



第三章 鸽巢原理

3.1 鸽巢原理的简单形式

3.2 鸽巢原理的加强形式

3.3 Ramsey定理

组合数学

- 存在性问题

- 鸽巢原理

- 计数问题

- 排列组合

- 容斥原理

- 生成函数、递推关系

- Pólya计数

- 组合设计

- 组合优化



第三章 鸽巢原理

3.1 鸽巢原理的简单形式

3.2 鸽巢原理的加强形式

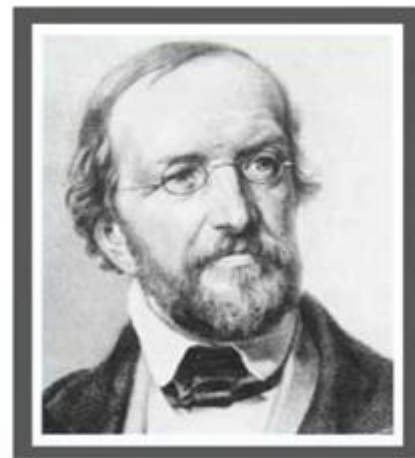
3.3 Ramsey定理

鸽巢原理

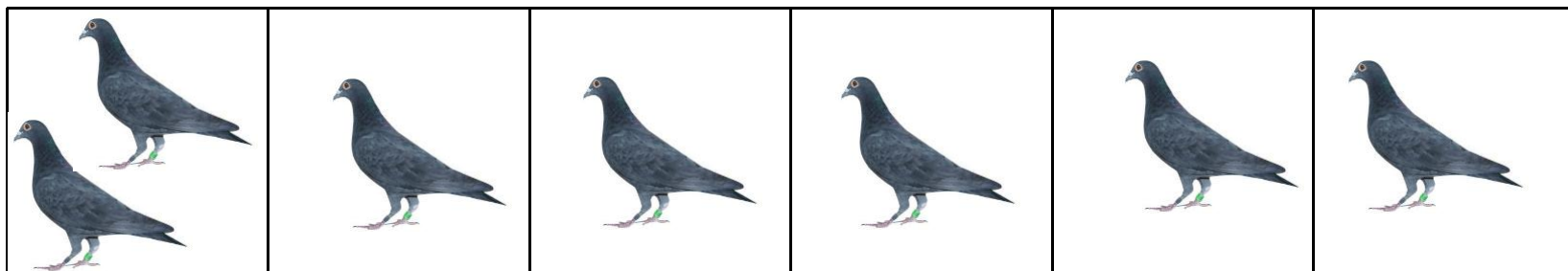
- 十九世纪德国数学家狄里克雷于1834年提出
鸽巢原理，当时命名为**抽屉原理**

(Schubfachprinzip, drawer principle)

- **7个鸽子飞进6个巢里，一定有一个巢至少有2只鸽子**



Dirichlet,
1805—1859



- 利用抽屉原理来建立有理数的理论，以后逐渐地应用到引数论、集合论、组合论等数学分支中，所以抽屉原理又称为**狄里克雷原理**

■ 两桃杀三士

□ 《晏子春秋·内篇谏下·第二十四》



齐景公



公孙接、田开疆、古冶子



晏子

■ 宋代费衎的《梁溪漫志》中，就曾运用抽屉原理来批驳“算命”一类迷信活动的谬论

“近世士大夫多喜谭命，往往自能推步。予尝见人言曰者阅人命，盖未始见年、月、日、时同者；纵有一二，必倡言于人以为异。尝略计之，若生时无同者，则一时生一人，一日生十二人，以岁记之，则有四千三百二十人；以一甲子计之，止（只）有二十五万九千二百人而已。今只从一大郡计，其户口之数尚不减数十万，况举天下之大，自五公大人以至小民何啻亿兆？虽明于数者有不能历算，则生时同者必不为少矣。其间五公大人始生之时则必有庶民同时而生者，又何贵贱贫富之不同也？”

- 把一个人出生的年、月、日、时（八字）作算命的根据，把“八字”作为“抽屉”，不同的抽屉只有 $12 \times 360 \times 60 = 259200$ 个。以天下之人为“物品”，其数“何啻亿兆”，进入同一抽屉的人必然千千万万，因而结论是“生时同者必不为少矣”。既然“八字”相同，“又何贵贱贫富之不同也？”

举例

- 13个同学，肯定至少有两个人出生在同一个月份。
- 假设有5对已婚夫妇，从中随机挑出6人，一定会挑出一对夫妇。
- 10位同学，每位同学至少认识其余9位同学中的一位，则至少有两位认识的人数相等。
- 在任意6个人中，或者有3个人两两互相认识，或者有3个人两两互相不认识（Ramsey定理）
- 月黑风高穿袜子：蓝色、黄色、红色袜子各3双，请问最少取多少只袜子，一定可以凑成一双？4只

知识点

数论问题

几何图形
类问题

连续时间
问题

棋盘着色

中国剩余
定理

满足条件的
最小物体
数

**存在性
问题**

完全图的一
种着色

**Ramsey
定理**

鸽巢原理

简单形式

加强形式

$n+1$ 个

n 个

n 个

m 个

物体

鸽子

盒子

巢

$$K_p \rightarrow K_{n_1}, K_{n_2}, \dots, K_{n_l}$$

$$K_p \rightarrow K_m, K_n$$

Ramsey数

鸽巢原理

定理3.1.1 如果把 $n+1$ 个物体放进 n 个盒子，那么至少有一个盒子包含两个或更多的物体。（反证法）

注意： 鸽巢原理只能用于证明某种现象的存在性。



■ 当 X , Y 为有限集时

- 如果 X 的元素多于 Y 的元素 ($|X| > |Y|$)，则 f 不是单射
- 如果 $|X| = |Y|$ ，且 f 是满射，则 f 是单射
(如果没有一个盒子为空，则每个盒子恰好有一个物体)

- 如果 $|X| = |Y|$ ，且 f 是单射，则 f 是满射

(如果没有盒子被放入多于一个物体，则每个盒子里有一个物体)

鸽巢原理→其他形式

定理3.1.1 如果把 $n+1$ 个物体放进 n 个盒子，那么至少有一个盒子包含两个或更多的物体。（反证法）

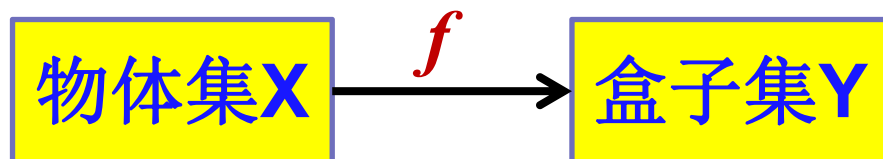
注意： 鸽巢原理只能用于证明某种现象的存在性。

■ 鸽巢原理的其他形式

- n 个物体放入 n 个盒子且没有一个盒子是空的, 那么, 每个盒子正好包含一个物体.
- n 个物体放入 n 个盒子且没有盒子被放入多于一个物体, 那么, 每个盒子有一个物体.

鸽巢原理→其他形式

定理3.1.1 如果把 $n+1$ 个物体放进 n 个盒子，那么至少有一个盒子包含两个或者更多的物体。



- n 个物体放入 n 个盒子且没有一个空的, 那么, 每个盒子正好包含一个物体.
- n 个物体放入 n 个盒子且没有盒子被放入多于一个物体, 那么, 每个盒子有一个物体.

例：如果有 $n+1$ 个整数，而这些整数是小于或等于 $2n$ ，是否一定会有一对数是互素的？为什么？

（匈牙利大数学家厄杜斯(Paul Erdős, 1913 - 1996) 向当年年仅11岁的波萨 (Louis Pósa) 提出这个问题，而小波萨思考了不足半分钟便能给出正确的答案。）

n 个盒子： $\boxed{1, 2}$ $\boxed{3, 4}$ $\boxed{5, 6}$... $\boxed{2n-1, 2n}$

从 n 个盒子中取出 $n+1$ 个数，一定会有一个盒子中的两个数同时被取出，即一对互素数。

例：证明，如果从 $\{1, 2, \dots, 2n\}$ 中选择 $n+1$ 个整数，那么存在两个整数，它们之间差为1。

例：如果从 $\{1, 2, \dots, 2n\}$ 中选择 $n+1$ 个不同的整数，证明一定存在两个整数，它们之间差为1。

n 个盒子： $\boxed{1, 2}$ $\boxed{3, 4}$ $\boxed{5, 6}$ \dots $\boxed{\begin{smallmatrix} 2n-1, \\ 2n \end{smallmatrix}}$

证明：把集合 $\{1, 2, \dots, 2n\}$ 划分成 n 个子集

$$S_1, S_2, \dots, S_n,$$

其中， $S_i = \{2i-1, 2i\}, i=1, 2, \dots, n$ 。

由鸽巢原理知，从 $\{1, 2, \dots, 2n\}$ 中取出 $n+1$ 个数，一定会有一个子集中的整数同时被取出，且这两个整数之间差为1。

例：如果有 $n+1$ 个不同的正整数，且这些正整数是小于或等于 $2n$ ，是否一定会有一对数是互素的？为什么？

匈牙利大数学家厄杜斯 (Paul Erdős, 1913 - 1996) 向当年年仅11岁的路易·波萨 (Louis Pósa) 提出这个问题，而小波萨思考了不足半分钟便给出了正确的答案。

n 个盒子： $\boxed{1, 2}$ $\boxed{3, 4}$ $\boxed{5, 6}$... $\boxed{\begin{matrix} 2n-1, \\ 2n \end{matrix}}$

例：如果从 $\{1, 2, \dots, 2n\}$ 中选择 $n+1$ 个不同的整数，证明一定存在两个整数，它们之间差为1。

证明：设选择的 $n+1$ 个整数为 $a_1 < a_2 < \dots < a_{n+1}$ 。

令 $b_1 = a_1 + 1, b_2 = a_2 + 1, \dots, b_{n+1} = a_{n+1} + 1$ ，则

$$1 < b_1 < b_2 < \dots < b_{n+1} \leq 2n+1。$$

现有 $2n+2$ 个数：

$$a_1, a_2, \dots, a_{n+1}, b_1, b_2, \dots, b_{n+1},$$

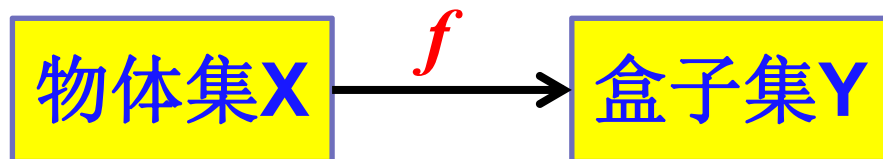
且每个数均属于 $\{1, 2, \dots, 2n+1\}$ 。

由鸽巢原理知，这 $2n+2$ 个数中至少有一对数相等。

由于 a_1, \dots, a_{n+1} 互不相等，且 b_1, \dots, b_{n+1} 互不相等，

因此存在一对 $b_j = a_j + 1$ 与 a_k ($j \neq k$) 相等，得 a_k 和 a_j 只相差1。

鸽巢原理的集合语言表述



令 X 和 Y 是两个有限集， $f: X \rightarrow Y$ 是一个由 X 到 Y 的函数。

- 如果 X 与 Y 含有相同个数的元素，且 f 是映上(满射)的，那么 f 是一对一的
- 如果 X 与 Y 含有相同个数的元素，且 f 是一对一的，那么 f 是映上的(满射)
- 如果 X 的元素多于 Y 的元素，那么 f 就不是一对一的

鸽巢原理：数论中的应用

例. 证明：在 m 个正整数 a_1, a_2, \dots, a_m 中, 存在 $0 \leq k < l \leq m$, 使得 $a_{k+1} + a_{k+2} + \dots + a_l$ 能够被 m 整除。

证：考虑 m 个和：

$$s_1 = a_1, s_2 = a_1 + a_2, s_3 = a_1 + a_2 + a_3, \dots, s_m = a_1 + a_2 + \dots + a_m$$

- (1) 若以上和中有一个能被 m 整除，则结论成立；
- (2) 否则，设 r_1, r_2, \dots, r_m 是 s_1, s_2, \dots, s_m 除以 m 的非零余数，则 $1 \leq r_i \leq m-1, i=1, \dots, m$ 。

由鸽巢原理知，存在 $r_l = r_k, l > k$ ，则

$$a_{k+1} + a_{k+2} + \dots + a_l = s_l - s_k \text{ 能被 } m \text{ 整除。}$$

例. 从整数 $1, 2, \dots, 200$ 中选取**101**个不同的整数。证明所选的数中存在两个整数，使得**其中一个是另一个的因子**。

分析：

- 任何整数可分解为一些**素数的乘积**，如对任何整数 n , $n = 2^k \times a$ ，其中， **a 为奇数**， **$k \geq 0$** 。
- 整数 $1, 2, \dots, 200$ 只能有**100个不同奇数**，故可对101个数运用鸽巢原理。

例. 从整数 $1, 2, \dots, 200$ 中选取**101**个不同的整数。证明所选的数中存在两个整数，使得**其中一个是另一个的因子**。

证：对于1到200间的整数 n ， n 可写作以下形式：

$$n = 2^k \times a \quad (1)$$

其中 a 是 $1, 2, \dots, 200$ 内的奇数。

由于要选取 101 个整数，而 200 内只有 100 个奇数，由鸽巢原理知**必存在两个整数 n_1 与 n_2 写作 (1) 式形式后，两个奇数相等**。

假设 $n_1=2^{k_1} \times b$, $n_2=2^{k_2} \times b$ ，其中 b 是 $1, 2, \dots, 200$ 内的奇数，显然，当 $k_1 > k_2$ 时， n_2 整除 n_1 ；否则 n_1 整除 n_2 。

例：对于任意给定的52个非负整数，证明：其中必存在两个非负整数，要么两者的和能被100整除，要么两者的差能被100整除。

证：对于任意一个非负整数，其整除100的余数可能为 $\{0, 1, 2, \dots, 99\}$ 中之一。

对这100个余数进行分组，构造如下51个集合：

$\{0\}, \{1, 99\}, \{2, 98\}, \{3, 97\}, \dots, \{49, 51\}, \{50\}.$

两种情况：

- (1) 52个非负整数中存在两个数除以100的余数相同，显然它们的差能被100整除；
- (2) 若52个非负整数除以100的余数各不相同，则必存在两个数的余数恰好构成上述两元集合中一个；此时它们的和能被100整除。

思考题：

1. 证明：在 $n+2$ 个任选的正整数中，存在两个数，或者其差能被 $2n$ 整除，或者其和能被 $2n$ 整除。

2. 一间房屋内有10个人，他们当中没有人超过 60 岁（年龄只能以整数给出），但又至少不低于 1 岁。

证明：总能找出两组人（两组人中不含相同的人），使得年龄和相同。题中的10能换成更小的数吗？

3. 证明：对任意正整数 n ，必存在由 0 和 3 组成的正整数能被 n 整除。

鸽巢原理：几何图形类应用

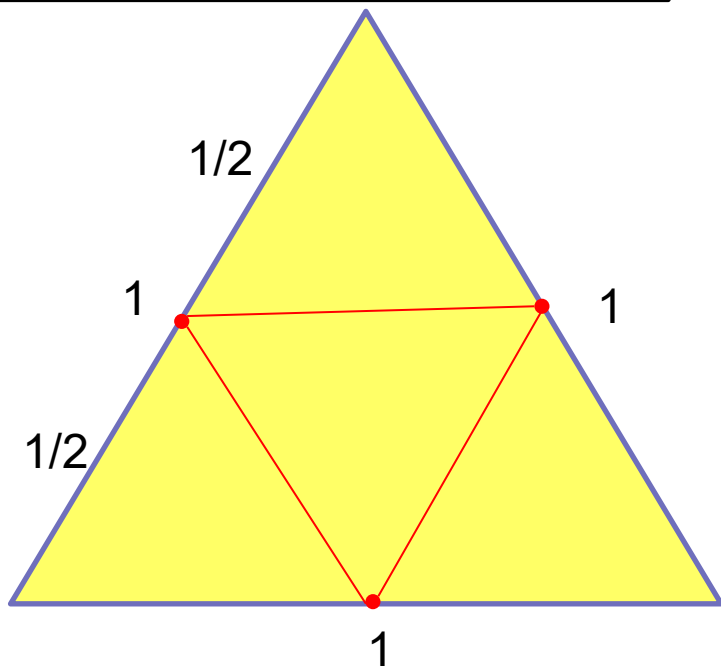
例5. 在边长为1的等边三角形内任意选择5个点。

证明：一定存在2个点，其距离至多为 $1/2$ 。

证明：如图所示，将等边三角形依每边中点分成四部分。

显然落在任意一个部分中的两点之间的距离至多为 $1/2$ 。

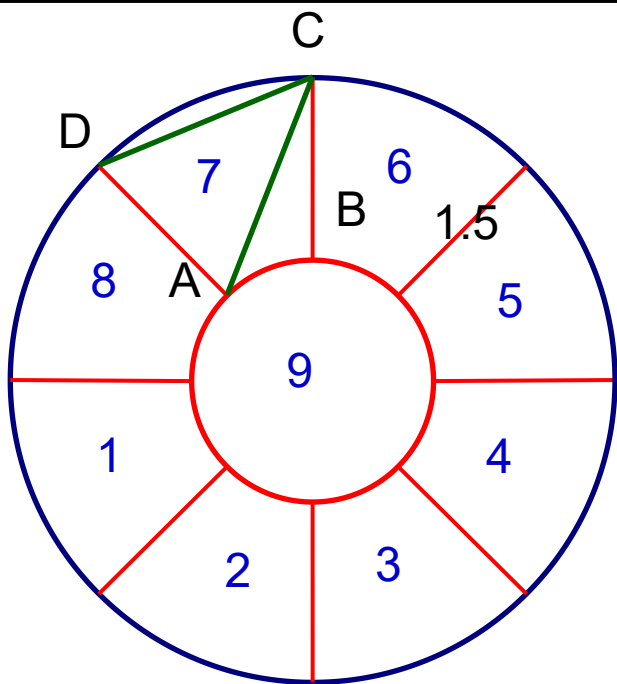
根据鸽巢原理，任意选择5个点，肯定有两个点落在同一个部分，因此这两点距离至多为 $1/2$ 。



思考：

1. 证明在边长为1的等边三角形中任意选择10个点，一定存在两个点，其距离至多为 $1/3$ 。
2. 确定一个整数 n_k ，使得如果在边长为1的等边三角形中任意选择 n_k 个点，一定存在2个点，其距离至多为 $1/k$ 。
3. 在直径为5的圆内任意给定10个点，证明存在两点，它们之间的距离小于2。

例：在直径为5的圆内任意给定10个点，
证明存在两点，它们之间的距离小于2。



用一个与已知圆同心，
半径为1的小圆，再把
圆环部分等分成8个部
分，构成9个抽屉。

$$|CD| = \sqrt{2 - \sqrt{2}}R = \sqrt{2 - \sqrt{2}} \cdot 5 < 1.92 < 2$$

$$|AC| = \sqrt{R^2 + r^2 - 2Rr \cos \frac{\pi}{4}}$$

$$= \sqrt{2.5^2 + 1^2 - 2 \times 2.5 \times 1 \times \frac{\sqrt{2}}{2}} < 1.93 < 2$$

证明：无论怎么样涂色，其中必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色。

[illegible]

例：将一个矩形分成**4行19列**的网格，每个单元格涂1种颜色，有**3种颜色**可以选择，

证明：无论怎么样涂色，其中**必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色**。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，**必有两个单元格的**颜色相同，其不同位置的组合有 **$C(4, 2)=6$** 种，

例：将一个矩形分成**4行19列**的网格，每个单元格涂1种颜色，有**3种颜色**可以选择，

证明：无论怎么样涂色，其中**必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色**。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，**必有两个单元格的**颜色相同，其不同位置的组合有 **$C(4, 2)=6$** 种，

例：将一个矩形分成4行19列的网格，每个单元格涂1种颜色，有3种颜色可以选择，

证明：无论怎么样涂色，其中必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，必有
两个单元格的顏色相同，其不同位置的组合有 $C(4, 2)=6$ 种，

例：将一个矩形分成4行19列的网格，每个单元格涂1种颜色，有3种颜色可以选择，

证明：无论怎么样涂色，其中必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
				黄	黄	黄				红	红	红				绿	绿	绿
		黄	黄			黄		红	红			红		绿	绿			绿
	黄		黄		黄		红		红		红		绿		绿		绿	
	黄	黄		黄			红	红		红			绿	绿		绿		

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，必有两个单元格的顏色相同，其不同位置的组合有 $C(4, 2)=6$ 种，

例：将一个矩形分成**4行19列**的网格，每个单元格涂1种颜色，有**3种颜色**可以选择，

证明：无论怎么样涂色，其中**必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色**。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
				黄	黄	黄				红	红	红				绿	绿	绿
		黄	黄			黄		红	红			红		绿	绿			绿
	黄		黄		黄		红		红		红		绿		绿		绿	
	黄	黄		黄			红	红		红			绿	绿		绿		

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，**必有两个单元格的**颜色相同，其不同位置的组合有 **$C(4, 2)=6$** 种，则3种颜色下，一列中两个同色单元格的位置组合共有**18种**，而现在有**19列**。

因此，由鸽巢原理，**必有两列的两个同色单元格位置相等且颜色相同**。

例：将一个矩形分成**4行19列**的网格，每个单元格涂1种颜色，有**3种颜色**可以选择，

证明：无论怎么样涂色，其中**必有一个由单元格构成的矩形的4个角上的格子被涂上同一种颜色**。

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
红	白	白	白	黄	黄	黄	白	白	白	红	红	红	白	白	白	绿	绿	绿
白	白	黄	黄	白	白	黄	白	红	红	白	白	红	白	绿	绿	白	白	绿
白	黄	白	黄	白	黄	白	红	白	红	白	红	白	绿	白	绿	白	绿	白
红	黄	黄	白	黄	白	白	红	红	白	红	白	白	绿	绿	白	绿	白	白

证：每一列有4行，但只有3个颜色，则由鸽巢原理知，**必有两个单元格的**颜色相同，其不同位置的组合有 $C(4, 2)=6$ 种，则3种颜色下，一列中两个同色单元格的位置组合共有**18种**，而现在有**19列**。

因此，由鸽巢原理，**必有两列的两个同色单元格位置相等且颜色相同**。

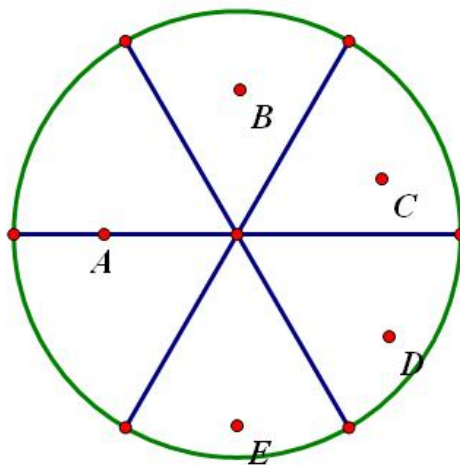
显然，这两列构成的矩形的4个角上的格子的颜色相同。证毕。

思考：随意地把一个3行9列棋盘的每个方格涂成红色或蓝色，求证：必有两列方格的涂色方式是一样的。

1	2	3	4	5	6	7	8	9

思考：

（英国数学奥林匹克1975年的问题）在一个半径为1单位的圆板上钉7个钉，使得两个钉的距离是大于或等于1，那么这7个钉一定会有一个位置恰好是在圆心上。



鸽巢原理：连续时间问题

例：某厂在五年期间的每一个月里至少试制一种新产品，
每年最多试制19种新产品。

试证明：一定存在连续几个月，恰好试制24种新产品。

证：设五年间每个月新产品数分别为 $a_1, a_2, \dots, a_{59}, a_{60}$ 。

构造出数列 a_n 的前 n 项和的数列 $s_1, s_2, \dots, s_{59}, s_{60}$,

则有： $1 \leq a_1 = s_1 < s_2 < \dots < s_{59} < s_{60} \leq 19 \times 5 = 95$,

而序列 $s_1+24, s_2+24, \dots, s_{59}+24, s_{60}+24$ 也是一个严格递增序列：

$$25 \leq s_1+24 < s_2+24 < \dots < s_{59}+24 < s_{60}+24 \leq 95+24 = 119。$$

于是，这120个数 $s_1, s_2, \dots, s_{59}, s_{60}$ 和 $s_1+24, s_2+24, \dots, s_{59}+24, s_{60}+24$ 都在区间 $[1, 119]$ 内。

根据鸽巢原理，必定存在两个数相等。

鸽巢原理：连续时间问题

例：某厂在五年期间的每一个月里至少试制一种新产品，
每年最多试制19种新产品。

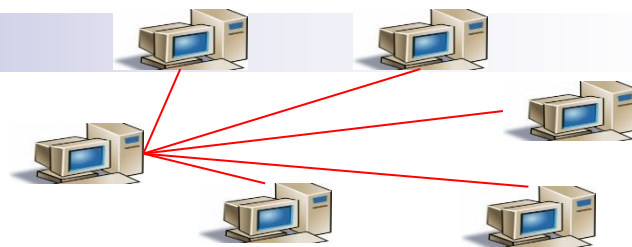
试证明：一定存在连续几个月，恰好试制24种新产品。

证：(续)：由于 $s_1, s_2, \dots, s_{59}, s_{60}$ 与 $s_1+24, s_2+24, \dots, s_{59}+24, s_{60}+24$ 均为严格单调的，因此必然存在一个 i 和 j ，使得

$$s_i = s_j + 24。$$

因此该厂在从第 $j+1$ 个月起到第 i 个月的这几个月时间里，
恰好试制了24种新产品。

应用-计算机网络



例. 假设有一个由**6台**计算机组成的网络，证明在这样网络中**至少存在两台计算机直接连接数量相同的其他计算机。**

证： 每台计算机的直接连接数**大于等于0,小于等于5**，
且0和5不能同时出现。

(1) 若一个计算机的直接连接数为**0**，此时其他计算机最大连接数为**4**

(2) 若一个计算机的直接连接数为**5**，则其他计算机的最小直接连接数为**1**

因此，计算机的直接连接数最多只能有**5**个数。由鸽巢原理，
6台计算机中至少有两台的直接连接数相同。

中国剩余定理

- 韩信点兵传说：韩信带1500名兵士打仗，战死四五百人。命令士兵

- ✓ 3人一排，多出2名；
- ✓ 5人一排，多出3名；
- ✓ 7人一排，多出2名。

- ✓ 韩信马上说出人数：1073人。

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

- 《孙子算经》：“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？”

- 宋朝数学家秦九韶于1247年《数书九章》卷一、二《大衍类》对“物不知数”问题做出完整系统的解答。

- 明朝数学家程大位编成了歌诀：
三人同行七十稀，五树梅花廿一枝，
七子团圆正半月，除百零五便得知。



例6 (中国剩余定理) 令 m, n 是互素的正整数, a 和 b 分别是小于 m 和 n 的非负整数。那么, 存在正整数 x , 使得 x 除以 m 余数为 a , 且除以 n 余数为 b , 即

$$x = pm + a, \quad x = qn + b。$$

分析:

1) 首先构造足够多 “除以 m 余数为 a ” 的整数

2) 证明在这些数中存在 “除以 n 余数为 b ” 的整数。

需要多少这样的数?

例6 (中国剩余定理) 令 m, n 是互素的正整数, a 和 b 分别是小于 m 和 n 的非负整数。那么, 存在正整数 x , 使得 x 除以 m 余数为 a , 且除以 n 余数为 b , 即 $x=pm+a$, $x=qn+b$ 。

证: 考虑 n 个除以 m 余数为 a 的整数:

$$a, m+a, \dots, (n-1)m+a$$

假设存在两个数 $im+a$ 和 $jm+a$ ($0 \leq i < j \leq n-1$) 除以 n 的余数都为 r , 即存在非负整数 k 和 l 使得

$$im+a = kn + r, \quad jm+a = ln + r$$

上两式相减得 $(j-i)m = (l-k)n$ 。由于 m, n 互素, 因此 n 是 $j-i$ 的因子。

又由于 $0 \leq j-i \leq n-1$, 矛盾。

故上述 n 个整数除以 n 的余数各不相同。

由鸽巢原理, n 个数 $0, 1, 2, \dots, n-1$ 中都出现在这些余数集之中, 因此 b 也出现。

设对应除以 n 余数为 b 的数为 $x = pm + a$ ($0 \leq p \leq n-1$), 同时 $x = qn + b$ ($0 \leq q \leq n-1$), 结论成立。

中国剩余定理一般形式

- 设 m_1, m_2, \dots, m_k 是 k 个两两互素的正整数, $0 \leq a_i < m_i$ ($i=1, \dots, k$), 则存在 x , 使得 x 除以 m_i 的余数为 a_i , 即 $x \equiv a_i \pmod{m_i}$ ($i=1, \dots, k$)。

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

解决实际问题中的意义

■ 密码问题

- 可以选取5个两两互素的整数 $m_i (i=1,2,\dots,5)$ ，每个股东秘密保存 b_i ，那么存在唯一的 x 使得 x 除以 m_i 的余数为 b_i ，用 x 作为密钥加密机密文件。
- **注意：**鸽巢原理仅提供了存在性证明，还需要设计求 x 的有效算法，这需要我们学习更多数学才能解决。

知识点

数论问题

几何图形
类问题

连续时间
问题

棋盘着色

中国剩余
定理

满足条件的
最小物体
数

**存在性
问题**

完全图的一
种着色

**Ramsey
定理**

鸽巢原理

简单形式

加强形式

$n+1$ 个

n 个

n 个

m 个

物体

鸽子

盒子

巢

$$K_p \rightarrow K_{n_1}, K_{n_2}, \dots, K_{n_l}$$

$$K_p \rightarrow K_m, K_n$$

Ramsey数

非对称密码体制

- 非对称密码体制提供的安全性取决于难以解决的数学问题，例如，将大整数因式分解成质数。
- 公钥系统使用这样两个密钥，一个是公钥，用来加密文本，另一个是安全持有的私钥，只能用此私钥来解密。也可以使用私钥加密某些信息，然后用公钥来解密，而公钥是大家都可以知道的，这样拿此公钥能够解密的人就知道此消息是来自持有私钥的人，从而达到了认证作用。

Diffie-Hellman 算法描述 (1976)

1. Alice 与 Bob 确定两个大素数 n 和 g , 这两个整数不保密, Alice 与 Bob 可以使用不安全信道确定这两个数.
2. Alice 选择另一个大随机数 x , 并计算 A 如下:
 1. $A = g^x \bmod n$
3. Alice 将 A 发给 Bob
4. Bob 选择另一个大随机数 y , 并计算 B 如下:
 1. $B = g^y \bmod n$
5. Bob 将 B 发给 Alice
6. 计算秘密密钥 K_1 如下:
 1. $K_1 = B^x \bmod n$
7. 计算秘密密钥 K_2 如下:
 1. $K_2 = A^y \bmod n$
8. $K_1 = K_2$

RSA 算法 (1977)

- 1977 年，即，Diffie-Hellman 的论文发表一年后，MIT 的三名研究人员根据这一想法开发了一种实用方法。这就是 RSA，它是以三位开发人员 — Ron Rivest、Adi Shamir 和 Leonard Adelman — 姓的首字母大写命名的，而且 RSA 可能是使用最广泛的公钥密码体制。
- 是一种块加密算法。
- 应用最广泛的公钥密码算法
- 只在美国申请专利，且已于2000年9月到期

小结

- 鸽巢原理用于证明某种结构的存在性。
- 运用鸽巢原理通常需要将问题转化。

1. 证明：在 $n+2$ 个任选的正整数中，存在两个数，或者其差能被 $2n$ 整除，或者其和能被 $2n$ 整除。

证明：已知所有正整数除以 $2n$ 的余数的取值只能为 $0, 1, 2, \dots, 2n-1$ 。

把以上余数构造以下 $n+1$ 个子集：

$\{1, 2n-1\}, \{2, 2n-2\}, \dots, \{n-1, n+1\}, \{n, n\}, \{0, 0\}$ 。

任选 $n+2$ 个正整数，由鸽巢原理知，一定存两个数，其除以 $2n$ 的余数来自同一个子集，设为 A 。

(1)若 A 是前 $n-2$ 个子集中一个，则这两个数的和能被 $2n$ 整除；

(2)若 A 是最后2个子集中一个，则这两个数的差能被 $2n$ 整除。

9. 一间房屋内有10个人，他们当中没有人超过60岁（年龄只能以整数给出），但又至少不低于1岁。

证明：总能找出两组人（两组人中不含相同的人），使得年龄和相同。题中的10能换成更小的数吗？

证明：(1) 10个人构成的子集一共是 $2^{10}=1024$ 个，去除掉空集与全集，一共1022个子集可以是找出的两组人中的一组。

由于这些子集的年龄和最小为1岁，且不超过 $60 \times 9 = 540$ 岁。因此，由鸽巢原理知，至少有两组人的年龄和相同，去除这两组人的相同人后，所得的两组人满足题目要求。

9. 一间房屋内有10个人，他们当中没有人超过60岁（年龄只能以整数给出），但又至少不低于1岁。

证明：总能找出两组人（两组人中不含相同的人），使得年龄和相同。题中的10能换成更小的数吗？

证明：(2) 当考虑9个人时，9个人构成的子集一共是 $2^9=512$ 个，去除掉空集与全集，一共510个子集可以是找出的两组人中的一组。

又这些子集的年龄和最小为1，最大为 $60*8=480$ 。

因此，由鸽巢原理知，至少有两组人的年龄和相同，去除这两组人的相同人后，所得的两组人满足题目要求。

例. 证明: 对任意正整数 n , 必存在由0和3组成的正整数能被 n 整除。

证明: 设有 $n+1$ 个数 a_1, a_2, \dots, a_{n+1} , 其中 $a_i = 33\dots3$, 由 i 个 3 构成 ($i=1, \dots, n+1$)。

由于任何正整数除以 n 的余数有 $0, 1, \dots, n-1$, 共 n 种情况。由鸽巢原理知, 一定存在两个数除以 n 后的余数相同。

假设这两个数为 a_i, a_j , 且 $a_i > a_j$, 则

$$a_i - a_j = 3\dots30\dots0 \quad (j \text{ 个 } 0, i-j \text{ 个 } 3)$$

能被 n 整除, 且是由0和3组成的正整数。