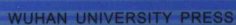
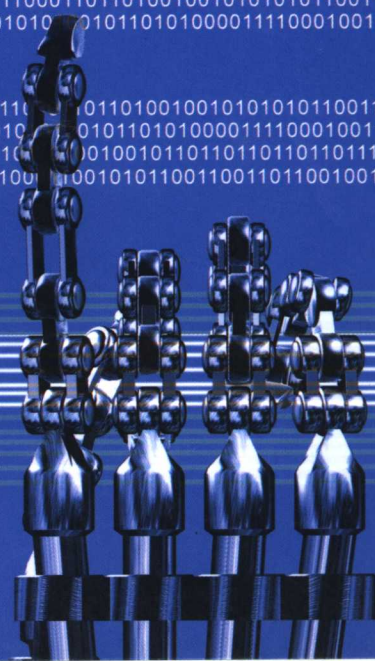




工 编 对 3 15 表 品 郑 巧 梅

00	10	010	100	100	101	001
☐	☐	☐	☐	☐	☐	☐
	☐		☐	☐	☐	



武汉大学出版社

计算机科学与技术系列教材

离散数学

主 编 刘学书 袁 磊 郑巧仙

武汉大学出版社

图书在版编目(CIP)数据

离散数学/刘学书,袁磊,郑巧仙主编. —武汉:武汉大学出版社,
2006.3

(计算机科学与技术系列教材)

ISBN 7-307-04930-9

I. 离… II. ①刘… ②袁… ③郑… III. 离散数学—高等学校—
教材 IV. O158

中国版本图书馆 CIP 数据核字(2006)第 003528 号

责任编辑:李汉保

责任校对:王建

版式设计:支笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.com.cn)

印刷:湖北省孝感日报社印刷厂

开本:787×980 1/16 印张:21.625 字数:442千字 插图:1

版次:2006年3月第1版 2006年3月第1次印刷

ISBN 7-307-04930-9/O·335 定价:29.00元

版权所有,不得翻印;凡购我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售
部门联系调换。

计算机科学与技术系列教材

编 委 会

主 任:何炎祥,武汉大学计算机学院院长,教授

副 主 任:康立山,中国地质大学(武汉)计算机学院院长,教授

陆际光,中南民族大学计算机科学学院院长,教授

编 委:(以姓氏笔画为序)

王江晴,中南民族大学计算机科学学院副院长,教授

王春枝,湖北工业大学计算机学院副院长,教授

牛冀平,黄冈师范学院计算机系主任,副教授

石曙东,湖北师范学院计算机科学与技术系主任,教授

朱 英,桂林电子工业学院计算机系副教授

孙扬波,湖北中医学院信息技术系信息管理与信息系统教研室
主任

刘腾红,中南财经政法大学信息学院副院长,教授

陈少平,中南民族大学电信学院副院长,教授

杜友福,长江大学计算机科学学院院长,教授

陆 迟,江汉大学数学与计算机科学学院计算机系主任,副教授

闵华松,武汉科技大学计算机科学与技术学院副院长,副教授

陈佛敏,咸宁学院信息工程学院计算机系主任,副教授

陈建新,孝感学院计算机科学系主任,副教授

李禹生,武汉工业学院计算机与信息工程系副主任,教授

李晓林,武汉工程大学计算机科学与工程学院副院长,副教授

张涣国,武汉大学计算机学院教授

余敦辉,湖北大学数学与计算机科学学院计算机系副主任
肖 微,湖北警官学院信息技术系副教授
钟 璐,武汉理工大学计算机科学与技术学院院长,教授
钟阿林,三峡大学电气信息学院计算机系主任
姜洪溪,襄樊学院电气信息工程系副主任,副教授
桂 超,湖北经济学院计算机与电子科学系副主任,副教授
黄求根,武汉科技学院计算机科学学院院长,教授
阎 菲,湖北汽车工业学院计算中心主任,副教授
韩元杰,桂林电子工业学院计算机系教授
谢坤武,湖北民族学院信息工程学院计算机系主任,副教授
戴光明,中国地质大学(武汉)计算机学院副院长,教授
魏中海,华中农业大学理学院计算机系副教授

执行编委:黄金文,武汉大学出版社副编审



内 容 简 介

本书是作者经过多年教学实践,并参考多种同类教材而编写的.全书共分十二章,分别介绍初等数论基础知识、数理逻辑、集合、关系、函数、代数系统及图论知识.内容广泛,讲解翔实,深入浅出,注重联系实际应用.贯穿从离散个体到共性特征、从个体关系到函数对应,从元素与运算构成系统到布尔代数以及从模型到直观图论的思维扩展结构.每章后配有一定量的习题,供读者加深理解有关知识,并提高分析和解决实际问题的能力.

本书可以作为计算机专业本科生的教材,也可以供自动控制、信息科学、管理学科等专业的教学用书.



前言

离散数学是以数学的方法研究离散体的结构特征、相互关系以及相互运算规律的学科。而计算机研究的对象正是离散信号和数据,计算机的硬件结构也正是由具有两态的元器件组成。所以离散数学是计算机科学与技术的核心基础理论课,是培养学生抽象思维和逻辑推演能力、掌握处理离散结构所必须的工具和方法。

离散数学是随着计算机科学的发展而逐步建立的,该学科形成于 20 世纪 70 年代,是一门新兴的工具性学科。计算机科学中的数据结构、操作系统、编译原理、逻辑设计、系统结构、容错诊断等,都与离散数学的理论密切相关。

本书是作者经过多年教学实践,并参考多种同类教材编写而成的。全书共分为十二章,包括初等数论知识、命题逻辑、谓词逻辑、集合论、关系、函数、代数系统、群论、环和域、布尔代数及图论。

本书编写过程中注重内容的结构联系,以研究自然科学的抽象,分类,推理,扩展,深入,细化的方法,讨论离散数学中各部分理论的联系及应用。

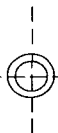
本书适合于计算机科学与技术专业、信息科学专业本科生 90 ~ 100 学时的教学任务,也可以适当删减部分内容作为计算机及应用专业、自动控制专业和管理学等专业本科生 70 ~ 80 学时的教学用书,作为学习离散数学的补充,同时编写有对应的习题解答。

全书由刘学书和袁磊拟定编写大纲,郑巧仙编写第二、三章;袁磊编写第七、八、九章;剩余章节由刘学书编写并对全书做统编和审核。本书在编写及出版过程中,得到襄樊学院电气信息工程系领导和程虹老师及同事们的大力支持和帮助,在此表示衷心感谢!

由于作者水平有限,难免有错误与不足,请读者批评指正。

作 者

2005 年 11 月



目 录

第一章 初等数论知识	1
§ 1.1 整数的整除性	1
§ 1.2 素数及其性质	5
* § 1.3 特殊性质的整数关系	7
1.3.1 毕氏数	7
1.3.2 形数	7
1.3.3 幻方	9
1.3.4 完全数	11
1.3.5 亲和数	12
1.3.6 水仙花数	13
1.3.7 同构数	14
* § 1.4 同余式	14
§ 1.5 初等数论的一些应用举例	16
第二章 命题逻辑	19
§ 2.1 抽象与定义	19
§ 2.2 命题及表示法	20
2.2.1 命题定义	20
2.2.2 命题的表示	22
2.2.3 命题的值	22
2.2.4 命题的类型	22
2.2.5 命题常数	22
2.2.6 命题变元	23
2.2.7 命题指派	23
§ 2.3 命题连接词	23
2.3.1 否定词(非运算)符号 $\neg$ 或 $\bar{}$	23
2.3.2 合取词(与运算)符号 $\wedge$ 或 $\cdot$	24
2.3.3 析取词(或运算)符号 $\vee$ 或 $+$	25
2.3.4 蕴含(条件)连接词(条件运算)符号 $\rightarrow$	25



2.3.5 等价连接词(等价运算)符号 $\leftrightarrow$	26
2.3.6 不可兼或连接词(又称异或,半加连接词)符号 $\overline{\vee}$	28
2.3.7 蕴含否定连接词 符号 $\xrightarrow{C}$	29
2.3.8 与非连接词 符号 $\uparrow$	29
2.3.9 或非连接词 符号 $\downarrow$	29
2.3.10 连接词完备集	31
§ 2.4 命题公式的真假性及等价公式	31
§ 2.5 重言式与蕴含式	33
* § 2.6 范式	37
§ 2.7 命题逻辑推理演算	43
2.7.1 真值表法	45
2.7.2 直接证法	46
2.7.3 间接证法	48
§ 2.8 命题逻辑的应用	50
第三章 谓词逻辑	58
§ 3.1 引言	58
§ 3.2 基本概念	59
§ 3.3 谓词公式与翻译	61
§ 3.4 变元的约束与谓词公式的真假性	63
§ 3.5 谓词等价式与蕴含式	65
§ 3.6 谓词演算的推理理论	69
第四章 集合	77
§ 4.1 集合的基本概念	77
§ 4.2 集合的运算	82
4.2.1 集合的交运算	83
4.2.2 集合的并运算	83
4.2.3 集合的补(差)运算	85
4.2.4 集合的对称差(环和)运算	88
4.2.5 集合的环积(对称差的补)运算	89
§ 4.3 集合的分划与覆盖	90
* § 4.4 多重集合	92
* § 4.5 集合的递归定义	93
§ 4.6 有限集合的元素个数与包含排斥原理	95



第五章 关系	100
§ 5.1 关系的基本概念	100
§ 5.2 关系及其表示法	103
§ 5.3 关系的性质	105
§ 5.4 关系的运算	108
5.4.1 关系的交、并、相对补运算	108
5.4.2 关系的逆运算	110
5.4.3 关系的复合运算	111
5.4.4 关系的闭包运算	113
§ 5.5 等价关系	117
5.5.1 等价关系的基本概念	117
5.5.2 等价类	119
§ 5.6 偏序关系	122
第六章 函数	131
§ 6.1 函数的概念	131
§ 6.2 几种特殊函数	134
§ 6.3 复合函数与逆函数	136
* § 6.4 归纳定义的函数——递归函数	141
§ 6.5 集合的基数	142
第七章 代数系统	151
§ 7.1 运算	151
7.1.1 运算的性质	151
7.1.2 代数系统中的特殊元素	154
§ 7.2 代数系统	157
§ 7.3 同态和同构	160
§ 7.4 同余关系	165
* § 7.5 积代数与商代数	167
第八章 群论	173
§ 8.1 半群与独异点	173
§ 8.2 群及其性质	175
§ 8.3 交换群、循环群、置换群	177
8.3.1 交换群(阿贝尔群)	177



8.3.2	循环群	179
8.3.3	置换群	181
* § 8.4	子群、陪集与拉格朗日定理	186
§ 8.5	群的同态与同构	190
* 第九章	环与域	196
§ 9.1	环的定义及其性质	196
§ 9.2	环的同态与同构	201
§ 9.3	域及其性质	203
第十章	格与布尔代数	209
§ 10.1	格的概念	209
§ 10.2	格的主要性质	214
§ 10.3	格的同态与同构	216
§ 10.4	特殊格	221
§ 10.5	布尔代数、布尔函数和布尔表达式	229
10.5.1	QUINE 法(崩因法即代数法化简)	234
10.5.2	几何化简法	236
第十一章	图论	245
§ 11.1	图的基本概念	245
§ 11.2	图的矩阵表示	254
§ 11.3	生成树、最短路径、关键路径	258
11.3.1	图的周游和生成树	258
11.3.2	最短路径、关键路径	264
§ 11.4	特殊图	269
11.4.1	欧拉图	269
11.4.2	哈密顿(Hamilton)图	274
11.4.3	平面图	280
11.4.4	二部图	285
§ 11.5	树	288
11.5.1	树的概念及性质	289
11.5.2	有向树	290
11.5.3	二叉树	294
11.5.4	决策树	299
11.5.5	树的同构	302

第十二章 离散数学在计算机科学中的应用	309
§ 12.1 时序线路和有限状态机	309
§ 12.2 串和语言	311
§ 12.3 形式文法	314
§ 12.4 有限状态自动机	318
§ 12.5 Turing 机	326
参考文献	332



第一章 初等数论知识

初等数论是研究整数的性质和方程(组)整数解的一门数学学科. 该学科在计算机科学、通讯工程、离散控制系统、代数编码等领域得到日益广泛的实际应用;同时, 在程序设计中也经常遇到诸如求素数、因式分解、求最大公约数、最小公倍数、求方程组的整数解等数论基础知识. 特别是将离散体抽象为整数元素, 从研究整数各种性质、规律、应用及研究方法, 推广到离散体进行理论研究, 更具有实际意义.

众所周知, 任何客观事物都具有质、形、量三种属性, 而量的表现方式有连续量和离散量. 在离散量的表现方式中, 人们首先熟悉的是 $1, 2, 3, \dots$ 这些正整数. 整数概念是人们熟知和公认的. 人们认识和描述客观事物的最基本属性时, 无需去定义, 而只是去承认.

人们熟悉整数之后, 随即熟悉整数之间进行加、减、乘运算所得的结果仍是整数. 但是, 用一个不等于零的整数去除另一个整数所得的商不一定是整数, 由此产生了初等数论中的第一个概念——数的整除性.

§ 1.1 整数的整除性

定义 1-1 任给两个整数 m, n , 其中 $n \neq 0$, 如果存在一个整数 k , 使得等式 $m = n \cdot k$ 成立, 则称 n 整除 m , 或称 m 被 n 整除, 记为 $m // n$, 并称 n 是 m 的一个因子, m 是 n 的倍数.

整除概念具有什么性质, 如何证明这些性质, 这就需进一步地研究.

定理 1-2 整除关系具有以下性质:

以 I 表示全体整数集合, 设 $m, n, k, x, y \in I$, 且 $m, n, k \neq 0$, 则

1. 对任何 $m \neq 0$, 有 $m // m$;
2. 若 $m // n$ 且 $n // m$, 则 $m = \pm n$;
3. 若 $m // n$ 且 $k // m$, 则 $k // n$;
4. 若 $m // n$, 则 $(m \cdot k) // n$;
5. 若 $m // n$ 且 $k // n$, 则 $(m \cdot x + k \cdot y) // n$;
6. 若 $m, n > 0$, 且 $m // n$, 则 $n \leq m$.

定义是将具体事物用数学形式加以描述而形成的概念, 不需要证明. 而定理则是要证明的, 最常用的方法之一是根据给定的条件用定义去判定.



证明 1 已知 $m \neq 0$, 存在正整数 1, 使得 $m = m \cdot 1$, 所以 $m \parallel m$. ■

证明 2 已知 $m \parallel n$, 则存在整数 x , 使得 $m = n \cdot x$, 又已知 $n \parallel m$, 则存在整数 y , 使得 $n = m \cdot y$, 两式相乘则成立 $m \cdot n = m \cdot n \cdot x \cdot y$, 所以 $x \cdot y = 1$ 即 $x = y = 1$ 或 $x = y = -1$, 于是 $m = -n$ 或 $m = n$ 所以 $m = \pm n$. ■

证明 3 已知 $m \parallel n$, 且 $k \parallel m$, 则存在整数 x, y , 使得 $m = n \cdot x, k = m \cdot y$, 故 $k = m \cdot y = n \cdot x \cdot y$ 即有 $x \cdot y$ 是整数, 满足 $k = n \cdot (x \cdot y)$, 所以 $k \parallel m$. ■

对 4~6 读者可以采用上述方法自行证明.

明确整数整除的性质之后, 还应研究整除关系的有关推理结论, 从而加深了解整数与整数之间的各类特殊关系.

定理 1-3 设 m, n 是两个整数, 其中 $n > 0$, 则存在两个惟一的整数 q 和 r , 使得 $m = n \cdot q + r$ 成立, 其中 $0 \leq r < n$ (r 称为 m 除以 n 的余数).

证明 首先证明存在满足上述条件的两个整数 q, r . 为此, 对给定的整数 m, n 作整数序列

$$\{k \cdot n\}, \quad k = 0, \pm 1, \pm 2, \pm 3, \dots$$

则 m 必在此序列的某两项之间, 即存在 $q = k$, 使得 $q \cdot n \leq m < (q+1) \cdot n$, 令 $r = m - n \cdot q$. 同时, 由于 m, n, q 均为整数, 则 r 也为整数, 于是 $m = n \cdot q + r$ 成立.

其次, 证明 q, r 的惟一性.

采用反证法也是推证中经常采用的方法之一. 通常是假设结论不成立, 继而推导出矛盾. 根据否定之否定即为肯定的原理, 即可证明结论成立.

假设另存在 q_1, r_1 也满足 $m = n \cdot q_1 + r_1$

由 $m = n \cdot q + r$ 可得

$$n \cdot q + r = n \cdot q_1 + r_1$$

故

$$n(q - q_1) = (r_1 - r)$$

注意到 $0 \leq r < n, 0 \leq r_1 < n$, 且 r, r_1 均为正整数, 于是得到 $|r_1 - r| < n$, 故

$$n \cdot |q - q_1| < n$$

上式欲成立, 只有 $|q - q_1| = 0$, 即 $q_1 = q$, 从而得出 $r_1 = r$. ■

如果 $m = n \cdot q + r$ 中的 $r = 0$, 就是 n 整除 m .

定义 1-4 m, n 是两个不同时为零的整数, 如果整数 $R \neq 0$ 满足:

(1) $m \parallel R$, 且 $n \parallel R$, 则称 R 为 m, n 的公因子, 也称为公约数.

(2) 对整数 $R \neq 0$, 若 $m \parallel R, n \parallel R$, 且 R 是所有公因子中最大的, 则称 R 为 m, n 的最大公因子. 记为 $R = (m, n)$.

一个整数, 至少有两个因子, 即 1 和其本身. 当 $m, n \neq 0$, 由于 m, n 是有限的, 所以它们的公因子也是有限的, 对此有限个因子总可以找出其中最大的公因子, 有且只有一个.

若一个正整数的因子只有 1 和其本身, 则称该数为素数; 若两个不为零的整数最大公因子为 1, 则称该两数互素.



定理 1-5 设 m, n, R 是三个不全为零的整数, 且 $m = n \cdot q + R$, 则 $(m, n) = (n, R)$. 即 m, n 的最大公约数等于 n, R 的最大公约数.

欲证明两数值相等, 通常采用的方法是证明 $m \leq n$, 同时又有 $m \geq n$; 这里应证明 $(m, n) \leq (n, R)$ 且 $(m, n) \geq (n, R)$.

证明 设 m, n 的最大公因子为 d , 显然有 $m // d, n // d$.

又已知 $m = n \cdot q + R$, 因而有 $R = m - n \cdot q$. 从而有 $R // d$, 于是 d 是 n, R 的公因子. 但不一定是 n, R 的最大公因子.

设 n, R 的最大公因子为 e , 即得 $d \leq e$ 即 $(m, n) \leq (n, R)$

从另一方面考虑, e 为 n, R 的最大公因子, 则 $R // e, n // e$, 而 $m = n \cdot q + R$.

所以 $m // e$. 又 $n // e$, 于是 e 为 m, n 的公因子, 由 d 是 m, n 的最大公因子, 则 $e \leq d$, 即 $(m, n) \geq (n, R)$. 从而 $(m, n) = (n, R)$. ■

推论 1-6 任给两个整数 $m, n > 0$, 则 (m, n) 就是带余除法最后一个不等于零的余数.

证明 任给 $m > 0, n > 0$ 不妨设 $m > n$, 则带余除法的过程为

$$\begin{array}{ll} m = n \cdot q_1 + r_1 & 0 < r_1 < n \\ n = r_1 \cdot q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2 \cdot q_3 + r_3 & 0 < r_3 < r_2 \\ \vdots & \vdots \\ r_{n-2} = r_{n-1} \cdot q_n + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = r_n \cdot q_{n+1} + r_{n+1} & \end{array}$$

因为 $n > r_1 > r_2 \cdots$, 经过有限次带余除法后, 总可得到 $r_{n+1} = 0$, 根据定理 1-5 可得

$$r_n = (0, r_n) = (r_n, r_{n-1}) = \cdots = (r_2, r_1) = (r_1, n) = (m, n). \quad \blacksquare$$

【例 1-1】 试求 1 970 与 1 066 的最大公约数.

$$1\,970 = 1 \cdot 1\,066 + 904$$

$$1\,066 = 1 \cdot 904 + 162$$

$$904 = 5 \cdot 162 + 94$$

$$162 = 1 \cdot 94 + 68$$

$$94 = 1 \cdot 68 + 26$$

$$68 = 2 \cdot 26 + 16$$

$$26 = 1 \cdot 16 + 10$$

$$16 = 1 \cdot 10 + 6$$

$$10 = 1 \cdot 6 + 4$$

$$6 = 1 \cdot 4 + 2$$

$$4 = 2 \cdot 2 + 0$$

因此 $(1\,970, 1\,066) = 2$

定理 1-7 任给 $m, n > 0$, 则存在两个整数 x, y (不一定是正整数), 使得



$$rn = (m, n) = m \cdot x + n \cdot y.$$

证明 根据推论 1-6 可知

$$r_n = r_{n-2} - r_{n-1} \cdot q_n$$

再将 $r_{n-1} = r_{n-3} - r_{n-2} \cdot q_{n-1}$ 代入上式得

$$r_n = r_{n-2} \cdot (1 + q_n \cdot q_{n-1}) - r_{n-3} \cdot q_n$$

再将 $r_{n-2} = r_{n-4} - r_{n-3} \cdot q_{n-2}$ 代入, 如此继续下去, 直到 m, n . 由于 x, y 是整数的加、减、乘的结果, 所以仍是整数, 于是可得

$$r_n = m \cdot x + n \cdot y \text{ 即 } (m, n) = m \cdot x + n \cdot y. \quad \blacksquare$$

例如 $(10, 8) = 2$ 可以表示为 $2 = 1 \times 10 - 1 \times 8$, $(42, 7) = 7$ 可以表示为 $7 = 1 \times 42 - 5 \times 7$.

定义 1-8 设 m, n 为整数, 如果整数 k 满足:

(1) $k // m, k // n$, 且 $k > 0$.

(2) 任意整数 R , 且 $R // m, R // n$, 且 $k \leq |R|$.

则称 k 为 m, n 的最小公倍数, 记为 $[m, n]$.

在程序设计时, 求两个整数的最小公倍数通常采用两种方法:

方法(一): 分别将两数进行素因式分解.

$$\text{例如 } a = p_1^{i_1} \cdot p_2^{i_2} \cdot \cdots \cdot p_r^{i_r}, b = p_1^{j_1} \cdot p_2^{j_2} \cdot \cdots \cdot p_s^{j_s}$$

其中 $p_1, p_2, \dots$ 均为素数. 则 a 与 b 的最小公倍数为: 相同因数取较大的指数, 不同的因数照取, 然后, 所取各因数之积就是最小公倍数.

【例 1-2】 试求 $a = 140, b = 110$ 的最小公倍数.

解 做质因数分解: $a = 2^2 \cdot 5^1 \cdot 7^1, b = 2^1 \cdot 5^1 \cdot 11^1$

$$\text{故 } [a, b] = 2^2 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 1\,540.$$

方法(二): 求出两数的最大公约数 (a, b) , 则 $[a, b] = \frac{a \cdot b}{(a, b)}$.

即两数的最小公倍数等于两数之积除以两数的最大公约数. 如 $(140, 110) = 10$

$$[140, 110] = \frac{140 \times 110}{10} = 1\,540.$$

定理 1-9 两个不为零的整数, 其最小公倍数等于该两数之积除以该两数的最大公约数.

证明 将两数素因数分解, 不妨令

$$a = p_1^{i_1} \cdot p_2^{i_2} \cdot \cdots \cdot p_r^{i_r}, b = p_1^{j_1} \cdot p_2^{j_2} \cdot \cdots \cdot p_s^{j_s}$$

将两数相乘, 底数相同的则指数相加, 底数不同则直接照写相乘. 由素因数分解式可见:

两数的最大公约数则是: 底数相同取指数最小的因素之积, 底数不同的则不取.

两数的最小公倍数是同底素数取指数最大, 且与不同底数的因数相乘.

于是 $(a, b) \cdot [a, b]$ 正好与 $a \cdot b$ 相同, 所以 $[a, b] = \frac{a \cdot b}{(a, b)}$. $\blacksquare$



§ 1.2 素数及其性质

以整数的各种特性及相互关系抽象地描述离散体的某些特性及相互关系是初等数论应用于实际的重要特点. 前节研究了整数的整除性, 从而定义了整除、最大公约数、最小公倍数等概念. 应用上述定义可以进一步探讨有关整数之间的某些特性, 如素数、亲和数、毕氏数、同构数、形数、完全数、水仙花数及幻方, 等等, 特别是哥德巴赫猜想更是数论理论的皇冠, 令人孜孜不倦地探索.

定义 1-10 一个大于 1 的整数, 如果它的正因数只有 1 和它本身, 则称该数为素数, 否则称为合数.

引理 1-11 设 a 是大于 1 的整数, 则 a 除去 1 之外的最小因数 q 必是素数.

证明 采用反证法. 因为 a 大于 1, 设 a 除 1 之外的最小因数 q 不是素数, 则必为合数, 有另一因数 q_1 存在且 $0 < q_1 < q$, 于是 $a // q_1, a // q$, 这与 q 是最小因数矛盾, 这个矛盾从何而来? 就是由于设 q 不是素数, 从而证明了最小因数 q 必是素数. ■

引理 1-12 设 p 是素数, a 是任一整数, 则 a 与 p 的最大公约数 $(p, a) = 1$, 或 $a // p$.

证明 因为 p 是素数, 只有 1, p 两个因数, 所以 (p, a) 有两种情况:

(1) 由于 a 的任意性, 不能保证 $a // p$, 也不能保证 $a = p$, 当 $a \neq p$ 时, a 绝对不是 p 的因数, 所以 $(p, a) = 1$

(2) 当 $a \neq p$ 时, a 可能是 p 的倍数, 即 $a // p$, 当 $a = p$ 时, $(p, p) = p$, 但这时只是对特殊的 $a = p$ 成立, 而不是对任意 a 成立.

所以 $(p, a) = 1$ 或 $a // p$. ■

定理 1-13 (整数的惟一分解定理) 任一大于 1 的整数能惟一分解为素数的乘积.

证明 先证存在性. 若 $a = 4$, 则 $a = 2 \times 2$ 总是存在的.

假设对小于 a 的一切整数都成立, 那么对大于 a 的整数是否也成立呢?

(1) 若 a 是素数, 则定理成立.

(2) 若 a 是合数, 则有两个整数 b, c 满足:

$$a = b \cdot c \quad 1 \leq b \leq c \leq a$$

此时, 若 b, c 为素数, 则定理成立.

若其中有 b 或 c 是合数, 可以再持续归纳分解.

于是存在 $a = p_1 \cdot p_2 \cdot \cdots \cdot p_n$ 成立, 其中 $p_1, p_2, \cdots, p_n$ 是素数, 存在性得证.

再证惟一性. 设 a 同时可以分解为两个素因数之积,

$$a = p_1 \cdot p_2 \cdot \cdots \cdot p_m \quad a = q_1 \cdot q_2 \cdot \cdots \cdot q_n$$

其中 $p_i, i = 1, 2, \cdots, m, q_j, j = 1, 2, \cdots, n$ 均为素数.

然而 $a // a$, 即 $(p_1 \cdot p_2 \cdots p_m) // (q_1 \cdot q_2 \cdots q_n)$, 于是必有某 q_j 可整除 p_i , 但 q_j, p_i 均