大纲

- $$\text{逻辑} \to \text{集合} \to \text{函数}$$
  $$\text{数论}$$
  $$\text{数学归纳法}$$
  $$\text{计数问题} \leftarrow \text{数列} \leftarrow \text{生成函数}$$
  $$Relation \to Graph \to Tree$$

Chapter 4

可除性(Divisibility)

- a 是 b 的倍数(mutiple)
  - $\exists k, b = ka$
  - 有多少不大于n的数可以整除d?

$$0 \leq p = kd \leq n$$
$$\Rightarrow k \leq \frac{n}{d} \Leftrightarrow k = \lfloor \frac{n}{d} \rfloor$$

- 基本性质：可加性、可乘性、传递性

同余关系

- $a \equiv b (\mod m) \Leftrightarrow a = km + b$
- 加法和乘法保持同余关系
- 在$\mathbb{Z}_m$上定义加法和乘法$\rightarrow$ 整数群在同余关系下的商群

质数

- Prime
- 质数筛
- 定理一：质因数分解定理
- 定理二：能整除n的质数一定小于$\sqrt{n}$
  - 证明113是质数

$$\sqrt{113} = 10.13, \text{由上述定理，有可能被}113\text{整除的质数只有}2, 3, 5, 7$$
$$\text{但他们都不能被}113\text{整除，所以}113\text{是质数}$$

  - 如何将一个数n质因数分解?
    - 枚举比$\sqrt{n}$小的质数，若能整除就一直除
- 定理三：有无限个质数
- 梅森质数（Mersenne Prime）：$2^p - 1$ 了解一下就好

最大公约数（gcd）和最小公倍数（lcm）

- 怎么找gcd/lcm

    - 质因数分解
        - mn = gcd * lcm(定理五)
    - 欧几里得算法（辗转相除法）
        - 引理 $a = bq + r, gcd(a, b) = gcd(b, r)$
- 用线性组合表示最小公约数
    - $gcd(a, b) = sa + tb$
    - 例$gcd(6, 14) = 2 = (-2) * 6 + 14$
    - 怎么求？**倒过来做辗转相除法**

        express gcd(252,198) = 18 as a linear combination of 252 and 198.

        Solution:

        First use the Euclidean algorithm to show gcd(252,198) = 18

        I. $252 = 1 \cdot 198 + 54$
        II. $198 = 3 \cdot 54 + 36$
        III. $54 = 1 \cdot 36 + 18$
        IV. $36 = 2 \cdot 18$

        - **Now working backwards, from Ⅲ and Ⅱ above**

          $18 = 54 - 1 \cdot 36$
          $36 = 198 - 3 \cdot 54$

          Substituting the 2nd equation into the 1st yields:

          $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$

          Substituting 54 = 252 − 1 ·198 (from Ⅰ)) yields:

          $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

乘法逆元

- $a\bar{a} = 1 \pmod m$，a与$\bar{a}$互为模m意义下的乘法逆元
- 定理：若a, m互质，则a有在模m意义下的乘法逆元，且该逆元对m的模唯一
- 怎么找？
    - 用上面的线性组合法
    - $gcd(a, m) = 1 = sa + tm$，则s就是a在模m意义下的逆元
- 用逆元解决同余问题

$$3x \equiv 4 \mod 7\text{，求}x$$
$$\text{先求3在模7意义下的逆元，}(-2) * 3 + 7 = 1$$
$$\text{所以逆元为} -2$$
$$\text{方程左右同乘} -2\text{得到}(-2) * 3x \equiv x \equiv (-2) * 4 \equiv -8 \equiv 6 \mod 7$$
$$\text{所以}x \equiv 6 \mod 7$$

  总结：先求逆元（用欧几里得算法），再利用逆元的性质解题（如两边同乘逆元，左边等于1）

- 中国剩余问题

$$考虑x \equiv a_i \mod m_i, i = 1,2,..,n，其中m_1, m_2, ..., m_n两两互质，求x$$

$$该问题有模m意义下的唯一解，其中m = m_1 m_2 ... m_n$$

$$考虑M_i = \frac{m}{m_i}，则由两两互质的性质可知，M_i与m_i互质，则M_i有在模m_i意义下的唯一逆元y_i$$

$$即M_i y_i \equiv 1 \mod m_i$$

$$考虑p = \sum_{i=1}^{n} a_i M_i y_i$$

$$因为M_i = \frac{m}{m_i},所以M_i可以被除了m_i以外的任何m_j整除,即M_i \equiv 0 \mod m_j, j \neq i$$

$$所以我们有p \equiv a_i M_i y_i \equiv a_i \mod m_i, \forall i = 1,2,..,n$$

$$所以p就是我们要求的x$$

- 也可用回代法求解中国剩余问题

Back Substitution

We can also solve systems of linear congruences with pairwise relatively prime moduli by rewriting a congruences as an equality, substituting the value for the variable into another congruence, and continuing the process until we have worked through all the congruences.

Example: Use the method of back substitution to find all integers x such that $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.

Solution: the first congruence can be rewritten as $x = 5t+1$, where t is an integer.

- Substituting into the second congruence yields $5t+1 \equiv 2 \pmod 6$.
- Solving this tells us that $t \equiv 5 \pmod 6$.
- Using Theorem 4 again gives $t = 6u + 5$ where u is an integer.
- Substituting this back into $x = 5t+1$, gives $x = 5(6u + 5) + 1 = 30u + 26$.
- Inserting this into the third equation gives $30u + 26 \equiv 3 \pmod 7$.
- Solving this congruence tells us that $u \equiv 6 \pmod 7$.
- By Theorem 4, $u = 7v + 6$, where v is an integer.
- Substituting this expression for u into $x = 30u + 26$, tells us that $x = 30(7v + 6) + 26 = 210u + 206$.

Translating this back into a congruence we find the solution $x \equiv 206 \pmod{210}$.

- 费马小定理

  $a^{p-1} \equiv 1 \mod p$

Chapter 6

计数原理

鸽巢原理

经典题型

- n个数的同余问题
  - 任意的n+1个数，一定有两个数对n同余
- 10 个人的party有两个人有相同数量friend
  - 朋友个数0~9 且不可能同时出现0和9

- 不超过2n的n+1个数有两个可除
  - 分解为$2^t q_i$，q_i为奇数
  - 小于2n的奇数至多有n个
- 前n项和问题
  - 任意的n个数，存在一个连续子列之和可以整除n
  - 用前n项和转化为n个数的同余问题
- 单调子列长度问题
  - （a,b）为以k为起点的最长单增列长度和最长单减列长度
- 计数和问题
  - 连续的k天里有p场比赛
  - 前n项和a_k, c_k = a_k + p
  - 用范围框定
- Ramsey Number

排列组合

- SUCCESS排列问题
- A，B，C，D一共有几种不同分法?
  - $$S(n,j) = \frac{n\text{到}j\text{的满射个数}}{j!} = \frac{\sum_{i=0}^{j}(-1)^i\binom{j}{i}(j-i)^j}{j!}$$
    $$\text{分法} = \sum_{j=0}^{n} S(n,j)$$
- r-combination
  - $x_1 + x_2 + x_3 = 6$
  - 生成函数
  - stars and bars
- Partition
  - 枚举

二项式定理

- double counting

Chapter 8

线性数列递推

- 从实际问题构造递推
  - 数字串（从短一点的数字串出发）
- 齐次型$a_n = \sum_{i=1}^{k} c_i a_{n-i}$
  - 特征方程$r^k - \sum_{i=1}^{k} c_i r^{k-i} = k$
  - 特征根$r_1, .., r_t$，重数$m_1 + ... + m_t = 0$
  - 通解$a_n = P_{m_1}(n) r_1^{m_1} + ... + P_{m_t}(n) r_t^{m_t}$
- 非齐次部分$F(n) = \sum_{i=1}^{p} Q_{t_i}(n) s_i^n$

  - 特解形式$a_n^{(p)} = \sum_{i=1}^{p} R_{t_i}(n) s_i^n \cdot n^{\alpha_i}$

生成函数

- 数列转化成生成函数
- 生成函数展开成数列
- 生成函数解决`r-combination`型问题
- 生成函数解决数列递推问题
- 生成函数解决恒等式证明问题

容斥原理

- 多并集计算

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cup A_j| + \sum_{1 \le i < j < k \le n} |A_i \cup A_j \cup A_k| \dots$$

- 性质计数 + 容斥原理

  $N(P) = \text{满足性质}P\text{的种类数}$

- 直接用容斥原理
  - 找出相应的性质
  - 用容斥原理
- 先找出反向的性质，再用容斥
  - **正面做不了就反过来做**
- 素数筛

  先找出$< \sqrt{n}$的素数，P_i代表能被p_i整除

- onto-function

  P_i代表b_i不在值域中

- 错排

  P_i代表第i个元素在本来的位置上

Chapter 9

Relation

- Relation性质和表示之间的关系/计数问题
  - 自反Reflexive
    - 特点：表示矩阵对角元全为1
    - 大小为n的集合上的自反关系有2^{n^2-n}个
  - 反-自反的Irreflexive
    - 特点：表示矩阵对角元全为0
    - 大小为n的集合上的反-自反关系有2^{n^2-n}个
  - 对称Symmetric
    - 特点：表示矩阵$A = A^T$
    - 计数：$2^{\frac{n^2+n}{2}}$
  - 反对称的Antisymmetric

        - 特点: 对称元不同时为1
        - 计数：$3^{\frac{n^2-n}{2}}2^n$
    - 非对称的Asymmetric
        - 特点：不是对称的
        - 计数:$2^{n^2}-2^{\frac{n^2+n}{2}}$
    - 注意：可以既对称又反对称,例如I
- Relation的复合(Composition)
    - 易错点:顺序

      $S\circ R=R\to S=M_R\cdot M_S$
- 定理:R是连通的，当且仅当R^n是R的子集，证明用数归
- P闭包
    - 包含
    - 满足性质P
    - 最小的：任何一个满足上面两条的都包含他、
- 连通性Connectivity $\to$ 传递性 Transitivity
    - $t(R)=R^*=\cup_{k=1}^{n}R^k$
- **WarShall 算法求传递闭包**

等价关系 Equivalence Relation

- 证明等价关系（回归定义）
    - 自反的
    - 对称的
    - 传递的
- 找等价类(equivalence class)：选人大
- **重要！！** A上的等价关系个数$\Leftrightarrow$ 找Partition(划分)
- 什么是Partition?
    - 非空的
    - 不交的
    - 完全的

偏序关系 Partial Ordering

- 什么是偏序关系（回归定义）
    - 自反的
    - 反对称的
    - 传递的
- **Hasse Diagram**
    - Maximal/Minimal （局部的）
    - Greatest/Least（全局的）
    - Upper Bound/ Lower Bound 上界/下界
    - Least Upper Bound / Greatest Lower Bound
- Well-Ordered 良序的
    - 任何子集有最小元
- Lattice

- 任何pair有glb和ulb
- 拓扑排序：炒菜模型

Chapter 10

Graph

- 各种定义
- Hand-shaking Theorm
  - $\sum_{v \in V} deg(v) = 2e$
- 分类
- K_n的子图有几种
  - $\sum_{k=1}^{n} C(n,k) 2^{C(k,2)}$
- entry 项
- 综合考察特殊图的性质和Adjacency matrix 和 Incidence Matrix的概念
- Isomorphism 同构
  - 映射
  - 邻接矩阵
  - 度数（判断不同构或是找同构映射时使用）
  - 环的大小
- 两点间的路径数
  - A^r
- 判断是否存在Euler/Hamilton Path / Circuit
  - Euler Circuit ⇔ 度数为偶数
  - Euler Path ⇔ 恰好两个点度数为奇数
  - Hamiltion Circult $deg(u) + deg(v) \geq n$
- Dijkstra求单源最短路
- 平面图
  - 欧拉定理：r = e-v+2
  - 必要条件：区域的最大边数为k→ 某个定理
  - 非平面 充要条件 子图和$K_{3,3}$或K_5同构
- 染色问题