

# ***Applications of IEP***

- *Combinations with repetition*
- Derangements
- Permutations with forbidden positions

# *Combinations with repetition*

- Example 1: Determine the number of 10-combinations of the multiset  $T = \{3\{a\}, 4\{b\}, 5\{c\}\}$ .
- Hint: Let  $T^* = \{\infty\{a\}, \infty\{b\}, \infty\{c\}\}$ ,  $P_1$  (resp.,  $P_2$ , and  $P_3$ ) be the property that a 10-combination of  $T^*$  has more than 3 a's (resp., 4 b's and 5 c's) and  $A_1$  (resp.,  $A_2$  and  $A_3$ ) be the 1—combinations of  $T^*$  which have property  $P_1$  (resp.,  $P_2$  and  $P_3$ ). We wish to determine the size of the set

$$\begin{aligned} |\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}| &= |S| - (|A_1| + |A_2| + |A_3|) \\ &\quad + (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) \\ &\quad - (|A_1 \cap A_2 \cap A_3|) \end{aligned}$$

## 10-combinations of the multiset $T = \{3\{a\}, 4\{b\}, 5\{c\}\}$ .

- $S: |S|=C(10+3-1,10) = 66$
- $A_1$ : consists of all 10-combinations of  $T^*$  in which  $a$  occurs at least 4 times.
  - The number of 10-combinations in  $A_1$  equals the number of 6-combinations of  $T^*$ .
  - $|A_1|=C(6+3-1,6) = 28$
- $A_2$ : consists of all 10-combinations of  $T^*$  in which  $b$  occurs at least 5 times.
  - $|A_2|=C(5+3-1,5) = 21$
- $A_3$ : consists of all 10-combinations of  $T^*$  in which  $c$  occurs at least 6 times.
  - $|A_3|=C(4+3-1,4) = 15$
- $A_1 \cap A_2$ : consists of all 10-combinations of  $T^*$  in which  $a$  occurs at least 4 times and  $b$  occurs at least 5 times.
  - $|A_1 \cap A_2| = C(1+3-1,1) = 3$
- $A_1 \cap A_3$ : consists of all 10-combinations of  $T^*$  in which  $a$  occurs at least 4 times and  $c$  occurs at least 6 times.
  - $|A_1 \cap A_3| = 1$
- $A_2 \cap A_3$ :
  - $|A_2 \cap A_3| = 0$        $|\overline{A_1} \cap \overline{A_2} \cap \overline{A_3}| = 66 - (28 + 21 + 15) + (3 + 1 + 0) - (0) = 6$
- $A_1 \cap A_2 \cap A_3$ :
  - $|A_1 \cap A_2 \cap A_3| = 0$

# *Derangements*

- A *derangement* of  $\{1, 2, \dots, n\}$  is a permutation  $i_1 i_2 \dots i_n$  of  $\{1, 2, \dots, n\}$  such that  $i_1 \neq 1, i_2 \neq 2, \dots, i_n \neq n$  (i.e., no integer is in its natural position).
- We denote by  $D_n$  the number of derangements of  $\{1, 2, \dots, n\}$ .
- For  $n = 1$ , there are no derangements.  $D_1 = 0$
- For  $n = 2$ , the only derangement is  $2\ 1$ .  $D_2 = 1$
- For  $n = 3$ , there are two derangements:  $D_3 = 2$   
 $2\ 3\ 1$  and  $3\ 1\ 2$ .
- For  $n = 4$ , there are 9 derangements:  $D_4 = 9$   
 $2143, 2341, 2413, 3142, 3412, 3421, 4123, 4312, 4321$ .

# Examples

- At a party there are  $n$  men and  $n$  women. In how many ways can the  $n$  women choose male partners for the first dance? How many ways are there for the second dance if everyone has to change partners?
- Answer: for the first dance there are  $n!$  possibilities.
- For the second dance, the number of possibilities is  $D_n$ .

## *Formulas for Counting $D_n$*

- For  $n \geq 1$

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

- Proof: A *derangement* of  $\{1, 2, \dots, n\}$  is a permutation  $i_1 i_2 \dots i_n$  of  $\{1, 2, \dots, n\}$  such that  $i_1 \neq 1, i_2 \neq 2, \dots, i_n \neq n$  (i.e., **no** integer is in its natural position).
- Let  $S$  be the set of all  $n!$  permutations
- Let  $P_j (j=1, 2, \dots, n)$  be the property that, in a permutation,  $j$  **is in** its natural position.
- Let  $A_j$  denote the set of permutations with property  $P_j (j=1, 2, \dots, n)$

$$D_n = |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}|$$

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

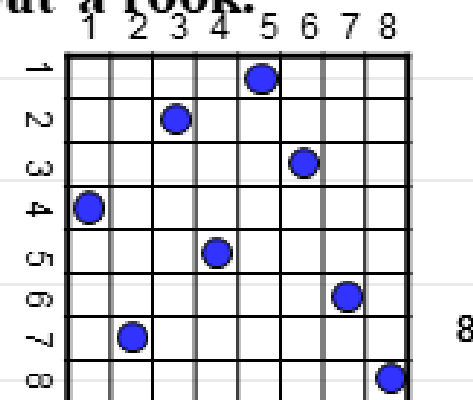
- S is the set of all  $n!$  permutations
  - $|S|=n!$
- $A_j$  is the set of permutations with property  $P_j(j=1,2,\dots,n)$  that  $j$  is in its natural position
  - $|A_j|=(n-1)!$
- $A_i \cap A_j$  is the set of permutations that  $i$  and  $j$  is in their natural positions
  - $|A_i \cap A_j|=(n-2)!$
- $a_k = |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}|$ 
  - $a_k=(n-k)!$
  - $\{i_1, i_2, \dots, i_k\}$  is a  $k$ -combination of  $\{1, 2, \dots, n\}$

$$\begin{aligned}
 & \bullet C(n, k) \\
 & |\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n}| = n! - C(n, 1)(n-1)! \\
 & \quad + C(n, 2)(n-2)! - \dots - \pm C(n, n)1! \\
 & = n! \left( 1 - \frac{1}{1!} + \frac{1}{2!} - \dots \pm \frac{1}{n!} \right)
 \end{aligned}$$

$C(n, i)(n-i)! = \frac{n!}{(n-i)! i!} (n-i)! = \frac{n!}{i!}$

# Examples

- How many possibilities are there for 8 non-attacking rooks on an 8-by-8 chessboard?
- (1) The rooks are indistinguishable for one another;
- The coordinates of rooks: only 1 rook for each row/column
  - (1,5) (2,3), (3,6),(4,1),(5,4),(6,7),(7,2),(8,8)
  - 8-permutations of  $\{1,2\dots 8\}$ :  $8!$
- **The permutations in  $P(X_1, X_2, \dots, X_n)$  correspond to placements of  $n$  non-attacking rooks on an  $n$ -by- $n$  board in which there are certain squares in which it is forbidden to put a rook.**





# An example

- Determine the number of ways to place 5 non-attacking rooks on the following 5-by-5 board, with forbidden positions as shown.

	1	2	3	4	5
1	X				
2	X	X			
3			X	X	
4			X	X	
5					

## ***Definition of $P(X_1, X_2, \dots, X_n)$***

- Let  $X_1, X_2, \dots, X_n$  be (possibly empty) subsets of  $\{1, 2, \dots, n\}$ . We denote by  $P(X_1, X_2, \dots, X_n)$  the set of all permutations  $i_1 i_2 \dots i_n$  of  $\{1, 2, \dots, n\}$  such that  $i_1$  is not in  $X_1$ ,  $i_2$  is not in  $X_2$  ...  $i_n$  is not in  $X_n$ .
- Let  $p(X_1, X_2, \dots, X_n) = |P(X_1, X_2, \dots, X_n)|$
- Let  $n = 4$  and let  $X_1 = \{1, 2\}$ ,  $X_2 = \{2, 3\}$ ,  $X_3 = \{3, 4\}$  and  $X_4 = \{1, 4\}$ . Then  $P(X_1, X_2, X_3, X_4)$  consists of all permutations  $i_1 i_2 i_3 i_4$  of  $\{1, 2, 3, 4\}$  such that  $i_1 \neq 1, 2$ ;  $i_2 \neq 2, 3$ ;  $i_3 \neq 3, 4$ ;  $i_4 \neq 1, 4$ .
- Only two permutations
  - $P(X_1, X_2, X_3, X_4) = \{3412, 4123\}$
  - $p(X_1, X_2, \dots, X_n) = 2$ .

## *Examples*

- Let  $X_k = \{k\}$  ( $k = 1, 2, \dots, n$ ). Then the set  $P(X_1, X_2, \dots, X_n)$  equals the set of all permutations  $i_1 i_2 \dots i_n$  of  $\{1, 2, \dots, n\}$  for which  $i_k \neq k$ .
- We conclude that  $P(X_1, X_2, \dots, X_n)$  is the set of derangements of  $\{1, 2, \dots, n\}$  and we have  $p(X_1, X_2, \dots, X_n) = D_n$ .

## An example

- Let  $n = 5$ ,  $X_1 = \{1\}$ ,  $X_2 = \{1, 2\}$ ,  $X_3 = \{3, 4\}$ ,  $X_4 = \{3, 4\}$ . Then  $P(X_1, X_2, X_3, X_4, X_5)$  are in one-to-one correspondence with the placement of 5 non-attacking rooks on the board with forbidden positions as shown.

	1	2	3	4	5
1	X				
2	X	X			
3			X	X	
4			X	X	
5					

- Let  $S$  be the set of all  $n!$  permutations without forbidden positions.
- $P_j$  means the property that the rook in the  $j$ th row is in a column belonging to  $X_j$   $|P(X_1, X_2, \dots, X_n)| = |A_1 \cap A_2 \cap \dots \cap A_m|$
- $A_i$  should be to Place  $n$  nonattacking rooks where the rook in row  $i$  is in one of the columns in  $X_i$ .
  - The  $i$ th element has  $|X_i|$  choices
  - $|A_i| = |X_i|(n-1)!$   $\sum |A_i| = \sum |X_i|(n-1)! = r_1(n-1)!$
- $A_i \cap A_j$  should be to Place  $n$  nonattacking rooks where the rook in rows  $i$  and  $j$  are in columns in  $X_i$  and  $X_j$ .
  - Suppose  $r_2$  equal the number of ways to place two nonattacking rooks on the board in forbidden positions.
  - $\sum |A_i \cap A_j| = r_2(n-2)!$

12

## *Placement of rooks in chess board*

- $r_k$  is the number of ways to place  $k$  non-attacking rooks on the  $n$ -by- $n$  board where each of the  $k$  rooks is in a forbidden position ( $k=1, 2, \dots, n$ ).
- The number of ways to place  $n$  non-attacking, indistinguishable rooks on an  $n$ -by- $n$  board with forbidden positions equals
- $n! - r_1(n-1)! + r_2(n-2)! - \dots + (-1)^k r_k(n-k)! + \dots + (-1)^n r_n.$

$$r_1(\square)=1, \quad r_1(\begin{array}{|c|} \hline \square \\ \hline \square \\ \hline \end{array})=2, \quad r_1(\begin{array}{|c|c|} \hline \square & \\ \hline & \square \\ \hline \end{array})=2,$$

$$r_2(\begin{array}{|c|} \hline \square \\ \hline \square \\ \hline \end{array})=0, \quad r_2(\begin{array}{|c|c|} \hline \square & \\ \hline & \square \\ \hline \end{array})=1.$$

## An example

- Determine the number of ways to place 5 non-attacking rooks on the following 5-by-5 board, with forbidden positions as shown.

1	x			
2	x	x		
3			x	x
4			x	x
5				

- $r_1 = 7$
- The set of forbidden positions can be partitioned into two “independent” parts
  - “Independent” means squares in different parts do not belong to a common row or column.
  - one part  $F_1$  containing three positions and the other part  $F_2$  containing four.
- $r_2$ : The rooks may be both in  $F_1$ , both in  $F_2$  or one in  $F_1$  and one in  $F_2$ .
  - $r_2 = 1 + 2 + 3 \times 4 = 15$ .
- $r_3 = 1 \times 4 + 3 \times 2 = 10$
- $r_4 = 1 \times 2 = 2$
- $5! - 7 \times 4! + 15 \times 3! - 10 \times 2! + 2 \times 1! = 226$

# C & A

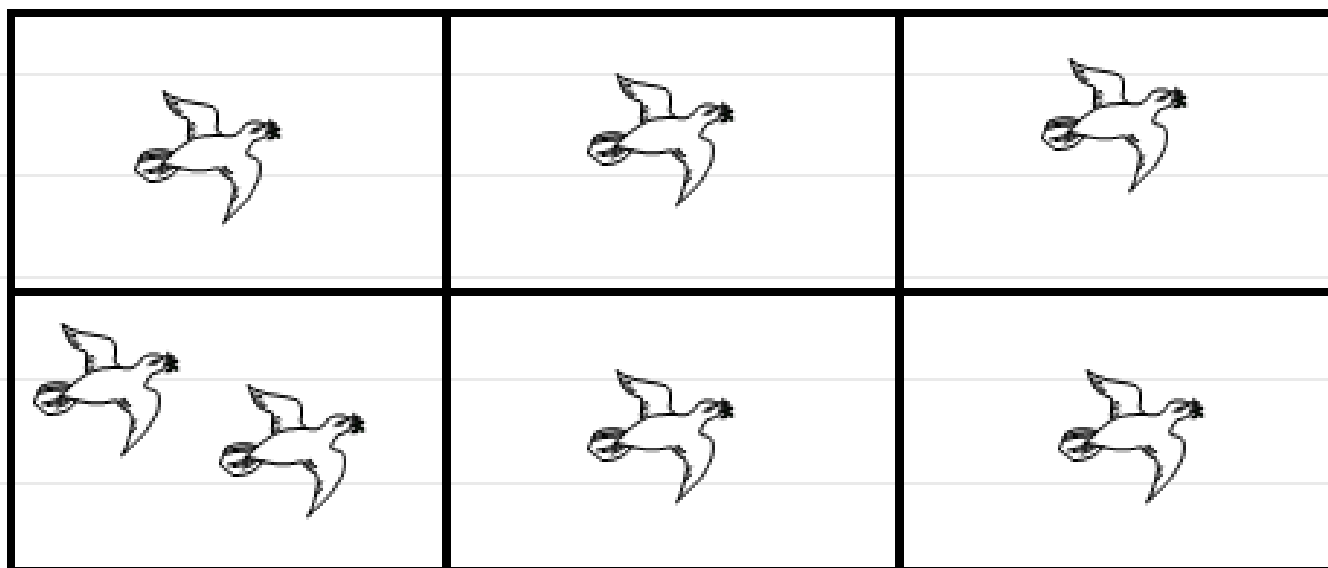
## *Chap. III* **Pigeonhole principle**

Yuchun Ma(马昱春)

## § 3. Pigeonhole principle

If there is  $n+1$  pigeons are flying to  $n$  holes,  
then at least one hole contains two pigeons.

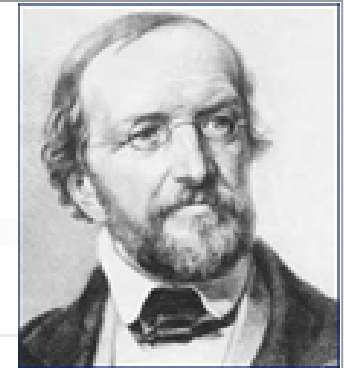
7 pigeons  
6 holes



Variety of names: pigeonhole principle, Dirichlet  
drawer principle, shoebox principle.....



# Dirichlet



- **Johann Dirichlet** (1805~1859)
- German mathematician, credited with the **modern formal** definition of a **function** and the foundation of **number theory**.
  - **Fermat's last theorem** : no three positive integers  $a$ ,  $b$ , and  $c$  satisfy the equation  $a^n + b^n = c^n$  for any integer value of  $n$  greater than 2
    - In 1825, a partial proof for the case  $n = 5$ ;
    - Later, a full proof for the case  $n = 14$ .
    - The first successful proof was released in 1994 by Andrew Wiles
  - **Pigeonhole principle**
    - In 1834, under the name *Schubfachprinzip* ("drawer principle" or "shelf principle")
    - Taken from: [http://episte.math.ntu.edu.tw/people/p\\_dirichlet/](http://episte.math.ntu.edu.tw/people/p_dirichlet/)<sup>17</sup>

# Simple Form

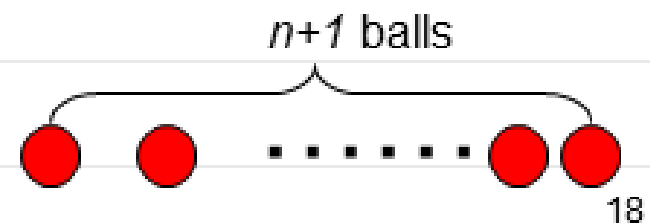
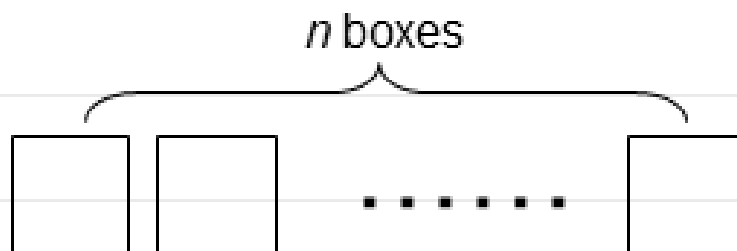
- **Theorem.** If  $n+1$  objects are put into  $n$  boxes, then at least one box contains two or more of the objects.

## Proof by contradiction

- **Proof.**

If each of the  $n$  boxes contains at most one of the objects, then the total number of objects is at most  $n$ .

Since we start with  $n+1$  objects, some box contains at least two of the objects. □



# Another Form

- **Pigeonhole principle** states that if  $n$  items are put into  $m$  holes with  $n > m$ , then at least one hole must contain more than one item.
- **Example.** Among 400 people there are two who have the same birthday.

单选题 1分

**Example** There are 4 pairs of red socks, 5 pairs of pink socks in a box. We randomly pick one sock from them for each time. How many picks are needed to guarantee that **a pair of socks** is selected?

A 2

B 3

C 4

D 5

# Simple Application

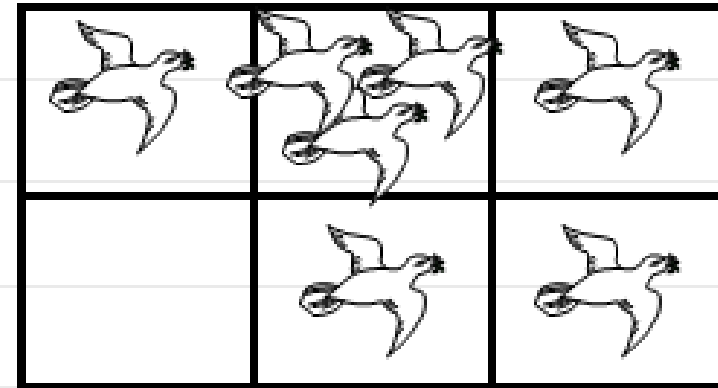
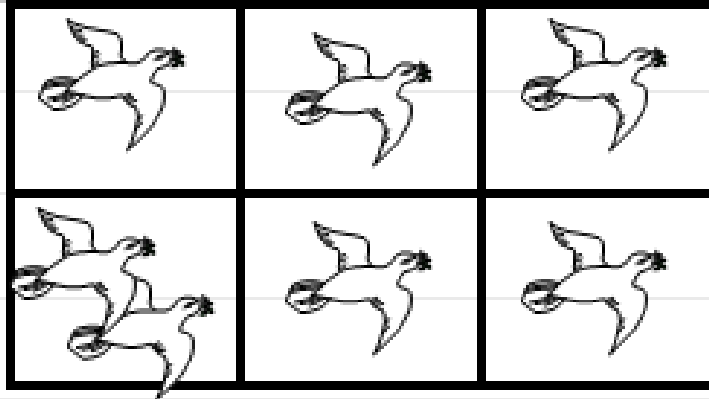
**Example** There are 4 pairs of red socks, 5 pairs of pink socks in a box. We randomly pick one sock from them for each time. How many picks are needed to guarantee that **a pair of socks** is selected?



$m = 2$  holes, using one pigeonhole per color

need only three socks ( $n = 3$  items).

# Pigeonhole Principle



- If  $n+1$  objects are put into  $n$  boxes, then at least one box contains two or more of the objects.
  - Only guarantee the **existence**
  - No help in finding a box that contains two or more of the objects
  - Keys: what are **pigeons** and what are **holes**?

# Generalized Pigeonhole Principle

**GPP.** If  $N$  objects are assigned to  $k$  boxes, then at least one box must be assigned at least  $\lceil N/k \rceil$  objects.

Top integral function  
Ceiling function

- *E.g.*, there are  $N=280$  students in this class.  
There are  $k=52$  weeks in the year.
  - Therefore, there must be at least 1 week during which at least  $\lceil 280/52 \rceil = \lceil 5.38 \rceil = 6$  students in the class have his or her birthday in this week.

# Proof of G.P.P.

**G.P.P:** If  $N$  objects are assigned to  $k$  boxes, then at least one box must be assigned at least  $\lceil N/k \rceil$  objects.

- Proof By contradiction. Suppose every box has  $< \lceil N/k \rceil$  objects, thus the number of objects in each box  $\leq (\lceil N/k \rceil - 1)$ .

- Then the total number of objects is at most

$$k \left( \left\lceil \frac{N}{k} \right\rceil - 1 \right) < k \left( \left( \frac{N}{k} + 1 \right) - 1 \right) = k \left( \frac{N}{k} \right) = N$$

- There are less than  $N$  objects, which contradicts our assumption of  $N$  objects. The original statement is true.



# Pigeonhole Principle



Mark Six (a lottery game)

49 labeled balls (1 to 49),  
Draw 6 balls randomly and then  
the 7<sup>th</sup> as a special number

# Pigeonhole Principle

Every time there must be two numbers among the 6 such that the first digit is the same. (Assume 1=01, 2=02, 3=03, 4=04).

Date	Draw Number	Draw Results
20/12/20 02	02/110	13 18 23 24 25 33 + 15
17/12/20 02	02/109	6 18 39 40 41 42 + 9
12/12/20 02	02/108	7 15 16 23 31 35 + 8
10/12/20 02	02/107	5 35 37 38 45 49 + 17
05/12/20 02	02/106	11 21 27 31 37 44 + 1
03/12/20 02	02/105	9 11 14 17 24 26 + 46
28/11/2002	02/104	17 19 26 31 37 43 + 38
26/11/2002	02/103	19 21 40 42 46 47 + 33
21/11/2002	02/102	4 16 18 25 29 41 + 21
19/11/2002	02/101	3 15 22 23 42 47 + 18

# Pigeonhole Principle

- Pick 6 master numbers every time.
- For every number, there are  $\{0,1,2,3,4\}$  5 choices for the first digit;
- By pigeonhole principle, 6 pigeons are flying to 5 pigeonholes. So there's at least one pigeonhole with 2 pigeons. This means that at least 2 numbers share their first-digits.

# Pigeonhole Principle (2)

- There are 20 shirts in a drawer, in which 4 are blue, 7 are grey, 9 are red. How many shirts do we need to pick to ensure that we have at least 4 shirts in the same color?
- Pigeonhole Principle (2):  $n$  pigeonholes,  $kn+1$  pigeons, at least 1 pigeonhole has  $k+1$  pigeons.
- Solution: 3 colors, 3 pigeonholes, so  $k+1=4$ .
- $K=3$ ,  $kn+1=10$ , we need to pick at least 10 shirts.

单选题 1分

There are 20 shirts in a drawer, in which 4 are blue, 7 are grey, 9 are red. How many shirts do we need to pick to ensure that we have at least 6 shirts in the same color?

A 15

B 16

C 18

D 20

## Pigeonhole Principle (2)

- There are 20 shirts in a drawer, in which there are 4 blue ones, 7 are grey, 9 are red. How many do we need to pick to ensure 6 same-colored shirts?
- Solution: (for 6 same-colored shirts) If we pick 4 blue ones at first, then choosing from red and grey ones:  $n=2, k+1=5$
- So we need to take  $4+5 \times 2+1=15$  shirts to have 6 with the same color
- .....

30

# Pigeonhole Principle

- We know  $n+1$  positive integers, all of them are  $\leq 2n$ , prove that at least 2 of them are relatively prime.
- Famous Hungarian mathematician Paul Erdos (1913-1996) asked 11-year-old Louis Pósa this problem. Pósa answered it in half minute.
- (Hint ....)
- Pósa thought: take  $n$  boxes, put 1 and 2 in the first one, 3 and 4 in the second one, 5 and 6 in the third one, so forth,  $2n-1$  and  $2n$  in the  $n^{\text{th}}$  one.
- Now we take  $n+1$  numbers from  $n$  boxes, so at least one box would be emptied. So there must be a pair of adjacent numbers among these  $n+1$  ones, and they are relatively prime.

31

## 主观题 10分

Take any  $n+1$  integers from 1 to  $2n$ , among them there's at least one pair such that one is the multiple of the other.



# Pigeonhole Principle

**Eg** Take any  $n+1$  integers from 1 to  $2n$ , among them there's at least one pair such that one is the multiple of the other.

**Proof** Assume the  $n+1$  numbers are  $a_1, a_2, \dots, a_{n+1}$ .

Dividing 2's until all of them becomes odd numbers.

Then it construct a sequence  $r_1, r_2, \dots, r_{n+1}$ .

These  $n+1$  numbers are still in  $[1, 2n]$  and they are all odd.

While there are only  $n$  odd numbers in  $[1, 2n]$ .

So There must be  $r_i = r_j = r$ , then  $a_i = 2^{k_i} r, a_j = 2^{k_j} r$

If  $a_i > a_j$ ,  $a_i$  is a multiple of  $a_j$ .

# Pigeonhole Principle

**Eg** Assume  $a_1, a_2, \dots, a_{100}$  is a sequence consists of 1 and 2. And any subsequence of 10 consecutive in it has a sum that is  $\leq 16$ :

$$a_i + a_{i+1} + \dots + a_{i+9} \leq 16, \quad 1 \leq i \leq 91$$

So  $\exists h$  and  $k$  such that  $k > h$  and

$$a_h + a_{h+1} + \dots + a_k = 39$$

**Proof** Let  $S_j = \sum_{i=1}^j a_i, \quad j = 1, 2, \dots, 100$

$$S_1 < S_2 < \dots < S_{100},$$

$$\text{And } S_{100} = (a_1 + \dots + a_{10})$$

$$+ (a_{11} + \dots + a_{20}) + \dots + (a_{91} + \dots + a_{100})$$

## § 3.7 Pigeonhole Principle

According to assumption  $a_i + a_{i+1} + \dots + a_{i+9} \leq 16, 1 \leq i \leq 91$

We have  $S_{100} \leq 10 \times 16 = 160$

Create sequence  $S_1, S_2, \dots, S_{100}, S_1 + 39, \dots, S_{100} + 39$ .

With 200 terms. The largest term  $S_{100} + 39 \leq 160 + 39 = 199$

By pigeonhole principle, there must be two equal terms.

And it must be a term in the first part and a term in the second part. Assume

$$S_k = S_h + 39, k > h \quad S_k - S_h = 39 \quad \text{So}$$

$$a_h + a_{h+1} + \dots + a_k = 39$$

# Examples

**Example:** Given  $m$  integers  $a_1, a_2, \dots, a_m$ , there exist integers  $k$  and  $l$  with  $0 \leq k < l \leq m$  such that  $a_{k+1} + a_{k+2} + \dots + a_l$  is divisible by  $m$ .

Hint. Consider the  $m$  sums

$$a_1, a_1+a_2, a_1+a_2+a_3, \dots, a_1+a_2+a_3+\dots+a_m.$$

If any of these sums is divisible by  $m$ , then the conclusion holds.

Thus suppose that each of the sums has a non-zero remainder when divided by  $m$ , and so a remainder equal to one of  $1, 2, \dots, m-1$ .

Since there are  $m$  sums and only  $m-1$  remainders, two of the sums have the same remainder when divided by  $m$ .

$$a_1+a_2+a_3+\dots+a_k = bm+r \qquad a_1+a_2+a_3+\dots+a_l = cm+r \quad (k < l)$$

$$\text{Subtracting: } a_{k+1}+a_{k+2}+a_{k+3}+\dots+a_l = (c-b)m;$$

Thus,  $a_{k+1} + a_{k+2} + \dots + a_l$  is divisible by  $m$ .

36  $\square$

# Examples

**Example:** Given  $m$  integers  $a_1, a_2, \dots, a_m$ , there exist integers  $k$  and  $l$  with  $0 \leq k < l \leq m$  such that  $a_{k+1} + a_{k+2} + \dots + a_l$  is divisible by  $m$ .

Let  $m=7$ , and let our integers be 2, 4, 6, 3, 5, 5 and 6.

Compute the sums of

remainders when divided by 7 are

$a_1=2,$	2		
$a_1+a_2=6,$	6		
$a_1+a_2+a_3=12,$	5	$a_1+a_2=6,$	
$a_1+a_2+a_3+a_4=15,$	1		
$a_1+a_2+a_3+a_4+a_5=20,$	6	$a_1+a_2+a_3+a_4+a_5=20,$	$\Rightarrow a_3+a_4+a_5=6+3+5=14$
$a_1+a_2+a_3+a_4+a_5+a_6=25,$	4		
$a_1+a_2+a_3+a_4+a_5+a_6+a_7=31,$	3		

Divisible by 7!

# Examples

- **Example: Hand shaking problem:** If there are  $n$  number of people who can shake hands with one another (where  $n > 1$ ), the pigeonhole principle shows that there is always a pair of people who will shake hands with the same number of people.
- Hint: As the 'holes', or  $m$ , correspond to number of hands shaken, and each person can shake hands with anybody from 0 to  $n - 1$  other people
- $n - 1$  possible holes.
  - either the '0' or the ' $n - 1$ ' hole must be empty
  - if one person shakes hands with everybody, it's not possible to have another person who shakes hands with nobody;
  - if one person shakes hands with no one there cannot be a person who shakes hands with everybody.
- This leaves  $n$  people to be placed in at most  $n - 1$  non-empty holes, guaranteeing duplication.

38

# Examples

- Example Chines Remainder Theorem

- *Hanxin Dianbing* (韩信点兵):

- a military general who served Liu Bang
- *Han Xin count his troops*
  - 3 soldiers in a line.....2 left at the end
  - 5 soldiers in a line.....3 left at the end
  - 7 soldiers in a line.....2 left at the end
  - The officer told Han Xin there are total 2395 soldiers?
  - Han Xin said "No, you are wrong, there should be 2333 soldiers."

- A third-century AD book *Sun Zi Suanjing* (孙子算经 The Mathematical Classic by Sun Zi)

- 今有物，不知其数，三三数之，剩二，五五数之，剩三，七七数之，剩二，问物几何
- We want to count the number of a pile of things, we only know that the remainder divided by 3 is 2, and the remainder divided by 5 is 3, the remainder divided by 7 is 2, what the number would be?



$$\begin{cases} x = 3a + 2 \\ x = 5b + 3 \\ x = 7c + 2 \end{cases}$$

- Find the smallest integer to satisfy this:
- List numbers such that  $x \div 3 \equiv 2$ :
  - 2, 5, 8, 11, 14, 17, 20, 23, 26...
- List numbers such that  $x \div 5 \equiv 3$ :
  - 3, 8, 13, 18, 23, 28 ...
- The first common number is 8. The least common multiple of 3 and 5 is 15.
  - Combine those 2 requirements, we need  $8 + 15 \times \text{integer}$ :
    - 8, 23, 38, ...
- Then list numbers such that  $x \div 7 \equiv 2$ :
  - 2, 9, 16, 23, 30...

40



# Chinese Remainder Theorem

- Find out the smallest non-negative integers solutions for the following equations: 
$$\begin{cases} x = 3a + 2 \\ x = 5b + 3 \\ x = 7c + 2 \end{cases}$$
- Construct the numbers
  - s is the smallest number which can be divided by 5 and 7 but the remainder divided by 3 is 1.  $s = 70$
  - $s*2=140$  will be divisible by both 5 and 7 but the remainder divided by 3 is 2.
  - t is the smallest number which can be divided by 3 and 7 but the remainder divided by 5 is 1.  $t = 21$
  - $t*3=63$  will be divisible by both 3 and 7 but the remainder divided by 5 is 3.
  - h is the smallest number which can be divided by 3 and 5 but the remainder divided by 7 is 1.  $h = 15$
  - $h*2=30$  will be divisible by both 3 and 5 but the remainder divided by 7 is 2.
  - $2s + 3t + 2h = 233$  should satisfy the equation array
  - To find the smallest one, 105 is the least common multiple of 3,5 and 7.
    - $233-105=128>105$ ,  $128-105=23$ .
  - The answer is 23

41

# Chinese Remainder Theorem

$$\begin{cases} x = 3a + 2 \\ x = 5b + 3 \\ x = 7c + 2 \end{cases}$$

- Chinese Remainder Theorem:  $m$  and  $n$  are relatively prime, for any non-negative integer  $a$  and  $b$  ( $a < m$ ,  $b < n$ ), there must be positive integer  $x$  which makes the equations solvable.

$$\begin{cases} x = pm + a \\ x = qn + b \end{cases}$$

$p, q$  are non-negative integers

- Proof: Consider  $n$  integers:  $a, m+a, 2m+a, \dots, (n-1)m+a$

There's no command remainders for the  $n$  numbers divided by  $n$ .  
[0,1,2..., $n-1$ ], a total of  $n$  ones.

So for  $b$  ( $b < n$ ), there must exist a number in the sequence which satisfies  $x = qn + b$

# Chinese Remainder Theorem

- **(Chinese Remainder Theorem, RT)** Assume  $m_1, m_2, \dots, m_k$  are relative prime, so  $\gcd(m_i, m_j) = 1, i \neq j, i, j = 1, 2, \dots, k$ , and the congruence equations:

$$x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_2 \pmod{m_2}$$

...

$$x \equiv b_k \pmod{m_k}$$

Mod  $[m_1, m_2, \dots, m_k]$  has solutions, this means with  $[m_1, m_2, \dots, m_k]$  there exists  $x$  which satisfies  $x \equiv b_i \pmod{[m_1, m_2, \dots, m_k]}, i = 1, 2, \dots, k$

# Pigeonhole Principle: Strong Form

Let  $q_1, q_2, \dots, q_n$  be positive integers. If  $q_1 + q_2 + \dots + q_n - n + 1$  objects are put into  $n$  boxes, then either the first box contains at least  $q_1$  objects, or the second box contains at least  $q_2$  object, ....., or the  $n$ th box contains at least  $q_n$  objects.

- Suppose that we distribute  $q_1 + q_2 + \dots + q_n - n + 1$  objects among  $n$  boxes.
- If for each  $i = 1, 2, \dots, n$  the  $i$ th box contains fewer than  $q_i$  objects
  - The total number of objects in all boxes does not exceed  $(q_1 - 1) + (q_2 - 1) + \dots + (q_n - 1) = q_1 + q_2 + \dots + q_n - n$ .
- Since this number is one less than the number of objects distributed, we conclude that for some  $i = 1, 2, \dots, n$ , the  $i$ th box contains at least  $q_i$  objects.

# Application Examples

- A bag contains 100 apples, 100 bananas, 100 oranges and 100 pears. How many fruits should be taken out such that we can be sure a dozen pieces of them are of the same kind?
  - Let  $q_1 = q_2 = \dots = q_n = r$ . The principle reads as follows: If  $n(r-1)+1$  objects are put into  $n$  boxes, then at least one of the boxes contains  $r$  or more the objects.
  - 4 boxes,  $q_1 = q_2 = \dots = q_n = 12$
  - If  $4*(12-1)+1 = 45$  fruits are taken out, then at least one of the boxes contains 12 fruits.

# To Do List

- OJ tasks
- Pre-class videos and quizzes
  - Generating Function
  - RainclassRoom