

# IOI-camp lecture Math

Meteor

February 7, 2017

# Introduction

程式競賽中的數學：

- 數學知識
- 數學想法

# Introduction

程式競賽中的數學：

- 數學知識
- 數學想法

# Introduction

程式競賽中的數學：

- 數學知識
- 數學想法

# Introduction – 數學知識例子

## 例題 (平方國的平方幣, TIOJ 1349)

給你一個正整數  $n$ ，請找出最小的  $k$ ，使得存在  $k$  個平方數  $a_1^2, a_2^2, \dots, a_k^2$  使得  $\sum a_i^2 = n$ 。 ( $n \leq 10^7$ )

- 一個很極端的「結論題」。
- 所有正整數都可以寫成 4 個平方數的和 (Lagrange 1770)。
- 太結論也不是很有趣……

# Introduction – 數學知識例子

## 例題 (平方國的平方幣, TIOJ 1349)

給你一個正整數  $n$ ，請找出最小的  $k$ ，使得存在  $k$  個平方數  $a_1^2, a_2^2, \dots, a_k^2$  使得  $\sum a_i^2 = n$ 。 ( $n \leq 10^7$ )

- 一個很極端的「結論題」。
- 所有正整數都可以寫成 4 個平方數的和 (Lagrange 1770)。
- 太結論也不是很有趣……

# Introduction – 數學知識例子

## 例題 (平方國的平方幣, TIOJ 1349)

給你一個正整數  $n$ ，請找出最小的  $k$ ，使得存在  $k$  個平方數  $a_1^2, a_2^2, \dots, a_k^2$  使得  $\sum a_i^2 = n$ 。 ( $n \leq 10^7$ )

- 一個很極端的「結論題」。
- 所有正整數都可以寫成 4 個平方數的和 (Lagrange 1770)。
- 太結論也不是很有趣……

# Introduction – 數學知識例子

## 例題 (平方國的平方幣, TIOJ 1349)

給你一個正整數  $n$ ，請找出最小的  $k$ ，使得存在  $k$  個平方數  $a_1^2, a_2^2, \dots, a_k^2$  使得  $\sum a_i^2 = n$ 。 ( $n \leq 10^7$ )

- 一個很極端的「結論題」。
- 所有正整數都可以寫成 4 個平方數的和 (Lagrange 1770)。
- 太結論也不是很有趣……



# Introduction – 數學知識例子 2

## 例題 (Taxes, Codeforces 735D)

在一個很古怪的國家，如果你賺了  $x$  元，你就要繳  $d$  塊錢的稅，其中  $d$  是  $x$  的因數且小於  $x$  裡最大的一個。

現在有一個人賺了  $n$  元，他想把  $n$  拆成  $n = n_1 + n_2 + \cdots + n_k$  然後  $n_i$  各自繳稅，請問他最多可以逃過多少稅？( $n \leq 2 \times 10^9$ )

- Goldbach's conjecture: 大於 2 的偶數都可以寫成兩個質數的和。

# Introduction – 數學知識例子 2

## 例題 (Taxes, Codeforces 735D)

在一個很古怪的國家，如果你賺了  $x$  元，你就要繳  $d$  塊錢的稅，其中  $d$  是  $x$  的因數且小於  $x$  裡最大的一個。

現在有一個人賺了  $n$  元，他想把  $n$  拆成  $n = n_1 + n_2 + \cdots + n_k$  然後  $n_i$  各自繳稅，請問他最多可以逃過多少稅？( $n \leq 2 \times 10^9$ )

- Goldbach's conjecture: 大於 2 的偶數都可以寫成兩個質數的和。

# Introduction – 數學想法例子

但大部份還是屬於「數學想法」的問題。

例題 (2015 ICPC Daejeon regional pE)

給你一堆數列  $a_1, a_2, \dots, a_n$ ，你要找一個排列  $\sigma$ ，使得

$$\max \left( \left| a_{\sigma(1)} - a_{\sigma(2)} \right|, \left| a_{\sigma(2)} - a_{\sigma(3)} \right|, \dots, \left| a_{\sigma(n)} - a_{\sigma(1)} \right| \right)$$

最小。 ( $n \leq 10^4$ )

定義

一個大小為  $n$  的**排列**是一個從  $[1, n]$  打到自己的一一對應函數。

# Introduction – 數學想法例子

但大部份還是屬於「數學想法」的問題。

例題 (2015 ICPC Daejeon regional pE)

給你一堆數列  $a_1, a_2, \dots, a_n$ ，你要找一個排列  $\sigma$ ，使得

$$\max \left( \left| a_{\sigma(1)} - a_{\sigma(2)} \right|, \left| a_{\sigma(2)} - a_{\sigma(3)} \right|, \dots, \left| a_{\sigma(n)} - a_{\sigma(1)} \right| \right)$$

最小。 $(n \leq 10^4)$

定義

一個大小為  $n$  的排列是一個從  $[1, n]$  打到自己的一一對應函數。

# Introduction – 數學想法例子

但大部份還是屬於「數學想法」的問題。

例題 (2015 ICPC Daejeon regional pE)

給你一堆數列  $a_1, a_2, \dots, a_n$ ，你要找一個排列  $\sigma$ ，使得

$$\max \left( \left| a_{\sigma(1)} - a_{\sigma(2)} \right|, \left| a_{\sigma(2)} - a_{\sigma(3)} \right|, \dots, \left| a_{\sigma(n)} - a_{\sigma(1)} \right| \right)$$

最小。 $(n \leq 10^4)$

定義

一個大小為  $n$  的**排列**是一個從  $[1, n]$  打到自己的一一對應函數。

# Introduction – 數學想法例子

## 解題四部曲：

- 嘗試、觀察：在計算紙上多試試
- 神猜結論
- (稍微)證明
- 寫 code

亂講的，多半要臨機應變，見招拆招。

# Introduction – 數學想法例子

解題四部曲：

- 1 嘗試、觀察：在計算紙上多試試
- 2 神猜結論
- 3 (稍微)證明
- 4 寫 code

亂講的，多半要臨機應變，見招拆招。

# Introduction – 數學想法例子

解題四部曲：

- 1 嘗試、觀察：在計算紙上多試試
- 2 神猜結論
- 3 (稍微)證明
- 4 寫 code

亂講的，多半要臨機應變，見招拆招。



# Introduction – 數學想法例子

解題四部曲：

- 1 嘗試、觀察：在計算紙上多試試
- 2 神猜結論
- 3 (稍微)證明
- 4 寫 code

亂講的，多半要臨機應變，見招拆招。

# Introduction – 數學想法例子

解題四部曲：

- 1 嘗試、觀察：在計算紙上多試試
- 2 神猜結論
- 3 (稍微)證明
- 4 寫 code

亂講的，多半要臨機應變，見招拆招。

# Introduction – 數學想法例子

解題四部曲：

- 1 嘗試、觀察：在計算紙上多試試
- 2 神猜結論
- 3 (稍微)證明
- 4 寫 code

亂講的，多半要臨機應變，見招拆招。

# Introduction – 數學想法例子

解題四部曲：

- 1 嘗試、觀察：在計算紙上多試試
- 2 神猜結論
- 3 (稍微)證明
- 4 寫 code

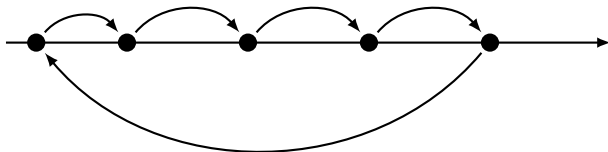
亂講的，多半要臨機應變，見招拆招。

# Introduction – 數學想法例子

- 1 嘗試、觀察
- 2 神猜結論

# Introduction – 數學想法例子

- 1 嘗試、觀察
- 2 神猜結論

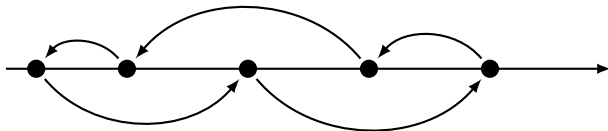


應該不是…

# Introduction – 數學想法例子

1 嘗試、觀察

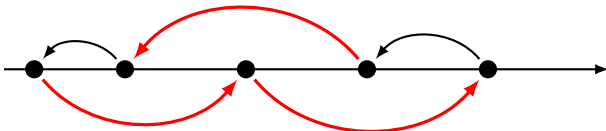
2 神猜結論



# Introduction – 數學想法例子

1 嘗試、觀察

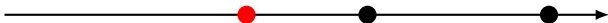
2 神猜結論





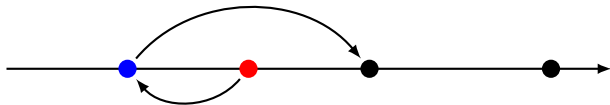
# Introduction – 數學想法例子

## 3 證明



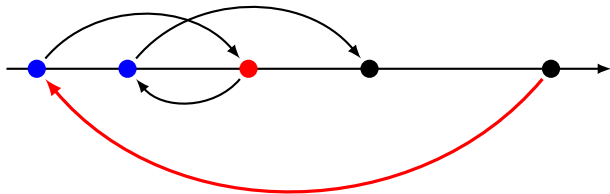
# Introduction – 數學想法例子

## 3 證明



# Introduction – 數學想法例子

## 3 證明



# Introduction – 數學想法例子

## 4 寫 code

---

```
1  sort(begin(a), end(a));
2  int ans = 0;
3  for (int i=0; i<n-2; i++)
4      ans = max(ans, a[i+2] - a[i]);
5  cout << ans << endl;
```

---

Very easy! — 有時漂亮的結論就會有很短的程式碼。

# Introduction – 數學想法例子

## 4 寫 code

---

```
1  sort(begin(a), end(a));
2  int ans = 0;
3  for (int i=0; i<n-2; i++)
4      ans = max(ans, a[i+2] - a[i]);
5  cout << ans << endl;
```

---

Very easy! — 有時漂亮的結論就會有很短的程式碼。

# Introduction

相同的題目就不會在出現第二次了。

但用類似想法的題目有可能會在出現！

要有舉一反三的能力！

# Introduction

相同的題目就不會在出現第二次了。

但用類似想法的題目有可能會在出現！

要有舉一反三的能力！

# Introduction

相同的題目就不會在出現第二次了。

但用類似想法的題目有可能會在出現！

要有舉一反三的能力！



# Introduction – 數學想法例子 2

例題 (2016 NTU PK pF)

給你一堆數列  $a_1, a_2, \dots, a_n$ ，你要找一個排列  $\sigma$ ，使得

$$\min_{1 \leq i < n} |a_{\sigma(i)} - a_{\sigma(i+1)}|$$

最大。 $(n \leq 2 \times 10^5)$

我們先想  $n$  是偶數的 case。

# Introduction – 數學想法例子 2

例題 (2016 NTU PK pF)

給你一堆數列  $a_1, a_2, \dots, a_n$ ，你要找一個排列  $\sigma$ ，使得

$$\min_{1 \leq i < n} |a_{\sigma(i)} - a_{\sigma(i+1)}|$$

最大。 $(n \leq 2 \times 10^5)$

我們先想  $n$  是偶數的 case。

# Introduction – 數學想法例子 2

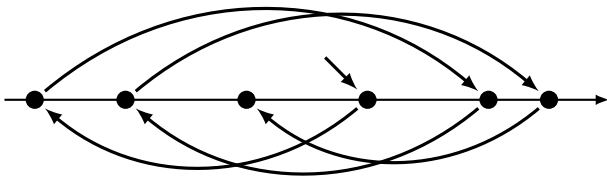
- 1 嘗試、觀察
- 2 神猜結論



# Introduction – 數學想法例子 2

1 嘗試、觀察

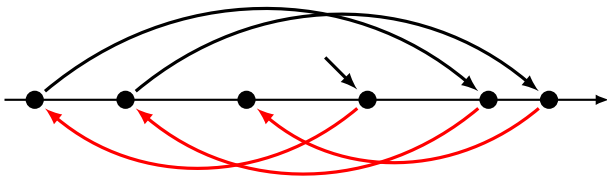
2 神猜結論



# Introduction – 數學想法例子 2

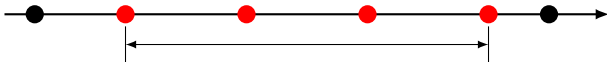
1 嘗試、觀察

2 神猜結論



# Introduction – 數學想法例子 2

## 3 證明



# Introduction – 數學想法例子 2

## 習題

請完成奇數的情況。

## 例題 (An Easy Problem, NTUJ 1423)

給你等式  $a^b \equiv c \pmod{d}$  中的其中 3 個，請找出剩下的一個。

1  $a^b \equiv ? \pmod{d}$ : 快速冪， $\mathcal{O}(\log b)$ 。

```
1 int fastpow(int a, int b, int m) {  
2     if (!b) return 1%m;  
3     int ret = fastpow(a*a%m, b/2, m);  
4     if (b&1) (ret *= a) %= m;  
5     return ret;  
6 }
```



## 例題 (An Easy Problem, NTUJ 1423)

給你等式  $a^b \equiv c \pmod{d}$  中的其中 3 個，請找出剩下的一個。

1  $a^b \equiv ? \pmod{d}$ : 快速幂， $\mathcal{O}(\log b)$ 。

```
1 int fastpow(int a, int b, int m) {  
2     if (!b) return 1%m;  
3     int ret = fastpow(a*a%m, b/2, m);  
4     if (b&1) (ret *= a) %= m;  
5     return ret;  
6 }
```

## 例題 (An Easy Problem, NTUJ 1423)

給你等式  $a^b \equiv c \pmod{d}$  中的其中 3 個，請找出剩下的一個。

1  $a^b \equiv ? \pmod{d}$ : 快速幂， $\mathcal{O}(\log b)$ 。

```
1  int fastpow(int a, int b, int m) {  
2      if (!b) return 1%m;  
3      int ret = fastpow(a*a%m, b/2, m);  
4      if (b&1) (ret *= a) %= m;  
5      return ret;  
6  }
```

■  $a^b \equiv c \pmod{?} \implies ? \mid a^b - c$

■  $a^? \equiv c \pmod{p}$ ,  $p$  prime :  $\mathcal{O}(\sqrt{p})$  , 有點難了。

$$a^{xk+y} \equiv c \pmod{p} \iff a^{xk} \equiv ca^{-y} \pmod{p}$$

怎麼求出  $a^{-y} \pmod{p}$  ?

2  $a^b \equiv c \pmod{?} \implies ? \mid a^b - c$

■  $a^? \equiv c \pmod{p}$ ,  $p$  prime :  $\mathcal{O}(\sqrt{p})$ , 有點難了。

$$a^{xk+y} \equiv c \pmod{p} \iff a^{xk} \equiv ca^{-y} \pmod{p}$$

怎麼求出  $a^{-y} \pmod{p}$ ?

2  $a^b \equiv c \pmod{?} \implies ? \mid a^b - c$

3  $a^? \equiv c \pmod{p}$ ,  $p$  prime :  $\mathcal{O}(\sqrt{p})$  , 有點難了。

$$a^{x^k+y} \equiv c \pmod{p} \iff a^{x^k} \equiv ca^{-y} \pmod{p}$$

問題

怎麼求出  $a^{-y} \bmod p$  ?

2  $a^b \equiv c \pmod{?} \implies ? \mid a^b - c$

3  $a^? \equiv c \pmod{p}$ ,  $p$  prime :  $\mathcal{O}(\sqrt{p})$  , 有點難了。

$$a^{xk+y} \equiv c \pmod{p} \iff a^{xk} \equiv ca^{-y} \pmod{p}$$

問題

怎麼求出  $a^{-y} \bmod p$  ?

我們先離題一下。

數學上喜歡把東西抽象化，只留下「本質」，去掉多餘的東西。

問題

運算的「本質」是什麼？

我們先離題一下。

數學上喜歡把東西抽象化，只留下「本質」，去掉多餘的東西。

問題

運算的「本質」是什麼？



我們先離題一下。

數學上喜歡把東西抽象化，只留下「本質」，去掉多餘的東西。

## 問題

運算的「本質」是什麼？

## 定義 (群)

一個**群**由一個集合  $G$  和一個運算  $\cdot$  構成，滿足

- 運算  $\cdot$  是一個函數  $(G, G) \rightarrow G$ ，也就是說  $x \cdot y \in G$ 。
- 有結合律： $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- 存在一個特別的元素  $1$  叫作單位元，滿足  $1 \cdot x = x \cdot 1 = x$ 。
- 對每一個  $x$  存在  $x^{-1} \in G$  叫作反元素，滿足
$$x \cdot x^{-1} = x^{-1} \cdot x = 1。$$

# 數論 – 群

## 定義 (群)

一個**群**由一個集合  $G$  和一個運算  $\cdot$  構成，滿足

- 運算  $\cdot$  是一個函數  $(G, G) \rightarrow G$ ，也就是說  $x \cdot y \in G$ 。
- 有**結合律**： $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- 存在一個特別的元素  $1$  叫作**單位元**，滿足  $1 \cdot x = x \cdot 1 = x$ 。
- 對每一個  $x$  存在  $x^{-1} \in G$  叫作**反元素**，滿足  $x \cdot x^{-1} = x^{-1} \cdot x = 1$ 。

## 定義 (群)

一個**群**由一個集合  $G$  和一個運算  $\cdot$  構成，滿足

- 運算  $\cdot$  是一個函數  $(G, G) \rightarrow G$ ，也就是說  $x \cdot y \in G$ 。
- 有**結合律**： $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- 存在一個特別的元素  $1$  叫作**單位元**，滿足  $1 \cdot x = x \cdot 1 = x$ 。
- 對每一個  $x$  存在  $x^{-1} \in G$  叫作**反元素**，滿足  $x \cdot x^{-1} = x^{-1} \cdot x = 1$ 。

# 數論 – 群

## 定義 (群)

一個**群**由一個集合  $G$  和一個運算  $\cdot$  構成，滿足

- 運算  $\cdot$  是一個函數  $(G, G) \rightarrow G$ ，也就是說  $x \cdot y \in G$ 。
- 有**結合律**： $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- 存在一個特別的元素  $1$  叫作**單位元**，滿足  $1 \cdot x = x \cdot 1 = x$ 。
- 對每一個  $x$  存在  $x^{-1} \in G$  叫作**反元素**，滿足
$$x \cdot x^{-1} = x^{-1} \cdot x = 1。$$

## 定義 (群)

一個**群**由一個集合  $G$  和一個運算  $\cdot$  構成，滿足

- 運算  $\cdot$  是一個函數  $(G, G) \rightarrow G$ ，也就是說  $x \cdot y \in G$ 。
- 有**結合律**： $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- 存在一個特別的元素  $1$  叫作**單位元**，滿足  $1 \cdot x = x \cdot 1 = x$ 。
- 對每一個  $x$  存在  $x^{-1} \in G$  叫作**反元素**，滿足
$$x \cdot x^{-1} = x^{-1} \cdot x = 1$$

# 數論 – 群的例子

- 整數對於加法  $(\mathbb{Z}, +)$  是一個群。
- 旋轉是一個群，如  $0, \pi/2, \pi, 3\pi/2$ 。
- 模  $m$  下的加法，寫作  $\mathbb{Z}/m\mathbb{Z}$ 。
- 一個元素生成的群  $\langle a \rangle \triangleq \{a^k \mid k \in \mathbb{Z}\}$ ，我們把這種群叫作循環群。

# 數論 – 群的例子

- 整數對於加法  $(\mathbb{Z}, +)$  是一個群。
- 旋轉是一個群，如  $0, \pi/2, \pi, 3\pi/2$ 。
- 模  $m$  下的加法，寫作  $\mathbb{Z}/m\mathbb{Z}$ 。
- 一個元素生成的群  $\langle a \rangle \triangleq \{a^k \mid k \in \mathbb{Z}\}$ ，我們把這種群叫作循環群。



# 數論 – 群的例子

- 整數對於加法  $(\mathbb{Z}, +)$  是一個群。
- 旋轉是一個群，如  $0, \pi/2, \pi, 3\pi/2$ 。
- 模  $m$  下的加法，寫作  $\mathbb{Z}/m\mathbb{Z}$ 。
- 一個元素生成的群  $\langle a \rangle \triangleq \{a^k \mid k \in \mathbb{Z}\}$ ，我們把這種群叫作循環群。

# 數論 – 群的例子

- 整數對於加法  $(\mathbb{Z}, +)$  是一個群。
- 旋轉是一個群，如  $0, \pi/2, \pi, 3\pi/2$ 。
- 模  $m$  下的加法，寫作  $\mathbb{Z}/m\mathbb{Z}$ 。
- 一個元素生成的群  $\langle a \rangle \triangleq \{a^k \mid k \in \mathbb{Z}\}$ ，我們把這種群叫作循環群。

# 數論 – 群的例子

- 整數對於加法  $(\mathbb{Z}, +)$  是一個群。
- 旋轉是一個群，如  $0, \pi/2, \pi, 3\pi/2$ 。
- 模  $m$  下的加法，寫作  $\mathbb{Z}/m\mathbb{Z}$ 。
- 一個元素生成的群  $\langle a \rangle \triangleq \{a^k \mid k \in \mathbb{Z}\}$ ，我們把這種群叫作循環群。

## 問題

模  $m$  下的乘法  $(\mathbb{Z}/m\mathbb{Z})^\times$  是一個群嗎？

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

剛剛那樣問並不精確，關鍵應是模  $m$  下哪些元素有反元素？

2 在模 12 下就沒有反元素。

$$xy \equiv 1 \pmod{m} \implies xy = mt' + 1 \implies xy + mt = 1$$

## 問題

給定  $a, b, c$ ， $ax + by = c$  什麼時候有整數解  $(x, y)$ ？

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

剛剛那樣問並不精確，關鍵應是模  $m$  下哪些元素有反元素？

2 在模 12 下就沒有反元素。

$$xy \equiv 1 \pmod{m} \implies xy = mt' + 1 \implies xy + mt = 1$$

## 問題

給定  $a, b, c$ ， $ax + by = c$  什麼時候有整數解  $(x, y)$ ？

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

剛剛那樣問並不精確，關鍵應是模  $m$  下哪些元素有反元素？

2 在模 12 下就沒有反元素。

$$xy \equiv 1 \pmod{m} \implies xy = mt' + 1 \implies xy + mt = 1$$

問題

給定  $a, b, c$ ， $ax + by = c$  什麼時候有整數解  $(x, y)$ ？

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

剛剛那樣問並不精確，關鍵應是模  $m$  下哪些元素有反元素？

2 在模 12 下就沒有反元素。

$$xy \equiv 1 \pmod{m} \implies xy = mt' + 1 \implies xy + mt = 1$$

問題

給定  $a, b, c$ ， $ax + by = c$  什麼時候有整數解  $(x, y)$ ？

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

剛剛那樣問並不精確，關鍵應是模  $m$  下哪些元素有反元素？

2 在模 12 下就沒有反元素。

$$xy \equiv 1 \pmod{m} \implies xy = mt' + 1 \implies xy + mt = 1$$

## 問題

給定  $a, b, c$ ， $ax + by = c$  什麼時候有整數解  $(x, y)$ ？



# 數論 - $ax + by = c$

## 定理

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$$

$$a\mathbb{Z} + b\mathbb{Z} \supseteq \gcd(a, b)\mathbb{Z} :$$

---

```
1 pair<int, int> extend_gcd(int a, int b) {
2     if(b == 0) return {1, 0};
3     else {
4         int k = a/b;
5         pair<int, int> xy = gcd(b, a%b);
6         return {xy.second, xy.first - k * xy.second};
7     }
8 }
```

---

# 數論 - $ax + by = c$

## 定理

$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$$

$$a\mathbb{Z} + b\mathbb{Z} \supseteq \gcd(a, b)\mathbb{Z} :$$

---

```
1 pair<int, int> extend_gcd(int a, int b) {  
2     if(b == 0) return {1, 0};  
3     else {  
4         int k = a/b;  
5         pair<int, int> xy = gcd(b, a%b);  
6         return {xy.second, xy.first - k * xy.second};  
7     }  
8 }
```

---

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

## 引理

$$x \in (\mathbb{Z}/m\mathbb{Z})^\times \iff \gcd(x, m) = 1$$

證明：

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

## 引理

$$x \in (\mathbb{Z}/m\mathbb{Z})^\times \iff \gcd(x, m) = 1$$

**證明：**

$$xy \equiv 1 \pmod{m} \text{ 有解} \iff xy + mt = 1 \text{ 有解}$$

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

## 引理

$$x \in (\mathbb{Z}/m\mathbb{Z})^\times \iff \gcd(x, m) = 1$$

**證明：**

$$\begin{aligned} xy \equiv 1 \pmod{m} \text{ 有解} &\iff xy + mt = 1 \text{ 有解} \\ &\iff \gcd(x, m) = 1 \end{aligned}$$

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

## 問題

$(\mathbb{Z}/m\mathbb{Z})^\times$  有多少元素？也就是  $[1, n]$  中有幾個數和  $n$  互質？

## 定理 (Euler $\varphi$ 函數)

$\varphi(n)$  表示  $[1, n]$  有幾個數和  $n$  互質，則如果  
 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ，則

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

## 問題

$(\mathbb{Z}/m\mathbb{Z})^\times$  有多少元素？也就是  $[1, n]$  中有幾個數和  $n$  互質？

## 定理 (Euler $\varphi$ 函數)

$\varphi(n)$  表示  $[1, n]$  有幾個數和  $n$  互質，則如果  
 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ，則

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

# 數論 – $(\mathbb{Z}/m\mathbb{Z})^\times$

證明這個定理需要用到中國剩餘定理：

定理 (Euler  $\varphi$  函數)

假設  $m = m_1 m_2 \cdots m_k$ ，且  $m_1, m_2, \dots, m_k$  兩兩互質，令

$$\psi(x) = (x \bmod m_1, x \bmod m_2, \dots, x \bmod m_k)$$

則  $\psi(x)$

- 1 是一個  $\mathbb{Z}/m\mathbb{Z}$  到  $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$  的一一對應函數。
- 2 這個函數保持了加法和乘法。



- 1 如果  $p$  是質數，則  $\varphi(p) = p - 1$ 。
- 2 如果  $p$  是質數，則  $\varphi(p^k) = p^{k-1}(p - 1)$ 。
- 3 如果  $m, n$  互質，則  $\varphi(mn) = \varphi(m)\varphi(n)$ 。

- 1 如果  $p$  是質數，則  $\varphi(p) = p - 1$ 。
- 2 如果  $p$  是質數，則  $\varphi(p^k) = p^{k-1}(p - 1)$ 。
- 3 如果  $m, n$  互質，則  $\varphi(mn) = \varphi(m)\varphi(n)$ 。

- 1 如果  $p$  是質數，則  $\varphi(p) = p - 1$ 。
- 2 如果  $p$  是質數，則  $\varphi(p^k) = p^{k-1}(p - 1)$ 。
- 3 如果  $m, n$  互質，則  $\varphi(mn) = \varphi(m)\varphi(n)$ 。

# 數論 – 子群

## 定義

如果  $H \subseteq G$  且  $H$  中任兩個元素的乘積、任一個元素的反元素還在  $H$  裡，我們就說  $H$  是  $G$  的**子群**。

- 所有偶數  $2\mathbb{Z}$  對於加法是  $\mathbb{Z}$  的子群。
- $H \triangleq \{\bar{1}, \bar{2}, \bar{4}\}$  對於乘法是  $\mathbb{Z}/7\mathbb{Z}$  的子群。

# 數論 – Lagrange's Theorem

定理 (Lagrange's theorem)

如果  $H$  是  $G$  的子群，則  $|G| = |G/H| |H|$ ，因此有  $|H| \mid |G|$ 。

定理 (Euler's theorem)

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

# 數論 – Lagrange's Theorem

## 定理 (Lagrange's theorem)

如果  $H$  是  $G$  的子群，則  $|G| = |G/H| |H|$ ，因此有  $|H| \mid |G|$ 。

## 定理 (Euler's theorem)

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

# 數論 – Euler's Theorem

**證明：**

如果  $n$  是最小的正整數使得  $a^n \equiv 1 \pmod{m}$ ，那  $H \triangleq \langle a \rangle = \{1, a, a^2, \dots, a^{n-1}\}$  有  $n$  個元素。

由 Lagrange's theorem， $n \mid |(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$ ，可令  $\varphi(m) = nk$ ，因此  $a^{\varphi(m)} = a^{nk} \equiv 1 \pmod{m}$ 。

## 引理

$$\gcd(a, m) = 1 \implies a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$$

# 數論 – Tonelli-Shanks algorithm

回到一開始的題目：

4  $x^b \equiv c \pmod{p}$ ,  $p$  prime  $\circ$

先看  $b = 2$  的情況  $\circ$

例題 (Square Roots in a Finite Group, 2013 大專院校 pJ)

給定一個質數  $p$  和  $a$ ，請求出  $x^2 \equiv a \pmod{p}$  的解  $x$  或輸出無解  $\circ (a, p < 2^{31})$



# 數論 – Tonelli-Shanks algorithm

回到一開始的題目：

4  $x^b \equiv c \pmod{p}$ ,  $p$  prime.

先看  $b = 2$  的情況。

例題 (Square Roots in a Finite Group, 2013 大專院校 pJ)

給定一個質數  $p$  和  $a$ ，請求出  $x^2 \equiv a \pmod{p}$  的解  $x$  或輸出無解。 $(a, p < 2^{31})$

# 數論 – Tonelli-Shanks algorithm

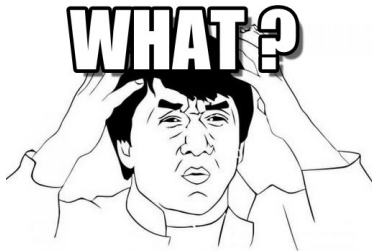
當時這一題有給一個小題示。

- 1 把  $p - 1$  寫作  $p - 1 = 2^s m$ ，其中  $m$  是奇數。
- 2 找一個  $b$  使得  $x^2 \equiv b \pmod{p}$  無解。
- 3 令  $b \leftarrow b^m$ ,  $x \leftarrow a^{(m+1)/2}$ ,  $t \leftarrow a^m$ ，  
可以驗證  $x^2 \equiv at \pmod{p}$ 。
- 4 想辦法把  $t$  調成 1 你就獲勝了。

# 數論 – Tonelli-Shanks algorithm

當時這一題有給一個小題示。

- 1 把  $p - 1$  寫作  $p - 1 = 2^s m$ ，其中  $m$  是奇數。
- 2 找一個  $b$  使得  $x^2 \equiv b \pmod{p}$  無解。
- 3 令  $b \leftarrow b^m$ ,  $x \leftarrow a^{(m+1)/2}$ ,  $t \leftarrow a^m$ ，  
可以驗證  $x^2 \equiv at \pmod{p}$ 。
- 4 想辦法把  $t$  調成 1 你就獲勝了。



# 數論 – 原根

要有一點先備知識。

## 定理

$$(\mathbb{Z}/m\mathbb{Z})^\times \text{ 是一個循環群 } \iff m = 1, 2, 4, p^k, 2p^k$$

## 定義

如果  $(\mathbb{Z}/m\mathbb{Z})^\times = \langle a \rangle$ ，我們就說  $a$  是模  $m$  下的原根。

# 數論 – 原根

要有一點先備知識。

## 定理

$$(\mathbb{Z}/m\mathbb{Z})^\times \text{ 是一個循環群 } \iff m = 1, 2, 4, p^k, 2p^k$$

## 定義

如果  $(\mathbb{Z}/m\mathbb{Z})^\times = \langle a \rangle$ ，我們就說  $a$  是模  $m$  下的原根。

# 數論 – 原根

要有一點先備知識。

## 定理

$$(\mathbb{Z}/m\mathbb{Z})^\times \text{ 是一個循環群 } \iff m = 1, 2, 4, p^k, 2p^k$$

## 定義

如果  $(\mathbb{Z}/m\mathbb{Z})^\times = \langle a \rangle$ ，我們就說  $a$  是模  $m$  下的原根。

# 數論 – 原根

舉個例子， $m = 11, a = 2$ 。

$\mathbb{Z}/10\mathbb{Z}$	0	1	2	3	4	5	6	7	8	9
$(\mathbb{Z}/11\mathbb{Z})^\times$	1	2	4	8	5	10	9	7	3	6

$$2 + 4 \equiv 6 \pmod{10}$$

$$\updownarrow \quad \quad \updownarrow \quad \quad \updownarrow$$

$$4 \times 5 \equiv 9 \pmod{11}$$

可定義  $\log_a$ ，如  $\log_2(9) = 6$ 。

# 數論 – 原根

舉個例子， $m = 11, a = 2$ 。

$\mathbb{Z}/10\mathbb{Z}$	0	1	2	3	4	5	6	7	8	9
$(\mathbb{Z}/11\mathbb{Z})^\times$	1	2	4	8	5	10	9	7	3	6

$$2 + 4 \equiv 6 \pmod{10}$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$4 \times 5 \equiv 9 \pmod{11}$$

可定義  $\log_a$ ，如  $\log_2(9) = 6$ 。



# 數論 – 原根

舉個例子， $m = 11, a = 2$ 。

$\mathbb{Z}/10\mathbb{Z}$	0	1	2	3	4	5	6	7	8	9
$(\mathbb{Z}/11\mathbb{Z})^\times$	1	2	4	8	5	10	9	7	3	6

$$2 + 4 \equiv 6 \pmod{10}$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$4 \times 5 \equiv 9 \pmod{11}$$

可定義  $\log_a$ ，如  $\log_2(9) = 6$ 。

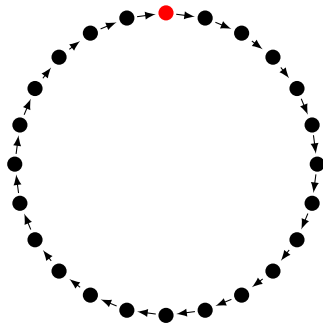
# 數論 – 原根

## 問題

如何找一個模  $m$  下的原根？

# 數論 – Tonelli-Shanks algorithm

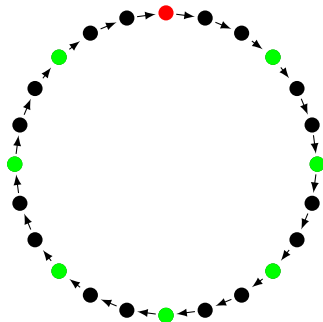
$$p = 25, \quad p - 1 = 2^s \cdot m = 2^3 \cdot 3$$



# 數論 – Tonelli-Shanks algorithm

$$p = 25, \quad p - 1 = 2^s \cdot m = 2^3 \cdot 3$$

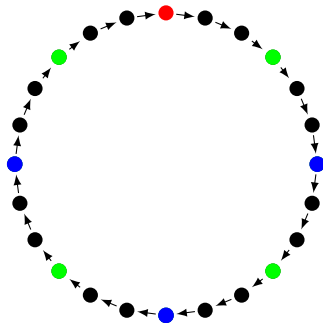
$$\log(t) = \log(a^m) = m \log(a) \circ$$



# 數論 – Tonelli-Shanks algorithm

$$p = 25, \quad p - 1 = 2^s \cdot m = 2^3 \cdot 3$$

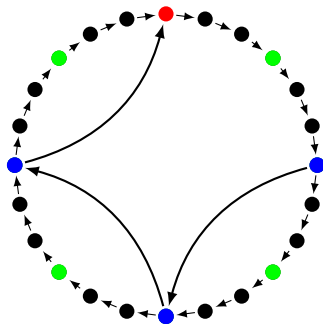
$\log(t) = \log(a^m) = m \log(a)$ 。如果  $x \leftarrow b$ ，那  $t \leftarrow b^2$ 。



# 數論 – Tonelli-Shanks algorithm

$$p = 25, \quad p - 1 = 2^s \cdot m = 2^3 \cdot 3$$

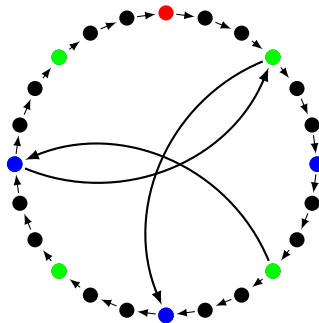
$\log(t) = \log(a^m) = m \log(a)$ 。如果  $x \leftarrow b$ ，那  $t \leftarrow b^2$ 。



# 數論 – Tonelli-Shanks algorithm

$$p = 25, \quad p - 1 = 2^s \cdot m = 2^3 \cdot 3$$

$\log(t) = \log(a^m) = m \log(a)$ 。如果  $x \leftarrow b$ ，那  $t \leftarrow b^2$ 。



# 數論 – Tonelli-Shanks algorithm

```
1 while (t != 1) {  
2     int k = 0, tp = t, tb = b;  
3     while (tp != 1) tp = (tp * tp) % p, k++;  
4     for (int i=0; i<s-k-1; i++) tb = (tb * tb) % p;  
5     x = x * tb % p;  
6     t = t * tb * tb % p;  
7 }
```

## 習題

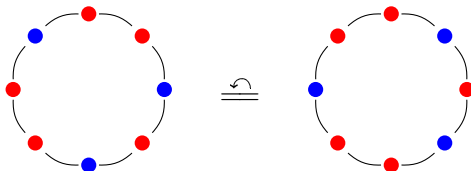
把剩下的細節弄清楚！



# Burnside's lemma

## 例題

用  $M$  種寶石可以做出多少  $N$  個寶石的項鍊，假設旋轉相同視為相同。



# Burnside's lemma – 問題的數學描述

- 旋轉會構成一個群  $G \triangleq \langle g \rangle$ 。
- 物品（項鍊）會構成一個集合  $X$ 。
- 用  $G$  把  $X$  分門別類，寫作  $X/G$ 。

# Burnside's lemma – 問題的數學描述

- 旋轉會構成一個群  $G \triangleq \langle g \rangle$ 。
- 物品（項鍊）會構成一個集合  $X$ 。
- 用  $G$  把  $X$  分門別類，寫作  $X/G$ 。

# Burnside's lemma – 問題的數學描述

- 旋轉會構成一個群  $G \triangleq \langle g \rangle$ 。
- 物品（項鍊）會構成一個集合  $X$ 。
- 用  $G$  把  $X$  分門別類，寫作  $X/G$ 。

# Burnside's lemma – 一些定義

## 定義

假設  $X$  是一個集合，我們說  $G$  透過一個運算，作用在  $X$  上，如果以下三點成立：

- $g \cdot x \in X$ 。
- $(gh) \cdot x = g \cdot (hx)$ 。
- 如果  $1$  是  $G$  的單位元，則  $1 \cdot x = x$ 。

# Burnside's lemma – 一些定義

## 定義

假設  $X$  是一個集合，我們說  $G$  透過一個運算  $\cdot$  作用在  $X$  上，如果以下三點成立：

- 1  $g \cdot x \in X$ 。
- 2  $(gh) \cdot x = g \cdot (hx)$ 。
- 3 如果  $1$  是  $G$  的單位元，則  $1 \cdot x = x$ 。

# Burnside's lemma – 一些定義

## 定義

假設  $X$  是一個集合，我們說  $G$  透過一個運算  $\cdot$  作用在  $X$  上，如果以下三點成立：

- 1  $g \cdot x \in X$ 。
- 2  $(gh) \cdot x = g \cdot (hx)$ 。
- 3 如果  $1$  是  $G$  的單位元，則  $1 \cdot x = x$ 。

# Burnside's lemma – 一些定義

## 定義

假設  $X$  是一個集合，我們說  $G$  透過一個運算  $\cdot$  作用在  $X$  上，如果以下三點成立：

- 1  $g \cdot x \in X$ 。
- 2  $(gh) \cdot x = g \cdot (hx)$ 。
- 3 如果  $1$  是  $G$  的單位元，則  $1 \cdot x = x$ 。



# Burnside's lemma – 再一些定義

## 定義

- 1  $G_x \triangleq \{g \in G : gx = x\}$ ，也就是固定  $x$  下，所有不會動到  $x$  的作用。
- 2  $X^g \triangleq \{x \in X : gx = x\}$ ，也就是固定一個作用  $g$  下的不動點。
- 3  $Gx \triangleq \{gx : g \in G\}$ ，也被稱作是  $x$  在  $G$  下的軌道。
- 4  $X/G \triangleq \{Gx : x \in X\}$ ，也就是  $X$  在  $G$  下所有的軌道。

# Burnside's lemma – 再一些定義

## 定義

- 1  $G_x \triangleq \{g \in G : gx = x\}$ ，也就是固定  $x$  下，所有不會動到  $x$  的作用。
- 2  $X^g \triangleq \{x \in X : gx = x\}$ ，也就是固定一個作用  $g$  下的**不動點**。
- 3  $Gx \triangleq \{gx : g \in G\}$ ，也被稱作是  $x$  在  $G$  下的**軌道**。
- 4  $X/G \triangleq \{Gx : x \in X\}$ ，也就是  $X$  在  $G$  下所有的軌道。

# Burnside's lemma – 再一些定義

## 定義

- 1  $G_x \triangleq \{g \in G : gx = x\}$ ，也就是固定  $x$  下，所有不會動到  $x$  的作用。
- 2  $X^g \triangleq \{x \in X : gx = x\}$ ，也就是固定一個作用  $g$  下的**不動點**。
- 3  $Gx \triangleq \{gx : g \in G\}$ ，也被稱作是  $x$  在  $G$  下的**軌道**。
- 4  $X/G \triangleq \{Gx : x \in X\}$ ，也就是  $X$  在  $G$  下所有的軌道。

# Burnside's lemma – 再一些定義

## 定義

- 1  $G_x \triangleq \{g \in G : gx = x\}$ ，也就是固定  $x$  下，所有不會動到  $x$  的作用。
- 2  $X^g \triangleq \{x \in X : gx = x\}$ ，也就是固定一個作用  $g$  下的**不動點**。
- 3  $Gx \triangleq \{gx : g \in G\}$ ，也被稱作是  $x$  在  $G$  下的**軌道**。
- 4  $X/G \triangleq \{Gx : x \in X\}$ ，也就是  $X$  在  $G$  下所有的軌道。

# Burnside's lemma

定理 (Burnside's lemma)

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

也就是說把每一個旋轉下的不動點加起來，除以旋轉的數量，就是種類數！

# Burnside's lemma

定理 (Burnside's lemma)

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

也就是說把每一個旋轉下的不動點加起來，除以旋轉的數量，就是種類數！

# Burnside's lemma – 證明

證明：

$$\begin{aligned}\frac{1}{|G|} \sum_{g \in G} |X^g| &= \frac{1}{|G|} \#\{(x, g) \mid x \in X, g \in G, xg = g\} \\&= \frac{1}{|G|} \sum_{x \in X} |G_x| \\&\stackrel{(1)}{=} \frac{1}{|G|} \sum_{x \in X} \frac{|G|}{|Gx|} \\&\stackrel{(2)}{=} \sum_{Gx \in X/G} \sum_{x \in Gx} \frac{1}{|Gx|} = \sum_{Gx \in X/G} 1 \\&= |X/G|\end{aligned}$$

# Burnside's lemma – 證明

關鍵：

$$1 \quad |G| = |Gx| |G_x|$$

$$2 \quad X = \bigsqcup_{Gx \in G/X} Gx$$



# Burnside's lemma – 應用

回到原本的例題，現在我們要算每個旋轉  $g$  下的不動點  $X^g$ 。

注意：不是只有  $\curvearrowright$  而已，有  $1, \curvearrowright, \curvearrowright^2, \dots$ 。

## 問題

如果今天在平面上旋轉  $\pi/2$  和對  $x$  軸鏡射要視為相同，要考慮哪些旋轉？

# Burnside's lemma – 應用

回到原本的例題，現在我們要算每個旋轉  $g$  下的不動點  $X^g$ 。

**注意：**不是只有  $\curvearrowright$  而已，有  $1, \curvearrowright, \curvearrowright^2, \dots$ 。

## 問題

如果今天在平面上旋轉  $\pi/2$  和對  $x$  軸鏡射要視為相同，要考慮哪些旋轉？

# Burnside's lemma – 應用

回到原本的例題，現在我們要算每個旋轉  $g$  下的不動點  $X^g$ 。

**注意：**不是只有  $\curvearrowright$  而已，有  $1, \curvearrowright, \curvearrowright^2, \dots$ 。

## 問題

如果今天在平面上旋轉  $\pi/2$  和對  $x$  軸鏡射要視為相同，要考慮哪些旋轉？

# Burnside's lemma – 應用

哪些項鍊是旋轉  $\curvearrowright^k$  下的不動點？有幾個觀察：

1 首先注意到  $X^{\curvearrowright^k} = X^{\curvearrowright^{\gcd(k, N)}}$

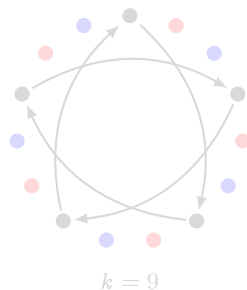
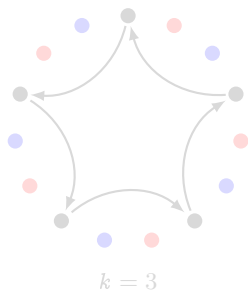


Figure:  $n = 15$

# Burnside's lemma – 應用

哪些項鍊是旋轉  $\curvearrowright^k$  下的不動點？有幾個觀察：

**1** 首先注意到  $X^{\curvearrowright^k} = X^{\curvearrowright^{\gcd(k, N)}}$

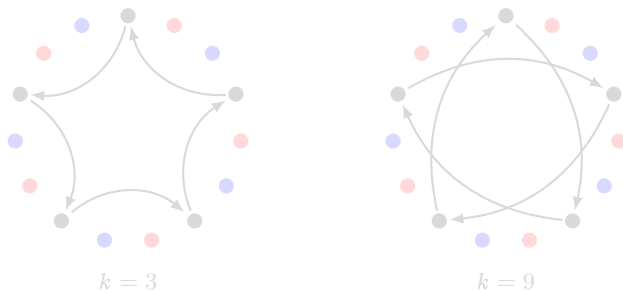


Figure:  $n = 15$

# Burnside's lemma – 應用

哪些項鍊是旋轉  $\curvearrowright^k$  下的不動點？有幾個觀察：

1 首先注意到  $X^{\curvearrowright^k} = X^{\curvearrowright^{\gcd(k, N)}}$

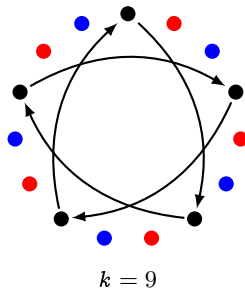
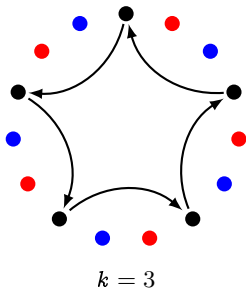


Figure:  $n = 15$

# Burnside's lemma – 應用

2 如果  $d \triangleq \gcd(k, N)$ ，則

$$\left| X^{\curvearrowright^k} \right| = \left| X^{\curvearrowright^{\gcd(k, N)}} \right| = M^d$$

3 用 Burnside's lemma 得出

$$|X/G| = \sum_{d|N} \#\{k \mid \gcd(k, N) = d\} M^d$$

## 問題

對於  $d \mid N$  的  $d$ ， $\#\{k \mid \gcd(k, N) = d\}$  如何求？

# Burnside's lemma – 應用

2 如果  $d \triangleq \gcd(k, N)$ ，則

$$\left| X^{\curvearrowright^k} \right| = \left| X^{\curvearrowright^{\gcd(k, N)}} \right| = M^d$$

3 用 Burnside's lemma 得出

$$|X/G| = \sum_{d|N} \#\{k \mid \gcd(k, N) = d\} M^d$$

## 問題

對於  $d \mid N$  的  $d$ ， $\#\{k \mid \gcd(k, N) = d\}$  如何求？



# Burnside's lemma – 應用

因為  $d \mid N$  ,

$$\#\{k \mid \gcd(k, N) = d\} = \#\{k \mid \gcd(k, N/d) = 1\} = \varphi(N/d)$$

總結答案：

$$\sum_{d \mid N} \varphi(N/d) M^d$$

## Burnside's lemma – 應用

因為  $d \mid N$  ,

$$\#\{k \mid \gcd(k, N) = d\} = \#\{k \mid \gcd(k, N/d) = 1\} = \varphi(N/d)$$

總結答案：

$$\sum_{d \mid N} \varphi(N/d) M^d$$

## C++17 Features 分享！

## ■ Class template deduction

---

```
pair pr("hao"s, 123);
```

---

## ■ Structure bindings

---

```
auto [a, b] = pair("hao"s, 123);
```

---

## ■ Initializers in if

---

```
if (int x = fun(); x > 3) { ... }
```

---

## ■ std::clamp

---

```
assert(clamp(a, low, high) == min(max(a, low), high));
```

---

## ■ Class template deduction

---

```
pair pr("hao"s, 123);
```

---

## ■ Structure bindings

---

```
auto [a, b] = pair("hao"s, 123);
```

---

## ■ Initializers in if

---

```
if (int x = fun(); x > 3) { ... }
```

---

## ■ std::clamp

---

```
assert(clamp(a, low, high) == min(max(a, low), high));
```

---

## ■ Class template deduction

---

```
pair pr("hao"s, 123);
```

---

## ■ Structure bindings

---

```
auto [a, b] = pair("hao"s, 123);
```

---

## ■ Initializers in if

---

```
if (int x = fun(); x > 3) { ... }
```

---

## ■ std::clamp

---

```
assert(clamp(a, low, high) == min(max(a, low), high));
```

---

## ■ Class template deduction

---

```
pair pr("hao"s, 123);
```

---

## ■ Structure bindings

---

```
auto [a, b] = pair("hao"s, 123);
```

---

## ■ Initializers in if

---

```
if (int x = fun(); x > 3) { ... }
```

---

## ■ std::clamp

---

```
assert(clamp(a, low, high) == min(max(a, low), high));
```

---

# 組合賽局 線性代數

我們先看一題遊戲題。

## 例題 (Takeover Wars, ACM-ICPC World Final pL)

兩個人玩一個遊戲，A 有  $a_1, a_2, \dots, a_k$  個數字，B 有  $b_1, b_2, \dots, b_h$  個數字。由 A 先開始行動，每次行動可以選一個進行：

- 1 融合：選兩個自己的數字  $x, y$ ，把  $x, y$  拿掉換成  $x + y$ 。
- 2 吃掉：選一個自己的數字  $x$  和對方的數字  $y$ ，如果  $x > y$ ，可以把  $y$  拿掉。
- 3 喵 PASS  $\sim \setminus (\cdot \cdot \cdot)$

誰沒有數字了就輸了，問誰會贏？( $k, h \leq 10^5$ )

有些題目沒想出來看到結論會氣死...



# 組合賽局 線性代數

我們先看一題遊戲題。

## 例題 (Takeover Wars, ACM-ICPC World Final pL)

兩個人玩一個遊戲，A 有  $a_1, a_2, \dots, a_k$  個數字，B 有  $b_1, b_2, \dots, b_h$  個數字。由 A 先開始行動，每次行動可以選一個進行：

- 1 融合：選兩個自己的數字  $x, y$ ，把  $x, y$  拿掉換成  $x + y$ 。
- 2 吃掉：選一個自己的數字  $x$  和對方的數字  $y$ ，如果  $x > y$ ，可以把  $y$  拿掉。
- 3 喵 PASS  $\sim \setminus (\cdot \cdot \cdot)$

誰沒有數字了就輸了，問誰會贏？( $k, h \leq 10^5$ )

有些題目沒想出來看到結論會氣死...

# 線性代數 – 例題

再看一題遊戲題。

例題 (Game on Bipartite Graph, 2015-2016 Saratov SU Contest)

給一個二分圖  $G$  和一個起點  $v$ ，兩人玩一個遊戲：輪流選一條和現在的點  $v$  相鄰的邊  $(v, u)$ ，並沿著這條邊走到  $u$ 。走過的邊就不能再走了，誰沒有辦法再走就輸了。問你先手贏還是後手贏。 $(|V| \leq 100)$

# 線性代數 – 例題

再看一題遊戲題。

例題 (Game on Bipartite Graph, 2015-2016 Saratov SU Contest)

給一個二分圖  $G$  和一個起點  $v$ ，兩人玩一個遊戲：輪流選一條和現在的點  $v$  相鄰的邊  $(v, u)$ ，並沿著這條邊走到  $u$ 。走過的邊就不能再走了，誰沒有辦法再走就輸了。問你先手贏還是後手贏。 $(|V| \leq 100)$

# 線性代數 – 例題

假設二分圖的兩個點集是  $X, Y$  每個人在他的回合一定是固定從某個點集出發。

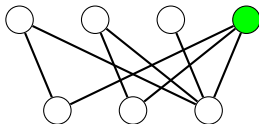
想一想後手什麼時候會贏？



# 線性代數 – 例題

假設二分圖的兩個點集是  $X, Y$  每個人在他的回合一定是固定從某個點集出發。

想一想後手什麼時候會贏？



# 線性代數 – 例題

假設二分圖的兩個點集是  $X, Y$  每個人在他的回合一定是固定從某個點集出發。不妨假設先手出發的是  $X$ 。

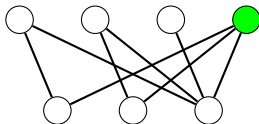
想一想後手什麼時候會贏？



# 線性代數 – 例題

假設二分圖的兩個點集是  $X, Y$  每個人在他的回合一定是固定從某個點集出發。不妨假設先手出發的是  $X$ 。

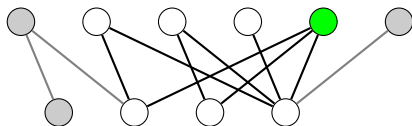
想一想後手什麼時候會贏？



# 線性代數 – 例題

假設二分圖的兩個點集是  $X, Y$  每個人在他的回合一定是固定從某個點集出發。不妨假設先手出發的是  $X$ 。

想一想後手什麼時候會贏？





# 線性代數 – 例題

現在對於  $X$  的第  $i$  個點，如果他連到下面  $i_1, i_2, \dots, i_k$  個點，就令  $v_i = \sum 2^{i_t}$ 。

從剛才的討論可以知道如果存在  $v_{j_1}, v_{j_2}, \dots, v_{j_m}$  使得

$$v_s \in \{j_t\} \quad \text{且} \quad v_{i_1} \oplus v_{i_2} \oplus \dots \oplus v_{i_m}$$

則後手會贏。

## 問題

- 1 怎麼找  $j_1, j_2, \dots, j_m$ ？
- 2 這個條件是否也是**必要條件**？

# 線性代數 – 例題

現在對於  $X$  的第  $i$  個點，如果他連到下面  $i_1, i_2, \dots, i_k$  個點，就令  $v_i = \sum 2^{i_t}$ 。

從剛才的討論可以知道如果存在  $v_{j_1}, v_{j_2}, \dots, v_{j_m}$  使得

$$v_s \in \{j_t\} \quad \text{且} \quad v_{i_1} \oplus v_{i_2} \oplus \dots \oplus v_{i_m}$$

則後手會贏。

## 問題

- 1 怎麼找  $j_1, j_2, \dots, j_m$ ？
- 2 這個條件是否也是**必要條件**？

# 線性代數 – 例題

現在對於  $X$  的第  $i$  個點，如果他連到下面  $i_1, i_2, \dots, i_k$  個點，就令  $v_i = \sum 2^{i_t}$ 。

從剛才的討論可以知道如果存在  $v_{j_1}, v_{j_2}, \dots, v_{j_m}$  使得

$$v_s \in \{j_t\} \quad \text{且} \quad v_{i_1} \oplus v_{i_2} \oplus \dots \oplus v_{i_m}$$

則後手會贏。

## 問題

- 1 怎麼找  $j_1, j_2, \dots, j_m$ ？
- 2 這個條件是否也是**必要條件**？

# 線性代數 – 例題

這些  $v_i$  其實可以看作是  $\mathbb{F}_2^n$  向量空間中的向量，其中  $n \triangleq |Y|$ 。  
即  $1 \triangleq (1, 0, 0, \dots, 0)$ ,  $2 \triangleq (0, 1, 0, \dots, 0)$  等等。

而條件也可以改寫成找到  $\{j_t\}$ ,  $v_s \neq j_t$  使得

$$v_s = v_{j_1} + v_{j_2} + \dots + v_{j_m}$$

在向量空間中我們會問更一般的問題：解

$$u = a_1 v_1 + a_2 v_2 + \dots + a_m v_m$$

## 線性代數 – 例題

這些  $v_i$  其實可以看作是  $\mathbb{F}_2^n$  向量空間中的向量，其中  $n \triangleq |Y|$ 。  
即  $1 \triangleq (1, 0, 0, \dots, 0)$ ,  $2 \triangleq (0, 1, 0, \dots, 0)$  等等。

而條件也可以改寫成找到  $\{j_t\}$ ,  $v_s \neq j_t$  使得

$$v_s = v_{j_1} + v_{j_2} + \dots + v_{j_m}$$

在向量空間中我們會問更一般的問題：解

$$u = a_1 v_1 + a_2 v_2 + \dots + a_m v_m$$

# 線性代數 – 例題

這些  $v_i$  其實可以看作是  $\mathbb{F}_2^n$  向量空間中的向量，其中  $n \triangleq |Y|$ 。  
即  $1 \triangleq (1, 0, 0, \dots, 0)$ ,  $2 \triangleq (0, 1, 0, \dots, 0)$  等等。

而條件也可以改寫成找到  $\{j_t\}$ ,  $v_s \neq j_t$  使得

$$v_s = v_{j_1} + v_{j_2} + \dots + v_{j_m}$$

在**向量空間**中我們會問更一般的問題：解

$$u = a_1 v_1 + a_2 v_2 + \dots + a_m v_m$$

# 線性代數 – 例題

其實就是

$$u = \begin{bmatrix} v_1 & v_2 & \cdots & v_m \end{bmatrix} a$$

因此追根到底就是要

問題

解  $b = Ax$ 。

這有一個大家都知道的高斯消去法。

# 線性代數 – 例題

其實就是

$$u = \begin{bmatrix} v_1 & v_2 & \cdots & v_m \end{bmatrix} a$$

因此追根到底就是要

問題

解  $b = Ax$ 。

這有一個大家都知道的高斯消去法。



# 線性代數 – 例題

其實就是

$$u = \begin{bmatrix} v_1 & v_2 & \cdots & v_m \end{bmatrix} a$$

因此追根到底就是要

問題

解  $b = Ax$ 。

這有一個大家都知道的高斯消去法。

# 線性代數 – 高斯消去法

---

```
void Gauss(int n, int **A) {  
    for (int i=0; i<n; i++) {  
        for (int j=i; j<n; j++) {  
            if (abs(A[j][i]) > EPS) {  
                swap(A[j], A[i]);  
                break;  
            }  
            if (j == n-1) goto loop_end;  
        }  
    }  
}
```

---

---

```
        for (int j=0; j<n; j++) {  
            if (j == i) continue;  
            double r = A[j][i] / A[i][i];  
            for (int k=i; k<n; k++) {  
                A[j][k] -= A[i][k] * r;  
            }  
        }  
loop_end: ;  
    }  
}
```

---

# 線性代數 – 高斯消去法

高斯消去法有很多應用：

- 1 解  $Ax = b$ 。
- 2 計算矩陣  $A$  的維度。
- 3 計算  $A^{-1}$ 。
- 4 計算  $\det A$ 。

# 線性代數 – 高斯消去法

高斯消去法有很多應用：

- 1 解  $Ax = b$ 。
- 2 計算矩陣  $A$  的**維度**。
- 3 計算  $A^{-1}$ 。
- 4 計算  $\det A$ 。

# 線性代數 – 高斯消去法

高斯消去法有很多應用：

- 1 解  $Ax = b$ 。
- 2 計算矩陣  $A$  的維度。
- 3 計算  $A^{-1}$ 。
- 4 計算  $\det A$ 。

# 線性代數 – 高斯消去法

高斯消去法有很多應用：

- 1 解  $Ax = b$ 。
- 2 計算矩陣  $A$  的維度。
- 3 計算  $A^{-1}$ 。
- 4 計算  $\det A$ 。

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \xrightarrow[\leftarrow +]{-1} \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} \mid \times (-1) \Rightarrow \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \xrightarrow[\leftarrow -2]{+} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

# 線性代數 – 高斯消去法

高斯消去法有很多應用：

- 1 解  $Ax = b$ 。
- 2 計算矩陣  $A$  的維度。
- 3 計算  $A^{-1}$ 。
- 4 計算  $\det A$ 。

$$\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \xrightarrow[\leftarrow +]{\quad}^{-1} \Rightarrow \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} \quad | \times (-1) \Rightarrow \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \xrightarrow[\quad]{\leftarrow +}_{-2} \Rightarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} \Rightarrow \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix}$$

# 線性代數 – 高斯消去法

高斯消去法有很多應用：

- 1 解  $Ax = b$ 。
- 2 計算矩陣  $A$  的維度。
- 3 計算  $A^{-1}$ 。
- 4 計算  $\det A$ 。



# 線性代數

我們只剩下最後一個問題：為何剛剛那個條件是必要條件。

## 定義

對於向量  $v_1, v_2, \dots, v_n$ ，

- 1 如果  $a_1v_1 + a_2v_2 + \dots + a_nv_n = 0 \implies a_i = 0, \forall i$ ，也就是沒有一個向量可以用其他的向量「湊出來」，我們就說這些向量**線性獨立**。
- 2 如果所有  $V$  裡的其他向量  $v$  都可以寫成  $v = a_1v_1 + a_2v_2 + \dots + a_nv_n$ ，我們就說這些向量是  $V$  的一個**生成集**。
- 3 如果這些向量同時是線性獨立並且生成  $V$ ，我們就說這些向量是  $V$  的一個**基底**。

# 線性代數

我們只剩下最後一個問題：為何剛剛那個條件是必要條件。

## 定義

對於向量  $v_1, v_2, \dots, v_n$ ，

- 1 如果  $a_1v_1 + a_2v_2 + \dots + a_nv_n = 0 \implies a_i = 0, \forall i$ ，也就是沒有一個向量可以用其他的向量「湊出來」，我們就說這些向量**線性獨立**。
- 2 如果所有  $V$  裡的其他向量  $v$  都可以寫成  $v = a_1v_1 + a_2v_2 + \dots + a_nv_n$ ，我們就說這些向量是  $V$  的一個**生成集**。
- 3 如果這些向量同時是線性獨立並且生成  $V$ ，我們就說這些向量是  $V$  的一個**基底**。

# 線性代數

## 定理

一個向量空間中，任何基底的大小是固定的。因此這個向量空間的**維度**就定義成任一個基底的大小。

假設

$$v_s = a_1 v_1 + a_2 v_2 + \dots + a_m v_m$$

無解，就表示

$\begin{bmatrix} v_1 & v_2 & \dots & v_m & v_s \end{bmatrix}$  的維度比  $\begin{bmatrix} v_1 & v_2 & \dots & v_m \end{bmatrix}$  多 1。

# 線性代數

## 定理

一個向量空間中，任何基底的大小是固定的。因此這個向量空間的**維度**就定義成任一個基底的大小。

假設

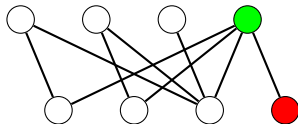
$$v_s = a_1 v_1 + a_2 v_2 + \dots + a_m v_m$$

無解，就表示

$\begin{bmatrix} v_1 & v_2 & \cdots & v_m & v_s \end{bmatrix}$  的維度比  $\begin{bmatrix} v_1 & v_2 & \cdots & v_m \end{bmatrix}$  多 1。

# 線性代數

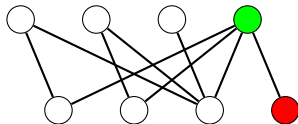
現在把圖上增加一個新點當起點，並且只連到本來的起點，然後先後手互換。



會對應到矩陣  $\begin{bmatrix} | & | & \cdots & | & | \\ v_1 & v_2 & \cdots & v_m & v_s \\ | & | & \cdots & | & | \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}^T$

# 線性代數

現在把圖上增加一個新點當起點，並且只連到本來的起點，然後先後手互換。



會對應到矩陣  $\begin{bmatrix} | & | & \cdots & | & | \\ \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_m & \mathbf{v}_s \\ | & | & \cdots & | & | \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}^T$

# 線性代數

## 定理

用  $\text{rank}(A)$  表示矩陣  $A$  的維度，則  $\text{rank}(A) = \text{rank}(A^T)$ 。

$$\begin{array}{ccc} \text{rank} = x & & \text{rank} = x + 1 \\ \left[ \begin{array}{cccc} v_1 & v_2 & \cdots & v_m \end{array} \right] & \xrightarrow{+1} & \left[ \begin{array}{ccccc} v_1 & v_2 & \cdots & v_m & v_s \end{array} \right] \\ \parallel & & \parallel \\ \left[ \begin{array}{cccc} \begin{array}{|c|} v_1 \end{array} & \begin{array}{|c|} v_2 \end{array} & \cdots & \begin{array}{|c|} v_m \end{array} \\ \hline 0 & 0 & \cdots & 0 \end{array} \right] & \xrightarrow{+1} & \left[ \begin{array}{ccccc} \begin{array}{|c|} v_1 \end{array} & \begin{array}{|c|} v_2 \end{array} & \cdots & \begin{array}{|c|} v_m \end{array} & \begin{array}{|c|} v_s \end{array} \\ \hline 0 & 0 & \cdots & 0 & 1 \end{array} \right] \\ \text{rank} = x & & \text{rank} = x + 1 \end{array}$$

# 線性代數

## 定理

用  $\text{rank}(A)$  表示矩陣  $A$  的維度，則  $\text{rank}(A) = \text{rank}(A^T)$ 。

$$\begin{array}{ccc} \text{rank} = x & & \text{rank} = x + 1 \\ \left[ \begin{array}{cccc} v_1 & v_2 & \cdots & v_m \end{array} \right] & \xrightarrow{+1} & \left[ \begin{array}{ccccc} v_1 & v_2 & \cdots & v_m & v_s \end{array} \right] \\ \parallel & & \parallel \\ \left[ \begin{array}{cccc} \begin{array}{|c|} v_1 \end{array} & \begin{array}{|c|} v_2 \end{array} & \cdots & \begin{array}{|c|} v_m \end{array} \\ \hline 0 & 0 & \cdots & 0 \end{array} \right] & \xrightarrow{+1} & \left[ \begin{array}{ccccc} \begin{array}{|c|} v_1 \end{array} & \begin{array}{|c|} v_2 \end{array} & \cdots & \begin{array}{|c|} v_m \end{array} & \begin{array}{|c|} v_s \end{array} \\ \hline 0 & 0 & \cdots & 0 & 1 \end{array} \right] \\ \text{rank} = x & & \text{rank} = x + 1 \end{array}$$



# 線性代數

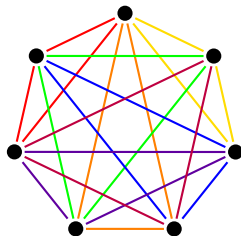
加了  $(0, 0, \dots, 0, 1)$  以後 rank 不變，表示  $(0, 0, \dots, 0, 1)$  可被其他列向量線性組合出  $\Rightarrow$  原本的先手贏。

# 線性代數

加了  $(0, 0, \dots, 0, 1)$  以後 rank 不變，表示  $(0, 0, \dots, 0, 1)$  可被其他列向量線性組合出  $\Rightarrow$  原本的先手贏。

例題 (均衡忍者出任務, 2015 ioi-camp)

請把  $K_n$  分解成互斥的三角形，其中  $n = 2^k - 1$ 。



如果可以找到函數  $f(x, y)$  使得  $x \neq y \implies f(x, y) \neq x, y$  且  $f(x, f(x, y)) = y, f(f(x, y), y) = x$ ，我們就做完了！

# Others – Prüfer sequence

## 例題

求  $n$  個有編號的點可以形成多少種不同的樹。

答案是  $n^{n-2}$ 。

# Others – Prüfer sequence

## 例題

求  $n$  個有編號的點可以形成多少種不同的樹。

答案是  $n^{n-2}$ 。

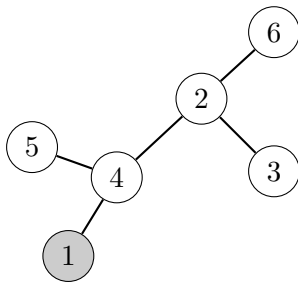
## Others – Prüfer sequence

每次找葉子中編號最小的點  $u$ ，假設他連出去的邊是  $(u, v)$ ，就記下  $v$  的編號，並把  $v$  和邊  $(u, v)$  從圖上刪除。重複直到圖上就只剩一個點了。

6

## Others – Prüfer sequence

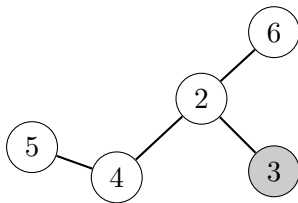
每次找葉子中編號最小的點  $u$ ，假設他連出去的邊是  $(u, v)$ ，就記下  $v$  的編號，並把  $v$  和邊  $(u, v)$  從圖上刪除。重複直到圖上就只剩一個點了。





## Others – Prüfer sequence

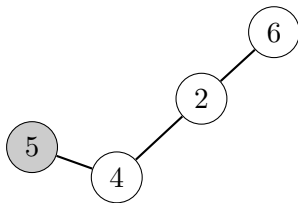
每次找葉子中編號最小的點  $u$ ，假設他連出去的邊是  $(u, v)$ ，就記下  $v$  的編號，並把  $v$  和邊  $(u, v)$  從圖上刪除。重複直到圖上就只剩一個點了。



$4 \rightarrow 2$

## Others – Prüfer sequence

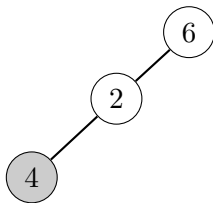
每次找葉子中編號最小的點  $u$ ，假設他連出去的邊是  $(u, v)$ ，就記下  $v$  的編號，並把  $v$  和邊  $(u, v)$  從圖上刪除。重複直到圖上就只剩一個點了。



$4 \rightarrow 2 \rightarrow 4$

## Others – Prüfer sequence

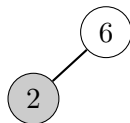
每次找葉子中編號最小的點  $u$ ，假設他連出去的邊是  $(u, v)$ ，就記下  $v$  的編號，並把  $v$  和邊  $(u, v)$  從圖上刪除。重複直到圖上就只剩一個點了。



$4 \rightarrow 2 \rightarrow 4 \rightarrow 2$

## Others – Prüfer sequence

每次找葉子中編號最小的點  $u$ ，假設他連出去的邊是  $(u, v)$ ，就記下  $v$  的編號，並把  $v$  和邊  $(u, v)$  從圖上刪除。重複直到圖上就只剩一個點了。

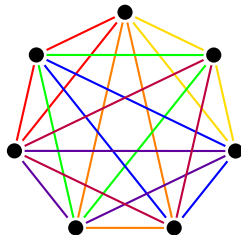


$$4 \rightarrow 2 \rightarrow 4 \rightarrow 2 \rightarrow 6$$

# Others – 構造

例題 (均衡忍者出任務, 2015 ioi-camp)

請把  $K_n$  分解成互斥的三角形，其中  $n = 2^k - 1$ 。



## Others – 構造

如果可以找到函數  $f(x, y)$  使得  $x \neq y \implies f(x, y) \neq x, y$  且  $f(x, f(x, y)) = y, f(f(x, y), y) = x$ ，我們就做完了！

事實上，只要  $n \equiv 1, 3 \pmod{6}$  就會有解！

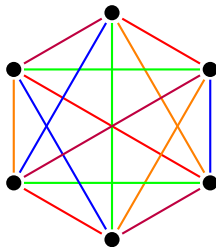
如果可以找到函數  $f(x, y)$  使得  $x \neq y \implies f(x, y) \neq x, y$  且  $f(x, f(x, y)) = y, f(f(x, y), y) = x$ ，我們就做完了！

事實上，只要  $n \equiv 1, 3 \pmod{6}$  就會有解！

# Others – 構造

例題 (Graph Factorization, ASC 35 pF)

請把  $K_{2n}$  分解成  $2n - 1$  個互斥的完美匹配。





## 例題 (Graph Game, Codeforces 235D)

現在有一個遊戲：一開始的分數是 0，並且有一個  $n$  個點的樹，每次從剩下的點中隨機且等機率的選出一個點  $v$ ，並把分數加上  $v$  所在的連通塊的大小，且把  $v$  和與  $v$  相鄰的邊全部刪掉。一直進行到圖上沒有點為止，問你得到的分數的期望值。

機率有關的題目通常會玩一個梗：

## 引理

$$\mathbf{E}[X + Y] = \mathbf{E}[X] + \mathbf{E}[Y]$$

### 例題 (Graph Game, Codeforces 235D)

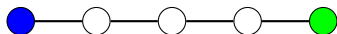
現在有一個遊戲：一開始的分數是 0，並且有一個  $n$  個點的樹，每次從剩下的點中隨機且等機率的選出一個點  $v$ ，並把分數加上  $v$  所在的連通塊的大小，且把  $v$  和與  $v$  相鄰的邊全部刪掉。一直進行到圖上沒有點為止，問你得到的分數的期望值。

機率有關的題目通常會玩一個梗：

### 引理

$$\mathbf{E}[X + Y] = \mathbf{E}[X] + \mathbf{E}[Y]$$

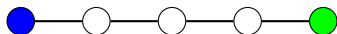
# Others



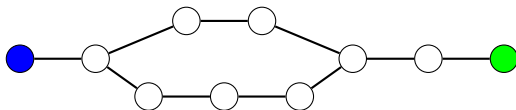
不過原本的題目其實是一棵水母。



# Others



不過原本的題目其實是一棵水母。



## 例題

給你許多點  $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ ，請找一個線性函數  $f$  使得  $\sum (f(x_i) - y_i)^2$  最小。

## 例題

給你許多點  $x_1, x_2, \dots, x_n$ ，請找一條線  $l$  使得  $\sum d(x_i, l)^2$  最小。

## 例題

給你許多點  $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ ，請找一個線性函數  $f$  使得  $\sum (f(x_i) - y_i)^2$  最小。

## 例題

給你許多點  $x_1, x_2, \dots, x_n$ ，請找一條線  $l$  使得  $\sum d(x_i, l)^2$  最小。