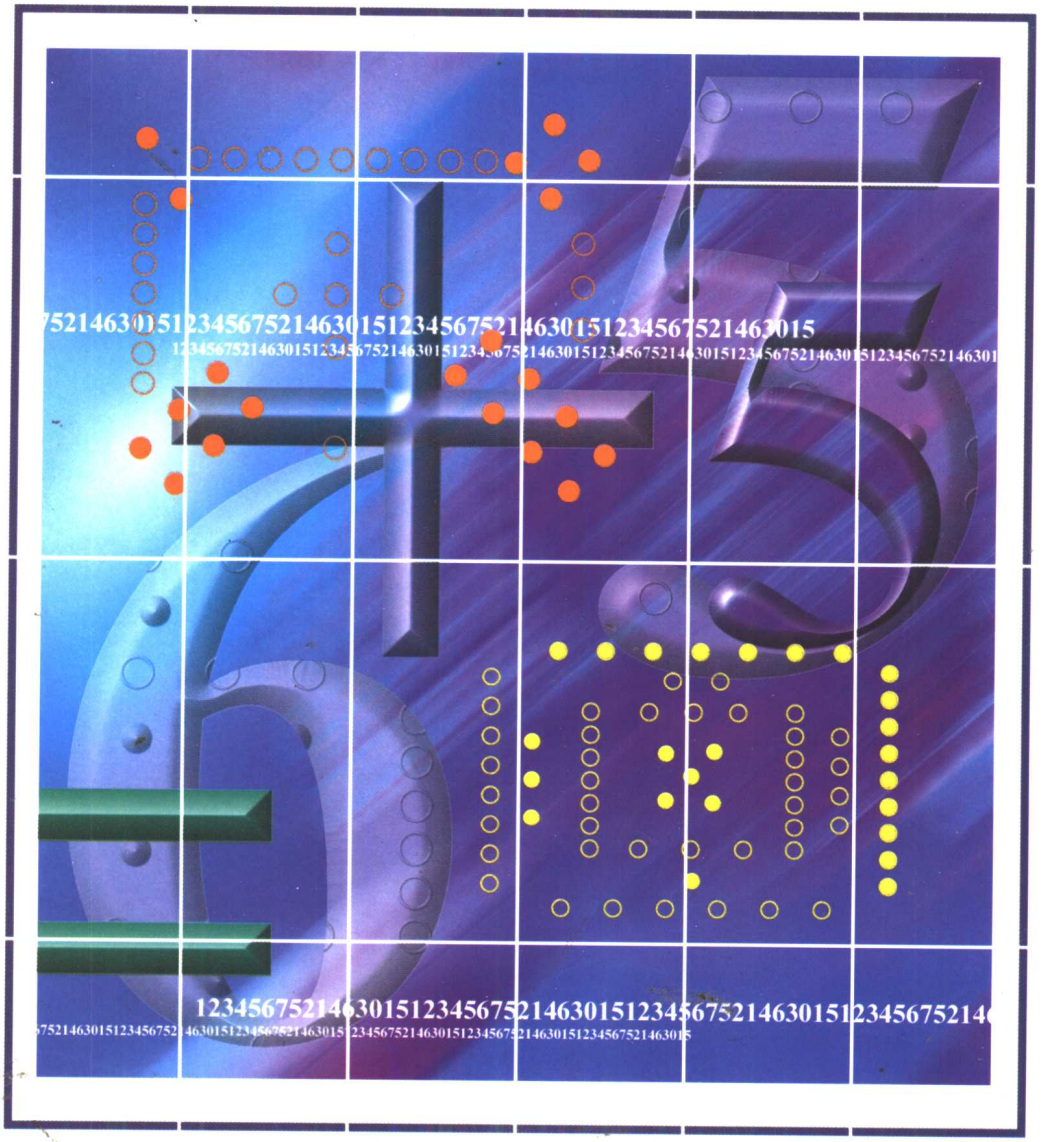
新世纪计算机类本科、研究生系列教材



组合数学

马光思　编著

西安电子科技大学出版社
http://www.xduph.com

新世纪计算机类本科、研究生系列教材

组合数学

马光思　编著

西安电子科技大学出版社

2002

内容简介

随着现代科学技术的发展，组合数学的应用日趋广泛。本书以作者1991年所编《组合数学》讲义为基础，并结合多年来的教学实践经验编撰而成。全书比较完整地阐述了组合数学的基本理论。

全书共8章。第一章介绍数论基础知识，为读者通读全书做一些准备工作；第二章是组合计数方面的经典内容，包括基本计数原理、鸽巢原理、Ramsey定理及排列与组合等；第三章详细讨论了生成函数技术及其应用；第四章反演公式和第五章递归关系是组合数学中深入、关键的技术和方法；第六章通过对群的讨论，引出了著名的Lagrange定理、Burnside定理和Polya定理；第七章概要阐述了组合设计与编码理论基础；第八章主要介绍了组合算法的设计和优化问题的处理方法，并简要介绍了计算模型Turing机、P问题、NP问题与计算复杂性及其相互关系。

全书理论结合实际，部分章节由浅入深，形成归纳；部分章节综合概括，以高起点结论推出若干应用结果。为了巩固概念，每章最后均有适当数量习题。书中文字叙述生动，实例丰富，注意启发性的同时又考虑了提高总结。

本书既可作为研究生教材，又可供高等院校理工科教师、学生、数学工作者和爱好者使用。

新世纪计算机类本科、研究生系列教材

组合数学

马光思　编著

责任编辑　夏大平　龙晖　王素娟
出版发行　西安电子科技大学出版社(西安市太白南路2号)
电　话　(029)8227828　　邮　编　710071
http://www.xduph.com　　E-mail：xdupfxb@pub.xaonline.com
经　销　新华书店
印　刷　西安文化彩印厂
版　次　2002年12月第1版　2002年12月第1次印刷
开　本　787毫米×1092毫米　1/16　印张17.25
字　数　406千字
印　数　1～4 000册
定　价　20.00元
ISBN 7-5606-0648-2/O·0035
XDUP　0918011－1
＊＊＊如有印装问题可调换＊＊＊

前　言

本书根据作者多年讲授研究生和高年级本科生“组合数学”课程的教学笔记整理编撰而成。其中，主要内容取自作者1991年所编《组合数学》讲义。结合多年来在教学工作中积累的素材和现阶段形势发展对“组合数学”课程的新要求，在书中对原讲义的内容作了较大幅度调整，去掉了半群、范畴等章节，增加了递归关系、组合设计及编码、组合算法与计算复杂性等章节，并对原讲义中有些章节的内容作了许多扩充，补充了各章的习题。

为了保持全书独立性，对“离散数学”等先驱课程中的基本概念和术语在各章节中使用之前都有简要说明。书中所用符号和术语力求保持与“离散数学”的习惯用法一致。其中，对最基本的逻辑符号合取“$\wedge$”、析取“$\vee$”、推导(永真蕴涵)“$\Rightarrow$”、等价“$\Leftrightarrow$”及集合运算符交“$\cap$”、并“$\cup$”等常用符号的含义和用法不再进一步解释，直接引用。

计算机科学中包含着大量组合数学的知识。由于教学和应用的需要，组合数学已成为计算机学科及与信息有关学科的基础理论课程。本书涉及组合分析、图论、抽象代数、编码理论、组合算法及算法复杂性等组合数学的几乎全部内容。所选内容基本符合《同等学历人员申请硕士学位计算机科学与技术学科综合水平全国统一考试大纲及指南》中“组合数学”的考试大纲要求。关于部分线性规划问题，一并纳入组合算法统一讨论。

全书共分八章。第一章数论基础是通读全书的预备知识，内容主要取自参考文献[1]。其中，同余式的一般性讨论是新增加部分。第二章基本计数原理，包括加法原理、乘法原理、鸽巢原理，以及排列与组合及其进一步讨论和应用；对集合元素计数的容斥原理及应用，因篇幅和技术处理上的需要，特别安排在第四章反演公式中，作为筛法公式的特殊情况给出。第三章对由Laplace和Euler提出的生成函数方法进行了全面讨论。第四章是反演公式，该章起点较高，逐渐演绎，最后给出了若干具体应用，部分内容请参考文献[3]。第五章系统讨论了递归关系，主要参考文献[6]。第六章除增加了部分例题之外，基本保持原讲义风貌，主要介绍了群及几个与计数有关的定理：Lagrange定理、Burnside定理、Polya定理及其应用。第七章组合设计及编码，简要介绍了相异及公共代表组，对均衡不完全区组的设计、正交拉丁方、Hadmard矩阵也有部分论述；最后给出了有关编码、译码的基本理论。该章内容主要参阅本书参考文献[4]。第八章组合算法与计算模型，主要介绍一些经典的组合算法设计技术及优化问题的解决方法，并特别讨论了计算模型Turing机，P及NP类语言和算法复杂性等计算机科学中核心而重要的课题；该章参考文献为[5]、[6]和[8]。

作者受参考文献[2]的影响最大，虽然在内容取舍、文字组织、符号表达等方面曾努力学习、仿效，但收效甚微。这使得一些论述有前后重复之嫌。从读者的立场看，部分重复未见得就是坏事，它可使人们从不同角度认识、解释同一现象，加深对概念的理解。

本书从准备到交稿历时近三年，中途因种种原因时断时续，经刘家佺教授多次严厉敦促，才得以完稿。刘林教授在百忙中对初稿进行了认真检查和审阅，提出了许多宝贵修改

意见，对作者帮助很大。在此谨向两位老师表示衷心的感谢。

书稿撰写期间，我的学生毛宏燕、顾敏苏、高志玲、王丹、王辉、陈涛、褚长洪等，耐心地承担了大部分辑录任务，在此一并向他们表示感谢。还要感谢我的家人，他们对我的工作给予了有力支持和理解。

西安电子科技大学出版社的总编和编辑同志，对本书的出版工作给予了热情的关怀，严格把关。尤其是出版社夏大平老师关于书稿存在问题的直面批评和严肃指点，使作者深受教益。在此一并致以感谢和敬意。

由于作者水平有限，书中错误在所难免，恳请同行不吝赐教。

作　者

2002 年 6 月

目　录

绪　论

组合数学也称为组合分析或组合学，按研究的对象归于离散数学家族。早在中国古代的洛书、河图中就有组合数学的基本思想。洛书、河图是以不同形状、个数的黑白点排列的图案，并有许多种神秘的解释，译为现代的记法如图 1 的(*a*)与(*b*)所示。其中，前者称为幻方，后者称为幻圆，它们都具有许多组合学性质。以图 1(*a*)所示幻方为例，其每行、每列及每条对角线的元素之和都是 15。数字 15 常称为幻和。

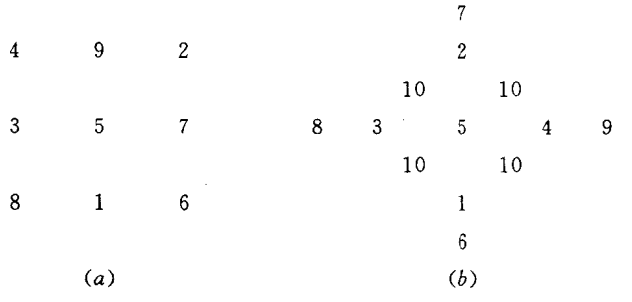


图 1　洛书与河图

推广到 n 阶幻方，即把 1，2，…，n^2 这 n^2 个数字填入 $n\times n$ 的方格图中，幻和为

$$1+2+\cdots+n^2=\frac{n^2(n^2+1)}{2}$$

从而，关于幻方的问题可归结为：

(1) 对任意的正整数 n，n 阶幻方存在吗？

(2) 对某个正整数 n，如果 n 阶幻方存在，有多少不同的形式？

(3) 构造存在的 n 阶幻方。

组合数学研究的核心问题是“把有限个离散对象按一定规则或模式进行安排”，这种安排被考究地称为组态(Configuration)。关于幻方的几个问题也正是组合数学要解决的问题，即组态的存在性问题、组态的计数问题和组态的构造问题。此外，还涉及组态的优化问题。

1. 组态的存在性

组合数学中解决组态存在性的方法很巧妙，其构思过程往往出人意料，让人拍案叫绝。其中，著名的例子就是众所周知的哥尼斯堡七桥问题。1736 年，年轻的大数学家 Euler 将人们在娱乐中提出的一个数学难题抽象为点线构成的图及寻找走边的一笔画问题，并给出了精巧的解答，即七桥问题无解。由此引出了一门新型数学学科——图论。Euler 也被后人誉为图论之父。

例 1　容易证明，不存在 2 阶幻方。但对其余的正整数 n，n 阶幻方都可以构造出来。这就证明了 n(正整数 $n\neq 2$)阶幻方的存在性。

组合数学认为，如果给出了构造组态的有效算法，即可算作证明了组态的存在性。但还需要给出构造算法的有效性证明。

例 2　若用 1×2 格的骨牌铺砌去掉了两个对角处格子的 8×8 残缺棋盘，问能否用 31 枚骨牌恰将其砌满？

解　答案是否定的。证明方法很巧妙，可以先将 8×8 棋盘黑白间隔染色，去掉的两个对角处格子不是同白，就是同黑。因此，8×8 残缺棋盘剩余的 64－2＝62 个格子中黑格数与白格数相差为 2。反之，若设能用 31 枚 1×2 格的骨牌，每枚覆盖相邻的 2 个方格，恰将残缺棋盘砌满，则黑格数与白格数应该相等。这就产生了矛盾。因此，不存在要求的覆盖。如果对不去掉对角处格子的 64 格 8×8 完好棋盘，则存在用 32 枚 1×2 格的骨牌恰将其砌满的许多方法。这时要讨论的就是确定有多少种不同覆盖方法的计数问题。

2. 组态的枚举、分类和计数

如果所要求的组态存在，则可能有不止一种的方案。问题是究竟有多少种可能的不同方案，如何对组态的不同方案进行分类、枚举。

例 3　对正三角形的三个顶点 u，v，w 染以红、蓝两种颜色，求不同的染色方案。

解　事实上，染色方案可自然地分为如下四类：

(1) 三点全染红色，只有 1 种方案：rrr；

(2) 三点全染蓝色，只有 1 种方案：bbb；

(3) 两点染红，一点染蓝，因蓝色可分别染于 u，v，w 三个顶点之一，故有 3 种方案：brr，rbr，rrb；

(4) 由对称性可知，两点染蓝，一点染红的方案也有 3 种方案：rbb，brb，bbr。

从而，总的方案数为 $2^3=8$ 种。

例 3 所述问题也可转化为求集合 $X=\{u, v, w\}$到 $Y=\{r, b\}$的函数的数目，由离散数学知，该数目为：$|Y^X|=|Y|^{|X|}=2^3=8$。

又若设三角形的三个顶点无区别，即将旋转重合的方案视为同一方案，则(3)、(4)两类中的 3 种方案都将归为 1 种。从而共有 4 种不同的方案。

例 4　n 元集上有多少个不同的自反关系，有多少个不同的对称关系？

解　设 $A=\{a_1, a_2, \cdots, a_n\}$，$A$ 上的自反关系 $R\subseteq A\times A$ 及对称关系 $S\subseteq A\times A$ 分别定义为

$$\forall\, x,\ x\in A\to xRx \quad 及 \quad \forall\, x, y\in A,\ xSy\to ySx$$

考察关系矩阵的特征，若 R 为自反关系，则其关系阵 $\boldsymbol{M}_R=(m_{ij})$的主对角元全为 1，其余上三角、下三角部分的 $n^2-n=n(n-1)$个元素或为 0 或为 1。若 S 为对称关系，则其关系矩阵 $\boldsymbol{M}_S=\boldsymbol{M}_S^{\mathrm{T}}$。

从而，不难求得 A 上不同的自反关系的数目为

$$C_{n(n-1)}^0+C_{n(n-1)}^1+\cdots+C_{n(n-1)}^{n(n-1)}=2^{n(n-1)}$$

类似地进行分析可知，A 上不同的对称关系的数目为

$$2^n\cdot\left(C_{n(n-1)/2}^0+C_{n(n-1)/2}^1+\cdots+C_{n(n-1)/2}^{n(n-1)/2}\right)=2^{n(n-1)/2}\cdot 2^n=2^{n(n+1)/2}$$

对 $n=5$，5 元集上自反关系的数目为 $2^{5\times(5-1)}=2^{20}=1024^2$；5 元集上对称关系的数目为 $2^{5\times(5+1)/2}=2^{15}=32\times 1024$。

3. 组态的构造

例 5　例 1 中已指出，可对不等于 2 的正整数 n 构造 n 阶幻方，构造 n 阶幻方的方法很多，如下仅给出 de la loubère 构造奇数阶幻方的算法：

№1　首先将 1 置于第一行中间的位置上；

№2　若 i 已填入适当位置，则对 $i+1$ 执行如下特殊条款：

№2.1　若 i 在第一行，则将 $i+1$ 填入 i 右边一列的最底行位置；

№2.2　若 i 在最后一列，则将 $i+1$ 填入 i 的上一行的第一列；

№2.3　若 i 在第一行最后一列或 $i+1$ 该填的位置已被填入值，则将 $i+1$ 填入 i 所在位置的下方；

№3　若 i 不在№2 中特殊条款之列，则将 $i+1$ 填入 i 紧右边一列的上一行。

例 6　正交拉丁方源于 Euler 提出的“36 军官问题”。设有 6 个不同军衔和来自 6 个不同团队的 36 名军官，问能否将他们排成 6×6 方阵，使得每行每列恰有不同军衔的军官各一名，且每个团队的军官各一名？

解　以 9 名军官为例，设 $i=1, 2, 3$ 表示军官的军衔，$j=1, 2, 3$ 表示军官的团队，则每个军官对应一个序偶(i, j)。从而可以排出：

$$\begin{bmatrix}(1,1) & (2,2) & (3,3)\\ (3,2) & (1,3) & (2,1)\\ (2,3) & (3,1) & (1,2)\end{bmatrix}\Rightarrow\begin{bmatrix}1 & 2 & 3\\ 3 & 1 & 2\\ 2 & 3 & 1\end{bmatrix}\begin{bmatrix}1 & 2 & 3\\ 2 & 3 & 1\\ 3 & 1 & 2\end{bmatrix}$$

左端方阵即为所求 9 名军官的一个解。又显见若将左端方阵的第一个分量与第二个分量拆开存放，则可得右端两个方阵。其中，前者表示 9 名军官的军衔，后者表示 9 名军官的团队。

对于 $n\times n$ 矩阵 $\boldsymbol{A}$，若其每行每列均为$\{1, 2, \cdots, n\}$中的一个不同的数，则称 $\boldsymbol{A}$ 为拉丁方。可证对 $\forall\, n\in\mathbf{Z}_+$，$n$ 阶拉丁方恒存在，如上面给出的右端的 2 个方阵。

设 $\boldsymbol{A}=(a_{ij})_{n\times n}$，$\boldsymbol{B}=(b_{ij})_{n\times n}$为两个拉丁方。若 n 阶序偶$(a_{ij}, b_{ij})(1\leqslant i, j\leqslant n)$均不相同，则称 $\boldsymbol{A}$ 与 $\boldsymbol{B}$ 互为正交的拉丁方。

$n=2$ 时，不存在 2 阶正交拉丁方，因为 2 阶拉丁方共有 2 个，即

$$\begin{bmatrix}1 & 2\\ 2 & 1\end{bmatrix},\quad\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}$$

但二者彼此不正交。

已经证明，也不存在 6 阶正交拉丁方。

设 p 为奇素数，α 为正整数，如下仅以 $n=p^{\alpha}$ 构造正交拉丁方组。

设 $A=\{0, 1, 2, \cdots, n-1\}$，就用这 n 个元素构造正交拉丁方。令

$$\boldsymbol{A}_k=(a_{ij}^{(k)})_{n\times n},\ a_{ij}^{(k)}\equiv k\cdot i+j(\mathrm{mod}\ n),\ 1\leqslant k\leqslant n-1,\ 0\leqslant i, j\leqslant n-1$$

则当 $n=p^{\alpha}$ 时，$\boldsymbol{A}_1, \boldsymbol{A}_2, \cdots, \boldsymbol{A}_{n-1}$为正交拉丁方组。

对 $n=5$，$A=\{0, 1, 2, 3, 4\}$，利用公式

$$a_{ij}^{(k)}\equiv k\cdot i+j(\mathrm{mod}\ 5),\ 1\leqslant k\leqslant 4,\ 0\leqslant i, j\leqslant 4$$

可算得 4 个两两正交的拉丁方组如下：

$$\boldsymbol{A}_1=\begin{bmatrix}0&1&2&3&4\\1&2&3&4&0\\2&3&4&0&1\\3&4&0&1&2\\4&0&1&2&3\end{bmatrix},\quad \boldsymbol{A}_2=\begin{bmatrix}0&1&2&3&4\\2&3&4&0&1\\4&0&1&2&3\\1&2&3&4&0\\3&4&0&1&2\end{bmatrix}$$

$$\boldsymbol{A}_3=\begin{bmatrix}0&1&2&3&4\\3&4&0&1&2\\4&0&1&2&3\\2&3&4&0&1\\1&2&3&4&0\end{bmatrix},\quad \boldsymbol{A}_4=\begin{bmatrix}0&1&2&3&4\\4&0&1&2&3\\3&4&0&1&2\\2&3&4&0&1\\1&2&3&4&0\end{bmatrix}$$

4. 组态的优化

优化问题是在一定的条件下找出一个(或几个)最优或较优的安排方案。有些组合问题求精确解是很困难的，所求结果有时只能给出一种接近的解。

例 7　把一个 3×3×3 的立方体木块切割成 27 个 1×1×1 的小立方块。如果切割过程中允许重新排列已切割木块的位置，求完成整个切割的最少次数。

解　这里的最优即指具有最少切割次数的方案，采用穷举方案并比较切割次数的方法一般不可取。本例的解法是先指出 6 次即可完成全部切割，即水平切 2 次，竖直、交叉各切 2 次。其次，可以证明少于 6 次不能完成题目要求的切割。事实上，对中心位置产生的小立方体而言，因其也具有 6 个面，且每个面都须被独立地切割一次才能出现。故至少需要 6 次才能切割完。

例 8　设产地 A_1，A_2，…，A_m 生产某种产品的产量分别为 a_1，a_2，…，a_m，销地 B_1，B_2，…，B_n 对该产品的需求量分别为 b_1，b_2，…，b_n。假设从产地 A_i 销到销地 B_j 的单位运费为 c_{ij}，产和销保持平衡，即

$$\sum_{i=1}^{m}a_i=\sum_{j=1}^{n}b_j$$

求合理安排该种产品的运输方案，使其总费用最少。

解　设从 A_i 到 B_j 的运量为 x_{ij}，则问题即为求解目标函数

$$\min Z=\sum_{i=1}^{m}\sum_{j=1}^{n}c_{ij}\cdot x_{ij}$$

且满足约束条件

(1) $\sum\limits_{j=1}^{n}x_{ij}\leqslant a_i$，$\sum\limits_{i=1}^{m}x_{ij}\leqslant b_j$，$x_{ij}\geqslant 0(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n)$；

(2) $\sum\limits_{i=1}^{m}\sum\limits_{j=1}^{n}x_{ij}=\sum\limits_{i=1}^{m}a_i=\sum\limits_{j=1}^{n}b_j$。

组态的存在性、分类计数及构造，一般都不是互相独立的，它们常集中在同一组合问题中。一般而言，若一组合问题的存在性需要大量研究时，则其计数问题的难度将难以想象。但若一组合问题已有一特定的解，则还是有机会计算其解的个数或对其进行分类。

原书缺页

(3) $b|0$;

(4) 若 $b|a \wedge c|b$，则 $c|a$;

(5) 若 $b|a$，则 $bc|ac$;

(6) 若 $c|d$，$c|e$，则对任意的 m，$n\in\mathbf{Z}$ 有 $c|(dm+en)$;

(7) 若 $bc|ac$，则 $b|a$。

证明 只证(6)式。

事实上

$$c|d \wedge c|e \Rightarrow \exists\, q_1, q_2 \in \mathbf{Z},\ d = cq_1,\ e = cq_2 \Rightarrow \forall\, m, n \in \mathbf{Z}$$

$$dm + en = cq_1m + cq_2n = c(q_1m + q_2n) = cq(q = q_1m + q_2n)$$

$$\Rightarrow c|(dm + en)$$

1.2 最大公约数(greatest common divisor)

定义 1 对任意正整数 m，若 $m|a \wedge m|b$，则称 m 为 a 和 b 的公约数。公约数中最大者，称为 a 与 b 的最大公约数。常记做

$$(a, b)$$

定义 2 若 $(a, b)=1$，称 a 与 b 互素。

例如：8 与 13 互素；13 与 21 互素；12 与 25 互素。

命题 1 如果 $a=bq+c$，则有 $(a, b)=(b, c)$。

证明 证明思路是：凡是 a、b 的约数，都是 b、c 的约数；凡是 b、c 的约数，都是 a、b 的约数。

对任意的 x 有

$$x|a \wedge x|b \Rightarrow a = xt_1 \wedge b = xt_2 \Rightarrow c = xt_1 - xt_2q = x(t_1 - t_2q) \Rightarrow x|c$$

即有

$$x|b \wedge x|c$$

反之

$$x|b \wedge x|c \Rightarrow x|a \wedge x|b$$

由 x 的任意性可知，a、b 的约数集合与 b、c 的约数集合相同，其中最大的约数应相同，故有

$$(a, b) = (b, c)$$

· 求最大公约数的 Euclid 算法

按照本节命题 1 有

$$\left.\begin{array}{ll} a = bq_1 + r_1, & 0 < r_1 < b \\ b = r_1q_2 + r_2, & 0 < r_2 < r_1 \\ \vdots & \vdots \\ r_{k-2} = r_{k-1}q_k + r_k, & 0 < r_k < r_{k-1} \\ \vdots & \vdots \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} = r_nq_{n+1}, & r_{n+1} = 0 \end{array}\right\} \tag{1.2.1}$$

因 $b>r_1>r_2>\cdots$ 是一递减的正整数列，包含至多 b 个正整数，上述等式组在有限步后必可做到 $r_{n+1}=0$。

由本节命题 1 还有

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = r_n$$

推论 1 数 a 和数 b 的公约数集合与它们的最大公约数的约数集合相同。

推论 2 这个最大公约数等于 $r_n(n\in\mathbf{Z}_+)$，即等于上述等式组中最后的不等于零的余数。

推论 3 若 $b|a$，则 $(a, b)=b$。

观察等式组(1.2.1)的构造过程不难发现：当某个余数 $r_k(k\in\mathbf{Z}_+)$不为 0 时，即将除数作为被除数，并将余数作为除数再写出一个等式，依此类推，直至余数是零为止。故可将 Euclid 算法改写如下：

· 改进的 Euclid 算法

№1 输入正整数 A，B；

№2 $M\Leftarrow A$；$N\Leftarrow B$；(保护原始数据)

№3 $K\Leftarrow M-[M/N]*N$；

№4 若 $K>0$，则 $M\Leftarrow N$，$N\Leftarrow K$，转№3；

№5 $GCD\Leftarrow N$(N 为最大公约数)；输出 A，B，GCD；

№6 结束。

命题 2 设 m 表示任意正整数，则有 $(am, bm)=(a, b)m$。

证明 对等式组(1.2.1)逐项地乘以 m，可得一新的等式组，在其中代替 $a,b,r_1,\cdots r_n$ 的是 am，bm，$\cdots$，r_nm，因此 $(am, bm)=r_nm=(a, b)m$。

命题 3 设 δ 表示数 a 和 b 的任意公约数，则有 $(a/\delta, b/\delta)=(a, b)/\delta$。特别地，当 $\delta=(a, b)$时有 $(a/(a, b), b/(a, b))=1$(即 a，b 分别被它们的最大公约数除后所得的两个商数互素)。

证明 借用命题 2 有

$$(a, b) = \left(\frac{a\delta}{\delta}, \frac{b\delta}{\delta}\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta \Rightarrow \left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{\delta}$$

命题 4 如果 $(a, b)=1$，则 $(ac, b)=(c, b)$。

证明 只需证 $(ac, b)|(c, b) \wedge (c, b)|(ac, b)$。

事实上，

$$(ac, b)|ac \wedge (ac, b)|b \Rightarrow (ac, b)|ac \wedge (ac, b)|bc$$

依推论 1 有

$$(ac, b)|(ac, bc) \Rightarrow (ac, b)|(a, b)c \Rightarrow (ac, b)|c \Rightarrow (ac, b)|b \wedge (ac, b)|c \Rightarrow (ac, b)|(b, c)$$

反之

$$(c, b)|ac \wedge (c, b)|b \Rightarrow (c, b)|(ac, b)$$

因而

$$(ac, b) = (c, b)$$

命题 5 若 $(a, b)=1 \wedge b|ac$，则 $b|c$。

证明 由于 $(a, b)=1 \Rightarrow (ac, b)=(c, b)$

又

$$b|ac \Rightarrow b|ac \wedge b|b \Rightarrow b|(ac, b) \Rightarrow b|(c, b) \Rightarrow b|c$$

命题 6　如果$(a_i, b_j)=1(i=1, 2, \cdots, m; j=1, 2, \cdots, n)$，则$\left(\prod_{i=1}^{m} a_i, \prod_{j=1}^{n} b_j\right)=1$

证明　利用命题 4 有

$$\left(\prod_{i=1}^{m} a_i, b_k\right)=\left(a_1\prod_{i=2}^{m} a_i, b_k\right)=\left(\prod_{i=2}^{m} a_i, b_k\right)=\left(a_2\prod_{i=3}^{m} a_i, b_k\right)$$

$$=\left(\prod_{i=3}^{m} a_i, b_k\right)=\cdots=(a_m, b_k)=1$$

同理可得

$$\left(\prod_{j=1}^{n} b_j, \prod_{i=1}^{m} a_i\right)=\left(\prod_{j=2}^{n} b_j, \prod_{i=1}^{m} a_i\right)=\cdots=\left(b_n, \prod_{i=1}^{m} a_i\right)=1$$

命题 7　求两个以上的数的最大公约数的问题，可以化成求两个数的最大公约数的问题。亦即，为了求数 $a_1, a_2, \cdots, a_n$ 的最大公约数，可写出如下的一串数：

$$(a_1, a_2)=d_2, (d_2, a_3)=d_3, (d_3, a_4)=d_4, \cdots, (d_{n-1}, a_n)=d_n$$

d_n 即为所有已知 n 个数的最大公约数。

证明　根据推论 1，数 a_1, a_2 的公约数集合与 d_2 的约数集合相同，所以数 a_1, a_2, a_3 公约数集合与数 d_2 和 a_3 的公约数集合相同，即与 d_3 的约数集合相同。然后肯定，数 a_1, a_2, a_3, a_4 的全体公约数所成之集与 d_4 约数集相同，…… 最后，数 $a_1, a_2, \cdots, a_n$ 的公约数所成之集与 d_n 约数之集相同。因而 d_n 的最大公约数是 d_n 自身，所以它就是数 $a_1, a_2, \cdots, a_n$ 的最大公约数。

观察以上证明，可以肯定推论 1 对两个以上的数也成立。命题 2 和命题 3 对两个以上的数也是成立的，这是因为用 m 去乘或者用 δ 去除所有的数 $a_1, a_2, \cdots, a_n$，正像所有 $d_2, d_3, \cdots, d_n$ 都被 m 乘或被 δ 除一样。

命题 8　对 a, b 的最大公约数 d，存在着二整数 s, t，使得 d 可表示为

$$d=sa+tb \tag{1.2.2}$$

证明　若有 $b|a$ 或 $a|b$，不妨设为前者，则 $d=b=0\cdot a+1\cdot b$，此即(1.2.2)式中各项的形式，下设 $a\nmid b \wedge b\nmid a$，辗转相除可有等式组(1.2.1)中各式。由等式组(1.2.1)的第一式得

$$\begin{bmatrix} a \\ b \end{bmatrix}=\begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} b \\ r_1 \end{bmatrix}$$

又由等式组(1.2.1)的第二式得

$$\begin{bmatrix} b \\ r_1 \end{bmatrix}=\begin{bmatrix} q_2 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_1 \\ r_2 \end{bmatrix}$$

依此类推，有

$$\begin{bmatrix} a \\ b \end{bmatrix}=\begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix}\cdots\begin{bmatrix} q_k & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix}$$

令

$$\begin{bmatrix} T_k & V_k \\ S_k & U_k \end{bmatrix}=\begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix}\cdots\begin{bmatrix} q_k & 1 \\ 1 & 0 \end{bmatrix} \tag{1.2.3}$$

则

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} T_k & V_k \\ S_k & U_k \end{bmatrix} \begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix} \tag{1.2.4}$$

注意到 $$\begin{vmatrix} q_1 & 1 \\ 1 & 0 \end{vmatrix} = \cdots = \begin{vmatrix} q_k & 1 \\ 1 & 0 \end{vmatrix} = -1$$

故 $$\begin{vmatrix} T_k & V_k \\ S_k & U_k \end{vmatrix} = (-1)^k$$

由(1.2.4)式不难得到

$$\begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix} = \begin{bmatrix} T_k & V_k \\ S_k & U_k \end{bmatrix}^{-1} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} (-1)^k U_k & (-1)^{k-1} V_k \\ (-1)^{k-1} S_k & (-1)^k T_k \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix}$$

特别地

$$r_k = (-1)^{k-1} S_k a + (-1)^k T_k b$$

取 $k=n$，则因 r_n 即 a，b 的最大公约数 d 而得

$$d = (-1)^{n-1} S_n a + (-1)^n T_n b$$

这又是(1.2.2)式的形式。

下面给出求 S_k，T_k 的递推公式：

令

$$\begin{bmatrix} T_k & V_k \\ S_k & U_k \end{bmatrix} = \begin{bmatrix} T_{k-1} & V_{k-1} \\ S_{k-1} & U_{k-1} \end{bmatrix} \begin{bmatrix} q_k & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} T_{k-1} q_k + V_{k-1} & T_{k-1} \\ S_{k-1} q_k + U_{k-1} & S_{k-1} \end{bmatrix}$$

比较前后两矩阵知

$$U_k = S_{k-1},\ V_k = T_{k-1} \Rightarrow U_{k-1} = S_{k-2},\ V_{k-1} = T_{k-2} \tag{1.2.5}$$

$$S_k = S_{k-1} q_k + U_{k-1},\ T_k = T_{k-1} q_k + V_{k-1} \tag{1.2.6}$$

由(1.2.5)式及(1.2.6)式有

$$S_k = S_{k-1} q_k + S_{k-2},\ T_k = T_{k-1} q_k + T_{k-2} \tag{1.2.7}$$

在(1.2.3)式中取 $k=1$ 有

$$\begin{bmatrix} T_1 & V_1 \\ S_1 & U_1 \end{bmatrix} = \begin{bmatrix} q_1 & 1 \\ 1 & 0 \end{bmatrix}$$

由此及(1.2.5)式可求得

$$T_0 = V_1 = 1,\ S_0 = U_1 = 0;\ T_1 = q_1,\ S_1 = 1 \tag{1.2.8}$$

用(1.2.8)式作为初值，用(1.2.7)式作为递推公式即可求得 S_k，T_k($k \geqslant 2$)。

· 求二数 A，B 的最大公约数及其表示式的算法

№1 输入 A，B；

№2 $M \Leftarrow A$；$N \Leftarrow B$；

$T_0 \Leftarrow 1$；$S_0 \Leftarrow 0$；

№3 若 $M=N$ 则

打印"$(A, B)=M=S_0 * M+T_0 * N$"；

或"$(A, B)=N=T_0 * M+S_0 * N$"；