第三章

3.1鸽巢原理简单形式及应用

北航计算机学院：李建欣

Tel：82339274（G506）

E-mail：lijx@buaa.edu.cn

http://act.buaa.edu.cn/lijx

主要内容

- 3.1鸽巢原理：简单形式
- 鸽巢原理应用例子

鸽巢原理，也称为抽屉原理。

将学习运用一个简单的数学原理去证明一些排列的存在性问题。

一道趣题

- **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？**

- 路易·波萨（Louis Pósa）是匈牙利的年青数学家，14岁时就已能够发表有相当深度的数学论文。大学还没有读完，就已获得科学博士的头衔。

扩展：存在多种证明方法

- 例5：证明，如果从{1,2, …, 2n}中选择n+1个整数，那么存在两个整数，它们之间差为1。

证明思路1：设选择的n+1个整数为a_1，a_2，…，a_{n+1})、，令$b_1=a_1+1$，$b_2=a_2+1$，…，$b_n=a_n+1$，则$1<b_1<b_2<\ldots<b_n<=2n$。a_1，a_2，…，a_{n+1}，b_1，b_2，…，b_n这2n+1个数中至少有一对相等，且$b_j=a_j+1$，$b_j=a_k$ 所有a_k和a_j只相差1

证明思路2：将整数集合{1，2，…，2n}划分成{1，2}，{3，4}，…{2n-1，2n}n个整数子集合。
要满足存在的两个整数之间相差不为1，

扩展：几个问题

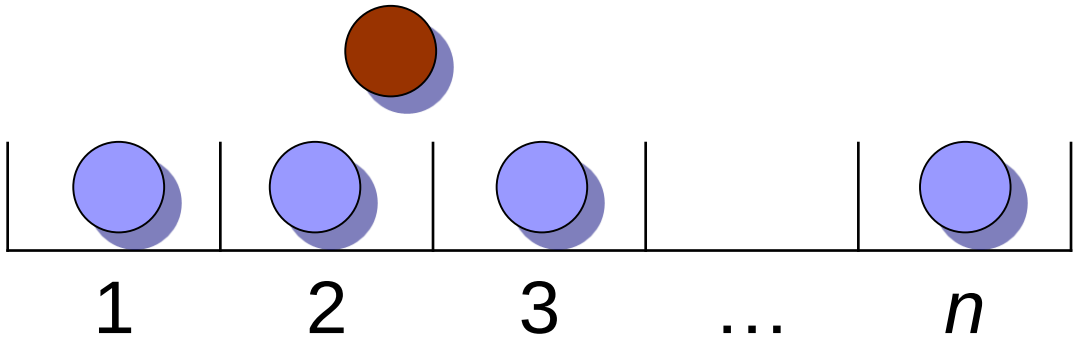
- 1.有理数m/n的十进制小数一个循环数？
- 2.一个由6台计算机组成的网络，证明在这样网络中至少存在两台计算机直接连接数量相同的其他计算机。
- 3.今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？
- **4.为信息安全提供一个方案：**

  公司的一份机密文件，需要公司所有董事会成员同时同意才能解密，而缺少其中任何1个股东不能解密该文件。

鸽巢原理简单形式

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

  转换描述： 用n种颜色的一种颜色对每个物体涂色。将n+1个物体用n中颜色涂色，必然有两个物体被涂成相同的颜色。



应用例子

- 例1. 13个人中存在两个人，他们的生日在同一个月份里。

- 例2. 设n对已婚夫妇. 为了保证能够有一对夫妇被选出，至少要从这$2n$个人中选出多少人?

例2的证明思路：

- $\binom{H_1}{W_1}$, $\binom{H_2}{W_2}$ …, $\binom{H_n}{W_n}$ 表示这n对夫妇.
- 首先, 人数应大于n, 否则选取H_1, …, H_n. 其中没有一对夫妇.
- n+1个是否足够? 运用鸽巢原理。

用于证明某种排列的存在性，
不能用于构造排列和计数。

鸽巢原理其他形式

- **n个物体放入n个盒子且没有一个是空的, 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.**

上述原理描述直观，但将问题转化为这样直观形式并不容易。

鸽巢原理的集合语言表述

令X和Y是两个有限集，f：$X \to Y$是一个由X到Y的函数。

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

鸽巢原理的集合语言表述

- 形式描述中，X对应物体集合, Y表示盒子集合，*f*表示一种物体放入盒子方法.
- 注：对无限集的情况上述结论不成立。
- 一个集合论问题：
  - A⊆B, 若存在映射*f*: A→B是一对一的, 那么, 是否一定有A=B?

鸽巢原理在数论中的应用

- **例3. 在m个整数$a_1, a_2, \ldots, a_m$, 存在$0 \le k < l \le m$, 使得$a_{k+1} + a_{k+2} + \ldots + a_l$ 能够被m整除。**
- 通俗原理：在序列$a_1, a_2, \ldots, a_m$中存在连续个a的和可以被m整除
- 思路：构造一些符合要求整数序列，利用余数定理转化为鸽巢原理形式。

令 $s_1=a_1$

$s_2=a_1+a_2$

… …

$s_m=a_1+a_2+\ldots+a_m$

由余数定理：$s_k=b_km+r_k$；$k=1,2,\ldots,m$

若存在$r_k=0$, 命题成立；

否则有：$1\le r_k\le m-1$, 由鸽巢原理存在$r_i=r_j, i\neq j$

因此，$m \mid s_j - s_i$

- 例4. 从整数1, 2, …，200中选取101个整数。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。
- **关键点：**

  任何整数可分解为一些素数的乘积， 即对任何整数

  故有形式: $n = 2^k \times a$, a是奇素数, $k \geq 0$

  a为奇数，200内只能有100个不同奇数，故可对101个数运用鸽巢原理。

例4的证明：

- 对于1到200间的整数，$n = 2^k \times a$ ，a只能是1, 3, 5, …, 199中的数
- 因此, 但选择101个数，应用鸽巢原理，存在两个数

$$n_1 = 2^{k1} \times a \quad n_2 = 2^{k2} \times a$$

- 当$k_1 \geq k_2$, 则n_2 整除n_1，否则n_1整除n_2

题目：多种领域-计算机网络

- 例6 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。
- 证明：每台计算机的直接连接数应大于等于0小于等于5，并且注意到0和5不能同时出现。因此，只能有5个数。

  由鸽巢原理6台计算机中至少有两台相同。

- **注：在这些证明中，很难直接应用鸽巢原理，通常需要我们尝试各种不同的解决方法，从而培养对问题敏感性。**

典型1：几何图形类

- 在边长为1的等边三角形内任意选择5个点，存在2个点，其间距离至多为1/2

证明：由题意，可以构造出4个抽屉，每个抽屉满足在其间的距离至多为1/2(见图1)。根据鸽巢原理，在4个抽屉里分别放置4个点，不论第5个点如何放置，都满足两点之间的距离最多为1/2。

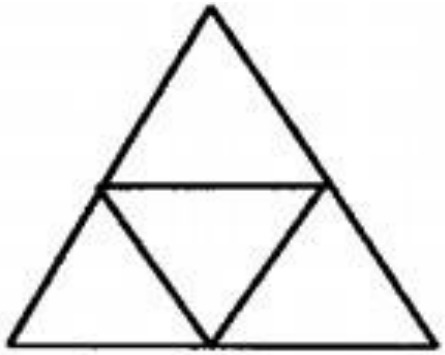
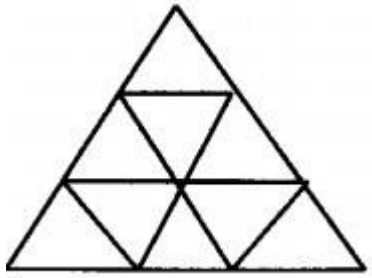


图1　4个抽屉

几何图形类(思考)

- 思考1：证明在边长为1的等边三角形内任意选择10个点，存在两个点，其间距离至多为1/3。
- 思考2：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。



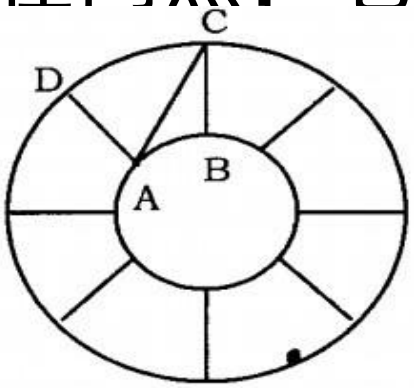


图3　9个抽屉

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

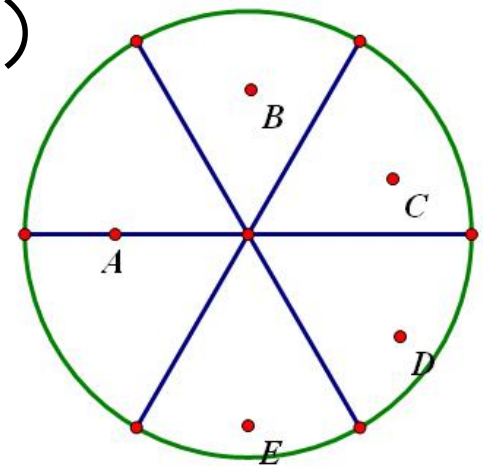
$$|AC| = \sqrt{R^2 + r^2 - 2Rr\cos\frac{\pi}{4}}$$

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

几何图形类(思考)

- 思考3：

（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。



典型2：思考：整数整除类

- 从1到2n的正整数中任取n+1个数，则这n+1个数中至少有两个数，其中一个数是另一个数的倍数。

典型3：连续时间问题

- 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
- 证明：设五年间新产品数分别为a_1，a_2，…，a_{59}，a_{60}

按题意，构造出数列a_n的前n项和的数列s_1，s_2，…s_{59}，s_{60}，

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

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

$25 \le s_1+24 < s_2+24 < \ldots < s_{59}+24 < s\_\{60\}+24 \le 95+24 = 119$

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

在[1，119]内，只有119个自然数，根据抽屉原理，必定存在两个数相等

上述两个数列又分别是严格单调的，因此必然存在一个i和j，使得$s_i = s_j + 24$。从而，该厂在从第j+1个月起到第i个月的这几个月时间里，恰

思考：连续时间问题

- 一个孩子每天至少看一个小时电视，总共看7周，但是每周看电视从不超过11小时。证明：存在连续若干天在此期间这个孩子恰好看电视20个小时。(假设这个孩子每天看电视时间为整数个小时)

中国余式定理

•韩信点兵传说：秦朝末年，楚汉相争。一次，韩信将**1500**名将士与楚王大将李锋交战。苦战一场，楚军不敌，败退回营，

•《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？”

三人同行七十稀，五树梅花廿一枝，
七子团员整半月，除百零五便得知。

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

$$70 \times 2 + 21 \times 3 + 15 \times 2 = 233$$

明 程大位

中国余式定理

- 例6 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$x=pm+a$；$x=qn+b$

思路：

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”的整数即可。

需要多少这样的数呢？考虑鸽巢原理（$b \le n-1$）.

中国余式定理（证明）

- 证明：考虑n个除以m余数为a的整数：

$$a，a+m，\ldots，(n-1)m+a$$

（1）断言：**用n除这n个整数得到余数都不相同**。注意每个余数是小于n的非负整数，由鸽巢原理n个数$0, 1, 2, \ldots，n-1$中每个数出现在这些余数集中，特别的b是其中一个余数，设对应除以n余数为b的数为$x=pm+a$（$0\le p\le n-1$），同时$x=qn+b$，结论成立。

（2）证明**用n除这n个整数得到余数都不相同**。

中国余式定理（证明）

- 证明：考虑n个除以m余数为a的整数：

$$a，a+m，\ldots，(n-1)m+a$$

（2）证明**用n除这n个整数得到余数都不相同**。

（反证法）假设存在余数相同情形,余数都为r

即

$$\left.\begin{aligned} im+a&=kn+r\\ jm+a&=ln+r \end{aligned}\right\} (j-i)m=(l-k)n$$

但m和n互为素数，不失一般性假设$(j-i)$可被n整除。

由于$0\le (j-i)\le n-1$, 不可能被n整除

所有矛盾，原命题成立。

中国余式定理一般形式

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

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

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,…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。

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：

   $A=g^x \bmod n$
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：

   $B=g^y \bmod n$
5. Bob将B发给Alice
6. 计算秘密密钥K1如下：

   $K1=B^x \bmod n$
7. 计算秘密密钥K2如下：

   $K2=A^y \bmod n$

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。

作业

P.51, 3.4练习题：

7）证明对任意给定52个整数，存在两个，要么两者之和被100整除，要么两者之差被100整除。

- 在Internet上查找关于**中国剩余定理**在计算机研究的相关文章，了解怎样应用数学技巧解决实际问题。

  搜索关键词：中国剩余定理、信息安全、公开密码算法