高等学校计算机专业规划教材

离散数学及应用

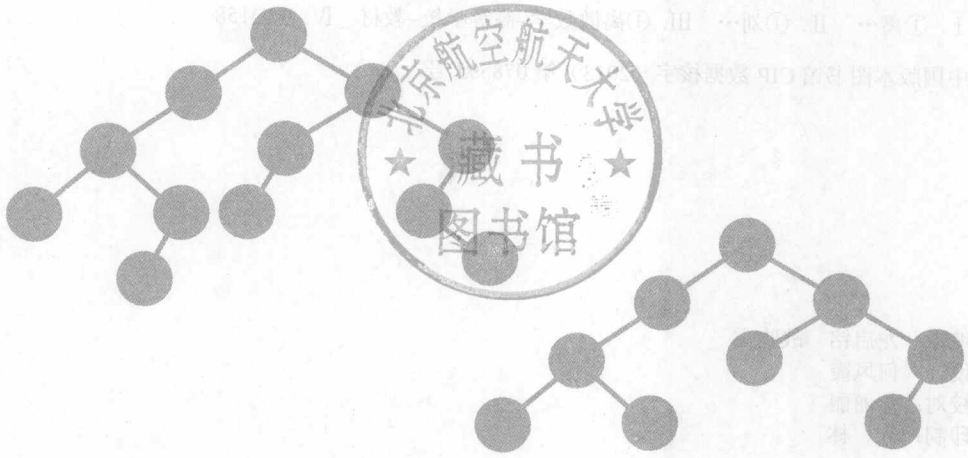
刘 铎 编著

清华大学出版社

高等学校计算机专业规划教

离散数学及应用

刘　铎　编著



清华大学出版社
北京

内 容 简 介

离散数学是现代数学的一个重要分支，是计算机专业和软件工程专业的基础主干课程，是进一步学习后续课程的研究和开发的基础。

本书是根据作者多年教学经验编写而成的，着重讲解离散数学的基本概念、基本方法及其应用，并给出大量典型例题和习题，以及若干离散数学应用案例和实验项目。全书共分 9 章，包括朴素集合论、数论基础、计数基础、命题逻辑、谓词逻辑、二元关系、函数、偏序关系与格、图论与树等。

本书结构紧凑、内容精炼、体系严谨、语言流畅、讲解详细，可作为高等院校计算机或软件工程专业本科生的“离散数学”课程教材，也可供其他专业学生和科技人员阅读参考。

图书在版编目（CIP）数据

离散数学及应用/刘铎编著. —北京：清华大学出版社，2013.6
高等学校计算机专业规划教材
ISBN 978-7-302-32015-9

Ⅰ. ①离… Ⅱ. ①刘… Ⅲ. ①离散数学–高等学校–教材 Ⅳ. ①O158

中国版本图书馆 CIP 数据核字（2013）第 078595 号

责任编辑：龙启铭　战晓雷
封面设计：何凤霞
责任校对：焦丽丽
责任印制：宋　林

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn, http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62795954
印 刷 者：三河市君旺印装厂
装 订 者：三河市新茂装订有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：18.75　　**字　　数**：434 千字
版　　次：2013 年 6 月第 1 版　　**印　　次**：2013 年 6 月第 1 次印刷
印　　数：1～2000
定　　价：29.50 元

产品编号：043550-01

前言

离散数学是现代数学的一个重要分支，是计算机专业和软件工程专业教学的基础主干课程，主要包含集合论、数理逻辑、图论和代数结构 4 部分基本内容，研究离散对象的结构、规律及相互关系。它在数据结构、操作系统、软件工程、数据库原理、计算机网络、人工智能、编译原理、软件设计形式化和信息安全等领域都有广泛的应用。该课程对于培养、训练和提高学生的问题抽象能力、逻辑推理能力、利用离散数学模型分析和解决实际应用问题的能力都有非常重要的作用，可以为学生进一步学习后续课程以及进行或参与创新性的研究和开发工作打下坚实基础。

本书的特点是着重讲解基本概念、基本方法及其应用，尽可能减少需要记忆的内容。除严谨系统的理论阐述和细致详尽的内容讲解外，本书给出了大量的典型例题、丰富的应用实例和难易程度不同的大量习题，还综合设计了几个不同的离散数学应用案例和实验项目，有利于学生加深对基本内容的理解和掌握，更可以使学生动手体会分析和解决问题的过程，提高学习的兴趣和效果。

本书的内容由浅入深，可读性强，部分内容比较抽象的章节在标题前加了*号，供教师参考实际情况选择使用。

本书可作为高等院校计算机或软件工程专业各方向本科生的一个学期的“离散数学”课程教材，也可供其他专业学生和科技人员阅读参考。

在编写过程中，作者参考了许多已经出版的同类书籍，在此对相关作者表示由衷的感谢！特别感谢孙波同志通读全稿并给出很多很好的意见和建议。

本书的出版得到了北京交通大学教学改革项目“《离散结构（双语）》课程研究性教学改革及课程资源建设”的支持。

清华大学出版社龙启铭编辑为本书的出版做了大量辛苦而细致的工作，作者在此表示深深的谢意。

最后，虽然作者在结构和内容上斟酌再三、几易其稿，但由于水平所限，书中难免有不妥或错误之处，恳请广大读者批评指正，可随时与作者联系（liuduo@bjtu.edu.cn）。

作　者

2013 年 3 月

目录

第 1 章 基础知识

本章主要介绍集合、序列、整除、同余、计数和布尔矩阵等内容，作为后续各章节的知识准备。

§1.1 集合与序列

§1.1.1 集合的基本概念

集合的概念和方法被广泛地应用于各种科学和技术领域，它也是计算机科学与软件工程的理论基础，在程序设计、形式语言、关系数据库和操作系统等计算机学科中都有重要的应用。

集合是数学中最基本的概念，无法给出严格精确的定义。通常，我们将若干个可确定、可分辨的对象构成的无序整体称为**集合**（set），常用大写英文字母 A、B、C、X、Y、Z 等表示。

定义 1.1 组成集合的对象称做该集合的**元素**（element），常用小写英文字母 a、b、c、x、y、z 等表示。若对象 a 是集合 S 的元素，则记做 $a\in S$，读做 a 属于 S；若对象 a 不是集合 S 的元素，则记做 $a\notin S$，读做 a 不属于 S。

【例 1.1】 R：“方程 $x^2-2=0$ 的所有实数解”、S：“12 的所有正约数”、P：“复平面上的所有点”、Q：“清华大学的全体学生”都是集合。3 是集合 S 的元素，即 $3\in S$；而 -3 不是该集合的元素，即 $-3\notin S$。而“很大的实数”、“清华大学的全体年轻教师”都不是集合，因为不能明确地判断任意一个对象是否属于该集合。

注：

（a）组成一个集合的条件是能够明确地判断任意一个对象是或者不是该集合的元素，二者必居其一。

（b）集合中的元素没有次序，一个集合中也没有相同的元素，如果一个集合中出现若干个相同的元素，则将它们作为一个元素。

（c）在同一个集合中的诸元素并不一定存在确定的关系。

（d）为了体系的严谨性，我们规定：对于任意集合 A 都有 $A\notin A$。[1]

【例 1.2】 本书规定使用一些特定的符号表示一些常用集合：自然数集 $\mathbb{N}$；整数集 $\mathbb{Z}$，正整数集 $\mathbb{Z}^+$，非零整数集 $\mathbb{Z}^*$；有理数集 $\mathbb{Q}$，非零有理数集 $\mathbb{Q}^*$；实数集 $\mathbb{R}$，非零实

1 在本书中，以（a）、（b）、（c）、…标明的各条目是并列关系，彼此之间没有明显的联系；而以（1），（2），（3），…标明的各条目表示须同时满足的条件。

数集$\mathbb{R}^*$；复数集$\mathbb{C}$，非零复数集$\mathbb{C}^*$。

使用形式化方法表示一个集合有两种方式，即外延表示法和内涵表示法：

（1）外延表示法（列举法）。逐个列出集合的元素，元素与元素之间用逗号“，”隔开，并将所有元素写在花括号“{ }”里，如：$A=\{a, b, c\}$，$B=\{0, 1, \cdots, 10\}$，$\mathbb{N}=\{0, 1, 2, \cdots\}$。

（2）内涵表示法（描述法）。假设$P(x)$是一个包含x的陈述句，表示x所具有的性质；对于每个确定的x，可以明确断定$P(x)$的正确与否。集合$\{x|P(x)\}$表示所有使$P(x)$为真的对象x所组成的集合，如：$\mathbb{Z}^+=\{x|x$是正整数$\}$，$R=\{x|x^2-2=0$且x是实数$\}$。

定义 1.2 设A和B是两个集合，如果A的任意一个元素都是B的元素，则称A为B的**子集**（subset），称B为A的**超集**（superset），记做$A\subseteq B$（或$B\supseteq A$），读做A包含于B或B包含A。

注：

（a）$\subseteq$表示集合与集合之间关系，而$\in$表示元素与集合之间关系。

（b）设A、B、C是3个集合，若$A\subseteq B$且$B\subseteq C$，则有$A\subseteq C$。

定义 1.3 设A和B是两个集合，如果$A\subseteq B$且$B\subseteq A$，则称A与B**相等**，记做$A=B$；否则称它们不相等，记做$A\neq B$。两个集合相等，当且仅当它们具有相同的元素。

定义 1.4 设A和B是两个集合，如果$A\subseteq B$且$A\neq B$，则称A为B的**真子集**（proper subset），记做$A\subset B$（或$B\supset A$）。

注：如果A是B的真子集，则集合A中的每一个元素都属于B，但集合B中至少有一个元素不属于A。

【例 1.3】 设集合$A=\{x|x$是6的正约数$\}$，$B=\{1, 2, 3, 6\}$，由于A和B具有相同的元素，故它们是同一个集合，即$A=B$。这说明很多集合可以用两种方法来表示，但也有些集合不可以用列举法表示，例如实数集合$\mathbb{R}$。

【例 1.4】 设集合$A=\{1, 2, 3, 4, 5, 6\}$，$B=\{0, 1, 2, 3, 4, 5, 6, 7\}$。由于对于任意$a\in A$，均有$a\in B$，故$A\subseteq B$。且由于$7\in B$而$7\notin A$，故$A\subset B$。

定义 1.5 在讨论的具体问题中，所讨论的对象全体称做**全集**（universal set），记做U。

注：由全集的定义可知，在讨论的具体问题中，所提及的集合均是全集的子集。而针对不同的具体问题可能会有不同的全集。

定义 1.6 不包含任何元素的集合称做**空集**（empty set），记做$\varnothing$。

定理 1.1 设A是任意一个集合，$\varnothing$是空集，则有$A\subseteq A$，$\varnothing\subseteq A$。

证明：

（a）对于任意集合A，它的任一元素都是其自身的元素，因而$A\subseteq A$。

（b）（反证法）若存在集合A使得$\varnothing$不是A的子集，则由定义1.2存在元素$x\in\varnothing$而且$x\notin A$；但这与空集的定义相矛盾，因此假设不成立，原结论成立。 □

推论 空集是唯一的。

证明：这里将使用一个后面还会经常使用的证明技巧。

设$\varnothing_1$和$\varnothing_2$都是空集，则由定理1.1，$\varnothing_1\subseteq\varnothing_2$且$\varnothing_2\subseteq\varnothing_1$，由定义1.3有$\varnothing_1=\varnothing_2$。□

定义 1.7 一个集合 A 所包含的元素数目称为该集合的**基数**或**势**（cardinality），记做 $|A|$或$\#A$ 或 $\mathrm{card}(A)$。

定义 1.8 若$|A|<\infty$，则称 A 为**有限集**或**有穷集**（finite set），否则称 A 为**无限集**或**无穷集**（infinite set）。

【例 1.5】 $|\{a, b, 2, a, \omega\}|=4$，$\mathrm{card}(\varnothing)=0$，它们都是有限集。而 $\mathbb{N}$、$\mathbb{Z}$、$\mathbb{Q}$、$\mathbb{Q}^*$、$\mathbb{R}$ 和 $\mathbb{C}$ 都是无限集。

事实上，无穷集又可分为**无穷可数集**和**无穷不可数集**，无穷可数集和无穷不可数集也分别称为**无穷可列集**和**无穷不可列集**。这部分内容将在第 5 章中详述。

定义 1.9 假设 A 是集合，A 的所有子集所组成的集合称做 A 的**幂集**（power set），记做 $\mathscr{P}(A)$，即 $\mathscr{P}(A)=\{x|x\subseteq A\}$。

【例 1.6】 假设集合 $A=\{a, b, c\}$，计算 $\mathscr{P}(A)$。

解：

A 的零元子集：$\varnothing$；

A 的一元子集：$\{a\}, \{b\}, \{c\}$；

A 的二元子集：$\{a,b\},\{a,c\},\{b,c\}$；

A 的三元子集：$\{a,b,c\}$；

于是 $\mathscr{P}(A)=\{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$。

【例 1.7】 $\mathscr{P}(\varnothing)=\{\varnothing\}$。

§1.1.2 集合的运算及性质

集合的运算就是由给定的集合按照确定的规则产生另外的集合。集合运算主要有以下 5 种：

定义 1.10 设 U 为全集，A、B 为 U 的两个子集，则：

（a）A 与 B 的**交集**（intersection）$A\cap B$ 定义为 $A\cap B=\{x|x\in A$ 且 $x\in B\}$；

（b）A 与 B 的**并集**（union）$A\cup B$ 定义为 $A\cup B=\{x|x\in A$ 或 $x\in B\}$；

（c）B 关于 A 的**相对补**（complement of B with respect to A）或 A 与 B 的**差集**（difference）$A-B$ 定义为 $A-B=\{x|x\in A$ 且 $x\notin B\}$，也记做 $A\backslash B$；

（d）A 关于全集 U 的相对补称做 A 的**绝对补**或**补集**（complement），记做 $\overline{A}$（或 $\sim A$），即 $\overline{A}=\{x|x\in U$ 且 $x\notin A\}$；

（e）A 与 B 的**对称差**（symmetric difference）$A\oplus B$ 定义为 $A\oplus B=\{x|x\in A$ 或 $x\in B$ 且 x 不同时属于 A 和 $B\}$。

注：

（a）由定义可得 $A-B=A\cap\overline{B}$，$A\oplus B=(A-B)\cup(B-A)$；

（b）交运算、并运算也可以扩展到多个集合上，如 $A\cap B\cap C=\{x|x\in A$ 且 $x\in B$ 且 $x\in C\}$，$A\cup B\cup C=\{x|x\in A$ 或 $x\in B$ 或 $x\in C\}$；常用记号为 $\bigcap_{i=1}^{n}A_i$ 和 $\bigcup_{i=1}^{n}A_i$。

【例 1.8】 设全集 $U=\{0, 1, \cdots, 9\}$，集合 $A=\{0, 1, 2, 3\}$，$B=\{1, 3, 5, 7, 9\}$，则 $A\cap B=\{1, 3\}$，$A\cup B=\{0, 1, 2, 3, 5, 7, 9\}$，$A-B=\{0, 2\}$，$B-A=\{5, 7, 9\}$，$\overline{A}=\{4, 5, 6, 7, 8, 9\}$，$\overline{B}=$

$\{0, 2, 4, 6, 8\}$，$A \oplus B = \{0, 2, 5, 7, 9\}$。

定理 1.2 设 A、B 是两个集合，则以下各表述彼此等价：

（a）$A \subseteq B$；

（b）$A \cap B = A$；

（c）$A \cup B = B$；

（d）$\mathscr{P}(A) \subseteq \mathscr{P}(B)$。

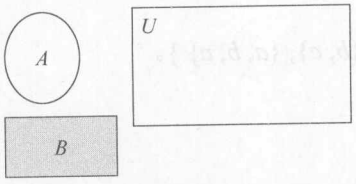
证明：只证明（a）与（d）等价，其他由定义易得。

证明集合 $X \subseteq Y$ 的基本方法是：对任意 $x \in X$，论证必有 $x \in Y$。

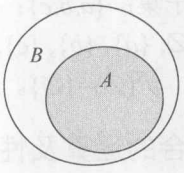
若 $A \subseteq B$，则对于任意 $X \in \mathscr{P}(A)$，有 $X \subseteq A$，故 $X \subseteq B$，所以 $X \in \mathscr{P}(B)$，即 $\mathscr{P}(A) \subseteq \mathscr{P}(B)$。

若 $\mathscr{P}(A) \subseteq \mathscr{P}(B)$，则对于任意 $a \in A$，有 $\{a\} \subseteq A$，即 $\{a\} \in \mathscr{P}(A)$，于是 $\{a\} \in \mathscr{P}(B)$，即 $\{a\} \subseteq B$，所以 $a \in B$，得到 $A \subseteq B$。 □

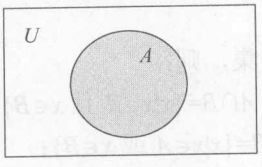
英国逻辑学家维恩（J. Venn，1834—1923）于 1881 年在《符号逻辑》一书中首先使用相交区域的图解来说明类与类之间的关系。后来人们以他的名字来命名这种用图形来表示集合间关系和集合运算的方法，称为**维恩图**（Venn diagrams）或**文氏图**，如图 1-1 所示。其构造方法如下。



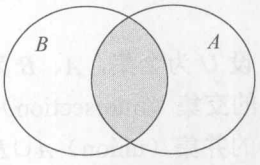
(a) 维恩图表示的集合与全集



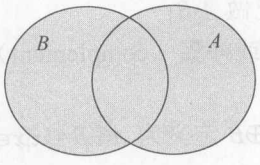
(b) $A \subseteq B$



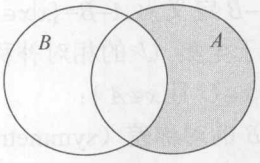
(c) $A \subseteq U$



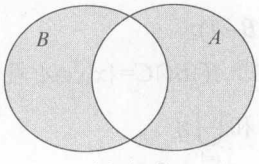
(d) $A \cap B$



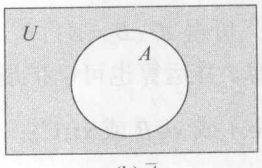
(e) $A \cup B$



(f) $A-B$



(g) $A \oplus B$



(h) $\overline{A}$

图 1-1 维恩图

（1）用一个大的矩形表示全集的所有元素（有时为简单起见，可将全集省略）。

（2）在矩形内画一些圆（或任何其他形状的闭曲线），用圆的内部的点表示相应集合的元素。不同的圆代表不同的集合。用阴影或斜线的区域表示新组成的集合。

维恩图的优点是形象直观，易于理解；而缺点是理论基础不够严谨。因此只能用于说明，不能用于证明。

定理 1.3 （集合运算的代数性质）设 U 为全集，A、B、C 为 U 的子集，$\varnothing$ 为空集，则有：

（a）交换律　$A\cup B=B\cup A$，$A\cap B=B\cap A$，$A\oplus B=B\oplus A$；

（b）结合律　$(A\cup B)\cup C=A\cup(B\cup C)$，$(A\cap B)\cap C=A\cap(B\cap C)$，$(A\oplus B)\oplus C=A\oplus(B\oplus C)$；

（c）分配律　$A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$，$A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$；

（d）吸收律　$A\cup(A\cap B)=A$，$A\cap(A\cup B)=A$；

（e）德·摩根律　$\overline{A\cup B}=\overline{A}\cap\overline{B}$，$\overline{A\cap B}=\overline{A}\cup\overline{B}$（绝对形式）；

$A-(B\cup C)=(A-B)\cap(A-C)$，$A-(B\cap C)=(A-B)\cup(A-C)$（相对形式）；

（f）幂等律　$A\cup A=A$，$A\cap A=A$；

（g）零律　$A\cup U=U$，$A\cap\varnothing=\varnothing$；

（h）同一律　$A\cup\varnothing=A$，$A\cap U=A$；

（i）排中律　$A\cup\overline{A}=U$；

（j）矛盾律　$A\cap\overline{A}=\varnothing$；

（k）余补律　$\overline{\varnothing}=U$，$\overline{U}=\varnothing$；

（l）双重否定律　$\overline{\overline{A}}=A$。

下面仅以例题的形式证明其中一部分，其余证明留给读者完成。

【例 1.9】　设 A、B、C 为任意集合，则 $A-(B\cap C)=(A-B)\cup(A-C)$。

证明：证明两个集合 X 和 Y 相等的一般方法是分别证明 $X\subseteq Y$ 和 $Y\subseteq X$。

（1）首先证明 $(A-B)\cup(A-C)\subseteq A-(B\cap C)$。

假设 $x\in(A-B)\cup(A-C)$，由定义有 $x\in A-B$ 或 $x\in A-C$。

若 $x\in A-B$ 则有 $x\in A$ 且 $x\notin B$，于是 $x\notin B\cap C$；

若 $x\in A-C$ 则有 $x\in A$ 且 $x\notin C$，于是 $x\notin B\cap C$。

总之有 $x\in A$ 且 $x\notin B\cap C$，故得 $x\in A-(B\cap C)$，因此 $(A-B)\cup(A-C)\subseteq A-(B\cap C)$。

（2）接着证明 $A-(B\cap C)\subseteq(A-B)\cup(A-C)$。

假设 $x\in A-(B\cap C)$，由定义有 $x\in A$ 且 $x\notin B\cap C$。

由 $x\notin B\cap C$，有 $x\notin B$ 或 $x\notin C$。再由 $x\in A$ 得 $x\in A-B$ 或 $x\in A-C$。

故 $x\in(A-B)\cup(A-C)$，进而 $A-(B\cap C)\subseteq(A-B)\cup(A-C)$。

综合（1）和（2），即得 $A-(B\cap C)=(A-B)\cup(A-C)$。　□

定理 1.3 中各定律并非彼此独立，即也可以使用部分定律证明其他定律。

【例 1.10】　设 A、B、C 为任意集合，则 $A-(B\cap C)=(A-B)\cup(A-C)$。

证明：$A-(B\cap C)=A\cap\overline{(B\cap C)}=A\cap(\overline{B}\cup\overline{C})=(A\cap\overline{B})\cup(A\cap\overline{C})=(A-B)\cup(A-C)$。□

使用上述定律还可以证明其他集合运算恒等式。

【例 1.11】 假设 $A \subseteq B$，则 $(B-A) \cup A = B$。

证明：$(B-A) \cup A = (B \cap \overline{A}) \cup A = (B \cup A) \cap (\overline{A} \cup A) = B \cap U = B$。 □

§1.1.3 序列

定义 1.11 **序列**（sequence）是被排成一列的对象，每个对象不是在其他对象之前，就是在其他对象之后，各对象之间的顺序非常重要。序列中的对象也称为**项**（item），项的个数（可能是无限的）称为序列的**长度**（length）。

【例 1.12】 以下诸例都是序列：

（a）1, 2, 3, 4, 5, 1, 2, 3

（b）2, 3, 5, 7, 11, 13, …

（c）1, 4, 9, 16, 25, 36, …

（d）apple, egg, egg, apple, egg, egg, …

（e）{a}, b, {{b}}

（f）d, i, s, c, r, e, t, e

序列可能是有限的（如例 1.12 中的（a）、（e）和（f）），也可能是无限的（如例 1.12 中的（b）、（c）和（d））。有限序列包含**空序列**（empty sequence），它没有任何项。

定义 1.12 对于给定的集合 A，定义 A^*为所有由 A 中元素生成的有限长度序列全体，A^*中的元素称为 A 上的**词**（word）或**串**（string）。在不引起混淆时，也可忽略序列各项间的“，”。A^*中的空序列称做**空串**（empty string），记做Λ。此时 A 也称做**字母表**（alphabet）。

【例 1.13】 假设 A ={a, b, c, …, z}为英文字母集合，则 A^*包含所有有限长度的英文“单词”，无论其是否具有意义，如：

（a）bat；

（b）cat；

（c）djoutrqoanlglkjr；

（d）asdfg。

定义 1.13 假设 A 是集合，$w_1=s_1s_2s_3\cdots s_n$ 和 $w_2=t_1t_2t_3\cdots t_k$ 都是 A^*中的元素，可定义 w_1 和 w_2 的**连接**（catenation）为 $s_1s_2s_3\cdots s_nt_1t_2t_3\cdots t_k$，记做 $w_1 \circ w_2$。

注：假设 A 是集合，$w \in A^*$，则 $w \circ \Lambda = \Lambda \circ w = w$。

【例 1.14】 假设 A ={a, b, c, …, z}，post, office$\in A^*$，则 post∘office=postoffice。

§1.2 数 论 基 础

本节主要讨论整数之间的性质，而带余除法是所讨论内容的基础。

定理 1.4 （**带余除法**）设 n 和 m 都是整数且 $n \neq 0$，则可以唯一地将 m 写为 $m=q \cdot n+r$，其中 q 和 r 是整数，且 $0 \leqslant r < |n|$。q 称做**商**（quotient），r 称做**余数**（remainder），记做 $r=m \bmod n$。

【例 1.15】 $-29=(-6)\cdot 5+1$；$143=11\cdot 13+0$；$915=11\cdot 78+57$。

定义 1.14 在定理 1.4 的表达式中，若余数 $r=0$，则称 ***m* 能被 *n* 整除**（m is dividable by n），或 ***n* 整除 *m***（n divides m），记做 $n|m$。此时，称 m 是 n 的一个**倍数**（multiple），称 n 是 m 的一个**约数**或**因子**（divisor）。

注：当 n 整除 m 当且仅当存在整数 q 使得 $m=q\cdot n$。

【例 1.16】 $3|12$，$3|(-15)$；12 的所有因子是$\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 12\}$。

定理 1.5 假设 a、b、c 是整数，$a\neq 0$，则

（a）若 $a|b$ 且 $a|c$，则对于任意的整数 x、y，有 $a|(xb+yc)$；

（b）若 $b\neq 0$，$a|b$ 且 $b|c$，则 $a|c$；

（c）若 $b\neq 0$，$a|b$ 且 $b|a$，则 $a=\pm b$。

证明：

（a）若 $a|b$ 且 $a|c$，则存在整数 k_1 及 k_2 使得 $b=k_1a$ 及 $c=k_2a$，于是 $xb+yc=xk_1a+yk_2a=(xk_1+yk_2)a$，即 $a|(xb+yc)$。

（b）若 $a|b$ 且 $b|c$，则存在整数 k_1 及 k_2 使得 $b=k_1a$ 及 $c=k_2b$，于是 $c=k_1k_2a$，即 $a|c$。

（c）若 $a|b$ 且 $b|a$，则存在整数 k_1 及 k_2 使得 $b=k_1a$ 及 $a=k_2b$，于是 $a=k_1k_2a$，$k_1k_2=\pm 1$，即 $a=\pm b$。 □

定理 1.6 对于任意正整数 a，有 $a|a$ 及 $1|a$。

证明：由 $a=1\cdot a=a\cdot 1$ 即得。 □

定义 1.15 若大于 1 的整数 p 的所有正因子只有 p 和 1，则称其为**质数**或**素数**（prime）；否则称其为**合数**（composite number）。

【例 1.17】 2, 3, 5, 7, 11, 13, 17, 19 都是素数；而 4, 6, 8, 9, 10, 12, 15, 16, 18 都是合数。

定理 1.7 有无穷多个素数。

证明：（反证法）假设只有有穷多个素数，设为 $p_1, p_2, \cdots, p_n$。令 $m=p_1p_2\cdots p_n+1$，显然有 $p_i\nmid m$，$1\leqslant i\leqslant n$。因此要么 m 本身是素数，要么存在大于 p_n 的素数整除 m，与假设产生矛盾。 □

定理 1.8（**算术基本定理**，arithmetic fundamental theorem）设正整数 $n>1$，则 n 可唯一地表示为 $p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$，其中 $p_1<p_2<\cdots<p_s$ 是 s 个相异的素数，指数 k_i 都是正整数。此定理又称做**唯一析因定理**。该表达式称做整数 n 的**素因子分解**。

推论 设正整数 a 的素因子分解是 $a=p_1^{k_1}p_2^{k_2}\cdots p_s^{k_s}$，则正整数 d 为 a 的因子的充分必要条件是 $d=p_1^{r_1}p_2^{r_2}\cdots p_s^{r_s}$，其中 $0\leqslant r_i\leqslant k_i$, $i=1, 2, \cdots, s$。

【例 1.18】 $150=2\times 3\times 5^2$，$168=2^3\times 3\times 7$。

定义 1.16 设 a 和 b 是两个不全为 0 的整数，若整数 d 满足 $d|a$ 且 $d|b$，则称 d 是 a、b 的**公因子**（common divisor），所有公因子中最大的称做 a 与 b 的**最大公因子**（greatest common divisor），记做 GCD(a, b)。

定义 1.17 设 a 和 b 是两个不全为 0 的整数，若正整数 m 满足 $a|m$ 且 $b|m$，则称 m 是 a、b 的**公倍数**（common multiple），所有公倍数中最小的称做 a 与 b 的**最小公倍数**（least common multiple），记做 LCM(a, b)。

定义 1.18 若整数 a 和 b 的最大公因子为 1，则称 a 与 b **互素**（relatively prime）。

注：对任意的正整数 a 有 GCD(0, a)=a, GCD(1, a)=1, LCM(1, a)=a。

【例 1.19】 GCD(12, 15)=3，LCM(12, 15)=60。8 和 15 互素，而 12 和 15 不互素，6、11、35 两两互素。

定理 1.9 设正整数 $a=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，$b=p_1^{s_1}p_2^{s_2}\cdots p_k^{s_k}$，其中 $p_1, p_2, \cdots, p_k$ 是互异素数，$r_1, r_2, \cdots, r_k, s_1, s_2, \cdots, s_k$ 是非负整数，则

$$\mathrm{GCD}(a,b)=p_1^{\min(r_1,s_1)}p_2^{\min(r_2,s_2)}\cdots p_k^{\min(r_k,s_k)}$$

$$\mathrm{LCM}(a,b)=p_1^{\max(r_1,s_1)}p_2^{\max(r_2,s_2)}\cdots p_k^{\max(r_k,s_k)}$$

推论 设 a、b 是正整数，则 GCD(a, b)·LCM(a, b)=a·b。

【例 1.20】 $150=2^1\times3^1\times5^2\times7^0$，$168=2^3\times3^1\times5^0\times7^1$，则

$$\mathrm{GCD}(150,168)=2^1\times3^1\times5^0\times7^0=6$$

$$\mathrm{LCM}(150,168)=2^3\times3^1\times5^2\times7^1=4200$$

当不知道整数 a 和 b 的因子分解时，也可以计算 a 和 b 的最大公因子。欧几里得（Euclid, 约公元前 325—265 年）在《几何原本》中提出了计算最大公因子的算法，这被公认是最早的算法，也是人类历史上最好的算法之一。在表述该算法之前，先给出下述定理，奠定算法的理论基础。

定理 1.10 设 $a=qb+r$，其中 a、b、q、r 都是整数，则

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r)$$

证明：若 $d|a$ 且 $d|b$，则由定理 1.5，有 $d|b$ 且 $d|r$。

若 $d|b$ 且 $d|r$，则由定理 1.5，有 $d|(qb+r)$，即 $d|a$。

于是，a 与 b 的公因子集合和 b 与 r 的公因子集合相同。继而，最大公因子相同。

□

下面给出计算最大公因子的欧几里得算法。

欧几里得算法（辗转相除法） GCD (a, b)

输入：整数 a, b。

输出：GCD(a, b)。

```
1.  If b=0 then return a
2.  Else return GCD(b, a mod b)
```

【例 1.21】 使用欧几里得算法求 168 与 150 的最大公因子。

解：

a	b	
168	150	168=1×150+18
150	18	150=8×18+6
18	6	18=3×6+0
6	0	

得 GCD(168, 150)=6。