离散数学

(229001.01)

教师：**邵帅，王超**

于 2025 年秋

目录

离散数学概述

研究对象：离散

离散数学的研究对象是**离散**的数学结构，主要包括以下几个方面：

1. **有限/可数 → 集合**
   离散数学从具体的对象出发，逐渐进行抽象化处理。我们主要研究有限集合和可数集合，这些集合中的元素是分离的、不连续的。

2. **对象间存在关系 → 特殊：二元关系**
   在离散数学中，我们不仅研究单个对象，更重要的是研究对象之间的关系。其中，二元关系是最常见和最重要的关系类型。

3. **常见离散对象**：
   (a) **整数 → 数论 → 代数结构**
   (b) **图 → 图论**

研究内容：满足一定条件

1. **有没有：存在性/构造性**
   研究在给定条件下是否存在满足要求的对象，以及如何构造这样的对象。
   典型例子：抽屉原理、图染色问题

2. **有多少：计数/唯一性**
   研究满足条件的对象有多少个，以及这些对象是否唯一。
   典型例子：排列组合、容斥原理、Möbius 反演

3. **找最优：优化问题**
   在满足条件的对象中寻找最优解。
   典型例子：最优数问题、最大匹配（完美匹配）

通过本课程的学习，我们将掌握离散数学的基本思想和方法，为后续的计算机科学、密码学、算法设计等领域打下坚实的数学基础。

1 抽屉原理

1.1 抽屉原理

定理 1.1.1 抽屉原理

将 $n+1$ 个物品放入 n 个抽屉中，那么一定存在一个抽屉中至少放 2 个物品。

问题 1.1.1

任意 $n+1$ 个正整数，一定存在两个数，模 n 同余。

证明： 构造抽屉：模 n 同余的数放入同一个抽屉。则一共有 n 个抽屉。

将 $n+1$ 个正整数放入 n 个抽屉中，那么一定存在一个抽屉中至少有两个数。即一定存在两个数，模 n 同余。

问题 1.1.2

$a_1, a_2, \ldots, a_n \in N$，证 $\exists k \neq l \in [n], s.t. \sum_{i=k}^{l} a_i$ 是 n 的倍数。

证明： 这里依然有明显的 n 个抽屉，关键就是怎么找到 $n+1$ 个数。但是条件只给了 n 个数，这个时候我们就要引入一个平凡的 0 来凑数。

考虑部分和序列：

$$
\begin{aligned}
S_0 &= 0 \\
S_1 &= a_1 \\
S_2 &= a_1 + a_2 \\
&\vdots \\
S_n &= a_1 + a_2 + \cdots + a_n
\end{aligned}
$$

我们构造了 $n+1$ 个部分和：$S_0, S_1, S_2, \ldots, S_n$。

将这 $n+1$ 个数按照模 n 的余数分类，由于只有 n 个可能的余数 $(0, 1, 2, \ldots, n-1)$，根据抽屉原理，必然存在两个不同的部分和 S_t 和 S_l（其中 $0 \leq t < l \leq n$）使得：

$$S_l \equiv S_t \pmod{n}$$

即：$S_l - S_t \equiv 0 \pmod{n}$，也就是 $n \mid (S_l - S_t)$。

注意到：

$$S_l - S_t = (a_1 + \cdots + a_l) - (a_1 + \cdots + a_t) = a_{t+1} + a_{t+2} + \cdots + a_l$$

令 $k=t+1$，则有 $1\le k\le l\le n$，且：

$$n \mid \sum_{i=k}^{l} a_i$$

问题 1.1.3

某同学每天至少玩一局游戏，但每周最多玩 *12* 局游戏。他一共玩了 *77* 天。证明：一定存在若干连续的天数，在这几天中他一共玩了 *21* 场游戏。

证明： 设 a_i 表示该同学在第 i 天玩的游戏场次，其中 $i=1,2,\ldots,77$。根据题意，我们有以下条件：

1. 每天至少玩一局游戏：$a_i\ge 1$ 对所有 $i\in\{1,2,\ldots,77\}$ 成立。
2. 每周最多玩 *12* 局游戏：对任意连续的 *7* 天（即对任意 k 使得 $1\le k\le 71$），有 $\sum_{i=k}^{k+6} a_i\le 12$。

我们需要证明存在整数 k,l 使得 $1\le k\le l\le 77$ 且 $\sum_{i=k}^{l} a_i=21$。

法 *1* 构造前缀和序列 S_j：设 $S_0=0$。对 $j=1,2,\ldots,77$，定义 $S_j=\sum_{i=1}^{j} a_i$。由于 $a_i\ge 1$，这个前缀和序列是严格递增的：$0=S_0<S_1<S_2<\ldots<S_{77}$。

现在我们考虑以下两组共 $2\times 78=156$ 个数：

- 集合 $A=\{S_0,S_1,\ldots,S_{77}\}$
- 集合 $B=\{S_0+21,S_1+21,\ldots,S_{77}+21\}$

这些数都在一个有限的范围内：

- 最小值：$S_0=0$。
- 最大值：S_{77} 是 *77* 天内玩游戏的总场次。由于 *77* 天是 *11* 周，且每周最多玩 *12* 局，所以 $S_{77}\le 11\times 12=132$。因此，集合 B 中的最大值为 $S_{77}+21\le 132+21=153$。

所以，所有这 *156* 个数都落在区间 $[0,153]$ 内。这个区间包含 $153-0+1=154$ 个不同的整数值。

根据抽屉原理，由于我们有 *156* 个数要放入 *154* 个”抽屉”（即可能的整数值），因此至少有两个数是相等的。

由于序列 S_j 是严格递增的，所以集合 A 中的所有数都互不相同。同理，集合 B 中的所有数也互不相同。因此，相等的两个数必然一个来自集合 A，另一个来自集合 B。即，存在 k,l 使得 $S_l=S_k+21$。

由于 $S_l = S_k + 21$ 且 S_j 是严格递增的，所以 $S_l > S_k$，这蕴含着 $l > k$。因此，我们可以找到 k, l 满足 $0 \le k < l \le 77$，使得：

$$S_l - S_k = \sum_{i=k+1}^{l} a_i = 21$$

所以，存在连续的天数从第 $k+1$ 天到第 l 天，在这段时间内玩的游戏总场次恰好是 *21* 场。

法 2 条件 $\sum_{i=k}^{l} a_i = 21$ 可以转化为 $21 \mid \sum_{i=k}^{l} a_i$ 且 $\sum_{i=k}^{l} a_i < 21 \times 2 = 42$。

如果一个指标集 S 的基大于 *21*，那么 $\sum_{i \in S} a_i > 21$。所以我们考虑某部分和的时候，需要保证其指标集的基小于等于 *21*（为连续 *3* 周）。

取 $l_0 - k_0 + 1 = 21$（$|S| = 21$），则有：

$$21 \le \sum_{i=k_0}^{l_0} a_i \le 12 \times 3 = 36 < 21 \times 2 = 42$$

其中 a_i 共有 *21* 个数，根据上题结论，其中存在连续几个数可以被 *21* 整除，且这几个数之和小于 *42*，所以存在 $k_0 \le k < l \le l_0$ 使得 $\sum_{i=k}^{l} a_i = 21$。

问题 1.1.4 更一般的情况

$a_i \ge 1$ 对所有 $i \in [77]$，且 $\sum_{i=t}^{t+6} a_i \le 12$ 对所有 $t \in [71]$。若存在 $1 \le k \le l \le 77$ 使得 $\sum_{i=k}^{l} a_i = m$ 的 m 的取值范围。

证明： 参考上述法 *2* 的思路，寻找一个连续区间使得其和满足：

$$m \le \sum_{i=k_0}^{l_0} a_i < 2m$$

为了构造这样的区间，我们采用以下策略：

- 尽量选择整周（*7* 天）的区间，整周最多能玩 *12* 局游戏
- 对于去除前面几整周剩余的天数，尽力多打游戏

例如，m=*22* 时，考虑 $22 = 3 \times 7 + 1$，则至多打游戏 $3 \times 12 + (12 - 6) = 42 < 22 \times 2 = 44$。

这个求和的上界为 $12 \times (m \mod 7) + (12 - m\%7)$，简化起见我们可以取 $\frac{12}{7}m + 5$（当然这个表达式可以再优化），

则要满足：

$$m \le \frac{12}{7}m + 5 < 2m \Rightarrow m > \frac{35}{2} = 17.5$$

则只要 $18 \le m \le 77$，均有连续几天，共打 m 局游戏。

1.2 构造抽屉的两个角度

在应用抽屉原理时，我们可以从两个不同的角度来构造抽屉：

1. **优化的角度**
2. **反问题的角度**

问题 1.2.1

一个边长为 1 的正方形中任取 5 个点，则它们之间一定存在两点，其距离小于 m，问 m 最小是多少？

方法一：直接构造抽屉 将边长为 1 的正方形 S 平均分成四个边长为 $\frac{1}{2}$ 的小正方形 S_1, S_2, S_3, S_4。

S_3	S_4
S_1	S_2

根据抽屉原理，如果在大正方形中任意取 5 个点，至少有一个小正方形中包含至少 2 个点。

在边长为 $\frac{1}{2}$ 的小正方形中，任意两点之间的最大距离是其对角线长度：

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

因此，$m \leq \frac{\sqrt{2}}{2}$。

为了证明 $m=\frac{\sqrt{2}}{2}$ 是最小值，我们构造一个反例：将 4 个点放在大正方形的四个顶点，第 5 个点放在正方形中心。此时，任意两点之间的最小距离恰好是 $\frac{\sqrt{2}}{2}$。

因此，m 的最小值为 $\frac{\sqrt{2}}{2}$。

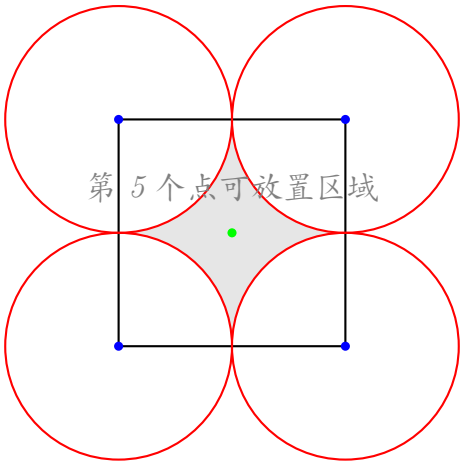
方法二：优化的角度 这个问题可以看作一个优化问题：最大化所有点对中最小距离的值，即

$$\max\left\{\min_{i\neq j} d(x_i,x_j) : x_1,x_2,x_3,x_4,x_5 \in S\right\}$$

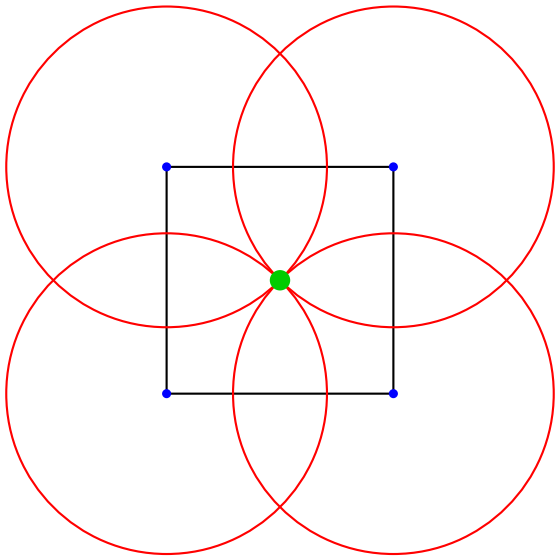
选出最短距离并加强短板

考虑将 4 个点放在正方形的四个顶点上，此时这四个点尽可能分散了，然后再来考虑第五个点的位置。

以四个顶点为圆心画半径为 r 的圆，将第五个点取在正方形内圆外的地方：



优化上述半径至 $\frac{\sqrt{2}}{2}$，此时第五个点只能取在正方形中心：



此时所有点对中的最小距离为 $\frac{\sqrt{2}}{2}$。

同上可以证明 $\frac{\sqrt{2}}{2}$ 就是最小值。

问题 1.2.2

从 *1* 到 *200* 中选取 m 个数，使得其中必存在两个数 a,b 满足 $a \mid b$ 或 $b \mid a$。问 m 的最小值是多少？

解： **反问题：**从 *1* 到 *200* 中选取若干个数，使得其中任意两个数都不存在整除关系。问最多能选取多少个数？

根据抽屉原理，构造尽可能多的抽屉，设为 k 个，其中每个抽屉内部两两之间均存在整除关系，当选取 $k+1$ 个数时，必然存在两个数满足整除关系。

针对上述**整除关系**，如果我们要多个数之间两两都存在整除关系，则可以选择一个基因子，任意两个数之间的倍数为这个基因子的幂。

例如选择基因子是 *2*，一个抽屉的代表元选作 *3*，则该抽屉中所有数为 $3, 6, 12, 24, 48, 96, 192$。

显然，基因子越小，抽屉能取的越多，所以选择基因子为 *2* 来**构造抽屉：**对于每个奇数 $x \in \{1, 3, 5, \ldots, 199\}$，构造抽屉 D_x：

$$D_x = \{x \cdot 2^k : k \geq 0, x \cdot 2^k \leq 200\}$$

即每个抽屉包含以某个奇数为”基因子”的所有 *2* 的幂次倍数。

示例：

- $D_{25} = \{25, 50, 100, 200\}$（因为 $25 \cdot 2^0 = 25, 25 \cdot 2^1 = 50, 25 \cdot 2^2 = 100, 25 \cdot 2^3 = 200$）
- $D_{49} = \{49, 98, 196\}$（因为 $49 \cdot 2^0 = 49, 49 \cdot 2^1 = 98, 49 \cdot 2^2 = 196$）
- $D_{99} = \{99, 198\}$（因为 $99 \cdot 2^0 = 99, 99 \cdot 2^1 = 198$）
- $D_{197} = \{197\}$（因为 $197 \cdot 2^0 = 197$，但 $197 \cdot 2^1 = 394 > 200$）

抽屉数量：奇数 $1, 3, 5, \ldots, 199$ 共有 $\frac{199-1}{2} + 1 = 100$ 个，因此构造了 *100* 个抽屉。

为了确保选取的数中任意两个都不存在整除关系，必须从每个抽屉中最多选取 *1* 个数。

因此，最多能选取 *100* 个数。一个具体的例子是 $\{101, 102, 103, \ldots, 200\}$

根据抽屉原理，当选取 $m = 100 + 1 = 101$ 个数时，必然有至少两个数落在同一个抽屉中，从而存在整除关系。

因此，m 的最小值为 *101*。

1.3 抽屉原理的其他形式

下面考虑将其推广到更一般的情况上:

命题 1.3.1 抽屉原理的一般形式

给定 n 个实数 $a_1, a_2, \ldots, a_n \in \mathbb{R}$. 若有 $\sum_{i=1}^{n} a_i = M$, 则:

1. 存在 i, 满足 $a_i \geq \frac{M}{n}$;
2. 存在 j, 满足 $a_j \leq \frac{M}{n}$.

证明: 对于 1, 使用反证法: 如果 $\forall i \in [n]$, 都有 $a_i < \frac{M}{n}$, 则有 $\sum_{i=1}^{n} a_i < M$, 矛盾.

2 的证明与之类似.

将引理 1.2 的情况限制到整数上, 则得到如下命题:

命题 1.3.2

给定 n 个整数 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. 若有 $\sum_{i=1}^{n} a_i = M$, 则:

1. 存在 i, 满足 $a_i \geq \lceil \frac{M}{n} \rceil$;
2. 存在 j, 满足 $a_j \leq \lfloor \frac{M}{n} \rfloor$.

证明: 对于 1, 直接根据引理 1.2 得到 $\exists i$ s.t. $a_i \geq \frac{M}{n}$. 由于 a_i 为整数, 故有 $a_i \geq \lceil \frac{M}{n} \rceil$.

2 的证明与之类似.

命题 1.3 的直观理解: 在 n 个抽屉中放入 M 只物品, 则必有至少一个抽屉, 其中有至少 $\lceil \frac{M}{n} \rceil$ 只物品. 从这个角度出发, 显然抽屉原理是强抽屉原理在 $M = n + 1$ 时的推论.

命题 1.3.3

给定 n 个实数 $a_1, a_2, \ldots, a_n \in \mathbb{R}$, 以及 n 个实数 $x_1, x_2, \ldots, x_n \in \mathbb{R}$. 若有 $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} x_i$, 则:

1. 存在 i, 满足 $a_i \geq x_i$;
2. 存在 j, 满足 $a_j \leq x_j$.

证明:

与命题 1.2 的证明类似, 运用反证法: 假设 $\forall i \in [n]$, 都有 $a_i < x_i$, 则有 $\sum_{i=1}^{n} a_i < \sum_{i=1}^{n} x_i$, 矛盾.

2 的证明与之类似.

同样将命题 1.4 的情况限制到整数上:

命题 1.3.4

给定 n 个整数 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, 以及 n 个整数 $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. 若有 $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} x_i$, 则:

1. 存在 i, 满足 $a_i \geq x_i$;
2. 存在 j, 满足 $a_j \leq x_j$.

同样可以直观地理解命题 1.5: 如果将 M 只物品放进 n 个抽屉里, 且有 $M = \sum_{i=1}^{n} x_i$, 则不可能每个抽屉中的物品数都少于对应的 x_i.

通过将实数上成立的命题 1.4 限制在整数上得到命题 1.5, 其给出的界是紧的吗?

通过尝试不难观察发现, 要使得每个抽屉中的物品数都少于对应的 x_i 即至多为 $x_i - 1$, 则总物品数至多为 $\sum_{i=1}^{n}(x_i - 1) = \sum_{i=1}^{n} x_i - n$. 换言之, 只要 $M \geq \sum_{i=1}^{n} x_i - n + 1$, 则必有至少某个抽屉中的物品数达到对应的 x_i. 此即所谓强抽屉原理:

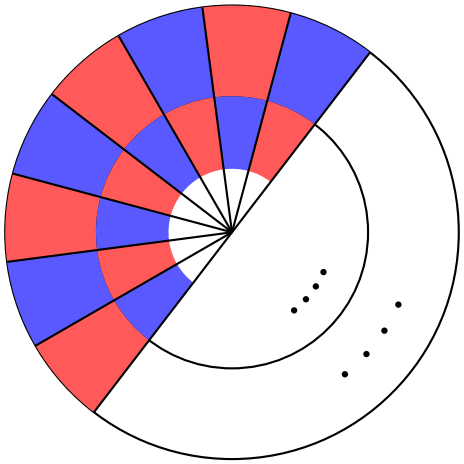
命题 1.3.5 (强抽屉原理)

给定 n 个整数 $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, 以及 n 个整数 $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. 若有 $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} x_i - n + 1$, 则存在 i, 满足 $a_i \geq x_i$;

1.4 抽屉原理的应用

问题 1.4.1

如图 *1* 所示，有大小两个圆盘，圆心重合，都被等分为 *200* 个扇形/扇环区域. 大圆盘可以转动，且转动的每个角度必定使小圆盘的每个区域恰与大圆盘的某个区域对齐. 已知大圆盘上有 *100* 个区域被涂成蓝色，另外 *100* 个区域被涂成红色；小圆盘上也有 *100* 个区域被涂成蓝色，另外 *100* 个区域被涂成红色. 证明：固定染色方案后，存在某个转动状态，使得大小圆盘的对应区域颜色相同的数量至少有 *100* 个.



每个圆盘都被等分为 200 个扇形区域；大圆盘可转动，小圆盘固定

证明： **问题转化：** 用 $a_1, a_2, ..., a_{200} \in \{-1, 1\}$ 和 $b_1, b_2, ..., b_{200} \in \{-1, 1\}$ 分别表示大小圆盘上 *200* 个内层扇形/外层扇环的颜色. 由此，第 i 个等分位上大小圆盘的区域颜色相同，当且仅当 $ai \cdot bj = 1$；同样，第 i 个等分位上大小圆盘的区域颜色不同，当且仅当 $ai \cdot bj = -1$.

将大圆盘顺时针转动 i 个单位后，大小圆盘的扇形的对应关系将从

$$\begin{matrix} a_1 & a_2 & \dots & a_{200} \\ b_1 & b_2 & \dots & b_{200} \end{matrix}$$

变化为

$$\begin{matrix} a_1 & a_2 & \dots & a_{200} \\ b_{i+1} & b_{i+2} & \dots & b_{i+200} \end{matrix}$$

(这里默认 $b_{i+200} = b_i, \forall i \in [200]$.)

则待证命题转化为，存在某个 i，使得 $P_i = \sum_{k=1}^{n} (a_i b_{k+i}) \geq 0$. 这是因为如果至少有 100 个位置上对应区域颜色相同，则这 200 项中应有至少 100 个 1，以及至多 100 个 -1.

将大圆盘分别顺时针转动 *1* 格,*2* 格,...,*200* 格 *(等效于不转动)*，则分别可以得到：

$$
\begin{aligned}
P_1 &= \sum_{k=1}^{200}(a_k b_{k+1}) = a_1b_2 + a_2b_3 + \ldots + a_{200}b_1 \\
P_2 &= \sum_{k=1}^{200}(a_k b_{k+2}) = a_1b_3 + a_2b_4 + \ldots + a_{200}b_2 \\
&\ldots \\
P_i &= \sum_{k=1}^{200}(a_k b_{k+i}) = a_1b_{i+1} + a_2b_{i+2} + \ldots + a_{200}b_i \\
&\ldots \\
P_{200} &= \sum_{k=1}^{200}(a_k b_k) = a_1b_1 + a_2b_2 + \ldots + a_{200}b_{200}
\end{aligned}
$$

根据题意，我们有：

$$
\begin{aligned}
\sum_{i=1}^{200} P_i &= \sum_{1\le i\le 200, 1\le k\le 200} a_i b_{i+k} \\
&= \sum_{1\le i\le 200, 1\le j\le 200} a_i b_j \\
&= (\sum_{i=1}^{200} a_i)(\sum_{j=1}^{200} b_i) \\
&= 0
\end{aligned}
$$

由命题 *1.5*，存在某个 i 使得 $P_i \ge 0$. 这就完成了原命题的证明.

问题 1.4.2

n^2+1 个互异的数构成的数列中，一定存在长为 $n+1$ 的递增子列或长为 $n+1$ 的递减子列。

证明：先枚举几个 n 比较小的例子：

1. $n=1$：序列有 $1^2+1=2$ 个数，显然存在长为 2 的递增或递减子列。
2. $n=2$：序列有 $2^2+1=5$ 个数，前两个大小顺序不影响后续讨论，直接设 $a_1 < a_2$。讨论第三个点：
   (a) 若 $a_3 > a_2$，则存在长为 3 的递增子列 a_1, a_2, a_3。

(b) 若 $a_1 < a_3 < a_2$，此时以 a_3 结尾有一个长为 2 的递增子列 a_1, a_3，还有一个长为 2 的递减子列 a_2, a_3，再增加一个点 a_4，若 $a_4 > a_3$，则存在长为 3 的递增子列 a_1, a_3, a_4，若 $a_4 < a_3$，则存在长为 3 的递减子列 a_2, a_3, a_4。

(c) 若 $a_3 < a_1$，再添加一个点 a_4：

i. 若 $a_4 > a_2$，则存在长为 3 的递增子列 a_1, a_2, a_4

ii. 若 $a_4 < a_3$，则存在长为 3 的递减子列 a_1, a_3, a_4，

iii. 若 $a_3 < a_4 < a_2$，则此时的 a_2, a_3, a_4 就同上面第二种情况中的 a_1, a_2, a_3 一样，再添加一个点，总会出现长为 3 的递增或递减子列。

原目标： 在 n^2+1 的序列中找到长为 $n+1$ 的递增或递减子序列。

转化目标： 在 n^2 的序列中找到一项，以该项为结尾存在长为 n 的递增和递减子序列。

前提： 在这 n^2 的序列中暂时不存在长为 $n+1$ 的递增或递减子序列。

法一（构造一一映射） 考虑每一项 a_i，找出以 a_i 结尾的最长的递增和递减子序列。

对每个 a_i，定义有序对 (m_i, n_i)：

- m_i：以 a_i 结尾的最长递增子序列的长度
- n_i：以 a_i 结尾的最长递减子序列的长度

前面已经假设不存在长为 $n+1$ 的递增或递减子序列，所以 $1 \le m_i \le n$，$1 \le n_i \le n$。

构造一一映射： 每个 (m_i, n_i) 有序对可以看作是从 $n \times n$ 网格中的一个点，其中 m_i 表示行，n_i 表示列。

推论 1.4.1

将 n 只物品放入 n 个抽屉中，若不存在某个抽屉放了至少两只物品，则一定是每个抽屉恰好放了一只物品。换句话说，给定两个有限集合 A, B 满足 $|A| = |B| = n$, 对于一个从 A 到 B 的映射 $f : A \to B$, 如果 f 是单射或满射, 则一定是双射.

反证： 假设存在 $i \neq j$ 使得 $(m_i, n_i) = (m_j, n_j)$。

1. 若 $a_i > a_j$: 由于 $n_i = n_j$，以 a_i 结尾的最长递减子序列长度为 n_i，将 a_j 添加到以 a_i 结尾的长度为 n_i 的递减子序列前面，得到以 a_j 结尾的长度为 n_i+1 的递减子序列。这与 n_j 是 a_j 结尾的最长递减子序列长度矛盾

2. 若 $a_i < a_j$: 由于 $m_i = m_j$，以 a_i 结尾的最长递增子序列长度为 m_i，将 a_j 添加到以 a_i 结尾的长度为 m_i 的递增子序列后面，得到以 a_j 结尾的长度为 m_i+1 的递增子序列。这与 m_j 是 a_j 结尾的最长递增子序列长度矛盾

两种情况都与原假设矛盾，因此每个 (m_i, n_i) 各不相同。

由于 $1 \le m_i \le n$，$1 \le n_i \le n$，所以 (m_i, n_i) 的可能取值只有 $n \times n = n^2$ 种。根据抽屉原理，存在某个 k 使得 $(m_k, n_k) = (n, n)$，即：

- 以 a_k 结尾的最长递增子序列长度为 n
- 以 a_k 结尾的最长递减子序列长度为 n

此时再添加一个点，总能得到长为 $n+1$ 的递增或递减子序列。

法二（归纳）

将原目标转化为证明在 n^2 个互异数中，一定存在一项，以该项结尾存在长为 n 的递增和递减子序列。

（假设前提：在这 n^2 个数中暂时不存在长为 $n+1$ 的递增或递减子列）

归纳基础： $n = 1$ 时，命题显然成立（两个不同的数必构成长度为 2 的单调子列）。

归纳假设： 设对某个 $n \ge 1$ 命题成立，即任意 n^2 个互异数的序列，都含有长为 n 的递增子列和递减子列。

归纳目标： 证明对 $n+1$ 也成立。也就是：任意 $(n+1)^2$ 个互异数的序列，都含有长为 $n+1$ 的递增子列和递减子列。

设给定序列为 $a_1, a_2, \ldots, a_{(n+1)^2}$。若前 $(n+1)^2$ 项中已经存在长为 $n+2$ 的递增/递减子列，则命题成立。于是我们只需考虑前 $(n+1)^2$ 项中没有长为 $n+2$ 的单调子列的情形。

先拿出前 n^2+1 个数，根据归纳假设，其中存在一项 a_{i_1}，以该项结尾存在长为 $n+1$ 的递增子列或递减子列，记做 l_1。

我们还有 $(n+1)^2 - (n^2+1) = 2n$ 个数，我们去掉上述的 a_{i_1}，然后再添上一项，又有 n^2+1 个数，再根据归纳假设，其中存在一项 a_{i_2}，以该项结尾存在长为 $n+1$ 的递增子列或递减子列 l_2。

以此类推我们可以得到 $2n+1$ 项，$a_{i_1}, a_{i_2}, \ldots, a_{i_{2n+1}}$，其中每一项 a_{i_k}，以该项结尾存在长为 $n+1$ 的递增子列或递减子列 l_k。

根据抽屉原理，$\{l_i\}_{i=1}^{2n+1}$ 至少有 $n+1$ 个子列，同为递增或者同为递减。

不妨假设我们拿到了 $n+1$ 个递增子列，将它们的**尾项**项按照原序列中顺序排序为：$b_1, b_2, \ldots, b_{n+1}$。

若在这个长为 $n+1$ 的序列 $\{b_i\}$ 中存在后项大于前项，即 $\exists j > i, b_j > b_i$，则拼上以 b_i 结尾的长为 n 的递增子列，可得到一个长为 $n+2$ 的递增子列。

反之，则这个序列本身成一个长为 $n+1$ 的递减子列。此时以 b_{n+1} 结尾既有一个长为 $n+1$ 的递减子列，又有一个长为 $n+1$ 的递增子列，则原命题得证。

法三（直接分组） 仍以原序列 $a_1, a_2, \ldots, a_{n^2+1}$ 为研究对象。对每个位置 i 定义

$$\ell_i = \text{以} a_i \text{ 结尾的最长递增子列的长度.}$$

情形 1： 若存在某个 i 使得 $\ell_i \geq n+1$，则我们已经找到一个长为 $n+1$ 的递增子列，命题成立。

情形 2： 否则，所有 ℓ_i 都落在集合 $\{1,2,\ldots,n\}$ 中。一共有 n 个“抽屉”（即可能的取值），却有 n^2+1 个元素，依抽屉原理，必存在某个 $t \in \{1,\ldots,n\}$，使得

$$\ell_{i_1} = \ell_{i_2} = \cdots = \ell_{i_{n+1}} = t$$

的下标个数至少为 $n+1$。按原序列的先后顺序排列这些下标：$i_1 < i_2 < \cdots < i_{n+1}$。

断言：$a_{i_1} > a_{i_2} > \cdots > a_{i_{n+1}}$，从而这 $n+1$ 个元素构成一个长为 $n+1$ 的递减子列。

证明断言：若对某对相邻下标 $i_k < i_{k+1}$ 有 $a_{i_k} \leq a_{i_{k+1}}$，则可以把以 a_{i_k} 结尾的最长递增子列（长度为 t）接上 $a_{i_{k+1}}$，得到一个以 $a_{i_{k+1}}$ 结尾的递增子列，其长度至少为 $t+1$，这与 $\ell_{i_{k+1}} = t$ 矛盾。因此必有 $a_{i_k} > a_{i_{k+1}}$，断言成立。

综上，在情形 2 下也必得到一个长为 $n+1$ 的递减子列。两种情形覆盖全部可能，命题得证。

问题 1.4.3

任一由 $mn+1$ 个实数构成的数列 $\{a_i\} = a_1, a_2, \ldots, a_{mn+1}$，其中要么存在长为 $n+1$ 的递增子列（任意一项不小于前一项）；要么存在长为 $m+1$ 的递减子列（任意一项不大于前一项）.

证明： 对于每个 i，考虑以元素 a_i 结尾的的最长递增子列，设其长度为 n_i；同样考虑以其为结尾的最长递减子列，设其长度为 m_i.

运用反证法：假定该列中不存在长为 $n+1$ 的单调子列，则对于每个 i，m_i 只能在 $[m]$ 中取值，n_i 只能在 $[n]$ 中取值，从而有序对 (m_i, n_i) 的情况只有 mn 种可能. 根据抽屉原理，这 n^2+1 个数中将存在两个数 a_i, a_j 满足 $(m_i, n_i) = (m_j, n_j)$，不妨设 $i < j$.

但，对于两个实数 a_i, a_j，$a_i \geq a_j$ 与 $a_i \leq a_j$ 两者必居其一. 如果前者成立，确定以 a_i 结尾的最长递减子列，将 a_j 拼接在其后便可得到一个长为 m_i+1 的递减子列，与反证假设矛盾；同理，如果后者成立，则可得到一个长为 n_i+1 的递增子列，同样矛盾.

练习 1.4.1

对于正整数 m, n，给出一个长为 mn 的实数列，使得其中不存在长为 $n+1$ 的递增子列或长为 $m+1$ 的递减子列.

问题 1.4.4 中国剩余定理

给定两个互素整数 m_1, m_2, 即 $(m_1, m_2) = 1$. 则如下同余方程的解在 $\mathrm{mod} m_1 m_2$ 的意义下有解 (且唯一):

$$\begin{cases} x \equiv a_1 (\mathrm{mod} m_1) \\ x \equiv a_2 (\mathrm{mod} m_2) \end{cases}$$

证明: 在 $\mathrm{mod} m_1$ 与 $\mathrm{mod} m_2$ 的意义下, 上述方程中的 a_1 有 m_1 种可能的不同取值, a_2 有 m_2 种可能的不同取值, 因此方程整体总共有 $m_1 m_2$ 种可能的状态. 而在 $\mathrm{mod} m_1 m_2$ 的意义下, x 的解也恰有 $m_1 m_2$ 种不同的情况. 根据推论 *1.7*, 为了证明每个方程均有解, 我们只需证明每个方程的解至多有一个.

运用反证法: 设某组 (a_1, a_2) 对应的方程在 $\mathrm{mod}\, m_1 m_2$ 的意义下有两种不同的解 x_1, x_2, 即同时有 $x_1 \equiv x_2 (\mathrm{mod} m_1)$ 与 $x_1 \equiv x_2 (\mathrm{mod} m_2)$ 成立. 这就意味着有 $m_1 | x_1 - x_2$ 与 $m_2 | x_1 - x_2$, 从而有 $[m_1, m_2] | x_1 - x_2$. 又根据 $(m_1, m_2) = 1$, 可以得出 $[m_1, m_2] = m_1 m_2$ 从而 $m_1 m_2 | x_1 - x_2$. 这就与反证假设矛盾.

1.5 Ramsey 问题

下面我们通过 Ramsey 问题展示抽屉原理在图论中的运用.

问题 1.5.1

对于完全图 K_6, 将其每条边染成红色或蓝色, 则必定存在导出子图 K_3, 其中的所有边颜色相同 (全为红色或全为蓝色).

证明: 运用反证法: 假定存在一种染色, 图中没有同色的导出子图 K_3.

任取 K_6 中一个点 v_1, 对于其 2 个邻点 v_2, v_3, 若边 v_1v_2 与 v_1v_3 均被染成红色, 则 v_2v_3 应为蓝色. 若 v_1 有至少 3 个以红色边相邻的点 v_2, v_3, v_4, 则这 3 个点之间两两以蓝色边相连, 构成了一个同色的 K_3, 矛盾. 这说明 v_1 至多有 2 个以红色边相邻的顶点. 同理 v_1 至多有 2 个以蓝色边相邻的顶点. 但 v_1 有 5 个邻点, 根据抽屉原理, 必定存在 3 个顶点与其以同色的边相邻.

练习 1.5.1

对于完全图 K_5, 给出一种进行 2-边染色的方式, 使得图中不存在同色的导出子图 K_3.

问题 1.5.2 Ramsey 问题

任给正整数 a, b, 是否存在正整数 n, 使得对于完全图 R_n 的任意 2-边染色, 都存在红色的导出子图 K_a 或蓝色的导出子图 K_b. 如果存在, 对于一组 (a, b), 求出最小的满足要求的 n. (显然, 如果一个正整数 n 具有此性质, 则任何正整数 $m > n$ 都具有此性质.)

对于一组 (a, b), 称最小的具有此性质的 n 为 (a, b) 的 Ramsey 数, 记为 $R(a, b)$. 自然, 有 $R(a, b) = R(b, a)$.

命题 1.5.1

对于任意自然数 a, $R(1, a) = 1, R(2, a) = a$.

证明: 这是显然的.

Ramsey 数的存在性问题的答案是肯定的. 我们可以归纳地证明这一点 (实际上给出 Ramsey 数的一个上界) .

定理 1.5.1

对于任意正整数 $a, b \geq 2$, $R(a, b) \leq R(a, b-1) + R(a-1, b)$.

证明： 记 $n = R(a,b), s = R(a,b-1), t = R(a-1,b)$. 我们使用反证法: 考虑完全图 K_s 上的 2-边染色, 其中既不存在红色的 K_a, 也不存在蓝色的 K_b.

任取其中的一个点 v_1, 假设其与至少 s 个点以蓝色边相邻. 根据假设, 这 s 个点的导出子图中要么存在红色的 K_a, 要么存在蓝色的 K_{b-1}. 再根据反证假设, 图中不存在红色的 K_a, 故只可能存在蓝色的 K_{b-1}. 由于 v_1 与这 s 个点全部以蓝色边相邻, 故与蓝色 K_{b-1} 中的点也全部以蓝色边相邻, 这 b 个点的导出子图就构成了一个蓝色的 K_b, 与反证假设矛盾. 这说明 v_1 至多与 $s-1$ 个点以蓝色边相邻.

同理, v_1 至多与 $t-1$ 个点以红色边相邻. 但在 K_n 中, v_1 有 $n-1 = s+t-1$ 个邻点. 根据抽屉原理, 其要么有 t 个以红色边相连的点, 要么有 s 个以蓝色边相邻的点, 矛盾.

练习 1.5.2

对于任意正整数 a, b, 证明 $R(a,b) \leq \binom{a+b-2}{a-1}$. 提示: 考虑使用数学归纳法.

2 数论

2.1 中国剩余定理

问题 2.1.1 中国剩余定理

$a, b \in \mathbb{N}^+$，对 $\forall 0 \leq x < a, 0 \leq y < b$，是否存在 s，使得：

$$\begin{cases} s \equiv x \pmod{a} \\ s \equiv y \pmod{b} \end{cases} \tag{1}$$

证明：

首先，上述命题不总成立，**反例：** $a = b, x \neq y$

尝试 *1*：如果 a, b 互素，即 $gcd(a, b) = 1$，这里 (x, y) 的取值有 $a \times b$ 种：

$$(x, y) \in \begin{pmatrix} (0,0) & \dots & (0,b) \\ \vdots & \dots & \vdots \\ (a,0) & \dots & (a,b) \end{pmatrix}$$

也即，余数的可能取值（抽屉）有 $a \times b$ 个

而 s 的取值有无数个，但是观察到：

$$s + ab \equiv s \pmod{[a/b/ab]}$$

引理 *2.1.1*

$\forall s_1, s_2 \in [ab-1]$ 有 $(s_1 \mod a, s_1 \mod b) \neq (s_2 \mod a, s_2 \mod b)$

证明： 反证：设存在 $s_1 < s_2 \in [ab-1]$ 使得：

$$\begin{cases} s_1 \equiv s_2 \pmod{a} \\ s_1 \equiv s_2 \pmod{b} \end{cases}$$

上式等价于：

$$\begin{cases} a|(s_1 - s_2) \\ b|(s_1 - s_2) \end{cases} \overset{用\ a\ b\ 互素}{\Rightarrow} ab|(s_1 - s_2)$$

注意这最后一步推导还未证明，请见下文**裴蜀公式**!!!

如果上式子成立，则 $s_1 \equiv s_2 \pmod{ab}$，与 $s_1 < s_2 \in [ab-1]$ 矛盾，就可以说明 s 两两不等，进而说明在 $[ab-1]$ 中，存在 s 对应上述的 (a,b) 位置，即有解。

注： 注意这里的条件可进一步放宽为 $a,\ b$ 的最大公约数整除 $x-y$，即 $gcd(a,b)|(x-y)$，此时在 $[ab-1]$ 中，s 的取值有 $gcd(a,b)$ 个。

2.2 裴蜀公式

定义 2.2.1 整除及相关概念

- 整除：$a|b$，即 $\exists k \in \mathbb{Z}, b = a \times k$
- 最大公约数：$gcd(a,b)$，即 $\exists k_1, k_2 \in \mathbb{Z}, a = k_1 \times gcd(a,b), b = k_2 \times gcd(a,b)$
- 最小公倍数：$lcm(a,b)$，即 $\exists k \in \mathbb{Z}, a = k \times lcm(a,b), b = k \times lcm(a,b)$

命题 2.2.1 整除的一个性质

$a \neq 1, a|b*c, (a,b) = 1 \Rightarrow a|c$

证明：

注意，这里的 $(a,b) = 1$，需要将"()"去掉则转为普通的加减乘除，才能进一步处理 $\exists t \ s.t. \ bc = at$，取 $b = qa + r$，其中 $0 \leq r < a$，则

$$at = bc = (qa + r)c = qac + rc \Rightarrow c = \frac{t - qc}{r}a$$

上式是否为整数？或者我们的问题是，能否找到一个 m 使得 $mb = qa + r$ 其中 $r = 1$？这就是我们要说的裴蜀定理：

定理 *2.2.1* 裴蜀定理

已知 $(a,b) = 1$，则 $\exists x, y \in \mathbb{Z}, ax + by = 1$

更一般的，$(a,b) = d$，则 $\exists x, y \in \mathbb{Z}, ax + by = d$

证明： 考虑集合 $Z(a,b) = \{ax + by | x, y \in \mathbb{N}\}$，取其中最小的正整数 r，设 a, b 的最大公约数为 d

先证明 $\forall s \in Z(a,b), r|s$：

取 $c = qr + r'$，其中 $0 \leq r' < r$，有

$$\begin{cases} c = xa + yb \\ r = ta + sb \end{cases} \Rightarrow c = (x - tq)a + (y - sq)b \in Z(a,b)$$

则 r' 只能是 0，故而 $r|c$

取 $(m,n) = (1,0)$ 可得 $r|a$，取 $(m,n) = (0,1)$ 可得 $r|b$，则 r 是 a, b 的公约数，进而 $r \leq d$

再 $d|a$ 且 $d|b$，$r \in Z(a,b)$，则 $\exists m_0, n_0 \in \mathbb{N}, r = m_0 a + n_0 b = (m_0 \frac{a}{d} + n_0 \frac{b}{d})d$

则 $d|r$，有 $d \leq r$

综上，$r = d$

故 $d = r$，即集合 $Z(a,b) = \{ax + by | x, y \in \mathbb{N}\}$ 中的最小正整数是 $gcd(a,b)$

2.3 整除

定理 2.3.1 整除的性质

设 $a,b,c\in\mathbb{Z}$，则整除具有以下性质：

1. $a\mid a$ （自反性）
2. $a\mid b$ 且 $b\mid a\Rightarrow a=\pm b$
3. $a\mid b$ 且 $b\mid c\Rightarrow a\mid c$ （传递性）
4. $a\mid b\Rightarrow a\mid bc$
5. $a\mid b$ 且 $a\mid c\Rightarrow a\mid(xb+yc)$ （线性性）
6. 若 $a,b>0$ 且 $a\mid b$，则 $b\geq a$，且 $b=a$ 或 $b\geq 2a$
7. $\forall c\neq 0$，$a\mid b\Leftrightarrow ac\mid bc$

2.3.1 最大公约数 $gcd(a,b)$ 的相关性质

定理 2.3.2 裴蜀定理

$d=(a,b)$，则 $\exists x,y\in\mathbb{Z},ax+by=d$

证明：

具体证明见上文**裴蜀公式**

注意： 此处的 (s,t) 不唯一：

$$d=sa+tb\Rightarrow d=(s-b)a+(t+a)b$$

不过可以加限制：

- 若限制 $s\in[b-1]=\{0,1,2,\cdots,b-1\}$ 中，仍有 $d=(s-\frac{b}{d})a+(t+\frac{a}{d})b$，于是在这个限制中可以有 $\frac{b}{d}$ 个解
- 于是可以再加限制：$1\leq s<\frac{b}{d}$，此时有且仅有一组解

注：下面这些结论看起来都很显然，但是都需要证明！！！主要借助的工具就是我们上面提到的裴蜀公式

引理 2.3.1

设 $a,b,c\in\mathbb{N}$，$m\in\mathbb{N}^+$，则

$$(ma,mb)=m(a,b)$$

特别的：

$$(a,b)=d\Rightarrow\left(\frac{a}{d},\frac{b}{d}\right)=1\quad(a,b)=\left(d\frac{a}{d},d\frac{b}{d}\right)=d\left(\frac{a}{d},\frac{b}{d}\right)=d$$

$$c\mid a,c\mid b\Rightarrow c\mid(a,b)\quad\left(c\frac{a}{c},c\frac{b}{c}\right)=c\left(\frac{a}{c},\frac{b}{c}\right)=cm=(a,b)\Rightarrow c\mid(a,b)$$

证明： 由裴蜀定理，$(ma,mb)=\min\{sma+tmb\mid s,t\in\mathbb{N}\}$。

令 $d=(a,b)$，则存在 $s,t\in\mathbb{N}$ 使得 $d=sa+tb$，因此

$$(ma,mb)=\min\{m(sa+tb)\mid s,t\in\mathbb{N}\}=m\cdot\min\{sa+tb\mid s,t\in\mathbb{N}\}=m(a,b)$$

引理 2.3.2

若 $(a,c)=1$，$(b,c)=1$，则 $(ab,c)=1$。

证明： 由裴蜀定理，存在 $s,t,m,n\in\mathbb{N}$，使得

$$sa+tc=1\tag{1}$$

$$mb+nc=1\tag{2}$$

用 *(1)* 乘以 m，用 *(2)* 乘以 s，再相加，得

$$smab+(tmb+sna+tnc)c=mab+yc=1$$

其中 $x=sm$，$y=tmb+sna+stnc$。因此，存在 $x,y\in\mathbb{N}$，使 $xab+yc=1$，即 $(ab,c)=1$。

引理 2.3.3

$(a,b)=(a,b+ac)$ （辗转相除法）

证明： 设 $A=\{xa+yb\mid x,y\in\mathbb{N}\}$，则

$$\begin{aligned}A&=\{xa+yb\mid x,y\in\mathbb{N}\}\\&=\{a(x+yc)+yb\mid x,y\in\mathbb{N}\}\\&=\{xa+y(b+ac)\mid x,y\in\mathbb{N}\}\end{aligned}$$

因此，$A=\{xa+yb\}=\min\{xa+y(b+ac)\}$，即 $(a,b)=(a,b+ac)$。

引理 2.3.4

若 $c \mid ab$，且 $(c,a)=1$，则 $c \mid b$。

证明： 由 $(c,a)=1$，根据裴蜀定理，存在 $s,t \in \mathbb{Z}$，使得 $sc+ta=1$。两边同时乘以 b，得 $scb+tab=b$。又因 $c \mid ab$，设 $ab=kc$，则

$$scb+tab=sbc+tab=sbc+tkc=(sb+tk)c$$

即 $b=(sb+tk)c$，所以 $c \mid b$。

引理 2.3.5

若 $a \mid c$，$b \mid c$，且 $(a,b)=1$，则 $ab \mid c$。

证明： 由 $(a,b)=1$，存在 $s,t \in \mathbb{Z}$，使得 $sa+tb=1$。又因 $a \mid c$，$b \mid c$，存在 $k,m \in \mathbb{Z}$，使得 $c=ka=mb$。两边同时乘以 c，得

$$sac+tbc=c$$

将 $c=mb$ 和 $c=ka$ 代入，得

$$sa \cdot mb+tb \cdot ka=c$$

即

$$ab(sm+tk)=c$$

所以 $ab \mid c$。

引理 2.3.6

若 $a \mid c$，$b \mid c$，且 $(a,b)=d$，则 $\dfrac{ab}{d} \mid c$。

证明： 设 $(a,b)=d$，则存在 $s,t \in \mathbb{Z}$，使得 $sa+tb=d$。又因 $a \mid c$，$b \mid c$，存在 $k,m \in \mathbb{Z}$，使得 $c=ka=mb$。两边同时乘以 c，得

$$sac+tbc=dc$$

将 $c=mb$ 和 $c=ka$ 代入，得

$$sa \cdot mb+tb \cdot ka=dc$$

即

$$ab(sm+tk)=dc$$

所以 $\dfrac{ab}{d} \mid c$。

事实上，$\dfrac{ab}{d} = \operatorname{lcm}(a,b)$，即 a,b 的最小公倍数。由于 $a \mid c$，$b \mid c$，c 是 a,b 的公倍数，所以 c 一定是 $\operatorname{lcm}(a,b)$ 的倍数，即

$$\operatorname{lcm}(a,b) \mid c$$

其中

$$\operatorname{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$$

定理 2.3.3 辗转相除法

设 $a,b \in \mathbb{Z}$，$a \geq b > 0$，则

$$(a,b) = (a, b+ka), \quad k \in \mathbb{Z}$$

特别地，欧几里得算法是有限步的。

证明： 由带余除法，存在 q_0, r_0，使得 $a = q_0 b + r_0$，$0 \leq r_0 < b$。于是

$$(a,b) = (q_0 b + r_0, b) = (r_0, b)$$

同理，对 b, r_0 继续做带余除法，得 $b = q_1 r_0 + r_1$，$0 \leq r_1 < r_0$，于是

$$(r_0, b) = (r_0, q_1 r_0 + r_1) = (r_0, r_1)$$

依此类推，得到如下序列：

$$\begin{aligned}
a &= q_0 b + r_0, \quad 0 \leq r_0 < b \\
b &= q_1 r_0 + r_1, \quad 0 \leq r_1 < r_0 \\
r_0 &= q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

当余数为 0 时，最后一个非零余数 r_n 即为 $\gcd(a,b)$。由于余数严格递减且非负，算法在有限步内终止。

2.4 素数与算数基本定理

定义 2.4.1 素数

$a \in \mathbb{N}^+$，a 为素数当且仅当 $\forall b \in \mathbb{N}^+$，若 $b \mid a$，则 $b = 1$ 或 $b = a$。

命题 2.4.1 性质

素数有无穷多个。

证明： 反证法。假设素数只有有限个，记为 $p_1, p_2, \ldots, p_n$。

考虑 $N = p_1 p_2 \cdots p_n + 1$。

N 要么是素数，要么有素因子。设 p_i 是 N 的某个素因子，则 $p_i \mid N$，又 $p_i \mid p_1 p_2 \cdots p_n$，所以 $p_i \mid (N - p_1 p_2 \cdots p_n) = 1$，矛盾。因此素数有无穷多个。

命题 2.4.2 素数的一般定义

$\mathbb{Z}$ 中，p 为素数当且仅当：$\forall a, b$，若 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$。

证明：

$\Rightarrow$：若 p 为素数，$p \mid ab$，

- 若 $(p, a) = 1$，则 $p \mid b$。
- 若 $(p, a) = d > 1$，由于 p 只有 1 和它本身两个约数，所以 $p = d \mid a$

$\Leftarrow$：若 p 满足 $\forall a, b \in \mathbb{Z}$，$p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$，则 p 必为素数。

反证，设存在 p 不是素数，满足 $\forall a, b \in \mathbb{Z}$，若 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$，

则 $p = st$，$1 < s < p$，$1 < t < p$，此时 $p \mid st$，但 $p \nmid s$ 且 $p \nmid t$，矛盾。

所以 p 必为素数。

定理 2.4.1 算数基本定理（唯一分解定理）

$\forall n \in \mathbb{N}^+, \exists$唯一分解 $: n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$，其中 p_i 为素数，且 $r_i \in \mathbb{N}^+$。

存在性： 任意整数都能分解为有限个素数的乘积。

反证：设存在不能分解为素数乘积的最小正整数 n_0。

n_0 不是素数，否则本身就是素数乘积。则为合数 $n_0 = ab$，$1 < a < n_0$，$1 < b < n_0$。

由最小性，a, b 都能分解为素数乘积，则 n_0 也能分解为素数乘积，矛盾。因此任意正整数都能分解为有限个素数的乘积。

唯一性：

引理 2.4.1

设 $n = p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k} = q_1^{s_1}q_2^{s_2}\cdots q_l^{s_l}$ 是 n 的两种素数分解，则 $\exists i$ 使得 $p_1 = q_i$。

证明： 不妨设 $\{p_i\}$ 和 $\{q_j\}$ 两序列均为单调增序列，则 $p_1 \le p_2 \le \cdots \le p_k$，$q_1 \le q_2 \le \cdots \le q_l$。

由 $q_1 \mid n = p_1\frac{n}{p_1}$，则 $q_1 \mid p_1$ 或 $q_1 \mid \frac{n}{p_1}$。

若 $q_1 \neq p_1$，则 $q_1 \mid \frac{n}{p_1}$，依此将右项分解，则存在 p_i 满足 $q_1 = p_i$。

开始做归纳：

基础： $n = 1, 2$ 时有唯一的素因子分解。

归纳假设： $1 \le n \le k$ 时唯一分解成立。

递推： $n = k+1$ 时，若 n 有两种分解：$n = p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k} = q_1^{s_1}q_2^{s_2}\cdots q_l^{s_l}$，

则由上引理，$\exists i$ 使得 $p_1 = q_i$。则考虑 $\frac{n}{p_1} = \frac{n}{q_i}$，此时 $\frac{n}{p_1} < k$，由归纳假设，$\frac{n}{p_1}$ 的分解唯一，所以 $n = \frac{n}{p_1}p_1$ 和 $n = \frac{n}{q_i}q_i$ 的分解一致。

因此，分解唯一。

2.5 环的定义、素元和不可约元

定义 2.5.1 环： $< R, +, \cdot >$

设 R 是一个集合，在 R 上定义了加法和乘法两种运算，若满足：

- $\forall a, b \in R,\ a + b \in R,\ a \cdot b \in R$（加法、乘法封闭）
- $0 \in R,\ 1 \in R$ （存在零元和单位元）
- $\forall a \in R,\ \exists -a \in R$ （存在加法逆元）

则称 R 为**环**（*Ring*）。
可以总结为对加法成群，对乘法成含幺半群，具体请见后面代数结构章节。

常见例子：$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ 等。
$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ 也是环。

定义 2.5.2 不可约元

设 $a \in R$，若 a 不是单位，且若 $a = bc$ $(b, c \in R)$ 时，b 或 c 为单位，则称 a 为**不可约元**。

定义 2.5.3 素元

设 $a \in R$，若 $a \neq 0$ 且 a 不是单位，且对任意 $b, c \in R$，若 $a \mid bc$，则 $a \mid b$ 或 $a \mid c$，则称 a 为**素元**。
其中 $a \mid bc$ 表示存在 $k \in R$ 使得 $ak = bc$。

命题 2.5.1 性质 1：素元一定是不可约元

素元一定是不可约元。

证明： 反证。假设 $p \in R$ 是素元但不是不可约元，则 p 可以分解为 $p = ab$，其中 a, b 都不是单位。

由于 p 是素元且 $p \mid ab$，所以 $p \mid a$ 或 $p \mid b$。
不妨设 $p \mid a$，则存在 $k \in R$ 使得 $a = kp$。
代入 $p = ab$ 得 $p = (kp)b = kpb$，即 $p = kpb$。
整理得 $p(1 - kb) = 0$。
由于 $p \neq 0$，所以 $1 - kb = 0$，即 $kb = 1$。
这说明 b 是单位，与假设矛盾。

因此素元一定是不可约元。

命题 2.5.2 性质 2：不可约元不一定是素元

不可约元不一定是素元。

证明： 以环 $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ 为例。

在 $\mathbb{Z}[\sqrt{-5}]$ 中，单位只有 $\pm 1, 2 \pm \sqrt{-5}$。

考虑元素 2：

- 2 是不可约元（如果 $2 = ab$，则 a 或 b 必须是单位）*(可以直接讨论所有模长小于 2 的元素)*
- 但 2 不是素元，因为 $2 \mid (1 - \sqrt{-5})(1 + \sqrt{-5}) = 6$，但 $2 \nmid (1 - \sqrt{-5})$ 且 $2 \nmid (1 + \sqrt{-5})$ 不是素元。

命题 2.5.3 性质 3：唯一分解与素元的关系

若环 R 中所有不可约元都是素元，则 R 中存在唯一分解。

证明： 这里我们暂时只看 $\mathbb{Z}[\sqrt{-5}]$，由于存在不可约元不是素元，所以不存在唯一分解。

例如：6 可以分解为：

$$6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$
$$6 = 2 \times 3$$

这两种分解都是不可约元的乘积，但分解不唯一。具体的环的唯一分解请看后面代数结构章节。

2.6 同余和中国剩余定理

2.6.1 同余基本性质

定义 2.6.1 同余

设 $a,b,m \in \mathbb{Z}$，若 a 与 b 除以 m 的余数相同，则称 a 与 b 模 m 同余，记作 $a \equiv b \pmod{m}$。

命题 2.6.1 同余的基本性质

设 $a,b,c,d \in \mathbb{Z}^+$，$m,d \in \mathbb{N}^+$，则：

1. **等价定义**：$a \equiv b \pmod{m} \iff m \mid (a-b)$
2. **自反性**：$a \equiv a \pmod{m}$
3. **对称性**：$a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$
4. **传递性**：$a \equiv b \pmod{m}, b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$
5. **运算性质**：若 $a \equiv b \pmod{m}$ 且 $c \equiv d \pmod{m}$，则：
   - $a \pm c \equiv b \pm d \pmod{m}$ （因为 $m \mid (a-b) \pm (c-d) = (a \pm c) - (b \pm d)$）
   - $ac \equiv bd \pmod{m}$ （因为 $m \mid (a-b)c + (c-d)b = ac - bd$）
   - $a^k \equiv b^k \pmod{m}$ （对任意正整数 k）
6. **整除性质**：若 $d \mid m$ 且 $a \equiv b \pmod{m}$，则 $a \equiv b \pmod{d}$ （因为 $d \mid m \mid (b-a)$）
7. **数乘性质**：若 $a \equiv b \pmod{m}$，则 $da \equiv db \pmod{m}$ （因为 $m \mid (b-a) \mid d(a-b)$）
8. **消去律**：若 $(d,m) = 1$，则 $a \equiv b \pmod{m} \iff da \equiv db \pmod{m}$ （因为 $(d,m) = 1$ 时，$m \mid (b-a) \iff m \mid d(b-a)$）

定义 2.6.2 一次同余方程

形如 $ax \equiv b \pmod{m}$ 的方程称为一次同余方程，其中 $a,b,m \in \mathbb{Z}$，$m > 0$。

定理 2.6.1 一次同余方程的解的存在性

一次同余方程 $ax \equiv b \pmod{m}$ 有解当且仅当 $(a,m) \mid b$。

证明：

$$\begin{aligned}
\text{有解} &\iff m \mid (ax-b) \\
&\iff \exists k \in \mathbb{Z}, \text{使得} ax-b=km \\
&\iff b=ax-km \\
&\iff b \in \{sa+tm \mid s,t \in \mathbb{Z}\} \quad (\text{裴蜀公式}) \\
&\iff (a,m) \mid b
\end{aligned}$$

定理 2.6.2 一次同余方程的解的个数

设 $d=(a,m)$，若 $d \mid b$，则一次同余方程 $ax \equiv b \pmod m$ 在模 m 的完全剩余系中有 d 个解。

注： 此处提到的模 m 的完全剩余系，指的是 $\{0,1,\ldots,m-1\}$。

证明： 由于若 x 是解，则 $x+m$ 也是解，所以我们只需在 $\{0,1,\ldots,m-1\}$ 中讨论解的个数。

设 (x_0,y_0) 是方程 $ax+my=b$ 的一个特解，则所有解为：

$$(x,y)=(x_0-\frac{m}{d}t, y_0+\frac{a}{d}t), \quad t \in \mathbb{Z}$$

因此模 m 的不同解为：

$$x \equiv x_0-\frac{m}{d}t \pmod m, \quad t=0,1,\ldots,d-1$$

共有 d 个解。

证明： 不从裴蜀公式来看，直接从同余方程推导：

设 x_0 是方程 $ax \equiv b \pmod m$ 的一个特解，$ax_0 \equiv b \pmod m$。

对于任意解 x，有 $ax \equiv b \pmod m$。

两式相减：$a(x-x_0) \equiv 0 \pmod m$。

设 $\Delta x=x-x_0$，则 $m \mid a\Delta x$。

设 $d=(a,m)$，则 $\frac{m}{d} \mid \frac{a}{d}\Delta x$。

而 $\left(\frac{m}{d},\frac{a}{d}\right)=1$，所以 $\frac{m}{d} \mid \Delta x$。

因此 $\Delta x=k \cdot \frac{m}{d}$，其中 $k \in \mathbb{Z}$。

所以通解为：$x=k \cdot \frac{m}{d}+x_0$，其中 $k \in \mathbb{Z}$。

在 $\{0,1,\ldots,m-1\}$ 中，k 取 $0,1,\ldots,d-1$ 时得到 d 个不同的解。

特别地，若 $(a,m)=1$，则 $d=1$，此时在 $\{0,1,\ldots,m-1\}$ 中有唯一解。

2.6.2 中国剩余定理回顾

定理 2.6.3 中国剩余定理回顾

考虑同余方程组：

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \end{cases}$$

何时有解：$\forall (a_1, a_2)$ 均有解 $\iff (m_1, m_2) = 1$。

定理 2.6.4 中国剩余定理的一般化

考虑 k 个同余方程：

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ x & \equiv a_2 \pmod{m_2} \\ & \vdots \\ x & \equiv a_k \pmod{m_k} \end{cases}$$

$\forall (a_1, \ldots, a_k)$ 有解 $\iff (m_i, m_j) = 1$ 对所有 $i \neq j$。

证明： 将原问题分解为 k 个子问题：

$$\begin{cases} x_1 & \equiv a_1 \pmod{m_1} \\ x_1 & \equiv 0 \pmod{m_2} \\ & \vdots \\ x_1 & \equiv 0 \pmod{m_k} \end{cases}, \begin{cases} x_2 & \equiv 0 \pmod{m_1} \\ x_2 & \equiv a_2 \pmod{m_2} \\ & \vdots \\ x_2 & \equiv 0 \pmod{m_k} \end{cases}, \cdots, \begin{cases} x_k & \equiv 0 \pmod{m_1} \\ x_k & \equiv 0 \pmod{m_2} \\ & \vdots \\ x_k & \equiv a_k \pmod{m_k} \end{cases}$$

得到各子问题的解后直接求和：$x = x_1 + x_2 + \cdots + x_k$。

引理 *2.6.1* 子问题的解的条件

对于子问题 i：

$$\begin{cases} x_i & \equiv a_i \pmod{m_i} \\ x_i & \equiv 0 \pmod{M/m_i} \end{cases} \text{ 有解} \iff (m_i, M/m_i) = 1$$

原问题有解 $\iff$ 须 $(m_i, m_j) = 1$ 对所有 $i \neq j$。

注： 这个思路是一个 *24* 年考试原题的思路哦 ~~~

2.7 欧拉定理

2.7.1 欧拉函数

定义 2.7.1 欧拉函数

设 $n \in \mathbb{N}^+$，定义：

$$C_n = \{a \in [n] \mid (a, n) = 1\}$$

则 $\varphi(n) = |C_n|$，即 $\varphi(n)$ 表示 $[n]$ 中与 n 互素的整数个数。
其中 $[n]$ 指模 n 完全剩余系 $\{0, 1, \ldots, n-1\}$，C_n 为模 n 缩系。

欧拉函数值表

n	1	2	3	4	5	...
$\varphi(n)$	1	1	2	2	4	...

说明：

- $\varphi(1) = 1$：$[1] = \{0\}$，$(0, 1) = 1$
- $\varphi(2) = 1$：$[2] = \{0, 1\}$，只有 1 与 2 互素
- $\varphi(3) = 2$：$[3] = \{0, 1, 2\}$，$1, 2$ 都与 3 互素
- $\varphi(4) = 2$：$[4] = \{0, 1, 2, 3\}$，$1, 3$ 都与 4 互素
- $\varphi(5) = 4$：$[5] = \{0, 1, 2, 3, 4\}$，$1, 2, 3, 4$ 都与 5 互素

2.7.2 欧拉定理

定理 2.7.1 欧拉定理

$\forall a, n$，若 $(a, n) = 1$，则 $a^{\varphi(n)} \equiv 1 \pmod{n}$。

证明： 由性质：$(a, n) = (a + kn, n)$，且 $(a + kn)^{\varphi(n)} \equiv a^{\varphi(n)} \pmod{n}$（直接展开即可验证）。
直接考虑 $a \in C_n$（$C_1, C_2, C_3, \ldots$ 可手动验证）。
取 $C_n = \{r_1, r_2, \ldots, r_{\varphi(n)}\}$，考虑集合 $aC_n = \{ar_i \mid r_i \in C_n\}$。

有 $\begin{cases} (r_i, n) = 1 \\ (a, n) = 1 \end{cases} \implies (ar_i, n) = 1$

在 aC_n 中，若 $ar_i \equiv ar_j \pmod{n}$，则 $n \mid a(r_i - r_j) \implies n \mid (r_i - r_j)$（因为 $(a, n) = 1$）。
但 $0 < |r_i - r_j| < n$，矛盾。故 aC_n 中任两个数 $\pmod{n}$ 均不同余。

则 aC_n 中元素均与 n 互素，且无 $\pmod n$ 同余，可得 $aC_n = C_n \pmod n$。

即 aC_n 与 C_n 中元素存在一一对应关系。

C_n, aC_n 中元素乘积：

$$C_n : r_1 r_2 \cdots r_{\varphi(n)}$$
$$aC_n : (ar_1)(ar_2)\cdots(ar_{\varphi(n)}) = a^{\varphi(n)} r_1 r_2 \cdots r_{\varphi(n)} \pmod n$$

取 $R = r_1 r_2 \cdots r_{\varphi(n)}$，则 $R \equiv a^{\varphi(n)} R \pmod n$。

而 $(R, n) = 1$，故 $a^{\varphi(n)} \equiv 1 \pmod n$。

另一种分析角度 考虑方程 $a^x \equiv 1 \pmod n$ 的解：

$x = 0$ 是一个平凡解。考虑 $a^1, a^2, \ldots, a^n$，若不存在 $a^r \equiv 1 \pmod n$，则必有 $i < j$ 使 $a^i \equiv a^j \pmod n$。由 $(a^k, n) = 1$，可得 $a^{|j-i|} \equiv 1 \pmod n$，即 x 在 $[n]$ 内总有解。

继续拆解解的性质，设已有 $a^{x_0} \equiv 1 \pmod n$，则有：

$$\forall k \in \mathbb{Z}, a^{kx_0} \equiv 1 \pmod n$$
$$\text{若存在} x_0, x_1 \in \mathbb{Z}, a^{x_i} \equiv a^{x_j} \equiv 1 \pmod n, \text{则} a^{k_1 x_1 + k_2 x_2} \equiv 1 \pmod n$$

换言之，若 x_1, x_2 均是解，则 $Z[x_1, x_2] = \{k_1 x_1 + k_2 x_2 \mid k_1, k_2 \in \mathbb{Z}\} = \{kd \mid d = \gcd(x_1, x_2), k \in \mathbb{Z}\}$ 也是解。

因此，$a^x \equiv 1 \pmod n$ 的解构成集合 $\{kd \mid d = \gcd(x_1, x_2, \ldots), k \in \mathbb{Z}^+\}$。

记 r 为 $a^x \equiv 1 \pmod n$ 的最小正整数解，目标是证明 $r \mid \varphi(n)$（相等是证明不了的，比如举一个反例：取 $a = 3, n = 20$，有 $\varphi(20) = 8$ 但是 $3^4 \equiv 1 \pmod{20}$，最小值解更小）。

若 $r = \varphi(n)$ 则直接成立，这里不妨直接设 $r < \varphi(n)$。

取出 $R = \{a^0, a^1, \ldots, a^{r-1}\}$，此时再乘 a 的结果也会落回这个集合中（在模 n 意义下）。我们将这个集合结合模 n 意义下的乘法运算，称成一个群（循环群）。

这里 $R \subsetneq C_n$，取 $b \in C_n \setminus R$，乘 R 得 $bR = \{ba, ba^2, \ldots, ba^r \pmod n\}$

由于 $(b, n) = 1$，所以 bR 中任意两个数模 n 不同余。有 $|bR| = |R|$

同时 $R \cap bR = \varnothing$，反证：若存在 $a^i \equiv ba^j \pmod n$，则 $a^{i-j} \equiv b \pmod n$，矛盾。

截止现在，若 $bR \cap R = C_n$，则 $r \mid \varphi(n)$。否则，取 $b_2 \in C_n \setminus (R \cup bR)$，重复上述过程。

由于 C_n 是有限集，上述过程必终止。

此时 $R \cup bR \cup b_2 R \cup \cdots \cup b_k R = C_n$，且 $R, bR, b_2 R, \ldots, b_k R$ 两两交集为空。

最终得 $r \mid \varphi(n)$。

注： 上述过程是群的**陪集分解**的过程。具体请见后文代数结构部分内容。

定理 2.7.2 费马小定理

若 p 是素数，则 $\forall a$，有 $a^{p-1} \equiv 1 \pmod p$。

证明： 由欧拉定理，若 p 是素数，则 $\varphi(p)=p-1$，故 $a^{p-1}\equiv 1 \pmod p$。
注： 费马小定理是欧拉定理的特例。

2.7.3 欧拉函数的计算

1. 若 $n=p$ 为素数，则 $\varphi(p)=p-1$。
2. 若 $n=p^k$，p 为素数，则 $\varphi(p^k)=p^k-p^{k-1}=p^{k-1}(p-1)$（只要不被 p 整除的数，都与 p^k 互素）。
3. 若 $n=pq$，p,q 互素，则 $\varphi(pq)=\varphi(p)\varphi(q)$。

   例： $n=15=3\times 5$，$\varphi(15)=\varphi(3)\times\varphi(5)=2\times 4=8$。

	0	1	2	3	4
0	15	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

   其中绿色部分 $\begin{pmatrix}1 & 7 & 13 & 4\\ 11 & 2 & 8 & 14\end{pmatrix}$ 是 ≤ 15 且与 15 互素的数。可以发现：

   $\{x\le 15 \mid (x,15)=1\}=\{x\le 15\mid (x,3)=1\}\cap\{x\le 15\mid (x,5)=1\}$

   说明 $\varphi(15)=\varphi(3)\times\varphi(5)$，且两集合间存在一一对应。
4. 若 $n=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，$p_i$ 互不相同素数，则

$$\begin{aligned}\varphi(n)&=\varphi(p_1^{r_1})\varphi(p_2^{r_2})\cdots\varphi(p_k^{r_k})\\&=p_1^{r_1}(1-\frac{1}{p_1})\times p_2^{r_2}(1-\frac{1}{p_2})\times\cdots\times p_k^{r_k}(1-\frac{1}{p_k})\\&=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\end{aligned}$$

   例： $n=12=2^2\times 3$，$\varphi(12)=\varphi(2^2)\times\varphi(3)=(4-2)\times 2=4$。

注： 欧拉函数的计算可以利用分解质因数后直接套用公式，复杂度 $O(\log n)$。

2.8 RSA 加密

RSA 算法是一种非对称加密算法，利用数论中的欧拉定理和大数分解难题实现加密与解密。

定义 2.8.1 RSA 加密基本思想

寻找一个加密函数 f，使得存在解密函数 d，满足 $d(f(M)) = M$，且解密过程在不知道私钥的情况下难以实现。

密钥生成步骤

1. **选择两个大素数** p, q，计算 $n = pq$。
2. **计算欧拉函数**：$\varphi(n) = (p-1)(q-1)$。
3. **选择加密指数** e，要求 $1 < e < \varphi(n)$ 且 $\gcd(e, \varphi(n)) = 1$。
4. **计算解密指数** d，使得 $ed \equiv 1 \pmod{\varphi(n)}$，即 d 是 e 关于 $\varphi(n)$ 的乘法逆元。
5. **公钥与私钥**：
   - 公钥 (n, e) 用于加密：$C = M^e \bmod n$
   - 私钥 $(p, q, \varphi(n), d)$ 用于解密：$M = C^d \bmod n$

安全性说明

n 的分解难度决定了 RSA 的安全性。若能高效分解 n，则可计算 $\varphi(n)$，进而求出 d。

定义 2.8.2 加密与解密过程

- **加密**：给定明文 M，计算密文 $C = f(M) = M^e \bmod n$
- **解密**：收到密文 C，用私钥 d 计算 $M = d(C) = C^d \bmod n$

正确性证明

$$\begin{aligned} &\text{加密：} \quad C = M^e \bmod n \\ &\text{解密：} \quad M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n \end{aligned}$$

由于 $ed \equiv 1 \pmod{\varphi(n)}$，存在整数 k 使 $ed = k\varphi(n) + 1$，因此：

$$M^{ed} = M^{k\varphi(n)+1} = (M^{\varphi(n)})^k \cdot M \equiv 1^k \cdot M \equiv M \pmod{n}$$

其中 M 与 n 互素时由欧拉定理成立，若 M 与 n 不互素，仍可证明 $M^{ed} \equiv M \pmod{n}$。

注意事项

- e 一般选取 65537 等常用值，便于计算且安全性高。
- p, q 必须足够大且随机，防止被分解。
- 明文 M 须小于 n。
- 实际应用中还需考虑填充、分组等安全措施。

3 代数结构

定义 3.0.1 代数结构

代数结构是指在一个非空集合 A 上配备一个或多个运算（如加法、乘法等），并研究这些运算满足的各种代数性质（如结合律、单位元、逆元等）的数学对象。

3.1 群

定义 3.1.1 半群

设 S 是一个非空集合，$*$ 是 S 上的一个二元运算。如果满足以下两个条件：

- **封闭性**：对任意 $a, b \in S$，有 $a * b \in S$；
- **结合律**：对任意 $a, b, c \in S$，有 $(a * b) * c = a * (b * c)$；

则称 $(S, *)$ 为**半群**（*Semigroup*）。

定义 3.1.2 含幺半群

如果半群 $(S, *)$ 中存在单位元 e，使得对任意 $a \in S$，有

$$e * a = a * e = a$$

则称 $(S, *)$ 为**含幺半群**（*Monoid*），e 称为单位元。

定义 3.1.3 群

如果含幺半群 $(G, *)$ 中，任意 $a \in G$ 都存在逆元 $a^{-1} \in G$，使得

$$a * a^{-1} = a^{-1} * a = e$$

则称 $(G, *)$ 为**群**（*Group*），e 为单位元，a^{-1} 为 a 的逆元。

定义 3.1.4 交换群

设 $(G,*)$ 是一个群。如果对任意 $a,b\in G$，有

$$a*b=b*a$$

则称该群为**交换群**（*Abel* 群）。

注：交换律是群中非常特殊的性质。大多数常见的数集（如整数加法群、实数加法群等）都是交换群，但也有许多重要的非交换群（如一般矩阵乘法群）。

以下是常见的群、半群、含幺半群的例子：

- **整数加法群**：所有整数集合 $\mathbb{Z}$ 在加法 $+$ 下构成一个群，记作 $\langle\mathbb{Z},+\rangle$，其中 0 是单位元。
- **整数乘法非群**：$\mathbb{Z}$ 在乘法 $\times$ 下不构成群，因为 0 没有逆元。
- **正整数乘法半群**：正整数集合 $\mathbb{Z}^+$ 在乘法 $\times$ 下，$\langle\mathbb{Z}^+,\times\rangle$ 只满足封闭性和结合律，是一个**半群**，不是群。
- **整数乘法含幺半群**：$\langle\mathbb{Z},\times\rangle$ 满足封闭性、结合律和单位元（1），但不是群，因为 0 没有逆元，是一个**含幺半群**。
- **有理数乘法群**：有理数集合 $\mathbb{Q}$ 在乘法 $\times$ 下不是群（0 没有逆元），但去除 0 后 $\langle\mathbb{Q}\backslash\{0\},\times\rangle$ 是群。
- **实数、复数乘法群**：同理，$\langle\mathbb{R}\backslash\{0\},\times\rangle$ 和 $\langle\mathbb{C}\backslash\{0\},\times\rangle$ 都是群。
- **矩阵加法群**：所有 2×2 实矩阵 $\mathbb{R}_{2\times2}$ 在加法 $+$ 下构成群，记作 $\langle\mathbb{R}_{2\times2},+\rangle$。
- **矩阵乘法非群**：$\langle\mathbb{R}_{2\times2},\times\rangle$ 不是群，因为不是所有矩阵都可逆。
- **特殊矩阵群**：
  - $\langle\mathbb{R}_{2\times2,\det=1},\times\rangle$ 是群（特殊线性群）。
  - $\langle\mathbb{R}_{2\times2,\det=2},\times\rangle$ 不是群，因为逆元不一定在集合内。
  - $\langle\mathbb{R}_{2\times2,\det=\pm1},\times\rangle$ 是群。
  - 更一般地，$\langle\mathbb{R}_{2\times2,\det=e^{\frac{k2\pi i}{n}},k\in[n]},\times\rangle$ 和 $\langle\mathbb{R}_{2\times2,\det\in\mathbb{Q}\backslash\{0\}},\times\rangle$ 都是群。

下面开始考虑另一种运算, 模. 很容易想到, 整数集合 $\{1,2,\ldots,m-1,m\}$ 在模 m 加法下, 可以构成一个群 $\langle \mathbb{Z}_m, +_{\bmod m}\rangle$, 元素 a 的逆元即是 $m-a$. 那么在乘法之下, 是否依旧可以构成一个群呢?

可以容易举出一个反例, 当 $m=4$ 的时候, 元素 2 无法找到一个逆元 x 使得 $2\times b \mod m = 1$. 实际上, $\langle \mathbb{Z}_m^*, \times_{\bmod m}\rangle$ 是一个群, 其中 $\mathbb{Z}_m^* = \{a\in[m]|(a,m)=1\}$. 作为一个练习, 可以试着证明如下定理:

对于任意正整数 a,m, $\exists b$ 使得 $ab\equiv 1\ (\mathrm{mod} m)$, 当且仅当 $(a,m)=1$.

接下来给出几个关于单位元与逆元的定理:

定理 3.1.1 单位元与逆元的左右唯一性

在群的定义中, 单位元和逆元可以分别拆分为左单位元、右单位元和左逆元、右逆元。

- **左单位元**: $e_L * a = a$ 对所有 $a\in G$ 成立
- **右单位元**: $a * e_R = a$ 对所有 $a\in G$ 成立
- **左逆元**: $a_L^{-1} * a = e$
- **右逆元**: $a * a_R^{-1} = e$

但在群中可以证明:

- 左单位元和右单位元必然相等, 且唯一。
- 左逆元和右逆元也必然相等, 且唯一。

证明:

若 e_L 是左单位元, e_R 是右单位元, 则 $e_L = e_L * e_R = e_R$。

若 a_L^{-1} 是左逆元, a_R^{-1} 是右逆元, 则 $a_L^{-1} = a_L^{-1} * (a * a_R^{-1}) = (a_L^{-1} * a) * a_R^{-1} = e * a_R^{-1} = a_R^{-1}$。

因此, 群的单位元和逆元都是唯一的。

定理 3.1.2 消去律

- **左消去律**: $a*b = a*c \implies b=c$
- **右消去律**: $b*a = c*a \implies b=c$

证明: 利用逆元和结合律, 左/右两边同乘以 a^{-1} 即可。

定理 3.1.3 线性方程组在群中有唯一解

对于任意 $a,b \in G$，方程 $a*x=b$ 和 $y*a=b$ 在 G 中都有唯一解：

- $x = a^{-1} * b$
- $y = b * a^{-1}$

证明： 设 $a*x_1 = a*x_2$，由左消去律 $x_1 = x_2$，唯一性成立。

定理 3.1.4 逆元的运算性质

- $(a^{-1})^{-1} = a$
- $(a*b)^{-1} = b^{-1} * a^{-1}$
- $a^{-1} * a = a * a^{-1} = e$
- $a^{-1}x(b^{-1}xa^{-1}) = axa^{-1} = e$

证明：

$$(a*b)^{-1} = \text{设 } (a*b)^{-1} = x,\ (a*b)x = e$$
$$\Longrightarrow\ a(bx) = e \ \Longrightarrow\ bx = a^{-1} \ \Longrightarrow\ x = b^{-1}a^{-1}$$

3.2 有限群和陪集分解

定义 3.2.1 有限群

元素个数有限的群 G 称为有限群。其元素个数称为群的阶，记做 $|G|$。

例如，$\langle \mathbb{Z}_m, + \rangle$ 是有限群，其阶为 m。

$\langle \mathbb{Z}_m^*, \cdot \rangle$ 是有限群 $(\forall a \in \mathbb{Z}_m^*, (a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m})$，其阶为 $\varphi(m)$。

问题 3.2.1

对于有限群 G，其阶为 $|G|$，则 $\forall a \in G$，方程 $a^x \equiv 1_G \pmod{|G|}$ 是否一定有解？

证明： 设 $|G| = k$

直接累乘，找到 $a^{x_1} = a^{x_2} \in G \Rightarrow a^{x_2 - x_1} = 1_G$，(群的阶是有限的，但是幂次是无限的)

取 $\forall a \in G$，有 $a^1, a^2, \cdots, a^{k+1} \in G$，由抽屉原理 $\exists 1 \leq i < j \leq k+1, a^i = a^j$，则 $a^{j-i} = 1_G$，所以 $a^x \equiv 1_G \pmod{|G|}$ 一定有解。

问题 3.2.2

对于有限群 G，其阶为 $|G|$，则 $\forall a \in G$，方程 $a^x \equiv 1_G \pmod{|G|}$ 一定有解，那 $|G|$ 是否是一个解呢？

定义 3.2.2 元素的阶

设 $a \in G$，若存在最小正整数 r 使得 $a^r = 1_G$，则称 r 为元素 a 的**阶**，记作 $|a| = r$。

定理 3.2.1 阶的性质

设 $a \in G$ 的阶为 r，则对任意整数 k，若 $a^k = 1G$，必有 $r \mid k$。

证明： 设 $a \in G$ 的阶为 r，则集合 $H = \{a^1, a^2, \ldots, a^r\}$ 是 G 的一个子群，且 $|H| = r$。

显然 H 对群运算封闭，且包含单位元 $a^r = 1_G$。

对任意 $a^i \in H$，其逆元为 $a^{r-i} \in H$。

因此 H 是 G 的子群，称为由 a 生成的**循环子群**。

下面我们直接来证明子群的阶整除群的阶。

定义 3.2.3 子群

群 $\langle H, \cdot \rangle$ 是 $< G, \cdot >$ 的子群，如果 $H \subseteq G$.

定理 3.2.2 Lagrange 定理

若 H 是 G 的子群，且 G 是有限群，则 $|H| \mid |G|$

证明： 若 $|H| = |G|$，显然 $|H| \mid |G|$.

不妨考虑 $|H| < |G|$，则 $\exists\, x_1 \in G, x_1 \notin H$，构建 H_1：$H_1 = x_1 \cdot H = \{x_1 \cdot y \mid y \in H\}$

引理 3.2.1

$|H| = |H_1|$

证明： 即证 $\forall\, y_1, y_2 \in H, y_1 \neq y_2,\ x_1 \cdot y_1 \neq x_1 \cdot y_2$

反证：设 $x_1 \cdot y_1 = x_1 \cdot y_2$，$x_1$ 在群 $|G|$ 存在 $x_1^{-1}, (x_1^{-1} \cdot x_1) \cdot y_1 = (x_1^{-1} \cdot x_1) \cdot y_2, e \cdot y_1 = e \cdot y_2$

推出 $y_1 = y_2$ 矛盾

引理 3.2.2

$H \cap H_1 = \emptyset$

证明： 反证：假设存在 $y \in H, x_1 \cdot y \in H$，取 y^{-1}，有 $y^{-1} \in H$，

又 $x_1 \cdot y \in H, (x_1 \cdot y) \cdot y^{-1} \in H$，推出 $x_1 \cdot (y \cdot y^{-1}) = x1 \cdot e = x_1 \in H$ 矛盾

由此，若 $H \cup H_1 = G, |H| = \frac{|G|}{2} \mid |G|$. 若 $H \cup H_1 \neq G, \exists\, x_2 \in G, x_2 \notin H, x_2 \notin H1$,

令 $H_2 = x_2 \cdot H = \{x_2 \cdot y \mid y \in H\}$，同理有 $|H_2| = |H|, H \cap H_2 = \emptyset$,

引理 3.2.3

$H_1 \cap H_2 = \emptyset$

证明： 假设存在 $y \in H$，$s.t.\ x_2 \cdot y \in H_1 = x_1 \cdot H, then\ \exists\, z \in H$，$s.t.\ x2 \cdot y = x_1 \cdot z$，取 $y^{-1} \in H$，$x_2 \cdot y \cdot y^{-1} = x_1 \cdot z \cdot y^{-1}$，$x_2 = x_1 \cdot (z \cdot y^{-1})$，又 $z \cdot y^{-1} \in H$，推出 $x_2 \in x_1 \cdot H = H_1$ 矛盾

若 $H \cup H_1 \cup H_2 = G$，$|H| = \frac{|G|}{3} || |G|$

否则递推可得 $H_0 \cup H_1 \cup H_2 \cup ... \cup H_k = G$，且有 $\forall i \in \{1, 2, ..., k\}$，$|H_i| = |H_0|$

$\forall\, i, j \in \{0, 1, 2, ..., k\}$，$H_i \cap H_j = \emptyset$，则可得 $|H| = \frac{|G|}{k+1} \mid |G|$

称 $G = H \cup x_1 \cdot H \cup x_2 \cdot H \cup ... \cup x_k \cdot H$ 为 G 关于子群的（左）陪集分解;

$G = H \cup H \cdot y_1 \cup H \cdot y_2 \cup ... \cup H \cdot y_k$ 为 G 关于子群的（右）陪集分解

定义 3.2.4 陪集

设 H 是群 G 的子群，$a \in G$，则：

- $aH = \{ah \mid h \in H\}$ 称为 H 的**左陪集**
- $Ha = \{ha \mid h \in H\}$ 称为 H 的**右陪集**

注： 显然 $eH = H = He$，其中 e 是单位元。

定理 3.2.3 陪集分解

群 G 可以分解为不相交的左陪集（或右陪集）的并集：

$$G = a_1H \cup a_2H \cup \cdots \cup a_kH$$

其中 a_iH 两两不相交，且所有陪集的大小都等于 $|H|$。

定义 3.2.5 正规子群

子群 H 称为 G 的**正规子群**，如果对任意 $a \in G$，都有 $aH = Ha$。记作 $H \triangleleft G$。

注： 对于交换群，所有子群都是正规子群。

定义 3.2.6 商群

若 $H \triangleleft G$，则集合 $G/H = \{aH \mid a \in G\}$ 在运算 $(aH) \cdot (bH) = (ab)H$ 下构成群，称为**商群**。

定理 3.2.4 商群的性质

- 单位元：$eH = H$
- 逆元：$(aH)^{-1} = (a^{-1})H$
- 阶：$|G/H| = \frac{|G|}{|H|}$

例：整数模 m 的商群：
考虑群 $(\mathbb{Z}, +)$ 和其子群 $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\}$。
由于 $(\mathbb{Z}, +)$ 是交换群，$m\mathbb{Z}$ 是正规子群。
不同的陪集为：$0 + m\mathbb{Z}, 1\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$。
商群 $\mathbb{Z}/m\mathbb{Z}$ 在运算 $(a + m\mathbb{Z}) + (b + m\mathbb{Z}) = (a + b) + m\mathbb{Z}$ 下与 $(\mathbb{Z}_m, +)$ 同构。

3.3 循环群和群同构

3.3.1 循环群

定义 3.3.1 循环群

群 G 是循环群，若存在 $a \in G$ 使得 $G = \langle a \rangle = \{a^k, (a^{-1})^s \mid k \geq 0, s \geq 0\} = \{a^t \mid t \in \mathbb{Z}\}$。
若 $G = \langle a \rangle$，则称 $\langle G, * \rangle$ 为循环群，a 称为生成元。

例：

- $\langle \mathbb{Z}, + \rangle$ 是循环群，生成元为 ± 1
- $\langle \mathbb{Q}, + \rangle$ 不是循环群
- $\langle \mathbb{Q} \setminus \{0\}, \times \rangle$ 不是循环群
- $\langle 1$ 的 n 次单位根$, \times \rangle$ 是循环群，生成元为 $e^{\pm i \frac{2\pi}{n} k}$，其中 $(k, n) = 1$

问题 3.3.1

循环群的生成元是否唯一？

答： 答案是否定的，生成元不唯一。以下是两个例子：

1. **n 次单位根群**：$\langle \{1\ n\quad\}, \times \rangle$ 的生成元为 $e^{i2\pi k}$，其中 $(k, n) = 1$。
   因此其生成元有 $\varphi(n)$ 个。

2. **模 m 加法群**：$\langle \mathbb{Z}_m, + \rangle$（其中 $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ 为模 m 的完全剩余系）
   若 $a \in \mathbb{Z}_m$ 为生成元，则等价于：
   - $\forall b \in \mathbb{Z}_m, \exists k \in \mathbb{Z}$ 使得 $ka \equiv b \pmod{m}$
   - $\exists k \in \mathbb{Z}$ 使得 $ka \equiv 1 \pmod{m}$
   - $(a, m) = 1$

   因此 $\langle \mathbb{Z}_m, + \rangle$ 的生成元有 $\varphi(m)$ 个。

问题 3.3.2

那 $\langle \mathbb{Z}_m, \times \rangle$，模 m 的乘法群的性质呢？

定理 3.3.1 循环群生成元的个数

- 对任意有限循环群 G_m，G_m 中有 $\varphi(m)$ 个生成元
- 对任意无限循环群 G，G 中只有两个生成元：$\langle a\rangle$ 和 $\langle a^{-1}\rangle$

注： 引入群同构再证明上述结论。

3.3.2 群同构

定义 3.3.2 群同态

设 $(G,*)$ 和 $(H,\circ)$ 是两个群。如果存在一个映射 $f:G\to H$，使得对任意 $a,b\in G$，都有

$$f(a*b)=f(a)\circ f(b)$$

则称 f 为一个**群同态**（*Group Homomorphism*）。群同态保持群的运算结构。

定义 3.3.3 群同构

如果群同态 $f:G\to H$ 是一个双射（即既是单射又是满射），则称 f 为一个**群同构**（*Group Isomorphism*）。若存在群同构，则称群 G 与群 H **同构**，记作 $G\cong H$。同构的群在代数结构上是完全相同的，可以看作是同一个群的不同表示。

例：

1. $\langle\mathbb{Z},+\rangle\cong\langle 2\mathbb{Z},+\rangle$（整数加法群与偶数加法群同构）

   映射：$f(x)=2x$

2. $\langle\mathbb{Z}_m,+\rangle\cong\langle C_m,\times\rangle$（$C_m=\{e^{\pm i\frac{2\pi}{m}k}\mid k\in\mathbb{Z}\}$，模 m 加法群与 m 次单位根群同构）

   映射：$f(k)=e^{i\frac{2\pi}{m}k}$

   验证：$f(k_1+k_2)=e^{i\frac{2\pi}{m}(k_1+k_2)}=e^{i\frac{2\pi}{m}k_1}\cdot e^{i\frac{2\pi}{m}k_2}=f(k_1)\cdot f(k_2)$

定理 3.3.2 同构的主要性质

设 $f: G \to G'$ 是一个群同构，则：

1. $f(e) = e'$（单位元映射到单位元）
2. $f(a^{-1}) = (f(a))^{-1}$（逆元映射到逆元）
3. 若 G 是交换群，则 G' 也是交换群
4. 若 G 是循环群，则 G' 也是循环群
5. 若 G 是有限群，则 $|G| = |G'|$（同阶）
6. 若 G 是无限群，则 G' 也是无限群
7. 若 G 有阶为 n 的元素，则 G' 也有阶为 n 的元素
8. 若 G 有 k 个阶为 n 的元素，则 G' 也有 k 个阶为 n 的元素

证明：

1. **单位元性质：** 对任意 $a \in G$，有

$$f(a) = f(e * a) = f(e) \circ f(a)$$
$$f(a) = f(a * e) = f(a) \circ f(e)$$

因此 $f(e)$ 是 G' 中的单位元。

2. **逆元性质：** 对任意 $a \in G$，有

$$f(a * a^{-1}) = f(e) = e' = f(a) \circ f(a^{-1})$$
$$f(a^{-1} * a) = f(e) = e' = f(a^{-1}) \circ f(a)$$

因此 $f(a^{-1}) = (f(a))^{-1}$。

3. **交换性保持：** 若 G 是交换群，则对任意 $a, b \in G$，有 $a*b = b*a$。因此 $f(a*b) = f(b*a)$，即 $f(a) \circ f(b) = f(b) \circ f(a)$，所以 G' 也是交换群。

4. **循环性保持：** 若 $G = \langle a \rangle$，则对任意 $x \in G$，存在整数 k 使得 $x = a^k$。因此 $f(x) = f(a^k) = (f(a))^k$，所以 $G' = \langle f(a) \rangle$。

5. **阶数相等：** 由于 f 是双射，所以 $|G| = |G'|$。

6. **无限性保持：** 若 G 是无限群，则 G' 也必须是无限群。

7. **元素阶数保持：** 若 $a \in G$ 的阶为 n，则 $a^n = e$ 且 n 是最小的正整数。因此 $(f(a))^n = f(a^n) = f(e) = e'$，且 n 是使 $(f(a))^n = e'$ 成立的最小正整数，所以 $f(a)$ 的阶也是 n。

8. **同阶元素个数保持：** 由于 f 是双射且保持元素阶数，所以同阶元素的个数也保持不变。

例：

1. $\langle \mathbb{Z}, + \rangle \cong \langle 2\mathbb{Z}, + \rangle$（整数加法群与偶数加法群同构）

   映射：$f(x) = 2x$

2. $\langle \mathbb{R}^+, \times \rangle \cong \langle \mathbb{R}, + \rangle$（正实数乘法群与实数加法群同构）

   映射：$f(x) = \ln x$

3. $\langle \mathbb{Z}_m, + \rangle \cong \langle C_m, \times \rangle$（模 m 加法群与 m 次单位根群同构）

   映射：$f(k) = e^{i\frac{2\pi}{m}k}$

   验证：$f(k_1 + k_2) = e^{i\frac{2\pi}{m}(k_1+k_2)} = e^{i\frac{2\pi}{m}k_1} \cdot e^{i\frac{2\pi}{m}k_2} = f(k_1) \cdot f(k_2)$

定理 3.3.3 无限循环群同构于整数加法群

设 $G = \langle a, * \rangle$ 是无限循环群，则 $G \cong \langle \mathbb{Z}, + \rangle$。

证明： 定义映射 $f : \langle \mathbb{Z}, + \rangle \to G$ 为 $f(k) = a^k$，其中 $a^0 = e$（单位元），a^{-1} 是 a 的逆元。

1. **同态性：** 对任意 $i, j \in \mathbb{Z}$，有

$$f(i + j) = a^{i+j} = a^i * a^j = f(i) * f(j)$$

2. **双射性：** 显然为一一映射（双射）

因此无限循环群 G_a 同构于 $\langle \mathbb{Z}, + \rangle$。

定理 3.3.4 无限循环群的生成元个数

无限循环群 G 只有两个生成元，与 $\langle \mathbb{Z}, + \rangle$ 的生成元一一对应。

证明： $\langle \mathbb{Z}, + \rangle$ 只有两个生成元：1 和 -1。

反证法： 假设 $b = a^k$ 是 G 的生成元，其中 $k \neq \pm 1$。

若 $G=\{(a^k)^j \mid j\in\mathbb{Z}\}$，则逆映射 f^{-1} 将 G 映射到 $\{k,2k,3k,\ldots,-k,-2k,-3k,\ldots\}$，这必须等于 $\mathbb{Z}$。因此 $k=\pm1$，矛盾。

另一种证明： 若 a^k 是 G 的生成元，则 a 必须能表示为 a^k 的幂，即存在整数 m 使得 $a=(a^k)^m$。

对两边应用逆同构 f^{-1}：

$$f^{-1}(a)=f^{-1}((a^k)^m)$$

由于 $f^{-1}(a)=1$ 且 $f^{-1}((a^k)^m)=km$，所以 $1=km$。

这意味着 $k=\pm1$ 且 $m=\pm1$，与假设 $k\neq\pm1$ 矛盾。

定理 3.3.5 有限循环群的同构

任意 m 阶有限循环群均同构于 $\langle\mathbb{Z}_m,+\rangle$。

证明： 设 $G=\langle a,*\rangle=\{e,a^1,a^2,\ldots,a^{m-1}\}$ 是一个 m 阶循环群，其中 e 是单位元，且 a 的阶为 m（即 $a^m=e$，且 m 是使此式成立的最小正整数）。

定义映射 $f:\mathbb{Z}_m\to G$ 为 $f(k)=a^k$。

1. **同态性：** 对任意 $i,j\in\mathbb{Z}_m$，我们有：

$$f(i+j)=a^{i+j}\quad\text{（根据映射定义）}$$

同时，在群 G 中，

$$f(i)*f(j)=a^i*a^j=a^{i+j}\quad\text{（根据群运算规则）}$$

因此，$f(i+j)=f(i)*f(j)$，映射 f 保持群运算。

2. **映射的良定义性与双射性：**

- **良定义性：** 若 $k_1\equiv k_2\pmod m$，则 $m\mid(k_1-k_2)$。由于 a 的阶为 m，这意味着 $a^{k_1-k_2}=e$，从而 $a^{k_1}=a^{k_2}$。所以 $f(k_1)=f(k_2)$，映射 f 是良定义的。
- **单射性：** 若 $f(k_1)=f(k_2)$，则 $a^{k_1}=a^{k_2}$，这意味着 $a^{k_1-k_2}=e$。由于 a 的阶为 m，所以 $m\mid(k_1-k_2)$，即 $k_1\equiv k_2\pmod m$。因此 f 是单射。
- **满射性：** 由于 $\mathbb{Z}_m$ 和 G 都是 m 阶有限群（元素个数均为 m），且 f 是单射，所以 f 也是满射。

综上，f 是一个双射，两群同构。

定理 3.3.6 同构群的生成元个数

m 阶循环群 $\langle G,*\rangle$ 和 $\langle \mathbb{Z}_m,+\rangle$ 的生成元个数相等，均为 $\varphi(m)$。

证明：

1. $\langle \mathbb{Z}_m,+\rangle$ **的生成元：** 在模 m 加法群 $\langle \mathbb{Z}_m,+\rangle$ 中，元素 $k\in\mathbb{Z}_m$ 是其生成元当且仅当 $\gcd(k,m)=1$。根据欧拉函数的定义，满足此条件的整数 k 的个数为 $\varphi(m)$。

2. $\langle G,*\rangle$ **的生成元：** 设 a 是 G 的一个生成元（即 $G=\langle a\rangle$）。我们证明 $a^k\in G$ 是 G 的生成元当且仅当 $\gcd(k,m)=1$。

   - **若 $\gcd(k,m)=1$，则 a^k 是 G 的生成元：** 由于 $\gcd(k,m)=1$，根据数论性质，对于任意 $i\in\mathbb{Z}_m$，同余方程 $kb\equiv i\pmod m$ 存在整数解 b。这意味着对于 G 中的任意元素 a^i（因为 a 是生成元，所有元素都可以表示为 a^i 的形式），我们可以找到一个整数 b 使得 $(a^k)^b=a^{kb}=a^i$。因此，a^k 可以生成 G 中的所有元素，即 a^k 是 G 的生成元。
   - **若 a^k 是 G 的生成元，则 $\gcd(k,m)=1$：** 如果 a^k 是 G 的生成元，那么 a^k 必须能够生成 G 中的所有元素，特别是 a^1（即 a 本身）。所以存在一个整数 b 使得 $(a^k)^b=a^1$，即 $a^{kb}=a^1$。这意味着 $kb\equiv 1\pmod m$。根据线性同余方程有解的条件，此方程有解当且仅当 $\gcd(k,m)\mid 1$，即 $\gcd(k,m)=1$。

   因此，$\langle G,*\rangle$ 的生成元个数也为 $\varphi(m)$。

定理 3.3.7 同构保持生成元

设 $f:G\to H$ 是一个群同构。如果 a 是群 G 的一个生成元，那么 $f(a)$ 是群 H 的一个生成元。

证明： 由于 a 是 G 的生成元，所以对任意 $x\in G$，存在整数 k 使得 $x=a^k$。因为 f 是同构，它保持群运算，所以 $f(x)=f(a^k)=(f(a))^k$。又因为 f 是满射（同构的性质），对任意 $y\in H$，存在 $x\in G$ 使得 $f(x)=y$。所以 $y=f(x)=(f(a))^k$。这意味着 $f(a)$ 可以生成 H 中的所有元素，因此 $f(a)$ 是 H 的一个生成元。

注： 上述定理说明，同构映射在群结构上是”保持”生成元的。这意味着如果两个群同构，它们不仅在元素数量上相等，而且在生成元的数量和对应关系上也保持一致。

3.3.3 自同构

定义 3.3.4 群的自同构

群 G 的**自同构**（*Automorphism*）是从 G 到 G 自身的同构映射。所有自同构的集合记为 $Aut(G)$。

定理 3.3.8 自同构群

$Aut(G)$ 在函数复合运算下构成一个群，称为 G 的**自同构群**。

证明：

1. **封闭性：** 若 $f, g \in Aut(G)$，则 $f \circ g$ 也是 G 到 G 的同构映射。
2. **结合律：** 函数复合满足结合律。
3. **单位元：** 恒等映射 id_G 是自同构，且是单位元。
4. **逆元：** 若 $f \in Aut(G)$，则 f^{-1} 也是自同构，且是 f 的逆元。

定理 3.3.9 $\langle \mathbb{Z}_m, + \rangle$ 的自同构

$\langle \mathbb{Z}_m, + \rangle$ 的自同构群 $Aut(\langle \mathbb{Z}_m, + \rangle)$ 同构于 $\langle \mathbb{Z}_m^*, \times \rangle$（模 m 乘法群）。

证明： 设 f_a 是 $\langle \mathbb{Z}_m, + \rangle$ 的自同构，定义为 $f_a(x) = ax$，其中 $(a, m) = 1$。

1. **同态性：** $f_a(x + y) = a(x + y) = ax + ay = f_a(x) + f_a(y)$
2. **双射性：** 由于 $(a, m) = 1$，所以 f_a 是双射
3. **复合运算：** $f_a \circ f_b = f_{ab}$

因此，$Aut(\langle \mathbb{Z}_m, + \rangle) \cong \langle \mathbb{Z}_m^*, \times \rangle$。

例：

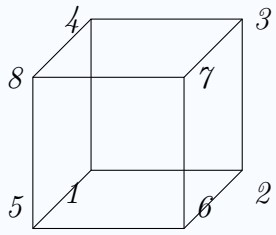
1. $\delta_1 : 1 \to 1, 2 \to 2, \ldots$ 对应 $f(\delta_1) = 1$
2. $\delta_a : 1 \to a$，其中 $(a, m) = 1$，则 $2 \to 2a, \ldots, m-1 \to (m-1)a$ 对应 $f(\delta_a) = a$

注： 本法用于定义加法运算的自同构。

3.4 置换群和轨道公式

接下来来介绍一下置换群的基本概念.

问题 3.4.1



有多少种旋转方法使得此正方体绝对位置不变？

保持“绝对位置”不变的所有置换构成一个置换群：

定义 3.4.1 置换

有限集合 D 上的一一映射被称为 D 上的置换.

以集合 $[n]=\{1,2,3,...,n\}$ 为例, $[n]$ 上的一个置换是将 $\{1,2,...,n\}$ 映射为 $\{\delta(1),\delta(2),...,\delta(n)\}$ 的一个一一映射.

在此基础上, 可以定义置换的复合运算 $\circ$. 一个置换 $\delta_1\circ\delta_2$ 等价于这样一个置换：对于有限集合 D 中的元素 x, 先将 x 通过置换映射为 $\delta_1(x)$, 然后将 $\delta_1(x)$ 映射为 $\delta_2(\delta_1(x))$.

将 $\delta_1\circ\delta_2$ 作用在 $[n]=\{1,2,...,n\}$ 上, $[n]$ 会被映射为 $\{\delta_1(\delta_2(1)),\delta_1(\delta_2(2)),...,\delta_1(\delta_2(n))\}$.

定理 3.4.1

$[n]=\{1,2,3,...,n\}$ 上所有置换的集合 S_n 关于置换的复合运算 $\circ$ 构成群, 叫做 n 元对称群, 通常记为 S_n.

证明： 1. 封闭性. 由上述复合运算的定义可以看到, $\delta_1\circ\delta_2\in S_n$, 即运算满足封闭性.

2. 由于映射的复合运算符合结合律, 因此置换的复合运算也满足结合律.

3. 单位元. 群 $\langle S_n,\circ\rangle$ 的单位元是这样的一个置换 $e_n(i)$, 使得每个元素都被映射到它本身.

因此 $\forall\delta,\forall i\in[n]$, $e_n\circ\delta(i)=e_n(\delta(i))=\delta(i)$, 因此 $e_n\circ\delta=\delta$ 同样的, $\forall\delta,\forall i\in[n]$, $\delta\circ e_n(i)=\delta(e_n(i))=\delta(i)$, 因此 $\delta\circ e_n=\delta$.

4. 逆元. 一个置换 δ 的逆元 δ^{-1} 被定义为 $\delta^{-1}(\delta(i))=i$, 容易验证 $\delta^{-1}\circ\delta=\delta\circ\delta^{-1}=e_n$

S_n 的阶数为 $|n!|$, S_n 的子群叫做 n 元置换群.

定义 3.4.2

对任意群 G, 任意集合 X, 且 G 是一个有限群, X 是一个有限集合. 定义一个二元函数 $G \times X \to X$ 为群 G 在集合 X 上的作用. 满足如下两条公理

1. $\forall g \in G, \forall a \in X, g(a) \in X$
2. $\forall g_1, g_2, \forall a \in X, (g_1 \circ g_2)(a) = g_1(g_2(a))$

考虑置换群 A_n 以及集合 $[n]$ 上的作用, 满足以下:

1. $\forall \delta \in A_n, \delta(i) \in [n]$
2. $\forall \delta_1 \delta_2 \in A_n, (\delta_1 \circ \delta_2)(i) = \delta_1(\delta_2(i))$

考虑集合 $O_a : \{g(a) | g \in G\}$, 称之为集合中的一个元素 a 在群 G 的作用下的轨道. 可以看到, 其代表的含义为元素 a 在群 G 的作用下, 所有的可能的取值.

接着考虑集合 $G_a : \{g \in G | g(a) = a\}$. 下面证明, G_a 关于置换的复合运算 $\circ$ 构成一个群.

1. 封闭性: $\forall g_1, g_2 \in G, (g_1 \circ g_2)(a) = g_1(g_2(a)) = g_1(a) = a$, 因此 $g_1 \circ g_2 \in G$
2. 结合律: 置换的结合律由映射的结合律保证.
3. 单位元: 容易验证恒等变换 e_n 是群的单位元.
4. 逆元: $\forall g \in G, g^{-1}(a) = g^{-1}(g(a)) = (g^{-1} \circ g)(a) = e(a) = a$, 即 $g^{-1} \in G$.

由引理 4.4, G_a 是 G 的一个子群, 可以知道 $G = G_a \cup g_b \circ G_a \cup g_c \circ G_a \cup \cdots$. 其中 $g_b \circ G_a = \{g_b \circ g | g \in G_a\}$, 是所有将元素 a 映射为 b 的集合. 因此我们可以得到轨道公式:

定理 3.4.2 轨道公式

$|G| = |G_a| \cdot |O_a|$, 其中 G_a 是 G 中保持元素 a 不变的置换构成的子群, O_a 是 a 在 G 中的轨道.

接下来回到最开始的问题:

问题 3.4.2

存在多少种不同的旋转方式, 使得正方体的位置保持不变.

证明： 正方体的旋转方式可以使用一个在 [8] 上的置换进行表示，因此保持正方体位置不变的置换构成 S_8 的子群.

首先考虑所有保持顶点 *1* 不变的置换方式，容易想到，一共只有三种方式：绕着体对角线旋转 *120°*, *240°*, 以及保持不动. 即 $|G_a| = 3$, 此外，顶点 a 在置换的作用下，一共有 *8* 种可能的取值（对应立方体的八个顶点），因此 $|O_a| = 8$, 因此 $|G| = |G_a| \cdot |O_a| = 24$

练习 3.4.1

考虑可重复圆排列问题.

以一个简单的例子来说明轨道定理在解决可重复圆排列的作用. 考虑长为 4 的圆排列，且仅有两个元素 $\{R, B\}$, 那么集合 X 可以被定义为：$X : \{\{1, 2, 3, 4\} \to \{R, B\}\}$, 并且考虑置换群 A_4. 考虑 X 中的元素 δ, $\delta(1) = R, \delta(2) = R, \delta(3) = R, \delta(4) = R$, 那么 $|G_a| = 4$, 可以得到 $|O_a| = 2^4/|G_a| = 4$.

3.5 环、整环和域

定义 3.5.1 环

设 $(R,+,\times)$ 是一个集合 R 上带有加法和乘法的代数结构，若满足：

- $(R,+)$ 是 *Abel* 群（即加法封闭、结合律、单位元、逆元、交换律）
- 乘法 $\times$ 对 R 封闭，且满足结合律
- 乘法对加法分配：$\forall a,b,c\in R$，有

$$a\times(b+c)=a\times b+a\times c,\quad (a+b)\times c=a\times c+b\times c$$

则称 $(R,+,\times)$ 为一个**环**。

注：

- 这里对加法的单位元我们称之为零元，记作 0_R。
- 若 $(R,\times)$ 中存在单位元 1_R，则称 R 为**含幺环**。
- 若乘法满足交换律，则称 R 为**交换环**。
- **不过我们在这门课上提到的大多数直接指的就是含幺环。**

例：

- $(\mathbb{Z},+,\times)$ 整数环
- $(\mathbb{Q},+,\times)$ 有理数环
- $(\mathbb{Z}_m,+,\times)$ 模 m 的整数环
- $(\mathbb{Z}[x],+,\times)$ 整系数多项式环
- $(\mathbb{Z}[i],+,\times)$ 高斯整数环
- $M_2(\mathbb{Z})$，即 2×2 整矩阵环

注： $(\mathbb{E}ven,+,\times)$（偶数加法与乘法）不是环，因为乘法没有单位元。
注： $M_2(\mathbb{Z})$ 不是交换环，因为矩阵乘法不可交换。

定义 3.5.2 整环

若交换环 $(R,+,\times)$ 中，R 无零因子（即 $\forall a,b\in R, ab=0 \implies a=0$ 或 $b=0$），则称 R 为**整环**（*Integral Domain*）。

注： 整环一定是交换环且无零因子。

例：

- $(\mathbb{Z},+,\times)$ 整数环
- $(\mathbb{Z}[x],+,\times)$ 整系数多项式环
- $M_2(\mathbb{Z})$ 整数二阶矩阵环**不是**整环，因为存在非零矩阵 A,B 使 $AB=0$。例如

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

定义 3.5.3 域

若交换环 $(F,+,\times)$ 中，$F\setminus\{0\}$ 在乘法下构成 *Abel* 群（即每个非零元都有乘法逆元），则称 F 为**域**（*Field*）。

例：

- $(\mathbb{Q},+,\times)$
- $(\mathbb{R},+,\times)$
- $(\mathbb{C},+,\times)$
- $(\mathbb{Q}(x),+,\times)$ 有理函数域
- $(\mathbb{Z}_p,+,\times)$，p 为素数时的模 p 整数域

注：

- 域比整环多了“每个非零元都有乘法逆元”
- 整环比一般交换环多了“无零因子”

定理 3.5.1

域一定是整环，但整环不一定是域（如 $\mathbb{Z}$）

证明： 设 F 是域，任取 $a \neq b \in F$，则必有一个不是零元，设 $a \neq 0_F$，如果 $ab = 0_F$，a 有逆元 a^{-1}，则 $a^{-1}ab = a^{-1}0_F = 0_F = b$，因此 F 是整环。

反之，整环不一定是域。例如 $\mathbb{Z}$ 是整环，但不是域，因为 $\mathbb{Z}$ 中没有乘法逆元。

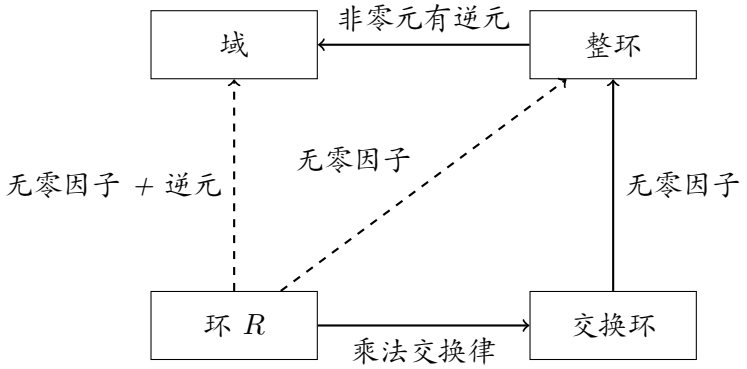
定理 3.5.2 有限整环一定是域（有限无零因子交换环必有逆元）

有限整环 R 中，任取 $0 \neq a \in R$，则存在 $b \in R$ 使 $ab = 1$，即 R 为域。

证明要点

- 取 $a \neq 0$，考虑 $\{a, a^2, a^3, \ldots\}$，因 R 有限，必有 $a^i = a^j$，$i > j$，得 $a^{i-j} = 1$。
- 由无零因子可推出 a 可消去，故存在 b 使 $ab = 1$。

总结



3.6 环的理想

定义 3.6.1 理想

设 R 为环，$I \subseteq R$。若：

1. $\forall x, y \in I$，有 $x - y \in I$（I 是 R 的加法子群）
2. 对任意 $r \in R, x \in I$，有 $rx \in I$ 且 $xr \in I$

则称 I 为 R 的一个**理想**，记作 $I \triangleleft R$。
若 R 为交换环，则只需 $rx \in I$。

证明： 证明 I 是 R 的加法子群：

- 单位元：$x - x = 0 \in I$
- 逆元：$x \in I$，则 $0 - x = -x \in I$
- 封闭性：$x, y \in I$，有 $-y \in I$，则 $x - (-y) \in I$
- 结合律：由环的结合律，故 I 上结合律也满足

例：

- $\langle 2 \rangle = 2\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想。
- $\langle k \rangle = k\mathbb{Z}$ 是 $\mathbb{Z}$ 的理想。
- $\langle \mathbb{Z}_6, +, \cdot \rangle$ 中，$\{0, 3\}$ 是 $\mathbb{Z}_6$ 的理想。

定义 3.6.2 主理想

设 R 为交换环，$a \in R$，$aR = \{ar \mid r \in R\}$ 称为 R 中由 a 生成的**主理想**。若 I 是 R 的主理想，则 $I = aR$。

证明： 证明 aR 是 R 的理想：

- $\forall x, y \in aR$，有 $x - y = ax' - ay' = a(x' - y')$，而 $x' - y' \in R$，故 $x - y \in aR$
- $\forall r \in R, x \in aR$，有

$$rx = rax' = a(rx') \in aR \quad \text{（用到了交换环的性质）}$$
$$xr = ax'r = a(x'r) \in aR$$

例： $\mathbb{Z}$ 中任意理想都是主理想，如 $\langle 12\rangle = 12\mathbb{Z}$。

$\langle 9, 12\rangle = \{9s + 12t \mid s, t \in \mathbb{Z}\}$ 等价于所有 3 的倍数、是 $\mathbb{Z}$ 的主理想。

定义 3.6.3 主理想环

若环 R 的任意理想都是主理想，则称 R 为**主理想环**（*PIR, Principal Ideal Ring*）。

若加上整环条件，则称 R 为**主理想整环**（*PID, Principal Ideal Domain*）。

例： $\mathbb{Z}$ 是 *PID*。

证明： 设 $I \subseteq \mathbb{Z}$ 是非零理想，则 I 中有最小正整数 a。证 $I = a\mathbb{Z}$:

$a \in I$，$a\mathbb{Z} \subseteq I$。对任意 $b \in I$，用带余除法 $b = qa + r$，$0 \le r < a$，$r = b - qa \in I$。若 $r \neq 0$，与 a 最小性矛盾，故 $r = 0$，即 $b \in a\mathbb{Z}$。所以 $I = a\mathbb{Z}$。

注： $\mathbb{Z}[x]$ 不是主理想环，例如 $\{\sum_{i=0}^{k} a_i x^i \mid i \in \mathbb{N}, a_0 \in \mathbb{Z}, 2 \mid a\}$ 是理想但不是主理想（不满足吸收率）。

定义 3.6.4 有限生成理想

设 R 为环，$a, b \in R$，则 $aR + bR = \{ar_1 + br_2 \mid r_1, r_2 \in R\}$ 是 R 的一个理想，称为由 a, b 生成的理想。

更一般地，若 $S = \{a_1, \ldots, a_k\}$，则 S 生成的理想为 $SR = \{a_1r_1 + \cdots + a_kr_k \mid r_i \in R\}$。

定义 3.6.5 主理想环 (PID)

若 R 的每个理想都是主理想，则 R 为主理想环。

例：

- $\mathbb{Z}$ 是 *PID*;
- $\mathbb{Z}[x]$ 不是 *PID*，可以有 $\{2, x\}\mathbb{Z}[x]$ 的环不是主理想;
- $\mathbb{Q}[x]$ 是 *PID*;

  证明： 设 $I \subseteq \mathbb{Q}[x]$ 是任意理想。取 I 中次数最小的首一多项式 $r(x)$（唯一到相联）。

  证 $I = \langle r(x)\rangle$。反证：假设存在 $b(x) \in I$，但 $b(x) \notin \langle r(x)\rangle$。

  做带余除法，$b(x) = k(x)r(x) + r'(x)$，其中 $\deg(r'(x)) < \deg(r(x))$ 且 $\deg(r'(x)) > 0$。

  由于 $r'(x) = b(x) - k(x)r(x)$，且 $b(x) \in I$，$k(x)r(x) \in I$，故 $r'(x) \in I$。

  这与 $r(x)$ 是 I 中次数最小的多项式矛盾。

  因此 $r(x) \mid b(x)$，即 $b(x) \in \langle r(x)\rangle$。则 $I = \langle r(x)\rangle$，即 $\mathbb{Q}[x]$ 是 *PID*。

定理 3.6.1

设 R 为 PID，则 R 的任意两个元素 a,b 生成的理想 $aR+bR$ 是主理想，且 $aR+bR=dR$，其中 d 为 a,b 的最大公因子。

思路 对任意 $a,b\in R$，$aR+bR$ 是主理想，设 $aR+bR=dR$，则 d 整除 a,b，且 d 是 a,b 的最大公因子。

定义 3.6.6 欧几里得环 (ED)

若 R 为整环，存在 $\delta:R\to\mathbb{N}$，满足：

- $\delta(0)=0$，$\delta(a)>0$ $(a\neq 0)$
- $\forall a,b\in R$ $(b\neq 0)$，存在 $q,r\in R$，使 $a=qb+r$，$0\leq\delta(r)<\delta(b)$

则 R 为欧几里得环（$Euclidean\ Ring$，ER）。

定理 3.6.2

凡是可以做带余除法的环都是欧式整环。且欧式整环一定是 PID。(反之不一定成立)

定义 3.6.7 唯一分解环 (UFD)

若 R 为整环，R 中每个非零非单位元都能唯一分解为不可约元的乘积（唯一性指分解式中各因子的顺序和单位元的不同），则 R 为唯一分解环（UFD）。

问题 3.6.1

什么样的环可以做唯一分解？

证明： 对于含幺交换环 R，定义 $\delta:R\to\mathbb{N}$，定义：

- 单位：$e\in R$ 表示 $\exists a\in R, eb=1_R$
- 素元：$p\in R$ 为素元，则 $\forall a,b\in R, p\mid ab\implies p\mid a$ 或 $p\mid b$
- 不可约元：$p\in R$ 为不可约元，则 $p=ab$ 则 a 或 b 为单位

素元一定是不可约元，但不可约元不一定是素元；
若不可约元 $\iff$ 素元，则 R 为 UFD。

注： $\mathbb{Z}$ 是 UFD，$\mathbb{Z}[\sqrt{-5}]$ 不是 UFD，如 $6=(1+\sqrt{-5})(1-\sqrt{-5})=2\times 3$。

定义 3.6.8 素理想和极大理想

- 素理想：$\forall a,b\in R$，若 $ab\in I$，则 $a\in I$ 或 $b\in I$，则 I 为素理想。
- 极大理想：I 为极大理想 $(I\neq R)$，若 J 为理想且 $I\subseteq J\subseteq R$，则 $J=I$ 或 $J=R$。

定义 3.6.9 素元和不可约元

- 素元：若 $p\mid ab$，则 $p\mid a$ 或 $p\mid b$，则 p 为素元。
- 不可约元：若 $p=ab$，则 a 或 b 为单位元，则 p 为不可约元。

定理 3.6.3

素元一定是不可约元。

证明： 反证：设 $p=ab$ 且 a,b 均为非单位。由素元定义 $p\mid a$ 或 $p\mid b$，不妨设 $p\mid a$，则 $\exists k\in R$ 使 $a=kp$，代入 $p=ab$ 得 $p=ab=kpb$，即 $a(kb-1)=0$。若 R 无零因子，则 $kb=1$，即 b 为单位。(故要求含幺交换整环)

定理 3.6.4

极大理想 $\Longrightarrow$ 素理想（在交换环或 *PID* 中）。

证明：

反证：设存在极大理想 I 不是素理想，则 $\exists a,b\in R$，$ab\in I$，但 $a\notin I$ 且 $b\notin I$。

现尝试构造更大的非 R 理想来推矛盾。

若 $aR=R$ 则 a 一定是一个单位 $(a^1\in R)$，若 $bR=R$ 则 b 一定是一个单位。

若 $a^{-1}ab\in a^{-1}I=I\Rightarrow b\in I$，矛盾。

则需 $aR\neq R$ 或 $bR\neq R$。此时 $I\subsetneq aR\subsetneq R$，与 I 为极大理想矛盾。

故 I 为素理想。

定理 3.6.5

在 *PID* 中：

- 主理想 $\Longleftrightarrow$ 由素元生成的理想
- 极大理想 $\Longleftrightarrow$ 由不可约元生成的理想

例： $\mathbb{Z}$ 中：

- $p\mathbb{Z}$ 为素理想 $\iff$ p 为素数 $\iff$ $p\mathbb{Z}$ 为极大理想
- $n\mathbb{Z}$ 为极大理想 $\iff$ n 为素数
- $n\mathbb{Z}$ 为主理想

3.7 子环、理想、商环

群论与环论结构对比

	群论	环论
子结构	子群	子环
“正规”结构	正规子群	理想
商结构	商群	商环

3.7.1 子环

定义 3.7.1 子环

设 R 是一个环，$S \subseteq R$，若 S 本身在环的加法和乘法下构成环，则称 S 为 R 的**子环**。

等价条件：S 为 R 的非空子集，且对任意 $a,b \in S$，有 $a-b \in S$ 且 $ab \in S$。

（即 S 在加法下为 *Abel* 群，乘法封闭，且分配律继承）

3.7.2 理想

定义 3.7.2 理想

设 R 为环，$I \subseteq R$。

- 若 $\forall a \in I, \forall r \in R$，$ra \in I$，则 I 为 R 的**左理想**。
- 若 $\forall a \in I, \forall r \in R$，$ar \in I$，则 I 为 R 的**右理想**。
- 若同时为左理想和右理想，则 I 为 R 的**双边理想**（简称理想）。

理想的本质：理想是环的“正规”子结构，能作为“模掉”的对象。

判别： I 为 R 的理想当且仅当 $\forall a,b \in I, \forall r \in R$，$a-b \in I$，$ra, ar \in I$。

3.7.3 商环

定义 3.7.3 商环

设 R 为环，I 为 R 的理想，则 $R/I = \{a+I \mid a \in R\}$，加法：$(a+I)+(b+I) = (a+b)+I$，乘法：$(a+I)\cdot(b+I) = (ab)+I$。

R/I 在上述运算下构成环，称为 R 关于理想 I 的**商环**。

（商环的定义类似于群的商群，理想的作用类似于群的正规子群）

3.7.4 举例

例： $\mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$，是 $\mathbb{Z}$ 模 $4\mathbb{Z}$ 的商环。

3.7.5 结构对比总结

- **群论：**
  - **子群**：封闭于群运算和逆元
  - **正规子群**：可作为模掉的对象，商群有良好结构
  - **商群**：G/N，N 为正规子群
- **环论：**
  - **子环**：封闭于加法、减法、乘法
  - **理想**：可作为模掉的对象，商环有良好结构
  - **商环**：R/I，I 为理想

注： 并非所有子环都是理想，只有理想才能用于构造商环。

4 组合计数

4.1 加法原理与乘法原理

组合计数的基础是所谓加法原理与乘法原理.

陈述 4.1.1 加法原理

设 A_1, A_2 为两个不交的集合, 记 $|A_1| = a_1, |A_2| = a_2$, 则从 A_1 或 A_2 中选取一个元素, 共有 $a_1 + a_2$ 种选法.

更进一步地, 设 $A_1, A_2, \ldots, A_n$ 为一列两两不交的集合, 记 $|A_i| = a_i$, 则从这些集合中选取一个元素, 共有 $\sum_{i=1}^{n} a_i$ 种选法.

根据加法原理, 我们还可以得到与之对应的所谓减法原理:

陈述 4.1.2 减法原理

设有两个集合 $A \subseteq X$, 记 $|A| = a, |X| = n$, 则从 U 中选取一个元素并确保其不在 A 中, 共有 $n - a$ 种选法.

陈述 4.1.3 乘法原理

设 A_1, A_2 为两个集合, 记 $|A_1| = a_1, |A_2| = a_2$, 则从 A_1 与 A_2 各中选取一个元素, 共有 $a_1 a_2$ 种选法.

更进一步地, 设 $A_1, A_2, \ldots, A_n$ 为一列集合, 记 $|A_i| = a_i$, 则从这些集合的每一个中选取一个元素, 共有 $\sum_{i=1}^{n} a_i$ 种选法.

根据乘法原理我们可以计算所谓的排列数.

定义 4.1.1 排列数

对于两个自然数 $k \leq n$, 定义 (n, k) 的排列数 $(n)_k = \frac{n!}{(n-k)!}$. 除了 $(n)_k$ 外, (n, k) 的排列数有时也记作 $P(n, k)$ 或 P_k^n.

根据乘法原理容易注意到, 排列数 $(n)_k$ 的组合含义为: 从 $[n]$ 中选取 k 个排成一列, 并认为两种排列相同当且仅当每个位置上的元素都对应相同, 总的排列方法数. 特别地, 当 $k = n$, 即需要将全部元素排成一列时, 总的方法数 $(n)_n = n!$. 这也正好是集合 $[n]$ 到自身的双射的数量.

以下是排列数几个常见的变种.

命题 4.1.1

(i) (圆排列数) 将集合 $[n]$ 中的元素顺时针排列成一个圆环，并认为两种排列相同当且仅当它们可以仅通过旋转得到彼此，则总的排列方法数为 $\frac{n!}{n}$.

(ii) (项链数) 将集合 $[n]$ 中的元素顺时针排列成一个圆环，并认为两种排列相同当且仅当它们可以仅通过旋转与翻折得到彼此，则总的排列方法数为 $\frac{n!}{2n}(n \geq 2)$.

证明： *(i)* 显然排列之间的相同关系是一种等价关系. 对于一个等价类中的一个排列，考虑其中某个特定元素元素的位置，容易看出每个排列可以旋转至 n 种不同的状态，故每个等价类的元素个数均为 n. 则等价类的数量为 $\frac{n!}{n}$.

(ii) 在 *(i)* 的基础上，一个排列所在的等价类还包括这个排列沿任何一处翻折得到的排列，故每个等价类的元素个数变为 $2n$. 则等价类的数量为为 $\frac{n!}{2n}$.

当然，需要注意当 $n = 1$ 时，翻折并不会带来新的排列，故总的排列方法数仍为 $\frac{1!}{1} = 1$. 这也与通过平凡的枚举法得到的数量相符.

与排列数关联紧密的是组合数. 在第一章中我们已经接触过组合数，这里我们引入正式的定义.

定义 4.1.2 组合数

对于两个自然数 $k \leq n$，定义 (n, k) 的组合数 $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. 除了 $\binom{n}{k}$ 外，(n, k) 的排列数有时也记作 $C(n, k)$ 或 C_k^n.

(n, k) 的组合数 $\binom{n}{k}$ 的组合含义同样是明确的: 从集合 $[n]$ 中选取一个 k 元子集，总的选取方法数. 我们可以基于排列数的组合含义说明二者相等: 注意到集合具有无序性，因此两个 k 元排列作为子集等价当且仅当它们含有的元素完全相同，故每个 k 元子集对应的等价类里恰有 $k!$ 个元素.

4.2 不定方程的解

下面我们运用组合数来研究不定方程的整数解的问题.

定理 4.2.1 不定方程的正整数解

对于正整数 n, 给出不定方程 $\sum_{i=1}^{k} x_i = n$, 其中 x_i 均为正整数. 则此方程的解组的个数为 $\binom{n-1}{k-1}$.

证明: 首先证明此方程的解数量有限: 每个元 x_i 均为正整数故 $x_i \geq 1$. 又因为其它元也为正整数, 故 $x_i \leq n-k+1$. 因此原方程的一组解 $(x_1, \ldots, x_k) \in [n-k+1]^k$, 而后者无疑是一个有限集.

下面我们来求解方程的解的数量:

法 1: 隔板法

将 n 个相同的物品排成一列. 在这 n 个物品形成的 $n-1$ 处间隙共插入 $k-1$ 个相同隔板, 并确保每处间隙只插入了最多一个隔板. 容易验证, 如果认为 $k-1$ 个隔板隔开形成的 k 个区间里的物品数量分别代表每个元 x_i 的值, 则每种插板方法与方程的每个整数解一一对应. 因此方程解的个数等于总的插板方法数, 即从 $n-1$ 个元素中无序地选择 $k-1$ 个的方法数. 答案即为组合数 $\binom{n-1}{k-1}$.

法 2: 数学归纳法

我们固定 n, 对 k 归纳地证明:

① $k=1$ 时, 仅有一组解 $x_1 = n$. 这与 $\binom{n-1}{k-1} = \binom{n-1}{0} = 1$ 相符.

② 若命题对于 k 成立, 则对于 $k+1$ 的情况:

考虑元 x_{k+1} 的值并对其分类讨论, 注意到其只能在 1 到 $n-k$ 中取值:

$x_{k+1} = 1$: 此时有 $\sum_{i=1}^{k} = n-1$. 根据归纳假设, 这种情况下方程的解的数量恰为 $\binom{n-2}{k-1}$;

$x_{k+1} = 2$: 此时有 $\sum_{i=1}^{k} = n-2$. 同样, 这种情况下方程的解的数量恰为 $\binom{n-3}{k-1}$;

$\ldots$

$x_{k+1} = n-k$: 此时有 $\sum_{i=1}^{k} = k$, 这种情况下方程的解的数量恰为 $\binom{k-1}{k-1} = 1$.

根据我们先前的结论, 以上情况合起来对原方程的解集构成了一个划分. 根据加法原理, 原方程的解的数量恰为 $\sum_{i=1}^{n-k} \binom{n-i-1}{k-1} = \binom{n-1}{k}$. 这就完成了证明.

注: 法 2 的证明中用到了等式 $\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1}$. 这个等式可以用等式 $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ 归纳地证明, 也可以利用组合意义证明.

据此我们可以得出如下推论:

推论 4.2.1

对于正整数 n，不定方程 $\sum_{i=1}^{n} x_i = n$ 的满足 $x_i \geq a_i \ \forall i$ (其中 a_i 均为整数) 的整数解有 $\binom{n-\sum_{i=1}^{k} a_i+k-1}{k-1}$ 组.

特别地，不定方程 $\sum_{i=1}^{n} x_i = n$ 的非负整数解有 $\binom{n+k-1}{k-1}$ 组.

证明： 我们将问题划归到定理 *2.7* 的情形：对于每个 i，设 $b_i = x_i - a_i + 1$. 则 b_i 均为正整数，问题转化为求 $\sum_{i=1}^{k} b_i = n - \sum_{i=1}^{k} a_i + k$ 的正整数解的数量. 直接利用定理 *2.7* 可得.

注： 注意为什么在 *2.8* 中插板法不再适用：以 $a_1 = \ldots = a_k = 0$，即求非负整数解的情况为例：读者或许会想到为了允许 $x_i = 0$ 这一类解存在，只需允许板插在序列的最外侧的两个位置，以及允许同一个间隙插多个板即可. 但这意味着我们无法通过组合数方便地计算插板的方法数. 如果改为逐个插板并使用乘法原理计数，则无法体现板之间的全等，会使得每种插板方案被计算多次. 越是有同一间隙插了多个板的插板方案，被重复计算的次数越少，因此也无法仿照 *2.5* 的情形用简单的除法求得等价关系的商集的大小.

练习 4.2.1

对于正整数 n，求不定方程 $\sum_{i=1}^{n} x_i = n$ 的满足 $a_i \leq x_i \leq b_i$ 的解的个数. 提示：考虑使用容斥原理.

排列数和组合数还可以用来求解如下多重排列与多重组合问题:

问题 4.2.1

现有 n 个球，每个球可能为 t 种颜色之一，且其中颜色 c_i 的球共有 k_i 个 (满足 $\sum_{i=1}^{t} k_i = n$). 颜色相同的球视为相同的. 将这 n 个求排成一列，求不同的排列方法数.

证明： 首先将这 n 个球看成不同的，任意排列这 n 个球，共有 $n!$ 种排法. 由于颜色相同的球被视为相同的，因此任意交换同种颜色的 k_i 个球得到的新排列与原排列是等价的，每个等价类里共有 $k_1!k_2!\ldots k_t! = \prod_{i=1}^{t} k_i!$ 个排列. 故等价类的数量为 $\frac{n!}{\prod_{i=1}^{t} k_i!}$.

问题 4.2.2

现有 n 个球，每个球可能为 t 种颜色之一，且其中颜色 c_i 的球共有 k_i 个 (满足 $\sum_{i=1}^{t} k_i = n$)．颜色相同的球视为相同的．从这 n 个球中取 r 个球，求不同的取法数．

证明： 问题等价于求不定方程 $\sum_{i=1}^{t} x_i = r$ 的满足 $\forall i\ 0 \le x_i \le k_i$ 的整数解的数量．这就划归到问题 *2.9*.

问题 4.2.3

在凸 n 边形中 $(n \ge 4)$，已知任意三条对角线不共点，求所有对角线总共形成的交点个数．

证明： 注意到每 4 个端点唯一确定一个对角线交点．且由于任意三条对角线不共点，不同的 4 个端点生成的对角线交点一定不同．因此问题转换为从 n 个顶点中取 4 个点的取法数，易知取法数为 $\binom{n}{4}$

注： 注意为什么直接从对角线个数出发计算交点数会带来困难：容易求出凸 n 边形共有 $\binom{n}{2} - n$ 条对角线，但并非任意两条对角线都有交点，以及交点都一定在凸 n 边形内部．而对于任意一对具体的对角线，分类讨论其是否有 n 边形内的交点是不现实的．

4.3 组合恒等式

关于组合数, 我们可以证明许多常用的组合恒等式.

定理 4.3.1

$$\forall n \in N, 2^n = \sum_{i=0}^{n} \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n}$$

证明: 我们首先提供两种典型的证法: 二项式系数法与组合意义法. 这两种方法都是证明组合恒等式中常用的方法. 除此之外, 归纳法对于某些组合恒等式的证明也十分适用, 我们在此一并展示.

法 1. 二项式系数法:

考虑二项式的幂 $(1+x)^n$, 其完全展开后共有 2^n 项. 而合并同类项后 x 的指数可以取遍 0 到 n 共 $n+1$ 种取法, 故这 $n+1$ 项的系数之和应恰为 2^n.

对于 i 次项 $a_i x^i$, 计算其系数 a_i 可根据组合数: 在 $(1+x)^n$ 的完全展开式中, 如果某一项为 x^i, 则一定是通过在恰好 i 个因式中选取了 x 并在剩余的因式中选取了 1 相乘得到. 因此 x^i 的系数恰好等于从 n 个元素中选取 i 个的选法数, 即组合数 $\binom{n}{i}$. 这就证明了 $2^n = \sum_{i=0}^{n} \binom{n}{i}$.

法 2. 组合意义法:

考虑在一个 n 元集合 A 确定一个子集 X, 求 X 的可能的总数. 我们有两种角度考虑这个过程:

① 考虑 A 中的每一个元素 a, 其可以有在或不在 X 中两种情况, 且每个元素的状态不同都会使得 X 不同. 根据乘法原理, X 的可能数是 $2^{|A|} = 2^n$, 即 A 有 2^n 个不同的子集.

② 考虑 $|X|$, 其取值可以取遍 0 到 n, 且 i 元子集 X 可能的数量为组合数 $\binom{n}{i}$, 且这些情况彼此互斥. 根据加法原理, X 的可能数是 $\sum_{i=0}^{n} \binom{n}{i}$.

由于两个过程的组合意义相同, 计算出的 X 的可能数自然也理应相同. 这就证明了命题.

法 3. 数学归纳法:

① $n = 0$ 时, 左侧 $LHS = 2^0 = 1$, 右侧 $RHS = \binom{0}{0} = 1$, 命题成立;

② 若对于 n 命题成立, 则对于 $n+1$:

我们知道 $\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}$. 又根据归纳假设, 有 $2^n = \sum_{i=0}^{n} \binom{n}{i}$.

考虑 $2^{n+1} = 2\sum_{i=0}^{n} \binom{n}{i}$, 我们将右侧的项作如下划分: 首先单独分出一个 $\binom{n}{0}$ 和一个 $\binom{n}{n}$, 它们都等于 1, 也就分别等于 $\binom{n+1}{0}$ 和 $\binom{n+1}{n+1}$; 对于剩下的项, 每一组 $\binom{n}{i}$ 与 $\binom{n}{i+1}$ 相加, 得

到 $\binom{n+1}{i+1}$，其中 i 取遍 0 到 $n-1$，故得到了 $\binom{n+1}{1}$ 到 $\binom{n+1}{n}$. 这就证明了右式等于 $\sum_{i=0}^{n}\binom{n}{i+1}$，也就完成了证明.

注： 上述法 *1* 的过程中，我们实际上证明了 $(x+1)^n=\sum_{i=0}^{n}\binom{n}{i}x^i$. 也可以在证明这个命题后，直接代入 $x=1$ 以完成 *2.13* 的证明. 这实际上等价于一种形式化的“统计项数”.

注： 上述法 *3* 的过程中，我们用到了关于组合数的结论 $\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}$. 由于求和的项数是固定的，这个结论可以直接代入组合数的定义证明，但也同样可以运用组合意义证明：考虑在 $n+1$ 个元素的集合 A 中确定一个 $k+1$ 元的子集 X，任取一个固定的元素 a，则要么有 $a\in X$，要么有 $a\notin X$. 前者等价于在 n 元集 $A\setminus\{a\}$ 中确定一个 k 元子集 $X\setminus\{a\}$；后者等价于在 n 元集 $A\setminus\{a\}$ 确定一个 $k+1$ 元子集 X. 这就完成了证明.

上面我们展示了组合意义法证明恒等式的思路：考虑一个具体的组合过程，用不同的方法计算其方法数，这样就证明两种计算法得到的结果是相等的. 组合意义法也因此俗称“算两遍”.

命题 4.3.1

$$\forall n\in N,2^{n-1}=\sum_{i\in[n],i=2k}\binom{n}{i}=\binom{n}{0}+\binom{n}{2}+\ldots+\binom{n}{2\lfloor\frac{n}{2}\rfloor}$$

证明： 我们依然使用两种方法分别证明.

法 1. 二项式系数法：

由 *2.14*，$(x+1)^n=\sum_{i=0}^{n}\binom{n}{i}x^i$. 在左侧中代入 $x=-1$，则有 $0=\sum_{i=0}^{n}\binom{n}{i}(-1)^i$. 将右侧中负项移到左侧，可知偶数次项 $((-1)^i=1)$ 的系数和与奇数次项 $((-1)^i=-1)$ 的系数和在 2^n 中各占一半. 这就完成了证明.

法 2. 组合意义法：

右侧的组合意义为 n 元集合 A 中元素个数为偶数的子集 X 的总数，因此我们只需证明这类集合在 A 的全体子集中占恰好一半. 考虑一个固定的元素 a，对于每个含有/不含有 a 的偶数元子集，在其中删去/添加 a 就得到了一个奇数元子集，且容易验证这种变换的过程是一一映射. 这就证明了 A 的子集中偶数元子集与奇数元子集数量相同，也就完成了证明.

命题 4.3.2

$$\forall n\in N,n2^{n-1}=\sum_{i=0}^{n}i\binom{n}{i}=0\cdot\binom{n}{0}+\binom{n}{1}+2\binom{n}{2}\ldots+n\binom{n}{n}$$

证明： 我们依然使用两种方法分别证明.

法 1. 二项式系数法：

由 *2.14*, $(x+1)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$. 此式两边都是关于 x 的多项式函数, 故对 x 求导后也应相同. 左式求导为 $n(x+1)^{n-1}$; 右式的每一项求导为 $i\binom{n}{i}x^{i-1}$, 求和后为 $\sum_{i=1}^{n} i\binom{n}{i}x^{i-1}$. 代入 $x=1$ 就完成了证明.

法 *2.* 组合意义法:

考虑如下组合过程: 在 n 元集合 A 中确定一个非空子集 $X \subseteq A$, 并在 X 中确定一个元素 $a \in X$. 认为两种选法相同当且仅当 $X_1 = X_2$ 且 $a_1 = a_2$. 我们有两种角度求解方法数:

① 先确定元素 a, 共有 n 种选法. 在确定集合 X 同时确保 $a \in X$, 这意味着在逐个判断元素是否属于 X 时不必再判断 a, 即乘法原理的过程中少乘一次 2, 故方法数为 2^{n-1}. 根据乘法原理, 整个过程总的方法数为 $n2^{n-1}$.

② 考虑 $|X|$, 其取值可以取遍 1 到 n, 且 i 元子集 X 可能的数量为组合数 $\binom{n}{i}$. 在 $|X| = i$ 时, 从中取一个元素 a 有 i 种取法. 故 $|X| = i$ 时, 整个过程的方法数为 $i\binom{n}{i}$. 根据加法原理, 总的方法数为 $\sum_{i=1}^{n} i\binom{n}{i}$.

由于两个过程的组合意义相同, 计算出的结果自然也理应相同. 这就证明了命题.

4.4 格点游走

计算格点游走过程的方法数是计数中的经典问题，其与概率论与随机过程中的随机游走有许多相通之处.

问题 4.4.1

一只蚂蚁在二维平面的整点 Z^2 上行走，从 $(0,0)$ 出发，每步可以向上或向右行走一个单位距离. 求走到 (m,n) 共有多少种走法.

证明： 根据行走规则，蚂蚁从 $(0,0)$ 到 (m,n)，一定用了恰好 $m+n$ 步，且其中恰有 m 步是向右行走. 因此求走法数等价于在 $m+n$ 步中选取 m 步的方法数，也就是 $\binom{n}{m}$.

注： 我们可以据此重新证明 $\binom{m+n}{m}=\binom{m+n-1}{m-1}+\binom{m+n-1}{m}$. 考虑蚂蚁到达 (m,n) 的前一步：其要么处在 $(m-1,n)$ *(最后一步向右)*；要么处在 $(m,n-1)$ *(最后一步向上)*. 故走到 (m,n) 的走法数应是走到 $(m-1,n)$ 与 $(m,n-1)$ 分别的走法数之和.

问题 4.4.2

一只蚂蚁在一维数轴的整点 Z 上行走，从 0 出发，每步可以向左或向右行走一个单位距离. 求 t 步后恰好走到 k 共有多少种走法.

证明： 显然，当 $t<k$ 时，t 步后走到 k 是不可能的，总的走法数为 0.

容易想到不同的走法来自于折返过程可以有不同安排，但每次折返到同一个点必然要花偶数步，因此 t 步后所处的位置 k 应该满足 $k\equiv t(\mathrm{mod}2)$. 所以，当 $t-k$ 为奇数时，总的走法数为 0.

当 $t-k$ 为非负偶数时，蚂蚁从 0 到 k 用了恰好 t 步，则其中应恰有 $\frac{t-k}{2}$ 步是向负方向即向左行走. 总的走法数为 $\binom{t}{\frac{t+k}{2}}$.

问题 4.4.3

一只蚂蚁在一维数轴的整点 Z 上行走，从 0 出发，每步可以向左或向右行走一个单位距离. 求 t 步后恰好走到 k，且中途穿过 k *(到达过 $k+1$)* 共有多少种走法.

证明： 我们只讨论 $t-k$ 为非负偶数的情况. 先改为考虑第 t 步处在 $k+2$ 的走法数，由 *2.18* 得走法数为 $\binom{t}{\frac{t+k+2}{2}}$. 对于其中的每一种走法，找到其第一次到达 $k+1$ 的时刻 t_1，并将那之后的所有步反向，则更改后的走法里蚂蚁在 t 时刻会处在位置 k，且过程中到达过 $k+1$. 由于映射不改变第一次到达 $k+1$ 的时刻 t_1，且 t_1 时刻后的变换是一个双射，因此映射整体也是一个双射. 这就证明了 t 步后处于 k 且到达过 $k+1$ 的走法与 t 步后处于 $k+2$ 的走法一一对应，故总的走法数为 $\binom{t}{\frac{t+k+2}{2}}$.

问题 4.4.4

一只蚂蚁在一维数轴的整点 Z 上行走, 从 0 出发, 每步可以向左或向右行走一个单位距离. 求 t 步后走到 k, 且中途从未到达过 $k+1$ 共有多少种走法.

证明: 根据 *2.18* 和 *2.19*, 由减法原理可得合法情况下走法数为 $\binom{t}{\frac{t+k}{2}} - \binom{t}{\frac{t+k+2}{2}}$.

练习 4.4.1

一只蚂蚁在一维数轴的整点 Z 上行走, 从 0 出发, 每步可以向左或向右行走一个单位距离. 求 t 步后首次走到 k, 且中途从未到达过 l 共有多少种走法. 提示: 考虑使用容斥原理.

4.5 容斥原理

在计算两个已知集合交集的元素数量时, 我们会用到容斥原理:

定理 4.5.1 容斥原理

给定两个集合 A, B, 有 $|A \cup B| = |A| + |B| - |A \cap B|$.

证明: 我们考虑将所有集合分解为最小的交集单元. 则 $A = (A \cap B) \sqcup (A \cap B^c), B = (A \cap B) \sqcup (A^c \cap B)$ (这里我们用 $\sqcup$ 表示集合的不交并). 由此我们可以写出

$$\begin{aligned}
|A \cup B| &= |(A \cap B) \sqcup (A \cap B^c) \sqcup (A^c \cap B)| \\
&= |A \cap B| + |A \cap B^c| + |A^c \cap B| \\
&= (|A \cap B| + |A \cap B^c|) + (|A \cap B| + |A^c \cap B|) - |A \cap B| \\
&= |A| + |B| - |A \cap B|
\end{aligned}$$

我们可以将抽屉原理推广到多个集合的情况.

定理 4.5.2 容斥原理对多个集合情况的推广

给定 n 个集合 $A_1, A_2, \ldots, A_n$. 记记 $\mathscr{A} = \{A_1, \ldots A_n\}$, 其中 i 个集合构成的集族具有形式 $\Gamma \in \binom{\mathscr{A}}{i}$, 该集族中所有集合的交记作 $\bigcap \Gamma$. 记 $S_i = \sum_{\Gamma \in \binom{\mathscr{A}}{i}} |\bigcap \Gamma|$. 则有

$$\begin{aligned}
|\bigcup_{i=1}^{n} A_i| &= \sum_{i=0}^{n} (-1)^{i+1} S_i \\
&= \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \ldots \\
&\quad + (-1)^t \sum_{1 \le i_1 < \ldots < i_t} |A_{i_1} \cap \ldots \cap A_{i_t}| + \ldots \\
&\quad + (-1)^n |A_1 \cap \ldots \cap A_n|
\end{aligned}$$

证明: 提示: 对 n 使用归纳法.

命题 4.5.1

给定 n 个集合 $A_1, A_2, \ldots, A_n$. 记记 $\mathscr{A} = \{A_1, \ldots A_n\}$, 其中 i 个集合构成的集族具有形式 $\Gamma \in \binom{\mathscr{A}}{i}$, 该集族中所有集合的交记作 $\bigcup\Gamma$. 记 $D_i = \sum_{\Gamma\in\binom{\mathscr{A}}{i}} |\bigcup\Gamma|$. 则有

$$
\begin{aligned}
|\bigcap_{i=1}^{n} A_i| &= \sum_{i=0}^{n}(-1)^{i+1}D_i \\
&= \sum_{1\le i\le n}|A_i| - \sum_{1\le i<j\le n}|A_i\cup A_j| + \sum_{1\le i<j<k\le n}|A_i\cup A_j\cup A_k| - \ldots \\
&\quad + (-1)^t \sum_{1\le i_1<\ldots<i_t}|A_{i_1}\cup\ldots\cup A_{i_t}| + \ldots \\
&\quad + (-1)^n|A_1\cup\ldots\cup A_n|
\end{aligned}
$$

证明: 我们考虑集合论中的德摩根定理: $(A_1\cup\ldots\cup A_n)^c = A_1^c\cup\ldots\cup A_n^c$, 基于此我们可以将集合的交集与并集相互转换.

定义 $S = \bigcup_{i=1}^{n} A_i$. 则 $|\bigcap_{i=1}^{n} A_i| = |(\bigcup_{i=1}^{n} A_i^c)^c| = |S| - |\bigcup_{i=1}^{n} A_i^c|$. 我们只需研究 $|\bigcup_{i=1}^{n} A_i^c|$ 即可. 根据多个集合的抽屉原理, 可以写出:

$$
\begin{aligned}
|\bigcup_{i=1}^{n} A_i^c| &= \sum_{1\le i\le n}|A_i^c| - \sum_{1\le i<j\le n}|A_i^c\cap A_j^c| + \sum_{1\le i<j<k\le n}|A_i^c\cap A_j^c\cap A_k^c| - \ldots \\
&\quad + (-1)^t \sum_{1\le i_1<\ldots<i_t}|A_{i_1}^c\cap\ldots\cap A_{i_t}^c| + \ldots \\
&\quad + (-1)^n|A_1^c\cap\ldots\cap A_n^c|
\end{aligned}
$$

为了将 $|A_i^c|$ 都转化为 $|A_i|$, 我们再次使用德摩根定理, 可以写出 $|A_{i_1}^c\cap\ldots\cap A_{i_t}^c| = |S| - |A_{i_1}\cup\ldots\cup A_{i_t}|$. 而在上式的每一项中, 贡献的 $|S|$ 的数量恰好为 $\binom{n}{t}$. 所以左式含有的 $|S|$ 的数量为 $1 + \sum_{t=1}^{n}(-1)^t\binom{n}{t} = 0$.

这样我们就证明了原式.

下面我们来看几个具体的例子.

问题 4.5.1

求出 $[120]$ 中不能被 2 或 3 或 5 整除的整数个数.

证明: 我们定义如下集合: $A = \{n \in [120] | n = 2k\}, B\{n \in [120] | n = 3k\}, C = \{n \in [120] | n = 5k\}$. 为了求出 $|A^c\cap B^c\cap C^c|$, 我们可以改为求 $|A\cup B\cup C|$, 从而需要求出 A, B, C 的每一重交集的元素数量. 可以写出:

$$|A| = 60, |B| = 40, |C| = 24$$

$$|A \cap B| = \{n \in [120] | n = 6k\} = 20$$

$$|A \cap C| = \{n \in [120] | n = 10k\} = 12$$

$$|B \cap C| = \{n \in [120] | n = 15k\} = 8$$

$$|A \cap B \cap C| = \{n \in [120] | n = 30k\} = 4$$

故有 $|A^c \cap B^c \cap C^c| = |S| - |A \cup B \cup C| = |S| - (|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|) = 32$.

问题 4.5.2

有三个班级男女生人数分别为 $(m_1, n_1), (m_2, n_2), (m_3, n_3)$, 三个班各取一人, 求都不取男生的选取方法数.

证明: 我们定义如下集合: $A =$ { 一班取到男生的取法 }, B { 二班取到男生的取法 }, $C =$ { 三班取到男生的取法 }. 同样, 为了求出 $|A^c \cap B^c \cap C^c|$, 我们改为求 $|A \cup B \cup C|$, 从而需要求出 A, B, C 的每一重交集的元素数量. 可以写出:

$$|A| = m_1(m_2 + n_2)(m_3 + n_3)$$

$$|B| = (m_1 + n_1)m_2(m_3 + n_3)$$

$$|C| = (m_1 + n_1)(m_2 + n_2)m_3$$

$$|A \cap B| = m_1 m_2(m_3 + n_3)$$

$$|B \cap C| = (m_1 + n_1)m_2 m_3$$

$$|A \cap C| = m_1(m_2 + n_2)m_3$$

$$|A \cap B \cap C| = m_1 m_2 m_3$$

故有:

$$\begin{aligned}
|A^c \cap B^c \cap C^c| &= |S| - |A \cup B \cup C| \\
&= |S| - (|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|) \\
&= (m_1 + n_1)(m_2 + n_2)(m_3 + n_3)(1 - \frac{m_1}{m_1 + n_1})(1 - \frac{m_2}{m_2 + n_2})(1 - \frac{m_3}{m_3 + n_3}) \\
&= n_1 n_2 n_3
\end{aligned}$$

这与我们直接用乘法原理得到的结果是一样的.

问题 4.5.3

对于正整数 n, 定义欧拉函数 $\phi(n)$ 为 $[n]$ 中与 n 互素的正整数的数量. 计算欧拉函数 $\phi(n)$.

证明: 根据质因数分解定理, 我们可以将任一正整数 n 表示成其质因数分解 $n = \prod_{i=1}^{k} p_i^{a_i} = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ (其中 p_i 表示 n 的第 i 个质因数, k 为 n 的不同质因数的个数). 对于 $a \in [n]$, $(a, n) = 1$ 当且仅当对 $p_1 \nmid a, p_2 \nmid a, \dots, p_k \nmid a$.

类似题 *3.4* 的做法, 当 $p_1, p_2, \dots$ $[n]$ 中满足这一条件的正整数的个数是 $n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$.

4.6 错排问题

问题 4.6.1

将 n 个数 $\{1,2,\ldots,n\}$ 排列为 $P=(a_1,a_2,\ldots,a_n)$，且满足 $\forall i\in[n],a_i\neq i$. 求满足如此条件的排列的方法数.

证明： 定义集合 A_i 为全体错排了第 i 个元素的排列构成的集合，即 $A_i=\{P|a_i\neq i\}$，则错排的数量可以这样计算：

$$|A_1\cap A_2\cap\ldots\cap A_n|=\sum_{i=1}^{n}|A_i|-\sum_{i,j}|A_i\cup A_j|+\ldots$$

注意到集合 $A_i\cup A_j=\{P|a_i\neq i\text{ 或 }a_j\neq j\}$ 的元素个数并不容易计算，反而是集合 $(A_i\cup A_j)^c=A_i^c\cap A_j^c=\{P|a_i=i\text{ 且 }a_j=j\}$ 的元素个数容易计算. 因此我们改为这样计算错排的数量：

$$\begin{aligned}|A_1\cap A_2\cap\ldots\cap A_n|=|S|-\sum_{i=1}^{n}|\overline{A_i}|+\sum_{1\le i<j\le n}|\overline{A_i}\cap\overline{A_j}|-\ldots\\+\sum_{1\le i_1<\cdots<i_t\le n}(-1)^t|\overline{A_{i_1}}\cap\ldots\cap\overline{A_{i_t}}|+\ldots\\+(-1)^n|\overline{A_1}\cap\overline{A_2}\cap\ldots\cap\overline{A_n}|\end{aligned}$$

记 $B_i=\overline{A_i}=\{P:a_i=i\}$，上述公式转变为：

$$\begin{aligned}|\overline{B_1}\cap\ldots\cap\overline{B_n}|=|S|-\sum_{i=1}^{n}|B_i|+\sum_{i,j}|B_i\cap B_j|-\ldots\\+(-1)^t\sum_{i_1,\ldots,i_t}|B_{i_1}\cap B_{i_2}\cap\ldots\cap B_{i_t}|+\ldots\\+(-1)^n|B_1\cap B_2\cap\ldots\cap B_n|.\end{aligned}$$

因为 $B_{i_1}\cap B_{i_2}\cap\ldots\cap B_{i_t}=\overline{A_{i_1}}\cap\overline{A_{i_2}}\cap\ldots\cap\overline{A_{i_t}}=\{P|a_{i_1}=i_1,a_{i_2}=i_2\ldots,a_{i_t}=i_t\}$. 所以 $|B_{i_1}\cap B_{i_2}\cap\ldots\cap B_{i_t}|$ 表示固定 $i_1,i_2,\cdots,i_t$ 个位置的数字，其余的 $(n-t)$ 个位置上无限制的方法数，也即 $(n-t)!$. 将其代入到之前的公式有

$$|\overline{B_1}\cap\overline{B_2}\ldots\overline{B_n}|=n!-n(n-1)!+\binom{n}{2}(n-2)!+\ldots+(-1)^t\binom{n}{t}(n-t)!+\cdots+(-1)^n\binom{n}{n}(n-n)!.$$

所以满足题意的错排的排法总数为

$$\begin{aligned}|A| &= \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)! \\ &= \sum_{i=0}^{n}(-1)^i\frac{n!}{i!(n-i)!}(n-i)! \\ &= \sum_{i=0}^{n}(-1)^i\frac{n!}{i!}\end{aligned}$$

定义 4.6.1 错排数

我们将上述结果记作 C_n^0. 它表示将 n 个数排列, 且存在 0 个位置, 也即不存在位置满足 $a_i = i$ 的方法数.

注： 注意到

$$\frac{C_n^0}{n!} = \sum_{i=0}^{n}\frac{(-1)^i}{i!}$$

恰好是 e^x 在 -1 处进行泰勒展开的前 $n+1$ 项和

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots$$

因此

$$\lim_{n\to\infty}\frac{C_n^0}{n!} = \lim_{n\to\infty}\sum_{i=0}^{n}\frac{(-1)^i}{i!} = \sum_{i=0}^{\infty}\frac{(-1)^i}{i!} = e^{-1}$$

这可以被解释为, 对于任意一个长度为 n 的排列, 当 n 足够大的时候, 这个排列是一个错排的概率趋近于 $\frac{1}{e}$.

我们可以考虑更一般的情况 C_n^t, 即将 n 个数进行排列, 其中恰好存在 t 个位置使得 $a_i = i$ 的方法数. 特别地, $t = 0$ 时, C_n^0 代表上文所求的错排数; C_n^n 代表对任意 i 都有 $a_i = i$, 显然这样的排列的数量有且只有一个.

定义 4.6.2 广义错排数

将 n 个数 $\{1, 2, \ldots, n\}$ 排列为 $P = (a_1, a_2, \ldots, a_n)$, 且满足恰有 t 个 $i \in [n]$ 满足 $a_i = i$. 满足如此条件的排列的方法数记作 C_n^t.

问题 4.6.2

求解 C_n^t.

证明： 考虑一般情况的 C_n^t，代表的是 n 个位置中，选出 t 个位置，在这 t 个位置上，满足 $a_i = i$，而对于剩余的 $(n-t)$ 个位置，是一个更小规模的错排，因此：

$$\begin{aligned} C_n^t &= \binom{n}{t} C_t^t C_{n-t}^0 \\ &= \binom{n}{t} \cdot 1 \cdot \left(\sum_{i=0}^{n-t} (-1)^i \frac{(n-t)!}{i!} \right) \\ &= \binom{n}{t} (n-t)! \left(\sum_{i=0}^{n-t} \frac{(-1)^i}{i!} \right) \\ &= \frac{n!}{t!} \left(\sum_{i=0}^{n-t} \frac{(-1)^i}{i!} \right) \end{aligned}$$

不难理解，C_n^t 对 $0 \le t \le n$ 的求和就是所有的排列情况，因此：

$$C_n^0 + C_n^0 + \cdots + C_n^n = n!$$

将 C_n^t 的表达式带入到上述等式，可以得到：

$$\sum_{t=0}^{n} C_n^t = \sum_{t=0}^{n} \frac{n!}{t!} \left(\sum_{i=0}^{n-t} \frac{(-1)^i}{i!} \right) = n!$$

通过两边同时消去 $n!$，可以得到一个组合恒等式：

命题 4.6.1

$\sum_{t=0}^{n} \frac{1}{t!} (\sum_{i=0}^{n-t} \frac{(-1)^i}{i!}) = 1$

上述的求解过程使用了归并的思想，将问题的求解转化为更小规模错排的求和，实际上，我们可以直接从集合的意义上对 C_n^t 进行求解.

考虑之前定义的集合 $B_i = \{P | a_i = i\}$，则 C_n^0 表示不属于任何集合 $B_1, B_2, \cdots, B_n$ 的元素的个数，即：

$$
\begin{aligned}
C_n^0 &= |\overline{B_1} \cap \overline{B_2} \cap \cdots \cap \overline{B_n}| \\
&= |\bigcap_{i=1}^{n} \overline{B_i}| \\
&= |S| - \sum_{i=1}^{n} |B_i| + \sum_{i,j} |B_i \cap B_j| - \ldots \\
&+ (-1)^t \sum_{i_1,\ldots,i_t} |B_{i_1} \cap B_{i_2} \cap \ldots \cap B_{i_t}| \\
&+ \ldots + (-1)^n |B_1 \cap B_2 \cap \ldots \cap B_n|.
\end{aligned}
$$

特别地, C_n^1 可以被表示为:

$$
C_n^1 = \sum_{i=1}^{n} |B_i \cap (\bigcap_{j \neq i} \overline{B_j})| = |B_1 \cap \overline{B_2} \cdots \cap \overline{B_n}| + |\overline{B_1} \cap B_2 \cdots \cap \overline{B_n}| + \ldots
$$

考虑 $n = 3$ 的简单情况, 则 C_3^1 可以被表示为:

$$
C_3^1 = |B_1 \cap \overline{B_2} \cap \overline{B_3}| + |\overline{B_1} \cap B_2 \cap \overline{B_3}| + |\overline{B_1} \cap \overline{B_2} \cap B_3|
$$

注意到:

$$
\begin{aligned}
|B_1 \cap \overline{B_2} \cap \overline{B_3}| &= |B_1| - |B_1 \cap B_2| - |B_1 \cap B_3| + |B_1 \cap B_2 \cap B_3| \\
|\overline{B_1} \cap B_2 \cap \overline{B_3}| &= |B_2| - |B_1 \cap B_2| - |B_2 \cap B_3| + |B_1 \cap B_2 \cap B_3| \\
|\overline{B_1} \cap \overline{B_2} \cap B_3| &= |B_3| - |B_1 \cap B_3| - |B_2 \cap B_3| + |B_1 \cap B_2 \cap B_3|
\end{aligned}
$$

因此有

$$
C_3^1 = \sum_{i=1}^{3} |B_i| - 2 \sum_{i,j} |B_i \cap B_j| + 3|B_1 \cap B_2 \cap B_3|
$$

类似地, 可以得到:

$$
\begin{aligned}
C_3^2 &= \sum_{i,j} |B_i \cap B_j| - 3|B_1 \cap B_2 \cap B_3| \\
C_3^3 &= |B_1 \cap B_2 \cap B_3|
\end{aligned}
$$

对于更一般的 n 的情况, 将在 Mobius 反演中进行讨论.

4.7 Menage 问题

问题 4.7.1 Menage 问题

n 对夫妇参加宴席，围坐一桌，要求男女相隔，且夫妇不相邻．求符合要求的坐法数量？

证明： 当 $n<3$ 时，易知这样的排列时不存在的，当 $n\geq 3$ 时，考虑先对男生进行排列，这样的排列等价于一个长度为 n 的圆排列，数量为 $(n-1)!$.

选定 n 个男生的一种入座方式，从某一位开始对男生按环形顺序进行编号为 $1,2,\cdots,n$，并将编号为 i 的男生的妻子也编号为 i. 记第 i 位男生与第 $i+1$ 位男生之间的位置位 i 号位置.

记 a_i 表示第 i 个男生和第 $i+1$ 个男生之间放置的女生的编号，由题意可知 $a_i\neq i$ 且 $a_i\neq i+1$. 记事件 $B_i=\{a_i=i \text{ 或 } a_i=i+1\}$，$B_i^c=\{a_i\neq i \text{ 且 } a_i\neq i+1\}$，所以女生的排法可以表示成下式，并用容斥原理进行展开：

$$\begin{aligned}|\overline{B_1}\cap\ldots\cap\overline{B_n}|=|S|-\sum_{i=1}^{n}|B_i|+\sum_{i,j}|B_i\cap B_j|-\ldots\\ +(-1)^t\sum_{i_1,\ldots,i_t}|B_{i_1}\cap B_{i_2}\cap\ldots\cap B_{i_t}|+\ldots\\ +(-1)^n|B_1\cap B_2\cap\ldots\cap B_n|\end{aligned}$$

注意到 $|S|$ 是 n 个女生的全排列，故 $|S|=n!$. 而 $|B_i|=2\times(n-1)!$，但是对于剩下项的求和并不容易计算，因此我们转变思路，将 $\sum_{i_1,\ldots,i_t}|B_{i_1}\cap B_{i_2}\cap\ldots\cap B_{i_t}|$ 直接作为一个整体进行求解.

考虑到这个求和的组合意义，我们可以转化为以下问题：从 n 个指标选取 $i_1,i_2,\ldots,i_t$，并且满足

$$\begin{aligned}a_{i_1}&\in\{i_1,i_1+1\}\\ a_{i_2}&\in\{i_2,i_2+1\}\\ &\cdots\\ a_{i_t}&\in\{i_t,i_t+1\}\\ a_{i_1}&\neq a_{i_2}\neq\ldots\neq a_{i_t}\end{aligned}$$

考虑到 $a_i=i$ 或 $a_i=i+1$，上述问题等价于从长度为 $2n$ 的圆排列 $1,2,2,3,3,4,\cdots,n,1$ 中选取 t 个互不相邻的数字. 因此在这个排列中取到两个相邻的数字等价于以下二者之一：1. 两个数字是一样的；或 2. 两个数字属于同一个二元集.

可以进一步将这个圆排列的问题转化成线排列的问题，排列的种数等价于从 $2n$ 个数的线排列中取 t 个两两不相邻的方法数减去从 $2n$ 个数的线排列中取 t 个两两不相邻，头尾都取到的方法数，即：

$$\binom{2n-t+1}{t}-\binom{2n-t-1}{t-2}$$

因此

$$\begin{aligned}\sum_{i_1,\ldots,i_t}|B_{i_1}\cap\ldots\cap B_{i_t}| &= \left(\binom{2n-t+1}{t}-\binom{2n-t-1}{t-2}\right)\cdot(n-t)!\\ &= \frac{2n}{2n-t}\binom{2n-t}{t}(n-t)!\end{aligned}$$

带入一开始的容斥原理的公式，可以得到：

$$\begin{aligned}|\overline{B_1}\cap\ldots\cap\overline{B_n}| &= n!-2n(n-1)!+\cdots\\ &\quad+(-1)^t\frac{2n}{2n-t}\binom{2n-t}{t}(n-t)!\\ &\quad+\cdots+(-1)^n 2.\end{aligned}$$

4.8 Mobius 反演

问题 4.8.1

考虑一个集合 S 及其四子集合 $A_1, A_2, A_3, A_4 \subseteq S$. 用 C_k 表示 S 中恰好属于 k 个集合 A_i 的元素的个数. 用 $\cap_0, \cap_1, \cap_2, \cap_3, \cap_4$ 表示 C_k

其中 $\cap_0 = |S|, \cap_1 = \sum_{i=1}^{4} |A_i|, \cap_2 = \sum_{ij} |A_i \cap A_j|, \cap_3 = \sum_{ijk} |A_i \cap A_j \cap A_k|, \cap_4 = |A_1 \cap A_2 \cap A_3 \cap A_4|$.

证明：

$$C_0 = \cap_0 - \cap_1 + \cap_2 - \cap_3 + \cap_4$$

$$C_1 = \cap_1 - 2\cap_2 + 3\cap_3 - 4\cap_4$$

$$C_2 = \cap_2 - 3\cap_3 + 6\cap_4$$

$$C_3 = \cap_3 - 4\cap_4$$

$$C_4 = \cap_4$$

写成矩阵形式寻找规律:

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 1 & -1 & 1 \\ & 1 & -2 & 3 & -4 \\ & & 1 & -3 & 6 \\ & & & 1 & -4 \\ & & & & 1 \end{pmatrix} \begin{pmatrix} \cap_0 \\ \cap_1 \\ \cap_2 \\ \cap_3 \\ \cap_4 \end{pmatrix}$$

$$\begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \end{pmatrix} = \begin{pmatrix} \binom{0}{0} & -\binom{1}{0} & \binom{2}{0} & -\binom{3}{0} & \binom{4}{0} \\ & \binom{1}{1} & -\binom{2}{1} & \binom{3}{1} & -\binom{4}{1} \\ & & \binom{2}{2} & -\binom{3}{2} & \binom{4}{2} \\ & & & \binom{3}{3} & -\binom{4}{3} \\ & & & & \binom{4}{4} \end{pmatrix} \begin{pmatrix} \cap_0 \\ \cap_1 \\ \cap_2 \\ \cap_3 \\ \cap_4 \end{pmatrix}$$

问题 4.8.2

一般地, 考虑 n 个子集 $A_1, \ldots, A_n$, 用 C_k^n 表示 S 中恰好属于 k 个子集 A_i 的元素个数. 用 $\cap_0^n, \ldots, \cap_n^n$ 表示 C_k^n.

其中 $\cap_k^n = \sum_{\binom{n}{k}} |A_{i1} \cap \ldots \cap A_{ik}|$.

证明： 根据上述规律:

$$C_k^n = \binom{k}{k} \cap_k - \binom{k+1}{k} \cap_{k+1} + \binom{k+1}{k} \cap_{k+2} - \ldots + (-1)^{n-k} \binom{n}{k} \cap_n$$

练习 4.8.1

采用数学归纳法证明以上结果.

问题 4.8.3

考虑四个子集 $A_1, A_2, A_3, A_4 \subseteq S$. 用 C_k 表示 $\cap_0, \ldots, \cap_4$.

证明：

$$\cap_0 = C_0 + C_1 + C_2 + C_3 + C_4$$

$$\cap_1 = C_1 + 2C_2 + 3C_3 + 4C_4$$

$$\cap_2 = C_2 + 3C_3 + 6C_4$$

$$\cap_3 = C_3 + 4C_4$$

$$\cap_4 = C_4$$

写成矩阵形式寻找规律:

$$\begin{pmatrix} \cap_0 \\ \cap_1 \\ \cap_2 \\ \cap_3 \\ \cap_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ & 1 & 2 & 3 & 4 \\ & & 1 & 3 & 6 \\ & & & 1 & 4 \\ & & & & 1 \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \end{pmatrix}$$

$$\begin{pmatrix} \cap_0 \\ \cap_1 \\ \cap_2 \\ \cap_3 \\ \cap_4 \end{pmatrix} = \begin{pmatrix} \binom{0}{0} & \binom{1}{0} & \binom{2}{0} & \binom{3}{0} & \binom{4}{0} \\ & \binom{1}{1} & \binom{2}{1} & \binom{3}{1} & \binom{4}{1} \\ & & \binom{2}{2} & \binom{3}{2} & \binom{4}{2} \\ & & & \binom{3}{3} & \binom{4}{3} \\ & & & & \binom{4}{4} \end{pmatrix} \begin{pmatrix} C_0 \\ C_1 \\ C_2 \\ C_3 \\ C_4 \end{pmatrix}$$

问题 4.8.4

一般地, 考虑 n 个子集 $A_1, A_2, ..., A_n$. 用 C_k^n 表示 $\cap_0^n, \ldots, \cap_n^n$.

证明： 根据上述规律:

$$\cap_k^n = \binom{k}{k}\cap_k - \binom{k+1}{k}C_{k+1} + \binom{k+2}{k}C_{k+2} + \ldots + \binom{n}{k}C_n$$

练习 4.8.2

采用数学归纳法证明上述结论.

定理 4.8.1 Mobius 反演

考虑 n 个子集 $A_1, A_2, ..., A_n \subseteq S$. 对于 $X \subseteq [n]$, 用 I_X 表示 S 中恰好属于所有的 A_i $(i \in X)$ 的元素的个数. 对于 $X \subseteq [n]$, 记 $f(X) = |\cap_X| = |\cap_{i\in X} A_i|, g(X) = |I_X|$. 则:

$$f(X) = \sum_{X\subseteq Y\subseteq[n]} g(Y)$$

$$g(X) = \sum_{X\subseteq Y\subseteq[n]} (-1)^{|Y|-|X|} f(Y)$$

问题 4.8.5 Mobius 反演 → 容斥原理

通过 *Mobius* 反演证明容斥原理.

证明： 令 $X = \phi$, 由 *Mobius* 反演可得:

$$g(\phi) = \sum_{X\subseteq[n]} (-1)^{|Y|} f(Y)$$

$$\begin{aligned}
|I_\phi| &= |S/A_1 \cup A_2 ... \cup A_n| \\
&= \sum_{Y\subseteq[n]} (-1)^{|Y|} |\cap_{i\in Y} A_i| \\
&= \sum_{k=0}^{n} \sum_{|Y|=k} (-1)^k |\cap_{i\in Y} A_i| \\
&= \sum_{k=0}^{n} (-)^k \sum_{i_1 i_2 ... i_k} |A_{i1} \cap A_{i2} ... \cap A_{ik}|
\end{aligned}$$

问题 4.8.6 Mobius 反演 → C_k^n 通项公式

通过 *Mobius* 反演证明 C_k^n 的通项公式.

证明：

$$\begin{aligned}
C_k^n &= \sum_{|X|=k} |I_X| \\
&= \sum_{|X|=k} \sum_{X\subseteq Y\subseteq[n]} (-1)^{|Y|-k} |\cap_{i\in Y} A_i| \\
&= \sum_{Y\subseteq[n]} \sum_{X\subseteq Y,|X|=k} (-1)^{|Y|-k} |\cap_{i\in Y} A_i| \\
&= \sum_{Y\subseteq[n]} \binom{|Y|}{k} (-1)^{|Y|-k} |\cap_{i\in Y} A_i| \\
&= \sum_{l=k}^{n} \sum_{|Y|=l} (-1)^{l-k} \binom{l}{k} |\cap_{i\in Y} A_i| \\
&= \sum_{l=k}^{n} (-1)^{l-k} \binom{l}{k} \sum_{i_1 i_2,\ldots i_l} |A_{i1} \cap A_{i2} \ldots \cap A_{il}| \\
&= \sum_{l=k}^{n} (-1)^{l-k} \binom{l}{k} \cap_l^n
\end{aligned}$$

问题 4.8.7 容斥原理 → Mobius 反演

通过容斥原理证明 *Mobius* 反演.

证明：

$$A_i = \{g(Y)|i \in Y \subseteq [n]\}$$

$$|A_i| = \sum_{i\in\subseteq[n]} g(Y) = f(\{i\})$$

$$A_i \cap A_j = \{g(Y)|i,j \in Y \subseteq [n]\}$$

$$|A_i \cap A_j| = \sum_{i,j\in Y\subseteq[n]} g(Y) = f(\{i,j\})$$

$$\begin{aligned}
|g_\phi| &= |S/A_1 \cup A_2 \ldots \cup A_n| \\
&= |S| - \sum |A_i| + \sum_{|} A_i \cap A_j| - \ldots + (-1)^n |A_1 \cap A_2 \ldots \cap A_n| \\
&= \sum_{k=0}^{n} \sum_{|Y|=k} (-1)^k |\cap_{i\in Y} A_i| \\
&= f(\phi) - \sum f(\{i\}) + \sum f(\{i,j\}) - \ldots + (-1)^n f([n]) \\
&= \sum_{Y\subseteq[n]} (-1)^{|Y|} f(Y)
\end{aligned}$$

4.9 数论上的 Mobius 反演

问题 4.9.1

设 f、g 是分别是定义在 $\mathbb{Z}^+$ 上的函数. 若对 $\forall a \in \mathbb{Z}^+$,

$$f(a) = \sum_{b \le a} g(b)$$

求解 $g(a)$ 的表达式？

证明：

$$f(a) = \sum_{1 \le b \le a} g(b) \tag{2}$$

$$f(a-1) = \sum_{1 \le b \le a-1} g(b) \tag{3}$$

(2)−(3) 得:

$$g(a) = \begin{cases} f(a) - f(a-1) & if\ a \ge 2 \\ f(a) & if\ a = 1 \end{cases}$$

若将上述问题中的求和的下标从 $b \le a$ 替换为 $b \mid a$, 即 $\forall a \in \mathbb{Z}^+$,

$$f(a) = \sum_{b \mid a} g(b)$$

那么 $g(a)$ 该如何使用 $f(a)$ 进行表达?

首先考虑 $a = 6$ 的简单情况, 根据定义, 我们可以写出以下表达式:

$$\begin{aligned} f(1) &= g(1) \\ f(2) &= g(1) + g(2) \\ f(3) &= g(1) + g(3) \\ f(4) &= g(1) + g(2) + g(4) \\ f(5) &= g(1) + g(5) \\ f(6) &= g(1) + g(2) + g(3) + g(6) \end{aligned}$$

我们可以定义如下三个集合:

$$\begin{aligned} A &= \{g(1), g(2)\} \\ B &= \{g(1), g(3)\} \\ S &= \{g(1), g(2), g(3), g(6)\} \end{aligned}$$

那么我们有：

$$|A| = g(1) + g(2) = f(2)$$
$$|B| = g(1) + g(3) = f(3)$$
$$|S| = g(1) + g(2) + g(3) + g(6) = f(6)$$

根据容斥原理，可以写出 $g(6)$ 的表达式：

$$g(6) = |S \setminus A \cup B| = |S| - |A| - |B| + |A \cap B| = f(6) - f(3) - f(2) + f(1)$$

考虑更复杂的 $g(30)$，我们仍然可以类似的写出：

$$f(30) = g(1) + g(2) + g(3) + g(5) + g(6) + g(10) + g(15) + g(30)$$

可以类似的定义集合：

$$A = \{g(1), g(2), g(3), g(6)\}$$
$$B = \{g(1), g(2), g(5), g(10)\}$$
$$C = \{g(1), g(3), g(5), g(15)\}$$
$$S = \{g(1), g(2), g(3), g(5), g(6), g(10), g(15), g(30)\}$$

$$|A| = g(1) + g(2) + g(3) + g(6) = f(6)$$
$$|B| = g(1) + g(2) + g(5) + g(10) = f(10)$$
$$|C| = g(1) + g(3) + g(5) + g(15) = f(15)$$
$$|S| = g(1) + g(2) + g(3) + g(5) + g(6) + g(10) + g(15) + g(30) = f(30)$$

由容斥原理，可以得到：

$$\begin{aligned} g(30) &= |S \setminus (A \cup B \cup C)| \\ &= |S| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C| \\ &= f(30) - f(6) - f(10) - f(15) + f(2) + f(3) + f(5) - f(1) \end{aligned}$$

问题 4.9.2

现在考虑一个更加一般的情况，假设 $n = \prod_{i=1}^{k} p_i$（$p_i \neq p_j$ 且每个 p_i 都是素数），求解 $g(n)$ 的表达式？

证明： 首先定义如下集合：

$$A_1 = \left\{ g(d) \mid d \mid \frac{n}{p_1} \right\}$$

$$A_2 = \left\{ g(d) \mid d \mid \frac{n}{p_2} \right\}$$

$$\cdots$$

$$A_k = \left\{ g(d) \mid d \mid \frac{n}{p_k} \right\}$$

$$S = \{ g(d) \mid d \mid n \}$$

其中,

$$|A_1| = \sum_{d \mid \frac{n}{p_1}} g(d) = f\left(\frac{n}{p_1}\right), |A_2| = f\left(\frac{n}{p_2}\right), \cdots, |A_k| = f\left(\frac{n}{p_k}\right)$$

接着考虑两个集合的交集

$$\begin{aligned} A_i \cap A_j &= \left\{ g(d) \mid d \mid \frac{n}{p_i} \ and \ d \mid \frac{n}{p_j} \right\} \\ &= \left\{ g(d) \mid d \mid \frac{n}{lcm(p_i, p_j)} \right\} \\ &= \left\{ g(d) \mid d \mid \frac{n}{p_i \cdot p_j} \right\} \end{aligned}$$

因此,

$$|A_i \cap A_j| = \sum_{d \mid \frac{n}{p_i \cdot p_j}} g(d) = f\left(\frac{n}{p_i \cdot p_j}\right)$$

将以上形式拓展到任意个集合的交集, 可以得到:

$$|A_{i_1} \cap \ldots \cap A_{i_t}| = f\left(\frac{n}{p_{i_1} \ldots p_{i_t}}\right)$$

因此，根据容斥原理，我们可以得到 $g(n)$ 的表达式：

$$\begin{aligned}
g(n) &= |S \setminus (A_1 \cup A_2 \cup \ldots \cup A_k)| \\
&= |S| - \sum_{i=1}^{k} |A_i| + \sum_{1\le i<j\le k} |A_i \cap A_j| - \sum_{1\le i<j<l\le k} |A_i \cap A_j \cap A_l| + \ldots + (-1)^{k+1} |A_1 \cap \ldots \cap A_k| \\
&= f(n) - f\left(\frac{n}{p_1}\right) - f\left(\frac{n}{p_2}\right) - \ldots - f\left(\frac{n}{p_k}\right) + f\left(\frac{n}{p_1 \cdot p_2}\right) + \ldots + f\left(\frac{n}{p_{k-1} \cdot p_k}\right) \\
&\quad + (-1)^t \sum_{i_1,\ldots,i_t} f\left(\frac{n}{p_{i_1} \ldots p_{i_t}}\right) + \ldots + (-1)^k f\left(\frac{n}{p_1 \cdot p_2 \ldots p_k}\right) \\
&= f(n) - f\left(\frac{n}{p_1}\right) - f\left(\frac{n}{p_2}\right) - \ldots - f\left(\frac{n}{p_k}\right) + f\left(\frac{n}{p_1 \cdot p_2}\right) + \ldots + f\left(\frac{n}{p_{k-1} \cdot p_k}\right) \\
&\quad + (-1)^t \sum_{i_1,\ldots,i_t} f\left(\frac{n}{p_{i_1} \ldots p_{i_t}}\right) + \ldots + (-1)^k f(1) \\
&= f(n) + \sum_{t=1}^{k} (-1)^t \sum_{1\le i_1<\ldots<i_t\le k} f(\frac{n}{p_{i_1} p_{i_2} \cdots p_{i_t}})
\end{aligned}$$

问题 4.9.3

考虑一个特殊的情况，$n = p^k$，求解 $g(n)$ 的表达式？

证明：

$$f(n) = \sum_{d|n} g(d) = g(p) + g(p^2) + \ldots + g(p^{k-1}) + g(p^k) \tag{4}$$

$$f(\frac{n}{p}) = \sum_{d|\frac{n}{p}} g(d) = g(p) + g(p^2) + \ldots + g(p^{k-1}) \tag{5}$$

(4)−(5) 得：

$$g(n) = g(p^k) = f(n) - f(\frac{n}{p}) \tag{6}$$

可以看到这个表达式和 $k = 1$ 时问题 3.24 的表达式是一致的，即 $g(n)$ 的表达式只与 n 的素因子有关，而与具体的素因子出现的次数无关. 这是可以理解的，因为所有在集合 $A' = \left\{ g(d) \mid d \mid \frac{n}{p_1^{l_i}} \right\}$ 出现的元素，一定也在集合 $A = \left\{ g(d) \mid d \mid \frac{n}{p_1} \right\}$ 中出现，因此无需考虑更小的集合.

问题 4.9.4

考虑 $n = \prod_{i=1}^{k} p_i^{l_i}$，求解 $g(n)$ 的表达式？

证明： 与问题 *3.24* 类似，可以写出集合 A_i 的定义，运用容斥原理，可以得出和问题 *3.24* 一样的表达式：

$$g(n) = f(n) + \sum_{t=1}^{k} (-1)^t \sum_{1 \le i_1 < \ldots < i_t \le k} f(\frac{n}{p_{i_1} p_{i_2} \ldots p_{i_t}})$$

4.10 数论上的 Mobius 函数

定理 4.10.1

给定定义在自然数集合 N 上的函数 f 和 g，对于任意的 $n \ge 1$，如果

$$f(n) = \sum_{d|n} g(d)$$

那么

$$g(n) = \sum_{d|n} f(\frac{n}{d}) \mu(d)$$

其中 $\mu(d)$ 是 *Mobius* 函数

从上一节我们可以知道，对于任意的 $n \ge 1$，我们可以将 n 表示为多个素数相乘的形式：

$$n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$$

.

因此 $g(n)$ 可以被表示为：

$$\begin{aligned} g(n) &= f(n) - \sum_{i=1}^{k} f(\frac{n}{p_i}) + \sum_{i,j} f(\frac{n}{p_i p_j}) + \ldots \\ &\quad + (-1)^t \sum_{i_1, i_2, \ldots, i_t} f(\frac{n}{p_{i_1}, p_{i_2}, \ldots, p_{i_t}}) + \ldots + (-1)^k f(1) \\ &= \sum_{d|n} f(\frac{n}{d}) \mu(d) \end{aligned}$$

其中 $\mu(d)$ 可以被表示为：

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1 \\ (-1)^k & \text{if } d = p_1 p_2 \ldots p_k \\ 0 & \text{if } d = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}, \exists p_i > 1 \end{cases}$$

引理 4.10.1

对于任意的 $n \geq 1$, 由如下等式成立:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & if\ n = 1 \\ 0 & if\ n > 1 \end{cases}$$

证明: 当 $n = 1$ 时,

$$\sum_{d|1} \mu(d) = \mu(1) = 1$$

当 $n > 1$ 时, n 可以被表示为:

$$n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$$

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \sum_{i=1}^{k} \mu(\frac{n}{p_i}) + \sum_{i,j} \mu(\frac{n}{p_i p_j}) + \dots + \sum_{i_1,i_2,\dots,i_t} \mu(\frac{n}{p_{i_1}, p_{i_2}, \dots, p_{i_t}}) + \dots + \mu(\frac{n}{n}) \\ &= 1 + k(-1)^1 + \binom{k}{2}(-1)^2 + \dots + \binom{k}{t}(-1)^t + \dots + \binom{k}{k}(-1)^k \\ &= 0 \end{aligned}$$

引理 4.10.2

给定定义在自然数集合 N 上的函数 f 和 g, 对于任意的 $n \geq 1$, 如果

$$g(n) = \sum_{d|n} f(\frac{n}{d})\mu(d)$$

那么

$$f(n) = \sum_{d|n} g(d)$$

其中 $\mu(d)$ 是 *Mobius* 函数

证明：

$$\begin{aligned}
\sum_{d|n} g(d) &= \sum_{d|n}(\sum_{d'|d} \mu(d^{'}) f(\frac{d}{d^{'}})) \\
&= \sum_{d|n} \sum_{d'|d} \mu(d^{'}) f(\frac{d}{d^{'}}) \\
&= \sum_{d'|d|n} \mu(d^{'}) f(\frac{d}{d^{'}}) \\
&= \sum_{d'\cdot r|n} \mu(d^{'}) f(r) \\
&= \sum_{r|n} f(r)(\sum_{d'|\frac{n}{r}} \mu(d^{'})) \\
&= f(n)
\end{aligned}$$

4.11 集合上的 Mobius 函数

定理 4.11.1

对于定义在集合 S 上的函数 f、g, 若:

$$f(X)=\sum_{Y\subseteq X}g(Y)$$

则:

$$g(X)=\sum_{Y\subseteq X}(-1)^{|X|-|Y|}f(Y)$$

证明:

$$\begin{aligned}\sum_{Y\subseteq X}(-1)^{|X|-|Y|}f(Y)&=\sum_{Y\subseteq X}(-1)^{|X|-|Y|}\sum_{Z\subseteq Y}g(Z)\\&=\sum_{Z\subseteq X}\sum_{Z\subseteq Y\subseteq X}(-1)^{|X|-|Y|}g(Z)\\&=\sum_{Z\subseteq X}\sum_{Y'\subseteq X\setminus Z}(-1)^{|Y'|}g(Z)\\&=\sum_{Z\subseteq X}\sum_{Y'\subseteq X\setminus Z}\mu(Y')g(Z)\end{aligned}\tag{7}$$

其中

$$\sum_{Y\subseteq X}\mu(Y)=\begin{cases}1 & if \quad X=\emptyset\\ 0 & if \quad X\neq\emptyset\end{cases}\tag{8}$$

i)$X=\emptyset$*:*

$$\sum_{Y\subseteq X}\mu(Y)=(-1)^{|\emptyset|}=1$$

ii)$X\neq\emptyset$*:*

$$\sum_{Y\subseteq X}\mu(Y)=\sum_{Y\subseteq X\wedge|Y|\ is\ even}1-\sum_{Y\subseteq X\wedge|Y|\ is\ odd}1$$

其中:

$$\sum_{Y\subseteq X\wedge|Y|\ is\ even}1=\sum_{i=0}^{\lfloor\frac{|X|}{2}\rfloor}\binom{|X|}{2i}\tag{9}$$

$$\sum_{Y\subseteq X\wedge |Y| \text{ is odd}} 1 = \sum_{i=1}^{\lceil \frac{|X|}{2} \rceil} \binom{|X|}{2i-1} \tag{10}$$

(9)−*(10)* 得:

$$\begin{aligned}\sum_{i=0}^{\lfloor \frac{|X|}{2} \rfloor} \binom{|X|}{2i} - \sum_{i=1}^{\lceil \frac{|X|}{2} \rceil} \binom{|X|}{2i-1} &= \sum_{i=0}^{|X|} (-1)^i \binom{|X|}{i} \\ &= (1-1)^{|X|} \\ &= 0\end{aligned}$$

即:

$$\sum_{Y\subseteq X} \mu(Y) = 0$$

(8) 得证.

所以:

$$\begin{aligned}\sum_{Y\subseteq X} (-1)^{|X|-|Y|} f(Y) &= \sum_{Z\subseteq X} \big(\sum_{Y'\subseteq X\setminus Z} \mu(Y') \big) g(Z) \\ &= \mu(\emptyset) g(X) + \sum_{Z\subset X} \big(\sum_{Y'\subseteq X\setminus Z} \mu(Y') \big) g(Z) \\ &= g(X) + 0 = g(X)\end{aligned}$$

定理 *3.23* 得证. 其中 $\mu(X)$ 即为集合上的 *Mobius* 函数.

4.12 Pólya 计数原理

4.12.1 群作用

定义 4.12.1 群作用

设 G 为群，X 为集合。若存在映射 $G \times X \to X$，记为 $(g,x) \mapsto g \cdot x$，满足：

- *(结合律)* $\forall g,h \in G, \forall x \in X,\ g \cdot (h \cdot x) = (gh) \cdot x$
- *(单位元)* $e \cdot x = x$，其中 e 为 G 的单位元

则称 G 在 X 上有一个**群作用**。

例： 正方体的旋转群 G。

定义 4.12.2 轨道与稳定子

设 G 作用于 X，对 $x \in X$，

- G 的**轨道**：$O_x = G \cdot x = \{g \cdot x \mid g \in G\}$
- x 的**稳定子**：$G_x = \{g \in G \mid g \cdot x = x\}$

定理 4.12.1 轨道-稳定子定理

$|O_x| = [G : G_x] = \frac{|G|}{|G_x|}$

证明： 设 G 为有限群，X 为 G 的作用集，$x \in X$。考虑 G 对 X 的作用。

定义映射

$$\varphi : G \to O_x, \quad g \mapsto g \cdot x$$

其中 $O_x = G \cdot x$ 为 x 的轨道。

注意到：φ 不是单射，但它的核正好是 x 的稳定子 $G_x = \{g \in G \mid g \cdot x = x\}$。

事实上，$g_1 \cdot x = g_2 \cdot x \iff g_2^{-1} g_1 \in G_x \iff g_1 G_x = g_2 G_x$，即 g_1 与 g_2 属于同一个左陪集。

因此，φ 在 G 到 O_x 之间建立了 G_x 为核的陪集分解。也就是说，O_x 中的每个元素对应 G 的一个 G_x 左陪集。

所以

$$|O_x| = [G : G_x] = \frac{|G|}{|G_x|}$$

证毕。

4.12.2 轨道公式与 Burnside 引理

定理 4.12.2 Burnside 引理/轨道公式

设有限群 G 作用于有限集合 X，则 G 在 X 上的不动点数的平均值等于 G 作用下的轨道数：

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$$

其中 $|X/G|$ 为轨道数，$\mathrm{Fix}(g) = \{x \in X \mid g\cdot x = x\}$ 为 g 的不动点集。

证明： 记 $A = \{(g,x) \mid g\cdot x = x\}$，则 $|A| = \sum_{g\in G}|\mathrm{Fix}(g)|$。另一方面，$|A| = \sum_{x\in X}|G_x|$。由轨道-稳定子定理，$\sum_{x\in X}|G_x| = \sum_{\text{轨道}}|G| = |G|\cdot(\text{轨道数})$。因此：

$$\sum_{g\in G}|\mathrm{Fix}(g)| = |G|\cdot|X/G| \implies |X/G| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$$

4.12.3 Pólya 计数原理

定理 4.12.3 Pólya 计数原理

设有限群 G 作用于 n 元集合 X，每个元素有 m 种颜色，则不同着色方案的等价类数（轨道数）为：

$$|X/G| = \frac{1}{|G|}\sum_{g\in G} m^{c(g)}$$

其中 $c(g)$ 为 g 在 X 上的循环数（即 g 的置换分解中循环的个数）。

证明： 对每个 $g \in G$，g 的不动着色方案数为 $m^{c(g)}$，因为每个循环必须同色。由 *Burnside* 引理，取平均即得。

问题 4.12.1 例题：正方形四顶点着色

用两种颜色给正方形四个顶点着色，只考虑旋转，有多少种不同着色方案？

证明： G 为正方形的旋转群 C_4，$|G| = 4$。四个元素分别为：

- e（恒等）：$c(e) = 4$，$2^4 = 16$
- r（顺时针 $90°$）：$c(r) = 1$，$2^1 = 2$
- r^2（$180°$）：$c(r^2) = 2$，$2^2 = 4$
- r^3（$270°$）：$c(r^3) = 1$，$2^1 = 2$

代入 *Pólya* 公式：

$$|X/G| = \frac{1}{4}(16+2+4+2) = \frac{24}{4} = 6$$

即有 *6* 种不同着色方案。

问题 4.12.2 例题：正三角形三顶点着色

用 *4* 种颜色给一个正三角形的 *3* 个顶点着色，考虑旋转和翻转，问有多少种不同的着色方案？

证明： 正三角形的所有对称构成的群 $G \cong S_3$，共有 *6* 个元素。

记 $S_3 = \{e, r, r^2, s, sr, sr^2\}$，其中 e 为恒等，r 为顺时针旋转 $120°$，r^2 为顺时针旋转 $240°$，s, sr, sr^2 为分别关于三个顶点的对称轴翻转。

逐一计算各元素的循环数：

1) **恒等变换** e**：** $c(e) = 3$，$4^3 = 64$

2) **顺时针旋转** $120°$ **(**r**)：** $c(r) = 1$，$4^1 = 4$

3) **顺时针旋转** $240°$ **(**r^2**)：** $c(r^2) = 1$，$4^1 = 4$

4) **关于** ***A*** **点的对称轴翻转 (**s**)：** $c(s) = 2$，$4^2 = 16$

5) **关于** ***B*** **点的对称轴翻转 (**sr**)：** $c(sr) = 2$，$4^2 = 16$

6) **关于** ***C*** **点的对称轴翻转 (**sr^2**)：** $c(sr^2) = 2$，$4^2 = 16$

代入 *Pólya* 公式：

$$|X/G| = \frac{1}{6}(64+4+4+16+16+16) = \frac{1}{6}(120) = 20$$

故共有 *20* 种不同的着色方案。

练习 4.12.1 例题：项链问题

用三种颜色给六珠项链着色，考虑旋转，有多少种不同着色方案？

5 图论

5.1 图论引入

问题 5.1.1 七桥问题

18 世纪，哥尼斯堡（今俄罗斯加里宁格勒）的普莱格尔河上有 *7* 座桥，将河中的两个岛和河岸连接起来。

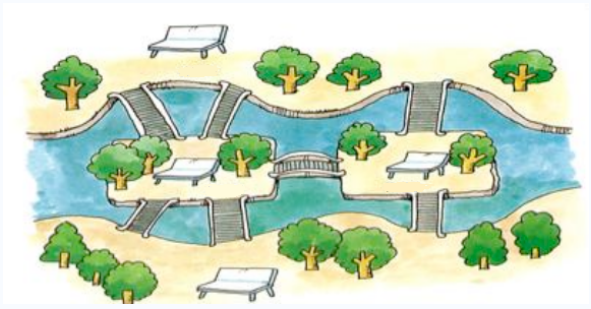


图 1: 哥尼斯堡七桥示意图

问是否能找到一条路径，穿过每座桥恰好一次（欧拉路径问题），或穿过每座桥恰好一次并回到起点（欧拉回路问题）。

证明： 首先将岸和岛抽象为顶点，桥抽象为边，构建一个多重无向图：

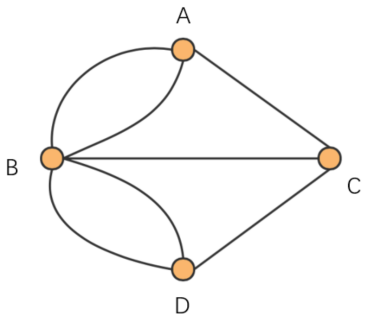


图 2: 七桥问题的图论抽象

分析图的度数：四个顶点（北岸、南岸、两个岛）的度数分别为 *3*、*3*、*5*、*3*，均为奇数。

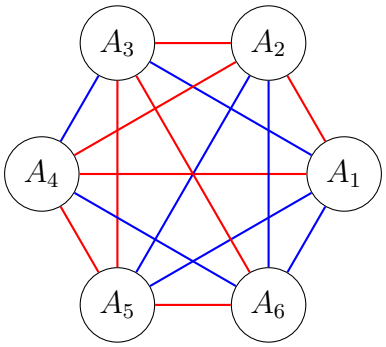
欧拉回路要求所有顶点度数为偶数，而欧拉路径要求最多两个顶点度数为奇数（起点和终点、后证）。这里有四个奇数度的顶点，因此既无欧拉回路也无欧拉路径。

直观解释：若从一个度数为奇数的顶点出发，每次过桥改变顶点状态，度数为奇数的顶点只能作为路径的起点或终点，但四个奇数度顶点无法同时满足路径条件。

问题 5.1.2 边染色问题

任取 6 个人，其中一定存在 3 个人，两两认识或两两不认识。

证明： 将 6 个人抽象为 6 个顶点，绘制一个完全图，如果两个人认识，将边染成红色，否则染成蓝色。



红色边：认识　蓝色边：不认识

图 3: 6 人完全图（红色边表示认识，蓝色边表示不认识）

考虑一个顶点 A_1，连接了 5 条边，根据抽屉原理，一定有 3 条同色边。不妨设为红色，即 A_1A_2, A_1A_3, A_1A_4 三边为红色。

现考虑 A_2, A_3, A_4 这三个点及它们之间的边：

1. 如果存在红色边，如 A_2A_3，则 A_1, A_2, A_3 组成一个红色三角形，对应三人两两认识。
2. 如果 A_2, A_3, A_4 之间没有红色边，则它们之间的边均为蓝色，即 A_2, A_3, A_4 三人两两不认识。

问题 5.1.3

给定一个 n 阶完全图 K_n，将 K_n 的边染成红色或蓝色，使得一定存在一个红 K_4 或者一个蓝 K_3，问 n 最少为多少？

证明：

将问题转化为：

1. 找多少条红色邻边，可以保证存在红色 K_4 或者蓝色 K_3。

   只需在“底边”（红色邻边相连的那些点）中找到一个红 K_3 或蓝 K_3，即可保证存在一个红 K_4 或者一个蓝 K_3。

2. 找多少条蓝色邻边，可以保证存在红色 K_4 或者蓝色 K_3。

只需在“底边”（蓝色邻边相连的那些点）中找到一个红 K_4 或一条蓝色边，即可保证存在一个红 K_4 或者一个蓝 K_3。

于是我们得到，一个点的所有邻边中需要有 6 条红色邻边或者 4 条蓝色邻边：

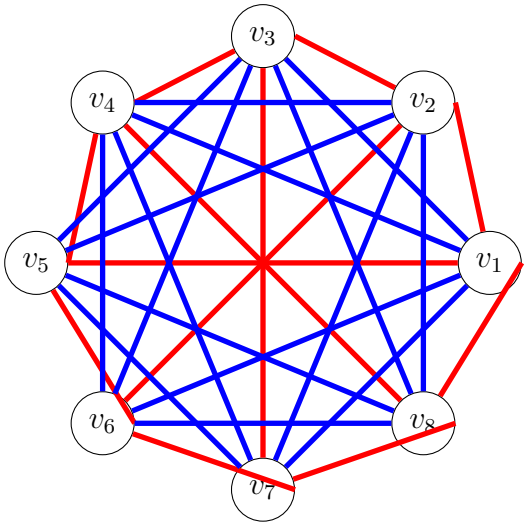
首先，有 9 条邻边时可以成立，对应 K_{10}

向下考虑，K_9 是否可以？如果不可以，则需要每个边都是 5 条红色邻边和 3 条蓝色邻边，此时蓝边数为 $\frac{9\times3}{2}=13.5\notin\mathbb{N}$，不可能。

也就是说，在 K_9 中也存在一个顶点，至少有 6 条红色邻边或者 4 条蓝色邻边。故而 K_9 也满足要求

再向下考虑，如果是 K_8 呢？我们尝试 5 红 2 蓝和 4 红 3 蓝的组合能不能构造一个既不存在红 K_4 也不存在蓝 K_3 的图：

注：



红色边：相邻点、正对点　蓝色边：其余对角线

图 4: 正八边形图：红色边连接相邻点和正对点，蓝色边连接其余对角线

再一般一点请看第一章的 Ramsey 数。

5.2 图论中的基本概念

5.2.1 图的基本定义

定义 5.2.1 图

一个**图** G 是一个有序对 $(V(G), E(G))$，其中：

- $V(G)$ 是顶点集（*vertex set*），元素称为顶点（*vertex*）或节点（*node*）
- $E(G)$ 是边集（*edge set*），元素称为边（*edge*）

定义 5.2.2 无向图、有向图

在**无向图**中，边没有方向，每条边连接两个顶点。边 $e = \{u, v\}$ 表示顶点 u 和 v 之间的连接。

在**有向图**中，边有方向，每条边从一个顶点指向另一个顶点。边 $e = \langle u, v\rangle$ 表示从顶点 u 指向顶点 v 的有向边。

例：

无向图示例　　有向图示例

图 5: 无向图与有向图示例（左：无向图，右：有向图）

定义 5.2.3 简单图

简单图是指没有自环（*self-loop*）和重边（*multiple edges*）的图。

- 自环：连接顶点到自身的边
- 重边：连接相同两个顶点的多条边

注： 简单有向图中，没有 *loop* 和 *multiple edge*，但是可以同时有 $\langle u, v\rangle$ 和 $\langle v, u\rangle$ 两条边。给定一个简单无向图，可以对 E 进行定向，从而得到一个简单有向图。

5.2.2 顶点的度数与图的度数

定义 5.2.4 无向图的度数

在无向图中，顶点 v 的**度数** (*degree*) $d(v)$ 是与 v 相邻的顶点个数，即与 v 相连的边的条数。

$$\forall u \in V, deg(u) = |\{vinV | uvinE\}|$$

定义 5.2.5 有向图的出度和入度

在有向图中：

- **出度** (*out-degree*) $d^+(v)$：从顶点 v 出发的边的条数 $d^+(v) = |\{uinV | \langle u, v\rangle inE\}|$
- **入度** (*in-degree*) $d^-(v)$：指向顶点 v 的边的条数 $d^-(v) = |\{uinV | \langle v, u\rangle inE\}|$
- **度数** (*degree*) $d(v) = d^+(v) + d^-(v)$

定义 5.2.6 平衡图

对于一个有向图，如果所有顶点的出度和入度相等，则称这个图是平衡图。

定理 5.2.1 度数定理

对于任意图 G，所有顶点的度数之和等于边数的两倍：

$$\sum_{v \in V(G)} d(v) = 2|E(G)|$$

证明： 设图 G 有 n 个顶点和 m 条边。对于每条边 $e = \{u, v\}$，它贡献给顶点 u 和 v 各一个度数。

因此，每条边在度数总和中被计算了两次。设所有顶点的度数分别为 $d_1, d_2, \ldots, d_n$，则：

$$\sum_{i=1}^{n} d_i = 2m \qquad \sum_{v \in V(G)} d(v) = 2|E(G)|$$

推论 5.2.1 奇数度数顶点定理

任意图中奇数度数的顶点个数必为偶数。

证明： 设奇数度数顶点个数为 k，偶数度数顶点个数为 m。由度数定理：

$$\sum_{v\in V(G)} d(v) = \sum_{\text{奇数度数}} d(v) + \sum_{\text{偶数度数}} d(v) = 2|E(G)|$$

由于偶数度数顶点的度数之和为偶数，且 $2|E(G)|$ 为偶数，所以奇数度数顶点的度数之和必为偶数。

设奇数度数顶点为 $v_1, v_2, \ldots, v_k$，其度数分别为 $d_1, d_2, \ldots, d_k$，则：

$$\sum_{i=1}^{k} d_i = d_1 + d_2 + \cdots + d_k$$

由于每个 d_i 都是奇数，如果 k 是奇数，则奇数个奇数之和为奇数，这与上述结论矛盾。因此 k 必为偶数。

定理 5.2.2 有向图度数定理

对于任意有向图 G：

$$\sum_{v\in V(G)} d^+(v) = \sum_{v\in V(G)} d^-(v) = |E(G)|$$

证明： 设图 G 有 m 条有向边。对于每条有向边 $e = \langle u, v\rangle$，它贡献给顶点 u 一个出度，贡献给顶点 v 一个入度。

因此，每条边在出度总和中被计算一次，在入度总和中也被计算一次。设所有顶点的出度分别为 $d_1^+, d_2^+, \ldots, d_n^+$，入度分别为 $d_1^-, d_2^-, \ldots, d_n^-$，则：

$$\sum_{i=1}^{n} d_i^+ = \sum_{i=1}^{n} d_i^- = m$$

即 $\sum_{v\in V(G)} d^+(v) = \sum_{v\in V(G)} d^-(v) = |E(G)|$。

5.2.3 路径相关概念与连通性

定义 5.2.7 路径相关概念

- ***Walk***：图中顶点和边的交替序列 $v_0, e_1, v_1, e_2, \ldots, e_k, v_k$，其中每条边 e_i 连接顶点 v_{i-1} 和 v_i，没有别的要求。
- ***Trail***：是不包含重复边的 *Walk*。
- ***Circuit/Closed Trail***：是一条 *Trail*，且起点和终点相同。如果是有向图，这个 *circuit* 中可以同时存在 $\langle u, v\rangle$ 和 $\langle v, u\rangle$ 两条边。
- ***Path***：是不含重复顶点的 *Walk*。
- ***Cycle***：是一条 *Path*，且起点和终点相同。

注：

- *Path* 一定是 *Trail*，*Cycle* 一定是 *Circuit*。
- *Path* 最长为 $|V|-1$，如果一条 *path* 长度为 $|V|-1$，则这条 *path* 经过每个顶点一次，称为 *Hamilton Path*。
- *Cycle* 最长为 $|V|$，如果一条 *cycle* 长度为 $|V|$，则除了起点和终点以外，这条 *cycle* 经过每个顶点一次，称为 *Hamilton Cycle*。
- *Trail* 最长为 $|E|$，如果一条 *trail* 长度为 $|E|$，则这条 *trail* 经过每条边一次，称为 *Eulerian Trail*。
- *Circuit* 最长为 $|E|$，如果一条 *circuit* 长度为 $|E|$，则这条 *circuit* 经过每条边一次，称为 *Eulerian Circuit*。

定义 5.2.8 特殊的 Trail/Circuit/Path/Cycle

- ***Eulerian Trail***：是经过图中每条边恰好一次的 *Trail*。
- ***Eulerian Circuit***：是经过图中每条边恰好一次的 *Circuit*。
- ***Hamilton Path***：是经过图中每个顶点恰好一次的 *Path*。
- ***Hamilton Cycle***：是经过图中每个顶点恰好一次的 *Cycle*。

定义 5.2.9 无向图连通性

图 G 是**连通**的，如果任意两个顶点之间都存在 *Walk*。

$$\forall u, v \in V(G), \exists Walk\langle u, v\rangle$$

定义 5.2.10 有向图连通性

- **两点之间单向连通**：$u, v \in V(G), \exists Walk\langle u, v\rangle \ or \ \langle v, u\rangle$
- **两点之间双向连通**：$u, v \in V(G), \exists Walk\langle u, v\rangle \ and \ \langle v, u\rangle$
- **有向图强连通**：任意两个顶点之间都存在有向路径和有向路径。

$$\forall u, v \in V(G), \exists Walk\langle u, v\rangle \ and \ \langle v, u\rangle$$

- **有向图单向连通**：任意两个顶点之间都存在有向路径。
- **弱连通**：将每条边去掉方向可以得到一个连通无向图。

定义 5.2.11 连通分量

连通分量（*connected component*）是图的一个极大连通子图。如果两个点之间存在 *walk*，则它们属于同一个连通分量。

5.2.4 割集与割点

定义 5.2.12 割

对于无向图 $G = (V, E)$，将其中的点集分为两部分 $V = S_1 \cup S_2$，且 $S_1 \cap S_2 = \emptyset$，则定义 S_1, S_2 的割为：

$$Cut(S_1, S_2) = \{(v_1, v_2) \in E | v_1 \in S_1, v_2 \in S_2\}$$

对于有向图 $G = (V, E)$，将其中的点集分为两部分 $V = S_1 \cup S_2$，且 $S_1 \cap S_2 = \emptyset$，则定义 S_1, S_2 的割为：

$$\overrightarrow{Cut}(S_1, S_2) = \{(v_1, v_2) \in E \mid v_1 \in S_1, v_2 \in S_2\}$$
$$\overrightarrow{Cut}(S_2, S_1) = \{(v_1, v_2) \in E \mid v_1 \in S_2, v_2 \in S_1\}$$

定理 5.2.3 连通性和割的关系

无向图是连通的 $\Leftrightarrow \forall S_1, S_2 \subseteq V, S_1 \cap S_2 = \emptyset, Cut(S_1, S_2) \neq \emptyset$

证明：

$\Rightarrow$：反证：假设连通图 G 中存在为空的割 $Cut(S_1, S_2)$，取 $u_1 \in S_1, u_2 \in S_2$，则 u_1, u_2 之间不存在 $walk$，与连通矛盾。

$\Leftarrow$：现有任意的割均非空，取 $S_1 = \{u_1\}, S_2 = V \setminus \{u_1\}$，则 $Cut(S_1, S_2) \neq \emptyset$，即 u_1 和 S_2 中的点之间存在相连的边，

不妨设 u_1 和 $u_2 \in S_2$ 之间存在边 e，将 S_1 扩充为 $S_1' = \{u_1, u_2\}$，考虑 $Cut(S_1', V \setminus S_1')$，

…

如此进行下去，最终得到 $S_1' = V$，即 G 是连通的。

定理 5.2.4 有向图连通性和割的关系

有向图是强连通的 $\Leftrightarrow \forall S_1, S_2 \subseteq V, S_1 \cap S_2 = \emptyset, \overrightarrow{Cut(S_1, S_2)} \neq \emptyset$ 且 $\overrightarrow{Cut(S_2, S_1)} \neq \emptyset$

证明： $\Rightarrow$：反证：假设强连通图 G 中存在为空的割 $\overrightarrow{Cut(S_1, S_2)}$，取 $u_1 \in S_1, u_2 \in S_2$，则 u_1, u_2 之间不存在 $\overrightarrow{Walk(u_1, u_2)}$，与强连通矛盾。

$\Leftarrow$:现有任意的割均非空,我们来证明任意点 u_i 到其余点 $u_j \in V \setminus \{u_i\}$ 都有 $\overrightarrow{Walk(u_i, u_j)}$。

取 $S_1 = \{u_1\}, S_2 = V \setminus \{u_1\}$，则 $\overrightarrow{Cut(S_1, S_2)} \neq \emptyset$，即存在 u_1 指向 S_2 中的点 u_2 的边，不妨设 $e_1 = \langle u_1, u_2 \rangle$，

将 S_1 扩充为 $S_1' = \{u_1, u_2\}$，考虑 $\overrightarrow{Cut(S_1', V \setminus S_1')}$，

…

如此进行下去，最终得到 $S_1' = V$，即 G 是强连通的。

说明：依据此处的规则，$\forall u_i \in S_1 \setminus \{u_1\}, \exists \overrightarrow{Walk(u_1, u_i)}$，所以我们将 S_1 扩充为 V 的过程就找到了从 u_1 到 V 中任意点的有向路径。

同理对所有的点都适用，所以我们说 G 是强连通的

定理 5.2.5

无向图中两个点之间存在 $walk$，则一定存在 $path$。

证明： $walk$ 可以有重复点，我们直接将重复点之间的点全部删除，剩下的点都不重复，这样就得到了一个 $path$。

例如，对于图 G，u, v 之间存在 $walk$ $u, a, b, c, d, a, f, g, h, v$，则 u, v 之间存在 $path$ u, a, f, g, h, v。

定义 5.2.13 割集、割点、桥

- **割集**（*cut*）是图 G 的一个边集 S，使得删除 S 中的所有边后，图的连通分量数增加。
- **割点**（*cut vertex*）是图 G 中的一个顶点 v，使得删除 v 及其关联的边后，图的连通分量数增加。
- **桥**（*bridge*）是图 G 中的一条边 e，使得删除 e 后，图的连通分量数增加。

问题 5.2.1

一个平衡有向图，它是连通的等价于它是强连通的。

证明： 强连通得到连通是显然的，现在我们主要证明连通 $\Rightarrow$ 强连通。

对于连通图，$\forall S_1 \cup S_2 = V, S_1 \cap S_2 = \emptyset$，有 $\overrightarrow{Cut}(S_1, S_2) \cup \overrightarrow{Cut}(S_2, S_1) \neq \emptyset$。

目标：对于平衡有向图，$\forall S_1 \cup S_2 = V, S_1 \cap S_2 = \emptyset$，有 $\overrightarrow{Cut}(S_1, S_2) \neq \emptyset$ 且 $\overrightarrow{Cut}(S_2, S_1) \neq \emptyset$。

反证：假设该图不是强连通的，则存在 $S_1 \cup S_2 = V, S_1 \cap S_2 = \emptyset$，使得 $\overrightarrow{Cut}(S_1, S_2) \neq \emptyset$ 且 $\overrightarrow{Cut}(S_2, S_1) = \emptyset$（不妨设）。

下面利用平衡图的性质：因为该图是平衡的，所以对于任意顶点集 S_1，有：

$$\begin{aligned}\sum_{v \in V(S_1)} \deg_G^+(v) &= \sum_{v \in S_1} \left(\sum_{u \in V(S_1)} I(< v, u > \in E) + \sum_{u \notin V(S_1)} I(< v, u > \in E) \right) \\ &= \sum_{v \in S_1} \sum_{u \in V(S_1)} I(< v, u > \in E) + \sum_{v \in S_1} \sum_{u \notin V(S_1)} I(< v, u > \in E)\end{aligned}$$

$$\begin{aligned}\sum_{v \in V(S_1)} \deg_G^-(v) &= \sum_{v \in V(S_1)} \left(\sum_{u \in V(S_1)} I(< u, v > \in E) + \sum_{u \notin V(S_1)} I(< u, v > \in E) \right) \\ &= \sum_{v \in S_1} \sum_{u \in V(S_1)} I(< u, v > \in E) + \sum_{v \in S_1} \sum_{u \notin V(S_1)} I(< u, v > \in E)\end{aligned}$$

两者做差，得到：

$$\begin{aligned}&\sum_{v \in V(S_1)} \deg_G^+(v) - \sum_{v \in V(S_1)} \deg_G^-(v) \\ &= \sum_{v \in S_1} \sum_{u \notin V(S_1)} I(< v, u > \in E) - \sum_{v \in S_1} \sum_{u \notin V(S_1)} I(< u, v > \in E) \\ &= 0\end{aligned}$$

于是有：

$$|\overrightarrow{Cut}(S_1, S_2)| = |\overrightarrow{Cut}(S_2, S_1)|$$

但是根据假设，$|\overrightarrow{Cut}(S_1, S_2)| > 0$ 且 $|\overrightarrow{Cut}(S_2, S_1)| = 0$，这与上式矛盾。

所以原假设错误，**平衡有向图的连通性等价于强连通性**。

问题 5.2.2

对于无向图 G，点集 $v_1, v_2, \cdots, v_n$，要求 $deg(v_1) \leq deg(v_2) \leq \cdots \leq deg(v_n)$，$\forall k \in [1, n - deg(v_n) - 1], deg(v_k) \geq k$

证明 G 是连通的。

证明：

反证：假设 G 不连通。则存在一个非平凡的顶点划分 $V = S_1 \cup S_2$，其中 $S_1 \neq \emptyset, S_2 \neq \emptyset, S_1 \cap S_2 = \emptyset$，使得 S_1 和 S_2 之间没有边连接。也即，$Cut(S_1, S_2) = \emptyset$。

不失一般性，设 v_n (度数最大的顶点) 属于 S_1。由于 S_1 和 S_2 之间没有边，这意味着 v_n 的所有邻居都必须在 S_1 中。因此，$|S_1| \geq 1 + deg(v_n) \geq n - deg(v_n)$。$(deg(v_n) \geq n - deg(v_n) - 1)$

同时 $|S_2| = n - |S_1| \leq n - 1 - deg(v_n)$ 令 $m = |S_2|$。则 $m \leq n - 1 - deg(v_n)$。

对于任意顶点 $v_i \in S_2$，由于 S_1 和 S_2 之间没有边，$deg(v_i) \leq |S_2| - 1 = m - 1$。

考虑 v_m，这里 $m \leq n - 1 - deg(v_n)$，有 $deg(v_m) \geq m$ 所以 v_m 需要在 S_1 中

于是有 $|S_2| \leq m - 1$，这与 $|S_2| = m$ 矛盾。所以原假设不成立，G 是连通的。

问题 5.2.3

有向图 $D = (V, E)$，$|V| = n. |E| = m$，且 $m > (n-1)^2$，证明该图强连通。

证明：

方法一，反证：假设 D 不是强连通的，则存在一个非平凡的顶点划分 $V = S_1 \cup S_2$，其中 $S_1 \neq \emptyset, S_2 \neq \emptyset, S_1 \cap S_2 = \emptyset$，使得从 S_1 到 S_2 没有边，即 $\overrightarrow{Cut}(S_1, S_2) = \emptyset$。

设 $|S_1| = k$，$|S_2| = n - k$，其中 $1 \leq k \leq n - 1$。

在这种情况下，边的数量最多为：

$$|E| \leq n(n-1) - k(n-k) \leq n(n-1) - (n-1) = (n-1)^2$$

与条件 $m > (n-1)^2$ 矛盾，所以假设错误，D 是强连通的。

注： 注意这里是有向图，所以在计算最多的边数的时候不用除以 2.

方法二：归纳：

已知当 $n = 1$ 时，图是强连通的（平凡情况）。当 $n = 2$ 时，条件变为 $m > 1$，即 $m \geq 2$。对于两个顶点的有向图，如果边数 ≥ 2，则必然存在双向边，因此图是强连通的。

现假设对于任意具有 k 个顶点（其中 $k < n$）的有向图，如果其边数 $m' > (k-1)^2$，则该图是强连通的。

考虑一个具有 n 个顶点和 $m > (n-1)^2$ 条边的有向图 D。从 V 中任意选择一个顶点 v_1，令 $S_1 = \{v_1\}$，$S_2 = V \setminus \{v_1\}$。

设 $C(S_1, S_2)$ 为连接 S_1 和 S_2 的边的集合，则 $|C(S_1, S_2)| \leq 2(n-1)$。

情况 *1*： 如果 $|C(S_1, S_2)| \geq 2(n-1)$，则 v_1 与 S_2 之间有足够多的连接，可以证明图是强连通的。

情况 *2*： 如果 $|C(S_1, S_2)| \leq 2(n-1)-1$，设 $E(S_2)$ 为 S_2 内部的边数。

则 $E(S_2) = m - |C(S_1, S_2)| \geq (n-1)^2 + 1 - (2(n-1)-1) = (n-2)^2 + 1$。

由于 S_2 有 $n-1$ 个顶点，且 $E(S_2) > (n-2)^2$，根据归纳假设，由 S_2 诱导的子图是强连通的。

此时，若 v_1 与 S_2 之间存在双向边，则图是强连通的。

反证：假设 v_1 与 S_2 之间不存在双向边，则 $|C(S_1, S_2)| \leq n-1$。此时，$m = E(S_2) + |C(S_1, S_2)| \leq (n-1)(n-2) + (n-1) = (n-1)^2$。与条件 $m > (n-1)^2$ 矛盾。

因此，v_1 与 S_2 之间必然存在双向边，整个图 D 是强连通的。

5.3 欧拉回路和哈密顿回路

定义 5.3.1

- ***Eulerian Trail***：是经过图中每条边恰好一次的 *Trail*（*Trail* 指无重复边）。
- ***Eulerian Circuit***：是经过图中每条边恰好一次的 *Circuit*（*Circuit* 指闭合的 *Trail*）。
- ***Hamilton Path***：是经过图中每个顶点恰好一次的 *Path*（*Path* 指无重复顶点）。
- ***Hamilton Cycle***：是经过图中每个顶点恰好一次的 *Cycle*（*Cycle* 指闭合的 *Path*）。

定理 5.3.1 连通有向图的 Eulerian Circuit 定理

有向图 D 存在 *Eulerian Circuit* 当且仅当所有顶点的入度等于出度

$$\forall v \in V(D), \deg_D^+(v) = \deg_D^-(v)$$

证明： $\Rightarrow$：如果存在 *Eulerian Circuit*，在 *Eulerian Circuit* 中，每个顶点被访问的次数等于其入度（或出度），且遍历每一条边，因此每个顶点的入度必等于出度。

$\Leftarrow$：

法一：分裂顶点 当所有顶点的入度等于出度等于 *1* 时，图是一个环，显然存在 *Eulerian Circuit*。

对于任意顶点 v_i，设 $deg_D^+(v_i) = deg_D^-(v_i) = k_i$。我们可以将 v_i 分裂为 k_i 个新顶点 $v_{i1}, v_{i2}, \ldots, v_{ik_i}$，将 v_i 的 k_i 条入边和 k_i 条出边分别分配给 $v_{i1}, v_{i2}, \ldots, v_{ik_i}$，每个新顶点的入度等于出度等于 *1*：

分裂后的图 G' 满足所有顶点的入度等于出度等于 *1*。

设 G' 的连通分量为 $C_1, C_2, \ldots, C_t$，根据归纳基础，G' 的每个连通分量 C_i $(i = 1, 2, \ldots, t)$ 均存在 *Eulerian Circuit*。

将 G' 的各连通分量的 *Eulerian Circuit* 中的 $v_{i1}, v_{i2}, \ldots, v_{ik_i}$ 合并回 v_i，得到 D 的 *Eulerian Circuit*。

法二：归纳 当顶点数为 *2*、边数为 *2* 时，图是一个自环，显然存在 *Eulerian Circuit*。

归纳假设： 假设对于任意边数 $\leq m$ 的连通有向图，如果所有顶点的入度等于出度，则存在 *Eulerian Circuit*。

归纳步骤： 考虑边数为 $m+1$ 的连通有向图 D，其中所有顶点的入度等于出度。

从任意顶点开始，沿着边行走，由于每个顶点的入度等于出度，必然能形成一个回路

C。

移除回路 C 得到图 $D' = D \setminus C$。由于：

- D' 中每个顶点的入度仍然等于出度
- D' 的边数 $\leq m$

根据归纳假设，D' 存在 *Eulerian Circuit* C'。由于 D 连通，C 和 C' 必有公共顶点。在公共顶点处合并 C 和 C'，得到 D 的 *Eulerian Circuit*。

法三：反证假设存在一个满足条件（所有顶点入度等于出度）但不存在 *Eulerian Circuit* 的图。在所有这样的图中，选择边数最少的图 G。

由于 G 满足条件，从任意顶点开始行走，必然能形成一个回路 C。

移除 C 得到 $G' = G \setminus C$。G' 仍然满足所有顶点入度等于出度的条件，且边数更少。

根据 G 的最小性，G' 存在 *Eulerian Circuit* C'。

由于 G 连通，C 和 C' 必有公共顶点，可以合并形成 G 的 *Eulerian Circuit*，矛盾。

因此，满足条件的图必然存在 *Eulerian Circuit*。

定理 5.3.2 平衡有向图中 Cycle 的存在性

给定简单连通有向图 D，若 $\forall v \in V(D)$，$\deg_D^+(v) = \deg_D^-(v)$，则 D 中存在 *Cycle*。

证明： 取任意两个顶点 $v_1, v_2 \in V(D)$，由于 D 连通且平衡，存在从 v_1 到 v_2 的路径 P_1 和从 v_2 到 v_1 的路径 P_2。

设 $P_1 : v_1 \to u_1 \to u_2 \to \cdots \to u_k \to v_2$，$P_2 : v_2 \to w_1 \to w_2 \to \cdots \to w_l \to v_1$。

在 P_2 中寻找最靠近 v_1 的重复出现的点 u_i（即 u_i 在 P_1 中出现，且在 P_2 中距离 v_1 最近）。

构造路径：$v_1 \to u_1 \to u_2 \to \cdots \to u_i \to v_1$。

由于 u_i 是最靠近 v_1 的重复点，所以：

- $v_1 \sim u_i$ 段无重复点
- $u_i \sim v_1$ 段无重复点
- 两条路径中无其他重复点

因此，$v_1 \to u_1 \to \cdots \to u_i \to v_1$ 构成一个 *Cycle*。

定理 5.3.3 简单有向图中 Cycle 的长度

考虑一个简单有向图 D，设：

$$s^+ = \min\{\deg_D^+(v) \mid v \in V(D)\}$$
$$s^- = \min\{\deg_D^-(v) \mid v \in V(D)\}$$
$$k = \max\{s^+, s^-\}$$

则 D 中一定存在一个长度至少为 $k+1$ 的 *Cycle*。

证明： **第一步：证明存在长度至少为 k 的 *Path***

取图中最长的一条 *Path*：$v_0 \to v_1 \to \cdots \to v_l$。由于这是最长 *Path*，所以满足：

- v_0 的所有入边对应的顶点都在 *Path* 中 $\Rightarrow l \geq \deg_D^-(v_0)$
- v_l 的所有出边对应的顶点都在 *Path* 中 $\Rightarrow l \geq \deg_D^+(v_l)$

因此，$l \geq k$。

第二步：构造 *Cycle*

考虑两种情况：

情况 *1*： 利用 v_0 的入边构造 *Cycle* 设存在边 (v_i, v_0)，其中 i 尽可能大。由于 v_0 的所有入边对应的顶点都在 *Path* 中，所以 $i \geq \deg_D^-(v_0)$。

构造 *Cycle*：$v_i \to v_0 \to \cdots \to v_{i-1} \to \cdots \to v_i$。

情况 *2*： 利用 v_l 的出边构造 *Cycle* 设存在边 (v_l, v_j)，其中 j 尽可能小。由于 v_l 的所有出边对应的顶点都在 *Path* 中，所以 $j \leq l - \deg_D^+(v_l)$。

构造 *Cycle*：$v_j \to v_{j+1} \to \cdots \to v_l \to v_j$。

因此，D 中存在长度至少为 $k+1$ 的 *Cycle*。

定理 5.3.4 简单连通无向图的 Eulerian Circuit 定理

简单连通无向图 G 存在 *Eulerian Circuit* 当且仅当所有顶点的度数都是偶数

证明： $\Rightarrow$：如果存在欧拉回路，直接沿着欧拉回路对边定向，则对于每个顶点其入度等于出度，在原本无向图中每个顶点的度数必为偶数。

$\Leftarrow$：当有三个顶点三条边的时候，显然存在 *Eulerian Circuit*。

假设对于边数小于 m 的连通无向图，所有顶点的度数都是偶数，则存在 *Eulerian Circuit*。

考虑边数为 $m+1$ 的连通无向图 G，所有顶点的度数都是偶数。这里我们尝试对 G 寻找一个 *cycle*，然后将这个 *cycle* 去掉。

在 G 中找最长的一条 *path*：$v_0 \to v_1 \to \cdots \to v_l$。则 v_0 的邻接点一定在这个 *path* 中（否则可以延长 *path*）。

故存在 *cycle*。将这个 *cycle* 去掉则剩下的图依然满足所有顶点的度数都是偶数，根据归纳假设，各连通分量存在 *Eulerian Circuit*，将这个 *cycle* 拼回，则得到 G 中存在 *Eulerian Circuit*。

定理 5.3.5 简单连通无向图的 Eulerian Trail 定理

简单连通无向图 G 存在 *Eulerian Trail* 当且仅当恰好有两个顶点的度数为奇数（作为起点和终点）

证明： $\Rightarrow$：如果存在 *Eulerian Trail*，则图必连通。依据 *Eulerian Trail* 对图中的所有的边进行定向，则除了起点和终点以外，其他顶点被访问的次数等于其度数的一半，因此这些顶点的度数必为偶数。再来考虑起点，则出度一定比入度多 *1*，因此起点度数为奇数。对于终点，则入度一定比出度多 *1*，因此终点度数为奇数。

$\Leftarrow$：在 G 中添加一条连接两个奇数度数顶点的边，得到图 G'。此时 G' 中所有顶点的度数都是偶数，由欧拉回路定理，G' 存在欧拉回路。删除添加的边，得到 G 的 *Eulerian Trail*。

定理 5.3.6 Hamiltonian Cycle 的必要条件

如果图 G 存在 *Hamiltonian Cycle*，则对于任意 $S \subseteq V(G)$，有：

$$W(G \setminus S) \leq |S|$$

其中 $W(G \setminus S)$ 表示从 G 中删除 S 中的点以及它们的邻边后，剩余图的连通分支个数。

证明： 设 C 为 G 的 *Hamiltonian Cycle*。

对于任意 $S \subseteq V(G)$，考虑 $C \setminus S$。

由于 C 是一个环，删除 $|S|$ 个顶点后，最多形成 $|S|$ 个连通分支。

因此，$W(C \setminus S) \leq |S|$。

而 $G \setminus S$ 是 $C \setminus S$ 的超图（因为 G 包含 C 的所有边，可能还有额外的边），所以：

$$W(G \setminus S) \leq W(C \setminus S) \leq |S|$$

定义 5.3.2 割点

对于无向图 $G = (V, E)$，如果存在一个点 $v \in V$，使得 $G \setminus \{v\}$ 的连通分支个数大于 G 的连通分支个数，则称 v 为割点。

定理 5.3.7 割点与 Hamiltonian Cycle

如果图 G 存在 *Hamiltonian Cycle*，则 G 中不存在割点。

证明： 根据上一页结论，若存在 *Hamiltonian Cycle*，则对于任意 $S \subseteq V(G)$，有 $W(G \setminus S) \leq |S|$。

特别地，当 $S = \{v\}$ 时（其中 v 是任意一个顶点），有 $W(G \setminus \{v\}) \leq 1$。

这意味着删除任意一个顶点后，图仍然连通，因此 G 中不存在割点。

定理 5.3.8 二部图中的 Hamiltonian Cycle

考虑二部图 $G = (V_1 \cup V_2, E)$，其中 $V_1 \cap V_2 = \emptyset$，且 $\forall e \in E$，$e = (u_1, u_2)$ 其中 $u_1 \in V_1$，$u_2 \in V_2$。

如果 G 存在 *Hamiltonian Cycle*，则 $|V_1| = |V_2|$。

证明： 设 C 为 G 的 *Hamiltonian Cycle*。

在 *Hamiltonian Cycle* 中，顶点必须交替出现在 V_1 和 V_2 中：

$$C : v_1 \to v_2 \to \cdots \to v_n \to v_1$$

其中 $v_1 \in V_1$，$v_2 \in V_2$，$v_3 \in V_1$，以此类推。

因此，V_1 和 V_2 中的顶点数量必须相等，即 $|V_1| = |V_2|$。

推论 5.3.1 奇数顶点二分图

包含奇数个顶点的二分图一定不存在 *Hamiltonian Cycle*。

定理 5.3.9 Dirac 定理

对于简单图 G，令 $\delta = \min\{\deg(v) \mid v \in V(G)\}$，若 $\delta \geq |V(G)|/2$，则 G 中存在 *Hamiltonian Cycle*。

证明： 首先证明图是连通的，反证：假设图 G 不连通，则存在多个连通分量。设 C 为最小的连通分量。满足 $|C| \leq |V(G)|/2$，所以对于 C 中的任意顶点 v_c，其度数满足：

$$\deg(v_c) \leq |C| - 1 < |C| \leq |V(G)|/2$$

与假设 $\delta \geq |V(G)|/2$ 矛盾。因此，G 是连通图。

然后我们来构造 *Hamiltonian Cycle*：

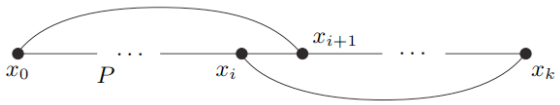
设 $P = x_0 \to x_1 \to \cdots \to x_k$ 为 G 中的最长路径。

由于 P 是最长路径，x_0 和 x_k 的所有邻居都在 P 上。

由于 $\deg(x_0) \geq |V(G)|/2$ 且 $\deg(x_k) \geq |V(G)|/2$，而 P 上除了 x_0 和 x_k 外最多只有 $|V(G)|-2$ 个位置。

根据**抽屉原理**，x_0 的邻居和 x_k 的邻居在 P 上必然有重叠。

因此，存在相邻的两个点 x_i 和 x_{i+1}，使得 x_i 是 x_0 的邻居，x_{i+1} 是 x_k 的邻居。



构造路径：$x_0 \to x_{i+1} \to x_{i+2} \to \cdots \to x_k \to x_i \to x_{i-1} \to \cdots \to x_1 \to x_0$。

这个路径是一个环，包含了 P 的所有点。

然后我们来证明环包含所有顶点：假设存在一个顶点 x 不在环中，但 x 与环中的某个顶点相邻。

将环从 x 处拆开，可以构造出一条比 P 更长的路径，与 P 是最长路径矛盾。

因此，环包含了图 G 的所有顶点，即存在 *Hamiltonian Cycle*。

定理 5.3.10 完全二分图的 Hamiltonian Cycle

考虑二分图 $G=(V_1 \cup V_2, E)$，其中 $|V_1|=|V_2|$，且 G 是完全二分图（即 $\forall u_1 \in V_1, u_2 \in V_2$，$(u_1,u_2) \in E$）。

则 G 中一定存在 *Hamiltonian Cycle*。

证明： 对于完全二分图，每个顶点的度数都等于另一个分部的顶点数。

由于 $|V_1|=|V_2|$，所以 $\delta = |V_1| = |V_2| = |V(G)|/2$。

根据 *Dirac* 定理，G 中存在 *Hamiltonian Cycle*。

5.4 图的表示与图同构

5.4.1 图的矩阵表示

定义 5.4.1 邻接矩阵

对于图 $G=(V,E)$，其中 $V=\{v_1,v_2,\ldots,v_n\}$，G 的**邻接矩阵** $A(G)$ 是一个 $n\times n$ 的矩阵，其中：

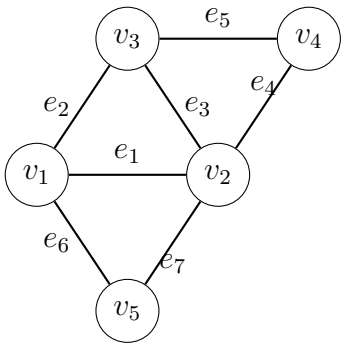
$$A_{ij}=\begin{cases}1, & \text{如果}(v_i,v_j)\in E\\ 0, & \text{否则}\end{cases}$$

定理 5.4.1 邻接矩阵的性质

对于图 G 的邻接矩阵 $A(G)$：

1. $A(G)$ 是对称矩阵（对于无向图）
2. $A(G)^k$ 的第 (i,j) 元素表示从 v_i 到 v_j 的长度为 k 的路径数量
3. 对角线元素为 0（对于简单图）
4. 行和（或列和）等于对应顶点的度数

例： 考虑以下无向图 G：



(a) 图 G

$$A(G)=\begin{pmatrix}0&1&1&0&1\\1&0&1&1&1\\1&1&0&1&0\\0&1&1&0&0\\1&1&0&0&0\end{pmatrix}$$

(b) 邻接矩阵

其中 $A_{ij}=1$ 当且仅当顶点 v_i 和 v_j 之间有边相连。

可以验证：

- $A(G)$ 是对称矩阵（无向图的性质）
- 对角线元素为 0（简单图无自环）

- 每行的 *1* 的个数等于对应顶点的度数($\deg(v_1)=3, \deg(v_2)=4, \deg(v_3)=3, \deg(v_4)=2, \deg(v_5)=2$)

定义 5.4.2 关联矩阵

对于图 $G=(V,E)$，其中 $V=\{v_1,v_2,\ldots,v_n\}$，$E=\{e_1,e_2,\ldots,e_m\}$，G 的**关联矩阵** $B(G)$ 是一个 $n\times m$ 的矩阵，

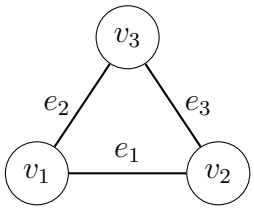
对于**无向图**，

$$B_{ij}=\begin{cases}1, & \text{如果边}e_j\text{是顶点}v_i\text{的一个端点}\\ 2, & \text{如果边}e_j\text{是顶点}v_i\text{的两个端点（自环）}\\ 0, & \text{否则}\end{cases}$$

对于**有向图**，

$$B_{ij}=\begin{cases}1, & \text{如果边}e_j\text{从顶点}v_i\text{出发}\\ -1, & \text{如果边}e_j\text{到达顶点}v_i\text{的终点}\\ 0, & \text{否则}\end{cases}$$

无向图的关联矩阵 考虑以下无向图 G：



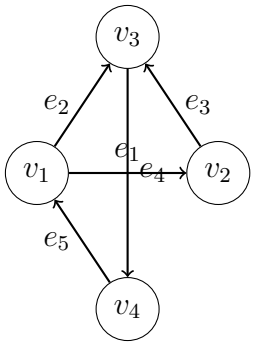
(a) 无向图 G

	e_1	e_2	e_3
v_1	1	1	0
v_2	1	0	1
v_3	0	1	1

(b) 关联矩阵 $B(G)$

其中行对应顶点 v_1,v_2,v_3，列对应边 e_1,e_2,e_3。

有向图的关联矩阵 考虑以下有向图 D：



(a) 有向图 D

	e_1	e_2	e_3	e_4	e_5
v_1	1	1	0	0	-1
v_2	-1	0	1	0	0
v_3	0	-1	-1	1	0
v_4	0	0	0	-1	1

(b) 关联矩阵 $B(D)$

其中行对应顶点 v_1, v_2, v_3, v_4，列对应边 e_1, e_2, e_3, e_4, e_5。
可以验证：

- 每列恰好有一个 *1* 和一个*-1*（每条有向边有一个起点和一个终点）
- 每行的 *1* 的个数等于对应顶点的出度
- 每行的*-1* 的个数等于对应顶点的入度

定义 5.4.3 度数矩阵

对于图 $G = (V, E)$，G 的**度数矩阵** $D(G)$ 是一个对角矩阵，其中：

$$D_{ii} = \deg(v_i), \quad D_{ij} = 0 \ (\text{当} i \neq j)$$

定理 5.4.2 关联矩阵的性质

对于图 G 的关联矩阵 $B(G)$：

1. 每列恰好有两个 *1*（对于简单图）
2. 每行的 *1* 的个数等于对应顶点的度数
3. $B(G) \cdot B(G)^T = A(G) + D(G)$，其中 $A(G)$ 是邻接矩阵，$D(G)$ 是度数矩阵

证明： **性质 *3*：** 设 $C = B(G) \cdot B(G)^T$，则：

$$C_{ij} = \sum_{k=1}^{m} B_{ik} \cdot B_{jk}$$

其中 m 是边的数量。
情况 *1*： $i = j$（对角线元素）

$$\begin{aligned} C_{ii} &= \sum_{k=1}^{m} B_{ik} \cdot B_{ik} = \sum_{k=1}^{m} B_{ik}^2 = \sum_{k=1}^{m} B_{ik} \quad (\text{因为} B_{ik} \in \{0, 1\}) \\ &= \deg(v_i) \quad (\text{第} i \text{ 行的 } 1 \text{ 的个数}) \end{aligned}$$

情况 *2*： $i \neq j$（非对角线元素）

$$C_{ij} = \sum_{k=1}^{m} B_{ik} \cdot B_{jk} = \sum_{k=1}^{m} B_{ik} \cdot B_{jk}$$

只有当边 e_k 同时与顶点 v_i 和 v_j 关联时，$B_{ik} \cdot B_{jk} = 1$，否则为 *0*。

因此：

$$C_{ij} = \begin{cases} 1, & \text{如果}(v_i, v_j) \in E \\ 0, & \text{否则} \end{cases}$$

综上：

$$C_{ij} = \begin{cases} \deg(v_i), & \text{如果} i = j \\ A_{ij}, & \text{如果} i \neq j \end{cases} = A_{ij} + D_{ij}$$

因此 $B(G) \cdot B(G)^T = A(G) + D(G)$。

定义 5.4.4 Laplace 矩阵

对于图 $G = (V, E)$，G 的 ***Laplace* 矩阵** $L(G)$ 定义为：

$$L(G) = D(G) - A(G)$$

其中 D 是度数矩阵，A 是邻接矩阵。

定理 5.4.3 Laplace 矩阵的性质

对于图 G 的 *Laplace* 矩阵 $L(G)$：

1. $L(G)$ 是对称半正定矩阵
2. $L(G)$ 的最小特征值为 0，对应的特征向量为全 1 向量
3. $L(G)$ 的零特征值的重数等于图的连通分量个数
4. 对于任意向量 x，$x^T L(G) x = \sum_{(i,j)\in E} (x_i - x_j)^2$

证明：性质 1： $D(G)$ 和 $A(G)$ 均为对称矩阵，因为 $D_{ij} = D_{ji} = 0$ $(i \neq j)$ 且 $A_{ij} = A_{ji}$（基于无向图的定义）。因此，$L(G) = D(G) - A(G)$ 也是对称矩阵。

定义半正定性：对于任意向量 $x \in \mathbb{R}^n$，计算二次型：

$$\begin{aligned} x^T L(G) x &= x^T (D(G) - A(G)) x \\ &= x^T D(G) x - x^T A(G) x \\ &= \sum_{i=1}^{n} \deg(v_i) x_i^2 - \sum_{(i,j)\in E} x_i x_j. \end{aligned}$$

将第二项重写为边的贡献：注意到 $A(G)$ 的非零项对应边 (i, j)，且 $x^T A(G) x = \sum_{(i,j)\in E} x_i x_j$

(每个边贡献两次，但无向图中计算需注意对称性)。调整为:

$$\begin{aligned} x^T L(G)x &= \sum_{i=1}^{n} \deg(v_i)x_i^2 - 2\sum_{(i,j)\in E} x_i x_j \quad (\text{每个边 } (i,j) \text{ 贡献 } x_i x_j + x_j x_i) \\ &= \sum_{(i,j)\in E} (\deg(v_i)x_i^2 + \deg(v_j)x_j^2 - 2x_i x_j) \quad (\text{通过度数展开}) \\ &= \sum_{(i,j)\in E} (x_i^2 + x_j^2 - 2x_i x_j) \quad (\text{度数贡献相抵}) \\ &= \sum_{(i,j)\in E} (x_i - x_j)^2 \geq 0. \end{aligned}$$

由于 $(x_i - x_j)^2 \geq 0$，且等于 *0* 当且仅当 $x_i = x_j$ 对于所有相邻顶点 (i,j)，$x^T L(G)x \geq 0$ 恒成立。因此 $L(G)$ 是半正定矩阵。

性质 *2*: 设 1 为全 *1* 向量（每个分量为 *1* 的向量)。计算:

$$L(G)\cdot 1 = (D(G) - A(G))\cdot 1.$$

对于 $D(G)\cdot 1$，第 i 项为 $\deg(v_i)$，而 $A(G)\cdot 1$ 的第 i 项为 $\sum_j A_{ij} = \deg(v_i)$（邻接顶点之和)。因此:

$$\begin{aligned} (D(G) - A(G))\cdot 1 &= D(G)\cdot 1 - A(G)\cdot 1 \\ &= (\deg(v_1), \deg(v_2), \ldots, \deg(v_n))^T - (\deg(v_1), \deg(v_2), \ldots, \deg(v_n))^T \\ &= 0. \end{aligned}$$

故 $L(G)\cdot 1 = 0$，*0* 是特征值，全 *1* 向量 1 是对应的特征向量。

性质 *3*: 假设图 G 有 k 个连通分量 $G_1, G_2, \ldots, G_k$。对于每个连通分量 G_i，构造特征向量 $x^{(i)}$，其中 $x_j^{(i)} = 1$ 若 $v_j \in V(G_i)$，否则 $x_j^{(i)} = 0$。则:

$$L(G)x^{(i)} = 0,$$

因为 $x^{(i)}$ 在 G_i 内为常数向量，且 $L(G)$ 的作用在连通分量内保持零特征值（基于性质 *2* 的推广)。这些向量线性无关，因为它们对应不同的连通分量。零特征值的重数等于线性无关的零特征向量个数，即 k。

性质 *4*: 已在前述性质 *1* 的推导中证明。对于任意向量 $x, x^T L(G)x = \sum_{(i,j)\in E}(x_i - x_j)^2$，这反映了图中相邻顶点间差值的平方和，直接由矩阵乘法和边的定义得出。

5.4.2 图的同构

定义 5.4.5 图同构

两个图 $G_1 = (V_1, E_1)$ 和 $G_2 = (V_2, E_2)$ 称为**同构**，记作 $G_1 \cong G_2$，如果存在一个双射 $f : V_1 \to V_2$，使得：

$$(u, v) \in E_1 \Leftrightarrow (f(u), f(v)) \in E_2$$

其中 f 保持边的结构，即若 u 和 v 在 G_1 中相邻，则 $f(u)$ 和 $f(v)$ 在 G_2 中也相邻。

定理 5.4.4 图同构的必要条件

如果 $G_1 \cong G_2$，则：

1. $|V(G_1)| = |V(G_2)|$
2. $|E(G_1)| = |E(G_2)|$
3. G_1 和 G_2 的度数序列相同
4. G_1 和 G_2 的连通分量个数相同
5. G_1 和 G_2 的 *Laplace* 矩阵的特征值相同（包括重数）

定理 5.4.5 邻接矩阵表示下的图同构

设 G_1 和 G_2 的邻接矩阵分别为 A_1 和 A_2，则 $G_1 \cong G_2$ 当且仅当存在置换矩阵 P，使得：

$$A_2 = P^T A_1 P$$

证明： $\Rightarrow$：如果 $G_1 \cong G_2$，则存在双射 $f : V_1 \to V_2$。

定义置换矩阵 P，其中 $P_{ij} = 1$ 当且仅当 $f(v_i) = v_j$。

则对于任意 i, j：

$$\begin{aligned}(P^T A_1 P)_{ij} &= \sum_{k,l} P_{ki} A_{1,kl} P_{lj} \\ &= A_{1,f^{-1}(i),f^{-1}(j)} \\ &= A_{2,ij}\end{aligned}$$

$\Leftarrow$：如果存在置换矩阵 P 使得 $A_2 = P^T A_1 P$，则定义 $f(v_i) = v_j$ 当且仅当 $P_{ij} = 1$。

这个映射 f 就是图同构。

定理 5.4.6 关联矩阵表示下的图同构

设 G_1 和 G_2 的关联矩阵分别为 B_1（$|V_1| \times |E_1|$ 矩阵）和 B_2（$|V_2| \times |E_2|$ 矩阵），其中 $B_{1,vi,e} = 1$ 若顶点 $v_i \in V_1$ 与边 $e \in E_1$ 相邻，$B_{1,vi,e} = 0$ 否则，B_2 类似定义。则 $G_1 \cong G_2$ 当且仅当存在置换矩阵 P_V（$|V_1| \times |V_2|$）和 P_E（$|E_1| \times |E_2|$）使得：

$$B_2 = P_V^T B_1 P_E$$

证明： $\Rightarrow$：如果 $G_1 \cong G_2$，存在双射 $f_V : V_1 \to V_2$ 和 $f_E : E_1 \to E_2$ 保持结构，即若边 $e = (u, v) \in E_1$，则 $f_E(e) = (f_V(u), f_V(v)) \in E_2$。构造置换矩阵 P_V（$P_{V,ij} = 1$ 当 $f_V(v_i) = v_j$）和 P_E（$P_{E,ij} = 1$ 当 $f_E(e_i) = e_j$）。对于 B_2 的元素 $(P_V^T B_1 P_E)_{vk}$，计算：

$$(P_V^T B_1 P_E)_{vk} = \sum_{i,j} P_{V,iv} B_{1,ij} P_{E,jk},$$

$P_{V,iv} = 1$ 当 $i = f_V^{-1}(v)$，$P_{E,jk} = 1$ 当 $j = f_E^{-1}(e_k)$，故 $(P_V^T B_1 P_E)_{vk} = B_{2,vk}$，因为 f_V 和 f_E 保持邻接关系。因此 $B_2 = P_V^T B_1 P_E$。

$\Leftarrow$：如果存在 P_V 和 P_E 使得 $B_2 = P_V^T B_1 P_E$，定义 $f_V(v_i) = v_j$ 当 $P_{V,ij} = 1$，$f_E(e_i) = e_j$ 当 $P_{E,ij} = 1$。由于 P_V 和 P_E 是置换矩阵，f_V 和 f_E 是双射。若 $B_{1,ui} = 1$（v_u 与 e_i 相邻），则 $(P_V^T B_1 P_E)_{f_V(u), f_E(i)} = 1$，故 $B_{2,f_V(u),f_E(i)} = 1$，即 $f_V(u)$ 与 $f_E(i)$ 相邻，f 保持结构。因此 $G_1 \cong G_2$。

定理 5.4.7 图同构的不变量

以下性质是图同构的不变量（即如果两个图同构，则这些性质必须相同）：

1. 顶点数和边数
2. 度数序列
3. 连通分量个数
4. 图的直径（最长最短路径长度）
5. 图的围长（图中最短环的长度，若存在）
6. 邻接矩阵的特征值（包括重数）
7. *Laplace* 矩阵的特征值（包括重数）
8. 图的色数（最小所需颜色数以正确着色）
9. 图的团数（最大完全子图的个数）

5.5 树

5.5.1 树的定义与性质

定义 5.5.1 树

树是一个连通无环图。即图 $T=(V,E)$ 是树当且仅当：

1. T 是连通的
2. T 中不存在环

定理 5.5.1 树的基本性质

对于树 $T=(V,E)$，以下性质等价：

1. T 是连通的且无环
2. T 中任意两个顶点之间有唯一路径
3. T 是连通的，但删除任意一条边后不再连通
4. T 中无环，但添加任意一条边后会产生环
5. T 是连通的且 $|E|=|V|-1$
6. T 中无环且 $|E|=|V|-1$

证明： (1) $\Rightarrow$ (2)：由于 T 连通，任意两个顶点间存在路径。假设存在两条不同路径 P_1 和 P_2，则 $P_1 \cup P_2$ 包含环，矛盾。

(2) $\Rightarrow$ (3)：删除边 $e=(u,v)$ 后，u 和 v 之间无路径，故不连通。

(3) $\Rightarrow$ (4)：添加边 $e=(u,v)$ 后，u 和 v 之间已有路径，形成环。

(4) $\Rightarrow$ (1)：显然连通且无环。

(1) $\Rightarrow$ (5)：对顶点数归纳。$|V|=1$ 时显然。假设对 $|V|=n-1$ 成立，考虑 $|V|=n$ 的树。删除一个叶子顶点，得到 $n-1$ 个顶点的树，边数为 $n-2$。原树边数为 $n-1$。

(5) $\Rightarrow$ (6)：显然。

(6) $\Rightarrow$ (1)：假设不连通，则边数 $\leq |V|-2$，矛盾。

定理 5.5.2 树的边数定理

对于简单连通无向图 $G=(V,E)$，有 G 是树当且仅当 $|E|=|V|-1$。

证明： $\Rightarrow$ 对顶点数归纳。

基础： $|V| = 1$ 时，$|E| = 0 = 1 - 1$。

归纳： 假设对 $|V| = n - 1$ 的树成立。考虑 $|V| = n$ 的树 T。

由于 T 无环且连通，存在叶子顶点 v（度数为 1 的顶点，否则有环，具体证明见前文）。删除 v 及其关联边，得到树 T'，有 $|V(T')| = n - 1$。

根据归纳假设，$|E(T')| = (n-1) - 1 = n - 2$。

因此 $|E(T)| = |E(T')| + 1 = (n-2) + 1 = n - 1$。

$\Leftarrow$ 设连通图 G 满足 $|E| = |V| - 1$，证明 G 无环。

假设 G 有环，删除环中任意一条边 e，得到图 G'。

由于 G 连通，删除环中的边后 G' 仍连通。

G' 满足 $|E(G')| = |E(G)| - 1 = |V| - 2$，且 $|V(G')| = |V|$。

但是连通图的边数不能小于 $|V| - 1$，矛盾。因此 G 无环，是树。

定义 5.5.2 森林

森林是无环的无向图。换句话说，森林是若干棵树的并集，每个连通分量都是一棵树。

定理 5.5.3 森林的边数

对于森林 F（无环图），有 $|E| = |V| - c$，其中 c 是连通分量数。

证明： 设森林 F 有 k 个连通分量 $T_1, T_2, \ldots, T_k$，每个 T_i 是树。

根据树的边数定理，$|E(T_i)| = |V(T_i)| - 1$。

因此：

$$\begin{aligned} |E| &= \sum_{i=1}^{k} |E(T_i)| \\ &= \sum_{i=1}^{k} (|V(T_i)| - 1) \\ &= \sum_{i=1}^{k} |V(T_i)| - k \\ &= |V| - k \end{aligned}$$

其中 $k = c$ 是连通分量数。

5.5.2 桥的概念

定义 5.5.3 桥

对于连通图 G，边 e 称为**桥**，如果删除 e 后图不再连通。

定理 5.5.4 桥的性质

边 e 是桥当且仅当 e 不在任何环中。

证明： $\Rightarrow$：如果 e 在某个环 C 中，删除 e 后，C 中其他边仍连接 e 的两个端点，图仍连通。

$\Leftarrow$：如果 e 不是桥，删除 e 后图仍连通，则 e 的两个端点间存在不经过 e 的路径，与 e 构成环。

定理 5.5.5 树中的边都是桥

对于树 T，任意边都是桥。

证明： 由于树无环，根据桥的性质，任意边都是桥。

5.5.3 生成子图与生成树

定义 5.5.4 生成子图与生成树

图 H 是图 G 的**生成子图**，如果 $V(H) = V(G)$ 且 $E(H) \subseteq E(G)$。

图 G 的**生成树**是 G 的连通生成子图，且是树。

定理 5.5.6 连通图存在生成树

连通图 G 存在生成树。

证明： **构造：** 从 G 开始，重复删除环中的边，直到无环。

算法步骤：

1. 初始化：$T = G$
2. 当 T 中存在环 C 时：
   - 选择环 C 中的任意边 e
   - 删除边 e：$T = T - e$ 由于每次删除环中的边，T 始终连通
3. 输出 T 最终 T 无环，是树

定理 5.5.7 生成树的边数

对于 n 个顶点的连通图 G，任意生成树都有 $n-1$ 条边。

证明： 生成树是树，根据树的边数定理，边数为 $|V|-1=n-1$。

5.5.4 最小生成树算法

定义 5.5.5 最小生成树

对于带权图 G，**最小生成树**是权重最小的生成树。

定理 5.5.8 Kruskal 算法的正确性

Kruskal 算法能够找到最小生成树。

算法过程：

1. 将边按权重升序排列
2. 初始化：$T=(V,\emptyset)$
3. 对于每条边 e：
   - 如果 $T+e$ 无环，则 $T=T+e$
   - 否则跳过 e
4. 输出 T

正确性证明： 设 T 是算法输出的树，T^* 是最小生成树。

引理 5.5.1

对于任意割 $(S,V-S)$，最小生成树包含该割的最小权重边。

证明： 假设 T^* 不包含割的最小权重边 e。将 e 加入 T^* 形成环，删除环中另一条边 f，得到更小的生成树，矛盾。

现对算法选择的边数归纳：空集显然是最小生成树的子集。

假设算法已选择边集 E'，且存在最小生成树 T^* 包含 E'。

算法选择下一条边 $e=(u,v)$。设 S 是 u 所在连通分量，则 e 是割 $(S,V-S)$ 的最小权重边。

根据引理，T^* 包含 e，因此存在最小生成树包含 $E' \cup \{e\}$。
因此算法输出的是最小生成树。

定理 5.5.9 Prim 算法的正确性

Prim 算法能够找到最小生成树。

算法过程：

1. 选择任意顶点 v_0，$S = \{v_0\}$
2. 重复直到 $S = V$：
   - 选择 S 到 $V - S$ 的最小权重边 $e = (u, v)$，其中 $u \in S$，$v \in V - S$
   - 将 v 加入 S，将 e 加入树

正确性证明： 每次选择的边都是当前割的最小权重边，根据割的性质，这些边都在最小生成树中。

Kruskal 算法与 Prim 算法的对比

- **基本思想**：
  - ***Kruskal* 算法**：每次选择全局范围内权值最小且不会产生环的边，逐步合并连通分量，直到所有顶点连通。
  - ***Prim* 算法**：每次从当前生成树出发，选择一条连接树内外的最小权值边，将新顶点加入生成树，直到所有顶点都被包含。
- **操作对象**：
  - ***Kruskal***：以“边”为核心，适合稀疏图。
  - ***Prim***：以“点”为核心，适合稠密图。
- **实现方式**：
  - ***Kruskal***：常用并查集（*Union-Find*）维护连通分量。
  - ***Prim***：常用优先队列（堆）维护可扩展的最小边。
- **适用场景**：
  - ***Kruskal***：边数远小于点数平方时效率高，适合稀疏图。
  - ***Prim***：点数较少或图较稠密时效率高，适合稠密图。

- **生成树结构**：
  - ***Kruskal***：生成树可能不是连通的中间状态，最终合并为一棵树。
  - ***Prim***：始终保持一个连通的生成树逐步扩展。
- **复杂度**：
  - ***Kruskal***：$O(E \log E)$，E 为边数。
  - ***Prim***：$O(E \log V)$，V 为顶点数（用堆实现）。

定理 5.5.10 生成树的数量

对于完全图 K_n，生成树的数量为 n^{n-2}（*Cayley* 公式）。

证明： **双射：**建立生成树与长度为 $n-2$ 的序列之间的双射。

1. 编码：对于生成树 T，重复删除编号最大的叶子顶点，记录其邻居，得到序列。
2. 解码：从序列重建生成树。

双射性质：每个序列对应唯一生成树，每个生成树对应唯一序列。
因此生成树数量等于序列数量：n^{n-2}。

5.6 平面图

定义 5.6.1 平面图及相关概念

如果一个图可以画在平面上，使得任意两条边只有公共端点处相交（即没有边的交叉），则称该图为**平面图**。

相关的概念：

- 将图画在平面上且无边交叉的方式称为该图的**平面嵌入**。
- 平面图的平面嵌入将平面划分为若干个区域，这些区域称为**面**（包括无限外部区域）。
- 平面图的任意子图仍然是平面图。

注： 不是所有图都是平面图。例如完全图 K_5 和完全二分图 $K_{3,3}$ 都不是平面图。

定理 5.6.1 平面图的基本性质

- 平面图可以有多种不同的平面嵌入方式，但面数等性质不变。
- 平面图的每条边至多属于两个面。
- 平面图的每个面都被一条闭合的边界包围。

定理 5.6.2 Euler 公式

设 G 是一个连通的平面图，v 为顶点数，e 为边数，f 为面数，则有：

$$v - e + f = 2$$

证明： 对边数归纳。

基础： G 为树时，$e = v - 1$，只有一个面（外部），$f = 1$，$v - (v-1) + 1 = 2$。

归纳： 若 G 有环，去掉一个环上的边，面数减少 1，$v - e + f$ 不变。最终归纳到树。

定理 5.6.3 平面图的边数上界

设 G 是一个连通的简单平面图，$v \geq 3$，则有：

$$e \leq 3v - 6$$

证明： 每个面至少被三条边围成，且每条边至多属于两个面：$2e \geq 3f$。由 *Euler* 公式 $f = e - v + 2$，代入得 $2e \geq 3(e - v + 2)$，化简得 $e \leq 3v - 6$。

推论 5.6.1

若 G 是平面图且无三角形（即每个面至少四条边），则 $e \leq 2v - 4$。

5.7 图的匹配

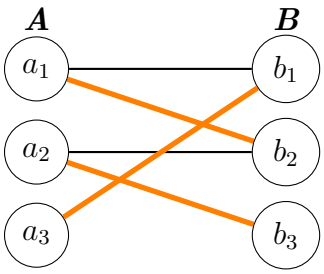
5.7.1 基本定义

定义 5.7.1 匹配及相关概念

在无向图 $G=(V,E)$ 中，**匹配**是指一组边的集合，使得任意两条边都没有公共端点。相关的概念还有：

- 如果匹配 M 覆盖了图中所有顶点（即每个顶点都恰好属于 M 中的一条边），则称 M 为**完美匹配**。
- 在图 G 中，边数最多的匹配称为**最大匹配**。
- 如果顶点集 V 可以分为两个不交的子集 A,B，且每条边都连接 A 中的顶点和 B 中的顶点，则 G 是**二分图**。

二分图匹配的例子 如下图所示，$G=(A\cup B,E)$ 是一个二分图，$A=\{a_1,a_2,a_3\}$，$B=\{b_1,b_2,b_3\}$。



上图中，橙色高亮的三条边构成了一个完美匹配：$\{(a_1,b_2),(a_2,b_3),(a_3,b_1)\}$，每个顶点都被唯一匹配。

5.7.2 二分图匹配与 Hall 定理

定义 5.7.2 二分图的匹配与完美匹配

设 $G=(A\cup B,E)$ 是二分图，匹配 M 是 E 的子集，且任意两条边不共享端点。若 $|A|=|B|$，且存在匹配 M 使得每个顶点都被 M 覆盖，则称 G 有**完美匹配**。

定理 5.7.1 Hall 定理

设 $G=(A\cup B,E)$ 是二分图，$|A|=|B|$。G 存在完美匹配当且仅当：

$$\forall S\subseteq A \text{ or } S\subseteq B,\quad |N(S)|\geq |S|$$

其中 $N(S)$ 表示 S 在 B 中的邻居集合。

证明： $\Rightarrow$：若 G 有完美匹配，则对任意 $S\subseteq A$，匹配中的边将 S 映射到 B 的 $|S|$ 个不同顶点，故 $|N(S)|\geq |S|$。

$\Leftarrow$：归纳：$|A|=1$ 时显然成立。

假设 $|A|=n$ 时成立，考虑 $|A|=n+1$。

若对所有 $S\subseteq A$，$|N(S)|>|S|$，则任选 $a\in A$，存在 $b\in N(\{a\})$，删去 a,b 及相关边，剩余二分图满足条件，归纳成立。

若存在 $S_0\subseteq A$，$|N(S_0)|=|S_0|$，则 $G[S_0\cup N(S_0)]$ 和 $G[(A\setminus S_0)\cup(B\setminus N(S_0))]$ 都满足 *Hall* 条件，分别递归匹配，合并即得全局完美匹配。

注： *Hall* 定理给出了二分图存在完美匹配的充要条件。