

XCPC 数学基础

ljh

2025 年 8 月 25 日

目录

第一章 组合数学	1
1.1 基本排列组合公式	1
1.2 重要组合恒等式	2
1.3 二项式系数	3
1.4 抽屉原理	4
1.5 容斥原理	6
1.5.1 容斥原理	6
1.5.2 计算有禁止位置的非攻击型车的方法数，有禁止位置 的排列数	7
1.5.3 莫比乌斯反演 I	11
1.5.4 莫比乌斯反演 II	15
1.6 递推关系和生成函数	16
1.6.1 生成函数	16
1.7 卡特兰数和第二类斯特林数	20
1.7.1 卡特兰数	20
1.7.2 斯特林数	20
1.7.3 球盒模型	23
1.8 二项式反演	24
1.8.1 高维二项式反演	25

目录	II
第二章 数论	26
2.1 整除	26
2.2 同余	29
2.2.1 同余	29
2.2.2 线性同余方程	31
2.3 乘性函数	35
第三章 求和	39
3.1 递归问题 RECURRENT PROBLEMS	39
3.1.1 repertoire method	39
3.1.2 约瑟夫问题	40
3.2 和式 SUMS	40
3.2.1 和式和递归式 SUMS AND RECURRENCES	40
3.2.2 和式的处理 MANIPULATION OF SUMS	42
3.2.3 扰动法 (perturbation method)	42
3.2.4 多重和式 MULTIPLE SUMS	43
3.2.5 一般性的方法 GENERAL METHODS	45
3.2.6 有限微积分	48
3.2.7 无限和式 INFINITE SUMS	51
第四章 概率论	53
4.1 基本概念和公式	53
4.2 重要公式与结论	57
4.2.1 数学期望 (均值) 与方差	59
4.3 期望经典问题入门	61
4.3.1 普通	61
4.3.2 拿球	64
4.3.3 游走	64

目录	III
4.3.4 解题方法	66
第五章 杂	67
5.1 最小二乘法	67
5.2 常用幂级数	68

第一章 组合数学

1.1 基本排列组合公式

1. 线性排列: n 个数的 r 排列 $P(n, r) = \frac{n!}{(n-r)!}$
2. 圆排列: n 个数的 r 排列 $\frac{P(n, r)}{r}$
3. 项链数: n 个不同的珠子串成一串项链, 则得到不同的项链数为

$$p = \begin{cases} 1, & (n \leq 2) \\ \frac{(n-1)!}{2}, & (otherwise) \end{cases}$$

4. 多重集合的排列: 有 k 种元素, 每种 n_1, n_2, \dots, n_k 个, 的排列公式为

$$\frac{n!}{\prod_{i=1}^k (n_i!)}$$

或记为

$$\binom{n}{n_1, n_2, \dots, n_k}$$

5. 组合:

$$\binom{n}{r} = \frac{P(n, r)}{r!}$$

6. 多重集的组合 设 S 是有 k 种元素的集合, 每种元素无限个 ($\geq r$), 则其 r 组合的个数为:

$$\binom{r+k-1}{r}$$

或者说有

结论 1.1.1. $x_1 + x_2 + \cdots + x_k = r (x_i \geq 0)$ 的整数解有

$$\binom{r+k-1}{r}$$

种.

1.2 重要组合恒等式

1. Pascal 公式

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

2.

$$\sum_{i=0}^n \binom{n}{i} = 2^n$$

3.

$$m \cdot \binom{n}{m} = n \cdot \binom{n-1}{m-1}$$

4.

$$\sum_{k=1}^n k \cdot \binom{n}{k} = n \cdot \sum_{k=1}^n \binom{n-1}{k-1} = n \cdot 2^{n-1}$$

5. 朱世杰恒等式

$$\binom{m+n+1}{n+1} = \sum_{i=0}^m \binom{n+i}{n}$$

6. 范德蒙德恒等式

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

特别地:

$$\binom{2n}{n} = \sum_{i=0}^n \binom{n}{i} \binom{n}{n-i}$$

结论 1.2.1. m 个 a , 和最多 n 个 b 的排列数等于

$$\binom{m+n+1}{m+1}$$

结论 1.2.2. 最多 m 个 a , 和最多 n 个 b 的排列数等于

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

7.

$$\sum_{1 \leq k \leq n} k \binom{n}{k} = n2^{n-1} \quad (n \geq 1)$$

8. 利用导数可以得到

$$\sum_{1 \leq k \leq n} k^2 \binom{n}{k} = n(n+1)2^{n-2} \quad (n \geq 1)$$

1.3 二项式系数

结论 1.3.1. 在杨辉三角中规定只能向下或者右下移动, 从 $(0,0)$ 到 (n,k) 的路径数为 $\binom{n}{k}$

定理 1.3.2. 二项式定理

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

定理 1.3.3. *Sperner* 定理:

设 S 是 n 元素集合. 那么 S 上的一个反链至多包含 $\binom{n}{\lfloor \frac{n}{2} \rfloor}$ 个集合.

其中, 这里的反链指的是以集合包含为偏序关系的反链, 即 S 的一个子集的集合, 任何两个集合没有关系.

结论 1.3.4. 多项式系数的帕斯卡公式

$$\binom{n}{n_1, n_2, \dots, n_t} = \binom{n-1}{n_1-1, n_2, \dots, n_t} + \binom{n-1}{n_1, n_2-1, \dots, n_t} + \dots + \binom{n-1}{n_1, n_2, \dots, n_t-1}$$

定理 1.3.5. 多项式定理

$$(x_1 + x_2 + \dots + x_t)^n = \sum \binom{n}{n_1, n_2, \dots, n_t} x_1^{n_1} x_2^{n_2} \dots x_t^{n_t}$$

定理 1.3.6. 牛顿多项式定理

$$(1+z)^a = \sum_{k=0}^{\infty} \binom{a}{k} z^k \quad (a \in R, |z| < 1)$$

定理 1.3.7. Dilworth 定理

设 (X, \leq) 是有限偏序集合, 而 m 是反链的最大大小, 则 X 可以被划分为 m 个链, 但不能被划分成小于 m 个链.

设 (X, \leq) 是有限偏序集合, 而 r 是链的最大大小, 则 X 可以被划分为 r 个反链, 但不能被划分成小于 r 个反链.

1.4 抽屉原理

简单形式

结论 1.4.1. 如果要把 $n+1$ 个物体放进 n 个盒子, 那么至少有一个盒子有至少 2 个物体

加强形式

结论 1.4.2. 设 q_1, q_2, \dots, q_n 是正整数. 如果将 $q_1 + q_2 + \dots + q_n - n + 1$ 个物体放进 n 个盒子. 那么要么第一个盒子含有 q_1 个物体, \dots , 要么第 n 个物体含有 q_n 个物体.

定理 1.4.3. *Ramsey* 定理

在 6 个人 (或者更多), 要么有 3 个人互相认识, 要么有 3 个人互相都不认识.

或者说

对于 $K_n (n \geq 6)$ 我们给他的所有边染红色或蓝色, 总存在一个红 K_3 或蓝 K_3 , 记为 $K_6 \rightarrow K_3, K_3$

推广

定理 1.4.4. 若 $m, n \geq 2$, 存在正整数 p , 使得 $K_p \rightarrow K_m, K_n$ 事实上, 注意到若 p 成立, 则对于 $q \geq p$ 都成立, 取一个子图即可. 我们记 *Ramsey* 数 $r(m, n)$ 为使之成立的最小的数. *Ramsey* 定理保证这样的数一定存在. 注意到

$$r(m, n) = r(n, m)$$

以及

$$r(2, m) = m$$

当 $m \geq 2$ 时, $r(2, m)$ 称为平凡的 *Ramsey* 数 (交换同理).

性质

1.

$$r(m, n) \leq r(m-1, n) + r(m, n-1) (m, n \geq 3)$$

2.

$$r(m, n) \leq \binom{m+n-2}{n-1}$$

(数学归纳法证明)

1.5 容斥原理

1.5.1 容斥原理

定理 1.5.1. 容斥原理

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = |S| - \sum |A_i| + \sum |A_i \cap A_j| + \cdots + (-1)^n |A_1 \cap A_2 \cap \cdots \cap A_n|$$

可根据贡献法证明.

应用: 不定方程整数解个数问题

例 1.5.2. 求下列方程整数解个数

$$x_1 + x_2 + x_3 + x_4 = 18$$

满足

$$1 \leq x_1 \leq 5, \quad -2 \leq x_2 \leq 4, \quad 0 \leq x_3 \leq 5, \quad 3 \leq x_4 \leq 9$$

解:

等价于

$$a_1 + a_2 + a_3 + a_4 = 16$$

满足

$$0 \leq a_1 \leq 4, \quad 0 \leq a_2 \leq 6, \quad 0 \leq a_3 \leq 5, \quad 0 \leq a_4 \leq 6$$

不加范围的解的个数为

$$|S| = \binom{16+4-1}{16} = 969$$

其中设 A_1 为 a_1 大于 4 的解的集合 A_2 为 a_2 大于 6 的解的集合 ...

$$|A_1| = \binom{11+4-1}{11} = 364$$

$$|A_2| = \binom{9+4-1}{9} = 220$$

$$|A_3| = \binom{13}{10} = 286$$

$$|A_4| = \binom{12}{9} = 220$$

同理算交集. 然后根据容斥原理可得出答案为 55

结论 1.5.3. 错位排列

$$D_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} \right)$$

有性质

1.

$$\frac{D_n}{n!} \approx e^{-1}$$

2. $D_1 = 0, D_2 = 1$

$$D_n = (n-1)(D_{n-1} + D_{n-2})$$

3.

$$D_n = (n-1)(D_{n-1} + D_{n-2})$$

$$\iff D_n - nD_{n-1} = -(D_{n-1} - (n-1)D_{n-2})$$

$$\iff D_n = nD_{n-1} + (-1)^n$$

结论 1.5.4.

$$Q_n = n! - \binom{n-1}{1}(n-1)! + \binom{n-1}{2}(n-2)! - \binom{n-1}{3}(n-3)! + \cdots + (-1)^{n-1} \binom{n-1}{n-1} 1!$$

为不出现 $i(i+1)$ 的排列数并且有

$$Q_n = D_n + D_{n-1}$$

1.5.2 计算有禁止位置的非攻击型车的方法数, 有禁止位置的排列数

在一个 $n \times n$ 的棋盘上, 某些格子是禁止位置 (不得放车)。将车理解为国际象棋中的 rook (只能沿行或列移动), 所谓“非攻击型车”即任意两车不在同一行也不在同一列。研究以下两类计数问题:

1. 在允许的位置上放满 n 个车（即一个合法的排列），并且所有车均不落在禁止位置上——计数所有这样的排列数。
2. 更一般地：在允许的位置上恰好放 k 个互不攻击的车的计数（任意 k ）。

定理 1.5.5. 设 B 为禁止位置集合。令 r_t 表示：仅在禁止位置上放置恰好 t 个互不攻击的车的方法数（即在禁止格子中选择 t 个格子，且两两不同行不列）。则通过包含-排除有下面的公式：

$$P = \sum_{t=0}^n (-1)^t r_t (n-t)!$$

这里 P 表示不在禁止位置上放置 n 个互不攻击车（即“允许格上满排”的数量）。

计算 r_t 是核心。一个常用、易实现的方法是按行进行状态压缩 DP（适合 $n \lesssim 20$ ）。设第 i 行的禁止列掩码为 f_i （长度为 n 的位掩码，若 j -位为 1 表示位置 (i, j) 被禁止）。我们枚举每行是否在该行的某个禁止列放一个车（并保证列不冲突）。

具体 DP 设：

$\text{dp}_i[\text{mask}] =$ 在处理了前 i 行后，已被禁止位置上的车占用的列集合为 mask 的方法数。

转移（对第 i 行）：

- 不在本行的禁止位置放车： $\text{dp}_{i+1}[\text{mask}] += \text{dp}_i[\text{mask}]$ ；
- 在本行放一个车：枚举本行的某个位 $j \in f_i$ 且在 mask 中未被占用，则 $\text{dp}_{i+1}[\text{mask} \cup \{j\}] += \text{dp}_i[\text{mask}]$ 。

最终，处理完 n 行后，对所有 mask 统计其位数 $t = \text{popcount}(\text{mask})$ ，累加得到 r_t 。

或者用积和式的表达式计算

将禁止的位置记作 0，其他为 1，得到矩阵 $a_{i,j}$ ，那么方法数为

定理 1.5.6.

$$F(X_n) = \sum_{S \subseteq X_n} (-1)^{n-|S|} \prod_{i=1}^n \left(\sum_{j \in S} a_{ij} \right)$$

Listing 1.1: 优化的 Ryser 实现: 先预处理每行的子集和, 时间复杂度 $O(n2^n)$

// ai 生成未验证

```
#include <bits/stdc++.h>
```

```
using namespace std;
```

```
using ll = long long;
```

```
const ll MOD = 998244353;
```

```
int main() {
```

```
    ios::sync_with_stdio(false);
```

```
    cin.tie(nullptr);
```

```
    int n;
```

```
    if (!(cin >> n)) return 0;
```

```
    vector<vector<ll>> a(n, vector<ll>(n));
```

```
    for (int i = 0; i < n; ++i)
```

```
        for (int j = 0; j < n; ++j) {
```

```
            ll x; cin >> x;
```

```
            a[i][j] = (x % MOD + MOD) % MOD;
```

```
        }
```

```
    int N = 1 << n;
```

```
    vector<vector<ll>> rowSum(n, vector<ll>(N, 0));
```

```
    for (int i = 0; i < n; ++i) {
```

```

    for (int mask = 1; mask < N; ++mask) {
        int low = mask & -mask;
        int bit = __builtin_ctz(low);
        rowSum[i][mask] = rowSum[i][mask ^ low] + a[i][bit];
        if (rowSum[i][mask] >= MOD) rowSum[i][mask] -= MOD;
    }
}

ll ans = 0;
for (int mask = 0; mask < N; ++mask) {
    ll prod = 1;
    for (int i = 0; i < n; ++i) {
        prod = prod * rowSum[i][mask] % MOD;
        if (prod == 0) break; // 剪枝：积为0则无需继续
    }
    int bits = __builtin_popcount((unsigned)mask);
    if (((n - bits) & 1)) {
        ans -= prod;
        if (ans < 0) ans += MOD;
    } else {
        ans += prod;
        if (ans >= MOD) ans -= MOD;
    }
}

cout << ans << '\n';
return 0;

```

}

1.5.3 莫比乌斯反演 I

容斥原理是莫比乌斯反演在有限偏序集上的一个实例.

偏序集形式的容斥原理

对于一个偏序集 $(\mathcal{P}(X_n), \subseteq)$, (X_n 为 n 元集), 若

$$F, G : \mathcal{P}(X_n) \rightarrow R$$

且

$$G(K) = \sum_{L \subseteq K} F(L) \quad (K \subseteq X_n)$$

考虑反解, 有:

$$F(K) = \sum_{L \subseteq K} (-1)^{|K|-|L|} G(L)$$

证明.

$$\begin{aligned} \sum_{L \subseteq K} (-1)^{|K|-|L|} G(L) &= \sum_{L \subseteq K} (-1)^{|K|-|L|} \sum_{T \subseteq L} F(T) \\ &= \sum_{T \subseteq K} F(T) \sum_{T \subseteq L \subseteq K} (-1)^{|K|-|L|} \\ &= F(K) \end{aligned}$$

□

这就是莫比乌斯反演.

因此我们可以对 F, G 下定义, 令 A_1, A_2, \dots, A_n 是有限集 S 的子集, 且 $K \subseteq X_n, F(K)$ 为恰好属于所有 A_i that $i \notin K$ 的元素个数, 即

$$F(K) = \left| \bigcap_{i \notin K} A_i - \bigcup_{i \in K} A_i \right|$$

显然有

$$F(X_n) = n - \left| \bigcup_{i \in X_n} A_i \right|$$

然后令

$$G(K) = \sum_{L \subseteq K} F(L) = \left| \bigcap_{i \notin K} A_i \right|$$

由莫比乌斯反演有

$$F(K) = \sum_{L \subseteq K} (-1)^{|K|-|L|} G(L)$$

有

$$|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = \sum_{J \subseteq K} (-1)^{|J|} \left| \bigcap_{i \in J} A_i \right|$$

等价于上面的容斥原理.

偏序集里的莫比乌斯反演

建议先看看代数系统. 下面将莫比乌斯反演推广到偏序集 (X, \leq) 里. 以下介绍的函数满足

$$f: X \times X \rightarrow \mathcal{R}$$

且 $f(x, y) = 0$ if $x \not\leq y$. 下面考察代数系统 $\langle \mathcal{F}, * \rangle$, 设其为 A

定义 1.5.7. 令 $h = f * g$ 为 f 和 g 的卷积, 如果满足:

$$h(x, y) = \begin{cases} \sum_{z: x \leq z \leq y} f(x, z)g(z, y) & , x \leq y \\ 0 & , other \end{cases}$$

显然卷积运算在该偏序集上是封闭的, 故这是一个广群. 并且显然其是满足结合律, 故其是一个半群.

定义 1.5.8. 科罗内尔 δ 函数:

$$\delta(x, y) = \begin{cases} 1 & , x = y \\ 0 & , other \end{cases}$$

显然有 $f * \delta = \delta * f = f$, 显然其为卷积运算的幺元. 故这个一个独异点.

定义 1.5.9. ζ 函数:

$$\zeta(x, y) = \begin{cases} 1 & , x \leq y \\ 0 & , other \end{cases}$$

定义 1.5.10. 逆函数:

对于 X 中所有的 y 满足 $f(y, y) \neq 0$, 有其逆元.

$$g(x, y) = \begin{cases} \frac{1}{f(y, y)}, & x = y \\ -\frac{1}{f(y, y)} \sum_{x \leq z < y} g(x, z) f(z, y), & x < y \\ 0, & other \end{cases}$$

证明. 若 $x \neq y$

$$\begin{aligned} (g * f)(x, y) &= g(x, y) f(y, y) + \sum_{x \leq z < y} g(x, z) f(z, y) \\ &= - \sum_{x \leq z < y} g(x, z) f(z, y) + \sum_{x \leq z < y} g(x, z) f(z, y) \\ &= 0 \end{aligned}$$

故 g 是其左逆元, 类似地可以证明其是右逆元. 故其是 f 的逆元. \square

定义 1.5.11. 莫比乌斯函数:

莫比乌斯函数为 ζ 函数的逆函数.

具体地:

$$\mu(x, y) = \begin{cases} 1 & , x = y \\ -\sum_{x \leq z < y} \mu(x, z) & , x < y \end{cases}$$

下面给出一些常见偏序集的莫比乌斯函数:

1. $(\mathcal{P}(X_n), \subseteq)$

$$\mu(A, B) = (-1)^{|B| - |A|}$$

2. (X_n, \leq) 即正整数集合上的全序关系

$$\mu(k, l) = \begin{cases} 1 & , l = k \\ -1 & , l = k + 1 \\ 0 & , other \end{cases}$$

3. $(X_n, |)$, 即正整数集合上的整除关系

有 $\mu(a, b) = \mu(1, \frac{b}{a})$

$$\mu(1, n) = \begin{cases} 1 & , n = 1 \\ (-1)^k & , n \text{ 是互不相同的素数乘积} \\ 0, & , other \end{cases}$$

4. 直积的莫比乌斯函数

线性有限偏序集 $(X, \leq_1), (Y, \leq_2)$, 且 μ_1, μ_2 分别为其莫比乌斯函数, 定义其笛卡尔积的偏序为

$$(x, y) \leq (x', y') \iff x \leq x' \text{ and } y \leq y'$$

那么新偏序集 $(X \times Y, \leq_3)$ 的莫比乌斯函数为

$$\mu((x, y), (x', y')) = \mu_1(x, x')\mu_2(y, y')$$

定理 1.5.12. 莫比乌斯反演:

设 (X, \leq) 是一个具有最小元的线性偏序集. 令 μ 是其莫比乌斯函数, 定义在 X 上的实值函数 $F, G: X \rightarrow \mathcal{R}$ 满足

$$G(x) = \sum_{z \leq x} F(z), \quad (x \in X)$$

那么有

$$F(x) = \sum_{y \leq x} \mu(y, x) G(y), \quad (x \in X)$$

证明.

$$\begin{aligned} \sum_{y \leq x} \mu(y, x) G(y) &= \sum_{y \leq x} \mu(y, x) \sum_{z \leq y} F(z) \\ &= \sum_{z \leq x} F(z) \sum_{z \leq y \leq x} \zeta(z, y) \mu(y, x) \\ &= \sum_{z \leq x} F(z) \delta(z, x) \\ &= F(x) \end{aligned}$$

□

这里最小元保证了和式有限, 因此不用判断敛散性.(这里对和式的一些变换在无穷和式有的有时不成立)

事实上, 莫比乌斯反演是卷积结合律的一个推论.

证明. 不妨设最小元为 0, 定义 $f, g \in \mathcal{F}(X)$

$$f(x, y) = \begin{cases} F(y) & , x = 0 \\ 0 & , other \end{cases}$$

$$g(x, y) = \begin{cases} G(y) & , x = 0 \\ 0 & , other \end{cases}$$

从而有 $g = f * \zeta$, 从而有 $g * \mu = f$,

□

1.5.4 莫比乌斯反演 II

定理 1.5.13. 存在最大元和最小元时。

$$\mu_{\leq}(x, y) = \mu_{\geq}(y, x)$$

1.6 递推关系和生成函数

一些斐波拉契数列的性质:

1.

$$\begin{pmatrix} F_n & F_{n+1} \end{pmatrix} = \begin{pmatrix} F_0 & F_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n$$

2. $F_{2k} = F_k(2F_{k+1} - F_k); F_{2k+1} = F_{k+1}^2 + F_k^2$

3.

$$\sum_{i=0}^n f_i = f_{n+2} - 1$$

4.

$$2|f_n \iff 3|n$$

1.6.1 生成函数

这里只做简单介绍

牛顿二项式定理

定理 1.6.1. 设 α 是一个实数. 对于任意 x, y with $0 \leq |x| < |y|$, 有性质

$$(x + y)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k y^{\alpha-k}$$

where

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}$$

设 $|z| < 1$, 特别地有

$$(1 + z)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} z^k$$

结论 1.6.2. 若 α 是一个负整数, 且 $\alpha = -n$ then

$$\begin{aligned}\binom{\alpha}{k} &= \binom{-n}{k} \\ &= \frac{-n(-n-1)\cdots(-n-k+1)}{k!} \\ &= (-1)^k \binom{n+k-1}{k}\end{aligned}$$

thus: for $|z| < 1$

$$(1+z)^{-n} = \frac{1}{(1+z)^n} = \sum_{k=0}^{\infty} (-1)^k \binom{n+k-1}{k} z^k$$

一般生成函数

无穷数列 h_0, h_1, \dots 的生成函数为 $g(x) = h_0 + h_1x + h_2x^2 + \dots$

生成函数的一些性质

设 H 为数列, F 为其对应的生成函数

1. $cH \rightarrow cF$
2. $H_1 + H_2 \rightarrow F_1 + F_2$
3. $0, 0, 0, \dots + H \rightarrow x^k F$
4. $iH(H_1, 2H_2, \dots) \rightarrow F'$
5. 令 $G_n = \sum_{i+j=n} H_{1i} \cdot H_{2j}$ 那么 $G \rightarrow F_1 \cdot F_2$

一面介绍两种重要的生成函数即: 多重集合的 n 组合级数的生成函数

根据泰勒级数

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$$

我们可以解 h_n 表示

$$e_1 + e_2 + \dots + e_k = n$$

的非负整数解的个数。

其生成函数为

$$g(x) = \sum_{n=0}^{\infty} \binom{n+k-1}{n} x^n = \frac{1}{(1-x)^k}$$

例 1.6.3. 设 $x_1 + x_2 + x_3 + x_4 = n$ 的整数解个数, 其中 x_1 是偶数, x_2 是 5 的倍数, $x_3 \leq 4, x_4 \leq 1$

解:

$$\begin{aligned} g(x) &= (1 + x^2 + x^4 + \cdots)(1 + x^5 + \cdots)(1 + x + x^2 + x^3 + x^4)(1 + x) \\ &= \frac{1}{1-x^2} \frac{1}{1-x^5} \frac{1-x^5}{1-x} (1+x) \\ &= \frac{1}{(1-x)^2} \\ &= \sum_{n=0}^{\infty} \binom{n+1}{n} x^n \end{aligned}$$

故为 $n+1$.

我们得到几个小结论:

1. 限制 $\geq k$, 可以乘 x^k
2. 限制 $\leq k$, 少写几项
3. 是 k 的倍数, 整体代换

指数生成函数

无穷数列 h_0, h_1, \cdots 的指数生成函数为 $g(x) = h_0 + h_1 \frac{x}{1!} + h_2 \frac{x^2}{2!} + \cdots$

下面给出一类常用的指数生成函数, 即多重集合的 n 排列数的生成函数.

定理 1.6.4. 设 S 是多重集合 $\{n_1 a_1 \cdots n_k a_k\}$, 其中 $n_i \geq 0$, 那么数列的指数生成函数为

$$g(x) = f_{n_1}(x) f_{n_2}(x) \cdots f_{n_k}(x)$$

其中

$$f_{n_i}(x) = \sum_{k=0}^{n_i} \frac{x^k}{k!}$$

例 1.6.5. 用红, 白, 蓝, 绿色给 $1 \times n$ 棋盘染色, 其中要求红色为偶数, 白色是奇数, 求方案数

解:

$$\begin{aligned} g(x) &= \left(\sum_{n=0}^{\infty} \frac{x^n}{n!} \right)^2 \left(1 + \frac{x^2}{2!} + \cdots \right) \left(x + \frac{x^3}{3!} + \cdots \right) \\ &= e^{2x} \left(\frac{e^x + e^{-x}}{2} \right) \left(\frac{e^x - e^{-x}}{2} \right) \\ &= \frac{e^{4x} - 1}{4} \\ &= \frac{1}{4} \sum_{n=0}^{\infty} 4^n \frac{x^n}{n!} - \frac{1}{4} \\ &= \sum_{n=1}^{\infty} 4^{n-1} \frac{x^n}{n!} \end{aligned}$$

故为 4^{n-1}

1. 对于偶数限制此项为

$$\frac{e^x - e^{-x}}{2}$$

2. 奇数限制

$$\frac{e^x + e^{-x}}{2}$$

对于求解线性齐次递推关系这里不做介绍

1.7 卡特兰数和第二类斯特林数

1.7.1 卡特兰数

折线图

只有两类线段 $(a,b)-(a+1,b+1)$ 或 $(a,b)-(a+1,b-1)$

结论 1.7.1. $A_0(a_0, b_0), A_n(a_n, b_n)$ 能用折线连接的充要条件是

$|b_n - b_0| \leq a_n - a_0 = n$ 且 $2 \mid (|b_n - b_0| + n)$

连接这两点的折线有

$$\binom{n}{\frac{n+b_n-b_0}{2}}$$

条.

卡特兰数:

$$C_n = \frac{1}{n+1} \binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n-1}$$

递推式

$$C_n = \sum_{k=1}^n C_{k-1} C_{n-k} = \frac{1}{n+1} (4n-2) C_{n-1}$$

Catalan 数列 C_n 可以应用于以下问题:

1.7.2 斯特林数

第二类斯特林数

$\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$: 表示将 n 个不同的球放到 k 个相同的盒子中的方案数, 且不能出现空盒。

有递推式:

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} + k \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\}$$

通项公式:

$$\left\{ \begin{matrix} n \\ m \end{matrix} \right\} = \frac{1}{m!} \sum_{i=0}^{m-1} (-1)^i \binom{n}{i} (m-i)^n$$

生成函数:

$$\sum_{i \geq k} \left\{ \begin{matrix} i \\ k \end{matrix} \right\} x^i = \frac{x^k}{\prod_{j=1}^k (1-jx)}$$

第一类斯特林数

$\left[\begin{matrix} n \\ k \end{matrix} \right]$: 表示 n 个不同的人坐 k 张圆桌的方案数。

有递推式:

$$\left[\begin{matrix} n \\ k \end{matrix} \right] = (n-1) \left[\begin{matrix} n-1 \\ k \end{matrix} \right] + \left[\begin{matrix} n-1 \\ k-1 \end{matrix} \right]$$

基本的斯特林恒等式

定义 1.7.2. 上升阶乘幂:

$$x^{\overline{n}} = \prod_{k=0}^{n-1} (x+k)$$

下降阶乘幂:

$$x^{\underline{n}} = \prod_{k=0}^{n-1} (x-k)$$

结论 1.7.3.

$$\binom{n}{k} \times k^{\underline{m}} = \binom{n-m}{k-m} \times n^{\underline{m}}$$

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = \left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = [n == 0]$$

$$\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)! [n > 0] \quad \left\{ \begin{matrix} n \\ 1 \end{matrix} \right\} = [n > 0]$$

$$\begin{bmatrix} n \\ 2 \end{bmatrix} = (n-1)! H_{n-1} [n > 0] \quad \left\{ \begin{matrix} n \\ 2 \end{matrix} \right\} = (2^{n-1} - 1) [n > 0]$$

$$\begin{bmatrix} n \\ n-1 \end{bmatrix} = \left\{ \begin{matrix} n \\ n-1 \end{matrix} \right\} = \binom{n}{2}$$

$$\begin{bmatrix} n \\ n \end{bmatrix} = \left\{ \begin{matrix} n \\ n \end{matrix} \right\} = \binom{n}{n}$$

结论 1.7.4.

$$x^{\bar{n}} = \sum_k \begin{bmatrix} n \\ k \end{bmatrix} x^k$$

结论 1.7.5.

$$x^n = \sum_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} (-1)^{n-k} x^{\bar{k}} = \sum_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} x^{\underline{k}}$$

结论 1.7.6.

$$x^{\underline{n}} = \sum_k \begin{bmatrix} n \\ k \end{bmatrix} (-1)^{n-k} x^k$$

结论 1.7.7. 多项式的下降阶乘幂表示:

$$f(x) = \sum_{i=0}^n b_i x^{\underline{i}}$$

要转化成点值表示 $(i, a_i), i = 0, 1, \dots, n$ 。只需：

$$a_k = \sum_{i=0}^n b_i k^i \iff \frac{a_k}{k!} = \sum_{i=0}^k b_i \frac{1}{(k-i)!}$$

1.7.3 球盒模型

有 n 个球， m 个盒子。

球是否相同，盒子是否相同，是否允许空盒子。

1. 不同，不同，空

$$m^n$$

2. 不同，不同，不空

$$m! \left\{ \begin{matrix} n \\ m \end{matrix} \right\}$$

3. 不同，同，空

$$\sum_{i=0}^m \left\{ \begin{matrix} n \\ i \end{matrix} \right\}$$

4. 不同，同，不空

$$\left\{ \begin{matrix} n \\ m \end{matrix} \right\}$$

5. 同，不同，空

$$\binom{n+m-1}{n}$$

6. 同，不同，不空，

$$\binom{n-1}{m-1}$$

7. 同，同，空

$$\frac{1}{(1-x)(1-x^2)\cdots(1-x^m)}$$

的 x^n 的系数。

8. 同, 同, 不空

$$\frac{x^m}{(1-x)(1-x^2)\cdots(1-x^m)}$$

的 x^n 的系数。

9. 把最多 m 个球放入 n 个不同的盒子里, 允许空的方案为

$$\binom{n+m}{m}$$

1.8 二项式反演

定理 1.8.1. 形式一:

$$G(x) = \sum_{i=0}^x \binom{x}{i} F(i) \iff F(x) = \sum_{i=0}^x (-1)^{x-i} \binom{x}{i} G(i)$$

形式二:

$$G(x) = \sum_{i=x}^n \binom{i}{x} F(i) \iff F(x) = \sum_{i=x}^m (-1)^{i-x} \binom{i}{x} G(i)$$

假设有 N 个限制, 两种形式的 $F(x)$ 都定义为, 恰好满足 x 个限制的结果, 这个东西往往比较难求, 对于 G , 我们分开定义。

形式一

$$G(X) = \sum_{J \subseteq X} F(J)$$

就是一个前缀和, 即最多满足 x 个条件的结果。

形式二

这并不是普通的后缀和，（如果是普通的后缀和可以用形式一变形。）

实际上这是加入了选出 x 个限制的过程，即是钦定 x 个限制后，其他随便选择。为什么要这么定义呢？用一个例子说明，

一个有 $*N*$ 个元素的集合有 2^N 个不同子集（包含空集），现在要在这 2^N 个集合中取出若干集合（至少一个），使得它们的交集的元素个数为 $*K*$ ，求取法的方案数。

这里一个自然的想法是计算选择 K 个元素，其他随便安排的方案数。然后就可以用二项式反演形式二了。如果去掉选择这一过程，直接算最多/最少满足 K 个限制的数量，是不好计算的。

1.8.1 高维二项式反演

定理 1.8.2. 设 $\mathbf{n} = (n_1, \dots, n_d)$ 和 $\mathbf{i} = (i_1, \dots, i_d)$ 且比较按坐标逐个比较 $\mathbf{i} \succeq \mathbf{n}$ 当且仅当每个 $i_k \geq n_k$ 。定义多维二项式系数为坐标乘积：

$$\binom{\mathbf{i}}{\mathbf{n}} = \prod_{k=1}^d \binom{i_k}{n_k}.$$

那么高维二项式变换与其逆变换为

$$G(\mathbf{n}) = \sum_{\mathbf{i} \succeq \mathbf{n}} \binom{\mathbf{i}}{\mathbf{n}} F(\mathbf{i}) \quad \Longleftrightarrow \quad F(\mathbf{n}) = \sum_{\mathbf{i} \succeq \mathbf{n}} (-1)^{|\mathbf{i}-\mathbf{n}|} \binom{\mathbf{i}}{\mathbf{n}} G(\mathbf{i}),$$

其中 $|\mathbf{i} - \mathbf{n}| = \sum_{k=1}^d (i_k - n_k)$ 。

第二章 数论

2.1 整除

结论 2.1.1. 令 a, b, c 为整数, 那么有:

$$\gcd(a + cb, b) = \gcd(a, b)$$

定义 2.1.2. $a, b, m, n \in \mathbb{Z}$, 称 $ma + nb$ 为 a, b 的线性组合

定理 2.1.3. 裴蜀定理:

如果 a, b 均为整数, 则有整数 m 和 n , 使得

$$ma + nb = \gcd(a, b)$$

其中该等式又被称为裴蜀等式, m, n 被称为裴蜀数.

可以用扩展欧几里得算法求出 $ma + nb = \gcd(a, b)$ 的特解, 然后有通解

$$\begin{cases} m = m_0 + k \frac{b}{\gcd(a, b)} \\ n = n_0 - k \frac{a}{\gcd(a, b)} \end{cases}$$

注意到

$$a(m + bu) + b(n - au) = \gcd(a, b)$$

故满足等式的 m, n 有无穷多对.

引理 2.1.4. 两个不全为 0 的整数 a, b 的最大公因数是其线性组合中最小的正整数.

证明. 不妨设 d 是 a, b 线性组合中最小的正整数. 考虑带余除法:

$$a = dq + r \text{ 从而有 } r = a - dq = a - q(ma + nb) = (1 - qm)a - qnb$$

因此 $d|a$, 同理 $d|b$, 故 d 为公因数.

不妨设 $e = \gcd(a, b)$, 那么 $d|e$, 又 $e|(ma + nb)$, 即 $e|d$

故 $e = d$ □

定理 2.1.5. 如果 a, b 是整数, 那么所有 a, b 的线性组合所构成的集合与所有 $\gcd(a, b)$ 的倍数所构成的集合相同. 换言之, 所有 a, b 的线性组合, 都是 $\gcd(a, b)$ 的倍数.

定理 2.1.6. 如果 a, b 是不全为 0 的整数, 那么正整数 d 是 a, b 的最大公因数, 当且仅当 1. $d|a, d|b$ 2. 若 $c|a, c|b$, 那么 $c|d$

定义 2.1.7. 令 a_1, a_2, \dots, a_n 为不全为 0 的整数, 如果 d 为他们公因子中最大的一个, 则称 d 为 a_1, a_2, \dots, a_n 的最大公因数. 记为 $\gcd(a_1, a_2, \dots, a_n) = d$

定理 2.1.8.

$$\gcd(a_1, a_2, \dots, a_n) = \gcd(a_1, a_2, \dots, \gcd(a_{k-1}, a_k), \dots, a_n)$$

定义 2.1.9. 我们称 a_1, a_2, \dots, a_n 互素如果 $\gcd(a_1, a_2, \dots, a_n) = 1$

定义 2.1.10. 我们称 a_1, a_2, \dots, a_n 两两互素, 如果任意两个数互素

定理 2.1.11. 若 $\gcd(a, m) = 1, \gcd(b, m) = 1$, 则 $\gcd(ab, m) = 1$

若 $\gcd(a, b) = 1$, 则 $\gcd(a^k, b^l) = 1$

定理 2.1.12. 设正整数 a, b 之积是一个整数的 $k(k \geq 2)$ 次幂. 若 $\gcd(a, b) = 1$. 则 a, b 都是整数的 k 次幂. 一般地: 设正整数 a_1, a_2, \dots, a_n 之积是一个正整数的 k 次幂. 若 a_1, a_2, \dots, a_n 两两互素, 则 a_1, a_2, \dots, a_n 都是整数的 k 次幂.

引理 2.1.13.

$$\gcd(a_1^k, a_2^k, \dots, a_n^k) = \gcd^k(a_1, a_2, \dots, a_n)$$

推论 2.1.14. 裴蜀定理可以推广到 n 个整数的情形: 设 a_1, a_2, \dots, a_n 是不全为零的整数, 则存在整数 x_1, x_2, \dots, x_n , 使得 $a_1x_1 + a_2x_2 + \dots + a_nx_n = \gcd(a_1, a_2, \dots, a_n)$ 。其逆定理也成立: 设 a_1, a_2, \dots, a_n 是不全为零的整数, $d > 0$ 是 a_1, a_2, \dots, a_n 的公因数, 若存在整数 x_1, x_2, \dots, x_n , 使得 $a_1x_1 + a_2x_2 + \dots + a_nx_n = d$, 则 $d = \gcd(a_1, a_2, \dots, a_n)$ 。

推论 2.1.15. 对自然数 a, b 和整数 n , a 与 b 互素, 考察不定方程: $ax + by = n$ 其中 x 和 y 为自然数。如果方程有解, 称 n 可以被 a, b 表示。记 $C = ab - a - b$ 。由 a 与 b 互素, C 必然为奇数。则有结论: 对任意的整数 n , n 与 $C - n$ 中有且仅有一个可以被表示。即: 可表示的数与不可表示的数在区间 $[0, C]$ 对称 (关于 C 的一半对称)。0 可被表示, C 不可被表示; 负数不可被表示, 大于 C 的数可被表示。

推论 2.1.16. 二元一次不定方程有非负整数解的条件

$a, b > 0$, 若 $ax + by = n, (a, b) = 1$, 则 $n > ab - a - b$ 时有解, 解的个数为 $\left\lfloor \frac{n}{ab} \right\rfloor \left\lfloor \frac{n}{ab} \right\rfloor + 1$

结论 2.1.17.

$$\gcd(a_1, a_2, \dots, a_n) = \gcd(a_1, a_2 - a_1, \dots, a_n - a_{n-1})$$

一些小结论

1. 在 $[1, 18]$ 的范围下, 一个数最多与连续 7 个数不互质.
2. 一个数能被 4 整除, 当且仅当末尾两位能被 4 整除

3. 一个数能被 25 整除, 当且仅当末尾两位能被 25 整除
4. 一个数能被 8 整除, 当且仅当末尾三位能被 8 整除
5. 一个数能被 125 整除, 当且仅当末尾三位能被 125 整除
6. 一个数能被 3 整除, 当且仅当各位数之和能被 3 整除
7. 一个数能被 9 整除, 当且仅当各位数之和能被 9 整除
8. 能被 7 整除的数的特征: a. 抹去个位数 b. 减去原个位数的 2 倍 c. 其差能被 7 整除。
9. 能被 11 整除的数的特征: a. 抹去个位数 b. 减去原个位数 c. 其差能被 11 整除。或: 奇数位上的数字和与偶数位上的数和相减, 其差能被 11 整除

2.2 同余

以下所有参数未特殊说明, 均为默认整数, 模数默认正整数

2.2.1 同余

定义 2.2.1. 设 m 是正整数, 若 $m|(a-b)$, 则称 a 和 b 模 m 同余. 记作 $a \equiv b \pmod{m}$

性质

1. $a \equiv b \pmod{m} \iff \exists k(k \in \mathbb{Z}), a = b + kz$
2. $a \equiv a \pmod{m}$
3. $a \equiv b \pmod{m} \rightarrow b \equiv a \pmod{m}$
4. $a \equiv b \pmod{m}, b \equiv c \pmod{m} \rightarrow a \equiv c \pmod{m}$
5. $a \equiv b \pmod{m}, c \equiv d \pmod{m} \rightarrow a + c \equiv b + d \pmod{m}, a - c \equiv b - d \pmod{m}, ac \equiv bd \pmod{m}$
6. $a^n \equiv b^n \pmod{m}$
7. $ac \equiv bc \pmod{m}, d = \gcd(c, m) \rightarrow a \equiv b \pmod{m/d}$

$$8. a \equiv b \pmod{m}, n|m \rightarrow a \equiv b \pmod{n}$$

$$9. a \equiv b \pmod{m}, a \equiv b \pmod{n} \rightarrow a \equiv b \pmod{\text{lcm}(m, n)}$$

定义 2.2.2. 设模为 n , 则根据余数可将所有的整数分为 n 类, 把所有与整数 a 模 n 同余的整数构成的集合叫做模 n 的一个剩余类, 记作 $[a]$. 并把 a 叫作剩余类 $[a]$ 的一个代表元。

定义 2.2.3. 从模 n 的每个剩余类中各取一个数, 得到一个由 n 数组成的集合, 叫做模 n 的一个完全剩余系。

结论 2.2.4. 若 r_1, r_2, \dots, r_m 是模 m 的一个完全剩余系, 且正整数 a 满足 $\gcd(a, m) = 1$, 则对任何整数 $b, ar_i + b$ 也为一个完全剩余类。

证明. 若不然, 则存在 $ar_i + b \equiv ar_j + b \pmod{m} \iff ar_i \equiv ar_j \pmod{m} \iff m|a(r_i - r_j) \iff m|a_i - a_j \iff r_i \equiv r_j \pmod{m}$ 与条件矛盾. 故得证 \square

结论 2.2.5. a_1, a_2, \dots, a_m 是模 m 的一个完全剩余系, b_1, b_2, \dots, b_n 是模 n 的一个完全剩余系, 且 $\gcd(n, m) = 1$ 那么 $na_i + mb_j$ 是模 mn 的一个完全剩余系

证明. 首先由乘法原理知道有 mn 个数, 那么只需证两两不同余即可

若不然则对于 $(a, b) \neq (a', b')$ $na + mb \equiv na' + mb' \pmod{mn} \iff mn|n(a - a') + m(b - b') \iff m|(a - a'), n|(b - b') \iff a \equiv a' \pmod{m}, b \equiv b' \pmod{n}$ 与条件矛盾. 故得证. \square

定义 2.2.6. 简化剩余系也称既约剩余系或缩系, 是 m 的完全剩余系中与 m 互素的数构成的子集, 如果模 m 的一个剩余类里所有数都与 m 互素, 就把它叫做与模 m 互素的剩余类. 在与模 m 互素的全体剩余类中, 从每一个类中各任取一个数作为代表组成的集合, 叫做模 m 的一个简化剩余系。

结论 2.2.7. 若 r_1, r_2, \dots, r_m 是模 m 的一个缩系, 且正整数 a 满足 $\gcd(a, m) = 1$, 则 ar_i 也为一个缩系.

证明. 由完系性质 1 可知其两两不同余, 故只需证明其与均 m 互质即可. 因为 $\gcd(r_i, m) = 1, \gcd(a, m) = 1 \Rightarrow \gcd(ar_i, m) = 1$ 得证 \square

结论 2.2.8. a_1, a_2, \dots, a_m 是模 m 的一个缩系, b_1, b_2, \dots, b_n 是模 n 的一个缩系, 且 $\gcd(n, m) = 1$ 那么 $na_i + mb_j$ 是模 mn 的一个缩系

证明. 只需证明其是所有与 mn 互质的剩余类.

$$\begin{aligned} \gcd(a_i, m) = 1, \gcd(b_j, n) = 1, \gcd(n, m) = 1 \\ \Rightarrow \gcd(na_i, m) = 1, \gcd(mb_j, n) = 1 \\ \Rightarrow \gcd(na_i + mb_j, n) = 1, \gcd(na_i + mb_j, m) = 1 \\ \Rightarrow \gcd(na_i + mb_j, mn) = 1 \end{aligned}$$

若将 a_i, b_j 扩展成完系, 若 $\gcd(na_i + mb_j, mn) = 1 \Rightarrow \gcd(na_i + mb_j, m) = 1, \gcd(na_i + mb_j, n) = 1 \Rightarrow \dots$ 逆着证回去即可. \square

2.2.2 线性同余方程

定义 2.2.9. 形如 $ax \equiv b \pmod{m}$ 的同余式称为一元线性同余方程

定理 2.2.10. $\gcd(a, m) = d, d \nmid b$, 则无解, 否则恰好有 d 个模 m 不同余的解.

证明. 若 $d \nmid b$, 则 $ax \equiv b \pmod{m} \iff ax - ym = b$, 根据贝祖定理显然无解.

若 $d \mid b$, 则显然有无穷多组解, 我们设其中一组特解为 x_0, y_0

其通解为 $x = x_0 + (m/d)t, y = y_0 + (a/d)t$

设 $x_1 = x_0 + (m/d)t_1, x_2 = x_0 + (m/d)t_2$

$x_1 \equiv x_2 \pmod{m} \iff t_1 \equiv t_2 \pmod{d}$

所以有 d 个不同于的解. \square

定义 2.2.11. $\gcd(a, m) = 1, ax \equiv 1 \pmod{m}$ 则称该同余方程的一个解为 a 模 m 的逆, 记为 a^{-1} . 显然 $\gcd(a^{-1}, m) = 1$

定理 2.2.12. 设 p 为素数, 正整数 $a = a^{-1}$, 当且仅当 $a \equiv \pm 1 \pmod{p}$.

证明. $a \equiv \pm 1 \pmod{p} \iff a^2 \equiv 1 \pmod{p}$ 反过来. 有

$$a^2 \equiv 1 \pmod{p} \Rightarrow p | (a^2 - 1) \Rightarrow p | (a + 1) p | (a - 1) \Rightarrow a \equiv \pm 1 \pmod{p} \quad \square$$

定理 2.2.13. 威尔逊定理

若 p 是素数, 则 $(p - 1)! \equiv -1 \pmod{p}$

证明. $p = 2$ 显然成立.

否则对于 $1 \leq a \leq p - 1$, 可以找到其逆元与之配对, 且除 1 和 $p - 1$ 都能两两配对.

$$\text{故 } (p - 1)! \equiv p - 1 \equiv -1 \pmod{p} \quad \square$$

定理 2.2.14. 威尔逊定理逆定理

若 $n \geq 2$ 是正整数, 且 $(n - 1)! \equiv -1 \pmod{n}$ 则 n 为质数

证明. 若不然, 设 n 为合数, 则其必存在小于 n 的素因子 p

所以有 $(n - 1)! \equiv -1 \pmod{n}, p | n \Rightarrow (n - 1)! \equiv -1 \pmod{p}$,

但是 $(n - 1)! \equiv 0 \pmod{p}$

而 $n > 1$ 矛盾. 故得证. \square

定理 2.2.15. 费马小定理

如果 p 是一个素数, a 是正整数且 a 不是 p 的倍数, 则 $a^{p-1} \equiv 1 \pmod{p}$.

证明. 因为 $\gcd(a, p) = 1$

所以 $\prod_{i=1}^{p-1} ia \equiv \prod_{i=1}^{p-1} i \pmod{p} \Rightarrow a^{p-1} \equiv 1 \pmod{p}$ 得证. \square

定义 2.2.16. 欧拉函数

对于正整数 n , 小于等于 n 且与 n 互质的正整数的个数, 称为欧拉函数, 记作 $\phi(n)$

定理 2.2.17. 设 m 是一个正整数, a 是一个正整数且 $\gcd(a, m) = 1$, $a^{\phi(m)} \equiv 1 \pmod{m}$

证明. 设 $r_1, r_2, \dots, r_{\phi(m)}$, 是不超过 m 的模 m 的一个缩系.

那么 $ar_1, ar_2, \dots, ar_{\phi(m)}$ 也是一个缩系

故 $ar_1 ar_2 \dots ar_n \equiv r_1 r_2 \dots r_n \pmod{m} \iff a^{\phi(m)} \equiv 1 \pmod{m}$

得证. □

定义 2.2.18. 同余方程组是指一组形如下面的方程的集合:

$$\begin{cases} a_1 \equiv b_1 \pmod{m_1} \\ a_2 \equiv b_2 \pmod{m_2} \\ \vdots \\ a_n \equiv b_n \pmod{m_n} \end{cases}$$

其中, a_i 和 b_i 是整数, m_i 是正整数。这组方程要求对于每个 i , a_i 除以 m_i 的余数等于 b_i 除以 m_i 的余数, 即 a_i 与 b_i 在模 m_i 下同余。解同余方程组就是要找到满足所有这些条件的整数解。

例 2.2.19.

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

我们可以使用迭代法 (逐级满足法) 解决. 由第一个式子得 $x = 3t + 1$ 然后带入 $3t + 1 \equiv 2 \pmod{5} \iff t \equiv 4 \pmod{5}$ 以此类推. 但是这只能解决一些简单的问题, 下面我们给出一般地解法.

定理 2.2.20. 中国剩余定理 (CRT)

设 m_1, m_2, \dots, m_r 是两两互素的正整数, 则同余方程

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

有模 $m_1 m_2 \dots m_r$ 的唯一解

$$x = \sum_{i=1}^r a_i M_i M_i^{-1}$$

其中

$$M_i = \frac{1}{m_i} \prod_{j=1}^r m_j, \quad M_i M_i^{-1} \equiv 1 \pmod{m_i}$$

证明. 先证明 x 是方程组的解.

对于任意一个方程有,

$$x \equiv a_k M_k M_k^{-1} \equiv a_k \pmod{m_k}, \text{ 显然成立.}$$

下证唯一性.

若 x_1, x_2 为方程组的 2 个解, 则有 $x_1 \equiv x_2 \pmod{m_k} \iff m_k | (x_1 - x_2) \iff M | (x_1 - x_2) \iff x_1 \equiv x_2 \pmod{M}$ □

定理 2.2.21. 拉格朗日定理

p 为素数, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ($p \nmid a_n$) 是模 p 意义下的整系数多项式方程, 则同余方程 $f(x) \equiv 0 \pmod{p}$ 在模 p 意义下至多有 n 个不同的解.

推论 2.2.22. 若超过 n 个解, 则 $p \mid a_i$ ($i = 0, 1, \dots, n$), 即 $f(x)$ 是模 p 意义下的零多项式

推论 2.2.23. 若 $n \leq p$ 则同余式 $f(x) = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \equiv 0 \pmod{p}$ 有 n 个解的充要条件是 $x^p - x$ 除以 $f(x)$ 所得的余式的一切系数都是 p 的倍数

这里介绍一个比较重要的多项式, 常用于构造

$$f(x) = \prod_{i=1}^{p-1} (x - i) - (x^{p-1} - 1)$$

定理 2.2.24. *wolstenholme* 定理

若 p 为大于 3 的素数, 则

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}$$

2.3 乘性函数

定义 2.3.1. 算术函数

定义在所有正整数上的函数称为算数函数.

定义 2.3.2. 乘性函数

若 $\gcd(m, n) = 1$, 均有 $f(mn) = f(m)f(n)$, 则称 f 为乘性函数.

结论 2.3.3. 若 f 为乘性函数, $n = \prod_{i=1}^k p_i^{a_i}$ 为一个素因数分解. 则 $f(n) = \prod_{i=1}^k f(p_i^{a_i})$ 由定义显然成立.

定义 2.3.4. 和函数

f 为一个算术函数, $F(n) = \sum_{d|n} f(d)$ 称为 f 的和函数

定义 2.3.5. 欧拉函数

$\phi(n) = \sum_{i=1}^n [\gcd(i, n) = 1]$, 称为欧拉函数.

结论 2.3.6. 设 p 是素数, $\phi(p^a) = p^a - p^{a-1}$

证明. 由定义, $\phi(p^a) = \sum_{i=1}^{p^a} [\gcd(i, p^a) = 1] = \sum_{i=1}^{p^a} 1 - [\gcd(i, p^a) \neq 1] = p^a - \sum_{i=1}^{p^a} [\gcd(i, p^a) \neq 1]$, 这样的 i 显然只有 p 的倍数, 有 p^{a-1} 个, 证毕. \square

结论 2.3.7. 欧拉函数是乘性函数

证明. 若 $\gcd(m, n) = 1$ 由缩系的定义知道, 显然模 m 的缩系有 $\phi(m)$ 个数, 模 n 的缩系有 $\phi(n)$ 个数, 由缩系的一个性质知模 mn 的缩系有 $\phi(m)\phi(n)$ 个数. 故 $\phi(mn) = \phi(m)\phi(n)$ \square

结论 2.3.8. $n > 2, \phi(n)$ 为偶数

结论 2.3.9.

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

证明. 容斥原理可证明这里用乘性函数的性质证明

$$\begin{aligned} \phi(n) &= \prod_{i=1}^k \phi(p_i^{a_i}) \\ &= \prod_{i=1}^k (p_i^{a_i} - p_i^{a_i-1}) \\ &= \prod_{i=1}^k p_i^{a_i} \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) \\ &= n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) \end{aligned}$$

\square

结论 2.3.10. 欧拉函数的和函数

$$F(n) = \sum_{d|n} \phi(d) = n$$

结论 2.3.11. 定义 C_d 为 1 到 n 中与 n 最大公因数为 d 的集合容易证明其是 1 到 n 构成的正整数集合的一个划分. 而 C_d 中有 $\phi(n/d)$ 个元素, (若 $a \in C_d$ 则 $\gcd(a/d, n/d) = 1$), 故 $n = \sum_{d|n} C_d = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$ 得证.

定义 2.3.12. 狄利克雷卷积

f, g 为算数函数, 定义狄利克雷积为

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

实际上这整数上一章的卷积在整除关系上的定义

性质

1. $f * g = g * f$
2. $(f * g) * h = f * (g * h)$
3. $f * (g + h) = f * g + f * h$

这里的算数函数就是 $f(1, x) \in \mathcal{F}$

故有逆元的条件是 $f(1) \neq 0$

定理 2.3.13. 如果 f, g 是乘性函数, 则 $f * g$ 也是乘性函数

定理 2.3.14. 若 $F = f * g, h$ 是 g 的逆函数, 那么 $f = F * h$

定理 2.3.15. 乘性函数的和函数也是乘性函数

定义 2.3.16. 因子和与因子个数函数

$$\sigma(n) = \sum_{d|n} d$$

$$\tau(n) = \sum_{d|n} 1$$

结论 2.3.17. 因子和与因子个数函数均为乘性函数

结论 2.3.18. 设 $n = \prod_{i=1}^k p_i^{a_i}$

$$\sigma(n) = \prod_{j=1}^k \frac{p_j^{a_j+1} - 1}{p_j - 1}$$

$$\tau(n) = \prod_{j=1}^k (a_j + 1)$$

定义 2.3.19. 莫比乌斯函数

$$\mu(n) = \begin{cases} 1, & (n = 1) \\ (-1)^r, & (n = \prod_{i=1}^r p_i) \\ 0, & (other) \end{cases}$$

定理 2.3.20. $f = F * \mu$

第三章 求和

一些记号

调和数 (harmonic number)

$$H_n = \sum_{k=1}^n \frac{1}{k}$$

基本公式

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

$$a^n - b^n = (a-b) \sum_{1 \leq k \leq n} a^{n-k} b^{k-1}$$

3.1 递归问题 RECURRENT PROBLEMS

3.1.1 repertoire method

例

$$f(1) = \alpha$$

$$f(2n) = 2f(n) + \beta$$

$$f(2n+1) = 2f(n) + \gamma$$

知

$$f(n) = A(n)\alpha + B(n)\beta + C(n)\gamma$$

通过对 $f(n)$ 赋值或 (α, β, γ) 赋值, 求解。

在参数较少的情况下, 可以将一些相同参数, 分别设为独立参数, 更容易找到有解的情况。

3.1.2 约瑟夫问题

形如

$$\begin{aligned} f(j) &= \alpha_j, & 1 \leq j < d \\ f(dn + j) &= cf(n) + \beta_j, & 0 \leq j < d, n \geq 1 \end{aligned}$$

有

$$f((b_m b_{m-1} \dots b_0)_d) = (\alpha_{b_m} \beta_{b_{m-1}} \dots \beta_{b_0})_c$$

3.2 和式 SUMS

用

$$\sum_{P(k)} a_k$$

表示。

3.2.1 和式和递归式 SUMS AND RECURRENCES

和式可以表示为递归形式:

$$\begin{aligned} S_0 &= a_0 \\ S_{n+1} &= S_n + a_{n+1} \end{aligned}$$

用 repertoire method 解。

例 3.2.1. 计算

$$\sum_{k=0}^n (a + bn)$$

写成递归式

$$S_0 = \alpha$$

$$S_n = S_{n-1} + \beta n + \gamma$$

其中

$$\alpha = \gamma = a, \beta = b$$

设

$$S_n = A(n)\alpha + B(n)\beta + C(n)\gamma$$

带入 $1, n, n^2$

解出

$$\begin{cases} A(n) = 1 \\ B(n) = \frac{n(n+1)}{2} \\ C(n) = n \end{cases}$$

故

$$S_n = a + na + \frac{n(n+1)}{2}b$$

递归式可以转化为和式

对于形如

$$a_n T_n = b_n T_{n-1} + c_n$$

的递归式，可以设求和因子 (summation factor)

$$s_n = \frac{\prod_{i=1}^n a_i}{\prod_{i=1}^n b_i} \cdot \frac{b_1}{a_n}$$

然后同时乘上求和因子即可得出

$$T_n = \frac{1}{s_n a_n} \left(s_1 b_1 T_0 + \sum_{k=1}^n c_k s_k \right)$$

注意：求和因子不能为 0

3.2.2 和式的处理 MANIPULATION OF SUMS

和式的变换

$$\begin{aligned} \sum_{k \in K} c a_k &= c \sum_{k \in K} a_k \\ \sum_{k \in K} (a_k + b_k) &= \sum_{k \in K} a_k + \sum_{k \in K} b_k \\ \sum_{k \in K} a_k &= \sum_{p(k) \in K} a_{p(k)} \\ \sum_{k \in K} a_k + \sum_{k \in K'} a_k &= \sum_{k \in K \cap K'} a_k + \sum_{k \in K \cup K'} a_k \end{aligned}$$

其中对于 $n \in K$ ，有且仅有一个整数满足 $p(k) = n$

3.2.3 扰动法 (perturbation method)

对一个和式记其为 S_n ，将其第一项和最后一项分离出来，用两种方法改写 S_{n+1} 。

类似于算两次法

例 3.2.2. 如求和式

$$S_n = \sum_{0 \leq k \leq n} k 2^k$$

有

$$\begin{aligned} S_n + (n+1)2^{n+1} &= S_{n+1} \\ &= \sum_{0 \leq k \leq n} (k+1)2^{k+1} \\ &= 2S_n + \sum_{0 \leq k \leq n} 2^{k+1} \end{aligned}$$

有

$$\begin{aligned} S_n &= (n+1)2^{n+1} - \sum_{0 \leq k \leq n} 2^{k+1} \\ &= (n+1)2^{n+1} - \frac{2(1-2^{n+1})}{1-2} \\ &= (n-1)2^{n+1} + 2 \end{aligned}$$

3.2.4 多重和式 MULTIPLE SUMS

基本性质

$$\sum_j \sum_k a_{j,k} [P(j, k)] = \sum_{P(j,k)} a_{j,k} = \sum_k \sum_j a_{j,k} [P(j, k)]$$

$$\sum_{j \in J} \sum_{k \in K(j)} a_{j,k} = \sum_{k \in K'} \sum_{j \in J'(k)} a_{j,k}$$

$$\sum_{j \in J} a_{f(j)} = \sum_{j \in J, k \in K} a_k [f(j) = k] = \sum_{k \in K} a_k \sum_{j \in J} [f(j) = k]$$

其中 $f: J \rightarrow K$

例 3.2.3. 求

$$S_n = \sum_{1 \leq j < k \leq n} \frac{1}{k-j}$$

有

$$\begin{aligned} S_n &= \sum_{1 \leq k \leq n} \sum_{1 \leq j < k} \frac{1}{k-j} \\ &= \sum_{1 \leq k \leq n} \sum_{0 < j \leq k-1} \frac{1}{j} \\ &= \sum_{1 \leq k \leq n} H_{k-1} \end{aligned}$$

不太好做，（可以交换求和次序解）

考虑直接把 $k-j$ 当成一个整体。

$$\begin{aligned} S_n &= \sum_{1 \leq j < k+j \leq n} \frac{1}{k} \\ &= \sum_{1 \leq k \leq n} \sum_{1 \leq j \leq n-k} \frac{1}{k} \\ &= \sum_{1 \leq k \leq n} \frac{n-k}{k} \\ &= nH_n - n \end{aligned}$$

有

$$\sum_{0 \leq k < n} H_k = nH_n - n$$

思考：

对含 $k+f(j)$ 的二重和式，可以考虑用 $k-f(j)$ 替换 k ，并先对 j 求和比较好。

几何观点：按对角线求和。

3.2.5 一般性的方法 GENERAL METHODS

以

$$S_n = \sum_{0 \leq k \leq n} k^2$$

为例

归纳法

如果注意到

$$S_n = \frac{n(n + \frac{1}{2})(n + 1)}{3}$$

就可以使用数学归纳法

扰动法

观察

$$\begin{aligned} \sum_{0 \leq k \leq n} k^2 + (n + 1)^2 &= S_{n+1} \\ &= \sum_{1 \leq k \leq n+1} k^2 \\ &= \sum_{0 \leq k \leq n} (k + 1)^2 \\ &= \sum_{0 \leq k \leq n} k^2 + 2 \sum_{0 \leq k \leq n} k + n + 1 \end{aligned}$$

虽然没有成功，但注意到我们，成功地解出了

$$\sum_{0 \leq k \leq n} k$$

考虑对

$$T_n = \sum_{0 \leq k \leq n} k^3$$

操作, 有

$$\begin{aligned}
 T_n + (n+1)^3 &= T_{n+1} \\
 &= \sum_{1 \leq k \leq n+1} k^3 \\
 &= \sum_{0 \leq k \leq n} (k+1)^3 \\
 &= T_n + 3S_n + 3 \sum_{0 \leq k \leq n} k + n + 1
 \end{aligned}$$

得到

$$\begin{aligned}
 3S_n &= (n+1)^3 - 3 \frac{n(n+1)}{2} - (n+1) \\
 &= (n+1) \left(n^2 + \frac{1}{2}n \right) \\
 &= n \left(n + \frac{1}{2} \right) (n+1)
 \end{aligned}$$

成套方法

有

$$R_0 = d$$

$$R_n = R_{n-1} + an^2 + bn + c$$

其解的一般形式为

$$R_n = aA(n) + bB(n) + cC(n) + dD(n)$$

设 $R_n = 1, n, n^2, n^3$

解得

$$\begin{cases} A(n) = \frac{n(n+\frac{1}{2})(n+1)}{3} \\ B(n) = \frac{1}{2}(n^2 + n) \\ C(n) = n \\ D(n) = 1 \end{cases}$$

故

$$R_n = A(n)$$

事实上对 (a,b,c,d) 赋值更简单。

微积分法

求

$$\begin{aligned} S_n - \int_0^n x^2 dx &= \sum_{1 \leq k \leq n} \left(k^2 - \int_{k-1}^k x^2 dx \right) \\ &= \sum_{1 \leq k \leq n} \left(k - \frac{1}{3} \right) \\ &= \frac{n(n+1)}{2} + \frac{n}{3} \end{aligned}$$

展开和收缩

转化为二重和式，以简化通项。

$$\begin{aligned} S_n &= \sum_{1 \leq k \leq n} k^2 \\ &= \sum_{1 \leq k \leq n} k \sum_{1 \leq j \leq k} 1 \\ &= \sum_{1 \leq j \leq n} \sum_{j \leq k \leq n} k \\ &= \sum_{1 \leq j \leq n} \frac{(j+n)(n-j+1)}{2} \\ &= \frac{n^3 + n^2}{2} + \frac{1}{2} \frac{n(n+1)}{2} - \frac{1}{2} S_n \end{aligned}$$

有限微积分

有 $k^2 = k^2 + k^1$

故

$$\begin{aligned}
 \sum_{0 \leq k \leq n} k^2 &= \sum_{0 \leq k < n+1} k^2 + k^1 \\
 &= \left(\frac{k^3}{3} + \frac{k^2}{2} \right) \Big|_0^{n+1} \\
 &= \left(\frac{(n+1)^3}{3} + \frac{(n+1)^2}{2} \right) \\
 &= \frac{(n+1)(n+\frac{1}{2})n}{3}.
 \end{aligned}$$

3.2.6 有限微积分

类似微分算子 D

$$Df(x) = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}$$

定义差分算子 Δ

$$\Delta f(x) = f(x+1) - f(x)$$

定义下降阶乘幂 (falling factorial power)

$$x^{\underline{m}} = x(x-1) \cdots (x-m+1) \quad (m \geq 0 \in \mathbb{Z})$$

和上升阶乘幂 (rising factorial power)

$$x^{\overline{m}} = x(x+1) \cdots (x+m-1) \quad (m \geq 0 \in \mathbb{Z})$$

注意到: $n! = n^{\underline{n}} = 1^{\overline{n}}$

有

$$\Delta(x^{\underline{m}}) = mx^{\underline{m-1}}$$

类比积分, 我们定义不定和式 (indefinite sum)

$$\sum g(x) \delta x$$

满足

$$g(x) = \Delta f(x) \iff \sum g(x) \delta x = f(x) + C$$

其中 C 为满足 $p(x+1) = p(x)$ 的任意一个函数 $p(x)$ 。

有限微积分有确定的和式 (sum)

$$\sum_a^b g(x) \delta x = f(x) \Big|_a^b = f(b) - f(a)$$

有以下性质

$$\begin{aligned} \sum_a^b g(x) \delta x &= \sum_{a \leq k < b} g(x) \quad a \leq b \\ \sum_a^b g(x) \delta x &= - \sum_b^a g(x) \delta x \\ \sum_a^b + \sum_b^c &= \sum_a^c \end{aligned}$$

并且阶乘幂满足二项式定理

负指数的下降阶乘幂定义如下

$$x^{\overline{-m}} = \frac{1}{(x+1)(x+2)\cdots(x+m)} \quad m > 0$$

从而有以下性质

$$x^{\overline{m+n}} = x^{\overline{m}}(x-m)^{\overline{n}}$$

$$\sum_a^b x^{\overline{m}} \delta x = \frac{x^{\overline{m+1}}}{m+1} \Big|_a^b, \quad (m \neq -1)$$

若 $m = -1$ 则为 $H_b - H_a$

$f = \sum g$	$\Delta f = g$	$f = \sum g$	$\Delta f = g$
$x^0 = 1$	0	2^x	2^x
$x^1 = x$	1	c^x	$(c-1)c^x$
$x^2 = x(x-1)$	$2x$	$\frac{c^x}{c-1}$	c^x
x^m	mx^{m-1}	cu	$c\Delta u$
$\frac{x^{m+1}}{m+1}$	x^m	$u+v$	$\Delta u + \Delta v$
H_x	$x^{-1} = \frac{1}{x+1}$	uv	$u\Delta v + Ev\Delta u$

分部求和 (summation by parts)

有

$$\Delta(u(x)v(x)) = u(x)\Delta v(x) + Ev(x)\Delta u(x)$$

其中, **E** 为移位算子 (shift operator) $Ef(x) = f(x+1)$

简记为

$$\Delta(uv) = u\Delta v + Ev\Delta u$$

从而有

$$\sum u\Delta v = uv - \sum Ev\Delta u$$

如

例 3.2.4.

$$\begin{aligned}
 \sum_{k=0}^n k2^k &= \sum_0^{n+1} x2^x \delta x \\
 &= \sum_0^{n+1} x\delta 2^x \\
 &= (n+1)2^{n+1} - \sum_0^{n+1} 2^{x+1} \delta x \\
 &= (n+1)2^{n+1} - 2^{n+2} + 2 \\
 &= (n-1)2^{n+1} + 2
 \end{aligned}$$

例 3.2.5.

$$\begin{aligned}
 \sum_{0 \leq k < n} k H_k &= \sum_0^n x H_x \delta x \\
 &= \frac{1}{2} \left(\sum_0^n H_x \delta x^2 \right) \\
 &= \frac{1}{2} \left(x^2 H_n - \sum_0^n x \delta x \right) \\
 &= \frac{1}{2} \left(x^2 H_n - \frac{n^2}{2} \right) \\
 &= \frac{n^2}{2} \left(H_n - \frac{1}{2} \right)
 \end{aligned}$$

3.2.7 无限和式 INFINITE SUMS

容易发现

$$\sum_{k \geq 0} x^k = \begin{cases} \frac{1}{1-x}, & 0 \leq x < 1 \\ \infty, & x \geq 1 \end{cases}$$

交错和

$$\sum_{k \in K} a_k = \sum_{k \in K} a_k^+ - \sum_{k \in K} a_k^-$$

设 $A^+ = \sum_{k \in K} a_k^+$, 类似定义 A^-

- 若均有限的值, 则称为绝对收敛。
- 若 $A^+ = \infty$, 而后者为有限的值, 则称发散于 $+\infty$, 反之发散于 $-\infty$
- 否则不做定义。

只要我们处理的是刚才所定义的绝对收敛的和式, 这一章里的所有操作都完全成立.

对复数分实部和虚部计算即可。

第四章 概率论

4.1 基本概念和公式

对概率运算规定一些简单的基本法则：

1. 设 A 是随机事件，则 $0 \leq P(A) \leq 1$,
2. 设 Ω 为必然事件，则 $P(\Omega) = 1$,
3. 若事件 A 和 B 不相容，则 $P(A \cup B) = P(A) + P(B)$,

可推广至无穷：

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

4. 一般情况下， $P(A \cup B) = P(A) + P(B) - P(AB)$ ， $P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(AB) - P(AC) - P(BC) + P(ABC)$
5. $P(\bar{A}) = 1 - P(A)$
6. $P(A - B) = P(A) - P(AB)$

定理 4.1.1. 全概率公式

设 B_1, B_2, \dots, B_n 是样本空间 Ω 中的两两不相容的一组事件，即 $B_i B_j = \phi$, $i \neq j$ ，且满足 $\bigcup_{i=1}^n B_i = \Omega$ ，则称 B_1, B_2, \dots, B_n 是样本空间 Ω 的一个分割（又称为完备事件群，英文为 *partition*）。设 $\{B_1, B_2, \dots, B_n\}$ 是样本空间 Ω

的一个分割, A 为 Ω 的一个事件, 则

$$P(A) = \sum_{i=1}^n P(A|B_i)P(B_i)$$

定理 4.1.2. 贝叶斯公式

设 $\{B_1, B_2, \dots, B_n\}$ 是样本空间的一个分割, A 为 Ω 中的一个事件, $P(B_i) > 0$, $i = 1, 2, \dots, n$, $P(A) > 0$, 则

$$P(B_i|A) = \frac{P(A|B_i)P(B_i)}{\sum_{j=1}^n P(A|B_j)P(B_j)}$$

用于因果转换.

定义 4.1.3. 事件的独立性

设 A, B 是随机试验中的两个事件, 若满足 $P(AB) = P(A)P(B)$, 则称事件 A 和 B 相互独立。

判断事件的独立, 应该是从实际出发, 如果能够判断事件 B 的发生与否对事件 A 的发生与否不产生影响, 则事件 A, B 即为独立。

设 \tilde{A} 表示事件 A 发生和不发生之一, \tilde{B} 表示事件 B 发生和不发生之一。有独立性的定义可推至 $P(\tilde{A}\tilde{B}) = P(\tilde{A})P(\tilde{B})$ (一共有四个等式)。可推广至:

$$P(\tilde{A}_1\tilde{A}_2\dots\tilde{A}_n) = P(\tilde{A}_1)\dots P(\tilde{A}_n)$$

上面有 2^n 个等式。

独立一定相容

重要公式与结论

$$(1) P(\bar{A}) = 1 - P(A)$$

$$(2) P(A \cup B) = P(A) + P(B) - P(AB)$$

$$(3) P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(AB) - P(AC) - P(BC) + P(ABC)$$

$$(4) P(A - B) = P(A) - P(AB)$$

$$(5) P(A\bar{B}) = P(A) - P(AB), P(A) = P(AB) + P(A\bar{B}),$$

$$P(A \cup B) = P(A) + P(\bar{A}B) = P(AB) + P(A\bar{B}) + P(\bar{A}B)$$

$$(6) P(\bar{A}_1|B) = 1 - P(A_1|B), P(A_1 \cup A_2|B) = P(A_1|B) + P(A_2|B) - P(A_1A_2|B)$$

$$P(A_1A_2|B) = P(A_1|B)P(A_2|A_1B)$$

$$(7) A_1, A_2, \dots, A_n \quad P\left(\bigcap_{i=1}^n A_i\right) = \prod_{i=1}^n P(A_i), P\left(\bigcup_{i=1}^n A_i\right) = \prod_{i=1}^n (1 - P(\bar{A}_i))$$

随机变量 (Random variable): 值随机会而定的变量, 研究随机试验的一串事件。可按维数分为一维、二维至多维随机变量。按性质可分为离散型随机变量以及连续型随机变量。

分布 (Distribution): 事件之间的联系, 用来计算概率。

示性函数 (Indication function): $I_A(\omega) = \begin{cases} 1 & \omega \in A \\ 0 & \text{反之} \end{cases}$, 事件 A 有随机变量

I_A 表示出来, I_A 称为事件 A 的示性函数。

定义 4.1.4. 概率函数:

设 X 为一随机变量, 其全部可能值为 $\{a_1, a_2, \dots\}$, 则 $p_i = P(X = a_i), i = 1, 2, \dots$ 称为 X 的概率函数。

定义 4.1.5. 概率分布函数:

定义: 设 X 为一随机变量, 则函数

$$F(X) = P(X \leq x) \quad (-\infty < x < \infty)$$

称为 X 的分布函数。(注: 这里并未限定 X 为离散型的, 它对任何随机变量都有定义。)

性质:

$F(x)$ 是单调非降的: 当 $x_1 < x_2$ 时, 有 $F(x_1) \leq F(x_2)$.

当 $x \rightarrow \infty$ 时, $F(x) \rightarrow 1$; 当 $x \rightarrow -\infty$ 时, $F(x) \rightarrow 0$.

离散型随机变量分布函数:

对于离散型随机变量, $F(X) = P(X \leq x) = \sum_{\{i|a_i \leq x\}} p_i, \quad p_i = P(X = i) = F(i) - F(i-1)$ 。

1. 连续型随机变量: 设 X 为一随机变量, 如果 X 不仅有无限个而且有不可数个值, 则称 X 为一个连续型随机变量。

定义 4.1.6. 概率密度函数:

设连续型随机变量 X 有概率分布函数 $F(x)$, 则 $F(x)$ 的导数 $f(x) = F'(x)$ 称为 X 的概率密度函数。

性质

1. 对于所有的 $-\infty < x < +\infty$, 有 $f(x) \geq 0$;

2. $\int_{-\infty}^{+\infty} f(x)dx = 1$;

3. 对于任意的 $-\infty < a \leq b < +\infty$, 有 $P(a \leq X \leq b) = F(b) - F(a) = \int_a^b f(x)dx$.

注:

1. 对于任意的 $-\infty < x < +\infty$, 有 $P(X = x) = \int_x^x f(u)du = 0$.
2. 假设有总共一个单位的质量连续地分布在 $a \leq x \leq b$ 上, 那么 $f(x)$ 表示在点 x 的质量密度且 $\int_c^d f(x)dx$ 表示在区间 $[c, d]$ 上的全部质量。

定义 4.1.7. 概率分布函数:

设 X 为一连续型随机变量, 则

$$F(x) = \int_{-\infty}^x f(u)du, \quad -\infty < x < +\infty$$

4.2 重要公式与结论

二项分布 $X \sim B(n, p)$ 的期望为 np , 方差为 $np(1-p)$

均匀分布 $X \sim U(a, b)$ 的期望为 $\frac{a+b}{2}$, 方差为 $\frac{1}{12}(b-a)^2$

定义 4.2.1. 边缘分布:

因为 X 的每个分量 X_i 都是一维随机变量, 故它们都有各自的分布 F_i ($i = 1, \dots, n$), 这些都是一维分布, 称为随机向量 X 或其分布 F 的边缘分布。

离散随机变量:

$$\begin{aligned} p_X(x_i) &= P(X = x_i) \\ &= \sum_j^m P(X = x_i, Y = y_j) \\ &= \sum_j^m p_{ij} = p_{i\cdot}, \quad i = 1, 2, \dots, n \end{aligned}$$

$$\begin{aligned}
 p_Y(y_i) &= P(Y = y_i) \\
 &= \sum_i^m P(X = x_i, Y = y_j) \\
 &= \sum_i^m p_{ij} = p_{j\cdot}, \quad j = 1, 2, \dots, n
 \end{aligned}$$

连续随机变量:

为求某分量 X_i 的概率密度函数, 只需把 $f(x_1, \dots, x_n)$ 中的 x_i 固定, 然后对 $x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n$ 在 $-\infty$ 到 ∞ 之间做定积分, 如

$$(X, Y) \sim f(x, y) f_X(u) = \int_{-\infty}^{+\infty} f(u, v) dv f_Y(u) = \int_{-\infty}^{+\infty} f(u, v) du$$

定义 4.2.2. 离散型随机变量的条件分布: 设 (X, Y) 为二维离散型随机变量, 对于给定的事件 $\{Y = y_j\}$, 其概率 $P(Y = y_j) > 0$, 则称

$$P(X = x_i | Y = y_j) = \frac{P(X = x_i, Y = y_j)}{P(Y = y_j)} = \frac{p_{ij}}{p_{j\cdot}}, \quad i = 1, 2, \dots$$

为在给定 $Y = y_j$ 的条件下 X 的条件分布律。类似的, 称

$$P(Y = y_i | X = x_j) = \frac{P(X = x_i, Y = y_j)}{P(X = x_j)} = \frac{p_{ij}}{p_{i\cdot}}, \quad j = 1, 2, \dots$$

为在给定 $X = x_j$ 的条件下 Y 的条件分布律。

连续型随机变量的条件分布: 设 (X, Y) 为二维连续型随机变量, 对于给定条件 $Y = y$ 下的条件概率密度为

$$f_{X|Y}(x|y) = \frac{f(x, y)}{f_Y(y)}, \quad f_Y(y) > 0.$$

类似的, 在 $X = x$ 下的条件概率密度为

$$f_{Y|X}(y|x) = \frac{f(x, y)}{f_X(x)}, \quad f_X(x) > 0.$$

可推广

定义 4.2.3. 随机变量的独立性

称随机变量 X_1, \dots, X_n 相互独立,

1. 离散型随机变量

则联合分布律等于各自的边缘分布律的乘积, 即

$$P(X_1 = x_1, \dots, X_n = x_n) = P(X_1 = x_1) \dots P(X_n = x_n)$$

其中 (x_1, \dots, x_n) 为 (X_1, \dots, X_n) 的值域中的任意一点。

2. 连续型随机变量

则联合密度等于各自的边缘密度的乘积, 即

$$f(x_1, \dots, x_n) = f_1(x_1) \dots f_n(x_n), \quad \forall (x_1, \dots, x_n) \in R^n$$

3. 一般地

设 X_1, \dots, X_n 为 n 个随机变量, 如果它们的联合分布函数等于各自边缘分布函数的乘积, 即

$$F(X_1, \dots, x_n) = F_1(x_1) \dots F_n(x_n), \quad \forall (x_1, \dots, x_n) \in R^n$$

则称随机变量 X_1, \dots, X_n 相互独立。

以下内容才是重点!!!!

以下内容才是重点!!!!

以下内容才是重点!!!!

4.2.1 数学期望（均值）与方差**定义 4.2.4. 数学期望**

设随机变量 X 只取有限个可能值 a_1, \dots, a_m , 其概率分布为 $P(X = a_i) = p_i$ ($i = 1, \dots, m$).

则 X 的数学期望记作 EX 或 $E(X)$, 定义为 $E(X) = a_1p_1 + a_2p_2 + \dots + a_mp_m$.

数学期望也常称为均值, 即指以概率为权的加权平均。

1. 离散型变量的数学期望: $E(X) = \sum_{i=1}^{\infty} a_i p_i$. (当级数绝对收敛, 即 $\sum_{i=1}^{\infty} |a_i| p_i < \infty$)

2. 连续型变量的数学期望: $E(X) = \int_{-\infty}^{\infty} x f(x) dx$. (当 $\int_{-\infty}^{\infty} |x| f(x) dx < \infty$)

性质

1. 若干个随机变量之和的期望等于各变量的期望值和, 即

$$E(X_1 + X_2 + \dots + X_n) = E(X_1) + E(X_2) + \dots + E(X_n).$$

2. 若干个独立随机变量之积的期望等于各变量的期望之积, 即

$$E(X_1 X_2 \dots X_n) = E(X_1) E(X_2) \dots E(X_n).$$

3. 设随机变量 X 为离散型, 有分布 $P(X = a_i) = p_i (i = 1, 2, \dots)$; 或者为连续型, 有概率密度函数 $f(x)$. 则

$$E(g(x)) = \sum_i g(a_i) p_i \quad (\text{当 } \sum_i |g(a_i)| p_i < \infty \text{ 时})$$

或

$$E(g(x)) = \int_{-\infty}^{\infty} g(x) f(x) dx \quad (\text{当 } \int_{-\infty}^{\infty} |g(x)| f(x) dx < \infty \text{ 时})$$

4. 若 c 为常数, 则 $E(cX) = cE(X)$.

定义 4.2.5. 条件数学期望

随机变量 Y 的条件期望就是它在给定的某种附加条件下的数学期望。

$E(Y|x) = \int_{-\infty}^{\infty} y f(y|x) dy$. 它反映了随着 X 取值 x 的变化 Y 的平均变化的情况如何。

在统计上, 常把条件期望 $E(Y|x)$ 作为 x 的函数, 称为 Y 对 X 的回归函数。

性质: 1. $E(Y) = \int_{-\infty}^{\infty} E(Y|x) f_X(x) dx$.

2. $E(Y) = E[E(Y|X)]$.

定义 4.2.6. 方差与标准差

设 X 为随机变量, 分布为 F , 则 $Var(X) = E(X - EX)^2$ 称为 X (或分布 F) 的方差,

其平方根 $\sqrt{Var(X)}$ (取正值) 称为 X (或分布 F) 的标准差。

性质: 1. $Var(X) = E(X^2) - (EX)^2$.

2. 常数的方差为 0, 即 $Var(c) = 0$.

3. 若 c 为常数, 则 $Var(X + c) = Var(X)$.

4. 若 c 为常数, 则 $Var(cX) = c^2 Var(X)$.

5. 独立随机变量和的方差等于各变量方差和, 即 $Var(X_1 + \dots + X_n) = Var(X_1) + \dots + Var(X_n)$.

4.3 期望经典问题入门

<https://notes.sshwy.name/Math/Expectation/Classic/#E-%E7%BB%8F%E5%85%B8%E9%A2%98> 重要公式与结论 1. 期望具有线性性

2. 独立事件的期望有

$$E(XY) = EXEY$$

3.

$$E(X) = E(E(X|Y))$$

4.3.1 普通

结论 4.3.1. 有 n 个随机变量 $\langle X_n \rangle$, 每个随机变量量都是从 $[1, m]$ 中随机一个整数, $\max \langle X_n \rangle$ 的期望为

$$m - \frac{1}{m^n} \sum_{i=1}^{m-1} i^n$$

。

证明. 设 $Y = \max \langle X_n \rangle$, 有

$$\begin{aligned}
 EY &= \sum_{1 \leq i \leq m} P(Y = i)i \\
 &= \sum_{1 \leq i \leq m} i(F_y(i) - F_y(i-1)) \\
 &= \frac{1}{m^n} \left(\sum_{1 \leq i \leq m} i^{n+1} - i \cdot (i-1)^n \right) \\
 &= \frac{1}{m^n} \left(\sum_{1 \leq i \leq m} i^{n+1} - \sum_{0 \leq i \leq m-1} i^{n+1} + i^n \right) \\
 &= \frac{1}{m^n} \left(m^{n+1} - \sum_{0 \leq i \leq m-1} i^n \right) \\
 &= m - \frac{1}{m^n} \sum_{i=1}^{m-1} i^n
 \end{aligned}$$

□

结论 4.3.2. 概率为 p 的事件期望 $\frac{1}{p}$ 次发生.

证明. 设随机变量 X 表示其在第 x 次发生.

$$\begin{aligned}
 EX &= \sum_{i=1}^{\infty} P(X = i)i \\
 &= \sum_{i=1}^{\infty} P(X = i) \sum_{j=1}^i 1 \\
 &= \sum_{j=1}^{\infty} P(X \geq j) \\
 &= \sum_{j=1}^{\infty} (1-p)^{j-1} \\
 &= \sum_{j=0}^{\infty} (1-p)^j \\
 &= \frac{1}{1 - (1-p)} \\
 &= \frac{1}{p}
 \end{aligned}$$

□

结论 4.3.3. 现在红包发了一个 w 元的红包, 有 n 个人来抢 (均匀分布)。那么请问第 k 个人期望抢到 $\frac{w}{2^k}$.

证明. 设第 k 个人抢到 X , 前面的人抢 Y . 有

$$E(X) = E(E(X|Y)) = E\left(\frac{w-Y}{2}\right) = \frac{w}{2} - \frac{1}{2}E(Y)$$

然后容易解出答案.

离散情况这样难以求解, 在取球一节有其他解法

□

结论 4.3.4. 赠券收集问题

一个 n 面的骰子, 期望 nH_n 次能使得每一面都被掷到。

证明. t_x 为设已经出现了 $x-1$ 面, 掷出第 x 面的次数.

设 $T = \sum t$. 有

$$E(T) = \sum_{i=1}^n E(t_i)$$

由于掷出第 x 面的概率为 $\frac{n-x+1}{n}$, 固

$$\begin{aligned} E(T) &= \sum_{i=1}^n E(t_i) \\ &= \sum_{x=1}^n \frac{n-x+1}{n} \\ &= n \cdot H_n \end{aligned}$$

□

同时他们也是相互独立的.

4.3.2 拿球

结论 4.3.5. 箱子里有 n 个球 $1, 2, \dots, n$, 你要从里面拿 m 次球, 拿了后不放回, 取出的数字之和的期望为 $\frac{m(n+1)}{2}$ 。

证明. 设随机变量 x_i :

$$x_i = \begin{cases} i & , \text{if } i \text{ is chosen} \\ 0 & , \text{if } i \text{ isn't chosen} \end{cases}$$

那么有

$$\begin{aligned} E\left(\sum_{i=1}^n x_i\right) &= \sum_{i=1}^n E(x_i) \\ &= \sum_{i=1}^n \frac{m}{n} i \\ &= \frac{m(n+1)}{2} \end{aligned}$$

发现是否放回不影响期望

□

结论 4.3.6. 箱子里有 n 个球 $1, 2, \dots, n$, 你要从里面拿 m 次球, 拿了后以 p_1 的概率放回, p_2 的概率放回两个和这个相同的球 (相当于增加一个球), 取出的数字之和的期望为 $\frac{m(n+1)}{2}$ 。

证明. 设 x_i 为第 i 个球的贡献, y_i 为其被拿出来的次数, 那么 $x_i = i \cdot y_i$

$$E\left(\sum_{i=1}^n x_i\right) = \sum_{i=1}^n E(y_i) \cdot i$$

因为 $E(y_i) = E(y_j)$, $\sum y_i = m$ 得出 $E(y_i) = \frac{m}{n}$ 故上式答案为 $\frac{m(n+1)}{2}$ □

4.3.3 游走

结论 4.3.7. 在一条 n 个点的链上游走, 从一端走到另一端的期望步数为 $(n-1)^2$ 。

证明. 假设步数是 S , 求 S 的期望. 我们定义一个随机变量 x_i 表示从 i 出发随机游走, 第一次到 $i+1$ 的步数。

$$E\left(\sum_{i=1}^{n-1} x_i\right) = \sum_{i=1}^{n-1} E(x_i)$$

又

$$EX_{i+1} = \frac{1}{2} + \frac{1}{2}(1 + EX_i + EX_{i+1})$$

故

$$EX_{i+1} = EX_i + 2$$

□

结论 4.3.8. 在一个 n 个点的完全图上游走, 从一个点走到另一个点的期望步数为 $n-1$ 。

证明. 由于是完全图, 所以任意两个点为起点和终点的期望步数是相同的. 于是有

$$E = \frac{1}{n-1} + \frac{n-2}{n-1}(1+E)$$

得到 $E = n-1$

□

结论 4.3.9. 在一个 n 个点的完全二分图 $K_{n,n}$ 上游走, 从一个点走到另一个点的期望步数为 $2n-1$ 。

证明. E_1 表示异侧点的期望, E_2 表示同侧点的期望。

$$E_1 = \frac{1}{n} + \frac{n-1}{n}(1+E_2)$$

$$E_2 = 1 + E_1$$

故 $E_1 = 2n-1, E_2 = 2n$

□

结论 4.3.10. 在一个 n 个点的菊花图上游走, 从一个点走到另一个点的期望步数为 $2n-3$ 。

证明与上类似

4.3.4 解题方法

1. 贡献法,

若不行可以尝试更换计算贡献的东西 (如边-> 点)

第五章 杂

5.1 最小二乘法

误差的平方和最小

$$L = \sum_{i=1}^n (y_i - f(x_i))^2$$

拟合直线 $y = kx + b$

$$\begin{cases} k &= \frac{\sum xy - n\bar{x}\bar{y}}{\sum x^2 - n\bar{x}^2} \\ b &= \bar{y} - k\bar{x} \end{cases}$$

5.2 常用幂级数

$$\begin{aligned}
 e^x &= \sum_{n=0}^{\infty} \frac{x^n}{n!} & x \in (-\infty, +\infty) \\
 \sin x &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!} & x \in (-\infty, +\infty) \\
 \cos x &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} & x \in (-\infty, +\infty) \\
 \frac{1}{x+1} &= \sum_{n=0}^{\infty} (-1)^n x^n & x \in (-1, 1) \\
 \ln(x+1) &= \sum_{n=0}^{\infty} (-1)^n \frac{x^{n+1}}{n+1} & x \in (-1, 1]
 \end{aligned}$$

复数

引入

从实数拓展复数，为了解决方程如 $x^2 + 1 = 0$ 在实数域无解的问题，引入虚数单位 i ，满足 $i^2 = -1$ ，所有形如 $a + bi$ 的数的集合称为复数集，记作 \mathbb{C} 。其中 a 为实部 $\Re(z)$ ， b 为虚部 $\Im(z)$ 。纯虚数当 $a = 0, b \neq 0$ 。

几何意义

两个复数相等当且仅当其实部与虚部分别相等，因此复数可在复平面中视为点 (a, b) 或向量 (a, b) 。复数模定义为

$$|z| = \sqrt{a^2 + b^2},$$

其几何意义为向量长度。复数的加减运算符合向量运算规则，满足交换律、结合律及分配律。

运算 & 共轭

对复数 $z_1 = a + bi$ 及 $z_2 = c + di$,

$$z_1 z_2 = (ac - bd) + (ad + bc)i$$

满足交换律、结合律及分配律。除法引入共轭复数 $\bar{z} = a - bi$ 来实母:

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \bar{z}_2}{|z_2|^2}.$$

共轭复数有:

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2.$$

辐角与主值

复数可表示为极坐标形式 (r, θ) , $r = |z|$, $\theta = \arg(z)$ 。辐角主值为 $\theta_0 \in (-\pi, \pi]$, 且任一辐角为 $\theta = \theta_0 + 2k\pi$ 。单位圆上的复数为模 1 的点, 单位复数为该圆上所有点。

欧拉公式 & 指数 / 三角函数

欧拉公式:

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

复指数函数定义为 $e^z = e^{x+iy} = e^x(\cos y + i \sin y)$, 具有:

$$|e^z| = e^x, \quad \arg(e^z) = y, \quad e^{z_1+z_2} = e^{z_1}e^{z_2}, \quad \text{周期性: 以 } 2\pi i \text{ 为基本周期.}$$

复三角函数定义为:

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}, \quad \sin z = \frac{e^{iz} - e^{-iz}}{2i},$$

其性质包括奇偶性、和差公式、周期性, 并且在复平面上无最大模界。

复数的三种形式

复数表示形式包括：- 代数形式： $a + bi$ ，- 三角形式： $r(\cos \theta + i \sin \theta)$ ，- 指数形式： $re^{i\theta}$ ，其中后三者适用于非零复数，有利于乘除与幂运算。

单位根

n 次单位根为满足 $z^n = 1$ 的复数，等分单位圆，共 n 个，通常取 $e^{2\pi ik/n}$ ， $k = 0, \dots, n-1$ 。本原单位根是那些其较低幂都不为 1 的单位根，共 $\varphi(n)$ 个。

编程语言中的复数

C++

- 提供 `<complex>`，类型为 `std::complex<float/double/long double>`;
- 成员函数：`real()`, `imag()`；非成员函数：`real(z)`, `imag(z)`, `abs(z)`, `arg(z)`, `norm(z)`, `conj(z)`, `exp(z)`, `log(z)`, `pow(z,w)`, `sqrt(z)`, `sin(z)`, `cos(z)`, `tan(z)`;
- C++14 字面量运算符支持 `100if`, `100i`, `100il` 表示不同类型的纯虚数。