Lecture 1

中国剩余定理 Chinese Remainder Theorem

Catalan数 Catalan Number

中国剩余定理(CRT)

- 南北朝时期的算术著作《孙子算经》中有一个“**物不知数**”问题：

  今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何？答曰：二十三。

- 一般性问题：

  求 N（非负整数）满足如下方程组：

$$\begin{cases} N = a_1 (mod\ m_1) \\ \vdots \\ N = a_k (mod\ m_k) \end{cases}$$

（$a_1 \sim a_k, m_1 \sim m_k$是给定的。$0 \le a_i < m_i$。）

$m_1 \sim m_k$两两互素的情况。

$$\begin{cases} N = a_1 (mod\ m_1) \\ \vdots \\ N = a_k (mod\ m_k) \end{cases} \qquad (1)$$

- 令$s_i = (m_1 * \cdots * m_k) / m_i$。
- 找到s_i 在 模m_i意义下的逆元 r_i。 即， $s_i r_i = 1 \pmod{m_i}$
  - 回顾逆元的含义（之前学过的内容）
- **定理**： $N = \sum_{i=1}^{k} a_i s_i r_i$是 (1) 的一个解。
  - 证明：
    - 由于$s_j \bmod m_i = 0$（对于$i \neq j$)
    - $N \bmod m_i = a_i s_i r_i \bmod m_i = a_i$。

举例

- $a_1 = 2, m_1 = 3$. $a_2 = 3, m_2 = 5$. $a_3 = 2, m_3 = 7$.
  三三数之剩二，五五数之剩三，七七数之剩二
- $s_1 = 35$. 注意35 模3为2， 逆元$r_1 = 2$。
- $s_2 = 21$. 注意21 模5为1， 逆元$r_2 = 1$。
- $s_3 = 15$. 注意15 模7为1， 逆元$r_3 = 1$。

$$N = \sum_{i=1}^{k} a_i s_i r_i$$
$$= 2 * 35 * 2 + 3 * 21 * 1 + 2 * 15 * 1$$
$$= 140 + 63 + 30 = 23 (\bmod 105)$$

(1)的通解？

$$\begin{cases} N = a_1 (mod\ m_1) \\ \vdots \\ N = a_k (mod\ m_k) \end{cases} \quad (1)$$

- 令$M = m_1 * \ldots * m_k$。记$N_0 = \sum_{i=1}^{k} a_i s_i r_i \ mod\ \mathrm{M}$。
- **定理**. 方程(1)在 [0,M-1]范围内**恰有一个**解 N_0。
  - 证明：固定$m_1 \sim m_k$时，$(a_1,\ldots,a_k)$的选择为M个。
    每一种选择，都有一个解N 在[0,M-1]内。
    而[0,M-1]中一共只有M个数。 因此，每种选择对应恰好一个解。
- 得到一一对应关系：
  - [0,M-1]中的N ⇔ $(a_1,\ldots,a_k)$。这是一种number system。
- **推论**. 方程(1)的通解为 $N_0 + iM$（i为任意整数）。

如果m_1~m_k不是两两互质的呢？

考虑两个方程：

$x = a \pmod{m}$, $x = b \pmod{n}$。 m,n**允许不互素**。 如何求x?

- $x = mp+a = nq+b$ 。因此 $mp-nq=b-a$ (2)。
- 如果 (m,n) 不整除 $(b-a)$，方程(2)无解，因此(1)无解。
- 下面假定 (m,n) 整除$(b-a)$。此时方程(2)有解。假设(p_0,q_0)是一个解。
- 方程(2)的通解是 $p=p_0+n/(n,m)\,\boldsymbol{t}$。 $q=q_0+m/(n,m)\,\boldsymbol{t}$。
- 可知 $x = mp+a$

$$= mn/(n,m)\,\boldsymbol{t} + (mp_0+a)$$

$$= \mathrm{lcm}(m,n)\,\boldsymbol{t} + (mp_0+a)。$$

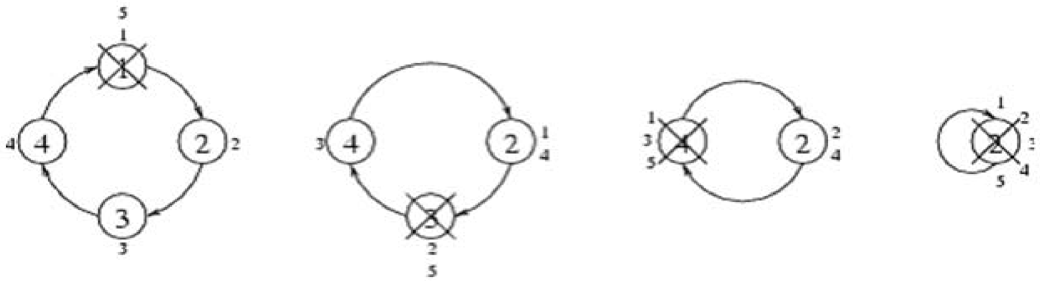
$$= mp_0+a \pmod{\mathrm{lcm}(m,n)}。$$

两个方程合并为了一个 $x=a'(\bmod m')$，其中 $a'=mp_0+a$, $m'=\mathrm{lcm}(m,n)$

如果多余两个方程，两两合并即可。最终解出x。

CRT例题

- 已知n个人按1~K（K待求）报数的出圈顺序，求最小正整数K。
- 比如，4个人按1~K报数，出圈顺序为1 3 4 2。 求K=?



N=4, K=5时的出圈情形

- K % 4 = 1. K%3=2. K%2=1。 解出K=5

CRT更多练习 (optional)

- 屠龙勇士（NOI-2018）
- https://www.luogu.com.cn/problem/P4774

CRT常见用途

- 假如有一个数 x 很大。范围是$0\sim10^{100}$。我们想要求出此数。
- 假定有一种方法，对于$<10^{10}$的m能够求出$x \bmod m$。
- 那么可以这样来求x。
  - 找若干个互素的数$m_1\sim m_k$。使得$M= m_1*\ldots*m_k$大于10^{100}。
  - 然后分别求出 $x \bmod m_1,\ldots\ x \bmod m_k$。
  - 最后利用CRT定理，解出x。

  - 计算x mod m可能比计算x，更容易（x太大，x mod m较小）。

Catalan数 与 Raney引理

问题提出

- **问题1：** n个左括号与n个右括号 的 合法括号序列的个数。
- 合法括号序列举例
  - ()()()　　(())()　　((()))
  - ()()()　　(())()　　((()))

每个括号都完美的匹配到一个相反的括号

- 不合法的例子
  -)(　　((())　　())(()

递归定义

1 空串合法

2 如果A合法，　则(A)合法。

3 如果A、B合法，　则AB 合法。

非递归定义

1 “(”个数与“(”个数相等

2 任意前缀中

“(”的个数 ≥ “)”的个数。

等价的问题

- **问题2**（ ⇔问题1）
  - 有多少个序列含n个1, n个-1满足：任意前缀和都**非负**数。
- 证明:
  - “(” 对应 1
  - ”)“ 对应-1。
  - 每个前缀中“(”个数 ≥ “)”个数 对应 每个前缀中1的个数≥ -1个数，即每个前缀和非负。
- **问题3**（⇔问题2）
  - 有多少个序列含n+1个1, n个-1满足：任意（真)前缀和都为**正**数。
  - 注：真前缀不包括长为0的前缀。

解法一： 利用Raney引理

- **定义**： Cyclic-shift of $H=(h_1,\ldots,h_L)$。
  - 把 $(H_k,\ldots H_L,H_1,\ldots,H_{k-1})$叫做 H的一个*cyclic-shift*。 （记作$H^{(k)}$）
  - 举例
    - H=(-1，1，2，1,-2)。 cyclic-shift 包括：
    - $H^{(1)}$=(-1，1，2，1,-2)
    - $H^{(2)}$=(1，2，1,-2,-1)
    - $H^{(3)}$=(2，1,-2,-1，1)
    - $H^{(4)}$=(1,-2,-1，1，2)
    - $H^{(5)}$=(-2,-1，1，2，1)

这一个cyclic-shift满足条件。

- **Raney引理**： 设$H=(h_1,\ldots,h_L)$是个整数序列， 满足$h_1+\ldots+h_L=1$。那么，在H的所有cyclic-shift中**恰有一个**满足： 它的各个(真)前缀和均为正。

基于Raney Lemma来 求解问题3.

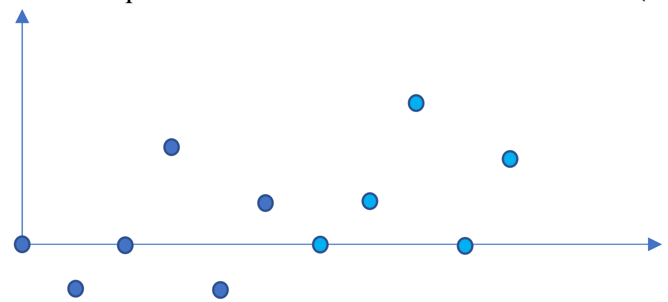
- 考虑 n+1 个1、n个-1的排列——共$\binom{2n+1}{n}$个。

  要统计它们有多少个满足 (1) （真)前缀和均为正数。
- 将这些排列中彼此为cyclic-shift（即，循环同构的）归为一类。
  容易证明每一类恰好有2n+1个排列。
  - 观察：H的cyclic-shift $H^{(1)},\ldots,H^{(2n+1)}$各不相同。证明留为作业。
- 根据Raney引理，每一类中恰有一个满足(1)。
  因此，答案为 $\binom{2n+1}{n}/(2n+1)$。

补充：Raney引理的证明（数形结合方法）

Raney引理：设$H=(h_1,\ldots,h_L)$是个整数序列，满足$h_1+\ldots+h_L=1$。那么，
在H的L个cyclic-shift中恰有一个满足：所有前缀和为正。

- 假定 $H=(h_1,\ldots,h_L)$ 。满足 $h_1+\ldots+h_L=1$。
- 扩展这个序列为 $(h_1,\ldots,h_L,h_1,\ldots,h_L)$。
  - $H_{i+L}=h_i$。 $(1<=i<=L)$
- 定义 $S_i= h_1+\ldots+h_i$。 为$0<=i<=2L$，构造点(i, S_i)。



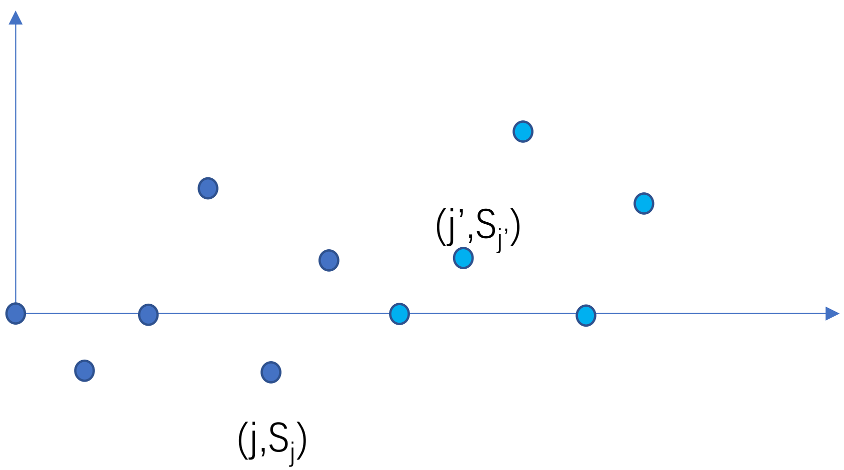
举例。

H= (-1, 1, 2,-3, 2,-1, 1, 2, -3, 2)。
S= (-1, 0, 2,-1, 1, 0, 1, 3, 0, 2)。

找到高度最低的点；如有多个选**其中最右边的**，设为(j,S_j)。
则，$H^{(j+1)}$即为所有cyclic-shift中唯一满足前缀和全正的。

① $H^{(j+1)}$ 的各个前缀和全正。
② 当$1\leqslant k\leqslant j$时，
$H^{(k)}$ 的某个前缀和$\leqslant 0$。
③ 当$j+2\leqslant k\leqslant L$时，
$H^{(k)}$ 的某个前缀和$\leqslant 0$。

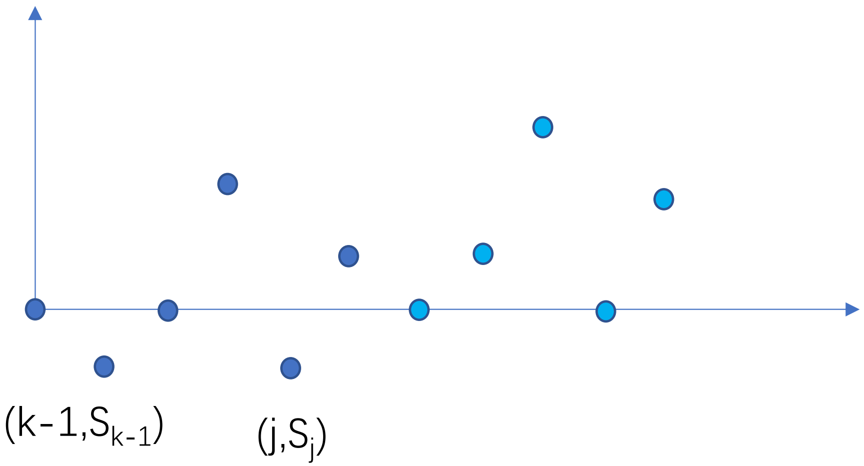
① $H^{(j+1)}$ 的各个前缀和全正。



- 对于j'⩾j+1来说，
  - Sj'>Sj。
  - 因此，Sj'-Sj>0。
  - 因此，$h_{j+1}+\cdots h_{j'} > 0$。
- 结论
  - $h_{j+1}>0$
  - $h_{j+1}+h_{j+2}>0$
  - $h_{j+1}+h_{j+2}+h_{j+3} >0$
  - …

  这说明 $H^{(j+1)}$的前缀和都

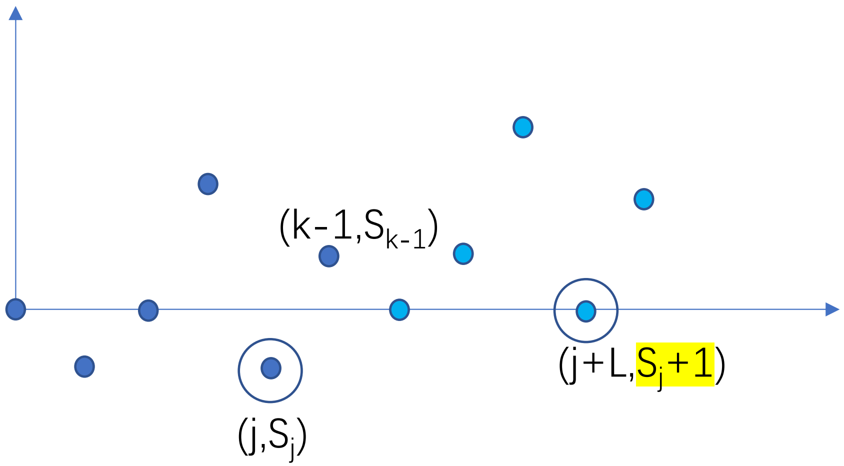
② 当$1\leqslant k\leqslant j$时，$H^{(k)}$ 的某个前缀和$\leqslant 0$



- 根据j的定义，$S_j \leqslant S_{k-1}$。
- 因此$S_j-S_{k-1} \leqslant 0$
- 得到 $h_k+\cdots+h_j \leqslant 0$。

- 故$H^{(k)}$的某个前缀和$\leqslant 0$

③ 当$j+2 \leqslant k \leqslant L$时， $H^{(k)}$ 的某个前缀和$\leqslant 0$



- 根据j的定义， $S_j < S_{k-1}$。
  - 因此$S_j + 1 \leqslant S_{k-1}$。
- 由于$h_1+\cdots+h_L=1$（已知）
  - 因此$S_{j+L} = S_j + 1$。
- 综合得到， $S_{j+L} \leqslant S_{k-1}$
- 因此$S_{j+L}-S_{k-1} \leqslant 0$
- 得到 $h_k+\cdots+h_{j+L} \leqslant 0$。
- 故$H^{(k)}$的某个前缀和$\leqslant 0$

解法二： 折线法

问题4（⇔ 问题2）

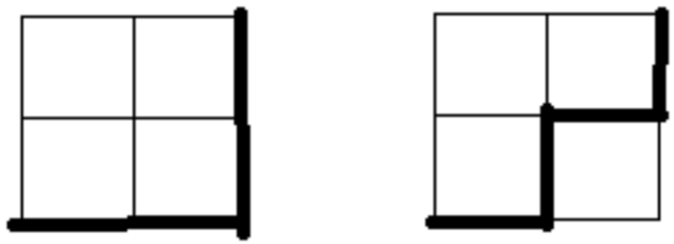
从 <u>左下角</u> (0,0)出发，前往 <u>右上角</u>(n,n)。

每次只允许向右 / 向上。n次向上，n次向右。

要求满足(1)： 只经过 $\{(x,y) \mid x \geq y\}$。

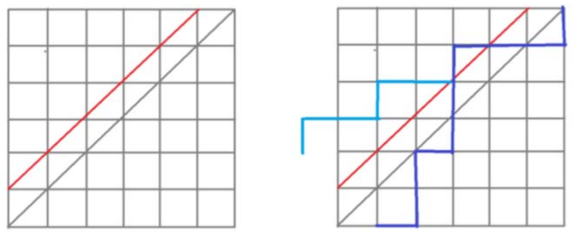
也就是说向右的次数>=向上的次数始终成立。求路径数。

举例



N=2时，有两条满足(1)的路径

路径计数



- **观察**: 从(0,0)到(n,n)的不到红线的路径数
  =从(1,0)到(n,n)的不到红线的路径数
  =从(1,0)到(n,n)路径数 - 从(1,0)到(n,n)的到过红线的路径数
  =从(1,0)到(n,n)路径数 - 从(-1,2)到(n,n)的路径数 (见上图)

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

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

$$=\frac{2(2n-1)!}{(n+1)!(n-1)!}=\frac{(2n)!}{(n+1)!n!}=\binom{2n}{n}/(n+1)。$$

小结

- 注意 $\binom{2n+1}{n}/(2n+1)=\binom{2n}{n}/(n+1)$

  左式= $\frac{(2n+1)!}{n!(n+1)!}/(2n+1)=\frac{(2n)!}{n!(n+1)!}$=右式。

- **总结**：问题1~4这些计数问题的答案，均为$\binom{2n}{n}/(n+1)$。
- 定义 $C_n = \binom{2n}{n} / (n+1)$. 称之为Catalan数。（卡特兰数）
- 例如C_0,C_1,…=1,1,2,5,14,42,132…. 均为Catalan数。

例题：stack-sortable排列的个数。

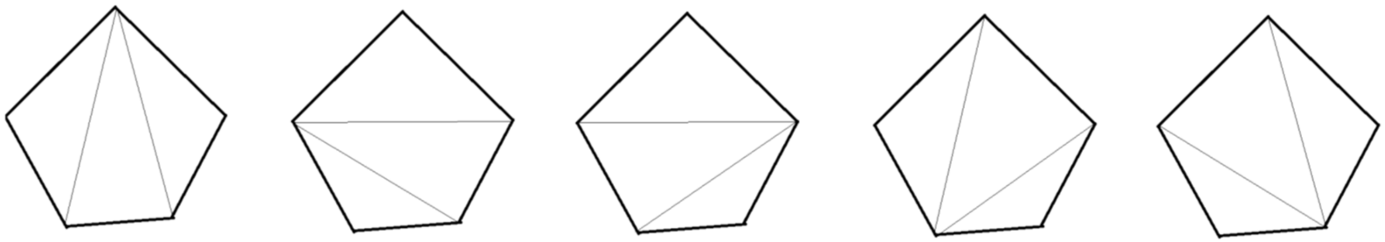
- 考虑1~n的一个排列a_1~a_n。如果$(a_1,\ldots,a_n)$依次进栈，出栈的顺序可以恰好为1…n（排好序了），就说a_1~a_n是stack-sortable的。
- 求问stack-sortable的排列有多少个？
- **举例**。 (1,2,3), (1,3,2),(2,1,3),(3,1,2),(3,2,1)是stack-sortable的。
- **反向思考**：n~1依次入栈，利用一个栈，有多少找出栈序列？

- 操作序列：n次入栈，n次出栈，入栈的个数>=出栈个数。
- 当操作序列不同时，很明显得到的是不一样的出栈序列。
- 因此，总的出栈序列个数=操作序列个数= C_n。

Catalan数的一个重要的递归公式

- **定理**. Catalan数满足$C_n = C_0C_{n-1}+C_1C_{n-2}+\ldots+C_{n-1}C_0$； $C_0=1$.
- 证明
  - 考虑合法括号序列。(())((()()))(())
  - 每个这样的序列中，第一个左括号都与某个右括号匹配。把这两个括号 叫做“第一对括号”。
  - 回顾：n对括号的合法括号序列的个数为 C_n
  - 采用分类计数：
    - 第一对括号中有0对括号：　　$C_0 * C_{n-1}$
    - 第一对括号中有i对括号：　　$C_i * C_{n-1-i}$
  - 因此，$C_n = C_0C_{n-1}+C_1C_{n-2}+\ldots+C_{n-1}C_0$。

例题 凸n边形的三角剖分的个数=?



- 令F_n 表示 n+2边形分解的方案。
- **观察**: $F_n = F_0*F_{n-1}+F_1*F_{n-2} +\cdots+ F_{n-1}*F_0$。$F_0=1$.
  - 板书证明
- 因此$F_n=C_n$。 因此凸n边形三角剖分的个数为$F_{n-2}=C_{n-2}$。

本课小节

- 一、CRT，解方程： $\begin{cases} N = a_1 (mod\ m_1) \\ \vdots \\ N = a_k (mod\ m_k) \end{cases}$
  - 互素的情况，有简单的公式。非互素的情况，仍存在有效算法。
- 二、Catalan数
  - 1 基于Raney Lemma的求解
  - 2 **折线法**，(1,0)-(n,n)路径数 – (-1,2)-(n,n)路径数。
  - C_n= (2n 选 n) / (n+1)。
  - **递推公式**： $C_n = C_0C_{n-1}+C_1C_{n-2}+\ldots+C_{n-1}C_0$； $C_0=1$.