基礎數學

許博翔

February 6, 2023

講師簡介

- 許博翔
- ICPC 台北站金牌
- 國際數學奧林匹亞銀牌
- IMOC、清華數學人才培育計畫講師
- 爲了學基礎數學來當講師
- Google 搜尋仙草

大綱

計數原理

基本定義與公式 – 符號定義

定義

- $\sum_{i=1}^{n} f(i) := f(1) + f(2) + \cdots + f(n)$

例子

$f(i) = i$

- $\sum_{i=1}^{5} f(i) = 1 + 2 + 3 + 4 + 5 = 15$

基本定義與公式 – 符號定義

定義

- $\sum_{i \in S} f(i) :=$ 所有 S 中的元素代入 f 後的總和
- $\sum_{i \in \emptyset} f(i) := 0$

例子

$f(i) = i$

- $\sum_{i \in \{1,3,5\}} f(i) = 1 + 3 + 5 = 9$

基本定義與公式 – 符號定義

定義

- $\prod_{i=1}^{n} f(i) := f(1)f(2)\cdots f(n)$

例子

$f(i) = i$

- $\prod_{i=1}^{5} f(i) = 1 \times 2 \times 3 \times 4 \times 5 = 120$

基本定義與公式 – 符號定義

定義

- $\prod_{i \in S} f(i) :=$ 所有 S 中的元素代入 f 後的積
- $\prod_{i \in \emptyset} f(i) := 1$

例子

$f(i) = i$

- $\prod_{i \in \{1,3,5\}} f(i) = 1 \times 3 \times 5 = 15$

基本定義與公式 – 符號定義

定義

- $\bigcup_{i=1}^{n} S_i := S_1 \cup S_2 \cup \cdots \cup S_n$

基本定義與公式 – 符號定義

定義

- $\bigcup_{i \in T} S_i :=$ 所有 T 中的元素（也是集合）聯集
- $\bigcup_{i \in \emptyset} S_i := \emptyset$

基本定義與公式 – 符號定義

定義

- $\bigcap_{i=1}^{n} S_i := S_1 \cap S_2 \cap \cdots \cap S_n$

基本定義與公式 – 符號定義

定義

- $\bigcap_{i \in T} S_i :=$ 所有 T 中的元素（也是集合）交集
- $\bigcap_{i \in \emptyset} S_i :=$ 所有有被包含在任何 S_i 中的元素

基本定義與公式 – 高中複習

定義

- $n!$ 是 n 個相異物的排列方法數。
- $\binom{n}{k}$（高中課本寫做：C_k^n）是從 n 不同物品取 k 個出來的方法數，也是 n 元集的 k 元子集的個數。
- $\left(\!\binom{n}{k}\!\right)$ 是滿足 $\sum_{i=1}^{n} x_i = k$ 的非負整數解 $(x_1, x_2, \ldots, x_n)$ 的個數，也是包含 k 相異元素的 n 元多重集的個數。

基本定義與公式 – 高中複習

公式

- $n! = \prod_{i=1}^{n} i$，特別定義 $0! = 1$。
- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$。
- $\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}$。

基本定義與公式 – 高中複習

公式

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

基本定義與公式 – 球與箱子

題目 (球與箱子 (1))

請求出把 n 顆相異的球放進 m 個相異箱子的方法數。

基本定義與公式 – 球與箱子

題目 (球與箱子 (1))

請求出把 n 顆相異的球放進 m 個相異箱子的方法數。

因爲每顆球都可以選擇要放進 m 個箱子中的哪個箱子，所以答案是 m^n。

基本定義與公式 – 球與箱子

題目 (球與箱子 (2))

請求出把 n 顆相同的球放進 m 個相異箱子的方法數。

基本定義與公式 – 球與箱子

題目 (球與箱子 (2))

請求出把 n 顆相同的球放進 m 個相異箱子的方法數。

設第 i 個箱子放了 x_i 顆球，這個問題的答案就是
$x_1 + x_2 + \cdots + x_m = n$ 的非負整數解數，也就是 $\left(\!\binom{m}{n}\!\right)$。

排容原理 – 排容原理

定理 (排容原理)

設有 n 個集合 $S_1, S_2, \ldots, S_n$，則

$$\sum_{T \subseteq \{1,2,\ldots,n\}} (-1)^{|T|} \left| \bigcap_{i \in T} S_i \right| = 0$$

，特別定義 $\bigcap_{i \in \emptyset} S_i = \bigcup_{i \in \{1,2,\ldots,n\}} S_i$，即 $(\{S_1, S_2, \ldots, S_n\}, \cap)$ 的單位元素。

排容原理 – 排容原理

定理 (排容原理)

設有 n 個集合 $S_1, S_2, \ldots, S_n$，則

$$\sum_{T \subseteq \{1,2,\ldots,n\}} (-1)^{|T|} \left| \bigcap_{i \in T} S_i \right| = 0$$

，特別定義 $\bigcap_{i \in \emptyset} S_i = \bigcup_{i \in \{1,2,\ldots,n\}} S_i$，即 $(\{S_1, S_2, \ldots, S_n\}, \cap)$ 的單位元素。

以 $n = 3$ 爲例，這個公式即是 $|S_1 \cup S_2 \cup S_3| - |S_1| - |S_2| - |S_3| + |S_1 \cap S_2| + |S_2 \cap S_3| + |S_3 \cap S_1| - |S_1 \cap S_2 \cap S_3| = 0$

排容原理 – 排容原理

定理 (集合上的莫比烏斯反演 (Möbius inversion of the power set))

令 $A = \{S_1, S_2, \ldots, S_n\}$，則

$$g(A) = \sum_{B \subseteq A} f(B) \iff f(A) = \sum_{B \subseteq A} \mu(A \setminus B) g(B)$$

，其中 $\mu : \mathcal{P}(A) \to \mathbb{Z}$ 定義如下：

$$\mu(B) = \begin{cases} 0 & \text{如果} B \text{中有重複的元素} \\ (-1)^{|B|} & \text{如果} B \text{中沒有重複的元素} \end{cases}$$

排容原理 – 排容原理

定理 (集合上的莫比烏斯反演 (Möbius inversion of the power set))

$$g(A) = \sum_{B \subseteq A} f(B) \iff f(A) = \sum_{B \subseteq A} \mu(A \setminus B) g(B)$$

回推排容原理：

$A = \{S_1, S_2, \ldots, S_n\}$

$f(B) = |\{s | s \in S \iff S \in B\}|$

$g(B) = \left| \bigcup_{S \in B} S \right|$

排容原理 – 錯排數

題目 (錯排數)

有多少個 $1, 2, \ldots, n$ 的排列沒有不動點？
其中若排列 $\sigma_i = i$，則稱 i 是 σ 的不動點。

排容原理 – 錯排數

這題的答案稱作第 n 個錯排數。
令 $S_i = \{\sigma : \sigma_i = i\}$。因爲

$$\bigcap_{i \in T} S_i = \{\sigma : \forall i \in T,\ \sigma_i = i\}$$

，也就是對於所有 T 中的元素都是不動點的排列，所以

$$\left| \bigcap_{i \in T} S_i \right| = (n - |T|)!$$

另外，

$$|\{T : |T| = k,\ T \subseteq \{1, 2, \ldots, n\}\}| = \binom{n}{k}$$

排容原理 – 錯排數

所以根據排容原理：

$$\begin{aligned}
\left|\bigcup_{i=1}^{n} S_i\right| &= -\sum_{T\neq\emptyset,\ T\subseteq\{1,2,\ldots,n\}} (-1)^{|T|}\left|\bigcap_{i\in T} S_i\right| \\
&= -\sum_{k=1}^{n}\sum_{|T|=k, T\subseteq\{1,2,\ldots,n\}} (-1)^{k}\left|\bigcap_{i\in T} S_i\right| \\
&= -\sum_{k=1}^{n}\sum_{|T|=k, T\subseteq\{1,2,\ldots,n\}} (-1)^{k}(n-k)! \\
&= -\sum_{k=1}^{n}\binom{n}{k}(-1)^{k}(n-k)! \\
&= -n!\sum_{k=1}^{n}\frac{(-1)^{k}}{k!}
\end{aligned}$$

排容原理 – 錯排數

因爲 $\bigcup_{i=1}^{n} S_i$ 爲所有有不動點的排列所形成的集合，所以

$$\begin{aligned} \text{第}n\text{個錯排數} &= n! - \left| \bigcup_{i \in T} S_i \right| \\ &= n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \end{aligned}$$

排容原理 – 沒有空箱

題目 (沒有空箱)

請求出把 n 顆不同的球放進 m 個相同的箱子且沒有空箱的方法數。

排容原理 – 沒有空箱

如果箱子是相異的，也就是給這些箱子加上編號，任意換另一種順序上編號都會得到不同的結果，因爲沒有兩個箱子的內容物是一樣的。換句話說，如果箱子是相異的，答案會剛好是原題答案的 $m!$ 倍，所以我們可以假設這些箱子是相異的，再把最後的答案除以 $m!$。

假設箱子是相異的，令 S_i 爲沒有球放進第 i 個箱子的方法所形成的集合。於是我們要的答案就是 $\bigcup_{i=1}^{m} S_i$ 的補集的大小。

因爲 $\bigcap_{i\in T} S_i$ 就是對於所有 T 中的元素都沒有球的方法，所以每次放球有 $m-|T|$ 種選擇，$\left|\bigcap_{i\in T} S_i\right| = (m-|T|)^n$。

排容原理 – 沒有空箱

另外，$|\{T : |T| = k,\ T \subseteq \{1, 2, \ldots, m\}\}| = \binom{m}{k}$。所以根據排容原理：

$$\begin{aligned}
\left|\bigcup_{i=1}^{m} S_i\right| &= -\sum_{T\neq\emptyset,\ T\subseteq\{1,2,\ldots,m\}} (-1)^{|T|} \left|\bigcap_{i\in T} S_i\right| \\
&= -\sum_{k=1}^{m} \sum_{|T|=k, T\subseteq\{1,2,\ldots,m\}} (-1)^{k} \left|\bigcap_{i\in T} S_i\right| \\
&= -\sum_{k=1}^{m} \sum_{|T|=k, T\subseteq\{1,2,\ldots,m\}} (-1)^{k}(m-k)^{n} \\
&= -\sum_{k=1}^{m} \binom{m}{k} (-1)^{k}(m-k)^{n}
\end{aligned}$$

排容原理 – 沒有空箱

而其補集大小，也就是相異箱子的答案是

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

而相同箱子的答案即爲

$$\sum_{k=0}^{m} \frac{(-1)^k (m-k)^n}{k!(m-k)!}$$

排容原理 – 球與箱子 (3)

題目 (球與箱子 (3))

請求出把 n 顆不同的球放進 m 個相同箱子的方法數。

排容原理 – 球與箱子 (3)

設 n 顆球放入剛好 i 個箱子的答案爲 a_i。
因爲這 n 顆球有可能放入剛好 $1, 2, \ldots, m$ 個箱子中，所以這題的答案即爲 $a_1 + a_2 + \cdots + a_m$。
在上個例題中我們得知：

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

排容原理 – 球與箱子 (3)

所以這題的答案即是

$$\begin{aligned}
\sum_{i=1}^{m} a_i &= \sum_{i=0}^{m} \sum_{k=0}^{i} \frac{(-1)^k (i-k)^n}{k!(i-k)!} \\
&= \sum_{k=0}^{m} \sum_{i=k}^{m} \frac{(-1)^k (i-k)^n}{k!(i-k)!} \\
&= \sum_{k=0}^{m} \sum_{j=0}^{m-k} \frac{(-1)^k j^n}{k!j!} \\
&= \sum_{j=0}^{m} \frac{j^n}{j!} \sum_{k=0}^{m-j} \frac{(-1)^k}{k!} \\
&= \sum_{j=0}^{m} \frac{j^n}{j!(m-j)!} d_{m-j}
\end{aligned}$$

，其中 d_{m-j} 爲第 $m-j$ 個錯排數。

遞迴 – 遞迴

定義

設數列 $\{a_i\}_{i=0}^{\infty}$ 與函數 f 滿足
$\forall n,\ a_n = f(n, a_{n-1}, a_{n-2}, \ldots, a_0)$，則稱 f 是 a_n 的遞迴式。

遞迴 – 錯排數

題目 (錯排數)

有多少個 $1, 2, \ldots, n$ 的排列沒有不動點？
其中若排列 $\sigma_i = i$，則稱 i 是 σ 的不動點。

遞迴 – 錯排數

設 a_n 爲第 n 個錯排數，計算以下兩種錯排 σ 的數量：

$\sigma_{\sigma_1} = 1$：
$\sigma_1 = i$, $\sigma_i = 1$ 的錯排數量，即爲 $\{2, 3, \ldots, n\} \setminus \{i\}$ 這 $n-2$ 個數字的錯排數量，有 a_{n-2} 種，而 σ_1 有 $n-1$ 種可能，所以這種錯排的數量爲 $(n-1)a_{n-2}$。

遞迴 – 錯排數

$\sigma_{\sigma_1} \neq 1$：
計算 $\sigma_1 = i$ 的錯排數量。設一個新的排列 $\sigma' : \{1, 2, \ldots, n\} \setminus \{i\}$ 爲 $\sigma'_1 = \sigma_{\sigma_1}$，$\sigma'_j = \sigma_j$，可知 σ' 是一個 $\{1, 2, \ldots, n\} \setminus \{i\}$ 這 $n-1$ 個數字的錯排，有 a_{n-1} 種，而 σ_1 有 $n-1$ 種可能，所以這種錯排的數量爲 $(n-1)a_{n-1}$。

綜合上述，

$$a_n = (n-1)(a_{n-1} + a_{n-2})$$

遞迴 – 線性遞迴

定義

設數列 $\{a_i\}_{i=0}^{\infty}$ 有遞迴式
$\forall n \geq k,\ a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$，則稱爲 k 階線性遞迴。

遞迴 – 線性遞迴

如果把遞迴式寫成以下矩陣的形式：

$$\begin{pmatrix} a_n \\ a_{n-1} \\ a_{n-2} \\ \vdots \\ a_{n-k+1} \end{pmatrix} = \begin{pmatrix} c_1 & c_2 & \cdots & c_{k-1} & c_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ a_{n-3} \\ \vdots \\ a_{n-k} \end{pmatrix}$$

遞迴 – 線性遞迴

設中間的矩陣爲 A，可以發現：

$$\begin{pmatrix} a_n \\ a_{n-1} \\ \vdots \\ a_{n-k+1} \end{pmatrix} = A^{n-k+1} \begin{pmatrix} a_{k-1} \\ a_{k-2} \\ \vdots \\ a_0 \end{pmatrix}$$

因此可以用矩陣快速冪在 $O(k^3 \log n)$ 的時間算出 A^{n-k+1}，再乘上 $\begin{pmatrix} a_{k-1} \\ a_{k-2} \\ \vdots \\ a_0 \end{pmatrix}$ 即可得到 a_n。

所以這是一個時間複雜度 $O(k^3 \log n)$ 的算法。

遞迴 – 費氏數列

定義 (費氏數列)

以 F_n 代表費氏數列第 n 項，
$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$。

遞迴 – 費氏數列

題目

有多少個 $S \subseteq \{1, 2, \ldots, n\}$ 滿足 $\forall i, j \in S,\ |i - j| \neq 1$？

遞迴 – 費氏數列

以 a_n 代表這題的答案。

S 有兩種：

$n \in S$：
$n-1 \notin S$，而 $S' := S \setminus \{n\}$ 即是一個 $\{1, 2, \ldots, n-2\}$ 的子集且 $\forall i, j \in S',\ |i-j| \neq 1$，所以這種 S 有 a_{n-2} 種。

$n \notin S$：
S 即是一個 $\{1, 2, \ldots, n-1\}$ 的子集且 $\forall i, j \in S',\ |i-j| \neq 1$，所以這種 S 有 a_{n-1} 種。

綜合上述 $a_n = a_{n-1} + a_{n-2}$，有跟費氏數列一樣的遞迴式，而 $a_0 = 1,\ a_1 = 2$，所以 $a_n = F_{n+2}$。

遞迴 – 球與箱子 (3)

題目 (球與箱子 (3))

請求出把 n 顆不同的球放進 m 個相同箱子的方法數。

遞迴 – 球與箱子 (3)

$a_{i,j}$：將 i 顆球放進 j 個相同箱子的方法數，且 j 個箱子每個都不是空的。

分成
(1) 第 i 顆球所在的那個箱子只有一顆球。
(2) 第 i 顆球所在的那個箱子有兩顆以上的球。

遞迴 – 球與箱子 (3)

我們將第 i 顆球拿掉，若是產生了空箱，代表剩下的 $i-1$ 顆球被放進 $j-1$ 個相同箱子且沒有空箱，也就是有 $a_{i-1,j-1}$ 種可能。

如果沒有產生空箱，代表剩下的 $i-1$ 顆球被放進 j 個相同箱子且沒有空箱，且第 i 顆球有可能是從任何箱子拿出來的，也就是有 $ja_{i-1,j}$ 種可能。

所以

$$a_{i,j} = a_{i-1,j-1} + ja_{i-1,j}$$

而答案就是

$$\sum_{j=1}^{m} a_{n,j}$$

遞迴 – 球與箱子 (4)

題目 (球與箱子 (4))

請求出把 n 顆相同的球放進 m 個相同箱子的方法數。

遞迴 – 球與箱子 (4)

$a_{i,j}$：將 i 顆球放進 j 個相同箱子的方法數，且 j 個箱子每個都不是空的。

球數最少的箱子，可以分成
(1) 只有一顆球。
(2) 有兩顆以上的球。

遞迴 – 球與箱子 (4)

如果只有一顆球，我們將那個箱子連同球一起拿掉，剩下的 $i-1$ 顆球被放進 $j-1$ 個箱子且沒有空箱，也就是有 $a_{i-1,j-1}$ 種可能。

如果有至少兩顆球，我們可以從所有箱子中的抽出一球，剩下的 $i-j$ 顆球被放進 j 個箱子且沒有空箱，也就是有 $a_{i-j,j}$ 種可能。

遞迴 – 球與箱子 (4)

所以

$$a_{i,j} = a_{i-1,j-1} + a_{i-j,j}$$

而答案就是

$$\sum_{j=1}^{m} a_{n,j}$$

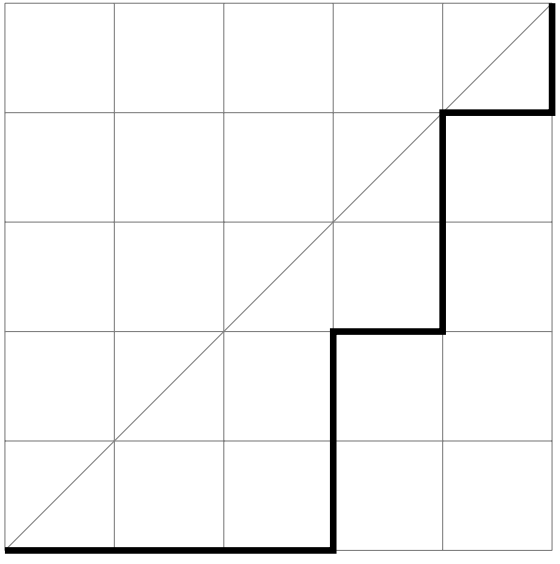
遞迴 – 卡特蘭數

定義 (Dyck Path)

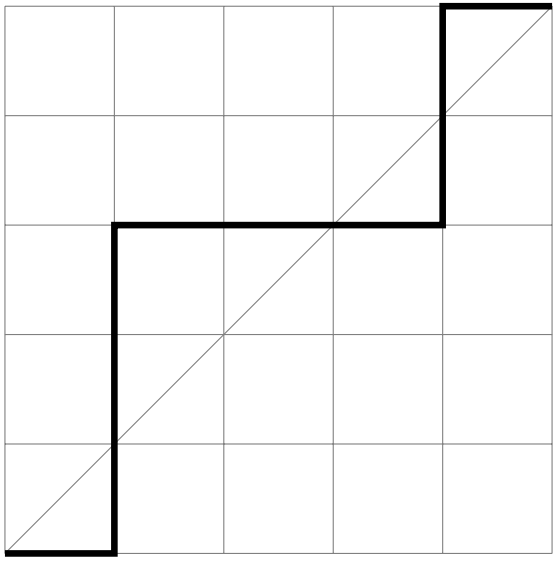
一條長度 $2n$ 的 Dyck Path 是指一條從在一個 $n \times n$ 的格線從左下角 $(0,0)$ 走到右上角 (n,n)，每一步只能往右或往上走的路徑，且整條路徑都在對角線 $(0,0) - (n,n)$ 之下或是剛好壓到對角線。

遞迴 – 卡特蘭數

Dyck Path:



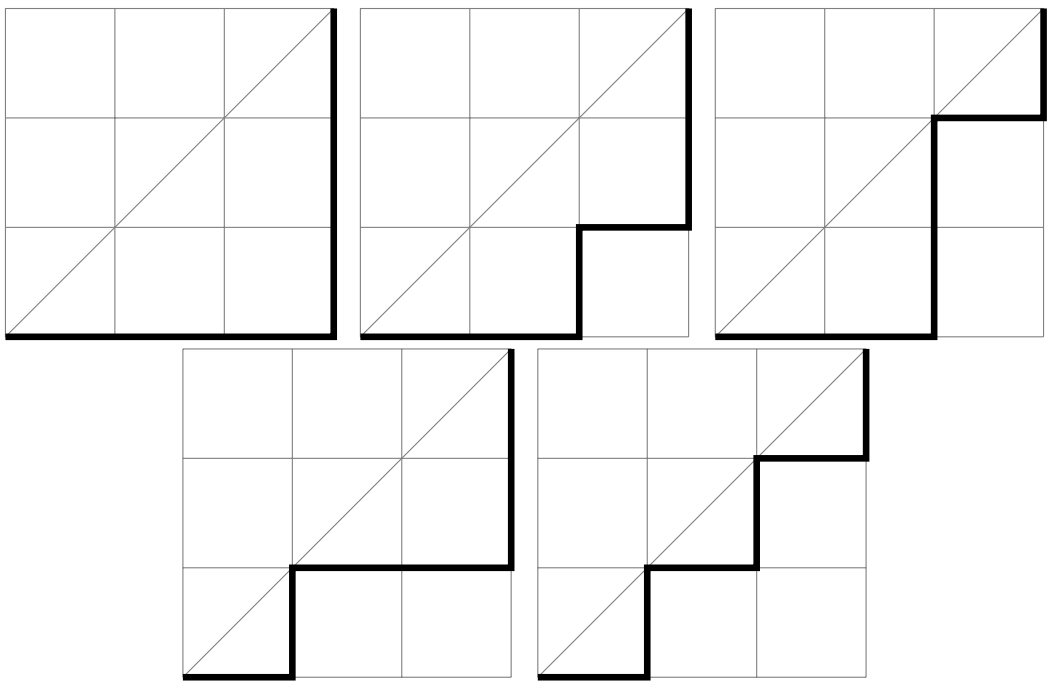
不是 Dyck Path:



遞迴 – 卡特蘭數

定義 (卡特蘭數)

以 C_n 代表卡特蘭數第 n 項，C_n 爲長度 $2n$ 的 Dyck Path 的數量。



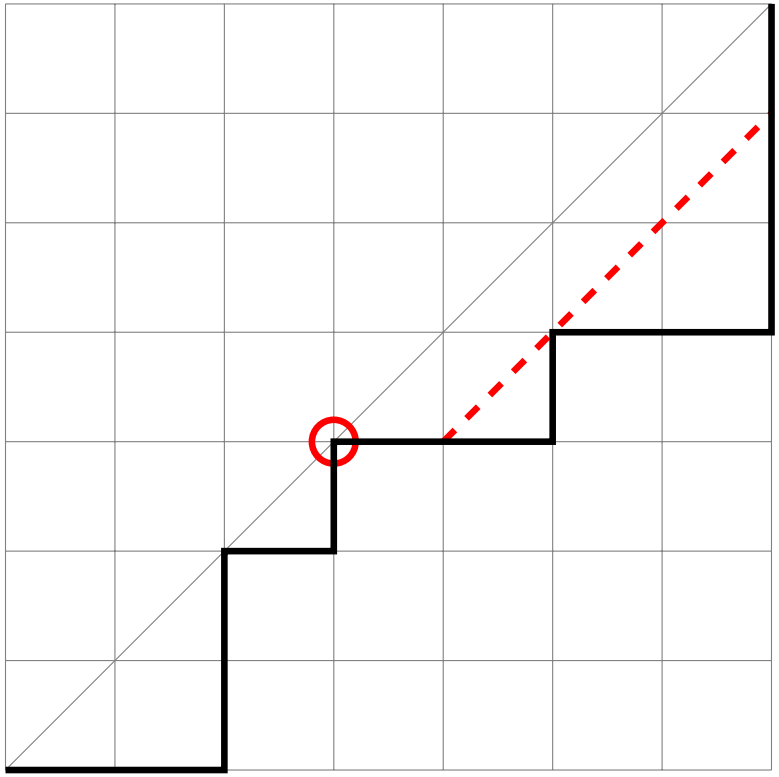
$$C_3 = 5$$

遞迴 – 卡特蘭數

公式

$$C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}$$

遞迴 – 卡特蘭數



- 從 $(0,0)$ 走到 (k,k)：有 C_k 種走法。
- 從 (k,k) 走到 $(2k+1,2k+1)$：有 C_{n-k} 種走法。
- $C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}$

組合對應 – 雙射函數

定義

設 $f : A \to B$ 爲一函數

- 單射（一對一）：$\forall x, y \in A,\ f(x) = f(y) \iff x = y$
- 滿射：$\forall z \in B,\ \exists x \in A \text{ s.t. } f(x) = z$
- 雙射：單射且滿射

組合對應 – 雙射函數

性質

設 $f : A \to B$ 爲一函數，則

- f 單射 $\Rightarrow |A| \leq |B|$
- f 滿射 $\Rightarrow |A| \geq |B|$
- f 雙射 $\Rightarrow |A| = |B|$

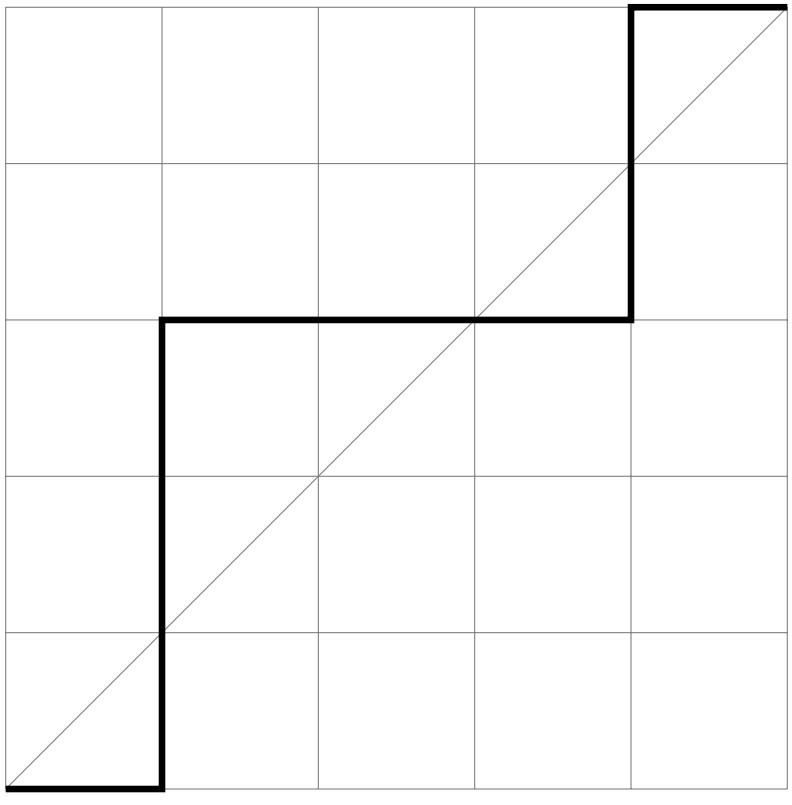
組合對應 – 卡特蘭數

公式

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

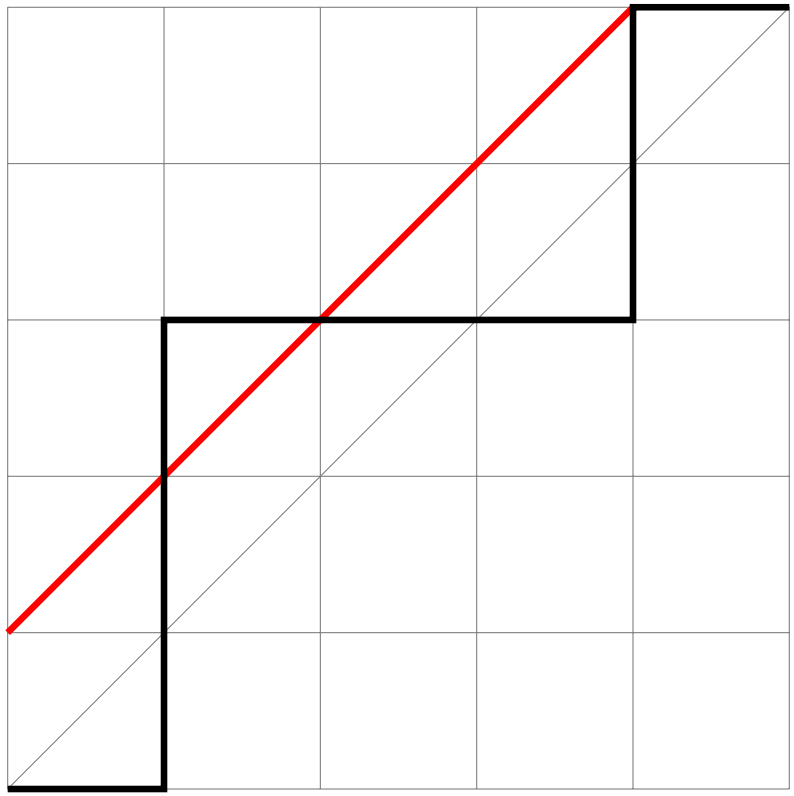
組合對應 – 卡特蘭數

不合法的路徑：



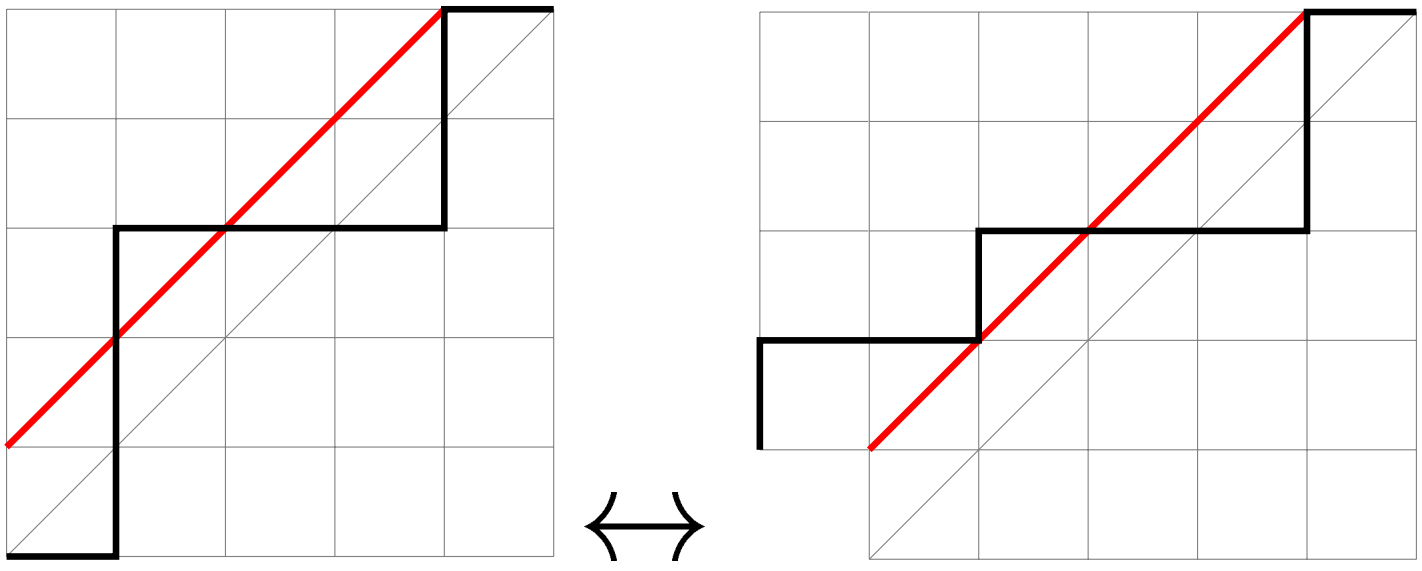
組合對應 – 卡特蘭數

不合法的路徑：



組合對應 – 卡特蘭數

不合法的路徑：



$$\text{不合法路徑數} = \binom{2n}{n-1}$$

組合對應 – 卡特蘭數

$$C_n = \text{合法路徑數} - \text{不合法路徑數} = \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}$$

組合對應 – 卡特蘭數

性質

以下問題的答案都是 C_n：

- 長度 $2n$ 的合法括號序列數量。
- 凸 $n+2$ 邊形分割成多個三角形的方法數。
- $n+1$ 個點的有根樹的數量（子結點有分順序）。
- n 個點的二元樹數量（子結點有分左右）。

組合對應 – Prufer's code

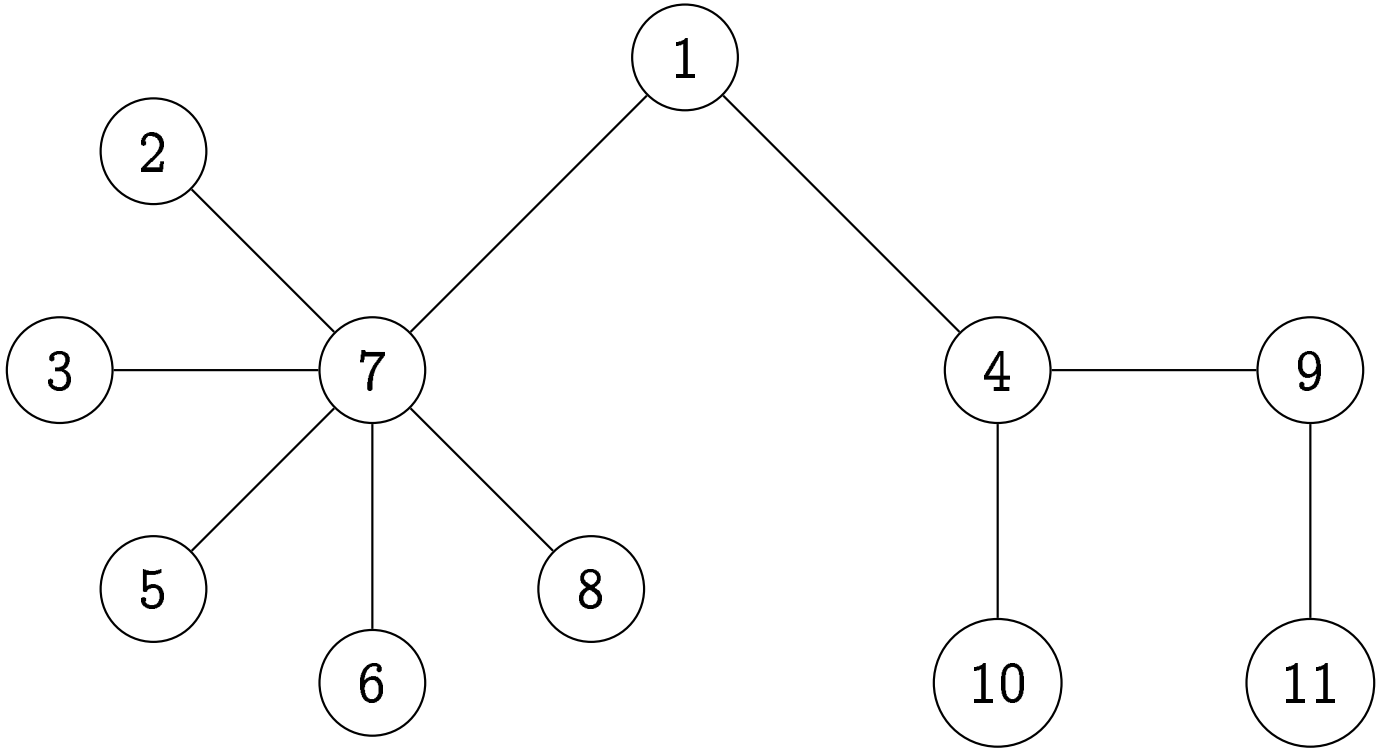
題目 (Prufer's code)

K_n 有多少個生成樹？

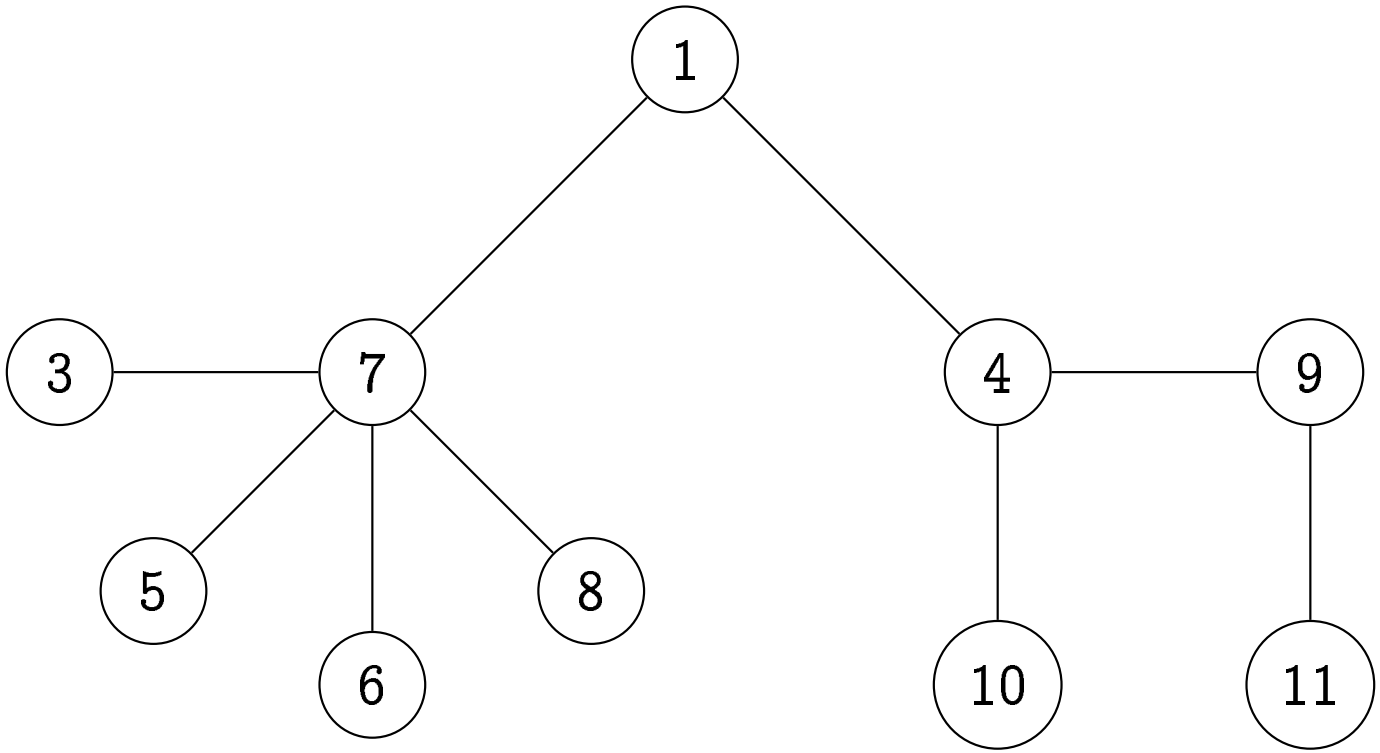
組合對應 – Prufer's code

- 答案是 n^{n-2}。
- 將生成樹與 $(a_1, a_2, \ldots, a_{n-2})$ 做對應（$a_i \in \{1, 2, \ldots, n\}$）。

組合對應 – Prufer's code

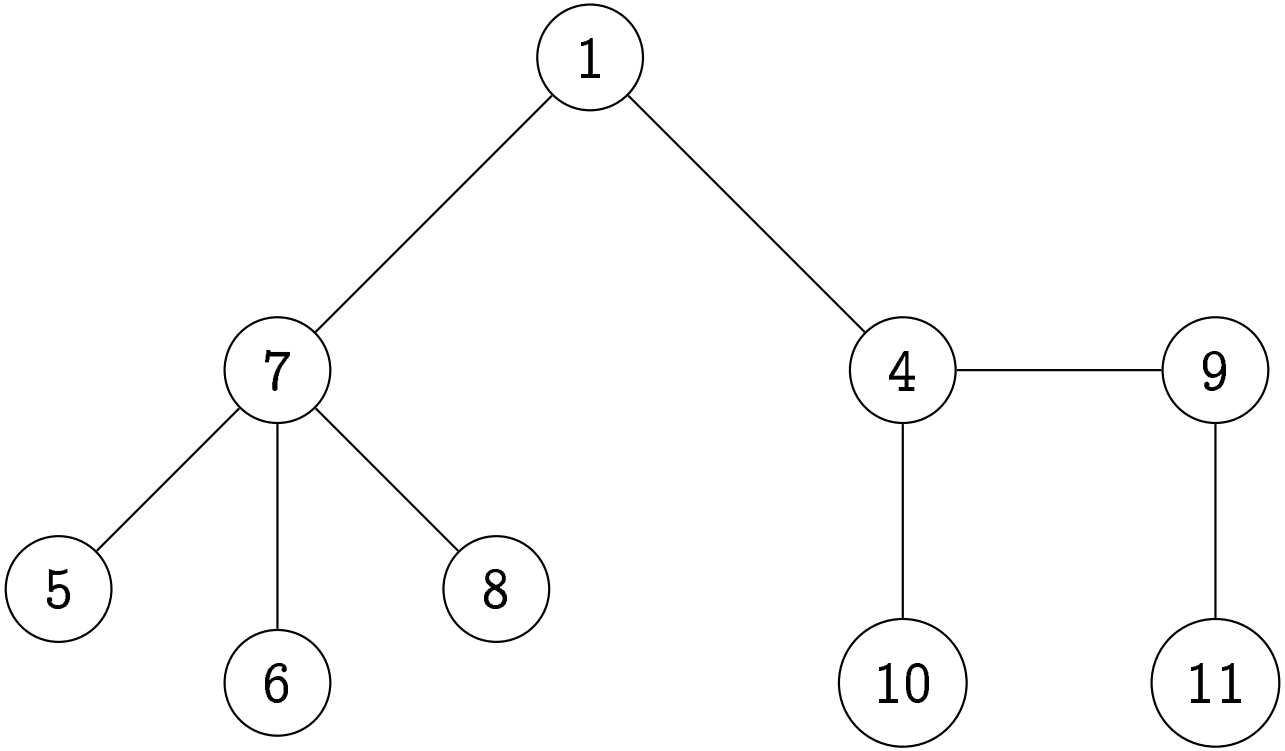


組合對應 – Prufer's code



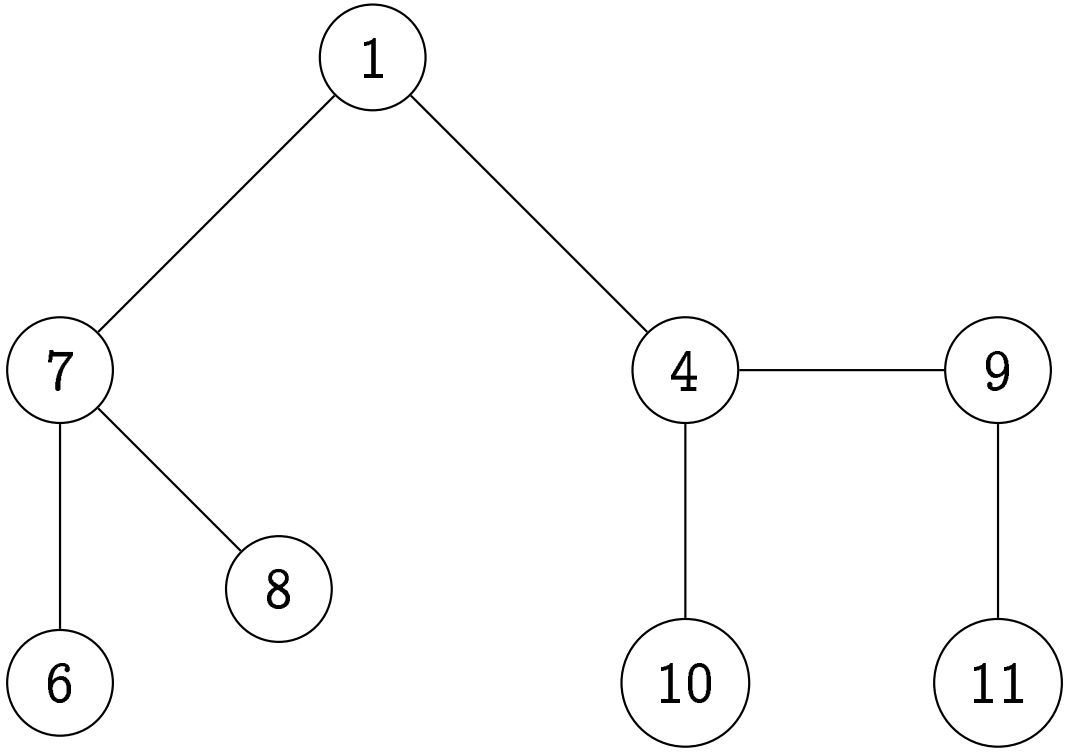
7

組合對應 – Prufer's code



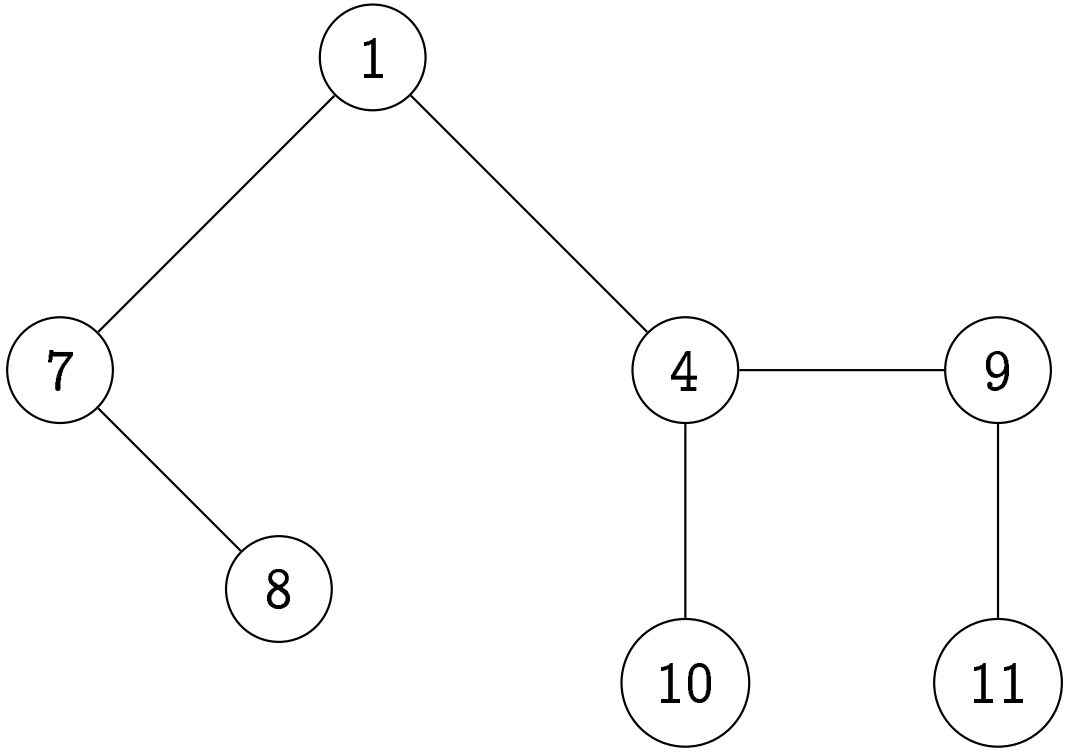
7 7

組合對應 – Prufer's code



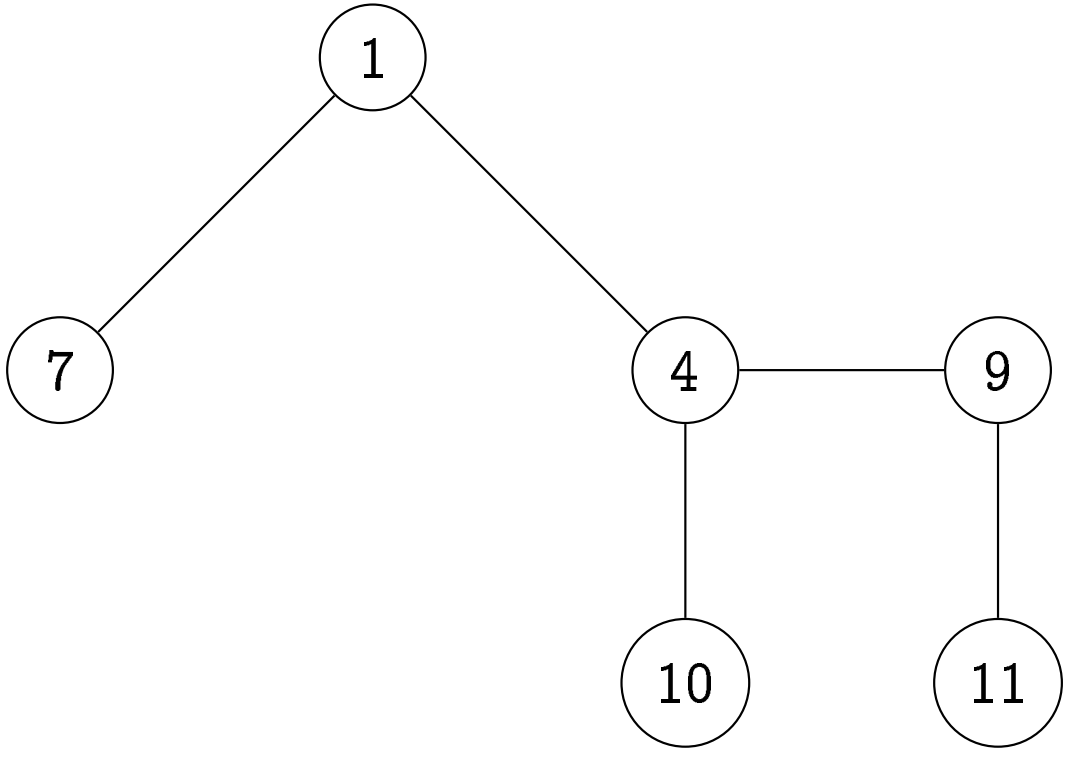
7 7 7

組合對應 – Prufer's code



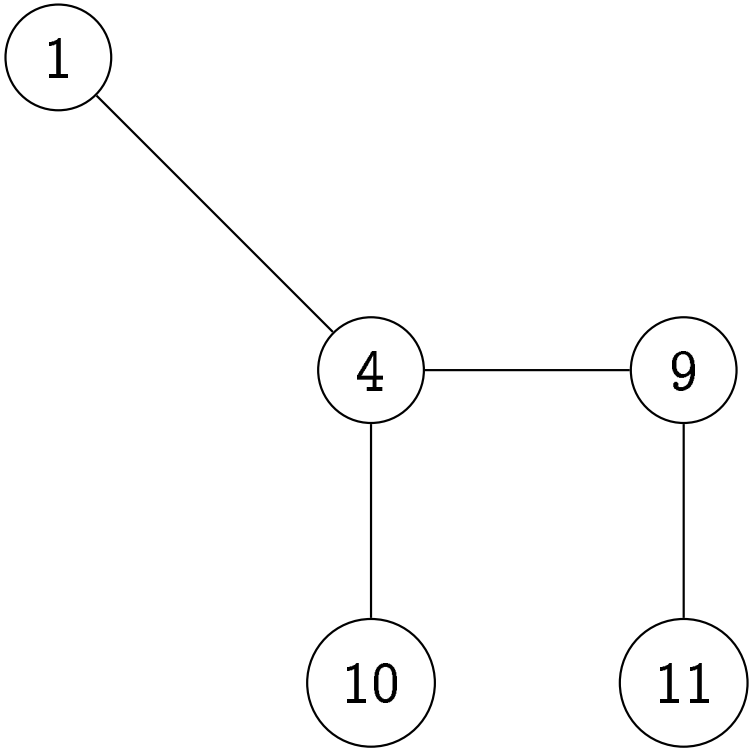
7 7 7 7

組合對應 – Prufer's code



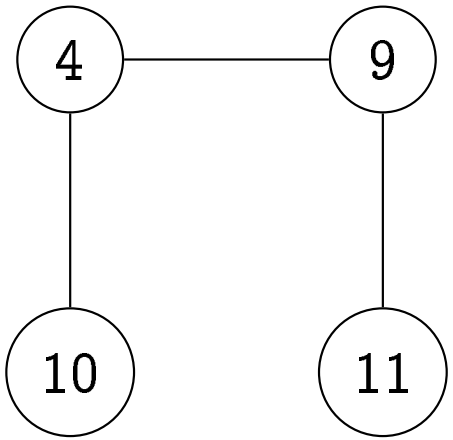
7 7 7 7 7

組合對應 – Prufer's code



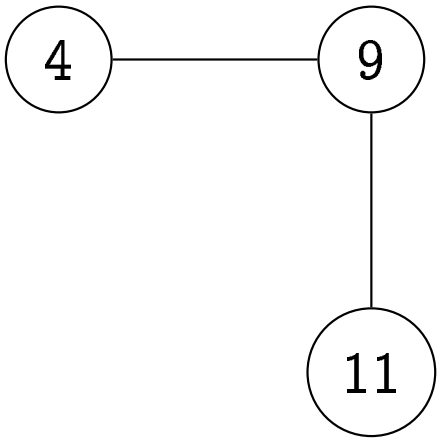
7 7 7 7 7 1

組合對應 – Prufer's code



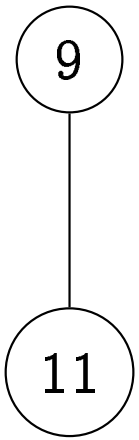
7 7 7 7 7 1 4

組合對應 – Prufer's code



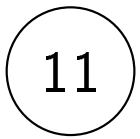
7 7 7 7 7 1 4 4

組合對應 – Prufer's code



7 7 7 7 7 1 4 4 9

組合對應 – Prufer's code



7 7 7 7 7 1 4 4 9 (11)

組合對應 – Prufer's code

7 7 7 7 7 1 4 4 9 (11)
2

組合對應 – Prufer's code

7 7 7 7 7 1 4 4 9 (11)
2 3

組合對應 – Prufer's code

7 7 7 7 7 1 4 4 9 (11)
2 3 5

組合對應 – Prufer's code

7	7	7	7	7	1	4	4	9	(11)
2	3	5	6						

組合對應 – Prufer's code

7	7	7	7	7	1	4	4	9	(11)
2	3	5	6	8					

組合對應 – Prufer's code

7	7	7	7	7	1	4	4	9	(11)
2	3	5	6	8	7				

組合對應 – Prufer's code

7	7	7	7	7	1	4	4	9	(11)
2	3	5	6	8	7	1			

組合對應 – Prufer's code

7	7	7	7	7	1	4	4	9	(11)
2	3	5	6	8	7	1	10		

組合對應 – Prufer's code

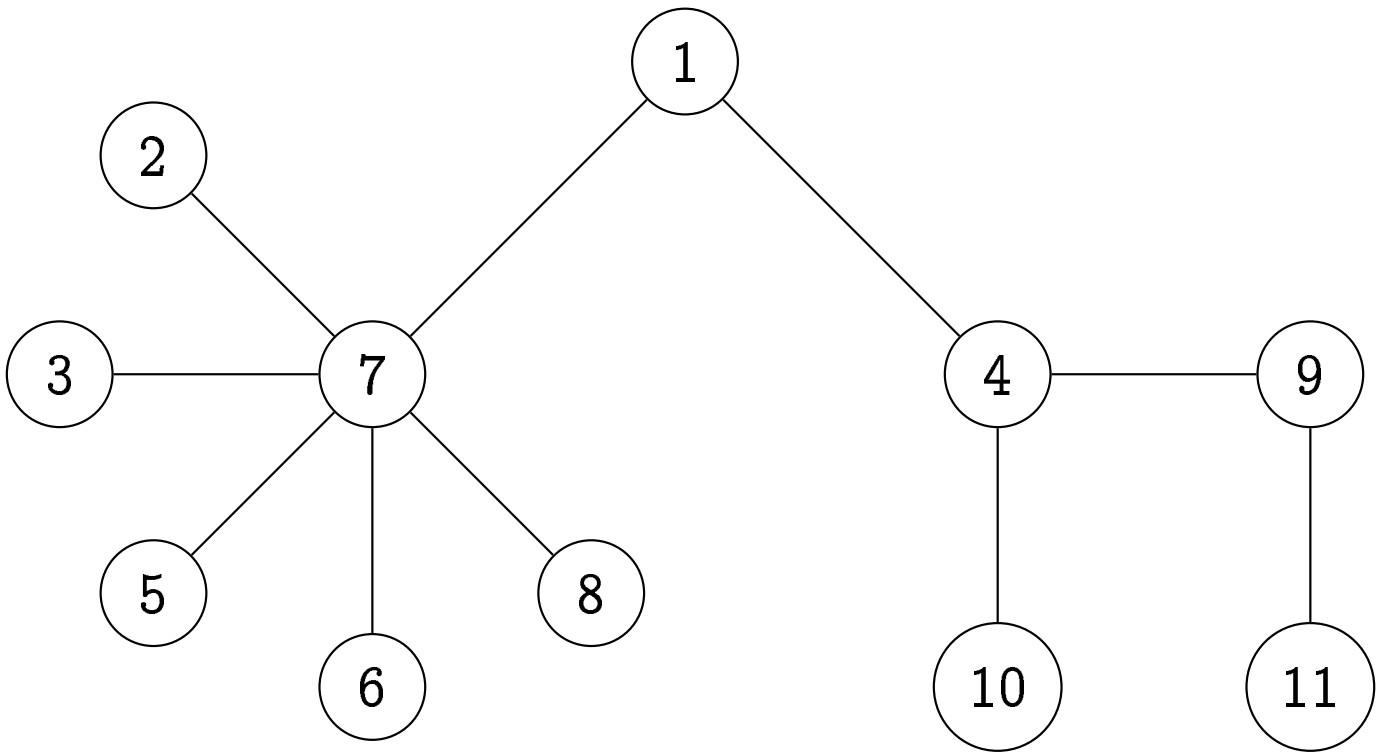
7	7	7	7	7	1	4	4	9	(11)
2	3	5	6	8	7	1	10	4	

組合對應 – Prufer's code

7	7	7	7	7	1	4	4	9	(11)
2	3	5	6	8	7	1	10	4	(9)

組合對應 – Prufer's code

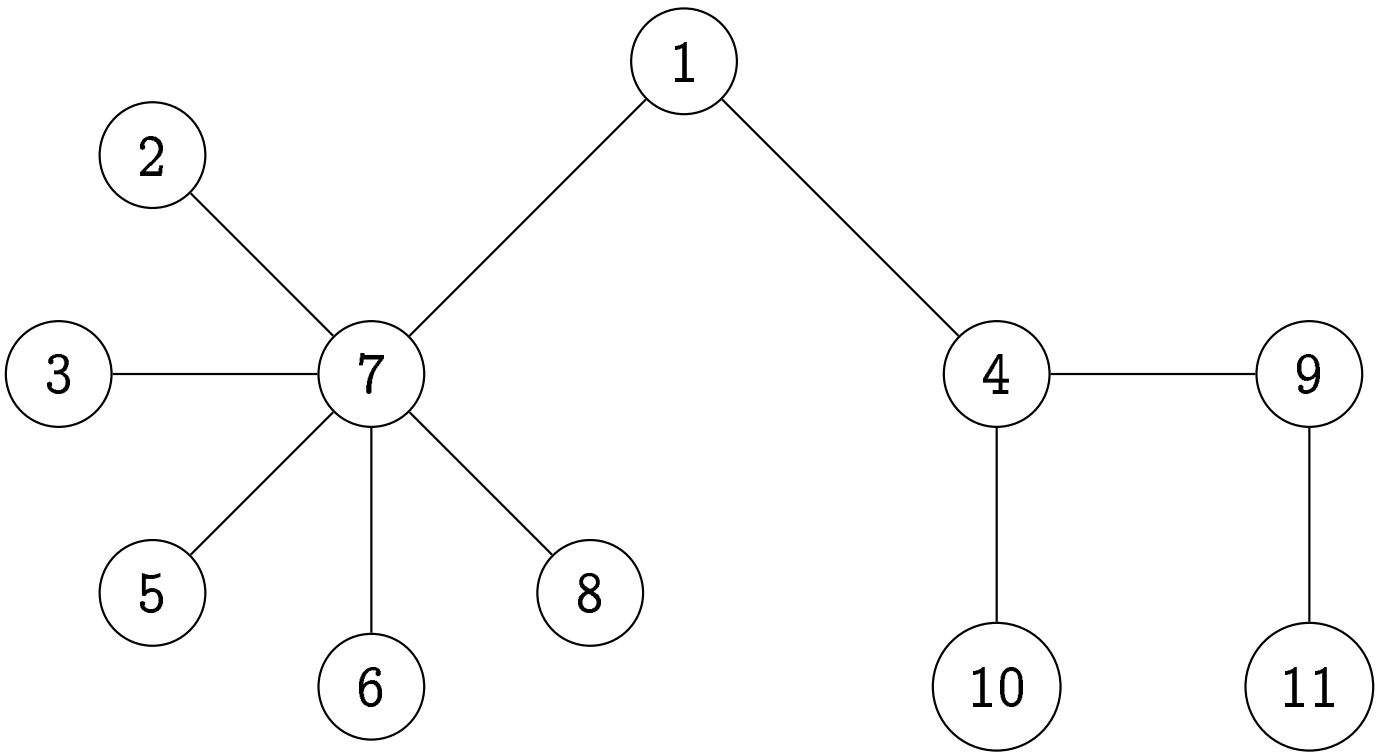
7	7	7	7	7	1	4	4	9	(11)
2	3	5	6	8	7	1	10	4	(9)



組合對應 – Prufer's code

7 7 7 7 7 1 4 4 9

↕



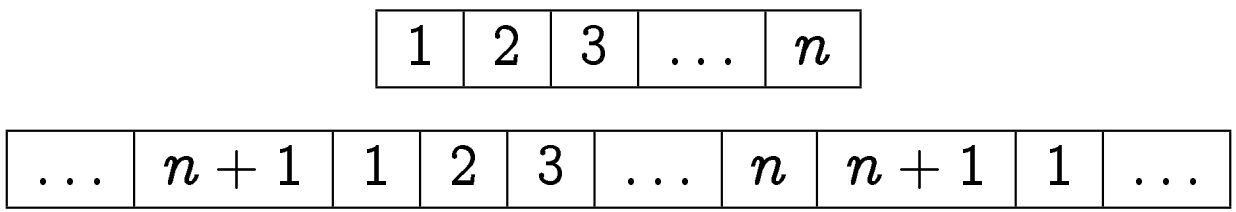
組合對應 – 停車問題

題目 (停車問題)

停車場有 n 個空的停車位，依序編號爲 $1, 2, \ldots, n$，有 n 台車想進去停車，第 i 台車想停在 p_i 這個位置，如果 p_i 這個位置已經有其他台車時，這台車就會開到 p_i 之後的第一個空位停車，如果 p_i 之後都沒有空位了這台車就會開出停車場。求有多少個 n 元數組 $(p_1, p_2, \ldots, p_n)$ 使得每一台車最終都會停在停車場中？

組合對應 – 停車問題

- 答案是 $(n+1)^{n-1}$。
- 加上第 $n+1$ 個停車位並將停車場變成環狀的。
- 調整 p_i 的值域：$p_i \in \{1, 2, \ldots, n+1\}$。
- 同樣是合法的定義不變。
- 合法 $\iff$ 最後第 $n+1$ 個停車位是空的。



組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2	3	4	5	6	7	8	9	10

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2	3	4	5	6	7	8	9 1	10

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2	3	4	5	6	7	8	9 1	10 2

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2 3	3	4	5	6	7	8	9 1	10 2

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2 3	3	4	5 4	6	7	8	9 1	10 2

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2 3	3	4	5 4	6 5	7	8	9 1	10 2

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2	3	4	5	6	7	8	9	10
6	3			4	5			1	2

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2	3	4	5	6	7	8	9	10
6	3	7		4	5			1	2

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2	3	4	5	6	7	8	9	10
6	3	7	8	4	5			1	2

組合對應 – 停車問題

$$(p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9) = (9, 10, 2, 5, 5, 9, 2, 2, 7)$$

1	2	3	4	5	6	7	8	9	10
6	3	7	8	4	5	9		1	2

組合對應 – 停車問題

$$(9+1, 10+1(=1), 2+1, 5+1, 5+1, 9+1, 2+1, 2+1, 7+1)$$

2	3	4	5	6	7	8	9	10	1
6	3	7	8	4	5	9		1	2

組合對應 – 停車問題

$$
\begin{array}{rrrrrrrrrl}
(9, & 10, & 2, & 5, & 5, & 9, & 2, & 2, & 7) & \text{空位8} \\
(10, & 1, & 3, & 6, & 6, & 10, & 3, & 3, & 8) & \text{空位9} \\
(1, & 2, & 4, & 7, & 7, & 1, & 4, & 4, & 9) & \text{空位10} \\
(2, & 3, & 5, & 8, & 8, & 2, & 5, & 5, & 10) & \text{空位1} \\
 & & & & \vdots & & & & & \\
(8, & 9, & 1, & 4, & 4, & 8, & 1, & 1, & 6) & \text{空位7}
\end{array}
$$

組合對應 – 停車問題

(9,	10,	2,	5,	5,	9,	2,	2,	7)	空位8
(10,	1,	3,	6,	6,	10,	3,	3,	8)	空位9
(1,	2,	4,	7,	7,	1,	4,	4,	9)	空位10
(2,	3,	5,	8,	8,	2,	5,	5,	10)	空位1
				⋮					
(8,	9,	1,	4,	4,	8,	1,	1,	6)	空位7

組合對應 – 停車問題

- $(n+1)^n$ 組 $(p_1, p_2, \ldots, p_n)$
- 每 $n+1$ 個分一類
- 每類有恰好一個是合法的
- $\frac{(n+1)^n}{n+1} = (n+1)^{n-1}$

組合對應 – 整數分割

題目 (整數分割)

整數分割是指將一個正整數分割成多個正整數的和，我們並不在乎分割後的正整數的順序。
舉例來說，4 有以下 5 種整數分割：

$$\begin{aligned} 4 &= 4 \\ &= 3+1 \\ &= 2+2 \\ &= 2+1+1 \\ &= 1+1+1+1 \end{aligned}$$

證明：將一個正整數的奇整數分割（即分割成多個正奇整數的和）的方法數 = 相異整數分割（即分割成多個相異整數的和）的方法數。

組合對應 – 整數分割

奇整數分割 $\rightarrow$ 相異整數分割：

$$3+3+3+3+3+5+5+5$$

組合對應 – 整數分割

奇整數分割 $\rightarrow$ 相異整數分割：

$$6 + 6 + 3 + 10 + 5$$

組合對應 – 整數分割

奇整數分割 $\rightarrow$ 相異整數分割：

$$12 + 3 + 10 + 5$$

組合對應 – 整數分割

相異整數分割 $\rightarrow$ 奇整數分割：

$$12 + 3 + 10 + 5$$

組合對應 – 整數分割

相異整數分割 $\rightarrow$ 奇整數分割：

$$6 + 6 + 3 + 10 + 5$$

組合對應 – 整數分割

相異整數分割 $\rightarrow$ 奇整數分割：

$$3+3+3+3+3+5+5+5$$

生成函數

普通生成函數 – 定義

定義

$$A(x) = \sum_{i=0}^{\infty} a_i x^i$$

稱爲 $\{a_i\}_{i=0}^{\infty}$ 的普通生成函數。

普通生成函數 – 公式

公式

$$A(x) = \sum_{i=0}^{\infty} \frac{A^{(i)}(c)}{i!}(x-c)^i = A(c) + A'(c)(x-c) + \frac{A''(c)}{2}(x-c)^2 + \cdots$$

將 c 帶 0 後即可得到

$$a_i = \frac{A^{(i)}(0)}{i!}$$

其中 $A(x)$ 不一定要在 c 的附近無窮可微，對於非無窮可微的則定義

$$A'(x) = \sum_{i=1}^{\infty} i a_i x^{i-1}$$

普通生成函數 – 常用性質

性質

一些普通生成函數的性質：

令 $A(x), B(x), C(x)$ 分別爲 $\{a_i\}_{i=0}^{\infty}, \{b_i\}_{i=0}^{\infty}, \{c_i\}_{i=0}^{\infty}$ 的普通生成函數

- $C(x) = A(x) + B(x),\ c_n = a_n + b_n$
- $C(x) = A(x)B(x),\ c_n = \sum_{i=0}^{n} a_i b_{n-i}$
- $B(x) = A(rx),\ b_n = r^n a_n$
- $B(x) = A(x)^r,\ b_n = \sum_{i_1+\cdots+i_k=n} a_{i_1} \cdots a_{i_k}$
- $B(x) = xA'(x),\ b_n = na_n$

普通生成函數 – 常見生成函數

公式

以下是一些常見的生成函數

- $a_n = \binom{m}{n}$ 的生成函數爲 $(1+x)^m$
- $a_n = r^n$ 的生成函數爲 $\frac{1}{1-rx} = 1 + rx + r^2x^2 + \cdots$
- $-\ln(1-x) = \sum_{i=1}^{\infty} \frac{1}{i} x^i$

其中 $\binom{m}{n}$ 的 m 不一定要是正整數，對於任意實數 $m \neq 0$，

$$\binom{m}{n} := \frac{m(m-1)\cdots(m-n+1)}{n!}$$

的生成函數也是 $(1+x)^m$。

普通生成函数 – 费氏数列

题目 (费氏数列)

求费氏数列的生成函数：$A(x) = \sum_{i=0}^{\infty} F_i x^i$。

普通生成函数 – 费氏数列

$$
\begin{array}{rrcccccccc}
 & A(x) & = & F_0 & + & F_1 x & + & F_2 x^2 & + & F_3 x^3 \\
 & -xA(x) & = & & - & F_0 x & - & F_1 x^2 & - & F_2 x^3 \\
+) & -x^2 A(x) & = & & & & - & F_0 x^2 & - & F_1 x^3 \\
\hline
 & (1-x-x^2)A(x) & = & F_0 & + & (F_1 - F_0)x & + & 0 & + & 0
\end{array}
$$

$$
\Rightarrow A(x) = \frac{F_0 + (F_1 - F_0)x}{1 - x - x^2} = \frac{x}{1 - x - x^2}
$$

普通生成函數 – 費氏數列

實際上，設 $\{a_i\}_{i=0}^{\infty}$ 有 k 階線性遞迴式

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

$$f(x) = \det\left(\begin{pmatrix} c_1 & c_2 & \cdots & c_{k-1} & c_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} - xI_k\right)$$

$$= x^k - c_1 x^{k-1} - c_2 x^{k-2} - \cdots - c_k$$

稱爲 $\{a_i\}_{i=0}^{\infty}$ 的特徵多項式。

普通生成函數 – 費氏數列

而生成函數

$$A(x) = \frac{g(x)}{x^k f(1/x)}$$

，其中 $\deg g(x) \leq k-1$，爲

$$(a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) x^k f(1/x)$$

的前 $k-1$ 項。

普通生成函數 – 卡特蘭數

題目 (卡特蘭數)

證明卡特蘭數第 n 項 $C_n = \frac{1}{n+1}\binom{2n}{n}$。

普通生成函數 – 卡特蘭數

設卡特蘭數的生成函數

$$A(x) = \sum_{i=0}^{\infty} C_i x^i$$

$A^2(x)$ 的 x^n 項係數爲

$$\sum_{i=0}^{n} C_i C_{n-i} = C_{n+1}$$

$$\Rightarrow x A^2(x) = \sum_{i=1}^{\infty} C_i x^i = A(x) - C_0 = A(x) - 1$$

$$\Rightarrow A(x) = \frac{1 \pm \sqrt{1-4x}}{2x}$$

普通生成函数 – 卡特蘭數

因爲

$$C_0 = \lim_{x \to 0} A(x)$$

而

$$\lim_{x \to 0^+} \frac{1 + \sqrt{1 - 4x}}{2x} = \infty$$

$$\lim_{x \to 0} \frac{1 - \sqrt{1 - 4x}}{2x} = \lim_{x \to 0} \frac{1 - 1 + 4x}{2x(1 + \sqrt{1 - 4x})} = 1$$

所以

$$A(x) = \frac{1 - \sqrt{1 - 4x}}{2x}$$

普通生成函数 – 卡特蘭數

計算 $A(x)$ 的 x^n 項係數，爲 $\frac{1-\sqrt{1-4x}}{2}$ 的 x^{n+1} 項係數，即爲：

$$\frac{1}{2}(-(-4)^{n+1}\binom{\frac{1}{2}}{n+1}) = -\frac{1}{2}(-4)^{n+1}\frac{\prod_{i=0}^{n}(\frac{1}{2}-i)}{(n+1)!}$$

$$= -2^n \cdot \frac{\prod_{i=0}^{n}(-1+2i)}{(n+1)!}$$

$$= 2^n \cdot \frac{\prod_{i=1}^{n}(2i-1)}{(n+1)!}$$

普通生成函数 – 卡特蘭數

$$
\begin{aligned}
&= \frac{\prod_{i=1}^{n} 2i}{\prod_{i=1}^{n} i} \cdot \frac{\prod_{i=1}^{n} (2i-1)}{(n+1)!} \\
&= \frac{(2n)!}{n!(n+1)!} \\
&= \frac{1}{n+1}\binom{2n}{n}
\end{aligned}
$$

普通生成函數 – 整數分割

題目 (整數分割)

證明：將一個正整數的奇整數分割（即分割成多個正奇整數的和）的方法數 = 相異整數分割（即分割成多個相異整數的和）的方法數。

普通生成函數 – 整數分割

設 a_n 是 n 的奇整數分割的方法數，b_n 是 n 的相異整數分割的方法數，$A(x)$ 是 a_n 的生成函數，$B(x)$ 是 b_n 的生成函數。

$$A(x) = (1 + x + x^2 + \cdots)(1 + x^3 + x^6 + \cdots)\cdots = \prod_{i=1}^{\infty} \frac{1}{1 - x^{2i-1}}$$

$$B(x) = (1 + x)(1 + x^2)(1 + x^3)\cdots = \prod_{i=1}^{\infty}(1 + x^i)$$

普通生成函数 – 整数分割

$$
\begin{aligned}
\frac{B(x)}{A(x)} &= \left(\prod_{i=1}^{\infty}(1+x^i)\right)\left(\prod_{i=1}^{\infty}(1-x^{2i-1})\right) \\
&= \left(\prod_{2\nmid i}(1+x^i)(1-x^i)\right)\left(\prod_{2\mid i}(1+x^i)\right) \\
&= \left(\prod_{2\mid i}(1+x^i)\right)\left(\prod_{i\equiv 2 \pmod 4}(1-x^i)\right) \\
&= \frac{B(x^2)}{A(x^2)} = \cdots = \frac{B(x^{2^k})}{A(x^{2^k})}
\end{aligned}
$$

普通生成函數 – 整數分割

因爲 $\forall n > 0$，

$$\frac{B(x)}{A(x)} = \frac{B(x^{2^{\lfloor \log_2 n \rfloor + 1}})}{A(x^{2^{\lfloor \log_2 n \rfloor + 1}})}$$

而其第 n 項係數爲 0，所以 $\frac{B(x)}{A(x)}$ 是常數函數，並且可以得到其常數項爲 1。

所以 $\frac{B(x)}{A(x)} = 1$，也就是 $A(x) = B(x)$。

$\therefore a_n = b_n$。

指數生成函數 – 定義

定義

$$A(x) = \sum_{i=0}^{\infty} \frac{a_i}{i!} x^i$$

稱爲 $\{a_i\}_{i=0}^{\infty}$ 的指數生成函數。

指數生成函數 – 例子

$1, 1, 1, \ldots$ 的普通生成函數：

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

$1, 1, 1, \ldots$ 的指數生成函數：

$$\sum_{i=0}^{\infty} 1 \cdot \frac{1}{i!} x^i = e^x$$

指數生成函數 – 公式

公式

$$A(x) = \sum_{i=0}^{\infty} A^{(i)}(c)(x-c)^i = A(c) + A'(c)(x-c) + A''(c)(x-c)^2 + \cdots$$

將 c 帶 0 後即可得到

$$a_i = A^{(i)}(0)$$

指數生成函數 – 一些性質

性質

一些指數生成函數的性質：

令 $A(x), B(x), C(x)$ 分別爲 $\{a_i\}_{i=0}^{\infty}, \{b_i\}_{i=0}^{\infty}, \{c_i\}_{i=0}^{\infty}$ 的指數生成函數

- $C(x) = A(x) + B(x),\ c_n = a_n + b_n$
- $C(x) = A(x)B(x),\ c_n = \sum_{i=0}^{n} \binom{n}{i} a_i b_{n-i}$
- $B(x) = A(rx),\ b_n = r^n a_n$
- $B(x) = A(x)^r,\ b_n = \sum_{i_1+\cdots+i_k=n} \frac{n!}{i_1!i_2!\cdots i_k!} a_{i_1} \cdots a_{i_k}$
- $B(x) = xA'(x),\ b_n = na_n$

指數生成函數 – Counting Sequence

題目 (2019ShangHai)

給定正整數 n, m，求有多少個 n 元正整數組 $(a_1, a_2, \ldots, a_n)$ 滿足 $\forall i,\ a_i \leq m$ 且 $\forall$ 偶數 $k,\ |\{i|a_i = k\}|$ 也是偶數。
$(n \leq 10^{18},\ m \leq 2 \times 10^5)$

指數生成函數 – Counting Sequence

先考慮另一個問題：如果 a_i 重新排列後算是相同的，那答案是多少？

令 $b_k = |\{i|a_i = k\}|$，每個 $(b_1, b_2, \ldots, b_m)$ 會唯一對應到一組 $\{a_1, a_2, \ldots, a_n\}$，而 b_{2k-1} 可以是 $0, 1, 2, 3, \ldots$，生成函數爲 $\frac{1}{1-x}$，b_{2k} 可以是 $2, 4, 6, 8, \ldots$，生成函數爲 $\frac{1}{1-x^2}$

所以

$$\prod_{i=1}^{m} \frac{1}{1 - x^{(i+1) \pmod 2 + 1}} = (1-x)^{-\lceil \frac{m}{2} \rceil}(1-x^2)^{-\lfloor \frac{m}{2} \rfloor}$$

$$= (1-x)^{-m}(1+x)^{-\lfloor \frac{m}{2} \rfloor}$$

的 x^n 項係數即爲答案。

指數生成函數 – Counting Sequence

回到原命題，$(b_1, b_2, \ldots, b_m)$ 會對應到 $\binom{n}{b_1, b_2, \ldots, b_m}$ 組 $(a_1, a_2, \ldots, a_n)$，也就是我們會在乎 b_i 個相同數字內部的排列以及最終 n 個數字的排列，所以此時如果將 b_i 對應到生成函數時在第 i 項多除一個階乘，即改爲指數生成函數，就可以解決這個問題。

指數生成函數 – Counting Sequence

b_{2k-1} 的生成函數是

$$1+x+\frac{x^2}{2}+\frac{x^3}{6}+\cdots=e^x$$

，b_{2k} 的生成函數是

$$1+\frac{x^2}{2}+\frac{x^4}{24}+\cdots=\frac{e^x+e^{-x}}{2}$$

所以

$$(e^x)^{\lceil\frac{m}{2}\rceil}(\frac{e^x+e^{-x}}{2})^{\lfloor\frac{m}{2}\rfloor}$$

的 x^n 項係數乘上 $n!$ 即爲答案。

指數生成函數 – Counting Sequence

令 $k = \lfloor \frac{m}{2} \rfloor$，

$$
\begin{aligned}
e^{m-k}\left(\frac{e^x + e^{-x}}{2}\right)^k &= 2^{-k} \sum_{i=0}^{k} \binom{k}{i} e^{(m-k)x} e^{(k-2i)x} \\
&= 2^{-k} \sum_{i=0}^{k} \binom{k}{i} e^{(m-2i)x} \\
&= 2^{-k} \sum_{i=0}^{k} \binom{k}{i} \sum_{j=0}^{\infty} (m-2i)^j \frac{x^j}{j!} \\
&= 2^{-k} \sum_{j=0}^{\infty} \sum_{i=0}^{k} \binom{k}{i} (m-2i)^j \frac{x^j}{j!}
\end{aligned}
$$

指數生成函數 – Counting Sequence

所以最終答案即爲

$$2^{-k}\sum_{i=0}^{k}\binom{k}{i}(m-2i)^n$$

群論

基礎定義 – 運算的專有名詞

定義

S 是一個集合，$\circ$ 是一個定義在 S 上的二元運算。

- 封閉：$\forall a, b \in S,\ a \circ b \in S$。
- 結合律 (associative law)：$\forall a, b, c \in S,\ (a \circ b) \circ c = a \circ (b \circ c)$。
- 交換律 (commutative law)：$\forall a, b \in S,\ a \circ b = b \circ a$。
- 單位元素 (identity)：若 $\forall a \in S,\ b \circ a = a \circ b = a$，則稱 b 爲單位元素，通常以 1 表示單位元素，或者是在 $\circ = +$ 時以 0 表示。
- 反元素 (inverse)：若 $a, b \in S,\ a \circ b = b \circ a = 1$，則稱 b 是 a 的反元素，寫作 $b = a^{-1}$。

基礎定義 – 運算的專有名詞

- 當 $\circ \neq +$ 時，會直接省略不寫，也就是會以 ab 表示 $a \circ b$。
- 假設 $\circ$ 是有結合律的運算。

基礎定義 – 單位元素與反元素的性質

性質

(1) 若 $\forall a,\ 1_L a = a,\ a 1_R = a$，則 $1_L = 1_R$。
(2) 若 $a b_R = b_L a = 1$，則 $b_L = b_R$。

基礎定義 – 單位元素與反元素的性質

證明：

(1) $1_L = 1_L 1_R = 1_R$。

(2) $b_L = b_L 1 = b_L a b_R = 1 b_R = b_R$。

基礎定義 – 單位元素與反元素的性質

- 單位元：1，因爲單位元素存在即唯一。
- 1 跟任何元素都可交換。
- a 的反元素：a^{-1}，因爲反元素存在即唯一。
- a^{-1} 跟 a 可交換。

基礎定義 – 單位元素與反元素的性質

例子 (經典題)

設 A, B 爲兩方陣滿足 $A + B = AB$，證明 $AB = BA$。

基礎定義 – 單位元素與反元素的性質

證明：

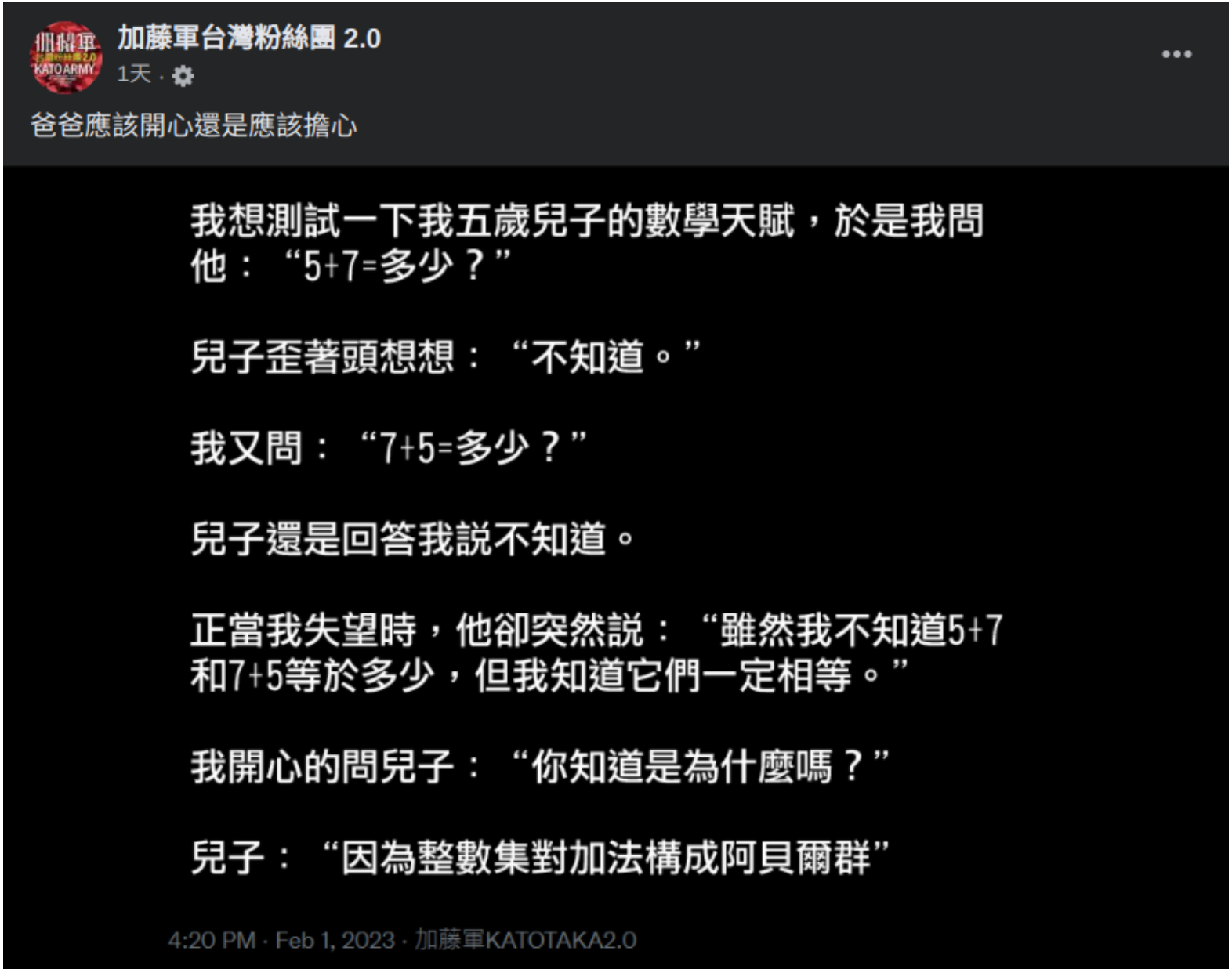
$$
\begin{aligned}
& A + B = AB \\
\Rightarrow & AB - A - B = 0 \\
\Rightarrow & AB - A - B + I = I \\
\Rightarrow & (A - I)(B - I) = I \\
\Rightarrow & (B - I)(A - I) = I \\
\Rightarrow & BA - A - B + I = I \\
\Rightarrow & BA = A + B = AB
\end{aligned}
$$

基礎定義 – 群

定義

若集合 S 與 S 上的二元運算 $\circ$ 在 S 中封閉，且有結合律、單位元素、反元素，則稱爲一個群 (group)。通常以 G 來表示一個群，並寫做 $G = (S, \circ)$。
若 $\circ$ 有交換律，則稱 G 是一個交換群，或說是阿貝爾群 (abelian group)。

基礎定義 – 群


加藤軍台灣粉絲團 2.0
1天 ·
爸爸應該開心還是應該擔心
我想測試一下我五歲兒子的數學天賦，於是我問他：“5+7=多少？”
兒子歪著頭想想：“不知道。”
我又問：“7+5=多少？”
兒子還是回答我說不知道。
正當我失望時，他卻突然說：“雖然我不知道5+7和7+5等於多少，但我知道它們一定相等。”
我開心的問兒子：“你知道是為什麼嗎？”
兒子：“因為整數集對加法構成阿貝爾群”
4:20 PM · Feb 1, 2023 · 加藤軍KATOTAKA2.0

基礎定義 – 各種群

- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\{1, -1\}, \cdot)$ 都是交換群。
- $(\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot), (\mathbb{C}, \cdot)$ 都不是群。
- $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ 分別定義成 $\mathbb{Q} - 0, \mathbb{R} - 0, \mathbb{C} - 0$，這三個集合配上 $\cdot$ 運算都是交換群。
- $(M_{2\times 2}^*, \cdot)$ 不是交換群。（$M_{2\times 2}$ 是指所有 2×2 矩陣的集合，而 $M_{2\times 2}^*$ 則是指所有可逆 2×2 矩陣的集合）

基礎定義 – 小引理

引理

若 $\forall a, b \in G,\ ab^{-1} \in G$，則 G 是一個群。

基礎定義 – 序

定義

- $|G|$：G 中元素的個數，稱作 G 的序 (order)。
- $|g|$：設 n 爲最小的正整數使得 $g^n = 1$，則 $|g| := n$，稱作 g 的序。當不存在這樣的正整數 n 時，定義 $|g| = \infty$。

基礎定義 – 序

性質

若 $|G|$ 有限，且 $\circ$ 在 G 中封閉，則 G 是一個群。

基礎定義 – 序

證明：
$\forall g \in G$，$|g| \leq |G|$ 有限，所以存在正整數 n 使得 $g^n = 1$
$\Rightarrow gg^{n-1} = 1$
$\Rightarrow g^{n-1} = g^{-1}$
因爲 $\circ$ 封閉，所以 $g^{n-1} \in G$
$\therefore \forall g, h \in G,\ g, h^{-1} \in G$，因爲 $\circ$ 封閉，所以 $gh^{-1} \in G$。

基礎定義 – 循環群

定義

- 若存在 $g \in G$ 使得 $G = \{g^n | n \in \mathbb{Z}\}$，則稱 G 是循環群 (cyclic group)，g 是 G 的生成元 (generator)，寫做 $G =< g >$。
- 若存在 $S \subseteq G$ 使得 $G = \{\prod_{s \in S} s^{n_s} | n_s \in \mathbb{Z}\}$，則稱 S 是 G 的生成集，寫做 $G =< S >$ 或 $G =< s_1, s_2, \ldots, >$。

基礎定義 – 循環群

- $(\mathbb{Z}_n, +)$ 是一個循環群，其中滿足 $\gcd(a, n) = 1$ 的 a 都是生成元。（$\mathbb{Z}_n$ 是指所有除以 n 的餘數所形成的集合，加法的定義則是相加之後取餘數）
- $(\mathbb{Z}, +)$ 也是一個循環群，其中 $1, -1$ 是生成元。
- $(\mathbb{Q}, +)$ 不是循環群，有生成集 $\{\frac{1}{p} | p \in \mathbb{P}\}$。

基礎定義 – 循環群

性質

循環群是交換群。

基礎定義 – 循環群

證明：

設 $G = < g >$ 是循環群。

$\forall a, b \in G$，設 $a = g^c, b = g^d$

$ab = g^c g^d = g^{c+d} = g^d g^c = ba$

所以 G 是交換群。

基礎定義 – 子群

定義

若 $H \subseteq G$ 且 H 是一個群，則稱 H 是 G 的子群 (subgroup)，寫做 $H \leq G$。

基礎定義 – 子群

$(n\mathbb{Z}, +)$ 是 $(\mathbb{Z}, +)$ 的一個子群。(其中 $n\mathbb{Z} := \{nm | m \in \mathbb{Z}\}$ 爲所有 n 的倍數的集合)

基礎定義 – 餘集

定義

$H \leq G$

- $gH := \{gh | h \in H\}$ 稱爲 H 的左餘集 (left coset)，
  $Hg := \{hg | h \in H\}$ 稱爲 H 的右餘集 (right coset)。
- $G/H := \{gH | g \in G\}$，所有左餘集所形成的集合。

基礎定義 – 餘集

$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$，也就是所有除以 n 的餘數所形成的集合，另外也把 $\mathbb{Z}/n\mathbb{Z}$ 寫做 $\mathbb{Z}_n$。

基礎定義 – 餘集

引理

$H \leq G$
(1) 若 G 有限，則 $\forall g \in G,\ |gH| = |H|$
(2) $\forall g_1, g_2 \in G$，若 $g_1 H \cap g_2 H \neq \emptyset$，則 $g_1 H = g_2 H$
(3) 若 G 有限，則 $|H| \mid |G|$

基礎定義 – 餘集

證明： (1) 定義函數 $f_1 : H \to gH,\ f_1(x) := gx$，$f_2 : gH \to H,\ f_2(x) := g^{-1}x$。可以發現 $\forall h \in H,\ (f_2 \circ f_1)(h) = g^{-1}gh = h$，所以 f_1, f_2 互爲反函數，因此 f_1 是雙射函數 H 與 gH 間的雙射函數，於是有 $|H| = |gH|$。

基礎定義 – 餘集

證明： (2) 設 $g_1H \cap g_2H \neq \emptyset$，也就是存在 $h_1, h_2 \in H$ 使得 $g_1h_1 = g_2h_2$

$\Rightarrow g_2^{-1}g_1 = h_2h_1^{-1} \in H$

$\forall g_1h_3 \in g_1H$

$$g_1h_3 = g_2g_2^{-1}g_1h_3 = g_2(h_2h_1^{-1}h_3) \in g_2H$$

所以有 $g_1H \subseteq g_2H$，反之亦然

$\therefore g_1H = g_2H$

基礎定義 – 餘集

證明： (3) 因爲 $1 \in H$，所以 $\bigcup_{g \in G} gH = G$

由 (2) 知：可以取出 G 中的某些元素 $S = \{g_1, g_2, \ldots, g_n\}$ 使得 $\forall 1 \leq i < j \leq n,\ g_i H \cap g_j H = \emptyset$ 且 $\forall g \in G - S$，存在 i 使得 $gH = g_i H$。

由 (1) 知：

$$|G| = |\bigcup_{g \in S} gH| = \sum_{g \in S} |gH| = \sum_{g \in S} |H| = |S||H| = |G/H||H|$$

所以

$$|H| \mid |G|$$

基礎定義 – Lagrange's theorem

定理 (Lagrange's theorem)

設 G 有限且 $H \leq G$，則 $|G| = |H||G/H|$。

基礎定義 – Lagrange's theorem

推論

設 G 有限，則

(1) $\forall g \in G,\ |g| \mid |G|$

(2) $\forall g \in G,\ g^{|G|} = 1$

基礎定義 – Lagrange's theorem

- $(\mathbb{Z}_n^*, \cdot)$ 是指除以 n 的餘數的乘法群，即所有跟 n 互質的餘數所形成的群。
- 透過上個定理可以直接推得之後數論會講的歐拉定理

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

基礎定義 – 子群性質

性質

設 $H \leq G, K \leq G$，則 $H \cap K \leq G$。

基礎定義 – 子群性質

證明：
設 $g_1, g_2 \in H \cap K$，因爲 $g_1 g_2^{-1} \in H, g_1 g_2^{-1} \in K$，所以 $g_1 g_2^{-1} \in H \cap K$
$\therefore H \cap K \leq G$。

基礎定義 – 子群性質

定理

設 $H \leq G, K \leq G$，則

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

，其中 $HK := \{hk | h \in H, k \in K\}$。

基礎定義 – 子群性質

證明： 注意到 $HK = \bigcup_{h \in H} hK$，且 $|hK| = |K|$，又因爲 $h \in G$，所以

$$h_1 K \cap h_2 K \neq \emptyset \iff h_1 K = h_2 K$$

基礎定義 – 子群性質

證明： 因爲

$$\begin{aligned} h_1K = h_2K &\iff h_2^{-1}h_1 \in K \\ &\iff h_2^{-1}h_1 \in H \cap K \\ &\iff h_1(H \cap K) = h_2(H \cap K) \end{aligned}$$

所以

$$\begin{aligned} |\{hK|h \in H\}| &= |\{h(H \cap K)|h \in H\}| \\ &= |H/(H \cap K)| \\ &= \frac{|H|}{|H \cap K|} \end{aligned}$$

基礎定義 – 子群性質

證明： 因此

$$|HK| = |K||H/(H \cap K)| = \frac{|H||K|}{|H \cap K|}$$

一些群 – Dihedral group

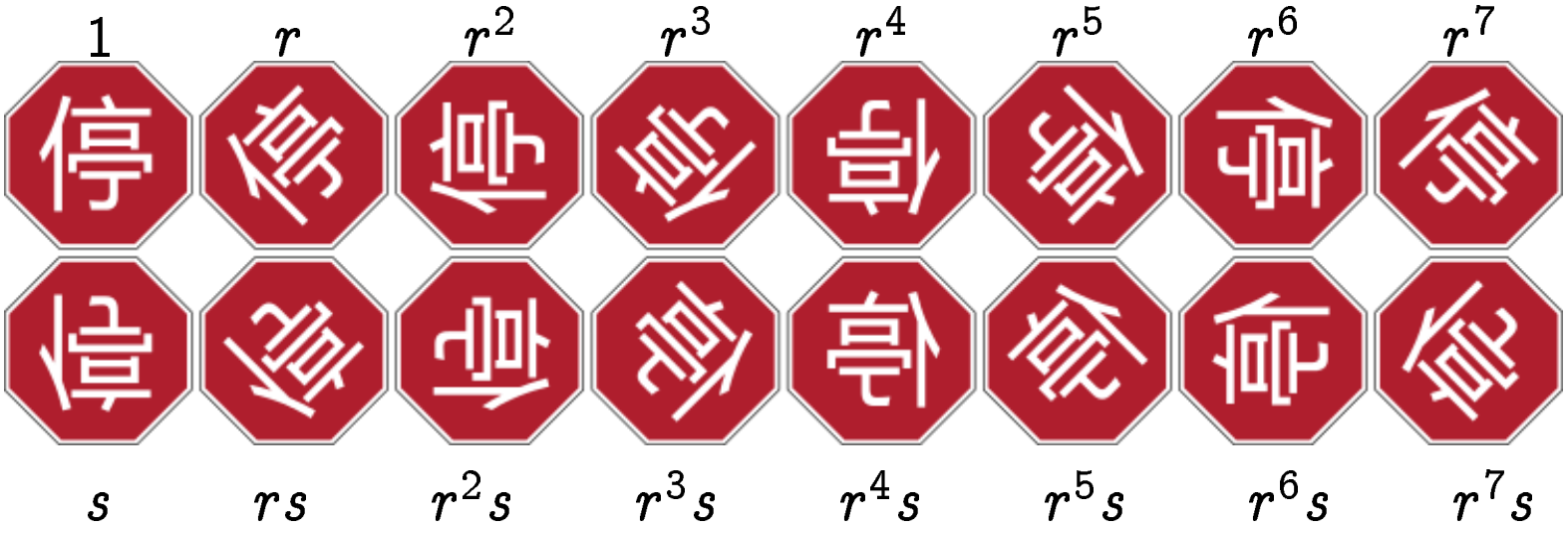
定義

設 G 是由所有旋轉與鏡射一個正 n 邊形但看不出改動的旋轉與鏡射所形成的群，群中的運算爲操作的合成，這個群稱作 Dihedral group，寫作 D_{2n}。

一些群 – Dihedral group

舉例來說，設 L 是一條正 n 邊形的對稱軸，r 是逆時針旋轉 $\frac{2\pi}{n}$，s 是對 L 作鏡射，則 rs 是指鏡射後逆時針旋轉 $\frac{2\pi}{n}$ 的操作。

可以發現對 L 做兩次鏡射跟沒做一樣，也就是 $s^2 = 1$。



（圖片來源：維基百科）

一些群 – Dihedral group

性質

$$D_{2n} =< r, s | r^n = s^2 = (sr)^2 = 1 >$$

一些群 – 排列群

定義

設 G 是由所有 $1, 2, \ldots, n$ 的排列所形成的群，排列可以看成是一個 $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ 的函數，群中的運算是排列函數的合成，這個群稱作對稱群 (Symmetric group)，寫作 S_n。

一些群 – 排列群

計算 $231 \circ 132$，即先把 $(1,2,3)$ 打到 $(1,3,2)$ 再把 $(1,2,3)$ 打到 $(2,3,1)$，所以

1 會先被打到 1 再被打到 2、
2 會先被打到 3 再被打到 1、
3 會先被打到 2 再被打到 3，

因此 $231 \circ 132 = 213$。

可以發現 $123\cdots n$ 相當於什麼都沒做的排列，也就是 $1(\text{identity}) = 123\cdots n$。

一些群 – 排列群

定義

設 $\sigma \in S_n$，若 $i \neq j,\ \sigma_i = j,\ \sigma_j = i,\ \forall k \neq i, j,\ \sigma_k = k$，則稱 σ 是一個 i, j 的置換，寫作 $\sigma = (ij)$。

一些群 – 排列群

性質

$$S_n = < (ij) | 1 \leq i < j \leq n >$$

一些群 – 排列群

性質

$$S_n = < (1i) | i \neq 1 >$$

群作用 – 名詞定義

定義

一個群 G 與一個集合 A 上的群作用 (group action) 是指滿足以下條件的一個運算 $\circ : G \times A \to A$：

- $\forall g_1, g_2 \in G, a \in A,\ (g_1 g_2) \circ a = g_1 \circ (g_2 \circ a)$
- $\forall a \in A,\ 1 \circ a = a$

群作用 – 名詞定義

定義

- $G_a := \{g \in G | ga = a\}$，稱爲 a 的 stabilizer
- $Ga := \{ga | g \in G\}$，稱爲 a 的軌道 (orbit)
- $A/G := \{Ga | a \in A\}$，爲所有軌道的集合
- $A^g := \{a \in A | ga = a\}$

群作用 – 小引理

引理

設 G 有限，則 $\forall a \in A$

$$|G| = |G_a||Ga|$$

群作用 – 小引理

證明： $\forall g_1, g_2 \in G_a$

$$g_1 g_2^{-1} a = g_1 g_2^{-1} g_2 a = g_1 a = a$$

所以 $G_a \leq G$。
$\forall g_1, g_2 \in G$

$$\begin{aligned} g_1 a = g_2 a &\iff g_1 g_2^{-1} a = a \\ &\iff g_1 g_2 - 1 \in G_a \\ &\iff g_1 g_2 - 1 = G_a \\ &\iff g_1 G_a = g_2 G_a \end{aligned}$$

群作用 – 小引理

證明： 所以

$$|\{ga|g \in G\}| = |\{gG_a|g \in G\}|$$

$\Rightarrow$ 由 Lagrange's theorem，

$$|G_a||Ga| = |G_a||G/G_a| = |G|$$

群作用 – Burnside's lemma

定理 (Burnside's lemma)

設 G 爲有限群，則

$$|A/G||G| = \sum_{g \in G} |A^g|$$

群作用 – Burnside's lemma

證明：

$$\begin{aligned}
\sum_{g\in G}|A^g| &= |\{(g,a)\in G\times A | ga=a\}| \\
&= \sum_{a\in A}|G_a| \\
&= \sum_{a\in A}\frac{|G|}{|Ga|} \\
&= \sum_{B\in A/G}\sum_{a\in B(=G_a)}\frac{|G|}{|Ga|} \\
&= \sum_{B\in A/G}\frac{|G|}{|B|}\cdot|B| \\
&= |A/G||G|
\end{aligned}$$

群作用 – 環狀塗色

例子 (環狀塗色)

有一條項鍊由 n 個寶石串成，其中有至多 m 種不同的寶石，因爲項鍊是環狀的，所以旋轉視爲相同的，請問有多少種不同的項鍊？

群作用 – 環狀塗色

首先假設旋轉視爲不同的，爲了避免混淆，我們說兩條項鍊是相異的如果在旋轉視爲不同時是相異的，而兩條項鍊是屬於同一種項鍊如果兩者旋轉後相同。

令 A 爲所有項鍊所形成的集合，G 爲所有旋轉所形成的群。

那麼 A/G 即爲所有項鍊的種類所形成的集合，因爲

兩條項鍊會被放在同個軌道上 $\iff$ 兩條項鍊之間是一個旋轉

$\iff$ 兩條項鍊是屬於同一種

群作用 – 環狀塗色

令逆時針旋轉一格的操作爲 g，可以知道

$$G =< g >= \{1, g, \ldots, g^{n-1}\}$$

設 $a \in A$ 爲一條項鍊，以 a_i 代表代表項鍊上第 i 個寶石的種類。

接下來我們來計算 A^{g^k}，若 $a \in A^{g^k}$，則
$\forall x \in \mathbb{Z},\ g^{xk} = (g^k)^x a = a$。

另外 $g^n a = 1a = a$。

所以

$$a \in A^h \iff h \in < g^k >= g^{<k,n>} = \{g^x | x \in k\mathbb{Z} + n\mathbb{Z}\}$$

群作用 – 環狀塗色

而 Bézout's theorem 告訴我們

$$k\mathbb{Z} + n\mathbb{Z} = \gcd(k, n)\mathbb{Z}$$

所以

$$\begin{aligned} a \in A^h &\iff h \in \{g^x | x \in \gcd(k, n)\mathbb{Z}\} \\ &\iff h = g^{\gcd(k,n)x} \end{aligned}$$

對於某個整數 x。

群作用 – 環狀塗色

因此，對於每個 $r \in \{0, 1, \ldots, \gcd(k, n) - 1\}$，都可以自由的選擇

$a_r, a_{r+\gcd(k,n)}, a_{r+2\gcd(k,n)}, \ldots$ 要共同有什麼顏色。

所以 a 有 $m^{\gcd(k,n)}$ 種選擇，即

$$|A^{g^k}| = m^{\gcd(k,n)}$$

群作用 – 環狀塗色

由 Burnside's lemma 知：

$$
\begin{aligned}
|A/G| &= \frac{1}{|G|}\sum_{g\in G}|A^g| \\
&= \frac{1}{n}\sum_{k\in\mathbb{Z}_n}|A^{g^k}| \\
&= \frac{1}{n}\sum_{k\in\mathbb{Z}_n} m^{\gcd(k,n)} \\
&= \frac{1}{n}\sum_{d|n}\sum_{\gcd(k,n)=d} m^d \\
&= \frac{1}{n}\sum_{d|n}\varphi(\frac{n}{d})m^d
\end{aligned}
$$

群作用 – 環狀排列習題

題目 (有鏡射的環狀塗色)

有一條項鍊由 n 個寶石串成，其中有至多 m 種不同的寶石，因爲項鍊是一個環，所以正面看反面看視爲相同的，且旋轉也視爲相同的，請問有多少種不同的項鍊？

證明： Hint：考慮 A/D_{2n}。

數論

同餘 – 整除

定義

設 a, b 爲整數，$a \neq 0$，若存在整數 c 使得 $b = ac$，則稱 a 整除 b，寫成：

$$a|b$$

這個定義在群論中就是 $a|b := b \in a\mathbb{Z}$。

同餘 – 同餘

定義

設 n, a, b 爲整數，$n \neq 0$，若 $n|a-b$，則稱 a 同餘 b 模 n，寫成：

$$a \equiv b \pmod{n}$$

這個定義在群論中就是 $a - b \in n\mathbb{Z}$。

同餘 – 同餘運算

性質

設 n, a, b 爲整數，$n \neq 0$，若 $n|a$, $n|b$，則 $\forall c, d \in \mathbb{Z}$，

$$n|ac + bd$$

同餘 – 同餘運算

證明：

$n|a, n|b$

$\Rightarrow$ 根據整除定義 $\exists x, y \in \mathbb{Z}$ s.t. $a = nx, b = ny$

$\Rightarrow ac + bd = cnx + dny = n(cx + dy)$

$\Rightarrow$ 根據整除定義 $n|ac + bd$。

同餘 – 同餘運算

$n\mathbb{Z}$ 是封閉的，並且是一個 $\mathbb{Z}$ 的子群。

同餘 – 同餘運算

性質

若 $a \equiv c \pmod{n}$, $b \equiv d \pmod{n}$，則：

$$(1)\ a + b \equiv c + d \pmod{n}$$
$$(2)\ a - b \equiv c - d \pmod{n}$$
$$(3)\ ab \equiv cd \pmod{n}$$

同餘 – 同餘運算

證明：

根據同餘定義 $n|a-c,\ n|b-d$

(1)

$$n|(a-c)+(b-d)=(a+b)-(c+d)$$
$$\Rightarrow a+b\equiv c+d \pmod{n}$$

(2)

$$n|(a-c)-(b-d)=(a-b)-(c-d)$$
$$\Rightarrow a-b\equiv c-d \pmod{n}$$

(3)

$$n|(a-c)b+(b-d)c=ab-bc+bc-cd=ab-cd$$
$$\Rightarrow ab\equiv cd \pmod{n}$$

同餘 – 計算問題

數論中：模之前做加法減法乘法 = 模之後做加法減法乘法。
程式中：不一定。
原因：

1. 溢位問題
   - int、long long 有可能會溢位
   - 先取模再做乘法再取模乘法的量級會較原先的小，可以減少溢位的發生
   - $a * b \% n \to (a \% n) * (b \% n) \% n$
2. 程式中的模並非餘數
   - 除法：向 0 取整而非向下取整
   - $9/4$ 是 2.25，向下取整與向 0 取整之後都是 2
   - $(-9)/4$ 是 -2.25，向下取整是 -3，但向 0 取整是 -2
   - $a \% b := a - (a/b) * b$，即拿 a/b 當作商去計算餘數，當商是向 0 取整但不是向下取整時，$a \% b$ 就會輸出負數而非 $\{0, 1, \ldots, b-1\}$ 中的餘數。
   - $9 \% 4 = 1$，$(-9) \% 4 = -1$。

同餘 – 快速冪

求 $a^b \% n$：

- 一個一個慢慢乘：$O(b)$
- 使用快速冪：$O(\log b)$
- 將 b 寫成 2 進位的型式 $b = (b_k b_{k-1} \cdots b_0)_2$
- 接著讓 i 從 0 跑到 k，如果 b_i 是 1 那就讓結果乘上 a^{2^i}，而 a^{2^i} 可以從 $a^{2^i} = a^{2^{i-1}} \times a^{2^{i-1}}$ 前一項推得。

同餘 – 快速冪

舉例：計算 $2^{100}\%19$

$100 = (1100100)_2$

i	0	1	2	3	4	5	6
b_i	0	0	1	0	0	1	1
2^i	1	2	4	8	16	32	64
2^{2^i}	2	4	16	9	5	6	17
ans	1	1	16	16	16	1	17

同餘 – 快速冪

```
1  #define ll long long
2  // 因爲通常模數是 int 量級的，所以要開 long long 才能避免乘法溢位
3  ll fpow(ll a, ll b, ll n){ // 計算 a^b%n
4      ll r=1;
5      for(; b; b>>=1, a=a*a%n)if(b&1)r=r*a%n;
6      return r;
7  }
```

質數與最大公因數 – 定義

定義

- a, b 爲整數且 $a \neq 0$，若 $a|b$，則稱 a 是 b 的因數。
- 若 c 同時是 a, b 的因數則稱 c 是 a, b 的公因數。
- a, b 是不全爲 0 的整數，a, b 的最大公因數寫成：$\gcd(a, b)$。
- 若 $p > 1$ 且 p 的正因數只有 $1, p$，則稱 p 爲質數。

如果沒有特別說明，p 就是一個質數。

質數與最大公因數 – 挨氏篩

```
1  bool prime[kN]={0};
2
3  void eratosthenes(){
4      for(int i=2; i<kN; ++i)prime[i]=1;
5      for(int i=2; i<kN; ++i)if(prime[i])
6          for(int j=i*i; j<kN; j+=i)prime[j]=0;
7  }
```

質數與最大公因數 – 質數個數

定義

$\pi(x) :=$ 小於等於 x 的質數個數。

質數與最大公因數 – 質數個數

舉例來說，$\pi(10) = 4$，因爲 $2, 3, 5, 7 \leq 10$；$\pi(13) = 6$，因爲 $2, 3, 5, 7, 11, 13 \leq 13$。

質數與最大公因數 – 質數個數

定理 (質數定理)

$$\pi(n) \sim \frac{n}{\log n}$$

質數與最大公因數 – 質數個數

定理 (質數倒數和)

$$\sum_{p \le n} \frac{1}{p} = \Theta(n \log \log n)$$

質數與最大公因數 – 線性篩

```cpp
int d[kN]; // 最小質因數
vector<int> prime;

void linearSieve(){
    for(int i=2; i<kN; ++i){
        if(!d[i])prime.push_back(i), d[i]=i;
        for(int p:prime){
            if(i*p>=kN)break;
            d[i*p]=p;
            if(i%p==0)break;
        }
    }
}
```

質數與最大公因數 – 積性函數

定義

設 $f : \mathbb{N} \to \mathbb{N}$ 滿足 $\forall \gcd(a, b) = 1$

$$f(ab) = f(a)f(b)$$

則稱 f 是積性函數。

積性函數也可以用類似線性篩的方法建表。

可參考進階數學講義。

質數與最大公因數 – 輾轉相除法

性質

$\forall k \in \mathbb{Z}$，

$$\gcd(a, b) = \gcd(a, b + ka) = \gcd(a + kb, b)$$

質數與最大公因數 – 輾轉相除法

證明：

$$\because d|\gcd(a,b) \iff d|\gcd(a,b+ka)$$
$$\therefore \gcd(a,b) = \gcd(a,b+ka)$$

質數與最大公因數 – 輾轉相除法

```
1  int gcd(int a, int b){
2      return b?gcd(b, a%b):a;
3  }
```

質數與最大公因數 – Bézout's theorem

定理 (Bézout's theorem)

$$\{ax + by | x, y \in \mathbb{Z}\} = \{k \gcd(a, b) | k \in \mathbb{Z}\}$$

質數與最大公因數 – Bézout's theorem

證明： 設 $d = ax_0 + by_0$ 爲 $S = \{ax + by | x, y \in \mathbb{Z}\}$ 中最小的正數。若 $d \nmid a$，設 $a = qd + r,\ 0 < r < d$，則

$$r = a - qd = a(1 - qx_0) + b(-qy_0) \in S$$

與 d 的最小性矛盾，所以 $d|a$。
同理 $d|b$，所以 $d|\gcd(a, b)$。

質數與最大公因數 – Bézout's theorem

證明： 另外

$$
\begin{aligned}
&\gcd(a,b)|a,\ \gcd(a,b)|b \\
\Rightarrow &\gcd(a,b)|ax+by \\
\Rightarrow &S \subseteq \{k\gcd(a,b)|k\in\mathbb{Z}\} \\
&\because \gcd(a,b)|ax_0+by_0=d \\
&\therefore d=\gcd(a,b) \\
\Rightarrow &k\gcd(a,b)=a(kx_0)+b(ky_0)\in S \\
&\therefore S=\{k\gcd(a,b)|k\in\mathbb{Z}\}
\end{aligned}
$$

質數與最大公因數 – 擴展歐幾里德算法

```cpp
// return (d, x, y) s.t. ax+by=d=gcd(a, b)
tuple<int, int, int> exgcd(int a, int b){
    if(!b)return make_tuple(a, 1, 0);
    int d, x, y;
    tie(d, x, y)=exgcd(a, b);
    return make_tuple(d, y, x-a/b*y);
}
```

質數與最大公因數 – 模逆元

定義

a 模 n 的模逆元 a^{-1} 是指滿足 $aa^{-1} \equiv a^{-1}a \equiv 1 \pmod{n}$ 的數，也就是 a 在 $\mathbb{Z}_n^*$ 中的反元素。

質數與最大公因數 – 模逆元

性質

a 模 n 有模逆元 $\iff \gcd(a, n) = 1$。

質數與最大公因數 – 模逆元

證明：

由 Bézout's theorem 可知：

$$\begin{aligned} a\text{模}n\text{有模逆元} &\iff \text{存在}x, y \in \mathbb{Z}\text{使得}ax + ny = 1 \\ &\iff \gcd(a, n) = 1 \end{aligned}$$

質數與最大公因數 – 模逆元

有些題目會要求某個有理數 $(= \frac{a}{b})$ 模 p，實際上就是要求某個數 c 使得 $bc \equiv a \pmod{p}$，而這個 $c \equiv \frac{a}{b} \pmod{p}$，可以用 $c = ab^{-1}$ 求得。

一些定理 – 中國剩餘定理

定理 (中國剩餘定理 (Chinese remainder theorem))

給定兩兩互質的正整數 $n_1, n_2, \ldots, n_m$，以及 $r_1, r_2, \ldots, r_m$，必存在 x 使得

$$\begin{cases} x \equiv r_1 \pmod{n_1} \\ x \equiv r_2 \pmod{n_2} \\ \vdots \\ x \equiv r_m \pmod{n_m} \end{cases}$$

且所有可能的 x 模 $n_1 n_2 \cdots n_m$ 同餘。

一些定理 – 中國剩餘定理

證明： 對 m 使用數學歸納法來證明中國剩餘定理中 x 的存在性。

當 $m = 1$ 時顯然。

設當 $m = k$ 時成立，此時 $x \equiv x_0 \pmod{n_1 n_2 \cdots n_k}$。

當 $m = k + 1$ 時，取

$$\begin{aligned} x &= x_0 + (n_1 n_2 \cdots n_k)(n_1 n_2 \cdots n_k)^{-1}(r_{k+1} - x_0) \\ &\equiv r_{k+1} \pmod{n_{k+1}} \end{aligned}$$

（其中 $(n_1 n_2 \cdots n_k)^{-1}$ 爲 $n_1 n_2 \cdots n_k$ 模 n_{k+1} 的模逆元）

一些定理 – 中國剩餘定理

證明： 同時

$$\begin{aligned} x &= x_0 + (n_1 n_2 \cdots n_k)(n_1 n_2 \cdots n_k)^{-1}(r_{k+1} - x_0) \\ &\equiv x_0 \pmod{(n_1 n_2 \cdots n_k)} \end{aligned}$$

所以 x 滿足中國剩餘定理的 $k+1$ 條同餘式。
根據數學歸納法，中國剩餘定理中 x 必存在。
另外，因爲 $(r_1, r_2, \ldots, r_m)$ 有 $n_1 n_2 \cdots n_m$ 種組合，而 x 模 $n_1 n_2 \cdots n_m$ 也有 $n_1 n_2 \cdots n_m$ 種相異的餘數，所以每個 $(r_1, r_2, \ldots, r_m)$ 會對應到唯一一種餘數的解。

一些定理 – 中國剩餘定理

定理

給定兩兩互質的正整數 $n_1, n_2, \ldots, n_m$，存在一個雙射函數

$$f : \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m} \to \mathbb{Z}_{n_1 n_2 \cdots n_m}$$

滿足

$$\forall (x_1, x_2, \ldots, x_m) \in \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m}, i \in \{1, 2, \ldots, m\}$$

$$f(x_1, x_2, \ldots, x_m) \equiv x_i \pmod{n_i}$$

一些定理 – Wilson's theorem

定理 (Wilson's theorem)

設 p 爲質數，則

$$(p-1)! \equiv -1 \pmod{p}$$

一些定理 – Wilson's theorem

證明： 若 $a = a^{-1}$，則 $a^2 \equiv 1 \pmod{p}$

$$p | a^2 - 1 = (a+1)(a-1)$$

因爲 p 是質數，所以 $p|a+1$ 或 $p|a-1$，於是

$$a \equiv \pm 1 \pmod{p}$$

所以 $\forall a \not\equiv \pm 1 \pmod{p}$, $a \neq a^{-1}$
另外，我們知道 $(a^{-1})^{-1} = a$，所以對於 $a \not\equiv \pm 1 \pmod{p}$，可以把 a, a^{-1} 兩兩湊對，也就是

$$\{2, 3, \ldots, p-2\} = \{a_1, a_1^{-1}, a_2, a_2^{-1}, \ldots, a_{\frac{p-3}{2}}, a_{\frac{p-3}{2}}^{-1}\}$$

一些定理 – Wilson's theorem

證明： 因此

$$\begin{aligned}(p-1)! &\equiv -2 \times 3 \times \cdots \times (p-2) \\ &\equiv -a_1 a_1^{-1} a_2 a_2^{-1} \cdots a_{\frac{p-3}{2}} a_{\frac{p-3}{2}}^{-1} \equiv -1 \pmod{p}\end{aligned}$$

一些定理 – 費馬小定理

引理 (Recall from 群論)

$\forall g \in G$

$$g^{|G|} = 1$$

一些定理 – 費馬小定理

定理 (費馬小定理)

設 p 是質數，$p \nmid a$，則

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

一些定理 – 費馬小定理

證明：
因爲 a^{-1} 存在，所以 $g \to ag$ 是一個雙射函數。
$\Rightarrow a, 2a, \ldots, (p-1)a$ 是一個 $1, 2, \ldots, p-1$ 的排列。
$\Rightarrow a^{p-1}(p-1)! \equiv a(2a)\cdots(p-1)a \equiv (p-1)! \pmod{p}$
$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$
另外，有一個群論的證明方法：因爲 a 是一個 $\mathbb{Z}_p^*$ 的元素，所以 $a^{p-1} = a^{|\mathbb{Z}_p^*|} = 1$。

一些定理 – 費馬小定理

計算模逆元：因爲 $aa^{p-2} \equiv a^{p-1} \equiv 1 \pmod{p}$，所以 $a^{p-2} \equiv a^{-1} \pmod{p}$。

一些定理 – 費馬小定理

- 另外一個求模逆元的方法（$O(p)$ 建表）
- 已知 $1^{-1}, 2^{-1}, (a-1)^{-1}$，求 a^{-1}
- 設 $p = aq + r$，其中 $1 \leq r \leq a - 1$
- $pr^{-1} = aqr^{-1} + 1$
- $-aqr^{-1} \equiv 1 \pmod{p}$
- $-qr^{-1} \equiv a^{-1} \pmod{p}$
- C++ 中 $q = p/a, r = p\%a$

一些定理 – 歐拉函數

定義

$\varphi(n) := |\{\gcd(a,n) = 1 | 0 \leq a \leq n-1,\ a \in \mathbb{Z}\}| = |\mathbb{Z}_n^*|$，也就是小於 n 且與 n 互質的非負整數個數。

一些定理 – 歐拉函數

性質

若 $\gcd(a,b)=1$，則 $\varphi(ab)=\varphi(a)\varphi(b)$，也就是 φ 是積性函數。

一些定理 – 歐拉函數

證明：

$$\gcd(d, ab) = 1 \iff \gcd(d, a) = 1, \gcd(d, b) = 1$$

$\therefore$ 在中國剩餘定理中的雙射函數 $f : \mathbb{Z}_a \times \mathbb{Z}_b \to \mathbb{Z}_{ab}$ 會把 $\mathbb{Z}_a^* \times \mathbb{Z}_b^*$ 送到 $\mathbb{Z}_{ab}^*$
因爲 f 雙射，所以

$$\varphi(a)\varphi(b) = |\mathbb{Z}_a^* \times \mathbb{Z}_b^*| = |\mathbb{Z}_{ab}^*| = \varphi(ab)$$

一些定理 – 歐拉函數

定義

設 p 爲質數，$\nu_p(n) :=$ 最大的整數 α 使得 $\frac{n}{p^\alpha}$ 爲整數。
其中 n 不一定要是整數，也可以是有理數。

一些定理 – 歐拉函數

公式

$$\varphi(n) = \prod_{p|n} (p-1) p^{\nu_p(n)-1}$$

一些定理 – 歐拉函數

證明：

$$\varphi(p^k) = |\{\gcd(a, p^k) = 1 | a \in \mathbb{Z}_{p^k}\}| = |\{p \nmid a | a \in \mathbb{Z}_{p^k}\}| = (p-1)p^{k-1}$$

由 φ 是積性函數知：

$$\varphi(n) = \prod_{p|n} \varphi(p^{\nu_p(n)}) = \prod_{p|n} (p-1)p^{\nu_p(n)-1}$$

一些定理 – 歐拉函數

公式

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

一些定理 – 歐拉函數

證明：

$$
\begin{aligned}
n &= \sum_{d|n} |\{\gcd(a,n) = d | a \in \mathbb{Z}_n\}| \\
&= \sum_{d|n} |\{\gcd(a,\frac{n}{d}) = 1 | a \in \mathbb{Z}_{\frac{n}{d}}\}| \\
&= \sum_{d|n} \varphi(\frac{n}{d}) \\
&= \sum_{d|n} \varphi(d)
\end{aligned}
$$

一些定理 – 歐拉函數

引理

定義數列：$a_0 = n,\ \forall i \geq 1,$

$$a_i = \begin{cases} \varphi(a_{i-1}), \text{ if } a_{i-1} \geq 2 \\ 0, \text{ if } a_{i-1} = 1 \end{cases}$$

則

$$\sum_{i=0}^{\infty} a_i = \Theta(n)$$

一些定理 – 歐拉函數

證明：

首先對於 $a_{i+1} > 0$，有 $a_{i+1} < a_i$。

如果 $2|a_i$，那麼 $a_{i+1} \leq \frac{a_i}{2}$。

如果 a_i 是偶數且 > 1，那麼 $a_{i+2} < a_{i+1} \leq \frac{a_i}{2}$

如果 a_i 是奇數且 > 1，其必有奇質數 p，而 $p-1|\varphi(a_i)$，a_{i-1} 是偶數，所以 $a_{i+2} \leq \frac{a_{i+1}}{2} < \frac{a_i}{2}$。

所以對於所有 $a_{i+2} > 0$，$a_{i+2} < \frac{a_i}{2}$。

於是

$$\sum_{i=0}^{\infty} a_i \leq \sum_{i=0}^{\infty} \frac{a_0}{2^{\lfloor \frac{i}{2} \rfloor}} = 2\sum_{i=0}^{\infty} \frac{a_0}{2^i} = 4a_0 = O(n)$$

又 $a_0 = n$，所以

$$\sum_{i=0}^{\infty} a_i = \Theta(n)$$

一些定理 – 歐拉定理

定理 (歐拉定理)

設 $\gcd(a, n) = 1$，則

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

一些定理 – 歐拉定理

證明： 因爲 $a \in \mathbb{Z}_n^*$，所以有 $a^{\varphi(n)} = a^{|Z_n^*|} = 1$。

一些定理 – 歐拉定理

歐拉定理即爲推廣至合數的費馬小定理。

因此在計算 $a^k \pmod{n}$ 時，其中 $\gcd(a, n) = 1$，如果 k 非常大，可以將 k 模 $\varphi(n)$ 之後再做計算。

一些定理 – 計算 $a^k \pmod n$

如果 $\gcd(a,n) \neq 1$，要怎麼計算 $a^k \pmod n$？

引理

設 $\gcd(a,n)$ 有質因數集 P，$b = \max_{p \in P}(\lceil \frac{\nu_p(n)}{\nu_p(a)} \rceil)$，$d = \prod_{p \in P} p^{\nu_p(n)}$，則 $\forall k \geq b$

$$a^k \equiv a^{k+\varphi(\frac{n}{d})} \pmod n$$

一些定理 – 計算 $a^k \pmod n$

證明： 因爲 $\forall k \geq b$

$$\forall p \in P,\ \nu_p(a^k) = k\nu_p(a) \geq b\nu_p(a) \geq \nu_p(n)$$
$$\forall p \notin P,\ \nu_p(a^k) = k\nu_p(a) = 0$$

一些定理 – 計算 $a^k \pmod n$

證明： 所以

$$
\begin{aligned}
& d | a^k \text{且} \frac{a^k}{d} \in \mathbb{Z}_{\frac{n}{d}}^*,\ a \in \mathbb{Z}_{\frac{n}{d}}^* \\
\Rightarrow & a^{\varphi(\frac{n}{d})} \equiv 1 \pmod{\frac{n}{d}} \\
\Rightarrow & \frac{a^k}{d} \equiv \frac{a^{k+\varphi(\frac{n}{d})}}{d} \pmod{\frac{n}{d}} \\
\Rightarrow & \frac{n}{d} \Big| \frac{a^k - a^{k+\varphi(\frac{n}{d})}}{d} \\
\Rightarrow & n | a^k - a^{k+\varphi(\frac{n}{d})} \\
\therefore & a^k \equiv a^{k+\varphi(\frac{n}{d})} \pmod n
\end{aligned}
$$

注意到因爲 $\varphi(\frac{n}{d}) | \varphi(n)$，所以 $a^k \equiv a^{k+\varphi(n)} \pmod n$。

一些定理 – 計算 $a^k \pmod n$

引理

$$\gcd(a^k, n) \neq \gcd(a^{k+1}, n) \iff k < b$$

，其中 b 的定義與上個定理相同。

一些定理 – 計算 $a^k \pmod n$

所以我們在算 $a^k \pmod n$ 時，可以先算出 b，注意到我們並不用去算 P，而是去找到最小的 x 使得
$\gcd(a^x, n) = \gcd(a^{x+1}, n)$，這個 x 就是 b。

因爲必須要存在某個質數 p 使得 $\nu_p(n) \geq b$，所以 b 的量級爲 $O(\log n)$。
如果 $k < b$ 那就直接算 $a^k \pmod n$，否則再算出
$d = \gcd(a^b, n)$。

將 $k - b$ 拿去算除以 $\varphi(\frac{n}{d})$ 的餘數得到 r，a^{b+r} 即爲所求。

一些定理 – 次方塔

例子 (次方塔)

給定 $n \leq 10^6$，計算

$$a_1^{a_2^{\cdot^{\cdot^{\cdot^{a_m}}}}} \pmod{n}$$

一些定理 – 次方塔

證明： 如果遇到某個 $a_i = 1$，那 a_i 後面的東西都不用算了。所以我們假設 $a_1, a_2, \ldots, a_m$ 都不是 1。

令 $b_i := a_i^{\cdot^{\cdot^{a_m}}} \pmod{n}$。

$\Rightarrow b_i = a_i^{b_{i+1}}$

令 $a = a_1, k = b_2$，並延續上個定理中使用的符號 b, d。

b 可以在 $O(\log n)$ 的時間算出來，因爲可以依序計算 $1, a, a^2, \ldots, a^x$ 然後看什麼時候 $\gcd(a^i, n) = \gcd(a^{i+1}, n)$。

而 d 其實不需要算。

一些定理 – 次方塔

證明： 先遞迴下去算 $b_2 \pmod{\varphi(n)}$，接著再回來算 $a_1^{b_2}$。

當然，如果 $b_2 < b$，可以在 5 層內判斷，因爲上去 k 層的結果至少爲 $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}$（其中有 k 個 2），而 $2^{2^{2^{2^2}}} = 2^{65536}$，遠超過 $\log n$ 也就是 b 的量級。

若 $b_2 \geq b$，算完 $r := (b_2 - b) \pmod{\varphi(n)}$ 之後，接著計算 $a^{b+r} \pmod{n}$ 即爲所求。

預先建表可以在 $O(n)$ 的時間算完所有 n 以內的 φ 值。

每一層遞迴會花 $O(\log n) + O(\log(b + r)) = O(\log n + \log(\log n + \varphi n)) \in O(n)$ 的時間，所以總時間複雜度爲

$$O(n) + O(n) + O(\varphi(n)) + O(\varphi(\varphi(n))) + \cdots = O(n)$$

階與原根 – 階

定義

設 $\gcd(a, n) = 1$，若 m 是最小的正整數使得 $a^m \equiv 1 \pmod{n}$，則稱 m 是 a 模 n 下的階，寫作 $\mathrm{ord}_n(a) = m$。

階與原根 – 階

引理

設 $\gcd(a, n) = 1$，若 $a^k \equiv 1 \pmod{n}$，則

$$\mathrm{ord}_n(a) | k$$

階與原根 – 階

證明：

設 r 爲 $k = q\text{ord}_n(a) + r$，其中 $0 \leq r \leq \text{ord}_n(a) - 1$。

$$a^r \equiv a^r \cdot 1^q \equiv a^r (a^{\text{ord}(a)})^q \equiv a^k \equiv 1 \pmod{n}$$

而我們假設 $\text{ord}_n(a)$ 是最小的正整數使得 $a^{\text{ord}_n(a)} = 1$，所以 r 不能是正整數，$r = 0$。

$\therefore \text{ord}_n(a) | k$。

階與原根 – 階

推論

設 $\gcd(a, n) = 1$，則

$$\operatorname{ord}_n(a) | \varphi(n)$$

階與原根 – 階

性質

設 $\gcd(a, n) = 1$，則 $1, a, a^2, \ldots, a^{\mathrm{ord}_n(a)-1}$ 兩兩相異。

階與原根 – 階

證明：
若 $0 \leq i < j \leq \text{ord}_n(a)-1$, $a^i = a^j$，則 $a^{j-i} \equiv a^j(a^i)^{-1} \equiv 1 \pmod{n}$，但是 $1 \leq j-i \leq \text{ord}_n(a)-1$，與 $\text{ord}_n(a)$ 的最小性矛盾。
所以 $a^i \neq a^j$，即 $1, a, a^2, \ldots, a^{\text{ord}_n(a)-1}$ 兩兩相異。

階與原根 – 階

引理

設 $\gcd(a, n) = 1$，則

$$\operatorname{ord}_n(a^k) = \frac{\operatorname{ord}_n(a)}{\gcd(\operatorname{ord}_n(a), k)}$$

階與原根 – 原根

定義

設 $\gcd(a, n) = 1$，若 $\mathrm{ord}_n(a) = \varphi(n)$，則稱 a 是模 n 下的原根。

階與原根 – 原根

如果 n 存在原根 a，那麼因爲 $1, a, \ldots, a^{\mathrm{ord}_n(a)-1}$ 兩兩相異，且 $|\mathbb{Z}_n^*| = \varphi(n)$，就有 $\{1, a, \ldots, a^{\mathrm{ord}_n(a)-1}\} = \mathbb{Z}_n^*$，也就是 a 是 $\mathbb{Z}_n^*$ 的生成元。此時 $\mathbb{Z}_n^* \cong \mathbb{Z}_{\varphi(n)}$，這個群就會變得非常容易討論。於是我們關心對於哪些 n 有原根。

階與原根 – 原根

定理

設 F 是一個 field，則 $\forall p \in F[x]$，即 p 是係數 $\in F$ 的多項式，

$$p(a) = 0 \iff x - a | p(x)$$

階與原根 – 原根

證明：

$(\Leftarrow)$

$$
\begin{aligned}
& x-a|p(x) \\
& \Rightarrow p(x)=q(x)(x-a) \text{ for some } q \\
& \Rightarrow p(a)=q(a)(a-a)=0
\end{aligned}
$$

$(\Rightarrow)$ 設 $p(x)=q(x)(x-a)+r(x)$，其中我們能保證 $\deg(r(x))<\deg(x-a)$，也就是 $r(x)$ 是個常數。

$$
\begin{aligned}
& 0=p(a)=q(a)(a-a)+r(a)=r(a) \\
& \Rightarrow r(a)=0 \\
& \Rightarrow p(x)=q(x)(x-a) \\
& \Rightarrow x-a|p(x)
\end{aligned}
$$

階與原根 – 原根

定理

設 F 是一個 field，則 $\forall p \in F[x]$，p 有至多 $\deg(p)$ 個根。

階與原根 – 原根

定理

$\mathbb{Z}_n^*$ 有原根 $\iff$ $n = 1, 2, 4, p^k, 2p^k$，其中 p 爲奇質數。

階與原根 – 原根

證明： 來證明 $n = p$ 是質數的 case。
令 $f(d) = \left|\{a | a \in \mathbb{Z}_p^*,\ \mathrm{ord}_p(a) = d\}\right|$。
設 $\mathrm{ord}_p(a) = d$，則 $1, a, a^2, \ldots, a^{d-1}$ 是所有 $x^d - 1$ 的根。

$$\mathrm{ord}_p(a^k) = d \iff \frac{\mathrm{ord}_p(a)}{\gcd(\mathrm{ord}_p(a), k)} = d \iff \gcd(d, k) = 1$$

$\therefore$ 一共有 $\varphi(d)$ 個數 b 使得 $\mathrm{ord}_p(b) = d$，即 $f(d) = \varphi(d)$。
若不存在 a 使得 $\mathrm{ord}_p(a) = d$，則 $f(d) = 0$。
所以 $f(d) \leq \varphi(d)$，等號成立若且唯若存在 a 使得 $\mathrm{ord}_p(a) = d$。
因爲 $\forall a \in \mathbb{Z}_p^*,\ \mathrm{ord}_p(a) | p - 1$，所以

$$\sum_{d | p-1} f(d) = p - 1$$

證明： 另外

$$\sum_{d|p-1} \varphi(d) = p - 1$$

所以

$$\sum_{d|p-1} f(d) = \sum_{d|p-1} \varphi(d)$$

也就是 $\forall d|p-1,\ f(d) = \varphi(d)$，因此

$$f(p-1) = \varphi(p-1)$$

所以質數有 $\varphi(p-1)$ 個原根。

質數與因數分解 – 隨機

降低標準：100% 正確 $\rightarrow$ 99.99% 正確

質數與因數分解 – 隨機

引理

設 $0 < \epsilon < 1$，若有一個隨機演算法，每次做會正確的機率都是 $\Omega(\frac{1}{f(n)})$ 且獨立的，則做 $O(f(n)(-\log \epsilon))$ 次即可保證每次都錯的機率 $< \epsilon$。

質數與因數分解 – 隨機

證明：

存在 c 使得每次正確的機率 $> c\frac{1}{f(n)}$

$\Rightarrow$ 每次錯誤的機率 $< 1 - c\frac{1}{f(n)}$

做 $\frac{1}{c}f(n)$ 次錯誤的機率 $< (1 - \frac{c}{f(n)})^{\frac{f(n)}{c}} < \frac{1}{e}$

$\Rightarrow$ 做 $\frac{1}{c}f(n)(-\log \epsilon)$ 次每次都是錯誤的機率 $< (e^{-1})^{-\ln \epsilon} = \epsilon$。

質數與因數分解 – 隨機

當 $\epsilon = \Omega(1)$ 時，做 $O(f(n))$ 次即可保證每次都錯的機率 $< \epsilon$。

質數與因數分解 – Miller-Rabin

給定一個正整數 n，要如何判斷 n 是不是質數呢？

可以枚舉 $2, 3, \ldots, \lfloor\sqrt{n}\rfloor$，看是不是 n 的因數，但這樣做的時間複雜度是 $\tilde{O}(\sqrt{n})$，實在是太慢了。

如果隨便找一個數 a，然後發現 $\gcd(a, n) \neq 1$ 且 $\gcd(a, n) \neq n$，那就可以說明 n 不是質數了。

但是在 $\mathbb{Z}_n$ 中與 n 滿足上述條件的數只有 $n - \varphi(n) - 1$ 個，對於是兩個差不多量級的質數 p, q 的乘積 n，
$n - \varphi(n) - 1 = pq - (p-1)(q-1) - 1 = p + q = \Theta(\sqrt{n})$，也就是與 n 不互質的數只有佔 $\mathbb{Z}_n$ 的 $\Theta(\frac{1}{\sqrt{n}})$。

隨機找 a 也要找 $\Theta(\sqrt{n})$ 次才能讓找不到 a 的機率爲 $\Omega(1)$，這樣時間複雜度同樣是 $\tilde{O}(\sqrt{n})$。

質數與因數分解 – Miller-Rabin

互質的 a 也能做事？

費馬小定理：如果 n 是質數，那就會有 $a^{n-1} \equiv 1 \pmod{n}$。

因此，若有 $a^{n-1} \not\equiv 1 \pmod{n}$，那麼 n 就不是質數。

對於每個 n 都存在這樣的 a 嗎？就算存在，容易找嗎？

事實上，有合數 n 使得不存在這樣的 a，像是 561，這種合數稱爲 Carmicahel 數，雖然 Cramicahel 數十分稀少，但我們仍不能忽視它們的存在。

而如果存在這樣的 a，找到的機率蠻高的。

質數與因數分解 – Miller-Rabin

引理

若 $\exists a \in \mathbb{Z}_n^*$ 使得 $a^{n-1} \not\equiv 1 \pmod{n}$，則 $|\{b|b \in \mathbb{Z}_n^*,\ b^{n-1} \not\equiv 1 \pmod{n}\}| \geq \frac{\varphi(n)}{2}$。

質數與因數分解 – Miller-Rabin

證明：

設 $G = \mathbb{Z}_n^*$, $H = \{b | b \in G,\ b^{n-1} \equiv 1 \pmod{n}\}$。

因爲 H 封閉且包含於 G，所以 H 是 G 的子群且因爲 a 的存在知 $H \neq G$

由 Lagrange's theorem 知 $|H| \mid |G|$，所以 $|H| \leq \frac{1}{2}|G| = \frac{\varphi(n)}{2}$

所以 $|\{b | b \in \mathbb{Z}_n^*,\ b^{n-1} \not\equiv 1 \pmod{n}\}| = |G - H| \geq \frac{\varphi(n)}{2}$。

質數與因數分解 – Miller-Rabin

所以要判斷不是 Carmichael 數的 n 是合數時，隨機取 a，要嘛取到 $a \notin \mathbb{Z}_n^*$，要嘛有 $\frac{1}{2}$ 的成功率可以判斷 n 是合數，所以只需要取 $O(1)$ 個 a 就能高機率正確判斷 n 是不是合數。

不過我們還可以再更進一步，如果 n 是質數，除了費馬小定理會滿足之外，還有其他性質。

若 $x^2 \equiv 1 \pmod{n}$，那麼 $(x+1)(x-1) \equiv 0 \pmod{n}$。

$\Rightarrow n | (x+1)(x-1)$

如果 n 是質數，$n | x+1$ 或 $n | x-1$

$\Rightarrow x \equiv \pm 1 \pmod{n}$

質數與因數分解 – Miller-Rabin

有了這個性質之後，我們可以取一個序列 $a^b, a^{2b}, a^{4b}, \ldots, a^{2^{\nu_2(n-1)}b} (= a^{n-1})$，如果 n 是質數，這個序列由費馬小定理最後一定會變成 1，而這個序列變成 1 的前一項必須是 -1。

因此，我們不僅僅驗費馬小定理，還額外驗這個序列，兩個只要有其中一個不成立就可以知道 n 不是質數，這就是 Miller Rabin 的運作原理。

另外，對於一些 n 的範圍，有人已經發現了驗檢查表中的 a 即可在該範圍內準確判斷 n 是不是質數。

質數與因數分解 – Miller-Rabin

```cpp
/*
檢查表：
n<2^32: 2, 7, 61
n<2^64: 2, 325, 9375, 28178, 450775, 9780504, 1795265022
*/
#define ll long long

// 要自己寫乘法與冪，因爲兩個 long long 相乘有可能會溢位
ll mul(ll a, ll b, ll n); // return a*b%n
ll fpow(ll a, ll b, ll n); // return a^b%n
```

質數與因數分解 – Miller-Rabin

```cpp
bool millerRabin(ll a, ll n){
    if(n==2)return 1;
    if(n<2||!(n&1))return 0;
    if(!(a%=n))return 1;

    ll b=n-1;
    int t=0;
    for(; !(b&1); b>>=1)++t;

    ll c=fpow(a, b, n);
    for(int i=0; i<t; ++i){
        ll c2=mul(c, c, n);
        if(c2==1&&c!=1&&c!=n-1)return 0;
        c=c2;
    }
    return c==1;
}
```

質數與因數分解 – Cycle Finding

例子 (Cycle finding)

給你一個函數 f 和 x_0，對於所有 $i \geq 1$ 令 $x_i := f(x_{i-1})$，如果 f 的確存在循環節，請找出 $i \neq j$ 使得 $x_i = x_j$。

我們希望空間複雜度 $O(1)$，如果有解，設最小的解爲 $x_i = x_j$, $i < j$，那要求時間複雜度是 $O(j)$（即進入循環節前的長度 + 循環節的長度）

質數與因數分解 – Cycle Finding

設最小的解爲 (i', j') 演算法：

- 剛開始令 $i = 1$
- 檢查是否有 $j \in (i, 2i]$ 使得 $x_i = x_j$
- 如果沒有就把 $i* = 2$

檢查次數：

- $j' \leq i < 2j'$ 時一定找得到對應的 j
- 設此時的 $i = 2^k$，檢查次數
  $= 2^k + 2^{k-1} + \cdots + 1 = 2^{k+1} - 1 < 2i < 4j' = O(j')$

質數與因數分解 – Birthday Paradox

例子 (Birthday paradox)

均勻隨機取 n 個人（設一年有 365 天且每天出生的人數相同），n 至少要是多少，能取到有兩個生日相同天的人的機率才會 $> 50\%$？

質數與因數分解 – Birthday Paradox

答案是 23。

我們來計算沒有兩個人的生日相同的機率 p。
將 n 個人一個一個加進來，第 i 個人加進來時，生日沒跟已經加進來的人重複的機率是 $\frac{365-i+1}{365}$，所以

$$p = \prod_{i=1}^{n} \frac{364-i}{365} = \prod_{i=0}^{n-1} \frac{365-i}{365} < \prod_{i=0}^{n-1} e^{-i/365} = e^{-n(n-1)/730}。$$

當 $n = 23$ 時，$e^{-n(n-1)/730} < e^{-0.69315} < \frac{1}{2}$。

將 365 推廣成任意的 m，只要使 $n = \Theta(\sqrt{m})$ 即足夠讓機率足夠小（能小於任意給定常數）。

質數與因數分解 – Pollard's rho

設我們要因數分解 $n = pq$，其中 $\gcd(p, q) = 1$，並且不失一般性假設 $p < q$。
隨機選多少個數即足夠找到兩個模 p 同餘的數？

由 Birthday Paradox 知：$\Theta(\sqrt{p})$ 個即足夠，也就是隨機一個一階遞迴數列（即只由前一項去推下一項的數列），有高機率循環節長度在 $\Theta(\sqrt{p})$ 以內。

質數與因數分解 – Pollard's rho

假設這個數列第 i 項是 x_i，若 $x_i \equiv x_j \pmod{p}$，有多高的機率 $x_i \equiv x_j \pmod{n}$？

答案是 $\frac{1}{q}$，因爲模 p 同餘與模 q 同餘可以想成是獨立事件（實際上不是獨立事件，但在這個例子中可以想成幾乎是獨立）

所以會有 $\frac{q-1}{q}$ 的機率 $x_i \not\equiv x_j \pmod{n}$，此時可以發現，$\gcd(x_i - x_j, n)$ 即是一個 n 的因數，且不是 n 也不是 1（因爲至少會被 p 整除）。

而失敗率是 $\frac{1}{q}$，表示我們只要做 $O(1)$ 次即可讓失敗率 $\to 0$。

質數與因數分解 – Pollard's rho

我們設 x_0 爲 $\{0, 1, \ldots, n-1\}$ 中隨機一個數，$x_i = x_{i-1}^2 + 1$
配合 Cycle finding，雖然我們沒辦法知道是否有 $p | x_i - x_j$，但是實際上只要去檢測 $\gcd(x_i - x_j, n)$ 是否不是 1 即可，時間複雜度是 $O($ 循環節長度 $)$，也就是 $O(\sqrt{p}) = O(\sqrt[4]{n})$。

質數與因數分解 – Pollard's rho

```
ll pollardRho(ll n) {
    if(n%2==0)return 2;
    ll xi, xj;
    int i=1, j=1;
    xi=xj=2;
    while(1){
        j++;
        xj=f(xj, n);
        int d=__gcd(abs(xi - xj), n);
        if(d!=1)return d;
        if(j==i*2)i<<=1, xi=xj;
    }
}
```

致謝

本篇講義特別感謝以前的 IOIC 數學講師、IMOC 數論講師、以及 zscoder 在 Codeforces 撰寫的生成函數教學。

補充講義與勘誤

計數原理

- 連加、連乘、聯集、交集符號
- 莫比烏斯反演回推排容原理
- 講義 p166，改成 n 顆相同的球放進 m 個相異的箱子
- 講義 p168，$n! - \left|\bigcap_{i\in T} S_i\right|$ 改成 $n! - \left|\bigcup_{i\in T} S_i\right|$
- 講義 p169，$\bigcap_{i\in T} S_i = \{\sigma : \forall i \in T,\ \sigma_i = i\}$ 改成 $\bigcap_{i\in T} S_i$
- 雙射函數的定義
- 講義 p186，令 $b_i = |\{i|a_i = k\}|$ 改成令 $b_k = |\{i|a_i = k\}|$

群論

- 單位元素與反元素性質的經典題
- 講義 p191：在 $|g|$ 的定義後面補上：當不存在這樣的正整數 n 時，定義 $|g| = \infty$。
- 講義 p191：$|g| < |G|$ 改成 $|g| \leq |G|$
- 講義 p191：若存在 $S \in G$ 改成 $S \subseteq G$
- 講義 p197：$\sum_{g \in G} |A^g| = \{(g, a) \in G \times A | ga = a\}$ 改成 $\sum_{g \in G} |A^g| = |\{(g, a) \in G \times A | ga = a\}|$
- 講義 p198：$g^{-1}Hg \in G$ 改成 $g^{-1}Hg = H$

數論

- 講義 p202：$(a\%n * b\%n)\%n$ 改成 $(a\%n) * (b\%n)\%n$
- 有理數如何模質數
- 模逆元可以用費馬小定理求得
- 講義 p209：$a_{i+2} \leq \frac{a_{i-1}}{2} < \frac{a_i}{2}$ 改成 $a_{i+2} \leq \frac{a_{i+1}}{2} < \frac{a_i}{2}$
- 講義 p213：$\mathbb{Z}_n^*$ 有原根 $\iff$ $n = 1, 2, 4, p^k, 2p^k$，加上 p 爲奇質數
- 講義 p214：每次做會正確的機率都是 $O(\frac{1}{f(n)})$ 改成每次做會正確的機率都是 $\Omega(\frac{1}{f(n)})$
- 講義上的全改成投影片的：整個 Pollard's rho 的章節（包括 Cycle finding、Birthday paradox 與 Pollard's rho）