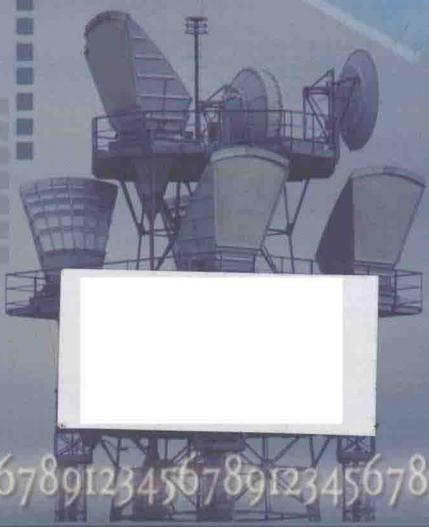
全国高校素质教育教材研究编审委员会审定

应用数论

YING YONG SHU LUN

主编★孙宝法



中国教育文化出版社

应 用 数 论

主编　孙宝法

中国教育文化出版社

图书在版编目（CIP）数据

应用数论/主编　孙宝法，—中国：中国教育文化出版社，2006 年 7 月

ISBN 988-98193-3-3

Ⅰ.应…　Ⅱ.孙…　Ⅲ. 应用数论

Ⅳ. O156

中国版本图书馆CIP数据核字（2006）

应用数论

主编　孙宝法

责任编辑：王方玉

封面设计：张骐年

出版发行：中国教育文化出版社

排　　版：科事洁文印中心

印　　刷：新颖印务有限公司

开　　本：850mm×1168mm　1/32

印　　张：7.75

字　　数：201 千字

版　　次：2006 年 7 月第 1 版

印　　次：2006 年 7 月第 1 次印刷

书　　号：ISBN 988-98193-3-3/G・392

定　　价：17.00 元

地址：北京市海淀区交大东路 62 号 307 室　100044

全国高校素质教育教材研究编审委员会
审定专家组名单

顾　问：顾明远

组　长：李恒光

副组长：尹占国　解思忠

成　员：柯红路　郑瑞伦

前　言

1. 关于数论

人类自从学会计数开始，就一直在和自然数打交道. 后来，由于实践的需要，数的概念进一步扩展. 自然数叫做正整数，它们的相反数叫做负整数，介于正整数和负整数之间的数叫做零. 正整数、负整数、零统称为整数.

整数可以进行加、减、乘、除四则运算. 其中加法、减法和乘法这三种运算在整数集合内是封闭的，任意两个整数相加、相减、相乘，它们的和、差、积仍然是一个整数. 但是，整数之间的除法在整数集合内不是封闭的.

人们在应用和研究整数的过程中，逐步熟悉了整数的特性. 比如，整数可分为两大类——奇数和偶数. 利用整数的这些基本性质，可以进一步探索许多有趣和复杂的数学规律.

数论这门学科最初是从研究整数开始的，所以叫做整数论. 后来整数论进一步发展，就叫做数论了. 确切地说，数论就是一门研究整数性质的学科.

自古以来，数学家一直十分重视对整数性质的研究，但是，直到 19 世纪，这些研究成果还只是孤立地记载在各个时期的算术著作中，没有形成完整统一的学科.

在我国古代许多著名的数学著作中，都有关于数论的内容，比如最大公约数、勾股数组、不定方程的整数解等等. 在国外，古

希腊的数学家对于数论中一个最基本的问题——整除就有了系统的研究，关于素数、合数、因数、倍数等一系列概念也已经被提出来了. 后来，各个时代的数学家对整数性质的研究也都作出过重大贡献，使数论的基本理论逐步得到完善.

在整数性质的研究中，人们发现素数是构成正整数的基本“材料”，要深入研究整数的性质，就必须研究素数的性质. 因此，关于素数性质的问题，一直受到数学家的关注.

到 18 世纪末，历代数学家积累的关于整数性质的零散的知识已经十分丰富，把它们整理加工成一门系统学科的条件已经成熟了. 德国数学家高斯集前人之大成，完成了著作《算术探讨》. 1800 年，高斯把该书寄给法国科学院，但是法国科学院拒绝了高斯的这部杰作，高斯只好在 1801 年自己发表了这部著作. 正是这部书，开始了现代数论的新纪元.

在《算术探讨》中，高斯把过去研究整数性质所用的符号标准化了，把当时现存的定理系统化，并进行了推广，把要研究的问题和已知的方法进行了分类，还引进了新的方法，使数论成为了一门独立的学科.

数论成为一门独立的学科后，随着数学其他分支的发展，研究数论的方法也在不断发展. 如果按照研究方法来说，可以把数论分成初等数论、解析数论、代数数论和几何数论四个分支.

初等数论是数论中不求助于其他数学学科的帮助、只依靠初等的方法来研究整数性质的分支. 比如中国古代有名的“中国剩余定理”，就是初等数论中的重要内容.

解析数论是使用数学分析这个工具来解决数论问题的分支. 数学分析是以函数作为研究对象，在极限概念的基础上建立起来的数学学科. 用数学分析来解决数论问题是由欧拉奠基的，俄国数学家切比雪夫等人也对它的发展作出过贡献. 解析数论是解决数论中艰深问题的强有力的工具. 比如，对于“素数有无限多个”这个命题，欧拉给出了解析方法的证明，其中利用了数学分析中有

关无穷级数的若干知识. 20 世纪 30 年代，苏联数学家维诺格拉多夫创造性地提出了“三角和方法”，这个方法对于解决某些数论难题有着重要的作用. 我国数学家陈景润在解决“哥德巴赫猜想”问题时使用的也是解析数论的方法.

代数数论是把整数的概念推广到代数整数的一个分支. 数学家把整数概念推广到一般代数数域上去，相应地建立了素整数、可除性等概念.

几何数论是由德国数学家、物理学家闵可夫斯基等人开创和奠基的. 几何数论研究的基本对象是“空间格网”. 什么是空间格网呢？在给定的直角坐标系上，坐标全是整数的点，叫做整点；全部整点构成的组就叫做空间格网. 空间格网对几何学和结晶学有着重大的意义. 由于几何数论涉及的问题比较复杂，必须具有相当的数学基础才能深入研究.

数论是一门高度抽象的数学学科，长期以来，它的发展处于纯理论的研究状态，它对数学理论的发展起到了积极的作用. 但是，大多数人并不清楚它的实际意义.

由于近代计算机科学和应用数学的发展，数论得到了广泛应用. 比如，在计算方法、代数编码、组合论等方面，都广泛使用了初等数论的许多研究成果. 又有文献报道，现在，有些国家应用“孙子定理”来进行测距，用原根和指数来计算离散傅立叶变换等. 此外，数论的许多比较深刻的研究成果也在近似分析、差集合、快速变换等方面得到了应用. 特别是现在，由于计算机的发展，用离散量的计算去逼近连续量而达到所要求的精度已成为可能.

数论在数学中的地位是独特的，高斯曾经说过：“数学是科学的皇后，数论是数学中的皇冠”. 因此，数学家都喜欢把数论中一些悬而未决的疑难问题，叫做“皇冠上的明珠”，以鼓励人们去摘取. 如费马大定理、孪生素数问题、哥德巴赫猜想、圆内整点问题、完全数问题等就是数论皇冠上几颗最明亮的“明珠”.

在我国近代，数论也是发展最早的数学分支之一. 从 20 世纪

30年代开始，我国数学家在解析数论、刁藩都方程、一致分布等方面都有过重要的贡献，出现了华罗庚、闵嗣鹤、柯召等第一流的数论专家. 其中，华罗庚在三角和估值、堆砌素数论方面的研究享有盛名. 1949 年以后，数论的研究得到了更大的发展，在筛法和哥德巴赫猜想方面的研究，我国占据了世界领先的地位.

特别值得一提的是，陈景润在 1966 年部分地证明了哥德巴赫猜想，在国际数学界引起了强烈反响. 数学界盛赞陈景润的论文是解析数论的名作，是筛法的光辉顶点. 至今，陈景润证明的结论仍是哥德巴赫猜想的最好结果.

2. 关于数论教材

长期以来，数论常常被看作是智者的游戏，有的人敬而远之. 数论，作为课程内容，常常被认为是一些基础知识的介绍；作为研究内容，常常被认为是一大批纯数学的难题. 总之，人们认为数论与实际应用没有多大的关系. 因此，在相当长的一段时期内，国内只有一些师范大学和综合大学的数学系开设《初等数论》这门课程.

随着计算机技术和数字通信技术的迅猛发展，编码和解码、加密和解密等应用技术都需要数学（特别是数论）等基础科学为之提供理论的支撑. 因此，为计算机、网络工程、数字通信、信号与信息处理等专业的学生开设《初等数论》课程，已经成为很多高等院校教育主管的共识.

现在的问题是，没有适合 IT 专业学生需要的教材. 那些已有的初等数论教材是为数学系的学生开设的，它们明显不适合计算机、网络工程、数字通信、信号与信息处理等 IT 专业学生的需要. 已有的教材比较注重系统的严格、理论的深度、推理的严密、逻辑的思辨，以纯粹数学面貌出现的这些教材，没有充分考虑数论

的研究成果在IT上的应用，而这正是IT专业学生所需要的. 因此，我们不能以简单的拿来主义的态度，把为数学系学生编写的教材直接施教于IT专业的学生身上.

笔者认为，为 IT 专业学生编写的初等数论教程，应该达到以下几个目标：

（1）强调基础知识和基本技能. 任何一门学科都是建立在基本概念、基础知识和正确思维的基础之上的，初等数论也不例外. 有了清晰准确的概念、必要的基础知识、正确的思维方式和熟练的技能技巧，学生就可以逐步掌握更多的知识，在应用时就容易理解和接受令人头疼的数学理论，甚至可以发现新的问题，并有所创新.

（2）适当的深度和广度. 为 IT 专业学生编写的初等数论教程，不必在某些难题上做过多的探究，不必过分强调理论深度和广度. 例如，可以省略数论函数、素数分布、多元和/或高次不定方程、连分数等较困难、较抽象、与应用没有直接关系的内容，并不会影响本学科的基础性和完整性.

（3）完备、简洁、直观的理论体系. 有的教材，为了建立某个理论体系，如最大公约数理论，介绍了多种途径，并证明这些途径彼此等价. 对于从事数论研究或从事数论教学工作的读者来说，这或许是适合的. 但是，对于以应用为目的、数学推理能力又比较薄弱的IT专业的学生来说，这样处理明显是不合适的，因为这样的教材会把学员的注意力吸引到研究理论体系的完备性上去，从而偏离本课程教学的主要目标. 好的教材只需用一种最简洁、最直观的方法，建立起完备的理论体系就足够了.

（4）加强应用内容的介绍. 虽然数论曾经给人们留下了阳春白雪、不食人间烟火的印象，但是，在计算机技术和信息科学的发展进程中，数论在实际应用的前沿作出了重大的贡献，而且，可以预见，在未来科学技术研究中，数论将发挥更加重要的作用. 在数论课程中适当介绍一些数论应用的内容，可以使学生对数论

这门学科有比较全面的认识，激发他们的学习兴趣和热情，还可以激发他们的创新灵感.

上述目标是本教材的出发点，也是本教材的归宿，笔者一直在朝着这个方向努力. 但是，由于水平有限，加之时间仓促，还有很多地方需要改进和提高，恳请广大读者批评指正，提出宝贵意见.

在本书的编写过程中，参考了后面所罗列文献的内容，在此，向这些著作的作者致以诚挚的谢意！全国高校素质教育教材研究编审委员会的王方玉老师、电子工程学院教保处的汤海峰参谋、数学教研室的同事、家人和朋友都给予了笔者极大的鼓励与支持，在此一并致谢！

孙宝法

2006年7月15日于庐州

目　录

第 1 章　整数的整除理论

整数是初等数论的主要研究对象，而整数的整除理论是初等数论的基础.

1.1 回顾了有关整数的知识，证明两个数学归纳法、最小自然数原理、最大自然数原理、抽屉原理. 这些方法和原理是后面定理证明的工具和依据. 1.2 讨论整除的概念及其基本性质，以此为基础，定义因数、倍数、素数、合数等概念. 1.3 引进研究初等数论的重要工具——带余除法和辗转相除法，介绍带余除法的应用. 1.4、1.5 定义最大公约数、最小公倍数等概念，研究最大公约数、最小公倍数的性质. 1.6 证明算术基本定理. 1.7 介绍实数的整数部分和小数部分，并讨论它们的性质. 1.8 给出阶乘 n！的素因数分解公式.

这些内容是本课程最基本的、最重要的部分.

1.1　整　数

$N=\{1,2,3,\cdots,n,\cdots\}$：自然数的集合.

$Z=\{\cdots,-n,\cdots,-3,-2,-1,0,1,2,3,\cdots,n,\cdots\}$：整数的集合.

$Z_{n_0}^{+}=\{n\mid n\geq n_0, n\in Z, n_0\in Z\}$：大于或等于 n_0 的整数的集合.

$Z_0^{+}=\{n\mid n\geq 0, n\in Z\}=\{0\}\bigcup N$：扩大的自然数集.

整数可以比较大小，可以求整数的绝对值.

在整数集合中，可以作加法、减法、乘法运算，运算的结果仍然是整数，即整数对加法、减法、乘法封闭. 加法运算满足交换律、结合律，乘法运算满足交换律、结合律，乘法对加法满足分配律. 两个整数相除，商不一定是整数，即整数对除法不封闭.

自然数及其运算源于人们的经验，其最本质的属性是归纳公理.

归纳公理 设 S 是 N 的一个子集. 如果 S 满足条件：

（1）$1\in S$；

（2）若 $n\in S$，则 $n+1\in S$，

那么，$S=N$.

根据归纳公理，可以证明第一数学归纳法.

定理 1 第一数学归纳法

设 $P(n)$ 是关于自然数 n 的一个命题. 如果

（1）当 $n=1$ 时，$P(1)$ 成立；

（2）若 $P(n)$ 成立，则 $P(n+1)$ 成立，

那么，$P(n)$ 对所有自然数 n 成立.

证明 设 S 是使 $P(n)$ 成立的所有自然数 n 的集合. S 是 N 的子集.

由条件（1）知，$1\in S$；

由条件（2）知，若 $n\in S$，则 $n+1\in S$.

根据归纳公理，$S=N$.

根据第一数学归纳法，可以证明在数学中常用的自然数的两个重要性质.

定理 2 最小自然数原理

设 T 是 N 的一个非空子集. 存在 $t_0\in T$，对任意 $t\in T$，有 $t_0\leqslant t$.

证明 设 $S=\{s\mid s\leq t,\forall t\in T\}$. 因为 1 满足 S 的条件，所以，

$1\in S$，S 非空.

下面证明，存在 $s_0\in S$，使得 $s_0+1\notin S$.

若不然，对于任意 $s_0\in S$，都有 $s_0+1\in S$，则 $S=N$.

另一方面，因为 T 非空，所以，存在 $t_1\in T$.

因为 $t_1+1>t_1$，所以，$t_1+1\notin S$. 故 $S\neq N$. 矛盾.

下面证明 $s_0\in T$.

若不然，则对 $\forall t\in T$，必有 $s_0<t$.

于是，$s_0+1\leq t$. 从而，$s_0+1\in S$. 矛盾.

取 $t_0=s_0$，就证明了定理.

定理 2 指出，N 的一个非空子集 T 一定有最小自然数.

定义　设 M 是 N 的一个非空子集. 若存在 $a\in N$，使得对任意 $m\in M$，有 $m\leq a$，则称 M 有上界，a 是 M 的一个**上界**. 若存在 $a\in N$，使得对任意 $m\in M$，有 $m\geq a$，则称 M 有下界，a 是 M 的一个**下界**.

定理 3　最大自然数原理

设 M 是 N 的一个非空子集. 若 M 有上界，则存在 $m_0\in M$，使得对 $\forall m\in M$，有 $m\leq m_0$.

证明　设 $T=\{t\mid m\leq t,\forall m\in M\}$. 因为 M 有上界，所以 T 非空.

根据定理 2，T 存在最小自然数 t_0. 下面证明 $t_0\in M$.

若不然，则对 $\forall m\in M$，必有 $m<t_0$.

于是，$m\leq t_0-1$. 从而，$t_0-1\in T$. 这与 t_0 是 T 中的最小自然数矛盾.

取 $m_0=t_0$，就证明了定理.

定理 3 指出，N 的一个非空、有上界的子集，一定有最大自然数.

根据最小自然数原理，可以证明第二数学归纳法.

定理 4　第二数学归纳法

设 $P(n)$ 是关于自然数 n 的一个命题. 如果

（1）当 $n=1$ 时， $P(1)$ 成立；

（2）设 $n>1$. 若对所有的自然数 $m\ (m<n)$， $P(m)$ 成立，则 $P(n)$ 成立，

那么， $P(n)$ 对所有自然数 n 成立.

证明　用反证法.

设 T 是使 $P(n)$ 不成立的所有自然数的集合. 若定理不成立，则 T 非空. 根据定理 2，T 存在最小自然数 t_0.

由于 $P(1)$ 成立，因此， $t_0>1$.

对于 $n=t_0$，由条件(2)，存在自然数 $m\ (m<t_0)$，使得 $P(m)$ 不成立.

由 T 的定义知， $m\in T$. 这与 t_0 是 T 中的最小自然数矛盾.

注意：

（1）在具体应用时，可能需要对两个数学归纳法作适当的变形. 一般情况下，需要在整数集合的子集 $Z_{n_0}^{+}$ 上运用数学归纳法.

（2）最小自然数原理和最大自然数原理可以推广为：若整数集合的子集 T 有上界，则 T 有最大整数；若整数集合的子集 T 有下界，则 T 有最小整数.

在初等数论的证明中，还经常用到抽屉原理.

定理 5　鸽巢原理、盒子原理、抽屉原理、Dirichlet 原理

设 n 是一个自然数. 现有 n 个盒子和 n+1 个物体. 把 n+1 个物体放入 n 个盒子，无论怎样放，一定有一个盒子被放了两个或两个以上物体.

证明　用反证法.

假设结论不成立，即每个盒子至多有一个物体，那么，这 n 个盒子中的物体总数不大于 n. 这与 n+1 个物体放入了 n 个盒子中相矛盾.

例 1　设 $a\ (a \geq 2)$ 是给定的整数. 证明：对任一正整数 n，存在唯一的整数 $k \geq 0$，使得 $a^k \leq n < a^{k+1}$.

证明　记 $T = \{t \mid n < a^t, t \in Z\}$.

因为 a^x 是 x 的增函数，并且 $n \geq a^0$，

所以，对于任意 $t \in T$，都有 $t > 0$.

因为 T 有下界，

所以，T 中存在最小的整数 t_0.　（注意（2））

根据 t_0 的含义，得 $a^{t_0-1} \leq n < a^{t_0}$，并且 t_0 是唯一的.

取 $k = t_0 - 1$，则 $k \geq 0$，并且，$a^k \leq n < a^{k+1}$.

习题 1.1

1. 设 k_0 是给定的正整数，$P(n)$ 是关于自然数 n 的一个命题. 如果

（1）当 $n = k_0$ 时，$P(k_0)$ 成立；

（2）若 $P(n)$ 成立，则 $P(n+1)$ 成立，

那么，$P(n)$ 对所有正整数 $n \geq k_0$ 成立.

2. 设 k_0 是给定的正整数，$P(n)$ 是关于自然数 n 的一个命题. 如果

（1）当 $n = k_0$ 时，$P(k_0)$ 成立；

（2）设 $n > k_0$. 若对所有的整数 $m\ (k_0 \leq m < n)$，$P(m)$ 成立，则 $P(n)$ 成立，

那么，$P(n)$ 对所有正整数 $n \geq k_0$ 成立.

3. 设 T 是整数的子集. 若 T 中有正整数，则 T 中有最小正整数.

4. 设 T 是整数的子集.

（1）若 T 有上界，则 T 中有最大整数.

（2）若 T 有下界，则 T 中有最小整数.