浙江大学
ZHEJIANG UNIVERSITY

秘密共享

浙江大学 谈之奕

秘密共享

数学建模

P D W K #W

- 秘密共享（secret sharing）
  - 一保密场所入口处有一安全门，相关5人中有3人及以上在场才能打开
  - 安全门上安装多把锁，所有锁同时打开时安全门才能打开。每人拥有部分锁的钥匙，每把钥匙只能打开一把锁，一把锁可以配多把钥匙
  - 在安全门上安装10把锁，每把锁配发3把钥匙，每人手中有6把锁的钥匙
    - 任取3列，必有任何锁的钥匙
    - 任取2列，必缺一把锁的钥匙
    - 每把锁与一个两人组合对应
    - 每个人拥有他不在的两人组合对应的锁的钥匙

$$\binom{5}{2}=10$$

$$\binom{4}{2}=6$$

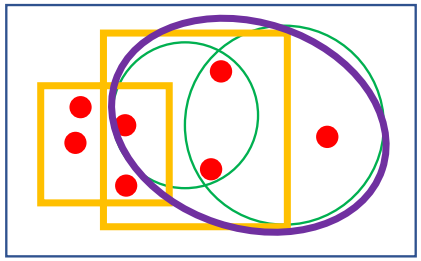
	A	B	C	D	E	
1			√	√	√	AB
2		√		√	√	AC
3		√	√		√	AD
4		√	√	√		AE
5	√			√	√	BC
6	√		√		√	BD
7	√		√	√		BE
8	√	√			√	CD
9	√	√		√		CE
10	√	√	√			DE

组合方法

数学建模

P D W K #W

- “少数”与“多数”
  - 设相关人共有 $2n+1$ 个，任意 n 人组成的“少数”团体不能打开安全门，任意 $n+1$ 人组成的“多数”团体可以打开安全门
    - 两个不同的“少数”团体联合必包含某个多数团体
    - 任一“少数”团体和不属该团体的任一人联合可成为多数团体
- 锁与钥匙
  - 安全门上至少需要 $\binom{2n+1}{n}$ 把锁 $\binom{11}{5}=462$
    - 任一“少数”团体至少有一把锁不能打开
    - 任意两个“少数”团体打不开的锁各不相同
  - 每个人至少需要 $\binom{2n}{n}$ 把钥匙 $\binom{10}{5}=252$
    - 每个人需拥有他所不属于的所有“少数”团体所打不开的锁的钥匙



Example 1-11 Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet such that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry? To answer

Liu, C.L. *Introduction to Combinatorial Mathematics.* McGraw-Hill, 1968.

密码学

数学建模

P D W K #W

- 密码学（Cryptology）
  - 研究如何安全地传递和存储保密信息的方法的科学
    - 明文（plaintext）：可懂的消息
    - 密文（ciphertext）：明文通过加密变换成的不可懂的消息
    - 加密（encryption）：从明文变换成密文的过程
    - 解密（decryption）：把密文变换成明文的过程
- 秘密共享（secret sharing）
  - 将秘密分成若干份，分发给不同的用户。用户特定子集共同提供各自的份额，才能重构初始秘密
- 门限机制（threshold scheme）(t,n)
  - 在 n 人之间共享秘密，其中任意 $t \le n$ 个人可求出秘密，任意 $t-1$ 个人无法求出秘密

Claude Elwood Shannon (1916-2001)
美国数学家

Alan Turing (1912-1954)
英国数学家、计算机科学家

Shamir门限机制

数学建模

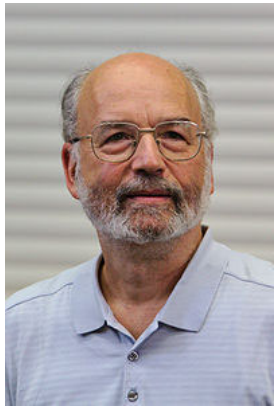
P D W K #W

- Shamir门限机制 (t,n)
  - 任选 $t-1$ 个整数 $x_1,x_2,\cdots,x_{t-1}$ 和 n 个互不相同的整数 $c_1,c_2,\cdots,c_n$ 。素数 $p>n+1$
  - 求 $b_j \equiv (K+c_j x_1 + {c_j}^2 x_2 + \cdots + {c_j}^{t-1} x_{t-1}) \pmod p$, $j=1,\cdots,n$，其中 $K \in \mathbb{Z}$ 为秘密
    - $f(c) = K + x_1 c + x_2 c^2 + \cdots + x_{t-1} c^{t-1}$, $b_j \equiv f(c_j) \pmod p$, $j=1,\cdots,n$
  - 将秘密份额 (c_j, b_j) 告知第 j 人

$n=5, t=3$ $K=13$ $(1,8),(2,7),(3,10),(4,0),(5,11)$

$x_1=10, x_2=2$ $p=17$ $b_j \equiv (13+10c_j+2{c_j}^2) \pmod{17}$, $j=1,\cdots,n$

$c_1=1, c_2=2, c_3=3, c_4=4, c_5=5$ $b_1=8, b_2=7, b_3=10, b_4=0, b_5=11$



Adi Shamir
(1952-)
以色列密码学家
2002年图灵奖得主
2008年以色列奖得主
RSA密码体制发明人之一

Shamir A. How to share a secret. *Communications of the ACM*, 1979, 22(11): 612-613.

Shamir门限机制

数学建模

P D W K #W

- Shamir门限机制
  - 若 t 个人 $j_1,\cdots,j_t$ 共享秘密份额 $\left(c_{j_i},b_{j_i}\right),i=1,\cdots,t$
    - 方程组 $b_{j_i}\equiv(K+c_{j_i}x_1+{c_{j_i}}^2x_2+\cdots+{c_{j_i}}^{t-1}x_{t-1})\ (\mathrm{mod}\ p)\ ,i=1,\cdots,t$ 在模 p 意义下有唯一解
  - 若 $t-1$ 个人 $j_1,\cdots,j_{t-1}$ 共享秘密份额 $\left(c_{j_i},b_{j_i}\right),i=1,\cdots,t-1$
    - 方程组 $b_{j_i}\equiv(K+c_{j_i}x_1+{c_{j_i}}^2x_2+\cdots+{c_{j_i}}^{t-1}x_{t-1})\ (\mathrm{mod}\ p)\ ,i=1,\cdots,t-1$ 含 $t-1$ 个方程，t 个未知数，在模 p 意义下有无穷多组解

$(1,8),(2,7),(3,10)\quad p=17$

$$b_j\equiv(K+c_jx_1+{c_j}^2x_2)\ (\mathrm{mod}\ p)\ ,\ j=1,\cdots,n$$

$$\begin{cases}8\equiv\left(1\cdot K+1\cdot x_1+1^2\cdot x_2\right)(\mathrm{mod}\,17)\\10\equiv\left(1\cdot K+3\cdot x_1+3^2\cdot x_2\right)(\mathrm{mod}\,17)\\11\equiv\left(1\cdot K+5\cdot x_1+5^2\cdot x_2\right)(\mathrm{mod}\,17)\end{cases}$$

$$K=13,x_1=10,x_2=2$$

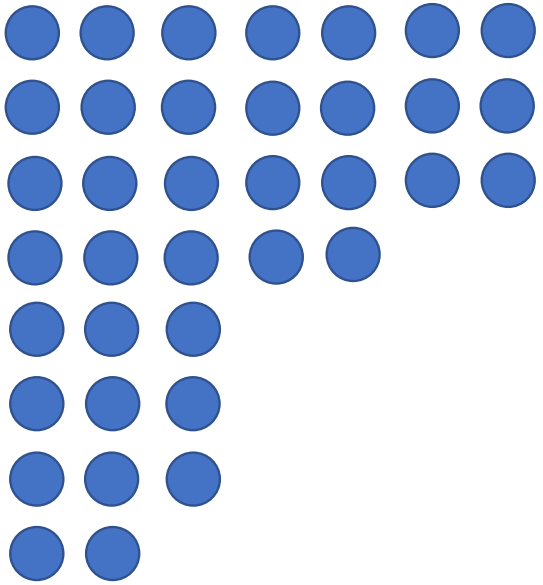
$$\begin{vmatrix}1 & c_1 & c_1^2 & \cdots & c_1^{t-1}\\1 & c_2 & c_2^2 & \cdots & c_2^{t-1}\\\vdots & \vdots & \vdots & \vdots & \vdots\\1 & c_{t-1} & c_{t-1}^2 & \cdots & c_{t-1}^{t-1}\\1 & c_t & c_t^2 & \cdots & c_t^{t-1}\end{vmatrix}\neq 0$$

Vandermonde行列式

Alexandre-Théophile Vandermonde (1735-1796)
法国数学家

中国剩余定理

- “物不知数”
  - 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？答曰：二十三
  - 术曰：三三数之，剩二，置一百四十；五五数之，剩三，置六十三；七七数之，剩二，置三十。并之，得二百三十三，以二百一十减之，即得
  - 凡三三数之，剩一，则置七十；五五数之，剩一，则置二十一；七七数之，剩一，则置十五。一百六以上，以一百五减之，即得

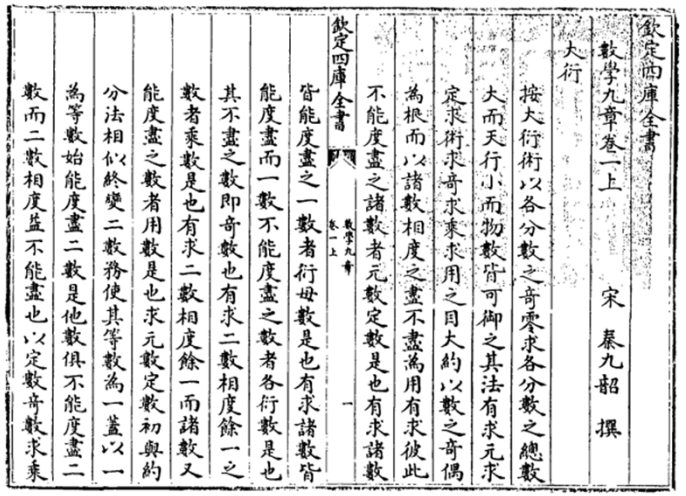



孫子算經序
孫子曰夫算者天地之經緯萬生之元首五常之本末陰陽之父母星辰之建號三光之表裏五行之準平四時之終始萬物之祖宗六藝之細紀稽叅倫之聚散考二氣之降升推寒暑之迭運步遠近之殊同觀天道精微之兆基察地理從橫之長短采神祇之所在極成敗之符驗窮道德之理究性命之情立規矩准方圓謹法度約尺丈立權衡平重輕剖毫氂析黍絫展億

《孙子算经》，中国数学著作。作者不详，约成书于公元400年前后。全书共三卷，卷上为预备知识，卷中、下为应用题。图为宋刻本序

中国剩余定理

- “大衍求一术”
  - 秦九韶在《数书九章》中提出的解一次同余方程组的方法。对《孙子算经》中的“物不知数”题的一般情形给出了具体求解方法，证明了孙子定理
- 中国剩余定理（Chinese remainder theorem）
  - 18世纪中叶起，Euler，Lagrange，Gauss相继研究同余式问题。Gauss在1801年撰写的《Disquisitiones Arithmeticae》（算术研究）中给出了关于同余式的一般性定理
  - 1852年，英国传教士伟烈亚力（Alexander Wylie）将“大衍求一术”传至欧洲。孙子定理在国际上被称为中国剩余定理


欽定四庫全書
數學九章卷一上
宋 秦九韶 撰
大衍
按大衍術以各分數之奇零求各分數之總數
大而天行小而物數皆可御之其法有求元求
定求術求奇求乘求用之目大約以數之奇偶
為根而以諸數相度之盡不盡為用有求彼此
不能度盡之諸數者元數定數是也有求諸數
欽定四庫全書
皆能度盡之一數者衍母數是也有求諸數皆
能度盡而一數不能度盡之數者各衍數是也
其不盡之數即奇數也有求二數相度餘一之
數者乘數是也有求二數相度餘一而諸數又
能度盡之數者用數是也求元數定數初與約
分法相似終變二數務使其等數為一蓋以一
為等數始能度盡二數是他數俱不能度盡二
數而二數相度益不能盡也以定數奇數求乘

秦九韶（约1202-约1261），南宋数学家，字道古。淳祐七年（1247年），撰成《数书九章》。全书分9类，81题，是中国宋元数学高潮的代表作之一。图为四库全书版

整除与同余

数学建模

P D W K #W

- 整除
  - 设 $a,b\in\mathbb{Z}$，$a\neq 0$。若存在 $q\in\mathbb{Z}$，使得 $b=aq$，则称 b 可被 a 整除，a 是 b 的约数。记为 $a|b$
  - 若正整数 $p\neq 1$ 除 $\pm 1,\pm p$ 外没有其他的约数，则称 p 为素数（prime number）
  - 设 $a_1,\cdots,a_k$ 为整数，若 $d\,|\,a_i,i=1,\cdots,k$，则称 d 为 $a_1,\cdots,a_k$ 的公约数
    - 整数 $a_1,\cdots,a_k$ 的公约数中最大的称为 $a_1,\cdots,a_k$ 的最大公约数（Greatest Common Divisor，GCD），记为 $(a_1,\cdots,a_k)$
  - 若 $(a_1,\cdots,a_k)=1$，则称 $a_1,\cdots,a_k$ 互素
- 同余
  - 设 $m\in\mathbb{Z}^+$，若 $m\,|\,(a-b)$，则称 a 同余于 b 模 m，记作 $a\equiv b\,(\mathrm{mod}\,m)$
    - 若 $a\equiv b\,(\mathrm{mod}\,m)$，则 $b\equiv a\,(\mathrm{mod}\,m)$

同余方程

数学建模

P D W K #W

- 逆
  - 设 $m \geq 1$，若存在 c 使得 $a \cdot c \equiv 1 \pmod{m}$，则称 a 模 m 可逆，且 c 称为 a 对模 m 的逆，记为 $a^{-1} \pmod{m}$ 或 a^{-1}
    - a 对模 m 可逆的充要条件是 $(a,m)=1$
- 一次同余方程
  - $ax \equiv b \pmod{m}$ 称为模 m 的一次同余方程
    - 方程有解的充要条件是 $(a,m) \mid b$
    - 当 $(a,m)=1$ 时，方程的解为 $a^{-1}b$，且小于 m 的非负整数解是唯一的

$6 \cdot c \equiv 1 \pmod{8}$

$6 \cdot x \equiv 2 \pmod{8}$

$x = 3, 7$

$3 \cdot x \equiv 2 \pmod{8}$

$3^{-1} \pmod{8} = 3$

$x = 6, 14, 22, \cdots$

$27^{-1} \pmod{64} = 19$

	1	**27**
		64
$64 = 2 \times 27 + 10$	**1**	**27**
	2	**10**
$27 = 2 \times 10 + 7$	**5**	**7**
$1 + 2 \times 2 = 5$	**2**	**10**
$10 = 1 \times 7 + 3$	**5**	**7**
$5 + 1 \times 2 = 7$	**7**	**3**
$7 = 2 \times 3 + 1$	**19**	**1**
$5 + 2 \times 7 = 19$	**7**	**3**

大衍求一數云置奇右上定居右下立天元一於左上
先以右上除右下所得商數與左上一相生入左下然
後乃以右行上下以少除多遞互除之所得商數隨即
遞互累乘歸左行上下須使右上末後奇一而止乃驗
左上所得以為乘率或奇數已見單一者便為乘率按此

中国剩余定理

数学建模

P D W K #W

- 中国剩余定理
  - 一次同余方程组 $x \equiv a_j \pmod{m_j}, 1 \le j \le k$ 小于 m 的非负整数解是唯一的，即为 $x \equiv N_1 N_1^{-1} a_1 + \cdots + N_k N_k^{-1} a_k \pmod{m}$
    - $m_1, \cdots, m_k$ 为两两互素的正整数，$m = m_1 \cdots m_k$，$a_1, \cdots, a_k$ 为任意整数。对任意 $1 \le j \le k$，记 $N_j = \dfrac{m}{m_j}$，N_j^{-1} 为 N_j 对模 m_j 的逆
    - 对任意 $l \in \mathbb{Z}$，$x + l \cdot m$ 也是同余方程组的解
- “物不知数”

$$\begin{cases} x \equiv 2 \pmod 3 & N_1 = 5 \cdot 7 = 35 & N_1^{-1} \pmod 3 = 2 \\ x \equiv 3 \pmod 5 & N_2 = 3 \cdot 7 = 21 & N_2^{-1} \pmod 5 = 1 \\ x \equiv 2 \pmod 7 & N_3 = 3 \cdot 5 = 15 & N_3^{-1} \pmod 7 = 1 \end{cases}$$

$$m = 3 \cdot 5 \cdot 7 = 105 \qquad 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233$$

$$x = 23 \equiv 233 \pmod{105}$$

凡三三数之，剩一，则置七十；五五数之，剩一，则置二十一；七七数之，剩一，则置十五。一百六以上，以一百五减之，即得

三人同行七十稀，五树梅花廿一支，七子团圆正半月，除百零五使得知。

——[明]程大位，《算法统宗》

Asmuth-Bloom门限机制

数学建模

P D W K #W

- **Asmuth-Bloom门限机制** (t,n)
  - 选取整数 p 与 $m_1,\cdots,m_n$
    - $p>K$ 且 p 与 $m_j,1\le j\le n$ 互素，$m_1<\cdots<m_n$ 且 $m_1,\cdots,m_n$ 两两互素
    - $$\frac{m_1\cdots m_t}{m_{n-t+2}\cdots m_n}>p$$
      - $m_1,\cdots,m_n$ 中任意 t 个数的乘积与任意 $t-1$ 个数的乘积之比大于 p
  - 令 $K'=K+r\cdot p$，其中 $r\in\mathbb{N}$ 满足 $0\le r\le\frac{m_1\cdots m_t}{p}-1$
    - $K'=K+r\cdot p\le K+m_1\cdots m_t-p<m_1\cdots m_t$
  - 令 $k_j\equiv K'\pmod{m_j},1\le j\le n$，将秘密份额 (k_j,m_j) 告知第 j 人

Asmuth AC, Bloom J. A modular approach to key safeguarding. *IEEE Transactions on Information Theory*, 29, 208-210, 1983.

$$n=3,t=2\quad K=3$$

$$p=5\quad m_1=7,m_2=9,m_3=11$$

$$\frac{m_1\cdot m_2}{m_3}=\frac{7\cdot 9}{11}>5=p$$

$$r=9<\frac{7\cdot 9}{5}-1=\frac{m_1\cdot m_2}{p}-1$$

$$K'=3+9\cdot 5=48<7\cdot 9$$

$$6=k_1\equiv 48(\bmod 7)$$

$$3=k_2\equiv 48(\bmod 9)$$

$$4=k_3\equiv 48(\bmod 11)$$

$$(6,7),(3,9),(4,11)$$

Asmuth-Bloom门限机制

数学建模

P D W K #W

- **Asmuth-Bloom门限机制**
  - 一次同余方程组（I） $x \equiv k_j \pmod{m_j}, 1 \le j \le n$ 有唯一的小于 $m_1 \cdots m_n$ 的非负整数解 K'
  - 若 t 个人 $j_1, \cdots, j_t$ 共享秘密份额 $(k_{j_i}, m_{j_i}), i = 1, \cdots, t$
    - 一次同余方程组（II） $x \equiv k_{j_i} \pmod{m_{j_i}},\ i = 1, \cdots, t$ 有唯一的小于 $m_{j_1} \cdots m_{j_t}$ 的正整数解 X
    - K' 也为方程组（II）的解，且 $K' < m_1 \cdots m_t < m_{j_1} \cdots m_{j_t}$。由解的唯一性，$X = K'$

$$k_j \equiv K' \pmod{m_j}, 1 \le j \le n$$

$$K' \equiv k_j \pmod{m_j}, 1 \le j \le n$$

$$K' = K + r \cdot p < m_1 \cdots m_t$$

$$K \equiv K' \pmod{p}$$

$$\text{(I)} \begin{cases} x \equiv k_1 \pmod{m_1} \\ x \equiv k_2 \pmod{m_2} \\ \cdots \\ x \equiv k_{t-1} \pmod{m_{t-1}} \\ x \equiv k_t \pmod{m_t} \\ \cdots \\ x \equiv k_n \pmod{m_n} \end{cases} \quad \text{(II)}$$

$n = 3, t = 2 \quad p = 5$

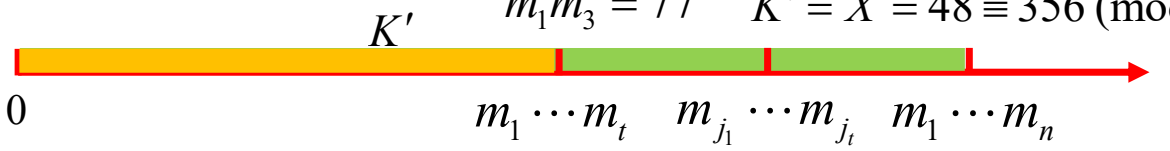
$m_1 = 7, m_2 = 9, m_3 = 11$

$k_1 = 6, k_2 = 3, k_3 = 4$

$$\begin{cases} x \equiv 6 \pmod 7 & N_1 = 11 \quad N_1^{-1} = 2 \\ x \equiv 4 \pmod{11} & N_3 = 7 \quad N_3^{-1} = 8 \end{cases}$$

$$N_1 N_1^{-1} k_1 + N_3 N_3^{-1} k_3 = 11 \cdot 2 \cdot 6 + 7 \cdot 8 \cdot 4 = 356$$

$$m_1 m_3 = 77 \quad K' = X = 48 \equiv 356 \pmod{77}$$



Asmuth-Bloom门限机制

数学建模

P D W K #W

- **Asmuth-Bloom门限机制**
  - 一次同余方程组（I） $x \equiv k_j \pmod{m_j}, 1 \le j \le n$ 有唯一的小于 $m_1 \cdots m_n$ 的非负整数解 K'
  - 若 $t-1$ 个人 $j_1, \cdots, j_{t-1}$ 共享秘密份额 $(k_{j_i}, m_{j_i}), i = 1, \cdots, t-1$
    - 一次同余方程组（III） $x \equiv k_{j_i} \pmod{m_{j_i}},\ i = 1, \cdots, t-1$ 有唯一的小于 $m_{j_1} \cdots m_{j_{t-1}}$ 的正整数解 Y
    - $Y + l \cdot m_{j_1} \cdots m_{j_{t-1}}, l \in \mathbb{Z}$ 均为方程组（III）的解，K' 为这些解中的某一个

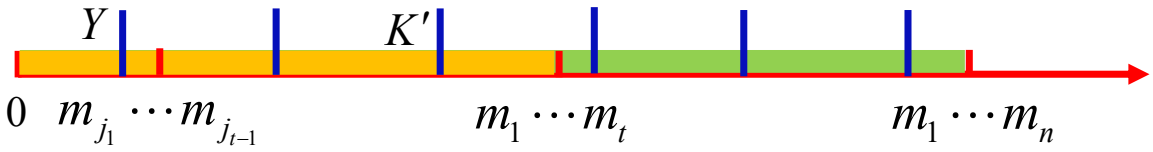
$n = 3, t = 2 \quad p = 5$

$m_1 = 7, m_2 = 9, m_3 = 11$

$k_1 = 6, k_2 = 3, k_3 = 4$

$\begin{cases} x \equiv 4 \pmod{11} \\ Y \equiv 4 \pmod{11} \end{cases}$

$K' = 4, 15, 26, 37, 48, 59, \cdots$?



$k_j \equiv K' \pmod{m_j}, 1 \le j \le n$

$K' \equiv k_j \pmod{m_j}, 1 \le j \le n$

$K' = K + r \cdot p < m_1 \cdots m_t$

$K \equiv K' \pmod{p}$

(I) $\begin{cases} x \equiv k_1 \pmod{m_1} \\ x \equiv k_2 \pmod{m_2} \\ \cdots \\ x \equiv k_{t-1} \pmod{m_{t-1}} \\ x \equiv k_t \pmod{m_t} \\ \cdots \\ x \equiv k_n \pmod{m_n} \end{cases}$ (III)


谢　谢