}^{n} b_j d_j - \sum_{i=1}^{n} a_i d_i \sum_{j=1}^{n} b_j c_j,$$

which rearranges to the claimed identity. ■

## Lemma 5

**Statement:**

For $k \in \mathbb{R}$, define

$$f_k(x) = \mathbb{I}(0 \leq k \leq x).$$

Then

$$\min\{a, b\} = \int_0^{+\infty} f_a(x)\, f_b(x)\, \mathrm{d}x.$$

**Proof:**

Note that $f_a(x)f_b(x) = 1$ exactly when $0 \leq x \leq \min\{a, b\}$, and vanishes otherwise. Hence

$$\int_0^{+\infty} f_a(x)f_b(x)\, \mathrm{d}x = \int_0^{\min\{a,b\}} 1\, \mathrm{d}x = \min\{a, b\}.$$

■

## Lemma 6

**Statement:**

For any $a, b > 0$,

$$\max\{a, b\} = \lim_{s\to\infty} \left(a^s + b^s\right)^{\frac{1}{s}}.$$

**Proof:**
Let $M = \max\{a, b\}$ and set

$$r = \frac{\min\{a, b\}}{M}, \quad 0 < r \leq 1.$$

Then

$$(a^s + b^s)^{\frac{1}{s}} = M\left[\left(\frac{a}{M}\right)^s + \left(\frac{b}{M}\right)^s\right]^{\frac{1}{s}} = M\left(1 + r^s\right)^{\frac{1}{s}}.$$

The case $a = b$ is trivial, consider $r < 1$, we have $r^s \to 0$ as $s \to \infty$. Hence

$$\lim_{s\to\infty} \left(1 + r^s\right)^{\frac{1}{s}} = \exp\left(\lim_{s\to\infty} \frac{\ln(1 + r^s)}{s}\right) = e^0 = 1.$$

It follows that

$$\lim_{s\to\infty} (a^s + b^s)^{\frac{1}{s}} = M \cdot 1 = \max\{a, b\},$$

as claimed. ■

### Theorem 26 *Taylor's Expansion*

**Statement:**

Let $f \in C^\infty(I)$ on an open interval $I$ containing $a$. Then for all $x \in I$,

$$f(x) \;=\; \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}\,(x-a)^n.$$

Following are some famous expansion,:

1. $e^x = \displaystyle\sum_{n=0}^{\infty} \frac{x^n}{n!}$.
2. $\sin x = \displaystyle\sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!}$.
3. $\cos x = \displaystyle\sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!}$.
4. $(1+x)^\alpha = \displaystyle\sum_{n=0}^{\infty} \binom{\alpha}{n} x^n$.

***Remark:*** **Maclaurin series** is the special case of Taylor' s theorem with $a = 0$.

**Proof:**
Define

$$P(x) = \sum_{n=0}^{k-1} \frac{f^{(n)}(a)}{n!}(x-a)^n, \quad h_k(x) = \begin{cases} \dfrac{f(x) - P(x)}{(x-a)^k}, & x \neq a, \\ 0, & x = a. \end{cases}$$

Since $f \in C^\infty(I)$, we have $f^{(j)}(a) = P^{(j)}(a)$ for $0 \le j \le k-1$. Hence both numerator and denominator vanish to order $k$ at $x = a$, and all hypotheses for **L' Hôpital' s rule** are satisfied. Applying L' Hôpital' s rule $k$ times gives

$$\lim_{x \to a} h_k(x) = \lim_{x \to a} \frac{\dfrac{d^k}{dx^k}\big(f(x) - P(x)\big)}{\dfrac{d^k}{dx^k}(x-a)^k} = \frac{f^{(k)}(a) - P^{(k)}(a)}{k!} = 0.$$

Therefore the remainder $R_k(x) = h_k(x)\,(x-a)^k$ tends to zero, and letting $k \to \infty$ yields

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

■

### Theorem 27 *Goldbach-Euler Theorem*

**Statement:**

Let $\mathscr{M}$ be the set of positive integer which is a perfect power, then

$$\sum_{m \in \mathscr{M}} \frac{1}{m-1} = 1.$$

**Proof:**
Every $m \in \mathscr{M}$ can be uniquely written as $m = a^k$ with $a \geq 2$ and $k \geq 2$. Hence

$$\sum_{m\in\mathscr{M}} \frac{1}{m-1} = \sum_{k=2}^{\infty}\sum_{a=2}^{\infty} \frac{1}{a^k-1} = \sum_{k=2}^{\infty}\sum_{a=2}^{\infty}\sum_{i=1}^{\infty} a^{-ik} = \sum_{n=2}^{\infty}\sum_{k=2}^{\infty} n^{-k} = \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty}\Big(\frac{1}{n-1} - \frac{1}{n}\Big) = 1.$$

■

## Lemma 7

**Statement:**

Let $n$ be an odd positive integer. Then for all $x, y \in \mathbb{C}$,

$$x^n - y^n = \prod_{k=0}^{n-1} \big(\zeta_n^k\, x - \zeta_n^{-k}\, y\big).$$

**Proof:**
Since the $n$th roots of unity are $1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$, we have the factorization

$$z^n - 1 = \prod_{k=0}^{n-1} \big(z - \zeta_n^k\big).$$

Substitute $z = x/y$ (with $y \neq 0$) to get

$$\frac{x^n}{y^n} - 1 = \prod_{k=0}^{n-1} \Big(\frac{x}{y} - \zeta_n^k\Big).$$

Multiplying both sides by $y^n$ yields

$$x^n - y^n = \prod_{k=0}^{n-1} \big(x - \zeta_n^k\, y\big). \tag{2.13}$$

Now, because $n$ is odd, the map $k \mapsto -k \pmod{n}$ permutes $\{0, 1, \ldots, n-1\}$. Hence

$$\prod_{k=0}^{n-1} \big(x - \zeta_n^k\, y\big) = \prod_{k=0}^{n-1} \big(x - \zeta_n^{-k}\, y\big).$$

On the other hand,

$$\prod_{k=0}^{n-1} \big(x - \zeta_n^{-k}\, y\big) = \prod_{k=0}^{n-1} \zeta_n^{-k} \prod_{k=0}^{n-1} \big(\zeta_n^k\, x - \zeta_n^{-k}\, y\big).$$

But $\sum_{k=0}^{n-1}(-k) = -\dfrac{n(n-1)}{2}$, and since $n$ is odd this exponent is a multiple of $n$. Therefore $\prod_{k=0}^{n-1} \zeta_n^{-k} = 1$. Substituting back gives

$$x^n - y^n = \prod_{k=0}^{n-1} \big(\zeta_n^k\, x - \zeta_n^{-k}\, y\big),$$

as claimed. ■

## 1.3 Polynomial

***Remark:*** All uppercase letters in this section are a **polynomial**.

### Theorem 28 *Little Bézout's Theorem*

**Statement:**

For any $r \in \mathbb{C}$ and $P(x) \in \mathbb{C}[x]$, $\exists!\ Q(x) \in \mathbb{C}[x]$ such that

$$P(x) = (x - r)\,Q(x) + P(r).$$

**Proof:**

Using the identity $x^k - r^k = (x - r)\,S_k$, where $S_k = \sum_{i=0}^{k-1} x^i r^{k-1-i}, S_1 = 1$, and writing $P(x) = \sum_{i=1}^{n} a_i x^i$, obtain

$$P(x) - P(r) = \sum_{k=0}^{n} a_k \big(x^k - r^k\big) = (x - r) \sum_{k=1}^{n} a_k S_k,$$

we are done. ■

### Theorem 29 *Factor Theorem*

**Statement:**

For $P \in \mathbb{C}[x]$, if $\alpha$ is a root of $P$, then $P(x) = (x - \alpha)Q(x)$ for some $Q$.

**Proof:** It is true by **Little Bézout's Theorem** since $P(\alpha) = 0$. ■

### Theorem 30 *Complex Conjugate Root Theorem*

**Statement:**

Let $P \in \mathbb{R}[x]$ and $z \in \mathbb{C}$. Then

$$P(z) = 0 \Leftrightarrow P(\overline{z}) = 0.$$

**Proof:**
Write

$$P(x) = \sum_{i=0}^{n} a_i\, x^i, \quad a_i \in \mathbb{R}.$$

Assume $P(z) = 0$. Taking complex conjugates gives

$$0 = \overline{P(z)} = \sum_{i=0}^{n} \overline{(a_i z^i)} = \sum_{i=0}^{n} a_i\, \overline{z}^i = P(\overline{z}).$$

■

## Theorem 31 *Fundamental Theorem of Algebra*

**Statement:**

*Form 1:*
Let $P \in \mathbb{C}[x]$ be a non-zero polynomial such that deg $P = n$, then $P$ has exactly $n$ complex roots, not necessary distinct.

*Form 2:*
Let $P \in \mathbb{C}[x]$ be a non-constant polynomial, then $P$ has at least one complex root.

**Proof**: (*by Frode Terkelsen*)
For non-constant $P \in \mathbb{C}[x]$, since $\lim\limits_{|z|\to\infty} |P(z)| = +\infty$, there exists $z_0 \in \mathbb{C}$ such that

$$|P(z_0)| \leq |P(z)|, \quad \forall z \in \mathbb{C}.$$

We now prove $P(z_0) = 0$, hence $z_0$ is a root of $P$.
Assume $P(z_0) \neq 0$. WLOG let $z_0 = 0, P(z_0) = 1$, otherwise we can replace $P(z)$ by $\dfrac{P(z+z_0)}{P(z_0)}$.
Write

$$P(z) = 1 + az^n + z^{n+1}Q(z),$$

where $n \in \mathbb{Z}_{>0}$, $a \neq 0$, and $Q \in \mathbb{C}[x]$.
Choose $w$ such that $aw^n \in \mathbb{R}_{<0}$ and $|w\,Q(w)| < \frac{1}{2}|a|$. Then

$$|P(w)| \leq 1 + a\,w^n + \left|w^{n+1}Q(w)\right| < 1 + \tfrac{1}{2}\,a\,w^n < 1,$$

a contradiction Therefore the theorem is proved. ■

***Remark:*** How can *Form 2* implies *Form 1*? Let $\alpha_1$ be a root of $P$, then $P(x) = (x-\alpha_1)P_1(x)$, for some $P_1$ with deg $P_1 = n-1$. Then we continue downgrade $P_1(x)$ until
$P(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1})(ax+b)$. It is clear that $ax+b$ has an unique root $\frac{-b}{a}$, so $P$ will have $n$ complex roots.

## Theorem 32 *Mahler's Coefficient*

**Statement:**

For $P \in \mathbb{C}[x]$ with deg $P = n$, $\exists!\ a_0, a_1, \cdots, a_n \in \mathbb{C}$ such that

$$P(x) = \sum_{k=0}^{n} a_k \binom{x}{k}.$$

Those $a_k$ is called the **Mahler's Coefficient**.

**Proof:** Apply induction on $n$: The case $n = 0$ is trivial, suppose Mahler's Coefficient exists for all polynomials with degree at most $n-1$, then consider $P$ such that deg $P = n$ and let its leading coefficient be $a$,
we take $a_n$ such that

$$\deg\left(P(x) - a_n\binom{x}{n}\right) = n-1.$$

Note that such $a_n$ is unique, which is $a_n = n!a$, also by inductive hypothesis, there exists unique $a_0, a_1, ..., a_{n-1}$ such that

$$P(x) - a_n\binom{x}{n} = \sum_{k=0}^{n-1} a_k \binom{x}{k}.$$

■

## Lemma 8

**Statement:**

If $\text{ran}(P) \subseteq \mathbb{Z}$, then the Mahler's Coefficient of $P$ are integers.

**Proof:**
Let $a_0, a_1, ..., a_{\deg P}$ be Mahler's Coefficient of $P$, we apply induction: Note that $a_0 = P(0) \in \mathbb{Z}$, now suppose $a_0, ...a_{k-1} \in \mathbb{Z}$, then consider

$$P(k) = a_0 \binom{k}{0} + a_1 \binom{k}{1} + \cdots + a_{k-1} \binom{k}{k-1} + a_k,$$

this equation give us $a_k \in \mathbb{Z}$. ■

## Theorem 33 *Rational Root Theorem*

**Statement:**

*Form 1:* For $P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, if $\frac{p}{q}$ is a rational root of $P$ for $(p, q) = 1$, then $p \mid a_0$ and $q \mid a_n$.

*Form 2:* If $P \in \mathbb{Z}[x]$ is monic, then all rational roots of $P$ are integer.

**Proof:**
Multiplying $q^n$ on both sides of equation $P\left(\frac{p}{q}\right) = 0$ gives

$$a_n p^n + a_0 q^n + \sum_{i=i}^{n-1} a_i p^i q^{n-i} = 0,$$

which means $p \mid a_0$ and $q \mid a_n$. ■

## Definition 3 *Elementary Symmetric Polynomial*

**Description:**

**Elementary Symmetric Polynomial** of $x_i$ is defined as

$$\sigma_k = \sum_{I \subseteq [n], |I| = k} \prod_{i \in I} x_i.$$

e.g $\sigma_1 = \sum_i x_i,\ \sigma_2 = \sum_{i<j} x_i x_j,\ \sigma_3 = \sum_{i<j<k} x_i x_j x_k,\ \cdots,\ \sigma_n = x_1 x_2 \cdots x_n.$

### Definition 4 *Symmetric Polynomial*

**Description:**

$P$ is a **symmetric polynomial** if for any permutation $y_1, y_2, \cdots, y_n$ of $x_1, x_2, \cdots, x_n$, has $P(y_1, y_2, ..., y_n) = P(x_1, x_2, \cdots, x_n)$.

### Theorem 34 *Fundamental Theorem of Elementary Symmetric Polynomial*

**Statement:**

For any symmetric polynomial $P(x_1, x_2, \ldots, x_n)$, there exists a unique polynomial

$$Q\big(\sigma_1, \sigma_2, \ldots, \sigma_n\big)$$

such that

$$P(x_1, x_2, \ldots, x_n) = Q\big(\sigma_1, \sigma_2, \ldots, \sigma_n\big),$$

where $\sigma_i$ is the elementary symmetric polynomial of $x_i$.

**Proof:**
Check out *Symmetric Polynomials: The Fundamental Theorem and Uniqueness* by Nicholas Kender. https://www.math.union.edu/~hatleyj/student_theses/kender.pdf

### Theorem 35 *Vieta' s Theorem*

**Statement:**

Let $P(x) = \sum_{i=0}^{n} a_i\, x^i, a_n \neq 0$, and let $r_1, r_2, \ldots, r_n$ be its roots, then for each $0 \leq k \leq n-1$,

$$a_k \;=\; (-1)^{\,n-k}\, a_n\, \sigma_{n-k},$$

where $\sigma_i$ is the elementary symmetric sum of $r_i$.

**Proof:**
Note that

$$P(x) = a_n \prod_{i=1}^{n} (x - r_i) = a_n \sum_{k=0}^{n} (-1)^{\,n-k}\, \sigma_{n-k}\, x^k,$$

Matching coefficients of $x^k$ in $\sum_{i=0}^{n} a_i\, x^i$ gives

$$a_k = (-1)^{\,n-k}\, a_n\, \sigma_{n-k},$$

as claimed. ■

## Theorem 36 *Newton's Identities*

**Statement:**

Consider $P(x) = \sum_{i=0}^{n} a_i x^i$, with complex roots $r_1, r_2, ..., r_n$, for $d \in \mathbb{Z}$, define $p_d = \sum_{i=1}^{n} {r_i}^d$, then

*Form 1:*

$$ka_{n-k} + \sum_{i=0}^{k-1} a_{n-i} p_{k-i} = 0, \quad \forall 1 \leq k \leq n$$

if consider $\sigma_i$ be the elementary symmetric polynomial of $x_i$, one may express the identity as

$$(-1)^k k\sigma_k + \sum_{i=0}^{k-1} (-1)^i \sigma_i \, p_{k-i} = 0.$$

*Form 2:* $\forall k \in \mathbb{Z}$,

$$\sum_{i=0}^{n} a_i p_{i+k} = 0, \quad \forall k \in \mathbb{Z}.$$

**Proof:** (*by Doron Zeilberger*)
Let $\mathscr{A}(n,k)$ be the set of triples $(A, j, \ell)$ such that

$$A \subseteq [n], \quad |A| \leq k, \quad j \in [n], \quad \ell = k - |A|,$$

with the extra condition that if $\ell = 0$ then $j \in A$. Define

$$w(A, j, \ell) = (-1)^{|A|} \left( \prod_{a \in A} x_a \right) x_j^{\ell}.$$

One checks by grouping terms that

$$(-1)^k k\sigma_k + \sum_{i=0}^{k-1} (-1)^i \sigma_i \, p_{k-i} = \sum_{(A,j,\ell) \in \mathscr{A}(n,k)} w(A, j, \ell).$$

Now define an involution $T : \mathscr{A}(n,k) \to \mathscr{A}(n,k)$ by

$$T(A, j, \ell) = \begin{cases} \big(A \setminus \{j\},\, j,\, \ell + 1\big), & j \in A, \\ \big(A \cup \{j\},\, j,\, \ell - 1\big), & j \notin A. \end{cases}$$

Since $w(T(A, j, \ell)) = -w(A, j, \ell)$ and $T^2 = \text{id}$, all weights cancel in pairs, yielding the desired identity. ■

***Remark:*** *Form 2* is trivial. Note that there are infinitely many identities: one for each choice of k. This is why a lot of people call the above theorem "Newton's identities" and not "Newton's identity."

### Definition 5 *Minimal Polynomial*

**Description:**

Let $\alpha \in \mathbb{A}$, the unique monic polynomial of least degree such that

$$P(x) \in \mathbb{Z}[x] \quad \text{with} \quad P(\alpha) = 0$$

is called the **minimal polynomial** of $\alpha$.

### Definition 6 *Cyclotomic Polynomial*

**Description:**

**Cyclotomic Polynomial** is the monic polynomial whose roots are the primitive $n^{th}$ roots of unity, denoted as

$$\Phi_n(x) = \prod_{\substack{\gcd(k,n)=1 \\ 1 \le k \le n}} (x - \zeta_n^k).$$

### Lemma 9

**Statement:**

For any $n \in \mathbb{Z}_{>0}$,

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

In particular for prime $p$,

$$\Phi_p(x) = \sum_{i=0}^{p-1} x^i.$$

**Proof:** Over $\mathbb{C}$ we have the complete factorization into roots of unity:

$$x^n - 1 = \prod_{\zeta^n=1} (x - \zeta).$$

Grouping the factors according to the order of $\zeta$ yields

$$\prod_{\zeta^n=1} (x - \zeta) = \prod_{d|n} \prod_{\substack{\gcd(k,d)=1 \\ 1 \le k \le d}} (x - \zeta_d^k) = \prod_{d|n} \Phi_d(x).$$

■

### Lemma 10

**Statement:**

$\Phi_n$ is irreducible over $\mathbb{Q}[x]$.

**Proof:** $\Phi_n$ is minimal polynomial of $\zeta_n^k$, $1 \le k \le n$, hence irreducible over $\mathbb{Z}[x]$, also since $\Phi_n$ monic, we have $\Phi_n$ irreducible over $\mathbb{Q}[x]$ by **Gauss's Irreducibility Lemma**. ■

## Lemma 11

**Statement:**

If $n > 1$ is odd, then

$$\Phi_{2n}(x) = \Phi_n(-x).$$

**Proof:**
Let $k := 2m + 1$ with $\gcd(m, n) = 1$. Then

$$\zeta_{2n}^k = \zeta_{2n}^{2m+1} = \zeta_{2n}^{2m}\,\zeta_{2n} = \zeta_n^m\,(-1) = -\zeta_n^m.$$

Hence

$$\Phi_{2n}(x) = \prod_{\gcd(k,2n)=1} (x - \zeta_{2n}^k) = \prod_{\gcd(m,n)=1} (x - (-\zeta_n^m)) = \prod_{\gcd(m,n)=1} (x + \zeta_n^m) = \Phi_n(-x).$$

■

## Lemma 12

**Statement:**

For any $n \in \mathbb{Z}_{>0}$, $\Phi_n \in \mathbb{Z}[x]$ and monic.

**Proof:** We argue by strong induction on $n$. For $n = 1$, $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Assume $\Phi_d(x) \in \mathbb{Z}[x]$ and monic for every proper divisor $d < n$. From the factorization

$$x^n - 1 \;=\; \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{n \neq d|n} \Phi_d(x).$$

The product $\displaystyle\prod_{n \neq d|n} \Phi_d(x) \in \mathbb{Z}[x]$ and monic so we are done. ■

## Theorem 37 *Lagrange Interpolation*

**Statement:**

Let $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ be $n$ distinct points with $x_i \neq x_j$ for $i \neq j$. Then the unique polynomial $P(x)$ of degree at most $n-1$ such that

$$P(x_i) = y_i, \quad \forall\, 1 \leq i \leq n,$$

is given by:

$$P(x) = \sum_{i=1}^{n} y_i \prod_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{x - x_j}{x_i - x_j}.$$

**Proof:**
Consider a polynomial of the form

$$f(x) = A_0 \prod_{j \neq 0} (x - x_j) + A_1 \prod_{j \neq 1} (x - x_j) + \cdots + A_n \prod_{j \neq n} (x - x_j).$$

Substitute $x = x_0$, we get:

$$f(x_0) = y_0 = A_0 \prod_{j \neq 0} (x_0 - x_j), \quad \Rightarrow \quad A_0 = \frac{y_0}{\prod_{j \neq 0} (x_0 - x_j)}.$$

Substitute $x = x_1$, we get:

$$f(x_1) = y_1 = A_1 \prod_{j \neq 1} (x_1 - x_j), \quad \Rightarrow \quad A_1 = \frac{y_1}{\prod_{j \neq 1} (x_1 - x_j)}.$$

Continue this process for each $i = 0, 1, \ldots, n$, we obtain

$$f(x) = \sum_{i=0}^{n} y_i \cdot \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)}.$$

Thus,

$$f(x) = \sum_{i=0}^{n} y_i \prod_{\substack{0 \leq j \leq n \\ j \neq i}} \frac{x - x_j}{x_i - x_j}.$$

■

## Lemma 13

**Statement:**

If $P(x) \in \mathbb{Z}$ for 1+ deg $P$ consecutive integers $x$, then $P(x) \in \mathbb{Z}$ for $\forall x \in \mathbb{Z}$.

**Proof:** Apply induction: The case deg $P = 0$ is trivial, suppose the statement is true for deg $P = n$, then for $n+1$, consider $A = \{a, a+1, ..., a+n+1\}$ such that $P(x) \in \mathbb{Z}$ for $\forall x \in A$. Note that $\deg(\Delta P(x)) = n - 1$ and it's also integer when take element of $A$ as argument, by inductive hypothesis $\Delta P(x) = 0$, for $\forall x \in \mathbb{Z}$. Consider $\Delta P(a) = P(a) - P(a-1) \in \mathbb{Z} \Rightarrow P(a-1) \in \mathbb{Z}$, simply apply induction to get $P(x) \in \mathbb{Z}$ for $\forall x \in \mathbb{Z}$. ■

## Theorem 38 *Descartes' Rule of Signs*

**Statement:**

Let $f(x) \in \mathbb{R}[x]$, then the number of positive real roots (counted with multiplicity) is either equal to the number of sign changes in the sequence of its nonzero coefficients or differs from it by an even number.
Likewise, the number of negative real roots is either the number of sign changes in the coefficients of $f(-x)$, or differs from it by an even number.

**Proof:** We prove the positive root case by induction on the degree $n$. Let $f(x) \in \mathbb{R}[x]$ and let $v(f)$ be the number of sign changes in the sequence of its nonzero coefficients.
If $f(x)$ has a positive real root $r > 0$, then we can factor

$$f(x) = (x - r)g(x), \quad \text{with } g(x) \in \mathbb{R}[x].$$

We will show that:

$$v(f) \geq v(g) + 1.$$

That is, factoring out a positive root reduces the number of sign changes by at least 1.
To see this, write:

$$f(x) = (x - r)(b_0 x^{n-1} + b_1 x^{n-2} + \cdots + b_{n-1}),$$

then:

$$f(x) = b_0 x^n + (b_1 - rb_0)x^{n-1} + (b_2 - rb_1)x^{n-2} + \cdots + (-rb_{n-1}).$$

Compare the sign sequence of coefficients: each term $(b_k - rb_{k-1})$ is a linear combination of previous coefficients and real positive number $r > 0$. At each step, if the sign of $b_k$ differs from that of $b_{k-1}$, there's a potential sign change in $f(x)$ even if $g(x)$ had none.
One can verify that factoring out a positive real root from a polynomial will cause either:
- the number of sign changes to drop by exactly one, or
- the number of sign changes to remain unchanged and the root has multiplicity $> 1$, so we still subtract an even number from the count.
Thus, the number of positive real roots $p$ (with multiplicity) satisfies

$$p \leq v(f), \quad \text{and } v(f) - p \text{ is even.}$$

A similar argument applies to $f(-x)$, whose positive roots correspond to negative roots of $f(x)$. So the number of negative real roots is bounded above by the number of sign changes in $f(-x)$, differing from it by an even number.

■

## Lemma 14

**Statement:**

If $P(\shortparallel) \subseteq \mathbb{Q}$, for all $q \in \mathbb{Q}$. then $P \in \mathbb{Q}[x]$.

**Proof:** Let $a_i$ be coefficient of $P$, $1 \leq i \leq n$. Note that

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & 1^1 & \cdots & 1^n \\ \vdots & \vdots & \ddots & \vdots \\ 1 & n^1 & \cdots & n^n \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} P(0) \\ P(1) \\ \vdots \\ P(n) \end{bmatrix}$$

where the square matrix on $LHS$ is **Vandermonde Matrix** with pairwise different elements in second column which is invertible. Thus, $a_i \in \mathbb{Q}$ since the coefficient of the inverse of the square matrix is rational.

■

**Theorem 39** *Dyson's Conjecture*

**Statement:**

Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}_{\geq 0}$. Then the constant term of $\displaystyle\prod_{\substack{1\leq i,j\leq n\\ i\neq j}} \left(1-\frac{x_i}{x_j}\right)^{a_i}$ is $\dfrac{\left(\displaystyle\sum_{i=1}^{n} a_i\right)!}{\displaystyle\prod_{i=0}^{n} a_i!}$.

**Proof:** (*by I.J. Good*)

Let $f(a_1, a_2, \ldots, a_n)$ be constant term of $\displaystyle\prod_{\substack{1\leq i,j\leq n\\ i\neq j}} \left(1-\frac{x_i}{x_j}\right)^{a_i}$,

and let

$$g(a_1, a_2, \ldots, a_n) := \frac{\left(\displaystyle\sum_{i=1}^{n} a_i\right)!}{\displaystyle\prod_{i=0}^{n} a_i!}.$$

We prove $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$ by induction on $\sum a_i$.
When $a_1 = a_2 = \cdots = a_n = 0$, both sides are 1, so the base case is clear.
Note that $g$ satisfies the recurrence: If $a_1, a_2, \ldots, a_n > 0$, then

$$g(a_1, a_2, \ldots, a_n) = g(a_1 - 1, a_2, \ldots, a_n) + \cdots + g(a_1, a_2, \ldots, a_n - 1).$$

If $a_k = 0$, then

$$g(a_1, \ldots, a_{k-1}, 0, a_{k+1}, \ldots, a_n) = g(a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n).$$

So it suffices to show that $f$ also satisfies the same recurrence.
When $a_k = 0$, clearly

$$f(a_1, \ldots, a_{k-1}, 0, a_{k+1}, \ldots, a_n) = f(a_1, \ldots, a_{k-1}, a_{k+1}, \ldots, a_n).$$

When all $a_i > 0$, we must show

$$f(a_1, a_2, \ldots, a_n) = f(a_1 - 1, a_2, \ldots, a_n) + \cdots + f(a_1, a_2, \ldots, a_n - 1).$$

It suffices to prove

$$\prod_{\substack{1\leq i,j\leq n\\ i\neq j}} \left(1-\frac{x_i}{x_j}\right)^{a_i} = \prod_{\substack{1\leq i,j\leq n\\ i\neq j}} \left(1-\frac{x_i}{x_j}\right)^{a_i} \cdot \sum_{i=1}^{n} \prod_{\substack{j=1\\ j\neq i}}^{n} \left(1-\frac{x_i}{x_j}\right)^{-1}.$$

That is, we need

$$1 = \sum_{i=1}^{n} \prod_{\substack{j=1\\ j\neq i}}^{n} \left(1-\frac{x_i}{x_j}\right)^{-1}.$$

Apply the **Lagrange interpolation** to the constant function $f(x) = 1$ at $x_1, x_2, \ldots, x_n$, we obtain:

$$1 = \sum_{i=1}^{n} \prod_{\substack{j=1\\ j\neq i}}^{n} \frac{x - x_j}{x_i - x_j}.$$

Set $x = 0$, then

$$1 = \sum_{i=1}^{n} \prod_{\substack{j=1\\ j\neq i}}^{n} \left(\frac{-x_j}{x_i - x_j}\right) = \sum_{i=1}^{n} \prod_{\substack{j=1\\ j\neq i}}^{n} \left(1-\frac{x_i}{x_j}\right)^{-1},$$

as desired. ■

## **Theorem 40** *Gauss–Lucas Theorem*

**Statement:**

Let $P(z) \in \mathbb{C}[z]$ be a nonconstant complex polynomial. Then all roots of $P'(z)$ lie in the convex hull of the roots of $P(z)$.

**Proof:**
Let

$$P(z) = c\prod_{i=1}^{n}(z - z_i), \quad c \in \mathbb{C},$$

then,

$$\frac{P'(z)}{P(z)} = \sum_{i=1}^{n} \frac{1}{z - z_i}.$$

Let $P'(w) = 0$. If $P(w) = 0$, then $w$ is a root of both $P$ and $P'$, and lies within the root set of $P$, so the conclusion holds trivially. Now assume $P(w) \neq 0$. Then:

$$\sum_{i=1}^{n} \frac{1}{w - z_i} = 0.$$

This gives us

$$\sum_{i=1}^{n} \frac{\overline{w - z_i}}{|w - z_i|^2} = 0.$$

Hence:

$$\sum_{i=1}^{n} \frac{1}{|w - z_i|^2} \cdot \overline{w} = \sum_{i=1}^{n} \frac{1}{|w - z_i|^2} \cdot \overline{z_i}.$$

Taking conjugate again gives us $w$ is a linear combination of $z_1, \ldots, z_n$, with positive coefficient and sum to 1, so lies in the convex hull of $\{z_i\}$.

■

## **Theorem 41** *Combinatorial Nullstellensatz*

**Statement:**

Let $\mathbb{F}$ be a field, and let $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}[x_1, x_2, \ldots, x_n]$ with $\deg f = d_1 + d_2 + ... + d_n$. Suppose the monomial $x_1^{d_1} x_2^{d_2} \cdots x_n^{d_n}$ appears in $f(x_1, \ldots, x_n)$ with nonzero coefficient.
If $S_1, \ldots, S_n \subseteq \mathbb{F}$ with $|S_i| > d_i$ for all $1 \leq i \leq n$, then there exists $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ such that

$$f(s_1, \ldots, s_n) \neq 0.$$

**Proof:** (*by R. N. Karasev and F. V. Petrov*)
Assume $|S_i| = d_i + 1$ for $1 \leq i \leq n$. By **Lagrange Interpolation**, we have the identity:

$$[x^{n-1}]g(x) = \sum_{i=1}^{n} g(x_i) \prod_{j \neq i} \frac{1}{x_i - x_j}.$$

Then for $e_i \leq d_i = |S_i| - 1$, let $g(x) = x^{e_i}$, then

$$\sum_{s_i \in S_i} s_i^{e_i} \prod_{t_i \in S_i \setminus \{s_i\}} \frac{1}{s_i - t_i} = [x^{d_i}]x^{e_i} = \delta_{e_i,d_i}$$

Now consider a monomial $x_1^{e_1} \cdots x_n^{e_n}$ in $f(x_1, \ldots, x_n)$ with $e_i \le d_i$. Then

$$\sum_{s_1 \in S_1} \sum_{s_2 \in S_2} \cdots \sum_{s_n \in S_n} s_1^{e_1} s_2^{e_2} \cdots s_n^{e_n} \prod_{i=1}^{n} \prod_{t_i \in S_i \setminus \{s_i\}} \frac{1}{s_i - t_i} = \prod_{i=1}^{n} \left( \sum_{s_i \in S_i} s_i^{e_i} \prod_{t_i \in S_i \setminus \{s_i\}} \frac{1}{s_i - t_i} \right) = \prod_{i=1}^{n} \delta_{e_i, d_i},$$

which is $\mathbb{I}(e_i = d_i, \forall 1 \le i \le n)$. Thus

$$[x_1^{d_1} \cdots x_n^{d_n}] f(x_1, \ldots, x_n) = \sum_{s_1 \in S_1} \sum_{s_2 \in S_2} \cdots \sum_{s_n \in S_n} f(s_1, \ldots, s_n) \prod_{i=1}^{n} \prod_{t_i \in S_i \setminus \{s_i\}} \frac{1}{s_i - t_i}.$$

By assumption, the left-hand side is nonzero. Hence implies there exists some $(s_1, \ldots, s_n) \in S_1 \times \cdots \times S_n$ such that

$$f(s_1, \ldots, s_n) \neq 0.$$

■

## Theorem 42 *Mason–Stothers Theorem*

**Statement:**

Let $f, g, h \in \mathbb{C}[x]$ be pairwise coprime, nonconstant polynomials satisfying

$$f(x) + g(x) + h(x) = 0.$$

Then the number of distinct complex roots of the product $f(x)g(x)h(x)$ is at least

$$\max\{\deg f, \deg g, \deg h\} + 1.$$

**Proof:**
From $f(x) + g(x) + h(x) = 0$, we differentiate:

$$f'(x) + g'(x) + h'(x) = 0.$$

Eliminating $f(x)$, we obtain:

$$f'(x)(g(x) + h(x)) = f(x)(g'(x) + h'(x)),$$

which gives:

$$f'(x)g(x) - f(x)g'(x) = f(x)h'(x) - f'(x)h(x) := P(x).$$

Let $(f, f')$ denote the greatest common divisor of $f(x)$ and $f'(x)$ as a polynomial, and similarly for $(g, g')$, $(h, h')$.
Then:

$$(f, f') \mid P(x), \quad (g, g') \mid P(x), \quad (h, h') \mid P(x).$$

Since $f(x), g(x), h(x)$ are pairwise coprime, the terms $(f, f')$, $(g, g')$, $(h, h')$ are also pairwise coprime. So:

$$(f, f') \times (g, g') \times (h, h') \mid P(x).$$

Suppose $P(x) = 0$. Then:

$$f'(x)g(x) = f(x)g'(x), \quad f(x)h'(x) = f'(x)h(x),$$

which implies $\dfrac{f(x)}{g(x)}$ and $\dfrac{f(x)}{h(x)}$ are both constant. This contradict to the statement $f, g, h$ are pairwise coprime and not all constant. Therefore $P(x) \neq 0$.

Hence,

$$\deg(f,f') + \deg(g,g') + \deg(h,h') \le \deg P.$$

Now write

$$f(x) = c\prod_{i=1}^{k}(x-x_i)^{\alpha_i},$$

with distinct $x_i$ and $\alpha_i \in \mathbb{Z}_{>0}$, $1 \le i \le k$. Then:

$$f'(x) = c\prod_{i=1}^{k}(x-x_i)^{\alpha_i-1}\left(\sum_{i=1}^{k}\prod_{j\neq i}(x-x_j)\right),$$

so

$$(f,f') = c\prod_{i=1}^{k}(x-x_i)^{\alpha_i-1} \quad\Rightarrow\quad \deg(f,f') = \sum_{i=1}^{t}(\alpha_i-1) = \deg f - n(f),$$

where $n(f)$ is the number of distinct roots of $f(x)$.
Also note:

$$\deg P(x) = \deg(f'g - fg') \le \deg f + \deg g - 1.$$

So:

$$\deg f - n(f) + \deg g - n(g) + \deg h - n(h) \le \deg f + \deg g - 1,$$

which gives

$$\deg h \le n(fgh) - 1.$$

The same argument holds for $f(x), g(x)$. ■

## Definition 7 *Chebyshev Polynomial of The First Kind*

**Description:**

The **Chebyshev polynomial of the first kind** $T_n$ is defined by the recurrence relation:

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x), \quad n \ge 1$$

with $T_0(x) = 1$ and $T_1(x) = x$.

## Lemma 15

**Statement:**

Let $T_n$ be the Chebyshev polynomials of the first kind, then for $x \in \mathbb{C}$ and $n \in \mathbb{Z}_{\ge 0}$,

$$T_n(\cos(x)) = \cos(nx).$$

**Proof:**
Let us define $f_n(x) := \cos(nx)$. We show that the sequence $f_n(\cos x)$ satisfies the same recurrence as $T_n(x)$.
Note that

$$f_0(\cos x) = \cos(0) = 1, \quad f_1(\cos x) = \cos x.$$

Using the identity

$$\cos((n+1)x) = 2\cos x \cdot \cos(nx) - \cos((n-1)x),$$

we deduce that

$$f_{n+1}(\cos x) = 2\cos x \cdot f_n(\cos x) - f_{n-1}(\cos x).$$

Therefore, $f_n(\cos x)$ satisfies the same recurrence as $T_n(x)$ and has the same initial values. ■

## Lemma 16

**Statement:**

For any $n \in \mathbb{Z}_{\geq 0}$, let $T_n(x)$ be the Chebyshev polynomials of the first kind, then the coefficient of the term $x^n$ in $T_n(x)$ is equal to $2^{n-1}$ for $n \geq 1$, and 1 for $n = 0$.

**Proof:** Letting $x = \cos\theta$, we start by using the identity:

$$T_n(x) = \cos(n\theta) = \frac{e^{in\theta} + e^{-in\theta}}{2} = \frac{(\cos\theta + i\sin\theta)^n + (\cos\theta - i\sin\theta)^n}{2},$$

we use the identity $\sin\theta = \sqrt{1-x^2}$, and so we obtain:

$$T_n(x) = \frac{(x+\sqrt{x^2-1})^n + (x-\sqrt{x^2-1})^n}{2}.$$

Then the leading coefficient of $T_n$ can be calculated by,

$$\lim_{x\to\infty} \frac{T_n(x)}{x^n} = \lim_{x\to\infty} \frac{\left(1+\sqrt{1-\frac{1}{x^2}}\right)^n + \left(1-\sqrt{1-\frac{1}{x^2}}\right)^n}{2} = 2^{n-1}.$$

■

## Lemma 17

**Statement:**

1. For $|x| \leq 1$, we have
$$|T_n(x)| \leq 1.$$

2. $T_n(x)$ has $n$ distinct real roots in $[-1, 1]$, given by
$$\cos\left(\frac{(2k-1)\pi}{2n}\right), \quad 1 \leq k \leq n.$$

3. $T_n(x)$ has $n+1$ extrema in $[-1, 1]$, occurring at
$$\cos\left(\frac{k\pi}{n}\right), \quad 0 \leq k \leq n,$$
and the extrema alternate between 1 and $-1$.

4. $T_n(x)$ is an even function if $n$ is even, and an odd function if $n$ is odd.

**Proof:** Trivial by the identity $T_n(x) := \cos(n\cos^{-1}(x))$. ■

## Definition 8 *Chebyshev Polynomial of Second Kind*

**Description:**

The **Chebyshev polynomials of second kind** $U_n(x)$ are defined recursively by:

$$U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x), \quad n \geq 1.$$

with $U_0(x) = 1$ and $U_1(x) = 2x$.

## Lemma 18

**Statement:**

For any integer $n \geq 0$ and $x \in \mathbb{C}$, $U_n$ be the Chebyshev polynomials of the second kind, then

$$U_n(\cos\theta)\sin\theta = \sin((n+1)\theta).$$

**Proof:** The case $\theta = k\pi$ is trivial, assume otherwise, define

$$f_n(\theta) := \frac{\sin((n+1)\theta)}{\sin\theta}.$$

We will prove that $f_n(\theta)$ satisfies the same recurrence as $f_n(\cos\theta)$, hence they are equal.
Note that:

$$f_0(\theta) = \frac{\sin\theta}{\sin\theta} = 1, \quad f_1(\theta) = \frac{\sin(2\theta)}{\sin\theta} = \frac{2\sin\theta\cos\theta}{\sin\theta} = 2\cos\theta.$$

and observe that

$$\begin{aligned} f_{n+1}(\theta) &= \frac{\sin((n+2)\theta)}{\sin\theta}, \\ &= \frac{2\cos\theta\,\sin((n+1)\theta) - \sin(n\theta)}{\sin\theta} \\ &= 2\cos\theta\frac{\sin((n+1)\theta)}{\sin\theta} - \frac{\sin(n\theta)}{\sin\theta}, \\ &= 2\cos\theta\, f_n(\theta) - f_{n-1}(\theta). \end{aligned}$$

Hence, $f_n(\theta)$ satisfies the same recurrence as $U_n(\cos\theta)$, and matches the initial values. ■

## Lemma 19

**Statement:**

1. $U_n(x)$ has $n$ distinct real roots in $[-1,1]$, given by
$$\cos\Big(\frac{k\pi}{n+1}\Big), \quad 1 \le k \le n.$$

2. $U_n(x)$ has $n+1$ extrema in $[-1,1]$, occurring at
$$x_k = \cos\Big(\frac{k\pi}{n+1}\Big), \quad 0 \le k \le n,$$
with
$$U_n(1) = n+1, \quad U_n(-1) = (-1)^n(n+1), \quad U_n\big(x_k\big) = (-1)^k \quad (1 \le k \le n-1).$$

3. $U_n(x)$ is even if $n$ is even, and odd if $n$ is odd.

**Proof:** Trivial by $U_n(\cos\theta)\sin\theta = \sin((n+1)\theta)$. ■

## Lemma 20

**Statement:**

Following are the recurrence relations between two kinds of Chebyshev Polynomial:
1. $T_n(x) = U_n(x) - x\,U_{n-1}(x)$.

2. $U_n(x) = \dfrac{T_n(x) - x\,T_{n+1}(x)}{1-x^2}$.

**Proof:**
Set $x = \cos\theta$. Then
$$T_n(x) = \cos(n\theta), \qquad U_n(x) = \frac{\sin((n+1)\theta)}{\sin\theta}.$$

(1)
$$\begin{aligned} U_n(x) - x\,U_{n-1}(x) &= \frac{\sin((n+1)\theta) - \cos\theta\,\sin(n\theta)}{\sin\theta} \\ &= \frac{\sin(n\theta)\cos\theta + \cos(n\theta)\sin\theta - \cos\theta\,\sin(n\theta)}{\sin\theta} \\ &= \cos(n\theta) = T_n(x). \end{aligned}$$

(2)
$$T_n(x) - x\,T_{n+1}(x) = \cos(n\theta) - \cos\theta\,\cos((n+1)\theta) = \sin\theta\,\sin((n+1)\theta),$$

so
$$\frac{T_n(x) - x\,T_{n+1}(x)}{1-x^2} = \frac{\sin\theta\,\sin((n+1)\theta)}{\sin^2\theta} = \frac{\sin((n+1)\theta)}{\sin\theta} = U_n(x).$$

■

## 1.4 Sequence

### Definition 9 *Fibonacci Sequence*

**Description:**

The **Fibonacci Sequence** $(f_n)_{n\geq 0}$ is defined by

$$f_n = f_{n-1} + f_{n-2}, \quad n \geq 2.$$

with $f_0 = 0$ and $f_1 = 1$. $f_n$ is called the **Fibonacci number**.

### Theorem 43 *Binet's Formula*

**Statement:**

Let $(f_n)_{n\geq 0}$ be Fibonacci Sequence, we have

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

where $\varphi = \dfrac{1+\sqrt{5}}{2}$, $\psi = \dfrac{1-\sqrt{5}}{2}$.

**Proof:**
Noted that the roots of the quadratic equation $x^2 - x - 1 = 0$ are $\varphi$ and $\psi$. We claim that

$$x^n = f_n x + f_{n-1}.$$

Apply induction: The case $n = 1$ is trivial, suppose for $n$ our claim is true, then for $n+1$,
$x^{n+1} = x \cdot x^n = x(f_n x + f_{n-1}) = f_n x^2 + f_{n-1}x = f_n(x+1) + f_{n-1}x = (f_n + f_{n-1})x + f_n = f_{n+1}x + f_n$.

■

### Theorem 44 *Cassini' s Identity*

**Statement:**

Let $(f_n)_{n\geq 0}$ be Fibonacci Sequence, then

$$f_{n-1}f_{n+1} \ - \ f_n^2 \ = \ (-1)^n.$$

for $n \in \mathbb{Z}_{>0}$.

**Proof:**

$$f_{n-1}f_{n+1} - f_n^2 = \begin{vmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{vmatrix} = \det\left(\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n\right) = \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}^n = (-1)^n.$$

■

### Theorem 45 *Catalan's Identity*

**Statement:**

Let $(f_n)_{n\geq 0}$ be Fibonacci Sequence, then

$$f_n{}^2 - f_{n+r}f_{n-r} = (-1)^{n-r}f_r{}^2.$$

For integer $0 \leq r \leq n$.

**Proof:**
Using **Binet' s formula**,

$$\begin{aligned}5\big(f_n^2 - f_{n-r}f_{n+r}\big) &= (\varphi^n - \psi^n)^2 - (\varphi^{n-r} - \psi^{n-r})(\varphi^{n+r} - \psi^{n+r}) \\ &= \varphi^{2n} - 2\varphi^n\psi^n + \psi^{2n} - \big[\varphi^{2n} - \varphi^{n-r}\psi^{n+r} - \varphi^{n+r}\psi^{n-r} + \psi^{2n}\big] \\ &= -2(\varphi\psi)^n + \varphi^{n-r}\psi^{n+r} + \varphi^{n+r}\psi^{n-r} \\ &= -2(-1)^n + (-1)^{n-r}\big(\varphi^{2r} + \psi^{2r}\big) \;=\; (-1)^{n-r}\big(\varphi^r - \psi^r\big)^2 \\ &= (-1)^{n-r}\,5\,f_r^2.\end{aligned}$$

■

### Theorem 46 *Gelin-Cesàro Identity*

**Statement:**

Let $(f_n)_{n\geq 0}$ be Fibonacci Sequence, then

$$f_n{}^4 - f_{n-2}f_{n-1}f_{n+1}f_{n+2} = 1.$$

for integer $n \geq 2$.

**Proof:**
WLOG let $2 \mid n$, by **Catalan's Identity** $(r = 1, 2)$,

$$f_{n+1}f_{n-1} - f_n{}^2 = 1 = f_n{}^2 - f_{n+2}f_{n-2},$$

then

$$f_n{}^4 - 1 = (f_n{}^2 - 1)(f_n{}^2 + 1) = f_{n-2}f_{n-1}f_{n+1}f_{n+2}.$$

■

### Theorem 47 *d' Ocagne' s Identity*

**Statement:**

Let $(f_n)_{n\geq 0}$ be Fibonacci Sequence, then

$$f_m\,f_{n+1} \;-\; f_{m+1}\,f_n \;=\; (-1)^n\,f_{m-n}.$$

for integers $m \geq n \geq 0$.

**Proof:**
By **Binet’s formula** we compute

$$\begin{aligned}
f_m\, f_{n+1} - f_{m+1}\, f_n &= \frac{1}{5}\Big[(\varphi^m - \psi^m)(\varphi^{n+1} - \psi^{n+1}) - (\varphi^{m+1} - \psi^{m+1})(\varphi^n - \psi^n)\Big] \\
&= \frac{1}{5}\Big[\varphi^m \psi^n (\psi - \varphi) - \psi^m \varphi^n (\psi - \varphi)\Big] \\
&= \frac{\psi - \varphi}{5}\,\big(\varphi^m \psi^n - \psi^m \varphi^n\big) = -\frac{\sqrt{5}}{5}\,\big(\varphi^{\,m-n} - \psi^{\,m-n}\big) \\
&= (-1)^n\, \frac{\varphi^{\,m-n} - \psi^{\,m-n}}{\sqrt{5}} \;=\; (-1)^n\, f_{m-n}.
\end{aligned}$$

■

## Theorem 48 *Vajda’s Identity*

**Statement:**

Let $(f_n)_{n\geq 0}$ be Fibonacci Sequence, then

$$f_{n+r}\, f_{n-s} \;-\; f_n\, f_{n+r-s} \;=\; (-1)^{\,n-s}\, f_r\, f_s.$$

For integers $n, m, r, s$ with $n \geq s$.

**Proof:**
By **Binet’s formula**, we compute

$$\begin{aligned}
&f_{n+r}\, f_{n-s} - f_n\, f_{n+r-s} \\
&\quad= \frac{1}{5}\Big[(\varphi^{n+r} - \psi^{n+r})(\varphi^{\,n-s} - \psi^{\,n-s}) - (\varphi^n - \psi^n)(\varphi^{\,n+r-s} - \psi^{\,n+r-s})\Big] \\
&\quad= \frac{1}{5}\Big[\varphi^{\,n-s}\psi^{\,n-s}(\varphi^r \psi^{-s} - \psi^r \varphi^{-s}) - \psi^{\,n-s}\varphi^{\,n-s}(\varphi^r \psi^{-s} - \psi^r \varphi^{-s})\Big] \\
&\quad= \frac{\varphi^{n-s} - \psi^{n-s}}{5}\,\left(\varphi^r \psi^{-s} - \psi^r \varphi^{-s}\right) \\
&\quad= \frac{(\varphi^r - \psi^r)(\varphi^s - \psi^s)}{5}\,(-1)^{\,n-s} = (-1)^{\,n-s} f_r\, f_s.
\end{aligned}$$

■

## Theorem 49 *Honsberger’s Identity*

**Statement:**

Let $(f_n)_{n\geq 0}$ be Fibonacci Sequence, then

$$f_{m-1} f_n + f_m\, f_{n+1} \;=\; f_{n+m}.$$

for integers $m \geq 1$ and $n \geq 0$.

**Proof:**

By **Binet' s formula**, we have

$$\begin{aligned}
f_{m-1}f_n + f_m\, f_{n+1} &= \frac{\varphi^{m-1}-\psi^{m-1}}{\sqrt{5}}\,\frac{\varphi^{n}-\psi^{n}}{\sqrt{5}} + \frac{\varphi^{m}-\psi^{m}}{\sqrt{5}}\,\frac{\varphi^{n+1}-\psi^{n+1}}{\sqrt{5}} \\
&= \frac{1}{5}\Big[\varphi^{m+n-1} - \varphi^{m-1}\psi^{n} - \psi^{m-1}\varphi^{n} + \psi^{m+n-1} \\
&\qquad + \ \varphi^{m+n+1} - \varphi^{m}\psi^{n+1} - \psi^{m}\varphi^{n+1} + \psi^{m+n+1}\Big] \\
&= \frac{1}{5}\Big[\varphi^{m+n-1}(1+\varphi^2) + \psi^{m+n-1}(1+\psi^2) \\
&\qquad - \ \varphi^{m-1}\psi^{n}\,(1+\varphi\psi) - \ \psi^{m-1}\varphi^{n}\,(1+\varphi\psi)\Big] \\
&= \frac{1}{5}\Big[\varphi^{m+n-1}(1+\varphi^2) + \psi^{m+n-1}(1+\psi^2)\Big] \quad (\varphi\psi=-1) \\
&= \frac{1}{5}\Big[\varphi^{m+n-1}(2+\varphi) + \psi^{m+n-1}(2+\psi)\Big] \quad (\varphi^2=\varphi+1,\ \psi^2=\psi+1) \\
&= \frac{1}{5}\Big[\varphi^{m+n-1}\frac{5+\sqrt{5}}{2} + \psi^{m+n-1}\frac{5-\sqrt{5}}{2}\Big] \\
&= \frac{\varphi^{m+n}-\psi^{m+n}}{\sqrt{5}} \ = \ f_{m+n}.
\end{aligned}$$

■

## Definition 10 *Lucas Sequence*

**Description:**

The **Lucas Sequence** $(L_n)_{n\geq 0}$ is defined by

$$L_n = L_{n-1} + L_{n-2}, \quad n \geq 2,$$

with $L_0 = 2$ and $L_1 = 1$. $L_n$ is called the **Lucas number**.

## Theorem 50 *Closed Form of the Lucas Sequence*

**Statement:**

The closed form of **Lucas Sequence** $(L_n)_{n\geq 0}$ is given by

$$L_n \ = \ \varphi^n + \psi^n,$$

where $\varphi = \dfrac{1+\sqrt{5}}{2}, \quad \psi = \dfrac{1-\sqrt{5}}{2}$.

**Proof:**
Consider the **characteristic polynomial** of the recurrence:

$$r^2 - r - 1 = 0,$$

whose two roots are $\varphi$ and $\psi$.
Hence the general solution of the recurrence is

$$L_n = A\,\varphi^n + B\,\psi^n$$

for constants $A, B$. Using the initial conditions:

$$\begin{cases} L_0 = 2 = A + B, \\ L_1 = 1 = A\,\varphi + B\,\psi, \end{cases}$$

we solve for $A$ and $B$. Since $\varphi + \psi = 1$, one finds

$$A = 1, \quad B = 1.$$

Therefore

$$L_n = \varphi^n + \psi^n,$$

as claimed. ■

## Definition 11 *Farey Sequence*

**Definition:**

The **Farey sequence** of order $n$ is the ascending sequence of all irreducible fractions $\frac{a}{b}$ with $0 \leq a \leq b \leq n$ and $\gcd(a, b) = 1$.

## Lemma 21

**Statement:**

Let $\frac{a}{b}$ and $\frac{a'}{b'}$ be consecutive terms in the Farey sequence of order $n$, with $\frac{a}{b} < \frac{a'}{b'}$. Then

$$b + b' \geq n + 1, \qquad a'b - ab' = 1.$$

**Proof:**
We try to confirm $\frac{a'}{b'}$. Consider $x, y \in \mathbb{Z}$ s.t

$$bx - ay = 1 \qquad \text{and} \qquad n - b < y \leq n,$$

there $\exists$ such $x, y$ because there is a solution for $ay \equiv -1 \pmod{b}$ which is $-a^{-1} \pmod{b}$ and consider the complete residue system mod $b$, $\{n, n-1, ..., n-(b-1)\} := R$, pick $y \in R$ and $y \equiv -a^{-1} \pmod{b}$.

Now we prove that infact $\frac{a'}{b'} = \frac{x}{y}$. Suppose not, recall that $\frac{a}{b}$ and $\frac{a'}{b'}$ are consecutive term, and $\frac{x}{y}$ also one of the term in Ferray Sequence of order $n$ (obviously we have $0 \leq y \leq n$ and $\gcd(x, y) = 1$), also

$$\frac{x}{y} = \frac{a}{b} + \frac{1}{by} > \frac{a}{b} \quad \Rightarrow \quad \frac{x}{y} > \frac{a'}{b'},$$

so

$$\frac{x}{y} - \frac{a'}{b'} = \frac{b'x - x'y}{b'y} \geq \frac{1}{b'y}.$$

Similarly,

$$\frac{a'}{b'} - \frac{a}{b} \geq \frac{1}{bb'},$$

hence

$$\frac{1}{by} = \frac{x}{y} - \frac{a}{b} \geq \frac{1}{b'y} + \frac{1}{bb'} \quad \Rightarrow \quad b' \geq y + b > n,$$

contradiction.
So we have $\frac{a'}{b'} = \frac{x}{y}$ which also means that

$$x = a', \;\; y = b'.$$

now

$$ba' - b'a = bx - ay = 1, \quad b + b' = b + y > n.$$

■

## Definition 12 *Characteristic Polynomial of Linear Recurrence Relation*

**Statement:**

Let

$$a_{n+k} = c_1\, a_{n+k-1} + c_2\, a_{n+k-2} + \cdots + c_k\, a_n, \qquad n \geq 0,$$

be a linear homogeneous recurrence with constant coefficients. Its **characteristic polynomial** is the polynomial degree $k$ .

$$p(x) = x^k - c_1 x^{k-1} - c_2 x^{k-2} - \cdots - c_k.$$

***Remark:*** consider linear transformation

$$A = \begin{bmatrix} c_1 & c_2 & \cdots & c_{k-1} & c_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix},$$

then we have

$$A \begin{bmatrix} a_{n+k-1} \\ a_{n+k-2} \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} a_{n+k} \\ a_{n+k-1} \\ \vdots \\ a_{n+1} \end{bmatrix}$$

then the characteristic polynomial of $A$ is actually the definition of characteristic polynomial of the linear recurrence.

**Theorem 51** *Closed Form Solution of a Linear Recurrence*

**Statement:**

Let $(a_n)_{n\geq 0}$ satisfy the linear homogeneous recurrence

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

and let the complex roots of its characteristic polynomial be $\lambda_1, \lambda_2, ..., \lambda_m$ with multiplicities $e_1, e_2, ..., e_m$ such that $\sum\limits_{i=1}^{m} e_i = k$ Then the general term admits the closed form

$$a_n \;=\; \sum_{i=1}^{m} P_i(n)\, \lambda_i^n,$$

where each $P_i(n)$ is a polynomial with $\deg P_i < e_i$.

**Proof:** We use linear algebra: define the forward shift operator $E$ by

$$Ea_n \;=\; a_{n+1}.$$

Then the recurrence is equivalent to

$$p(E)\, a_n \;=\; \bigl(E^k - c_1 E^{k-1} - \cdots - c_k I\bigr)\, a_n \;=\; 0,$$

where $I$ is the identity operator. Since

$$p(x) = \prod_{i=1}^{m} (x - \lambda_i)^{e_i} \quad\Longrightarrow\quad p(E) = \prod_{i=1}^{m} (E - \lambda_i I)^{e_i},$$

we have

$$\prod_{i=1}^{m} (E - \lambda_i I)^{e_i}\, a_n = 0.$$

Since the factors $(E - \lambda_i I)^{e_i}$ are pairwise coprime as polynomials in $E$, we have

$$\ker p(E) \;=\; \bigoplus_{i=1}^{m} \ker\bigl(E - \lambda_i I\bigr)^{e_i}.$$

For a fixed root $\lambda$ of multiplicity $e$, the equation

$$(E - \lambda I)^e\, u_n = 0$$

expands to a linear difference equation of order $e$, whose general solution is

$$u_n \;=\; \sum_{j=0}^{e-1} C_j\, n^j\, \lambda^n,$$

i.e. a polynomial in $n$ of degree $< e$ times $\lambda^n$. Hence

$$\dim(\ker(E - \lambda_i I)^{e_i}) = e_i, \quad 1 \leq i \leq m$$

with basis $\{n^j \lambda_i^n : 0 \leq j < e_i\}$. Summing over all $i$ yields

$$a_n \;=\; \sum_{i=1}^{m} \sum_{j=0}^{e_i - 1} C_{i,j}\, n^j\, \lambda_i^n \;=\; \sum_{i=1}^{m} P_i(n)\, \lambda_i^n,$$

with $\deg P_i < e_i$. This completes the proof. ■

## 1.5 Complex Number

***Remark:*** In this section, we use $i := \sqrt{-1}$ as the imaginary unit.

**Theorem 52** *De Moivre's Theorem*

**Statement:**

For any $\theta \in \mathbb{R}$ and $n \in \mathbb{Z}$,

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

**Proof:**
We first prove that it is true for all $n \in \mathbb{Z}_{\geq 0}$. The base case is trivial. Assume for some $k \in \mathbb{Z}_{\geq 0}$,

$$(\cos\theta + i\sin\theta)^k = \cos(k\theta) + i\sin(k\theta).$$

Then

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

$$= \cos k\theta\cos\theta - \sin k\theta\sin\theta \;+\; i\big(\cos k\theta\sin\theta + \sin k\theta\cos\theta\big) = \cos\big((k+1)\theta\big) + i\sin\big((k+1)\theta\big),$$

completing the step.
For $n < 0$, write $n = -m$ with $m > 0$. Then

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

using the fact that cos is even and sin is odd.

■

## Theorem 53 *Euler's Formula*

**Statement:**

For any $\theta \in \mathbb{R}$, one has

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

**Proof:** (*Power-series proof*)
Recall the **Taylor expansions** for real $x$:

$$e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!}, \quad \cos x = \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k}}{(2k)!}, \quad \sin x = \sum_{k=0}^{\infty}(-1)^k\frac{x^{2k+1}}{(2k+1)!}.$$

Substitute $x = i\theta$ into the exponential series:

$$e^{i\theta} = \sum_{n=0}^{\infty}\frac{(i\theta)^n}{n!} = \sum_{k=0}^{\infty}\frac{(i\theta)^{2k}}{(2k)!} + \sum_{k=0}^{\infty}\frac{(i\theta)^{2k+1}}{(2k+1)!}.$$

Noting $i^{2k} = (-1)^k$ and $i^{2k+1} = (-1)^k\,i$, this becomes

$$e^{i\theta} = \sum_{k=0}^{\infty}(-1)^k\frac{\theta^{2k}}{(2k)!} \;+\; i\sum_{k=0}^{\infty}(-1)^k\frac{\theta^{2k+1}}{(2k+1)!} = \cos\theta + i\sin\theta.$$

■

## Theorem 54 *Euler's Identity*

**Statement:**

$$e^{i\pi} + 1 = 0.$$

**Proof:**
by **Euler' s formula**. ■

## Theorem 55 *Gauss Sum*

**Statement:**

Let $p$ be an odd prime, then

$$\sum_{k=1}^{p-1} \zeta_p^{k^2} = \begin{cases} \pm\sqrt{p}, & p \equiv 1 \pmod 4, \\ \pm i\sqrt{p}, & p \equiv 3 \pmod 4. \end{cases}$$

**Proof:**
Define the polynomial

$$g_p(x) := \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) x^k.$$

where $\left(\frac{k}{p}\right)$ is the **Legendre Symbol**. Our goal is to show

$$g_p(\zeta_p)^2 \;=\; \left(\frac{-1}{p}\right) p.$$

Recall that

$$\left(\frac{a}{p}\right) = 0 \quad \text{whenever } p \mid a.$$

Then one may equally write

$$g_p(x) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) x^k.$$

Observe

$$g_p(\zeta_p)^2 = \sum_{j=0}^{p-1} \sum_{k=0}^{p-1} \left(\frac{j}{p}\right) \left(\frac{k}{p}\right) \zeta_p^{j+k}.$$

Since $\zeta_p^p = 1$, reduce exponents mod $p$ and collect like terms to get

$$g_p(\zeta_p)^2 = \sum_{k=0}^{p-1} a_k \zeta_p^k, \tag{1.1}$$

where for each $n \in \mathbb{Z}_p$,

$$a_n \;=\; \sum_{j+k \equiv n \pmod p} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right). \tag{1.2}$$

Since

$$g_p(1) = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) = 0$$

(because $\mathbb{Z}_p^\times$ has equally many residues and non-residues), it follows $g_p(1)^2 = 0$ and hence

$$\sum_{k=0}^{p-1} a_k = 0. \tag{1.3}$$

By (1.2),

$$a_0 = \sum_{j+k \equiv 0 \pmod p} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right) = \sum_{j=0}^{p-1} \left(\frac{-j}{p}\right)\left(\frac{j}{p}\right).$$

But

$$\left(\frac{-j}{p}\right)\left(\frac{j}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{j^2}{p}\right) = \begin{cases} 0, & j = 0, \\ \left(\frac{-1}{p}\right), & 1 \le j \le p-1, \end{cases}$$

so

$$a_0 = \sum_{j=1}^{p-1} \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)(p-1). \tag{1.4}$$

For $n \in \{1, \dots, p-1\}$, by (1.2)

$$a_n = \sum_{j+k \equiv n \pmod p} \left(\frac{j}{p}\right)\left(\frac{k}{p}\right).$$

Set $j = nj'$, $k = nk'$. Then $j' + k' \equiv 1 \pmod p$ and

$$a_n = \sum_{j'+k' \equiv 1 \pmod p} \left(\frac{nj'}{p}\right)\left(\frac{nk'}{p}\right) = \sum_{j'+k' \equiv 1 \pmod p} \left(\frac{j'}{p}\right)\left(\frac{k'}{p}\right) = a_1,$$

hence

$$a_1 = a_2 = \cdots = a_{p-1}. \tag{1.5}$$

Combining (1.3) and (1.5) gives

$$a_0 + (p-1)\, a_1 = 0 \quad \Longrightarrow \quad a_1 = -\frac{a_0}{p-1}.$$

By (1.4),

$$a_1 = -\left(\frac{-1}{p}\right),$$

so from (1.1)

$$g_p(\zeta_p)^2 = \left(\tfrac{-1}{p}\right)\big((p-1) - (\zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1})\big).$$

But $1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$, hence $\zeta_p + \cdots + \zeta_p^{p-1} = -1$, and

$$g_p(\zeta_p)^2 = \left(\tfrac{-1}{p}\right) p.$$

This completes the proof of the Gauss sum formula. ■

## 1.6 Function

### Definition 13 *Injection*

**Description:**

A function $f : X \to Y$ is injective iff:

$$f(x) = f(x') \quad \Rightarrow \quad x = x'.$$

In other words $\forall x \in X, \exists$ different $y \in Y$ such that $x$ map to $y$ by $f$, so we can conclude that if there's an injection maps $X$ to $Y$, then $|X| \leq |Y|$.

### Definition 14 *Surjection*

**Description:**

A function $f : X \to Y$ is surjective iff:

$$\forall y \in Y, \exists x \in X \text{ such that } f(x) = y,$$

which also gives us that if there's a surjection maps $X$ to $Y$, then $|X| \geq |Y|$.

### Definition 15 *Bijection*

**Description:**

A function $f : X \to Y$ is bijective iff it is both injective and surjective, so if there exists a bijection maps $X$ to $Y$ or the oher way round, then $|X| = |Y|$.

### Definition 16 *Involution*

**Description:**

A function $f : X \to X$ is an involuon iff

$$f(f(x)) = x, \quad \forall x \in X.$$

### Lemma 22

**Statement:**

$f$ is an involution $\Rightarrow$ $f$ is bijective.

**Proof:** omitted. ■

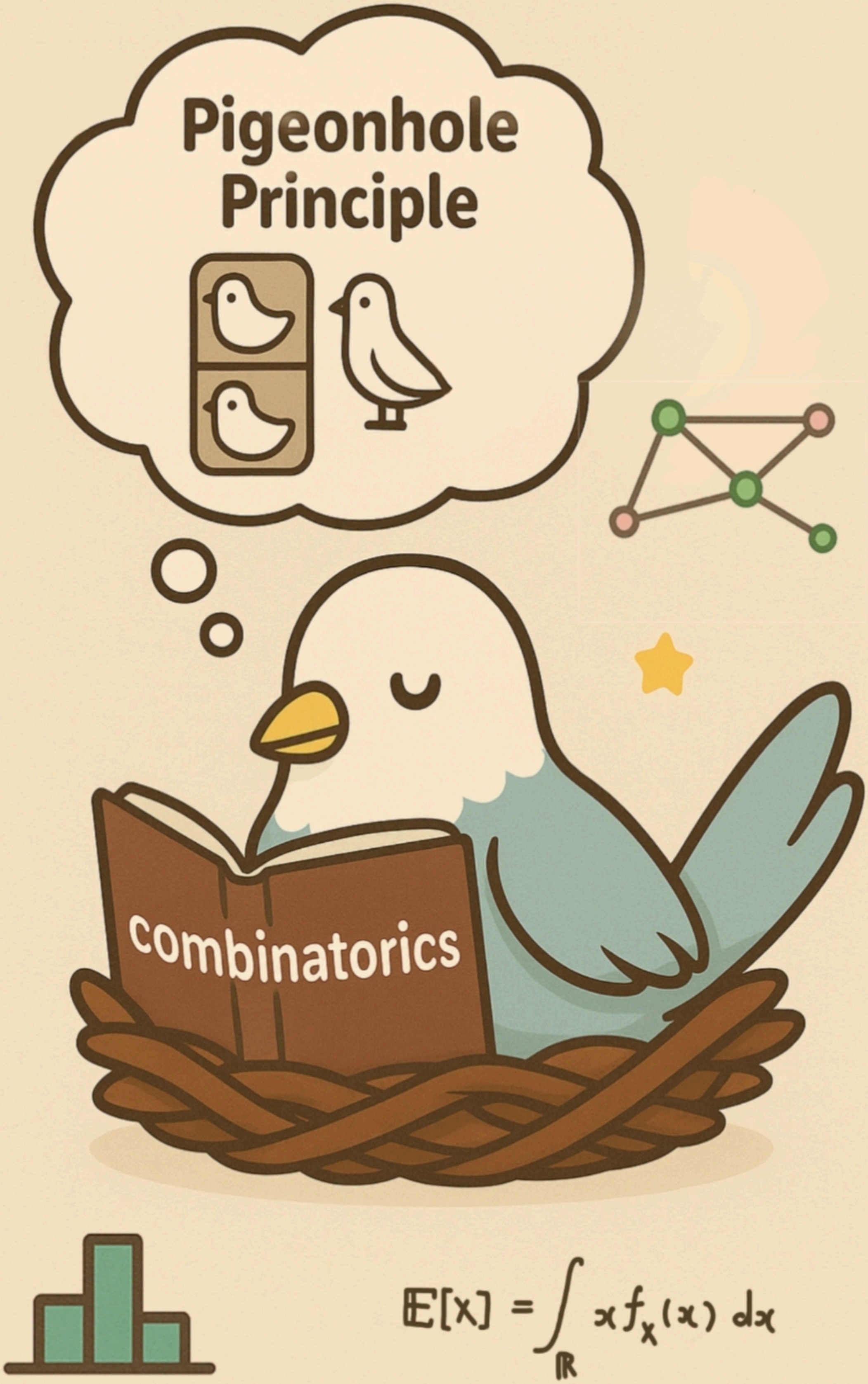
## Definition 17 *Concave and convex function*

**Description:**

$f : \mathrm{dom}(f) \to \mathbb{R}$ is called a **concave function** if $\forall x, y \in \mathrm{dom}(f)$ and $\forall \lambda \in [0, 1]$, the inequality

$$f(\lambda x + (1 - \lambda)y) \geq \lambda f(x) + (1 - \lambda)f(y)$$

always holds. (for convex, change the inequality sign to $\leq$)


Pigeonhole Principle
combinatorics
$\mathbb{E}[X] = \int_{\mathbb{R}} x f_X(x)\, dx$

# Chapter 2

# Combinatorics

## 2.1 Combinatorial Identity

### Definition 18 *Gaussian Binomial Coefficient*

**Description:**

$n, k, q \in \mathbb{Z}_{\geq 0}$, $q > 1$, we defined **Gaussian Binomial Coefficient** as:

$$\binom{n}{k}_q = \frac{(q^n - 1)(q^{n-1} - 1)\cdots(q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)\cdots(q - 1),}$$

for $k \leq n$, and it's equal to 0 when $k > n$.

### Theorem 56 *Pascal's Identity*

**Statement:**

*Form 1:*
For $k, n \in \mathbb{Z}_{>0}$,

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

*Form 2:* (Gaussian Binomial Coefficient's version)
For $n, k, q \in \mathbb{Z}_{>0},\ q > 1$,

$$\binom{n}{k}_q = q^k \binom{n-1}{k}_q + \binom{n-1}{k-1}_q.$$

**Proof:**
Proof of *Form 1*
The case $k \geq n$ is trivial. Consider $k < n$, then

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} = (n-1)! \cdot \frac{n}{k!(n-k)!} = \binom{n}{k}.$$

□

Proof of *Form 2*

Again assume $k < n$, let $q^k - 1 = x_k$, then the equation we want to prove is equivalent to

$$\frac{\prod_{i=n-k+1}^{n} x_i}{\prod_{i=1}^{k} x_i} = q^k \frac{\prod_{i=n-k}^{n-1} x_i}{\prod_{i=1}^{k} x_i} + \frac{\prod_{i=n-1}^{n-k+1} x_i}{\prod_{i=1}^{k-1} x_i} \Leftrightarrow x_n = q^k x_{n-k} + x_k.$$

which is true. ■

## Theorem 57 *Root of Unity Filter*

**Description:**

The technique **root of unity filter** allow us to extract numbers that divisible by $n$ using $n^{th}$ roots of unity

$$\mathbb{I}(k \mid n) = \frac{1}{k} \sum_{t=0}^{k-1} \zeta_k^{tn}.$$

We can also express in polynomial form

$$\frac{1}{k} \sum_{t=0}^{k-1} P(\zeta_k^t) = \sum_{k|t \leq n} a_t,$$

where $a_i, 1 \leq i \leq n$ are coefficient of $P$.

## 2.2 Extremal Combinatorics

### Theorem 58 *Pigeonhole Principle*

**Statement:**

If $m$ objects are put into $n$ boxes, then $\exists$ one box contains $\geq \left\lfloor \dfrac{m-1}{n} \right\rfloor + 1$ object, and one box contains $\leq \left\lfloor \dfrac{m}{n} \right\rfloor$ object.

**Proof:** Suppose in contrary, if all boxes contain $\leq \left\lfloor \dfrac{m-1}{n} \right\rfloor$ objects, then total object $\leq n \left\lfloor \dfrac{m-1}{n} \right\rfloor < m$, contradiction. Similarly we can prove the other case. ∎

### Theorem 59 *Well-Ordering Principle*

**Statement:**

For $S \subseteq \mathbb{Z}_{\geq 0}$ and $S \neq \varnothing$, then there exists $m \in S$ such that

$$m \ \leq \ s \quad \forall s \in S.$$

**Proof:**
Assume, for contradiction, that there is a non-empty $S \subseteq \mathbb{Z}_{\geq 0}$ with no least element. Choose any $s_1 \in S$. Since $s_1$ is not minimal, there must exist $s_2 \in S$ with $s_2 < s_1$. Continuing in this way produces an infinite strictly decreasing sequence

$$s_1 > s_2 > s_3 > \cdots$$

of natural numbers, which is impossible since the smallest element in $\mathbb{Z}_{\geq 0}$ is 0. Hence $S$ must have a least element. ∎

## 2.3 Probability

### Definition 19 *Expected Value*

**Description:**

The **expected value** of a discrete random variable $X$ is define as

$$\mathbb{E}[X] := \sum_x x \cdot \mathbb{P}(X = x),$$

while for continuous random variable,

$$\mathbb{E}[X] := \int_{\mathbb{R}} x f_X(x) \, \mathrm{d}x,$$

where $f_X$ is the probability density function.

Following is the list of the expected value of some distribution: the value for $\mathbb{E}[X]$ of
**Binomial Distribution** $X \sim \mathrm{B}(n, p)$ is $np$,
**Bernuolli Distribution** $X \sim \mathrm{Bern}(p)$ is $p$,
**Geometric Distribution** $X \sim \mathrm{Geo}(p)$ is $\frac{1}{p}$,
**Normal Distribution** $X \sim \mathrm{N}(\mu, \sigma^2)$ is $\mu$,
**Standard Normal Distribution** $X \sim \mathrm{N}(0, 1)$ is 0.
**Poisson Distribution** $X \sim \mathrm{Po}(\lambda)$ is $\lambda$.
**Exponential Distribution** $X \sim \exp(\lambda)$ is $\frac{1}{\lambda}$.

### Theorem 60 *Linearity of Expectation*

**Statement:**

For random variables $X_1, X_2, \cdots, X_n$, we have

$$\mathbb{E}\left[\sum_{i=1}^{n} X_i\right] = \sum_{i=1}^{n} \mathbb{E}[X_i].$$

**Proof:** We prove the case $n = 2$; the general case follows by induction. All summations below are over the ranges of the corresponding variables.

$$\mathbb{E}[X+Y] = \sum_i \sum_j (\, i + j \,)\, \mathbb{P}\big((X = i) \cap (Y = j)\big)$$

$$= \sum_i \sum_j i\, \mathbb{P}\big((X = i) \cap (Y = j)\big) \; + \; \sum_i \sum_j j\, \mathbb{P}\big((X = i) \cap (Y = j)\big)$$

$$= \sum_i i \sum_j \mathbb{P}\big((X = i) \cap (Y = j)\big) \; + \; \sum_j j \sum_i \mathbb{P}\big((X = i) \cap (Y = j)\big)$$

$$= \sum_i i\, \mathbb{P}(X = i) \; + \; \sum_j j\, \mathbb{P}(Y = j) \; = \; \mathbb{E}[X] + \mathbb{E}[Y].$$

■

### Definition 20 *Indicator variable*

**Description:**

An **Indicator variable** is a random variable that takes only 0 or 1 as value to indicate whether a subject satisfy given condition or not, let $X_i$ be the indicator variable of $x_i \in S$, then

$$X_i = \begin{cases} 1, & x_i \in S, \\ 0, & \text{otherwise,} \end{cases}$$

we also have a useful result which is

$$\mathbb{E}[X_i] = \mathbb{P}(x_i \in S),$$

and hence we can deduce that

$$\mathbb{E}[\#\ x_i \in S] = \sum_{i=1}^{n} \mathbb{P}(x_i \in S).$$

### Theorem 61 *Union Bound*

**Statement:**

For events $A_1, A_2, \cdots, A_n$, if

$$\sum_{i=1}^{n} \mathbb{P}(A_i) < 1$$

then there $\exists$ a non-zero event such that none of $A_i$ occur.

**Proof:** If $\nexists$ such event, then $A_i$ should cover up all the possibility that might occur which mean

$$\sum_{i=1}^{n} \mathbb{P}(A_i) \geq, 1$$

contradiction. ■

### Theorem 62 *Boole's Inequality*

**Statement:**

For events $A_1, A_2, \cdots, A_n$,

$$\mathbb{P}\left( \bigcup_{i=1}^{n} A_i \right) \leq \sum_{i=1}^{n} \mathbb{P}(A_i).$$

**Proof:** Apply induction on $n$: The case $n = 1$ is trivial, suppose it is true for $n$, then for $n + 1$, by **Inclusive-exclusive Principle**,

$$\mathbb{P}\left( \bigcup_{i=1}^{n+1} A_i \right) = \mathbb{P}\left( \bigcup_{i=1}^{n} A_i \right) + \mathbb{P}(A_{n+1}) - \mathbb{P}\left( A_{n+1} \cap \bigcup_{i=1}^{n} A_i \right) \leq \mathbb{P}\left( \bigcup_{i=1}^{n} A_i \right) + \mathbb{P}(A_{n+1}) \leq \sum_{i=1}^{n+1} \mathbb{P}(A_i).$$

■

## Theorem 63 *Bonferroni's Inequality*

**Statement:**

For events $A_1, A_2, \cdots, A_n$,

$$\mathbb{P}\bigg(\bigcap_{i=1}^{n} A_i\bigg) \geq 1 - \sum_{i=1}^{n} \mathbb{P}(A_i').$$

**Proof:** Similarly apply induction, again we have a trivial base case and suppose $n$ is true, then for $n+1$, we have

$$\mathbb{P}\bigg(\bigcap_{i=1}^{n+1} A_i\bigg) = \mathbb{P}\bigg(\bigcap_{i=1}^{n} A_i \cap A_{n+1}\bigg) = \mathbb{P}\bigg(\bigcap_{i=1}^{n} A_i\bigg) + \mathbb{P}(A_{n+1}) - \mathbb{P}\bigg(\bigcap_{i=1}^{n} A_i \cup A_{n+1}\bigg).$$

Now remains to prove that

$$\mathbb{P}(A_{n+1}) - \mathbb{P}\bigg(\bigcap_{i=1}^{n} A_i \cup A_{n+1}\bigg) \geq -\mathbb{P}(A_{n+1}'),$$

which is equivalent to

$$\mathbb{P}\bigg(\bigcap_{i=1}^{n} A_i \cup A_{n+1}\bigg) - \mathbb{P}(A_{n+1}) \leq \mathbb{P}(A_{n+1}') = 1 - \mathbb{P}(A_{n+1})$$

and is obviously true. ■

## Theorem 64 *Lovász Local Lemma*

**Statement:**

For events $A_1, A_2, \cdots, A_n$ such that they are independent to each other except at most $d$ of them, consider $p = \max\{\mathbb{P}(A_i)\}$, then if

$$epd \leq 1$$

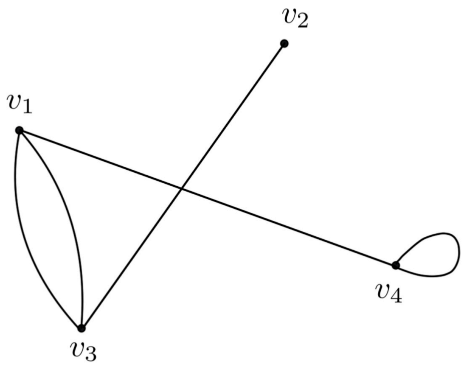
then there $\exists$ a non-zero event such that none of $A_i$ occur.

## 2.4 Graph Theory

### Definition 21 *Graph*

**Description:**

A **graph** is an ordered pair $G = (V, E)$ of multiset $E$ with elements takes in $V^2$, where $V = V(G)$ is called the **vertex set** of $G$ while $E = E(G)$ is called the **edge set** of $G$. We can simply write edge $\{u, v\}$ as $uv$.
A graph is called a **empty graph** if $V = E = \varnothing$.



$$V = \{v_1, v_2, v_3, v_4\}$$

$$E = \{v_1v_3, v_1v_3, v_1v_4, v_2v_3, v_4v_4\}$$

### Definition 22 *Simple Graph*

**Description:**

A **simple graph** is a graph $G = (V, E)$ such that it has no **loop** (edge with same end like $v_4v_4$) or **multiple edges** (two or more identical edges appear in a graph like $v_1v_3$) i.e

$$E \subseteq \{uv \mid u, v \in V, u \neq v\}.$$

otherwise it is called a **multigraph**.

### Definition 23 *Order of Graph*

**Description:**

The **order of graph** is the number of vertices of the graph, denoted as

$$|G| := |V(G)|.$$

A graph with $|G| \in \{0, 1\}$ is called **trivial graph**.

### Definition 24 *Length of Graph*

**Description:**

The **length of graph** is is the number of edges of the graph, denoted as

$$||G|| := |E(G)|.$$

A graph with $||G|| = 0$ is called a **null graph**.

## Definition 25 *Incident*

**Description:**

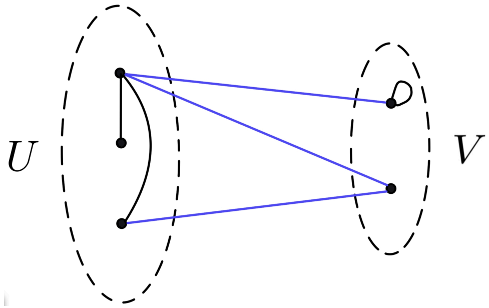
A vertex $v \in V$ is said to be **incident** with an edge $e \in E$ if $v \in e$. In that case $v$ is also called an **end** of $e$.

## Definition 26 *U-V edge*

**Description:**

If $U \sqcup V$ is a partition of the vertex set and $u \in U,\ v \in V$, then $uv$ is called a $U$–$V$ edge and the collection of all such edges is denoted

$$E(U, V) := \{\, uv \in E \mid u \in U,\ v \in V \}.$$



## Definition 27 *Adjacent*

**Description:**

Two distinct vertices $u, v \in V$ are **adjacent** if $u, v \in E$, in which case we write $u \sim v$; while Two edges $e, f \in E$ are **adjacent** if $e \neq f$ and $e \cap f \neq \varnothing$, i.e. they have a common end.

## Definition 28 *Neighborhood*

**Description:**

The **neighborhood** of a vertex $v$ is the set of vertices that incident to $v$, denoted as

$$N(v) := \{\, u \in V \mid u \sim v\}.$$

while the set of edges incident to $v$ is also defined

$$E(v) = \{\, e \in E \mid v \in e\},$$

## **Definition 29** *Complete Graph*

**Description:**

A graph $G = (V, E)$ is **complete** if every pair of distinct vertices is adjacent. The complete graph on $n$ vertices is denoted $K_n$.

## **Definition 30** *Graph Isomorphism*

**Description:**

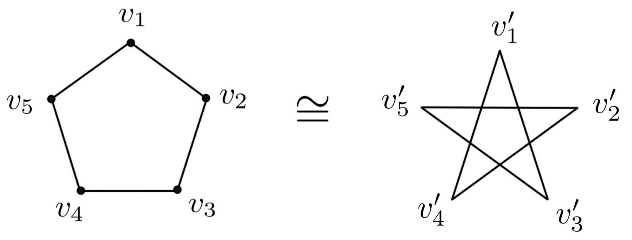
Let $G = (V, E)$ and $G' = (V', E')$ be two graphs. They are **isomorphic**, written $G \cong G'$, if there exists a bijection

$$\varphi : V \longrightarrow V'$$

such that for all $u, v \in V$,

$$\{u, v\} \in E \iff \{\varphi(u), \varphi(v)\} \in E'.$$

Such a map $\varphi$ is called an **isomorphism**.



$$v_1 \overset{\varphi}{\mapsto} v_1', \quad v_2 \overset{\varphi}{\mapsto} v_3', \quad v_3 \overset{\varphi}{\mapsto} v_5', \quad v_4 \overset{\varphi}{\mapsto} v_2', \quad v_5 \overset{\varphi}{\mapsto} v_4'$$

## **Definition 31** *Graph Invariant*

**Description:**

A **graph invariant** is any function $\alpha$ defined on all graphs such that

$$G \cong G' \implies \alpha(G) = \alpha(G').$$

### Definition 32 *Subgraph and Supergraph*

**Description:**

Let $G = (V, E)$ and $G' = (V', E')$ be graphs. If $V' \subseteq V$ and $E' \subseteq E$, then $G'$ is a **subgraph** of $G$ and $G$ is a **supergraph** of $G'$, denoted $G' \subseteq G$.

### Definition 33 *Induced Subgraph*

**Description:**

If $G' = (V', E') \subseteq G = (V, E)$ and

$$E' = \{uv \in E \mid u, v \in V'\},$$

then $G'$ is the **induced subgraph** of $G$ on $V'$, denoted

$$G' = G[V'].$$

### Definition 34 *Spanning Subgraph*

**Description:**

A subgraph $G' = (V', E')$ of $G = (V, E)$ is **spanning** if $V' = V$.

### Definition 35 *Complement Graph*

**Description:**

The **complement** $\overline{G}$ of a simple graph $G = (V, E)$ is the graph on the same vertex-set $V$ whose edge-set is

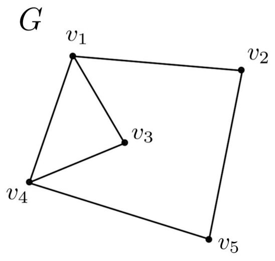
$$E(\overline{G}) = V^2 \setminus E.$$

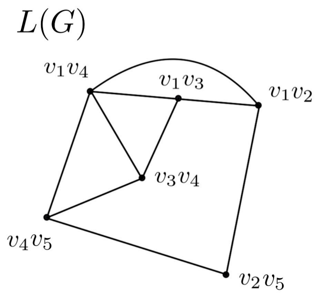
If $G \cong \overline{G}$, $G$ is called **self-complementary**.

### Definition 36 *Line Graph*

**Description:**

The **line graph** $G = (V, E)$, denoted as $L(G)$ has vertex set $E(G)$, and two vertices $e, f \in E(G)$ are adjacent in $L(G)$ whenever $e \sim f$ in $G$.





## Lemma 23

**Statement:**

Let $K_n$ be the complete graph whose edges are coloured with $k$ colours. Suppose every triangle in $K_n$ is either monochromatic or rainbow (all three edges different). Then

$$n \leq k(k-1)+2.$$

**Proof:** Let $|G| = n$, and let the number of colours be $k$. If edged of all triangle either all same or all different colour, WLOG let $v$ incident to $\geq 2$ different colour edges and among $E(v)$, colour $c$ appear the most. Let $vv_1, ..., vv_N$ be colour $c$, $v'$ be colour $d$, then $v_1, ..., v_N$ pairwise connected edges with colour $c$; colour of all $v'v_1, ..., v'v_N$ pairwise different and also not $c$ or $d$, then $k \geq N+2$, also since colour $c$ appear the most, $N \geq \dfrac{\deg v}{k} = \dfrac{n-1}{k} \quad \Rightarrow n \leq (k-1)^2$. ■

.

## Definition 37 *Degree of Vertex*

**Description:**

The **degree** of a vertex $v \in V$ is the number of edges incident with $v$, denoted

$$\deg(v) := |E(v)|.$$

A vertex $v \in V$ with $\deg(v) = 0$ is called an **isolated vertex**.
A vertex $v \in V$ with $\deg(v) = 1$ is called a **leaf**.
A vertex $v \in V$ is called an **even vertex** if $\deg(v)$ is even, and an **odd vertex** if $\deg(v)$ is odd.
The **minimum degree** of $G$ is denoted as

$$\delta(G) = \min_{v \in V} \deg(v),$$

and the **maximum degree** of $G$ is denoted as

$$\Delta(G) = \max_{v \in V} \deg(v).$$

The **average degree** of $G$ is denoted as

$$d(G) = \frac{1}{|V|} \sum_{v \in V} \deg(v).$$

## **Theorem 65** *Erdős–Gallai Theorem*

**Statement:**

A nonincreasing sequence of nonnegative integers $d = (d_1, \ldots, d_n)$ is the degree sequence of some simple graph if and only if $\sum_{i=1}^{n} d_i$ is even and for every $1 \le k \le n$

$$\sum_{i=1}^{k} d_i \;\le\; k(k-1) \;+\; \sum_{i=k+1}^{n} \min\{d_i, k\}.$$

**Proof:** (*by S.A. Choudum*)

## **Definition 38** *k-Regular Graph*

**Description:**

A graph $G = (V, E)$ is called $k$**-regular** if $\deg(v) = k$ for every $v \in V$.

## **Theorem 66** *Friendship Theorem*

**Statement:**

Let $G$ be a finite simple graph such that any two vertices have exactly one common neighbor. Then there exists a vertex adjacent to all other vertices.

**Proof:**
Suppose, for sake of contradiction, that no vertex is adjacent to every other.
We prove $G$ is $k$-regular. Pick two non-adjacent vertices $A$ and $B$. Let

$$N(A) = \{a_1, \ldots, a_k\}, \quad N(B) = \{b_1, \ldots, b_\ell\},$$

so $\deg(A) = k$, $\deg(B) = \ell$. For each $a_i$, its unique common neighbor with $B$ cannot be $A$, so must be some $b_j$. If two distinct $a_i, a_{i'}$ shared the same $b_j$, then $A$ and $b_j$ would have two common neighbors, impossible. Hence $k \le \ell$. By symmetry $\ell \le k$, so $k = \ell$. Thus $\deg(v) = k$ for all $v \in G$.

Count ordered triples $(A; B, C)$ where $A \sim B, C$, and $B \sim C$. First way: choose $A$ in $n$ ways and then two of its $k$ neighbors, giving $n\binom{k}{2}$. Second way: choose an edge $\{B, C\}$ in $\binom{n}{2}$ ways, then its common neighbor $A$.
Equating gives

$$n\binom{k}{2} \;=\; \binom{n}{2},$$

whence $n = k^2 - k + 1$.
Let $A = (a_{ij})$ be the adjacency matrix of $G$. The condition "each pair has exactly one common neighbor" reads

$$A^2 = \begin{bmatrix} k & 1 & \cdots & 1 \\ 1 & k & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & k \end{bmatrix}.$$

Thus

$$\det(\lambda I - A^2) = (\lambda - (k + n - 1))\;(\lambda - (k-1))^{n-1}.$$

Hence $A^2$ has eigenvalues $k+n-1=k^2$ (simple) and $k-1$ (multiplicity $n-1$). It follows that the eigenvalues of $A$ are $\pm k$ (simple) ,$\sqrt{k-1}$ (multiplicity $a$) and $-\sqrt{k-1}$ (multiplicity $b$), where $a+b=n-1$. So $\operatorname{tr}(A)=0$, the sum of all eigenvalues vanishes:

$$\pm k+(a-b)\sqrt{k-1}=0,$$

gives $k-1 \mid k^2$, force $k=2$, $n=3$. Therefor $G \cong K_3$, contradiction. ■

## Theorem 67 *Euler's Handshaking Lemma*

**Statement:**

For $G=(V,E)$,

$$\sum_{v\in V} \deg v = 2|E|.$$

**Proof**: We count every edges exactly twice when we sum up all the degree of vertex since once from each of its ends. ■

## Lemma 24

**Statement:**

For any graph $G$,

$$\delta(G) \ \leq \ d(G) \ \leq \ \Delta(G).$$

**Proof:**
By **Pigeonhole Principle.** ■

## Lemma 25

**Statement:**

In any graph $G$, the number of vertices of odd degree is even.

**Proof:**
By **Euler' s Handshaking Lemma**, $\sum_{v\in V} \deg(v) = 2|E|$ is even. Split the sum into contributions from even-degree and odd-degree vertices:

$$\sum_{\substack{v\in V\\ 2|\deg(v)}} \deg(v) \ + \ \sum_{\substack{v\in V\\ 2\nmid\deg(v)}} \deg(v)$$

is even. The first sum is even, so the second sum being even and hence must be a sum of an even number of odd terms. Hence there are an even number of odd vertices. ■

## Lemma 26

**Statement:**

For the complete graph $K_n$ on $n$ vertices,

$$||K_n|| = \binom{n}{2} = \frac{n(n-1)}{2}.$$

**Proof:**
Every edge of $K_n$ corresponds uniquely to an unordered pair of distinct vertices. There are $\binom{n}{2}$ such pairs, hence $||K_n|| = \binom{n}{2} = \dfrac{n(n-1)}{2}$. ■

## Definition 39 *Path and Cycle*

**Description:**

A **path** $P = v_0v_1 \cdots v_k$ is a simple graph with

$$V(P) = \{v_0, v_1, \dots, v_k\}, \qquad E(P) = \big\{v_{i-1}v_i \mid 1 \le i \le k\big\},$$

where the vertices $v_0, \dots, v_k$ are pairwise distinct. The path of length $k$ is denoted as $P_k$.
If $v_0 = v_k$, then $P$ is called a **cycle**. Equivalently, a cycle of length $k$ is denoted $C_k$.

A **subpath** of $P$ is any path of the form

$$v_iv_{i+1} \cdots v_j, \quad 0 \le i \le j \le k.$$

In particular, we write
(1) $Pv_i = v_0 \cdots v_i$,
(2) $v_iP = v_i \cdots v_k$,
(3) $v_iPv_j = v_i \cdots v_j$,
(4) $v_1Pv_2P'v_3 = v_1Pv_2 \cup v_2P'v_3$.

## Definition 40 *Girth and Circumference of Graph*

**Description:**

The **girth** of $G$, denoted $g(G)$, is the minimum length of cycle in $G$ while the **circumference** of $G$ is the maximum length of cycle in $G$.

## Definition 41 *Walk*

**Description:**

A **walk** in $G$ is a sequence

$$v_0e_1v_1e_2 \dots e_kv_k$$

of vertices and edges such that each $e_i = \{v_{i-1}, v_i\}$. Vertices and edges may repeat.

### **Definition 42** *Trail and Circuit*

**Description:**

A **trail** $e_1e_2\cdots e_k$ is a walk with pairwise distinct $e_i,\ 1 \leq i \leq k$. If $e_1 = e_k$, it is called a **circuit**.

### **Definition 43** *Chord of Cycle*

**Description:**

A **chord** of a cycle $C$ is an edge $e \notin E(C)$ joining two vertices of $C$.

### **Definition 44** *Distance Between Vertices*

**Description:**

The **distance** between two vertices $u, v$, denoted $d(u, v)$, is the length of a shortest $u{-}v$ path in $G$.

### **Definition 45** *Eccentricity, Diameter and Radius*

**Description:**

The **eccentricity** of a vertex $v$, denoted $\varepsilon(v)$, is

$$\varepsilon(v) = \max_{w\in V} d(v, w).$$

Moreover, The **diameter** of $G$ is

$$\mathrm{diam}(G) = \max_{v\in V} \varepsilon(v).$$

and the **radius** of $G$ is

$$\mathrm{rad}(G) = \min_{v\in V} \varepsilon(v).$$

### **Definition 46** *Center of Graph*

**Description:**

The **center** of $G$ is the set of vertices realizing the radius:

$$C(G) = \big\{v \in V \mid \varepsilon(v) = \mathrm{rad}(G)\big\}.$$

### **Lemma 27**

**Statement:**

Every graph $G$ contains

- a path of length $\delta(G)$, and
- if $\delta(G) \geq 2$, a cycle of length at least $\delta(G)+1$.

**Proof:**
Let $P = v_0 v_1 \cdots v_k$ be a longest path in $G$. Then every neighbor of $v_k$ lies on $P$, so

$$k \;\geq\; \deg(v_k) \;\geq\; \delta(G).$$

Thus $P$ has length $\geq \delta(G)$. If $\delta(G) \geq 2$, pick the smallest index $i < k$ with $v_i \sim v_k$. Then

$$i \;\leq\; k - \deg(v_k) \;\leq\; k - \delta(G),$$

and the cycle

$$v_i v_{i+1} \cdots v_k v_i$$

has length

$$k - i + 1 \;\geq\; k - (k - \delta(G)) + 1 = \delta(G) + 1.$$

■

## Lemma 28

**Statement:**

$$g(G) \;\leq\; 2\,\mathrm{diam}(G) + 1.$$

**Proof:**
Let $C \subseteq G$ be a shortest cycle, and pick two vertices $u, v \in C$ such that$d_C(u,v) \geq \mathrm{diam}(G)+1$, but then obviously

$$d_G(u,v) < \mathrm{diam}(G) + 1 \leq d_C(u,v),$$

so replace the shortest $u - v$ path in $C$ to the shortest $u - v$ path in $G$ we get a cycle shorter then $C$, contradiction ■

## Lemma 29

**Statement:**

Let $G$ be a graph with radius $\mathrm{rad}(G) \leq k$ and maximum degree $\Delta(G) \leq d$. Then

$$|G| \leq \; 1 + kd^k.$$

**Proof:**
Choose a central vertex $c$, let

$$D_i = \{\, v \in V(G) \mid d(c,v) = i\}$$

so $V(G) = \displaystyle\bigcup_{i=0}^{k} D_i$ and $D_0 = \{c\}$. Since $\Delta(G) \leq d$, we have

$$|D_0| = 1, \quad |D_1| \leq d, \quad |D_i| \leq (d-1)D_{i-1} \; (\forall\, i \geq 2),$$

hence $|D_i| \leq d(d-1)^i$, $\forall\, 0 \leq i \leq k$.
Then

$$|G| = \left|\bigcup_{i=0}^{k} D_i\right| \leq \sum_{i=0}^{k} |D_i| \leq 1 + d\sum_{i=0}^{k-1}(d-1)^i \leq 1 + kd(d-1)^{k-1} \leq 1 + kd^k.$$

■

## Definition 47 *H-Path*

**Description:**

Let $H \subseteq G$ be a subgraph. A path $P \subseteq G$ is called an $H$**-path** if $P$ meet $H$ exactly in its ends and no internal vertex of $P$ lies in $H$.

## Definition 48 *Tree and Forest*

**Description:**

A graph with no cycle is called a **tree**. A **forest** is a graph whose every connected component is a tree (equivalently, a disjoint union of trees).

## Lemma 30

**Statement:**

If $T$ is a tree with at least two vertices, then $T$ has at least two leaves.

**Proof:**
Let $P = v_0 v_1 \cdots v_k$ be a longest path in $T$. Since $T$ has no cycle, neither $v_0$ nor $v_k$ can have degree exceeding 1 (otherwise $P$ could be extended), so $\deg(v_0) = \deg(v_k) = 1$. Thus there are at least two leaves. ■

## Lemma 31

**Statement:**

Let $T$ be a graph on $n$ vertices. The following five statements are equivalent:

1. $T$ is a tree.
2. For every pair $u, v \in T$ there is a unique $u{-}v$ path in $T$.
3. $T$ is connected but $T \setminus e$ is disconnected for all $e \in T$.
4. $T$ has no cycle and $||T|| = n - 1$.
5. $T$ is connected and $||T|| = n - 1$.

**Proof:**
We sketch the standard cycle of implications:
(1) ⇒ (2): If $T$ is a tree then it is connected and contains no cycle. Existence of at least one $u - v$ path follows from connectedness; uniqueness holds because two distinct $u - v$ paths would form a cycle.
(2) ⇒ (3): If there were an edge $e$ whose deletion did not disconnect $T$, then the two ends of $e$ would still be joined by a path not using $e$, contradicting uniqueness.
(3) ⇒ (4): If $T$ is connected and every edge is a bridge, then removing any edge reduces the number of connected components by one. Starting from $T$ and removing edges one by one until no edges remain, one sees there must have been exactly $n-1$ edges to achieve $n$ isolated vertices. Absence of any cycle also follows since a cycle edge cannot be a bridge.
(4) ⇒ (5): Trivial, since (4) already asserts no cycle and $|E| = n-1$, which in particular implies $T$ is connected (a disconnected acyclic graph on $n$ vertices with $n-1$ edges would have too many edges in some component).
(5) ⇒ (1): A connected graph with $n$ vertices and $n-1$ edges cannot contain a cycle (removing an edge from a cycle would still leave the graph connected, contradicting the edge–count). ■

## Definition 49 *Connected Graph*

**Description:**

An undirected graph $G$ is **connected** if for every pair of vertices $u, v \in V(G)$ there exists a walk from $u$ to $v$.
A **connected component** of an undirected graph $G$ is a connected subgraph that is not part of any larger connected subgraph.

## Definition 50 *Clique*

**Description:**

A **clique** in a graph $G = (V, E)$ is a vertex set $C \subseteq V$ such that every two distinct vertices in $C$ are adjacent (i.e. induce a complete subgraph). The **clique number** of $G$, denoted $\omega(G)$, is the cardinality of a largest clique in $G$.

## Theorem 68 *Caro–Wei Theorem*

**Statement:**

For any graph $G$,

$$\alpha(G) \;\geq\; \sum_{v \in G} \frac{1}{1+\deg(v)}.$$

**Proof:**
Assigned an order to all $v \in G$ randomly and uniformly, consider
$I = \{v \in G \mid v \text{ appears before all } u \in N(v)\}$, then $I$ is an independent set. Note that for any $v \in G$,

$$\mathbb{P}(v \in I) = \frac{1}{1+\deg v},$$

let $X_i = \mathbb{I}(v_i \in I)$, then

$$\mathbb{E}[|I|] = \sum_i \mathbb{P}(X_i) = \sum_{v \in G} \frac{1}{1 + \deg v}.$$

■

## Definition 51 *Independent Set*

**Description:**

An **independent set** in $G = (V, E)$ is a vertex set $I \subseteq V$ such that no two distinct vertices in $I$ are adjacent. The **independence number** of $G$, denoted $\alpha(G)$, is the cardinality of a largest independent set in $G$.

## Lemma 32

**Statement:**

For any graph $G$ on $n$ vertices,

$$\omega(G) \ \geq \ \sum_{v \in G} \frac{1}{n - \deg(v)}.$$

**Proof:**
Apply the Caro–Wei to the complement $\overline{G}$:

$$\alpha(\overline{G}) \geq \sum_{v \in G} \frac{1}{1 + \deg_{\overline{G}}(v)} = \sum_{v \in G} \frac{1}{n - \deg_G(v)}$$

. Since $\alpha(\overline{G}) = \omega(G)$, the result follows. ■

## Theorem 69 *Ramsey' s Theorem*

**Statement:**

Every graph $G$ on $|V(G)| \geq 6$ vertices satisfies

$$\max\{\omega(G),\, \alpha(G)\} \ \geq \ 3.$$

**Proof:**
Let $G$ be any graph on $n \geq 6$ vertices, and pick a vertex $v$. Since $v$ has $n - 1 \geq 5$ other vertices, by the pigeonhole principle either

$$|N(v)| \geq 3 \quad \text{or} \quad \bigl|V(G) \setminus \bigl(N(v) \cup \{v\}\bigr)\bigr| \geq 3.$$

– If $|N(v)| \geq 3$, let $x, y, z \in N(v)$. In the subgraph induced by $\{x, y, z\}$, either two are adjacent (giving a clique of size 3 together with $v$), or none are adjacent (giving an independent set of size 3).
– If $|V(G) \setminus (N(v) \cup \{v\})| \geq 3$, pick three vertices non-adjacent to $v$. In that set again either two are non-adjacent (yielding an independent set of size 3 together with $v$), or two are adjacent (yielding a clique of size 3).
In either case we find a clique or independent set of size at least 3, completing the proof. ■

## Definition 52 *Directed Graph*

**Description:**

A **directed graph** is a graph in which each edge is assigned an orientation, called a **directed edge**. If $e$ is a directed edge in a digraph, then $\text{init}(e)$ denotes its *initial* vertex and $\text{ter}(e)$ its *terminal* vertex and if $\text{init}(e) = u$ and $\text{ter}(e) = v$, we write $u \to v$.

## Definition 53 *In-Degree and Out-Degree*

**Description:**

The **in-degree** of a vertex $v$ in a digraph, denoted $\deg^{-}(v)$, is the number of edges directed *into* $v$, while the **out-degree** of a vertex $v$ in a digraph, denoted $\deg^{+}(v)$, is the number of edges directed *out of* $v$.

## Lemma 33

**Statement:**

In any directed graph,

$$\sum_{v\in V} \deg^{+}(v) \;=\; \sum_{v\in V} \deg^{-}(v) \;=\; |E|.$$

**Proof:**
Each directed edge contributes exactly 1 to the out-degree of its tail and exactly 1 to the in-degree of its head; summing over all vertices counts each edge once in each sum. ■

## Definition 54 *Tournament*

**Description:**

A **tournament** $\overline{K}_n$ is an orientation of the complete graph on $n$ vertices: for every pair of distinct vertices $u, v$, exactly one of the directed edges $u \to v$ or $v \to u$ is present.

## Lemma 34

**Statement:**

In every tournament $\overline{K}_n$ there exists a vertex $v$ from which every other vertex can be reached by a directed path of length at most 2.

**Proof:**
Let $v_1$ be the vertex has the greatest out-degree. Suppose there exists no such vertex, then $\exists\, v_2 \notin N^{+}(v_1)$ and for all $u \in N^{+}(v_1),\ v_2 \to u$ and $v_2 \to v_1$, thus $|N^{+}(v_2)| > |N^{+}(v_1)|$, contradiction.
■

## Lemma 35

**Statement:**

A tournament $\overline{K}_n$ contains a directed triangle if and only if there exist two vertices $u, w$ with $\deg^+(u) = \deg^+(w)$.

**Proof:**
*Sufficiency:* WLOG let $v \to w \to v_1, ..., v_k,\ k = \deg^+(w)$, then $\exists\ v_i \to v$ otherwise $\deg^+(v) \geq k+1 > \deg^+(w)$, contradiction

□

*Necessity:* If $\forall\ v, w,\ \deg^+(v) \neq \deg^+(w)$, we prove by induction. Base case is trivial, suppose the statement true for some $n$, consider $\overline{K}_{n+1}$, WLOG let $\deg^+(v_i) = i+1$, by inductive hypotesis, $\overline{K}_{n+1} \setminus v_{n+1}$ don't have a directed triangle, so $\overline{K}_{n+1}$ don't have either. ■

## Lemma 36

**Statement:**

Every tournament $\overline{K}_n$ has a Hamiltonian directed path of length $n-1$.

## Definition 55 *k-partite Graph*

**Description:**

A ***k*-partite graph** is a graph $G = \left(\bigsqcup_{i=1}^{k} V_i, E\right)$ such that no edge has both ends in the same $V_i$. In particular, a **bipartite graph** is a graph $G = (X \sqcup Y, E)$, which is a 2-partite graph.

## Definition 56 *Complete k-partite Graph*

**Description:**

The **complete *k*-partite graph**, denoted as $K_{n_1, n_2, ..., n_k}$, is defined as

$$K_n \setminus \{e \mid e \in E(V_i, V_i),\ i \in [k]\},$$

i.e. connect everything that can connect across parts.

## Definition 57 *Turán Graph*

**Description:**

The **Turán graph** $T(n, k)$ is defined as the complete $k$-partite graph $K_{n_1, n_2, ..., n_k}$, where $n_1 = n_2 = \cdots = n_r = m+1$, $n_{r+1} = \cdots = n_k = m$ for $n = mk + r$ with $0 \leq r < m$.

## Lemma 37

**Statement:**

Let $T(n,k)$ be the Turán graph, and set $m = \left\lfloor \frac{n}{k} \right\rfloor$. Then

$$\big|\big|T(n,k)\big)\big|\big| = \binom{n-m}{2} \;+\; (k-1)\binom{m+1}{2}.$$

In particular, for $k \leq 7$ one has the succinct expression $\big|\big|T(n,k)\big)\big|\big| \;=\; \left\lfloor \left(1 - \frac{1}{k}\right)\frac{n^2}{2} \right\rfloor$.

## Theorem 70 *Turán' s Theorem*

**Statement:**

Let $G$ be a graph on $n$ vertices and fix $k \geq 1$. If $G$ contains no $(k+1)$-clique, then

$$||G|| \;\leq\; \big|\big|T(n,k)\big|\big|,$$

with equality if and only if $G \cong T(n,k)$.

*weaker version:* Let $G$ be an $n$-vertex graph. If $||G|| > \big|\big|T(n,k)\big)\big| \;=\; \left\lfloor \left(1 - \frac{1}{k}\right)\frac{n^2}{2} \right\rfloor$, then $G$ contains a clique of size at least $k+1$.

## Theorem 71 *Mantel' s Theorem*

**Statement:**

If $G$ is an $n$-vertex graph with no triangle, then

$$||G|| \;\leq\; \left\lfloor \frac{n^2}{4} \right\rfloor.$$

**Proof:**
Immediate from Turán' s Theorem by setting $k = 2$. ■

## Lemma 38

**Statement:**

Let $G$ be an $n$-vertex graph with $e = ||G||$. Then the number of triangles in $G$ is at least

$$\frac{1}{3}\left(\frac{4e^2}{n} - e\,n\right).$$

**Proof:**

For each edge $uv$, there are $\deg(u) + \deg(v) - n$ common neighbors $w$ forming a triangle $uvw$. Summing over all $e$ edges counts each triangle three times, giving

$$3\,T \;\geq\; \sum_{uv \in E} \bigl(\deg(u) + \deg(v) - n\bigr) \;=\; \sum_{v} (\deg(v))^2 - en.$$

By Cauchy–Schwarz, $\sum_v (\deg(v))^2 \geq \frac{1}{n}\bigl(\sum_v \deg(v)\bigr)^2 = \frac{4e^2}{n}$, hence $T \geq \frac{1}{3}(4e^2/n - en)$. ■

## 2.5 Linear Algebra in Combinatorics

### Definition 58 *Adjacency Matrix*

**Description:**

Let $G = (V, E)$ be a simple graph with $|V| = n$ and fix an ordering $V = \{v_1, v_2, \ldots, v_n\}$. The **adjacency matrix** of $G$ is the $n \times n$ matrix

$$(a_{ij})_{1 \leq i,j \leq n}, \quad a_{ij} = \begin{cases} 1, & \text{if } v_i \sim v_j, \\ 0, & \text{otherwise.} \end{cases}$$

# Chapter 3

# Number Theory

***Remark:*** all alphabet in Number Theory is **integer** except where otherwise stated.

## 3.1 Divisibility

### Theorem 72 *Properties of Divisibility*

**Statement:**

The divisibility relation has the following properties:

*1.* (*reflexivity*) $n \mid n$. ($0 \mid 0$ is valid)

*2.* (*transitivity*) $a \mid b, \ \ b \mid c \ \ \Rightarrow \ \ a \mid c$.

*3.* $1 \mid n$ and $n \mid 0$ both true.

*4.* $a \mid b \ \ \Leftrightarrow \ \ |a| \bigm| |b|$

*5.* For $1 \leq i \leq n$ and any $c_i$, if $a \mid b_i$, then $a \Bigm| \sum_{i=1}^{n} c_i b_i$.

*6.* $a \mid n \Leftrightarrow \dfrac{n}{a} \Bigm| n$. (divisor appear in pairs except for perfect square)

**Proof:**
Properties *1*,*2*,*3* and *4* can directly obtain from definition. For property *5*, let $b_i = ak_i$ then

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

For property *6*, let $n = ka$ then $\dfrac{n}{a} = k \mid n$. ■

### Theorem 73 *Euclid's Division Lemma*

**Statement:**

For any $a, b,$, there $\exists !\ k, r$ such that $0 \leq r < b$ and

$$a = bk + r.$$

**Proof:**
*Uniqueness:*
Suppose that we have two presentations $a = bk + r = bk' + r'$, then $|b| > |r - r'| = |(k' - k)| \cdot |b| \geq |b|$ lead to a contradiction.

□

*Existence:*
Take $k = \lfloor \frac{a}{b} \rfloor$ then

$$0 = a - b \cdot \frac{a}{b} \leq a - b\Big\lfloor \frac{a}{b} \Big\rfloor = r < a - b\Big(\frac{a}{b} - 1\Big) = b$$

■

## Theorem 74 *Gauss' Divisibility Lemma*

**Statement:**

For coprime $a, b$,

$$a \mid bn \quad \Rightarrow \quad a \mid n.$$

**Proof:** In $\mathbb{Z}/a\mathbb{Z}$, $bn \equiv 0 \Rightarrow n \equiv b^{-1}bn \equiv 0$. ■

## Theorem 75 *Euclid's Lemma*

**Statement:**

For prime $p$,

$$p \mid ab \quad \Rightarrow \quad p \mid a \quad \text{or} \quad p \mid b.$$

**Proof:** by **Gauss' Lemma**. ■

## Lemma 39

**Statement:**

For any positive integer $k$, let $d$ be positive divisor of $k$, then:

*1.* $a - b \mid a^k - b^k$.

*2.* $a^d - b^d \mid a^k - b^k$.

*3.* If $2 \nmid k, \quad a + b \mid a^k + b^k$.

*4.* If $2 \nmid \frac{k}{d}, \quad a^d + b^d \mid a^k + b^k$.

**Proof:** It's obvious by the $x^n \pm y^n$ identities. ■

## Lemma 40

**Statement:**

For $m, n, a \in \mathbb{Z}_{>0}, a \geq 2$,
$$n \mid m \quad \Leftrightarrow \quad a^n - 1 \mid a^m - 1.$$

**Proof:** Let $m = kn + r$, $0 \leq r < n$, then

$$(a^m - 1) - (a^r - 1) = a^m - a^r = a^{kn} - 1 = (a^n - 1)\sum_{i=0}^{k-1} a^i b^{k-1-i},$$

which means $a^n - 1 \mid a^m - 1 \Leftrightarrow a^n - 1 \mid a^r - 1 \Leftrightarrow r = 0$ since $n > r$. ■

## Lemma 41

**Statement:**

If $a \mid b$, then either $b = 0$ or $|a| \leq |b|$.

**Proof:** Consider $b \neq 0$, $a \mid b \Rightarrow |a| \,\Big|\, |b|$, let $|b| = k|a|$, then $k \geq 1 \Rightarrow |b| = k|a| \geq |a|$. ■

## Lemma 42

**Statement:**

Let $f \in \mathbb{Z}[x]$, then
$$a - b \mid f(a) - f(b).$$

**Proof:** Let $f(x) = \sum_{i=1}^{m} c_i x^i$, then $a - b \,\Bigg|\, \sum_{i=1}^{m} c_i (a-b)^i = f(a) - f(b)$. ■

## Lemma 43

**Statement:**

Let $f \in \mathbb{Z}[x]$, then there exists infinitely many $b$ such that $f(a) \mid f(b)$.

**Proof:** Take $b = a + k|f(a)|$, then by ***lemma*** , $f(a) \mid k|f(a)| = b - a \mid f(b) - f(a)$ which means $f(a) \mid f(b)$ for $\forall k \in \mathbb{Z}$. ■

## Lemma 44

**Statement:**

Let $2 \nmid n \geq 1$, then
$$2^{n+2} \mid a^{2^n} - 1.$$

**Proof:** Observed that

$$a^{2^n} - 1 = (a-1)(a+1)\prod_{i=2}^{n-1}(a^{2^i}+1),$$

since $n$ is odd, then $(a-1)(a+1) = a^2 - 1 \equiv_8 0$, and we also have $a^{2^i+1}$ are even then we are done. ■

## 3.2 Congruence

### Theorem 76 *Properties of Congruence*

**Statement:**

In mod $n$, the congruence relation has the following properties:

*1.* (*reflexivity*) $a \equiv a$.

*2.* (*symmetry*) $a \equiv b \Leftrightarrow b \equiv a$.

*3.* (*transitivity*) If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.

*4.* If $a \equiv c$, $b \equiv d$, then $a \pm b \equiv c \pm d$ and $ac \equiv cd$.

*5.* If $a \equiv b$, then $ac \equiv bc \pmod{n}$ and $ac \equiv bc \pmod{nc}$ both true.

*6.* If $ac \equiv bc \pmod{n}$, then $a \equiv b \left(\bmod \dfrac{n}{\gcd(n,c)}\right)$

*7.* If $a \equiv b \pmod{n}$, and $d \mid n$ then $a \equiv b \pmod{d}$.

**Proof:** Properties *1,2* are obvious. For *3*, $n \mid a-b, b-c \Rightarrow n \mid a-b+b-c = a-c$. For Property *4*, the former is by definition and the latter is by **Property 5 of divisibility**. ■

### Theorem 77 *Euler's Theorem*

**Statement:**

For coprime $a, n$,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

**Proof:** Note that $a(\mathbb{Z}/n\mathbb{Z})^\times$ is a reduce residue class modulo $n$ . Hence

$$a^{|(\mathbb{Z}/n\mathbb{Z})^\times|} \prod_{s\in(\mathbb{Z}/n\mathbb{Z})^\times} s \equiv \prod_{s\in(\mathbb{Z}/n\mathbb{Z})^\times} s \pmod{n} \quad \Leftrightarrow \quad a^{\varphi(n)} \equiv 1 \pmod{n}.$$

■

### Lemma 45

**Statement:**

Let $f \in \mathbb{Z}[x]$, then

$$a \equiv b \pmod{n} \Leftrightarrow f(a) \equiv f(b) \pmod{n}.$$

**Proof:** Let $f(x) = \sum_{i=1}^{m} c_i x^i$, then $f(a) - f(b) = \sum_{i=1}^{m} c_i (a-b)^i \equiv 0 \pmod{a-b}$. ■

### **Theorem 78** *Fermat's Little Theorem*

**Statement:**

For prime $p \nmid a$,
$$a^{p-1} \equiv 1 \pmod{p}.$$

**Proof:** By **Euler' s Theorem**. ■

### **Theorem 79** *Wilson's Theorem*

**Statement:**

$p$ is prime if and only if
$$(p-1)! \equiv -1 \pmod{p}.$$

**Proof:**
*Necessity:*
The case $p = 2$ is trivial, now discuss odd prime $p$. Consider

$$\mathbb{F}_p \ni f(x) = x^{p-1} - 1 - \prod_{i=1}^{p-1}(x-i),$$

and we substitute any $a \in [p-1]$ and apply **Fermat's Little Theorem** give

$$f(a) = a^{p-1} - 1 \equiv 0 \pmod{p},$$

which means $f$ has $p-1$ roots but $\deg f \leq p-2$, by **Lagrange's Theorem** (see Chapter of Polynomial) $f(x) \equiv 0 \pmod{p}$ for $\forall x \mod p$ then substitute $x = 0 \mod p$ yields

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

□

*Sufficiency:*
Suppose $p$ is composite, let prime $q \mid p$ then

$$(p-1)! \equiv -1 \pmod{p} \Rightarrow -1 \equiv (p-1)! \equiv 0 \pmod{q}.$$

which is a contradiction. ■

### **Theorem 80** *Chinese Remainder Theorem*

**Statement:**

*Form 1:*
Let $m_1, m_2, ..., m_n$ be pairwise coprime integer, then for any $a_1, a_2, ..., a_n$, the system

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \qquad \vdots \\ x \equiv a_n \pmod{m_n}. \end{cases}$$

has exactly one solution which is

$$x \equiv \sum_{i=1}^{n} a_i M_i {M_i}^{-1} \pmod{M},$$

where $M = \prod_{i=1}^{n} m_i$ and $M_i = \frac{M}{m_i}$.

*Form 2:*
Let $m_1, m_2, ..., m_n$ be pairwise coprime integer and $M = \prod\limits_{i=1}^{n} m_i$, then the ring

$$\mathbb{Z}/M\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times ... \times (\mathbb{Z}/m_n\mathbb{Z}).$$

**Proof:**
Only need to prove *Form 1* because it implies *Form 2*.

*Uniqueness:*
Suppose there are two distinct solution for $x$, called them $k, t$ mod $M$, then $m_i \mid k - t$ for $\forall 1 \leq i \leq n$. Since $m_i$ pairwise coprime, then $M \mid k - t$ too, which is a contradiction.

□

*Existence:* Since $\gcd(M_i, m_i) = 1$, Then there exists $N_i = {M_i}^{-1}$ mod $m_i$, take

$$x \equiv \sum_{i=1}^{n} a_i M_i N_i \pmod{M},$$

then we have

$$x \equiv a_j M_j N_j \equiv a_j(1 - m_j n_j) = a_j \pmod{m_j}, \quad \text{for} \forall\ 1 \leq j \leq n$$

where the existence of such $n_j$ is by **Bézout's Lemma**. ■

## Theorem 81 *Freshman's Dream*

**Statement:**

For any $a, b$, prime $p$ and $i \geq 0$,

$$(a + b)^{p^i} \equiv a^{p^i} + b^{p^i} \pmod{p}.$$

**Proof:**
Apply induction on $i$: when $i = 1$, by ***lemma***

$$(a + b)^p \equiv a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} \equiv a^p + b^p \pmod{p}.$$

Suppose Freshman's Dream holds true for some $i$, then for $i+1$

$$(a+b)^{p^{i+1}} \equiv [(a+b)^{p^i}]^p \equiv (a^{p^i}+b^{p^i})^p \equiv a^{p^{i+1}}+b^{p^{i+1}} \pmod p.$$

■

## Theorem 82 *Wolstenholme's Theorem*

**Statement:**

*Form 1:* For prime $p \geq 5$,

$$\sum_{i=1}^{p-1}\frac{1}{i^2} \equiv 0 \pmod p.$$

*Form 2:* For prime $p \geq 5$,

$$\sum_{i=1}^{p-1}\frac{1}{i} \equiv 0 \pmod {p^2}.$$

*Form 3:* For prime $p \geq 5$,

$$\binom{2p-1}{p-1} \equiv 1 \pmod {p^3}.$$

**Proof:**
Proof of *Form 2*
*Method 1:* (by algebraic method)
Compute

$$2\sum_{i=1}^{p-1}\frac{1}{i} = \sum_{i=1}^{p-1}(\frac{1}{i}+\frac{1}{p-i}) = \sum_{i=1}^{p-1}\frac{p}{i(p-i)} \equiv -p\sum_{i=1}^{p-1}\frac{1}{i^2} = -p\sum_{i=1}^{p-1}i^2 = -\frac{p^2(p-1)(2p-1)}{6} \equiv 0 \pmod {p^2}.$$

*Method 2:* (by Taylor Series)
Consider polynomial

$$f(x) = \prod_{i=1}^{p-1}(x-i) = x^{p-1}+a_1x^{p-2}+a_2x^{p-3}+...+a_{p-2}x+(p-1)!,$$

for some $a_1, a_2, ..., a_{p-2}$. We use the fact $x^{p-1}-1 \equiv f(x) \pmod p$ that have been proven at the proof of **Wilson Theorem**, cancel out the equal terms from both side give

$$a_1x^{p-2}+a_2x^{p-3}+...+a_{p-2}x \equiv 0 \pmod p$$

for any $x$. By **Lagrange's Theorem**, $p \mid a_j$, $\forall\ 1 \leq j \leq p-2$. Noticed that $f(0) = (n-1)! = f(p)$, we compute

$$f'(0) = -\sum_{i=1}^{p-1}\prod_{j\neq i}j, \quad f''(0) = a_{p-3},$$

then consider **Taylor Series** of $f(p)$,

$$f(p) = f(0)+\sum_{i=0}^{\infty}\frac{f^{(i)}(0)}{i!}p^i \Leftrightarrow 0 = \sum_{i=1}^{\infty}\frac{f^{(i)}(0)}{i!}p^{i-1} = f'(0)+\frac{f''(0)}{2}p+\sum_{i=3}^{\infty}\frac{f^{(i)}(0)}{i!}p^{i-1}.$$

Since $p \mid a_{p-3} = f''(0)$, then $p^2 \mid \frac{f''(0)}{2}p$ which means

$$p^2 \mid f'(0) \Leftrightarrow p^2 \mid (p-1)!\sum_{i=1}^{p-1}\prod_{j\neq i}j = \sum_{i=1}^{p-1}\frac{1}{i} \equiv 0 \pmod {p^2}.$$

□

Proof of *Form 1*
Directly obtain from *Method 1* of proof of *Form 2*.

□

## Lemma 46

**Statement:**

Let $n = \overline{a_k a_{k-1} ... a_0}$. For $1 \le i \le k$, denoted

$$S(n) = \sum_i a_i, \quad S_0 = \sum_{2|i} a_i \quad \text{and} \quad S_1 = \sum_{2\nmid i} a_i,$$

then
(a) $S(n) \equiv n \pmod 9$.
(b) $S_0 - S_1 \equiv n \pmod{11}$.

**Proof:**
(a)

$$n \equiv \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i = S(n) \pmod 9.$$

(b)

$$n \equiv \sum_{i=0}^{k} a_i 10^i \equiv \sum_{i=0}^{k} a_i (-1)^i = S_0 - S_1 \pmod{11}.$$

■

## 3.3 GCD and LCM

### Theorem 83 *Properties of GCD*

**Statement:**

GCD has the following properties:

*1.* (*commutativity*) $\gcd(a, b) = \gcd(b, a)$.

*2.* (*associativity*) $\gcd(a_1, a_2, ..., a_n) = \gcd(\gcd(a_1, a_2, ..., a_k), a_{k+1}, ..., a_n)$ for some $1 \leq k \leq n$.

*3.* (*multiplicity*) For coprime $a, b$, $\gcd(ab, c) = \gcd(a, c)\gcd(b, c)$.

*4.* (*distributivity over lcm*) $\gcd(a, \operatorname{lcm}(b, c)) = \operatorname{lcm}(\gcd(a, b), \gcd(a, c))$.

*5.* $n \mid a, b \Leftrightarrow n \mid \gcd(a, b)$.

*6.* $\gcd(na_i)_{1\leq i\leq n} = |n| \gcd(a_i)_{1\leq i\leq n}$.

*7.* $\gcd(a, n) = \gcd(b, n) = 1 \Leftrightarrow \gcd(ab, n) = 1$

*8.* $\gcd(a, b) = 1 \Leftrightarrow \gcd(a^n, b^n) = 1$.

*9.* $\gcd(a, b) = d \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

*10.* If $ab = n^k$ with $\gcd(a, b) = 1$, then $a = \gcd(a, n)^k, b = \gcd(b, n)^k$.

*11.* $\gcd(a^n, b^n) = \gcd(a, b)^n$.

**Proof:** Property *1,5* is by definition. For *2,3,6,7,8,9,10* and *11*, think $\gcd(a_i)$ as the intersection of the prime divisor of $a_i$ then can easily proved. For *4*, let $p$ be any prime divisor of $a, b$ or $c$, and let $s_a, s_b, s_c$ be its exponent in each of those numbers. Let $x = \operatorname{lcm}(a, \gcd(b, c))$, then the exponent of $p$ in $x$ is $\max\{s_a, \min\{s_b, s_c\}\} = \min\{\max\{s_a, s_b\}, \max\{s_a, s_c\}\}$. Hence follows that lcm is distributive over gcd.

■

### Lemma 47

**Statement:**

For $a, b, m, n \geq 0$, if $\gcd(a, b) = 1$, then

$$\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$$

**Proof**
Replacing $a, b, m, n$ by $a^{\gcd(m,n)}$, $b^{\gcd(m,n)}$, $\frac{m}{\gcd(m,n)}$, $\frac{n}{\gcd(m,n)}$ respectively, we may assume $\gcd(m, n) = 1$. Since $a \equiv b \pmod{a - b}$, it follows that $a^k \equiv b^k \pmod{a - b}$ for all $k \geq 1$. Hence $a - b \mid \gcd(a^m - b^m,\ a^n - b^n)$. Conversely, let

$$d := \gcd(a^m - b^m,\ a^n - b^n).$$

Then

$$a^m \equiv b^m \pmod{d} \quad \text{and} \quad a^n \equiv b^n \pmod{d},$$

so for all $k, l \geq 1$ $a^{mk} \equiv b^{mk} \pmod{d}, a^{nl} \equiv b^{nl} \pmod{d}$. Since $\gcd(m,n) = 1$, **Bézout' s lemma** yields integers $k, l \geq 1$ with $km = ln + 1$. Thus

$$a^{ln+1} = a^{mk} \equiv b^{mk} = b^{nl+1} \equiv b\, a^{nl} \pmod{d},$$

which gives $d \mid a^{nl}(a-b)$. But $\gcd(a,d) = 1$ (since $\gcd(a,b) = 1$ and $d \mid a^m - b^m$), so by **Gauss' lemma**, $d \mid a - b$. This completes the proof. ■

## Lemma 48

**Statement:**

Let for any $k$,

$$\gcd(a,b) \;=\; \gcd\big(a,\; b + k\,a\big).$$

**Proof:**
Set $d := \gcd(a,b)$. Since $d \mid a, b$, it follows that $d \mid (b + k\,a)$. Hence $d$ is a common divisor of $a$ and $b + k\,a$, so

$$d \mid \gcd\big(a, b + k\,a\big).$$

Conversely, let $d' = \gcd(a, b + k\,a)$. Then $d' \mid a$ and $d' \mid (b + k\,a)$, which implies $d' \mid b$. Thus $d'$ is a common divisor of $a$ and $b$, giving

$$d' \mid \gcd(a,b).$$

Since $\gcd(a,b)$ and $\gcd(a, b + k\,a)$ are nonnegative integers dividing each other, they must be equal. ■

## Theorem 84 *Euclidean Algorithm*

**Statement:**

Let $a > b > 0$,

$$r_0 = a, \quad r_1 = b,$$

and for as long as $r_i \neq 0$, let $r_{i+1}$ be the remainder when $r_{i-1}$ is divided by $r_i$. Then there exists a smallest $n \geq 1$ such that

$$r_n = 0,$$

Moreover,

$$r_{n-1} = \gcd(a,b).$$

**Proof:** First, by construction each remainder satisfies $0 \leq r_{n+1} < r_n$. Since the sequence $\{r_n\}$ consists of nonnegative integers strictly decreasing whenever $r_n > 0$, it must terminate at some first index $N$ with $r_N = 0$.
Next, for each $n \geq 1$, the division

$$r_{n-1} = q_n\, r_n + r_{n+1}$$

shows that $r_{n+1} \equiv r_{n-1} \pmod{r_n}$. Hence every common divisor of $r_{n-1}, r_n$ also divides $r_{n+1}$, and by induction every common divisor of $a, b$ divides each subsequent $r_n$. In particular, it divides $r_{N-1}$.
On the other hand, since $r_N = 0$, we have $r_{N-1} \mid r_{N-2}$, and then by "lifting back' ' through the divisions one sees $r_{N-1}$ divides $r_{N-2}, r_{N-3}, \ldots, r_0 = a$ and $r_1 = b$. Thus $r_{N-1}$ is a common divisor of $a$ and $b$. Combining these two facts, $r_{N-1}$ is the greatest common divisor of $a$ and $b$. ■

### Theorem 85 *Properties of LCM*

**Statement:**

LCM has the following properties:

1. (*commutativity*) $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a)$.
2. (*associativity*) $\operatorname{lcm}(a_1, a_2, ..., a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, a_2, ..., a_k), a_{k+1}, ..., a_n)$ for some $1 \leq k \leq n$.
3. (*distributivity over gcd*) $\operatorname{lcm}(a, \gcd(b,c)) = \gcd(\operatorname{lcm}(a,b), \operatorname{lcm}(a,c))$
4. $a, b \mid n \Leftrightarrow \operatorname{lcm}(a,b) \mid n$.
5. $\operatorname{lcm}(na, nb) = |n| \operatorname{lcm}(a,b)$.

**Proof:**
Property *1* is by definition. For *2*,*4* and *5*, think $\operatorname{lcm}(a_i)$ as the union of prime divisor of $a_i$. For *3*, let $p$ be any prime divisor of $a, b$ or $c$, and let $s_a, s_b, s_c$ be its exponent in each of those numbers. Let $x = \gcd(a, \operatorname{lcm}(b,c))$, then the exponent of $p$ in $x$ is $\min\{s_a, \max\{s_b, s_c\}\} = \max\{\min\{s_a, s_b\}, \min\{s_a, s_c\}\}$. Hence follows that gcd is distributive over lcm.

■

### Lemma 49

**Statement:**

For any integers $a, b$,

$$\gcd(a,b)\operatorname{lcm}(a,b) = |ab|.$$

**Proof:**
Write the prime factorizations

$$a = \prod_p p^{e_p}, \quad b = \prod_p p^{f_p},$$

where the product runs over all primes $p$ and $e_p, f_p \geq 0$. Then

$$\gcd(a,b) = \prod_p p^{\min(e_p, f_p)}, \qquad \operatorname{lcm}(a,b) = \prod_p p^{\max(e_p, f_p)}.$$

Therefore

$$\gcd(a,b)\operatorname{lcm}(a,b) = \left|\prod_p p^{\min(e_p,f_p)+\max(e_p,f_p)}\right| = \left|\prod_p p^{e_p+f_p}\right| = |ab|.$$

■

### Theorem 86 *Bézout's Lemma*

**Statement:**

For any $a_1, a_2, \cdots, a_n$ that not all zero, $\exists\, b_1, b_2, \cdots, b_n$ such that

$$\sum_{i=1}^{n} a_i b_i = \gcd(a_1, a_2, \cdots, a_n).$$

**Proof:**

Let $S$ be the set of all linear combinations of $\sum_{i=1}^{n} a_i x_i$, with $x_i \in \mathbb{Z}_{>0}$. Note $a_1^2 + \cdots + a_n^2 \in S$ is a positive integer, so by the **Well-ordering principle** $S$ has a least positive element

$$d = \min\{s \in S : s > 0\}.$$

Since $d \in S$, we can write

$$d = a_1 x_1 + \cdots + a_n x_n,$$

showing $d$ is a multiple of any common divisor of the $a_i$. Now take any $s \in S$ and divide by $d$:

$$s = qd + r, \quad 0 \le r < d.$$

Then $r = s - qd \in S$, so minimality of $d$ forces $r = 0$. Hence $d \mid s$, and in particular $d \mid a_i$ for each $i$. Therefore $d = \gcd(a_1, \ldots, a_n)$. ■

## Theorem 87 *Erdös-Szekeres Theorem*

**Statement:**

For $1 \le k, m < n$,

$$\gcd\left(\binom{n}{k}, \binom{n}{m}\right) \neq 1.$$

**Proof:** Suppose in contrary, noted that

$$\binom{n}{k} \cdot \binom{k}{m} = \frac{n!}{k!(n-k)!} \cdot \frac{k!}{m!(k-m)!} = \frac{n!}{m!(n-m)!} \cdot \frac{(n-m)!}{(k-m)!(n-k)!} = \binom{n}{m} \cdot \binom{n-m}{k-m}.$$

Then $\binom{n}{m} \,\Bigg|\, \binom{n}{k} \cdot \binom{k}{m}$ and by **Gauss' Lemma** we have $\binom{n}{m} \,\Bigg|\, \binom{k}{m}$, which is contradict to $n > k$. ■

## 3.4 Diophantine Equation

### Theorem 88 *Fermat Last Theorem*

**Statement:**

For $n \geq 3$, the only solution over $\mathbb{Q}^3$ for

$$x^n + y^n = z^n$$

is $(0, 0, 0)$.

**Proof:** Andrew Wiles’ s original paper:
Modular elliptic curves and Fermat’ s Last Theorem ■

### Theorem 89 *Euler’ s Four-Square Identity*

**Statement:**

For $a, b, c, d, w, x, y, z \in \mathbb{C}$,

$$\begin{aligned}\left(a^2+b^2+c^2+d^2\right)\left(w^2+x^2+y^2+z^2\right) = \quad & (aw+bx+cy+dz)^2 \\ & + (ax-bw+cz-dy)^2 \\ & + (ay-bz-cw+dx)^2 \\ & + (az+by-cx-dw)^2.\end{aligned}$$

**Proof:** One can just expand both sides to prove the identity, but here is the derivation using quaternions (only applicable for $a, b, c, d, w, x, y, z \in \mathbb{R}$):
Consider $p, q \in \mathbb{H}$ s.t

$$p = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}, \quad \text{and} \quad q = w + x\boldsymbol{i} + y\boldsymbol{j} + z\boldsymbol{k},$$

where

$$\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = -1, \quad \boldsymbol{ij} = \boldsymbol{k},\ \boldsymbol{ji} = -\boldsymbol{k}, \quad \boldsymbol{jk} = \boldsymbol{i},\ \boldsymbol{kj} = -\boldsymbol{i}, \quad \boldsymbol{ki} = \boldsymbol{j},\ \boldsymbol{ik} = -\boldsymbol{j},$$

we expand and simplify:

$$\begin{aligned}pq &= (a + b\,\boldsymbol{i} + c\,\boldsymbol{j} + d\,\boldsymbol{k})(w + x\,\boldsymbol{i} + y\,\boldsymbol{j} + z\,\boldsymbol{k}) \\ &= aw + ax\,\boldsymbol{i} + ay\,\boldsymbol{j} + az\,\boldsymbol{k} + bw\,\boldsymbol{i} + bx\,\boldsymbol{i}^2 + by\,\boldsymbol{ij} + bz\,\boldsymbol{ik} \\ &\quad + cw\,\boldsymbol{j} + cx\,\boldsymbol{ji} + cy\,\boldsymbol{j}^2 + cz\,\boldsymbol{jk} + dw\,\boldsymbol{k} + dx\,\boldsymbol{ki} + dy\,\boldsymbol{kj} + dz\,\boldsymbol{k}^2 \\ &= (aw - bx - cy - dz) + (ax + bw + cz - dy)\,\boldsymbol{i} + (ay - bz + cw + dx)\,\boldsymbol{j} + (az + by - cx + dw)\,\boldsymbol{k}.\end{aligned}$$

Hence,

$$|pq| = \sqrt{(aw-bx-cy-dz)^2 + (ax+bw+cz-dy)^2 + (ay-bz+cw+dx)^2 + (az+by-cx+dw)^2}.$$

Since $|pq| = |p|\,|q|$, square both sides and adjust the sign of each term, we will obtain the identity. ■

### Theorem 90 *Brahmagupta–Fibonacci Identity*

**Statement:**

For $a, b, c, d \in \mathbb{C}$,
$$(a^2 + b^2)\,(c^2 + d^2) \;=\; (ac - bd)^2 + (ad + bc)^2.$$

**Proof:**
For $a, b, c, d \in \mathbb{R}$, consider complex numbers.

$$z = a + b\,i, \qquad w = c + d\,i,$$

then
$$\mathrm{Norm}(zw) = \mathrm{Norm}((ac - bd) + (ad + bc)i) = (ac - bd)^2 + (ad + bc)^2,$$

and
$$\mathrm{Norm}(z) = a^2 + b^2, \quad \mathrm{Norm}(w) = c^2 + d^2.$$

By the multiplicity of the complex norm, we have

$$(ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)\,(c^2 + d^2),$$

as claimed. (Just expand both side to easily prove the case where $a, b, c, d \in \mathbb{C}$.) ■

### Theorem 91 *Sophie Germain' s Identity*

**Statement:**

For $a, b \in \mathbb{C}$,
$$a^4 + 4b^4 = (a^2 + 2ab + 2b^2)\,(a^2 - 2ab + 2b^2).$$

**Proof:**
Observe that
$$a^4 + 4b^4 = a^4 + 4a^2b^2 + 4b^4 \;-\; 4a^2b^2 = (a^2 + 2b^2)^2 - (2ab)^2.$$

By the difference of squares,

$$(a^2 + 2b^2)^2 - (2ab)^2 = \big(a^2 + 2b^2 - 2ab\big)\,\big(a^2 + 2b^2 + 2ab\big),$$

which is exactly the stated factorization. ■

### Theorem 92 *Candido' s Identity*

**Statement:**

Let $x, y \in \mathbb{C}$, then
$$\big(x^2 + y^2 + (x + y)^2\big)^2 \;=\; 2\big(x^4 + y^4 + (x + y)^4\big).$$

**Proof:** Omitted. ■

### Theorem 93 *Simon' s Favorite Factoring Trick*

**Statement:**

For any $x, y \in \mathbb{R}$ and constants $k, l \in \mathbb{R}$, the Diophantine equation

$$xy + kx + ly = n$$

is equivalent to

$$(x + l)(k + a) = n + kl.$$

Furthermore, if $xy$ has a coefficient:

$$sxy + kx + ly = n$$

Multiply both side by $s$ and the equation can be write as

$$(sx + l)(sy + k) = sn + kl.$$

**Proof:** Just expand. ■

## 3.5 Arithmetic Function

### Definition 59 *Euler's Totient Function*

**Description:**

**Euler's Totient Function** counts the integers between 1 to $n$ that are that coprime to $n$ (inclusive):

$$\varphi(n) := \sum_{\substack{1\le i\le n \\ \gcd(i,n)=1}} 1.$$

Let $n = \prod_{i=1}^{k} {p_i}^{\alpha^i}$, we have formula of $\varphi(n)$:

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

and specifically let $p$ be prime then

$$\varphi(p^k) = p^k - p^{k-1}.$$

### Definition 60 *Divisor Function*

**Description:**

For $z \in \mathbb{C}$, the **Division Function** is defined as

$$\sigma_z(n) := \sum_{d|n} d^z,$$

specifically we have

$$\sigma_0(n) := \tau(n) = \sum_{d|n} 1,$$

is the **number of divisor function** and

$$\sigma_1(n) := \sigma(n) = \sum_{d|n} d,$$

is the **sum of divisor function**, when $n = \prod_{i=1}^{k} {p_i}^{\alpha^i}$, we have formula

$$\sigma_{z\neq 0}(n) = \prod_{i=1}^{k} \frac{{p_i}^{z(\alpha_i+1)}+1}{{p_i}^z - 1},$$

and

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

### Definition 61 *Prime Omega Functions*

**Description:**

**Prime Omega Functions** $\omega(n)$ and $\Omega(n)$ counts the number of distinct prime divisor and the total number of prime divisor of $n$ respectively, again if $n = \prod_{i=1}^{k} {p_i}^{\alpha_i}$, then

$$\omega(n) = k, \qquad \Omega(n) = \sum_{i=1}^{n} \alpha_i.$$

## Definition 62 *Liouville Function*

**Description:**

**Liouville Function** gives a value of $+1$ if $n$ is the product of an even number of primes, and gives $-1$ if otherwise:

$$\lambda(n) = (-1)^{\Omega(n)}.$$

## Definition 63 *Möbius Function*

**Description:**

Called a number **square-free** if it doesn't divisible by any perfect square greater than 1, then we can defined **Möbius Function**:

$$\mu(n) := \begin{cases} 1 & , n = 1; \\ (-1)^{\omega(n)} & , n \text{ square-free}; \\ 0 & , n \text{ isn't square-free}. \end{cases}$$

or more neatly,

$$\mu(n) := \lambda(n)\delta_{\omega(n),\Omega(n)},$$

we also can immediately deduce that

$$\mu(n)^2 = \mathbb{I}(n \text{ is square-free}).$$

## Definition 64 *Von Mangoldt Function*

**Description:**

The **Von Mangoldt Function** is defined as

$$\Lambda(n) = \begin{cases} \log p & , \exists \text{ prime } p \text{ and } k \geq 1 \text{ s.t } n = p^k \\ 0 & , \text{otherwise}. \end{cases}$$

## 3.6 Multiplicative Number Theory

### Definition 65 *Indicator Function*

**Description:**

For a statement $P$,

$$\mathbb{I}(P) = \begin{cases} 1 & , P \text{ is true;} \\ 0 & , \text{otherwise.} \end{cases}$$

### Definition 66 *Constant One Function*

**Description:**

It is defined for convenience

$$\mathbb{1}(n) :\equiv 1, \quad \forall n \in \mathbb{C}.$$

### Definition 67 *Identity Function*

**Description:**

It just simply defined as

$$\text{id}(n) := n, \forall n \in \mathbb{C}.$$

### Definition 68 *Kronecker Delta Function*

**Description:**

A two variables function, is defined by

$$\delta_{i,j} := \mathbb{I}(i = j),$$

In order to make the **Dirichlet Convolution** part more convenient later, we denote $\delta_{1,n} = \delta(n)$.

### Definition 69 *Multiplicative Function*

**Description:**

A **Multiplcative Function** is an arithmetic function that satisfy

$$f(mn) = f(m)f(n), \quad \forall\, a, b \text{ s.t } \gcd(a, b) = 1,$$

below are some examples: For $\forall$ coprime $m, n$,
**Greatest Common Divisor**, $\gcd(mn, k) = \gcd(m, k)\gcd(n, k)$ if fix $k$,

**Euler Totient Function**, $\varphi(mn) = \varphi(m)\varphi(n)$,
**Möbius Function**, $\mu(mn) = \mu(m)\mu(n)$,
**Divisor Function**, $\sigma_k(mn) = \sigma_k(m)\sigma_k(n)$.

### **Definition 70** *Completely Multiplicative Function*

**Description:**

A function is called **completely multiplicative** iff

$$f(mn) = f(m)f(n), \quad \forall\, n, m \in \mathrm{dom} f,$$

below are some examples:
**Kronecker Delta Function**, $\delta_{mn,k} = \delta_{m,k}\delta_{n,k}$,
**Constant One Function**, $\mathbb{1}(mn) = \mathbb{1}(m)\mathbb{1}(n)$,
**Identity Function**, id$(mn)$=id$(m)$id$(n)$,
**Jacobi's Symbol** (and hence **Legendre's Symbol**) $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n}) = (\frac{ab}{p_1})^{\alpha_1} \cdots (\frac{ab}{p_k})^{\alpha_k}$ (multiplicative in two ways),
**Expected Value**, $\mathbb{E}[XY] = \mathbb{E}[X]\mathbb{E}[Y]$),
**Determinant**, det$(AB)$ =det$A$·det$B$,
**Power Function**, $(mn)^k = m^k \cdot n^k$,
**Sign Function**, sgn$(mn)$ =sgn$(m)$·sgn$(n)$,
**Norm**, Norm$(wz)$ =Norm$(w)$Norm$(m)$,
**Complex Conjugate**, $\overline{wx} = \overline{w}\overline{z}$,
**Liouville Function**, $\Lambda(mn) = \Lambda(m)\Lambda(n)$.

### **Definition 71** *Dirichlet Convolution*

**Description:**

For two arithmetic function $f, g$, the **Dirichlet Convolution** of them is defined by

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

There are some properties of $*$:
*1.* (*Commutativity*) $f * g = g * f$,
*2.* (*Associativity*) $(f * g) * h = f * (g * h)$,
*3.* (*Identity*) $f * \delta = f$,
*4.* (*Distributivity over addition*) $f * (g * h) = f * g + f * h$.
*5.* Dirichlet Convolution of two multiplicative function is also multiplicative.

### **Theorem 94** *Möbius Inversion*

**Statement:**

Let $f, g$ be two arithmetic function, then for $\forall n \in \mathbb{Z}_{>0}$,
*Form 1:*

$$g = f * \mathbb{1} \quad \Leftrightarrow \quad f = g * \mu.$$

we also have the product version,
*Form 2:*

$$f(n) = \prod_{d|n} g(d) \Leftrightarrow g(n) = \prod_{d|n} f(d)^{\mu(\frac{n}{d})}.$$

**Proof:**
<u>Proof of *Form 1*</u>
Suppose $g = f * \mathbb{1}$. Convolving both sides with $\mu$ gives

$$g * \mu \;=\; (f * \mathbb{1}) * \mu \;=\; f * (\mathbb{1} * \mu) \;=\; f * \delta \;=\; f.$$

Conversely, if $f = g * \mu$, convolving with $\mathbb{1}$ yields

$$f * \mathbb{1} \;=\; (g * \mu) * \mathbb{1} \;=\; g * (\mu * \mathbb{1}) \;=\; g * \delta \;=\; g,$$

so $g = f * \mathbb{1}$.

<u>Proof of *Form 2*</u>
Assume $f(n) = \prod_{d|n} g(d)$. Taking natural logarithms gives the additive relation

$$\ln f(n) = \sum_{d|n} \ln g(d).$$

By the additive Möbius inversion just proved,

$$\ln g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \ln f(d).$$

Exponentiating both sides yields

$$g(n) = \exp\Big(\sum_{d|n} \mu(n/d) \ln f(d)\Big) = \prod_{d|n} f(d)^{\mu(\frac{n}{d})}.$$

The converse follows by the same argument applied to the inverse relation. ■

## Definition 72 *Möbius Pair*

**Description**:

If $f$ and $g$ are two arithmetic function satisfying condition $f = g * \mathbb{1}$, then we call the order pair $(f, g)$ a **Möbius Pair**, here are some examples: $(\delta, \mu)$, $(\tau, \mathbb{1})$, $(\sigma, \mathrm{id})$, $(\mathbb{1}, \delta)$ and $(\mathrm{id}, \varphi)$.

## Definition 73 *Popovici Function*

**Description**

A generalized Möbius Function to be the $k$-fold Dirichlet Convolution of itself:

$$\mu_k = \mu * \mu * \cdots * \mu.$$

It has a nice property, which is

$$\mu_k(p^\alpha) = (-1)^\alpha \binom{k}{\alpha},$$

for prime $p$ and $\alpha \geq 0$.

## Lemma 50

**Statement:**

For $n > 0$,

$$\sum_{i \geq 1} \varphi(i) \left\lfloor \frac{n}{i} \right\rfloor = \frac{1}{2} n(n+1).$$

**Proof**:

$$\sum_{i\geq 1} \varphi(i) \left\lfloor \frac{n}{i} \right\rfloor = \sum_{i \geq 1} \varphi(i) \sum_{\substack{m \leq n \\ i \mid m}} 1 = \sum_{i \geq 1} \sum_{\substack{m \leq n \\ i\ i \mid m}} \varphi(i) = \sum_{\substack{m \leq n \\ 1 \leq i \mid m}} \varphi(i) = \sum_{m=1}^{n} \sum_{1 \leq i \mid m} \varphi(i) = \sum_{m=1}^{n} m.$$

■

## 3.7 Primes

### Theorem 95 *Euclid's Theorem*

**Statement:**

> There exists infinitely many primes.

**Proof:** Suppose, to the contrary, that there are only finitely many primes, say $p_1, p_2, \ldots, p_k$. Consider the integer

$$N = p_1 p_2 \cdots p_k + 1.$$

Since $N > 1$, it must have at least one prime divisor $p$. But $p$ cannot be any of $p_1, \ldots, p_k$, for each of those divides $p_1 \cdots p_k$ and hence leaves remainder 1 when dividing $N$. This contradiction shows there is no finite list of all primes. ■

### Theorem 96 *Fundamental Theorem of Arithmetic*

**Statement:**

> Every $n > 1$ can be represented in exactly one way as a product of prime powers
>
> $$n = \prod_{i=1}^{k} {p_i}^{\alpha_i},$$
>
> where $p_1 < p_2 < \cdots < p_k$ are primes and $\alpha_i = v_{p_i}(n)$.

**Proof:**
*Existence:*
We prove by strong induction on $n \geq 2$ that $n$ is a product of primes. Clearly 2 is prime. Assume every integer $2 \leq k < n$ factors as a product of primes. If $n$ itself is prime, we are done. Otherwise write $n = ab$ with integers $1 < a \leq b < n$. By the induction hypothesis both $a$ and $b$ factor into primes, say

$$a = p_1 p_2 \cdots p_j, \quad b = q_1 q_2 \cdots q_k.$$

Hence $n = ab = p_1 p_2 \cdots p_j \, q_1 q_2 \cdots q_k$ is a product of primes.

*Uniqueness:*
Suppose, to the contrary, there is an integer $n > 1$ admitting two distinct prime factorizations:

$$n = p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k,$$

with all $p_i, q_i$ prime and the two multisets $\{p_i\} \neq \{q_i\}$. Choose $n$ minimal with this property. Then $p_1$ divides $q_1 q_2 \cdots q_k$, so by Euclid' s lemma $p_1$ divides some $q_i$. Since $p_1$ and $q_i$ are prime, $p_1 = q_i$. Canceling this common factor from both sides yields a smaller integer $n/p_1 = p_2 \cdots p_j = q_1 \cdots q_{i-1} q_{i+1} \cdots q_k$ with two distinct prime factorizations, contradicting the minimality of $n$. Thus the prime factorization must be unique. ■

### Theorem 97 *Dirichlet's Theorem*

**Statement:**

Given any coprime $a, b$, there exists infinitely many $ak + b$ type primes.

**Proof:** See Wang Zi Jian's proof:
https://math.uchicago.edu/~may/REU2017/REUPapers/WangZijian.pdf. ■

### Theorem 98 *Green-Tao Theorem*

**Statement:**

For $n \geq 3$, $\exists$ an arithmetic progression with $n$ terms, and all of them are primes.

**Proof:** Check out https://math.mit.edu/~fox/paper-green-tao.pdf. ■

### Theorem 99 *Schur's Theorem*

**Statement:**

Let $S$ be the set of all values of the non-constant polynomial $P \in \mathbb{Z}[x]$, then there exists infinitely many primes divide some element of $S$.

**Proof:** If $P(0) = 0$ we are done, otherwise let $S = \{P(n) \neq 0 : n \in \mathbb{Z}\}$. We shall show there are infinitely many primes dividing some element of $S$. Set

$$g(x) = \frac{P\big(x\,P(0)\big)}{P(0)}.$$

Since $P \in \mathbb{Z}[x]$ and $P(0) \neq 0$, we see $g \in \mathbb{Z}[x]$ and $g(0) = 1$. Now for any positive integer $n$, consider

$$g\big(n!\big) = \frac{P\big(n!\,P(0)\big)}{P(0)}.$$

Because $\gcd\big(n!, g(n!)\big) = 1$, each prime factor of $g(n!)$ is strictly larger than $n$. As $n \to \infty$, this produces infinitely many distinct primes dividing various values $g(n!)$, and therefore also dividing the corresponding values $P\big(n!P(0)\big) \in S$.

In either case, $S$ must be divisible by infinitely many primes. ■ ■

## Theorem 100 *Kobayashi's Theorem*

**Statement:**

Let $\mathscr{M}$ be an infinite set of positive integers such that the set of prime divisors of the element in $\mathscr{M}$ is finite, then the set of primes dividing the element of $\mathscr{M} + a$ is infinite, for $\forall a \geq 0$.

**Proof:** Suppose

$$a_n = \prod_{i=1}^{m} p_i^{x_i}, \qquad a_n + t = \prod_{i=1}^{l} q_i^{y_i},$$

with $\{p_i\}$ and $\{q_i\}$ finite sets of primes. It suffices to show there are only finitely many integer solutions $(x_1, \ldots, x_m, y_1, \ldots, y_l)$.
For $k = 0, 1, 2$ let

$$R_k = \{\, 1 \leq i \leq m : x_i \equiv k \pmod 3\}.$$

Then we may factor

$$\prod_{i=1}^{m} p_i^{x_i} = \Big(\prod_{i \in R_1} p_i\Big)\Big(\prod_{i \in R_2} p_i^2\Big) \cdot \Big(\prod_{i \in R_0} p_i^{x_i/3}\Big)\Big(\prod_{i \in R_1} p_i^{(x_i-1)/3}\Big)\Big(\prod_{i \in R_2} p_i^{(x_i-2)/3}\Big).$$

Set

$$A = \prod_{i \in R_1} p_i \cdot \prod_{i \in R_2} p_i^2, \qquad X = \prod_{i \in R_0} p_i^{x_i/3} \prod_{i \in R_1} p_i^{(x_i-1)/3} \prod_{i \in R_2} p_i^{(x_i-2)/3}.$$

Then $\prod_{i=1}^{m} p_i^{x_i} = A\,X^3$.

Similarly, defining residue-classes $S_k = \{\, 1 \leq i \leq l : y_i \equiv k \pmod 3\}$, one finds $\prod_{i=1}^{l} q_i^{y_i} = B\,Y^3$ for uniquely determined integers $B, Y$.
Hence the original equation

$$\prod_{i=1}^{l} q_i^{y_i} \; - \; \prod_{i=1}^{m} p_i^{x_i} \; = \; t$$

becomes

$$B\,Y^3 \; - \; A\,X^3 \; = \; t.$$

By **Thue' s theorem** each choice of nonzero $(A, B, t)$ admits only finitely many integer solutions $(X, Y)$. Since $(x_1, \ldots, x_m, y_1, \ldots, y_l)$ is uniquely recovered from $(A, X, B, Y)$, there are only finitely many such exponent-tuples. ■

## Lemma 51

**Statement:**

For $n > 0$, there $\exists$ a set $\mathscr{P}$ which has $n$ elements and all of them are primes such that for $\forall p, q \in \mathscr{P}$, $\frac{p+q}{2}$ also a prime.

## Lemma 52

**Statement:**

Let $\mathscr{P} = \{p \mid p < n, p \text{ is prime}\}$, if there's an arithmetic progression that has $n \geq 3$ term and all of them are primes, then the common difference,

$$d = k \prod_{p \in \mathscr{P}} p$$

for some $k$.

## 3.8 Quadratic Residue

### Definition 74 *$n^{th}$ Power Residue mod $m$*

**Description:**

Let $m > 1, n \geq 1$. An integer $a$ is called a $\boldsymbol{n^{th}}$ **power residue mod $\boldsymbol{m}$** if there exists an integer $x$ such that

$$x^n \equiv a \pmod{m}.$$

If no such $x$ exists, then $a$ is called a $\boldsymbol{n^{th}}$ **power non-residue mod $\boldsymbol{m}$**.
Specifically, when $n = 2$, we say $a$ is a **quadratic residue mod $\boldsymbol{m}$** (also called QR mod $m$).

### Theorem 101 *Euler' s Criterion*

**Statement:**

Let $m > 1$ and $n \geq 1$ be integers, then $a$ is an $n^{th}$ power residue mod $m$ if and only if

$$a^{\frac{\varphi(m)}{\gcd(n,\varphi(m))}} \equiv 1 \pmod{m}.$$

**Proof:**
Let $G = (\mathbb{Z}/m\mathbb{Z})^\times$, then $|G| = \varphi(m)$. The set of all $n$th powers in $G$ is the subgroup

$$H = \{\, g^n : g \in G\},$$

whose index in $G$ equals $\dfrac{|G|}{|H|} = \gcd(n, \varphi(m)) = d$. Hence $H$ consists exactly of those elements of $G$ whose $d$th power is the identity. Concretely,

$$g \in H \iff g^d = 1_G \iff g^{\varphi(m)/d} \equiv 1 \pmod{m}.$$

Taking $g = a$ gives the desired criterion. ■

### Definition 75 *Legendre Symbol*

**Description:**

Let $p$ be an odd prime and $a \in \mathbb{Z}$. The **Legendre symbol** $\left(\dfrac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a, \\ 1, & p \nmid a,\ a \text{ is a quadratic residue mod } p, \\ -1, & a \text{ is a quadratic nonresidue mod } p. \end{cases}$$

### Definition 76 *Jacobi Symbol*

**Description:**

Let $n > 1$ be an odd positive integer with prime factorization $n = \prod_{i=1}^{k} p_i^{e_i}$. For $a \in \mathbb{Z}$, the **Jacobi symbol** $\left(\frac{a}{n}\right)$ is defined by

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i},$$

where each $\left(\frac{a}{p_i}\right)$ is the Legendre symbol. In particular, $\left(\frac{a}{n}\right) = 0$ if and only if $\gcd(a, n) > 1$.

## Theorem 102 *Lagrange' s Lemma*

**Statement:**

Let $p$ be an odd prime. Then

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4, \\ -1, & p \equiv 3 \pmod 4. \end{cases}$$

**Proof:**
By **Euler' s Criterion**,

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

If $p = 4k + 1$, then $\frac{p-1}{2} = 2k$ is even, so

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

If $p = 4k + 3$, then $\frac{p-1}{2} = 2k + 1$ is odd, so

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

This completes the proof. ■

## Theorem 103 *Gauss' s Lemma*

**Statement:**

Let $p$ be an odd prime and suppose $p \nmid a$. Consider the least positive residues of

$$a,\ 2a,\ 3a,\ \ldots,\ \tfrac{p-1}{2}a \pmod p,$$

and let $n$ count the number of these residues that are greater than $\frac{p}{2}$, then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

**Proof:**

Write

$$r_1, r_2, \ldots, r_n \quad \text{(for those } > p/2), \qquad s_1, s_2, \ldots, s_m \quad \text{(for those } \leq p/2).$$

Then $n + m = (p-1)/2$. Observe that the numbers $\{\, p - r_1, \ldots, p - r_n\} \cup \{\, s_1, \ldots, s_m\}$ form a permutation of $\{1, 2, \ldots, (p-1)/2\}$. Hence

$$\Bigl(\frac{p-1}{2}\Bigr)! \;=\; \prod_{i=1}^{n}(p - r_i) \,\prod_{j=1}^{m} s_j \;\equiv\; (-1)^n \,\Bigl(\prod_{i=1}^{n} r_i\Bigr)\,\Bigl(\prod_{j=1}^{m} s_j\Bigr) \pmod{p}.$$

On the other hand, by definition each $r_i$ or $s_j$ is congruent to $ka$ for some $1 \leq k \leq (p-1)/2$, so

$$\prod_{i=1}^{n} r_i \,\prod_{j=1}^{m} s_j \equiv \bigl(1 \cdot 2 \cdots \frac{p-1}{2}\bigr)\, a^{\frac{p-1}{2}} \;=\; \Bigl(\frac{p-1}{2}\Bigr)!\, a^{\frac{p-1}{2}} \pmod{p}.$$

Combining these two displays gives

$$\Bigl(\frac{p-1}{2}\Bigr)! \;\equiv\; (-1)^n \,\Bigl(\frac{p-1}{2}\Bigr)!\, a^{\frac{p-1}{2}} \pmod{p}.$$

Since $\gcd\bigl((p-1)/2)!,\, p\bigr) = 1$, we may cancel $\bigl((p-1)/2\bigr)!$ to obtain

$$(-1)^n \, a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

By **Euler' s Criterion**,

$$\Bigl(\frac{a}{p}\Bigr) = (-1)^n,$$

as claimed. ■

## Lemma 53

**Statement:**

Let $p$ be an odd prime. Then

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

**Proof:**
By **Gauss' s lemma**, for any integer $a$ with $\gcd(a,p) = 1$, $\left(\frac{a}{p}\right) = (-1)^n$, where $n$ is the number of least positive residues of $\{a, 2a, \ldots, \frac{p-1}{2}a\}$ exceeding $p/2$. Take $a = 2$; then the set of even residues

$$F = \{2, 4, 6, \ldots, p-1\}$$

has size $\frac{p-1}{2}$. One checks:

$$n = \#\{\, x \in F : x > p/2\} = \begin{cases} \frac{p-1}{4}, & p \equiv \pm 1 \pmod{8}, \\ \frac{p+1}{4}, & p \equiv \pm 3 \pmod{8}. \end{cases}$$

Hence

$$\left(\tfrac{2}{p}\right) = (-1)^n = \begin{cases} (-1)^{\frac{p-1}{4}} = 1, & p \equiv \pm 1 \pmod{8}, \\ (-1)^{\frac{p+1}{4}} = -1, & p \equiv \pm 3 \pmod{8}. \end{cases}$$

Noting that

$$\frac{p^2-1}{8} = \begin{cases} \frac{(8k\pm1)^2-1}{8} = 8k^2 \pm 2k \equiv 0 \pmod{2}, & p \equiv \pm 1 \pmod{8}, \\ \frac{(8k\pm3)^2-1}{8} = 8k^2 \pm 6k + 1 \equiv 1 \pmod{2}, & p \equiv \pm 3 \pmod{8}, \end{cases}$$

we conclude

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

■

## Theorem 104 *Eisenstein' s Lemma*

**Statement:**

Let $p$ and $q$ be odd primes. Then

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor}.$$

**Proof:**
As in the proof of Gauss' s lemma, consider the least positive residues modulo $p$ of

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

Write those residues exceeding $p/2$ as $r_1, r_2, \dots, r_n$ and those $\le p/2$ as $s_1, s_2, \dots, s_m$. Clearly

$$n + m = \frac{p-1}{2}.$$

By the **Euclid's Division Lemma**, for each $1 \le k \le \frac{p-1}{2}$ there is an integer $\lfloor kq/p \rfloor$ and a least residue $r_k$ such that

$$kq = p\left\lfloor \frac{kq}{p} \right\rfloor + r_k, \quad 0 < r_k \le p-1.$$

Summing this identity over $k = 1, 2, \dots, \frac{p-1}{2}$ yields

$$\sum_{k=1}^{\frac{p-1}{2}} kq = p\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j.$$

On the other hand, if we replace each $r_j$ by $p - r_j$ (which runs over the same set of "large" residues), we get the same total $\sum kq$. Hence

$$\sum_{k=1}^{\frac{p-1}{2}} kq = p\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^{n} (p - r_j) + \sum_{j=1}^{m} s_j.$$

Now $\{p - r_j\} \cup \{s_j\}$ is a permutation of $1, 2, \dots, \frac{p-1}{2}$. Thus

$$\sum_{j=1}^{n} (p - r_j) \; + \; \sum_{j=1}^{m} s_j = 1 + 2 + \cdots + \frac{p-1}{2} = \frac{\frac{p-1}{2}\left(\frac{p-1}{2} + 1\right)}{2} = \frac{p^2-1}{8}.$$

Subtracting (2.2) from (2.4) gives

$$\frac{p^2-1}{8} - \left(\sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j\right) = \sum_{j=1}^{n} (p - r_j) - \sum_{j=1}^{n} r_j = np - 2\sum_{j=1}^{n} r_j.$$

But from (2.2) we also have $\sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j = \sum_{k=1}^{\frac{p-1}{2}} kq - p\sum_{k=1}^{\frac{p-1}{2}} \lfloor kq/p \rfloor$. Combining and simplifying shows that

$$(q-1)\,\frac{p^2-1}{8} = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor - n\right) + 2\sum_{j=1}^{n} r_j.$$

Since $p$ and $q$ are odd primes, the left side and $2\sum r_j$ are even, hence $\sum_{k=1}^{\frac{p-1}{2}}\lfloor kq/p\rfloor - n$ is even. Therefore

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\lfloor kq/p\rfloor - n} = 1,$$

and so

$$(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\lfloor kq/p\rfloor} = (-1)^n.$$

Finally, by Gauss' s lemma $\left(\frac{q}{p}\right) = (-1)^n$. Comparing with (2.5) completes the proof:

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor \frac{kq}{p}\right\rfloor}.$$

■

## Theorem 105 *Quadratic Reciprocity Law*

**Statement:**

Let $p$ and $q$ be distinct odd primes. Then their Legendre symbols satisfy

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

**Proof:** (*by Rousseau*)
By **Chinese remainder theorem** there is an isomorphism of groups

$$G = (\mathbb{Z}/pq\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times.$$

We identify an element of $G$ with a pair $(a,b)$, where $a \in \{1,2,\dots,p-1\}$ and $b \in \{1,2,\dots,q-1\}$. Let

$$H = \{(1,1),\ (-1,-1)\}$$

and form the quotient $G/H$ and take their product $\Pi$. We choose as representatives of $G/H$ first all of $(\mathbb{Z}/p\mathbb{Z})^\times$ times the first half of $(\mathbb{Z}/q\mathbb{Z})^\times$, namely

$$\{(a,b) : 1 \le a \le p-1,\ 1 \le b \le \frac{q-1}{2}\}.$$

Since each $a$–value appears $\frac{q-1}{2}$ times, their product modulo $p$ is

$$(p-1)!^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \pmod p \quad (\text{by } \textbf{Wilson' s theorem}).$$

Each $b \in \{1,\dots,\frac{q-1}{2}\}$ is repeated $p-1$ times, so the $b$–component of the product is

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

Hence the product of these representatives is

$$\Pi \equiv \left((-1)^{\frac{q-1}{2}} \bmod p,\ (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \bmod q\right).$$

On the other hand, choose representatives by taking the first half of $(\mathbb{Z}/pq\mathbb{Z})^\times$: all integers $1 \le n \le \frac{pq-1}{2}$ not divisible by $p$ or $q$. Let

$$A = \{n : 1 \le n \le \tfrac{pq-1}{2},\ p \nmid n,\ q \nmid n\},$$

and let

$$B = \{q, 2q, \ldots, \tfrac{p-1}{2}q\} \subset A$$

be those divisible by $q$. Then the $a$–component of the product of $A \setminus B$ is

$$\prod_{n \in A,\ q \nmid n} n \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p \quad \text{(by Euler' s criterion).}$$

Similarly the $b$–component is

$$(-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod q.$$

Thus this choice of representatives multiplies to

$$\pi \equiv \big((-1)^{\frac{q-1}{2}} (\tfrac{q}{p}) \bmod p,\ (-1)^{\frac{p-1}{2}} (\tfrac{p}{q}) \bmod q\big).$$

Since $\pi$ is determined only up to a sign $\pm 1$, so

$$\pm\big((-1)^{\frac{q-1}{2}},\ (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\big) = \big((-1)^{\frac{q-1}{2}} (\tfrac{q}{p}),\ (-1)^{\frac{p-1}{2}} (\tfrac{p}{q})\big).$$

Analyzing the two cases $(+)$ and $(-)$ shows in either event

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

■

## 3.9 Integer Coefficient Polynomial

### Definition 77 *Primitive Polynomial*

**Description:**

A nonzero polynomial

$$f(x) = \sum_{i=0}^{n} a_i\, x^i \;\in\; \mathbb{Z}[x]$$

is called **primitive** if the greatest common divisor of its coefficients is 1, i.e.

$$\gcd(a_0, a_1, \dots, a_n) = 1.$$

### Theorem 106 *Gauss' s Lemma in Polynomial*

**Statement:**

If $f(x), g(x) \in \mathbb{Z}[x]$ are primitive, then their product $f(x)\,g(x)$ is also primitive.

**Proof:**
Write

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{j=0}^{m} b_j x^j,$$

with $\gcd(a_i)_{0\le i\le n} = \gcd(b_i)_{0\le i\le n} = 1$. Suppose a prime $p$ divides every coefficient of $f(x)g(x)$. Then in the product

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \quad c_k = \sum_{i+j=k} a_i b_j,$$

each sum $\displaystyle\sum_{i+j=k} a_i b_j$ is divisible by $p$. In particular, by **Eucid's Lemma**

$$c_0 = a_0 b_0 \equiv 0 \pmod{p} \quad \Longrightarrow \quad p \mid a_0 \quad \text{or} \quad p \mid b_0.$$

WLOG assume $p \mid a_0$. Let $r$ be the smallest index with $p \nmid a_r$. Then looking at

$$c_r = a_r b_0 + a_{r-1} b_1 + \cdots + a_0 b_r,$$

all terms except $a_r b_0$ are divisible by $p$, yet $c_r \equiv 0 \pmod{p}$. Hence $p \mid b_0$. Repeating the same argument on increasing indices shows $p \mid b_i$ for all $i$. This contradicts $\gcd(b_i)_{0\le i\le n} = 1$. Thus no prime divides all coefficients of $fg$, so $fg$ is primitive. ∎

### Definition 78 *Irreducible Polynomial*

**Description:**

Let $\mathbb{F}$ be a field and let $f(x) \in \mathbb{F}[x]$ be nonconstant. We say $f(x)$ is **irreducible over** $\mathbb{F}$ if whenever

$$f(x) = g(x)\,h(x) \quad \text{with } g(x), h(x) \in \mathbb{F}[x],$$

then one of the factors is a nonzero constant.

### Theorem 107 *Gauss' s Irreducibility Lemma*

**Statement:**

A nonconstant polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$ if and only if it is both primitive and irreducible in $\mathbb{Z}[x]$.

**Proof:**
"⇒" is trivial.
Conversely, assume $f$ is primitive and irreducible in $\mathbb{Z}[x]$, but factors in $\mathbb{Q}[x]$ as

$$f(x) = G(x)\,H(x), \quad G, H \in \mathbb{Q}[x],\ \deg G, \deg H > 0.$$

Choose minimal positive integers $c_1, c_2$ such that $c_1G, c_2H \in \mathbb{Z}[x]$. Then

$$c_1c_2\,f(x) = \bigl(c_1G(x)\bigr)\,\bigl(c_2H(x)\bigr)$$

is a product of primitive polynomials, so by *Form 1* both $c_1G$ and $c_2H$ are primitive. Since $f$ itself is primitive, $c_1c_2$ must be $\pm1$, forcing $G, H \in \mathbb{Z}[x]$. This contradicts irreducibility of $f$ in $\mathbb{Z}[x]$. ■

### Theorem 108 *Eisenstein' s Criterion*

**Statement:**

Let

$$P(x) = \sum_{i=0}^{n} a_i x^i \ \in\ \mathbb{Z}[x], \quad a_n \neq 0.$$

If there exists a prime $p$ such that

1. $p \nmid a_n$,
2. $p \mid a_i$ for all $0 \le i \le n-1$,
3. $p^2 \nmid a_0$,

then $P(x)$ is irreducible in $\mathbb{Q}[x]$.

**Proof:** First we show that $P(x)$ is irreducible in $\mathbb{Z}[x]$. Suppose, to the contrary, that

$$P(x) = \left(\sum_{i=0}^{m} b_i\,x^i\right)\left(\sum_{j=0}^{\ell} c_j\,x^j\right), \quad m, \ell \ge 1,$$

with $b_i, c_j \in \mathbb{Z}$.
Since $p \nmid a_n = b_m\,c_\ell$, neither $b_m$ nor $c_\ell$ is divisible by $p$. On the other hand $p \mid a_0 = b_0\,c_0$ but $p^2 \nmid a_0$, so exactly one of $b_0, c_0$ is a multiple of $p$. WLOG assume $p \mid b_0$ and $p \nmid c_0$.
Let $t$ be the smallest index with $1 \le t \le m$ such that $p \nmid b_t$. Then $p \mid b_i$ for all $0 \le i < t$. Compare coefficients of $x^t$:

$$a_t = \sum_{i+j=t} b_i\,c_j = b_t\,c_0\ +\ \sum_{i=0}^{t-1} b_i\,c_{t-i}.$$

All terms in the second sum are divisible by $p$, and since $t < n$ we have $p \mid a_t$. Hence $p \mid b_t\,c_0$. But $p \nmid b_t$ and $p \nmid c_0$, a contradiction.
Therefore no nontrivial factorization is possible, and $P(x)$ is irreducible in $\mathbb{Z}[x]$.
Moreover, if $\text{cont}(P) > 1$, let $P(x) := \text{cont}(P) \cdot P_1(x)$, then by **Gauss' Irreducibility Lemma**, $P_i$ irreducible over $\mathbb{Q}$ implies $P$ also irreducible over $\mathbb{Q}$. ■

## **Theorem 109** *Cohn's Irreducibility Criterion*

**Statement:**

Let $b \geq 2$ be an integer. Suppose the number

$$\overline{a_n a_{n-1} \cdots a_0} \quad (a_n \neq 0)$$

is a prime written in base $b$. Then the polynomial

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

is irreducible in $\mathbb{Z}[x]$.

**Proof:** (*by M. Ram Murty*)
**Claim 1:** For any root $\alpha$ of $P(x)$, we have $\Re(\alpha) \leq 0$ or

$$|\alpha| < \frac{1+\sqrt{4b-3}}{2}.$$

*Proof of Claim 1:* We may assume $\Re(\alpha) > 0$ and $|\alpha| > 1$.
Since $P(\alpha) = 0$, we get

$$\left| a_n + \frac{a_{n-1}}{\alpha} \right| = \left| \sum_{j=2}^{n} \frac{a_{n-j}}{\alpha^j} \right|.$$

Note that

$$\Re\left(\frac{1}{\alpha}\right) = \frac{\Re(\alpha)}{|\alpha|^2} > 0$$

and $a_n \geq 1$, so

$$\left| a_n + \frac{a_{n-1}}{\alpha} \right| \geq \Re\left(a_n + \frac{a_{n-1}}{\alpha}\right) \geq 1.$$

By **Triangle Inequality**,

$$\left| \sum_{j=2}^{n} \frac{a_{n-j}}{\alpha^j} \right| \leq \sum_{j=2}^{n} \frac{|a_{n-j}|}{|\alpha|^j} \leq (b-1) \sum_{j=2}^{n} \frac{1}{|\alpha|^j} < \frac{b-1}{|\alpha|^2 - |\alpha|}.$$

Hence

$$1 < \frac{b-1}{|\alpha|^2 - |\alpha|},$$

so

$$|\alpha| < \frac{1+\sqrt{4b-3}}{2}.$$

□

**Claim 2:** When $b = 2$, for any root $\alpha$ of $P(x)$, we have

$$\Re(\alpha) < \frac{3}{2}.$$

*Proof of Claim 2:* Again we assume $\Re(\alpha) > 0$ and $|\alpha| > 1$. When $n = 1, 2$, it is easy to verify that $x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ all satisfy the requirement.
When $n \geq 3$, we use $P(\alpha) = 0$ to get

$$\left| a_n + \frac{a_{n-1}}{\alpha} + \frac{a_{n-2}}{\alpha^2} \right| = \left| \sum_{j=3}^{n} \frac{a_{n-j}}{\alpha^j} \right|.$$

If $|\arg \alpha| \leq \frac{\pi}{4}$, then

$$\Re\left(\frac{1}{\alpha^2}\right) \geq 0, \quad \text{and } a_n \geq 1,$$

so

$$\left|a_n+\frac{a_{n-1}}{\alpha}+\frac{a_{n-2}}{\alpha^2}\right|\geq\Re\left(a_n+\frac{a_{n-1}}{\alpha}+\frac{a_{n-2}}{\alpha^2}\right)\geq 1.$$

By **Triangle Inequality**,

$$\left|\sum_{j=3}^{n}\frac{a_{n-j}}{\alpha^j}\right|<\sum_{j=3}^{n}\frac{1}{|\alpha|^j}<\frac{1}{|\alpha|^3-|\alpha|^2}.$$

So

$$1<\frac{1}{|\alpha|^3-|\alpha|^2},\quad \text{i.e., } |\alpha|^3-|\alpha|^2-1<0,\quad \Rightarrow\Re(\alpha)\leq|\alpha|<\frac{3}{2}.$$

Now if $|\arg\alpha|>\frac{\pi}{4}$, then by Lemma 1:

$$|\alpha|<\frac{1+\sqrt{5}}{2},\quad \text{so } \Re(\alpha)<|\alpha|\cos\frac{\pi}{4}<\frac{1+\sqrt{5}}{2\sqrt{2}}<\frac{3}{2}.$$

□

Return to the original problem. Suppose $P(x)\in\mathbb{Z}[x]$ is reducible. Let

$$P(x)=f(x)g(x),$$

where $f(x),g(x)\in\mathbb{Z}[x]$ are nonconstant integer-coefficient polynomials. Since $P(b)$ is a prime and $f(b),g(b)\in\mathbb{Z}$, we may assume:

$$|f(b)|=1.$$

Let the roots of $f(x)$ be $\alpha_1,\ldots,\alpha_m$. By Lemma 1, $\Re(\alpha_i)\leq 0$ or

$$|\alpha_i|<\frac{1+\sqrt{4b-3}}{2},\quad \text{for } i=1,\ldots,m.$$

When $b\geq 3$,

$$b-\frac{1+\sqrt{4b-3}}{2}\geq 1,\quad \Rightarrow|b-\alpha_i|>1,$$

so

$$|f(b)|=\left|\prod_{i=1}^{m}(b-\alpha_i)\right|>1.$$

Contradiction.
When $b=2$, by Lemma 2:

$$\Re(\alpha_i)<\frac{3}{2},\quad 1\leq i\leq m,$$

and the leading coefficient of $f(x)$ is 1. So

$$|f(2)|=\left|\prod_{i=1}^{m}(2-\alpha_i)\right|>\left|\prod_{i=1}^{m}(1-\alpha_i)\right|=|f(1)|\geq 1.$$

Contradiction. ■

## **Theorem 110** *Perron' s Criterion*

**Statement:**

Let

$$P(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$$

be a monic polynomial, i.e $a_n = 1$. If

$$|a_{n-1}| > 1 + \sum_{i=0}^{n-2} |a_i| \quad \text{and} \quad a_0 \neq 0,$$

then $P(x)$ is irreducible in $\mathbb{Z}[x]$.

**Proof:**
We first show that $P(x)$ has at most one root with modulus $\geq 1$.
Assume $P(x)$ has a root $\alpha$ with $|\alpha| = 1$. Since $P(\alpha) = 0$, by **Triangle Inequality**

$$|a_{n-1}| = |a_{n-1}\alpha^{n-1}| = \left|\alpha^n + \sum_{i=0}^{n-2} a_i \alpha^i\right| \leq |\alpha^n| + \sum_{i=0}^{n-2} |a_i \alpha^i| \leq 1 + \sum_{i=0}^{n-2} |a_i|,$$

contradicting the hypothesis.
Now suppose $P(x)$ has a root $\alpha$ with $|\alpha| > 1$. Write

$$P(x) = (x - \alpha)\left(x^{n-1} + \sum_{i=0}^{n-2} b_i x^i\right).$$

By comparing coefficients, we obtain

$$\begin{aligned} a_{n-1} &= b_{n-2} - \alpha, \\ a_{n-2} &= b_{n-3} - \alpha b_{n-2}, \\ &\vdots \\ a_1 &= b_0 - \alpha b_1, \\ a_0 &= -\alpha b_0. \end{aligned}$$

Substitute these into the inequality:

$$|a_{n-1}| > 1 + \sum_{i=0}^{n-2} |a_i|,$$

we get:

$$|b_{n-2} - \alpha| > 1 + \sum_{i=0}^{n-3} |b_i - \alpha b_{i+1}| + |\alpha b_0|.$$

Using triangle inequality:

$$|b_{n-2}| + |\alpha| > 1 + \sum_{i=0}^{n-3} (|\alpha||b_{i+1}| - |b_i|) + |\alpha||b_0|.$$

Group terms and simplify:

$$|\alpha| - 1 > (|\alpha| - 1)\left(\sum_{i=0}^{n-2} |b_i|\right),$$

so

$$1 > \sum_{i=0}^{n-2} |b_i|.$$

Now suppose

$$x^{n-1} + \sum_{i=0}^{n-2} b_i x^i$$

has a root $\beta$ with $|\beta| > 1$. Then

$$|\beta|^{n-1} = \left| \sum_{i=0}^{n-2} b_i \beta^i \right| \leq \sum_{i=0}^{n-2} |b_i||\beta|^i \leq \left( \sum_{i=0}^{n-2} |b_i| \right) |\beta|^{n-1},$$

so

$$1 \leq \sum_{i=0}^{n-2} |b_i|.$$

contradiction.
Back to the original problem.
Suppose for contradiction that $P(x)$ is reducible in $\mathbb{Z}[x]$. Let

$$P(x) = f(x)g(x)$$

where $f, g$ are nonconstant monic polynomials with integer coefficients.
By **Vieta's Theorem**, product of roots of $f$ is positive integer, so there's a root of $f$ with modulus $\geq 1$. Similarly $g$ also has a root with modulus $\geq 1$, and hence $P$ has at least 2 roots with modulus $\geq 1$, contradiction. ■

## 3.10 Combinatorial Number Theory

### Theorem 111 *Erdös-Ginzburg-Ziv Theorem*

**Statement:**

Let $n > 1$, we can always find $n$ integers from arbitrary $2n-1$ integers such that their arithmetic mean is integer.

**Proof:** WLOG, assume

$$0 \le a_1 \le a_2 \le \cdots \le a_{2p-1} < p.$$

If there exists $1 \le i \le p-1$ such that $a_i = a_{i+p-1}$, then

$$\sum_{j=i}^{i+p-1} a_j = p\,a_i \equiv 0 \pmod{p}.$$

If for every $1 \le i \le p-1$ we have $a_i \ne a_{i+p-1}$, set

$$A_i = \{a_i,\ a_{i+p-1}\}, \quad 1 \le i \le p-1, \qquad A_p = \{a_{2p-1}\}.$$

By the Cauchy–Davenport theorem,

$$\left|\sum_{i=1}^{p} A_i\right| \ \ge\ \min\Big\{p,\ \sum_{i=1}^{p} |A_i| \ -\ (p-1)\Big\} \ =\ p.$$

Hence

$$\sum_{i=1}^{p} A_i \ =\ \mathbb{Z}_p,$$

completing the proof. ■

## 3.11 Analytic Number Theory

### Definition 79 *Riemann Zeta Function*

**Description:**

The **Riemann zeta function** $\zeta(s)$ is defined for $\Re(s) > 1$ by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

### Theorem 112 *Euler Product*

**Statement:**

For $\Re(s) > 1$,

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

**Proof:**
we set

$$\prod_p \quad \text{or} \quad \sum_p$$

asq a product or sum over prime $p$.
Every positive integer $n$ may be written uniquely as

$$n = \prod_{p \text{ prime}} p^{c_p},$$

where each exponent $c_p \geq 0$ and $c_p = 0$ for all but finitely many primes. Hence

$$\prod_p \Big( \sum_{c_p=0}^{\infty} p^{-c_p s} \Big)$$

expands formally to

$$\sum_{(c_p)} \prod_p p^{-c_p s} = \sum_{n=1}^{\infty} n^{-s},$$

since $\prod_p p^{-c_p s} = (\prod_p p^{c_p})^{-s} = n^{-s}$ and each $n$ arises exactly once. Absolute convergence for $\Re(s) > 1$ justifies this rearrangement. Finally, each factor is a geometric series:

$$\sum_{c_p=0}^{\infty} p^{-c_p s} = \frac{1}{1 - p^{-s}},$$

so

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

■

## 3.12 Algebraic Number Theory

### Definition 80 *Algebraic Number*

**Description:**

A complex number $\alpha$ is called an **algebraic number** (denoted as $\alpha \in \mathbb{A}$) if there exists a nonzero polynomial

$$P(x) \in \mathbb{Z}[x]$$

such that

$$P(\alpha) = 0.$$

If no such polynomial exists, $\alpha$ is said to be **transcendental**.

# Chapter 4

# Geometry

## 4.1 Argand Plane

***Remark:*** In this section, all points use the **same letter** to represent the corresponding complex number in the Argand Plane. The proof of unit circle version of each formula is **not** given.

### Lemma 54

**Statement:**

In the Argand Plane, if $z \in \mathbb{C}$ lies on circumference of the unit circle, then

$$\overline{z} \; = \; \frac{1}{z}.$$

**Proof:**
Since $|z| = 1$, we have $z\overline{z} = |z|^2 = 1$. Rearranging gives

$$\overline{z} = \frac{1}{z}.$$

■

### Theorem 113 *Parallelity Criterion in Argand Plane*

**Statement:**

For $A, B, C, D \in \mathbb{C}$, $AB \parallel CD$ if and only if

$$\frac{A-B}{C-D} \in \mathbb{R}.$$

*unit circle form:* If $A, B, C, D$ lie on circumference of unit circle,

$$AB = CD.$$

**Proof:**

$$AB \parallel CD \Leftrightarrow \arg(A-B) = \arg(C-D) \Leftrightarrow \arg\left(\frac{A-B}{C-D}\right) = 0 \Leftrightarrow \frac{A-B}{C-D} \in \mathbb{R}.$$

■

### Theorem 114 *Perpendicularity Criterion in Argand Plane*

**Statement:**

*Form 1:* For $A, B, C, D \in \mathbb{C}$, $AB \perp CD$ if and only if

$$\frac{A-B}{C-D} \in i\mathbb{R}.$$

*Form 2:* For $A, B, C, D \in \mathbb{C}$, $AB \perp CD$ if and only if

$$(A-B)\overline{(C-D)} \in i\mathbb{R}.$$

*unit circle form:* If $A, B, C, D$ lie on circumference of unit circle,

$$AB + CD = 0.$$

To prove *Form 1*, only need to notice that $AB \perp CD$ if and only if exits some $\alpha \in \mathbb{R}$ such that $A - B = i\alpha(C - D)$. Now we can prove *Form 2* by *Form 1*:

$$\frac{A-B}{C-D} \in i\mathbb{R} \Leftrightarrow |C-D|^2\frac{A-B}{C-D} = (A-B)\overline{(C-D)} \in i\mathbb{R}.$$

■

### Theorem 115 *Collinearity Criterion in Argand Plane*

**Statement:**

*Form 1:* For $A, B, C \in \mathbb{C}$, $A, B, C$ collinear if and only if

$$\frac{A-B}{C-B} \in \mathbb{R}.$$

*Form 2:* For $A, B, C \in \mathbb{C}$, $A, B, C$ collinear if and only if

$$\begin{vmatrix} 1 & A & \overline{A} \\ 1 & B & \overline{B} \\ 1 & C & \overline{C} \end{vmatrix} = 0.$$

*Form 3:* For $A, B, C \in \mathbb{C}$, $A, B, C$ collinear if and only if

$$(\overline{A} - \overline{B})C - (A-B)\overline{C} + A\overline{B} - \overline{A}B = 0.$$

*unit circle form:* If $A, B$ lie on circumference of unit circle,

$$C = A + B - AB\overline{C}$$

**Proof:**

*Form 1* is true by **Complex Parallelity Criterion**, notice that

$$\frac{A-B}{C-B} = \overline{\left(\frac{A-B}{C-B}\right)} \Leftrightarrow \begin{vmatrix} A-B & \overline{A}-\overline{B} \\ C-B & \overline{C}-\overline{B} \end{vmatrix} = 0.$$

then we can immediately prove *Form 2* by compute

$$\begin{vmatrix} A-B & \overline{A}-\overline{B} \\ C-B & \overline{C}-\overline{B} \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 1 & A-B & \overline{A}-\overline{B} \\ 1 & C-B & \overline{C}-\overline{B} \end{vmatrix} = \begin{vmatrix} 1 & A & \overline{A} \\ 1 & B & \overline{B} \\ 1 & C & \overline{C} \end{vmatrix} = 0.$$

and after expand the determinant we get *Form 3*. ■

## **Theorem 116** *Equation of Straight Line in Argand Plane*

**Statement:**

For $A, B \in \mathbb{C}$, the equation of straight line $AB$ is

$$(\overline{A} - \overline{B})z - (A - B)\overline{z} = \overline{A}B - A\overline{B}.$$

***Remark:*** Noted that $\overline{A}B - A\overline{B} \in i\mathbb{R}$.

**Proof:** True by **Complex Collinearity Criterion**. ■

## **Theorem 117** *Concurrency Criterion in Argand Plane*

**Statement:**

For three pairwise non parallel lines $l_1, l_2, l_3$, where $l_i : \overline{a_i}z - a_i\overline{z} = b_i$ for $i = 1, 2, 3$, then they are concurrent if and only if

$$\begin{vmatrix} a_1 & \overline{a_1} & b_1 \\ a_2 & \overline{a_2} & b_2 \\ a_3 & \overline{a_3} & b_3 \end{vmatrix} = 0.$$

**Proof:**

Noticed that $l_i$ concurrent if and only if the system of equation

$$\begin{cases} \overline{a_1}z - a_1\overline{z} = b_1, \\ \overline{a_2}z - a_2\overline{z} = b_2, \\ \overline{a_3}z - a_3\overline{z} = b_3. \end{cases}$$

has a solution $z^*$. By **Cramér's Rule**, the intersection point of $l_1, l_2$

$$z^* = \frac{\begin{vmatrix} b_1 & -a_1 \\ b_2 & -a_2 \end{vmatrix}}{\begin{vmatrix} \overline{a_1} & -a_1 \\ \overline{a_2} & -a_2 \end{vmatrix}} = \frac{\begin{vmatrix} b_1 & a_1 \\ b_2 & a_2 \end{vmatrix}}{\begin{vmatrix} \overline{a_1} & a_1 \\ \overline{a_2} & a_2 \end{vmatrix}}.$$

Then by **Complex Collinearity Criterion**, its equivalent to

$$b_3 = \overline{a_3}\frac{\begin{vmatrix} b_1 & a_1 \\ b_2 & a_2 \end{vmatrix}}{\begin{vmatrix} \overline{a_1} & a_1 \\ \overline{a_2} & a_2 \end{vmatrix}} - a_3\frac{\begin{vmatrix} -b_1 & \overline{a_1} \\ -b_2 & \overline{a_2} \end{vmatrix}}{\begin{vmatrix} a_1 & \overline{a_1} \\ a_2 & \overline{a_2} \end{vmatrix}} = \overline{a_3}\frac{\begin{vmatrix} b_1 & a_1 \\ b_2 & a_2 \end{vmatrix}}{\begin{vmatrix} \overline{a_1} & a_1 \\ \overline{a_2} & a_2 \end{vmatrix}} - a_3\frac{\begin{vmatrix} b_1 & \overline{a_1} \\ b_2 & \overline{a_2} \end{vmatrix}}{\begin{vmatrix} \overline{a_1} & a_1 \\ \overline{a_2} & a_2 \end{vmatrix}}$$

since $b_i \in i\mathbb{R}$. Multiply the denominator to both side yield

$$0 = \overline{a_3}\begin{vmatrix} b_1 & a_1 \\ b_2 & a_2 \end{vmatrix} - a_3\begin{vmatrix} b_1 & \overline{a_1} \\ b_2 & \overline{a_2} \end{vmatrix} - b_3\begin{vmatrix} \overline{a_1} & a_1 \\ \overline{a_2} & a_2 \end{vmatrix} = \begin{vmatrix} a_1 & \overline{a_1} & b_1 \\ a_2 & \overline{a_2} & b_2 \\ a_3 & \overline{a_3} & b_3 \end{vmatrix}.$$

■

### Theorem 118 *Complex Parallelogram*

**Statement:**

For $A, B, C, D \in \mathbb{C}$, $ABCD$ is a parallelogram if and only if

$$A + C = B + D.$$

**Proof:** $\overrightarrow{AB} = \overrightarrow{DC} \Leftrightarrow A - B = D - C.$ ■

### Theorem 119 *Complex Midpoint*

**Statement:**

For $A, B \in \mathbb{C}$, then $C$ is midpoint of segment $AB$ if and only if

$$C = \frac{A + B}{2}.$$

**Proof:** Let $D = A + B$, consider Parallelogram $OADB$, since midpoint of $AB$ intercept midpoint of $OD$, then midpoint of $AB = \dfrac{D}{2} = \dfrac{A + B}{2}$. ■

### Theorem 120 *Equation of Perpendicular Bisector in Argand Plane*

**Statement:**

For $A, B \in \mathbb{C}$, the equation of perpendicular bisector of segment $AB$ is

$$(\overline{A} - \overline{B})z + (A - B)\overline{z} = |A|^2 - |B|^2.$$

**Proof:**
Let the perpendicular bisector of segment $AB$ be $l$, then its normal vector will be $A - B$ which means the vector $(A - B)i$ has the same direction with $l$. Also remember that $l$ pass through $\frac{A+B}{2}$, then by **Equation of Straight Line in Argand Plane**,

$$-i(\overline{A} - \overline{B})z - i(A - B)\overline{z} = -i(\overline{A} - \overline{B})\left(\frac{A + B}{2}\right) - i(A - B)\left(\frac{\overline{A} + \overline{B}}{2}\right)$$

$$\Leftrightarrow (\overline{A} - \overline{B})z + (A - B)\overline{z} = |A|^2 - |B|^2.$$

■

### Theorem 121 *Complex Reflection Over a Line Formula*

**Statement:**

For $X, X', A, B \in \mathbb{C}$, then $X'$ is the reflection of $X$ over line $AB$ if and only if

$$X' = \frac{(A-B)\overline{X} + \overline{A}B - A\overline{B}}{\overline{A} - \overline{B}}.$$

*unit circle form:* If $A, B$ lie on circumference of unit circle,

$$X' = A + B - AB\overline{X}.$$

**Proof:** Noticed that $\dfrac{X'-A}{A-B} = \overline{\left(\dfrac{X-A}{A-B}\right)}$. After arrangement give us the desired. ■

## Theorem 122 *Foot of Altitude in Argand Plane*

**Statement:**

For $X, F, A, B \in \mathbb{C}$, then $F$ is the foot of altitude of $X$ to line $AB$ if and only if

$$F = \frac{(\overline{A} - \overline{B})X + (A-B)\overline{X} + \overline{A}B - A\overline{B}}{2(\overline{A} - \overline{B})}.$$

*unit circle form:* If $A, B$ lie on circumference of unit circle,

$$F = \frac{1}{2}(X + A + B - AB\overline{X}).$$

**Proof:** It's obvious by **Complex midpoint** and **Complex Reflection Over a Line Formula** because $F$ is the midpoint of segment $XX'$. ■

## Theorem 123 *Intersection in Argand Plane*

**Statement:**

For $A, B, C, D, P \in \mathbb{C}$, $P$ is the intersection point of line $AB$ and line $CD$ if and only if

$$P = \frac{(\overline{A}B - A\overline{B})(C-D) - (A-B)(\overline{C}D - C\overline{D})}{(\overline{A} - \overline{B})(C-D) - (A-B)(\overline{C} - \overline{D})}.$$

*unit circle form:* If $A, B, C, D$ lie on circumference of unit circle,

$$P = \frac{AB(C+D) - CD(A+B)}{AB - CD}.$$

**Proof:**
Recall that the **equation of the straight line** through $A, B \in \mathbb{C}$ may be written in the form

$$(\overline{A} - \overline{B})\, z - (A-B)\, \overline{z} = \overline{A}B - A\overline{B}.$$

Thus the intersection $P$ of lines $AB$ and $CD$ is the unique solution $z = P$ of the simultaneous system

$$\begin{cases} (\overline{A} - \overline{B})\, z - (A - B)\, \overline{z} = \overline{A}B - A\overline{B}, \\ (\overline{C} - \overline{D})\, z - (C - D)\, \overline{z} = \overline{C}D - C\overline{D}. \end{cases}$$

By **Cramer’ s rule** the solution for $z$ is

$$P = \frac{\begin{vmatrix} \overline{A}B - A\overline{B} & A - B \\ \overline{C}D - C\overline{D} & C - D \end{vmatrix}}{\begin{vmatrix} \overline{A} - \overline{B} & A - B \\ \overline{C} - \overline{D} & C - D \end{vmatrix}} = \frac{(\overline{A}B - A\overline{B})(C - D) - (A - B)(\overline{C}D - C\overline{D})}{(\overline{A} - \overline{B})(C - D) - (A - B)(\overline{C} - \overline{D})}.$$

■

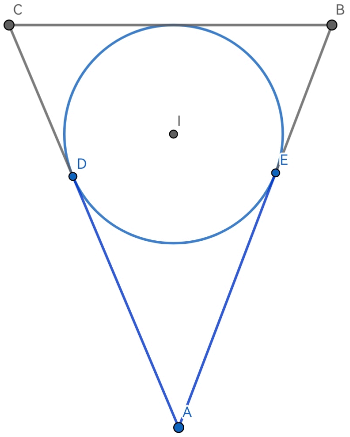
## Theorem 124 *Ice Cream Cone Formula*

**Statement:**

For $A, B, C \in \mathbb{C}$, if the incircle of $\triangle ABC$ is the unit circle, and $AC, AB$ tangent to it at $D, E$ respectively, then

$$A = \frac{2DE}{D + E}.$$

**Proof:** Applying unit circle form of **Complex Intersection Formula** by setting the lines as $DD$ and $EE$. ■



## Theorem 125 *Complex Shoelace Formula*

**Statement:**

Let $A, B, C \in \mathbb{C}$ with affixes $a, b, c$. The signed area $[\Delta ABC]$ of triangle $ABC$ may be written in two equivalent forms:
*Form 1:*

$$[\triangle ABC] = \frac{i}{4}\begin{vmatrix} 1 & a & \overline{a} \\ 1 & b & \overline{b} \\ 1 & c & \overline{c} \end{vmatrix}.$$

*Form 2:*

$$[\triangle ABC] = \frac{1}{2}\,\Im\big(\overline{a}b + \overline{b}c + \overline{c}a\big).$$

**Proof:**
Consider $\overrightarrow{OP} := x + yi, \overrightarrow{OQ} := u + vi$, then the directed area of the parallelogram with side $OP$ and $OQ$ will be $xv - yu = \Im(\overline{P}Q)$, so $[\triangle OPQ] = \dfrac{1}{2}\Im(\overline{P}Q)$. Hence, we have

$$[\triangle ABC] = \sum_{cyc}[\triangle OAB] = \frac{1}{2}\Im\left(\sum_{cyc}\overline{a}b\right),$$

so we solved *Form 2*.
Expanding the $3 \times 3$ determinant in *Form 1* along the first column gives

$$\begin{vmatrix} 1 & a & \overline{a} \\ 1 & b & \overline{b} \\ 1 & c & \overline{c} \end{vmatrix} = a\,\overline{b} + b\,\overline{c} + c\,\overline{a} - a\,\overline{c} - b\,\overline{a} - c\,\overline{b}.$$

Multiplying by $\frac{i}{4}$ and using $i(z - \overline{z}) = 2\,\Im(z)$ yields

$$\frac{i}{4}\Big(a\,\overline{b} + b\,\overline{c} + c\,\overline{a} - a\,\overline{c} - b\,\overline{a} - c\,\overline{b}\Big) = \frac{1}{2}\Im\big(\overline{a}b + \overline{b}c + \overline{c}a\big),$$

which is exactly *Form 2*. ■

## Theorem 126 *Complex Similar Triangles*

**Statement:**

Let $A, B, C, D, E, F \in \mathbb{C}$. The triangles $\triangle ABC$ and $\triangle DEF$ are directly similar if and only if

$$\begin{vmatrix} 1 & A & D \\ 1 & B & E \\ 1 & C & F \end{vmatrix} = 0.$$

Moreover, $\triangle ABC$ is opposite-similar to $\triangle DEF$ (mirror image) if and only if

$$\begin{vmatrix} 1 & A & \overline{D} \\ 1 & B & \overline{E} \\ 1 & C & \overline{F} \end{vmatrix} = 0.$$

## Theorem 127 *Complex Circumcenter*

**Statement:**

For $A, B, C \in \mathbb{C}$, the circumcenter of $(ABC)$ is

$$O_{\triangle ABC} = \frac{\begin{vmatrix} 1 & A & |A|^2 \\ 1 & B & |B|^2 \\ 1 & C & |C|^2 \end{vmatrix}}{\begin{vmatrix} 1 & A & \overline{A} \\ 1 & B & \overline{B} \\ 1 & C & \overline{C} \end{vmatrix}}.$$

## Theorem 128 *Complex Centroid*

**Statement:**

For $A, B, C \in \mathbb{C}$, the centroid of $\triangle ABC$ is

$$G = \frac{A+B+C}{3}.$$

## Theorem 129 *Complex Incenter*

**Statement:**

For $A, B, C \in \mathbb{C}$, let $A = a^2, B = b^2, C = c^2$, then the incenter of $\triangle ABC$ is

$$I = -\sum_{cyc} ab.$$

## Theorem 130 *Complex Center of Nine Point Circle*

**Statement:**

For $A, B, C \in \mathbb{C}$, if $(ABC)$ is unit circle, then the center of nine point circle of $\triangle ABC$ is

$$n_9 = \frac{A+B+C}{2}.$$

## Theorem 131 *Concyclic Criterion in Argand Plane*

**Statement:**

$A, B, C, D \in \mathbb{C}$, are concyclic if and only if

$$\frac{A-B}{C-B} \cdot \frac{C-D}{A-D} \in \mathbb{R}.$$

**Theorem 132** *Complex Equilateral Triangle*

**Statement:**

For $A, B, C \in \mathbb{C}$, $\triangle ABC$ is equilateral if and only if

$$A^2 + B^2 + C^2 = AB + BC + CA.$$

# Chapter 5

# Advance Math

## 5.1 Real Analysis

### Theorem 133 *L' Hôpital' s Rule*

**Statement:**

Let $f, g \in C^1((a,b))$ and suppose $g'(x) \neq 0$ for all $x \in (a,b)$. Let $c$ be a point in $[a,b]$ (or a finite endpoint) such that

$$\lim_{x\to c} f(x) = \lim_{x\to c} g(x) = 0 \quad \text{or} \quad \lim_{x\to c} f(x) = \lim_{x\to c} g(x) = \pm\infty.$$

If

$$L \ = \ \lim_{x\to c} \frac{f'(x)}{g'(x)}$$

exists (finite or infinite), then

$$\lim_{x\to c} \frac{f(x)}{g(x)} \ = \ L.$$

**Proof:**
We give the classical proof in the 0/0 case; the $\infty/\infty$ case is analogous. For $x \neq c$ in $(a,b)$, since $f(c) = g(c) = 0$, by Cauchy' s Mean Value Theorem there exists $\xi$ between $x$ and $c$ such that

$$\frac{f(x) - f(c)}{g(x) - g(c)} = \frac{f'(\xi)}{g'(\xi)}.$$

Hence

$$\frac{f(x)}{g(x)} = \frac{f'(\xi)}{g'(\xi)}.$$

As $x \to c$, we have $\xi \to c$, so by the hypothesis $\lim_{x\to c} f'(x)/g'(x) = L$, therefore

$$\lim_{x\to c} \frac{f(x)}{g(x)} = \lim_{x\to c} \frac{f'(\xi)}{g'(\xi)} = L.$$

■