浙江大学
ZHEJIANG UNIVERSITY

数论模型

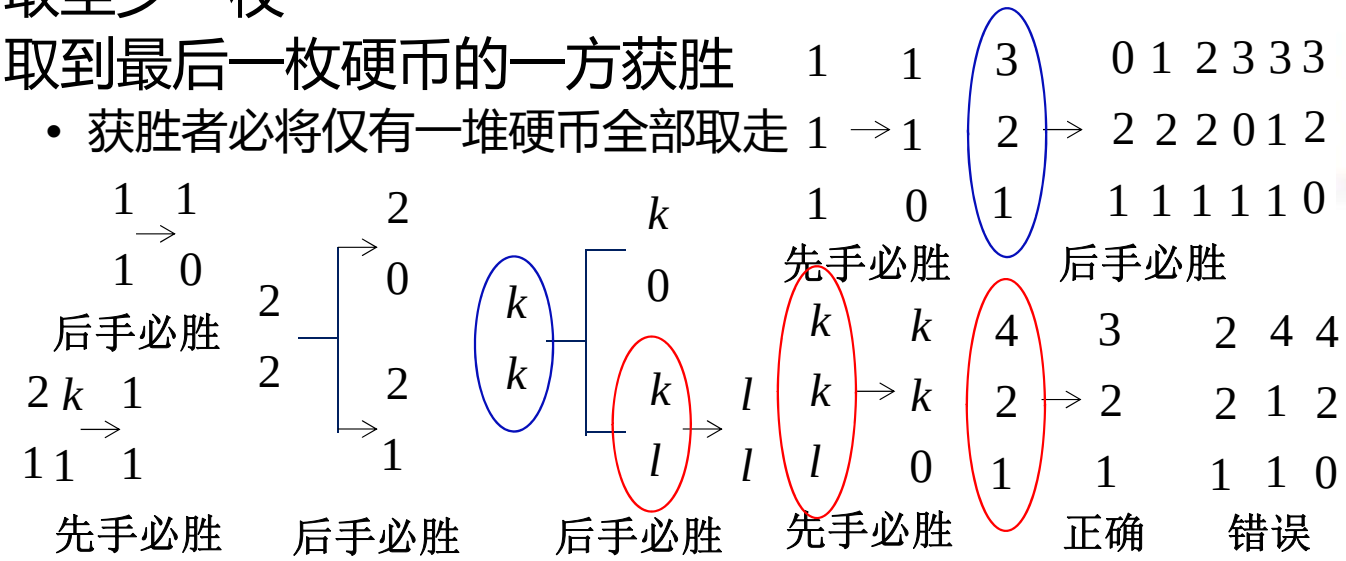
浙江大学 谈之奕

NIM游戏

数学建模

MATH T

- NIM游戏
  - 现有 n 堆硬币，每堆数量一定
  - 两人轮流取硬币，每次只能从其中一堆中取，每次取至少一枚
  - 取到最后一枚硬币的一方获胜
    - 获胜者必将仅有一堆硬币全部取走



Bouton CL. Nim, a game with a complete mathematical theory. *Annals of Mathematics*, 3: 35-39, 1901.

nehmen: vt. 拿，取，拿起

nimm：nehmen的命令式

Charles Leonard Bouton
（1869-1922）
美国哈佛大学数学系副教授，**1898**年于德国莱比锡大学取得博士学位

记数法

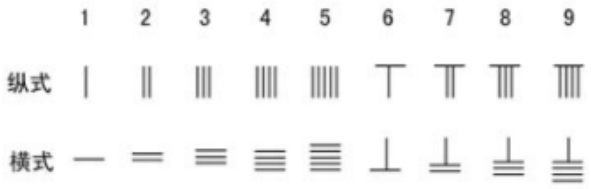
数学建模

MATH T

- 记数法（number system）
  - 记录或标志数目的方法
- 位值制记数法（positional numeral system）
  - 用一组有顺序的数字来表示一个数。每个数字所表示的大小，既取决于它本身的数值，又取决于它所在的位置
  - 十进制记数法

罗马数字	Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	Ⅵ	Ⅶ
含义	**1**	**2**	**3**	**4**	**5**	**6**	**7**
罗马数字	Ⅷ	Ⅸ	Ⅹ	Ⅼ	Ⅽ	Ⅾ	Ⅿ
含义	**8**	**9**	**10**	**50**	**100**	**500**	**1000**

巴比伦	六十进制
古印度	十进制
中国古代	十进制
玛雅人	二十进制



从右到左，纵横相间

CCLIX **259**

$259 = 2\cdot10^2 + 5\cdot10 + 9$

木楼式时刻更钟
[清]乾隆
故宫博物院藏

二进制

数学建模

MATH T

- 位值制记数法
  - 选定进位制的基底 b ，给定 $0,1,2,\cdots,b-1$共 b 个数码，任何一个自然数 N ， 均可用某个以这些数码为系数的 b 的多项式表示出来

$$N = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b + a_0$$

$$\Rightarrow (a_k a_{k-1} \cdots a_1 a_0)_b,\ a_0, a_1, \cdots, a_{k-1} \in \{0,1,\cdots,b-1\}$$

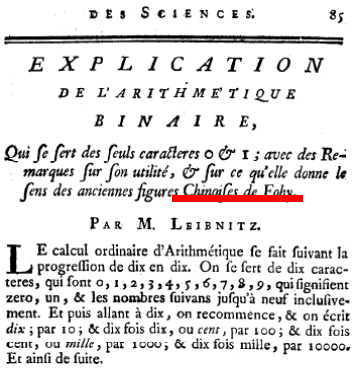
    - 任意数的 b 进制表示是唯一的
    - 任意两个不同数的 b 进制表示不同
- 二进制（binary number system）
  - 基底为 2 ，用数码 0 和 1 表示的记数法

二进制在电子计算机中得到了广泛的应用。计算机由逻辑电路组成，电路中通常只有两个状态：开关接通和断开。两种状态恰好可用 1和 0表示

$$0+0=0$$

$$0+1=1$$

$$1+1=10$$



DES SCIENCES. 85

EXPLICATION
DE L'ARITHMETIQUE
BINAIRE,

Qui ſe ſert des ſeuls caracteres 0 *&* 1 *; avec des Remarques ſur ſon utilité, & ſur ce qu'elle donne le ſens des anciennes figures Chinoiſes de Fohy.*

PAR M. LEIBNITZ.

LE calcul ordinaire d'Arithmétique ſe fait ſuivant la progreſſion de dix en dix. On ſe ſert de dix caracteres, qui ſont 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, qui ſignifient zero, un, & les nombres ſuivans juſqu'à neuf inclusivement. Et puis allant à dix, on recommence, & on écrit *dix* ; par 10 ; & dix fois dix, ou *cent*, par 100 ; & dix fois cent, ou *mille*, par 1000 ; & dix fois mille, par 10000. Et ainſi de ſuite.

Gottfried Wilhelm Leibniz（1646-1716）德国哲学家、数学家

Leibniz G, Explanation of binary arithmetic, which uses only the characters 1 and 0, with some remarks on its usefulness, and on the light it throws on the ancient Chinese figures of Fu Xi, *Memoires de mathématique et de physique de l'Académie royale des sciences, Académie royale des sciences*, 1703

NIM游戏

- “安全” 与 “不安全”
  - 将每堆硬币数表示为二进制，若它们每一位上数字之和为 0 ，则当前状态为安全的，否则为不安全
    - 取走最后一枚硬币前，状态为不安全的
  - 若当前状态安全，对任意取法，状态变为不安全
    - 在某堆硬币中取，该堆硬币数的二进制表示中至少有一位数字有变化
  - 若当前状态不安全，存在一种取法，状态变为安全
    - 按自左至右的顺序确定第一个数字之和不为 0 的位，寻找该位数字为 1 的堆，从该堆中取走若干枚使得状态变为安全
- 必胜策略
  - 己方取后，状态为安全的
    - 若初始状态不安全，先手方存在必胜策略
    - 若初始状态安全，后手方存在必胜策略

数学建模

MATH T

2	10	2	10
12	1100	12	1100
13	1101	13	1101
21	10101	3	11
	10110		0000

2	10	2	10
9	1001	9	1001
8	1000	13	1101
3	11	3	11
	0000		0101

数论

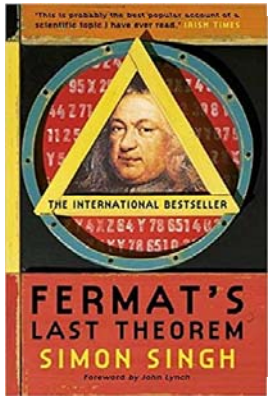
数学建模

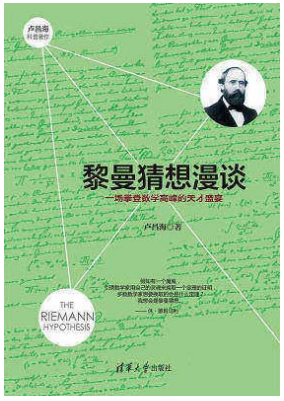
MATH T

- 数论（number theory）
  - 研究整数性质的数学分支
    - 数论问题的表述大多是算术的，但绝大多数问题用初等方法根本无法讨论。对数论的研究常常综合应用几何、代数和分析方法
    - 数论在计算机科学、信息科学、组合分析、密码学、计算数学、管理科学等领域获得广泛应用
    - 数论在中国古代有着悠久光辉的研究历史和成就，也是中国近代数学最早开拓并取得瞩目成就的数学研究领域之一

华罗庚 (1910-1985)　柯召 (1910-2002)　闵嗣鹤 (1913-1973)

王元 (1930-2021)　潘承洞 (1934-1997)　陈景润 (1933-1996)





Singh S, Fermat's Last Theorem, Harpercollins Pub Ltd, 2002(中译本：费马大定理-一个困惑了世间智者358年的谜，薛密译，广西师范大学出版社，2013)

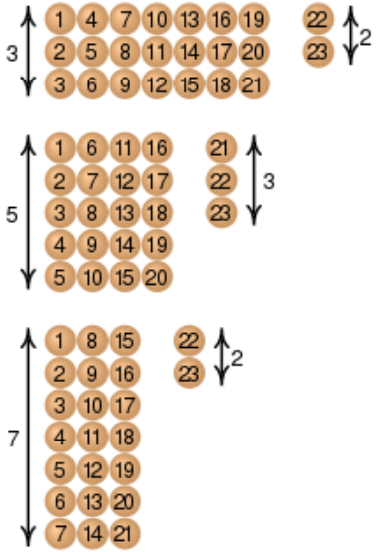
卢昌海，黎曼猜想漫谈：一场攀登数学高峰的天才盛宴，清华大学出版社，2016

中国剩余定理

数学建模

MATH T

- “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綱紀稽幽倫之聚徹考三氣之降升推冥昧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準方圓謹法度約尺丈立權衡平重輕剖毫氂析秒忽靡億

《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

数学建模

MATH T

- “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解法的一般性定理
  - 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
定求衍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
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

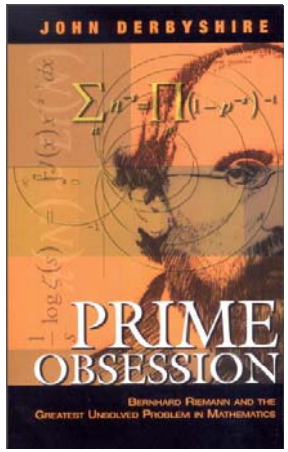
秦九韶（约1202-约1261），南宋数学家，字道古。淳祐七年（1247年），撰成《数书九章》。全书分9类，81题，是中国宋元数学高潮的代表作之一。图为四库全书版

整除

数学建模

MATH T

- 整除 $a|b$
  - 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
    - b 是 a 的倍数
    - a 是 b 的约数
- 素数（prime number）
  - 正整数 $p\neq 1$ ，除了 $\pm 1,\pm p$ 外没有其他的约数
- 最大公约数（Greatest Common Divisor，GCD）
  - 设 $a_1,\cdots,a_k$ 为整数，若 $d\mid a_i,i=1,\cdots,k$ ，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，记为 $(a_1,\cdots,a_k)$
- 互素
  - 若 $(a_1,\cdots,a_k)=1$ ，则称 $a_1,\cdots,a_k$ 互素



Derbyshire J, Prime obsession Bernhard Riemann and the greatest unsolved problem in Mathematics, Joseph Henry Press, 2002(中译本：素数之恋：黎曼和数学中的未解之谜，陈为蓬译，上海科技教育出版社，2018)

同余

数学建模

MATH T

- 同余
  - 设 $m \geq 1$，若 $m \mid (a-b)$，则称 a 同余于 b 模 m，记作 $a \equiv b \pmod{m}$

$18 \equiv 48 \pmod{10}$　　$48 \equiv 18 \pmod{10}$

$6 \cdot 3 \equiv 6 \cdot 8 \pmod{10}$　　~~$3 \equiv 8 \pmod{10}$~~

- 逆
  - 设 $m \geq 1$，若存在 c 使得 $a \cdot c \equiv 1 \pmod{m}$，则称 a 可逆，且 c 称为 a 对模 m 的逆，记为 $a^{-1} \pmod{m}$ 或 a^{-1}
  - a 可逆的充要条件是 $(a,m)=1$

~~$5 \cdot c \equiv 1 \pmod{10}$~~

- 一次同余方程
  - 当 $(a,m)=1$ 时，模 m 的一次同余方程 $ax \equiv b \pmod{m}$ 有解 $a^{-1}b$，小于 m 的非负整数解是唯一的

$a \cdot c + m \cdot k = 1$

$3 \cdot x \equiv 2 \pmod{8}$　　$6 \cdot x \equiv 2 \pmod{8}$　　$27^{-1} \pmod{64} = 19$

$3^{-1} \pmod{8} = 3$　　$x = 6, 14, 20, \cdots$　　$x = 3, 7$

奇　　定　　乘率

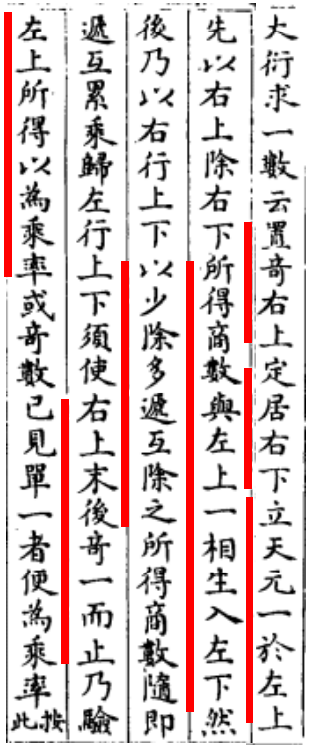
1	27
	64

1	27
2	10

5	7
2	10

5	7
7	3

19	1
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此

中国剩余定理

数学建模

MATH T

- 中国剩余定理
  - 设 $m_1,\cdots,m_k$ 为两两互素的正整数，$a_1,\cdots,a_k$ 为任意整数，$x_j \equiv a_j \pmod{m_j}, 1 \le j \le k$ 称为一次同余方程组
  - 记 $m = m_1 \cdots m_k$，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
  - 同余方程组小于 m 的非负整数解是唯一的，即为

$$x \equiv N_1 N_1^{-1} a_1 + \cdots + N_k N_k^{-1} a_k \pmod{m}$$

- “物不知数”

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

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

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

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》

三岁孩儿七十稀，五留廿一事尤奇。
七度上元重相会，寒食清明便可知。
——[宋]周密

秘密共享

数学建模

MATH T

- 门限机制（threshold scheme）(t,n)
  - 在 n 人之间共享密钥 $K\in\mathbb{Z}$，其中任意 $t\le n$ 个人可求出 K，任何 $t-1$ 个人无法求出 K
- **Asmuth-Bloom门限机制**
  - 选取整数 p 与 $m_1,\cdots,m_n$ 满足
    - $p>K$ 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
    - $\dfrac{m_1\cdots m_t}{m_{n-t+2}\cdots m_n}>p$ 最小的 t 个数的乘积 / 最大的 $t-1$ 个数的乘积；任意 t 个数的乘积与任意 $t-1$ 个数的乘积之比大于 p
  - 选取整数 $0\le r\le \dfrac{m_1\cdots m_t}{p}-1$，$K'=K+r\cdot p\le K+m_1\cdots m_t-p<m_1\cdots m_t$
  - 令 $k_j\equiv K'\pmod{m_j}, 1\le j\le n$，将秘密份额（share）$(k_j,m_j)$ 告知第 j 人

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

$n=3,t=2$

$K=3\quad p=5$

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

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

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

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

$6=k_1\equiv 48\pmod 7$

$3=k_2\equiv 48\pmod 9$

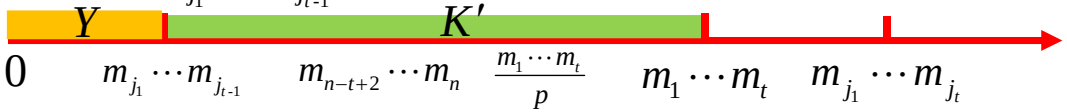
$4=k_3\equiv 48\pmod{11}$

秘密共享

数学建模

MATH T

- **Asmuth-Bloom门限机制**
  - 一次同余方程组（I） $x \equiv k_j \pmod{m_j}, 1 \le j \le n$ 有唯一的非负整数解 $K' < m_1 \cdots m_t$
  - 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' 也为一次同余方程组（I） $x \equiv k_{j_i} \pmod{m_{j_i}},\ i = 1, \cdots, t$ 的解，且 $K' < m_1 \cdots m_t < m_{j_1} \cdots m_{j_t}$。由解的唯一性，$X = K'$
  - 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，方程组的所有解为 $Y + l \cdot m_{j_1} \cdots m_{j_{t-1}}, l \in \mathbb{Z}$，$K'$ 为这些解中的某一个



$K' = K + r \cdot p < m_1 \cdots m_t, \quad k_j \equiv K' \pmod{m_j}, 1 \le j \le n \quad K \equiv K' \pmod{p}$

$n = 3, t = 2$

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

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

$$\begin{cases} x \equiv 6 \pmod 7 & N_1 = 11 \quad N_1^{-1} = 2 \\ x \equiv 4 \pmod{11} & N_2 = 7 \quad N_2^{-1} = 8 \end{cases}$$

$11 \cdot 2 \cdot 6 + 7 \cdot 8 \cdot 4 = 356$

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

$\{x \equiv 4 \pmod{11}$

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


谢　谢