奥林匹克数学教程

数论基础

张君达　主编

北京科学技术出版社

图书在版编目(CIP)数据

数论基础/张君达主编. —北京：北京科学技术出版社，2002.8

奥林匹克数学教程

ISBN 7-5304-2610-9

Ⅰ.数… Ⅱ.张… Ⅲ.数论-师资培训-教材 Ⅳ.0156

中国版本图书馆 CIP 数据核字(2002)第 037784 号

数论基础

作　　者：张君达
责任编辑：刘长梅
责任印制：藏桂芬
封面设计：李　辉
出 版 人：张敬德
出版发行：北京科学技术出版社
社　　址：北京西直门南大街 16 号
邮政编码：100035
电话传真：0086-10-66161951(总编室)
0086-10-66113227　0086-10-66161952(发行部)
电子信箱：bkjpress@95777.com
经　　销：新华书店
印　　刷：三河市腾飞胶印厂
开　　本：850mm×1168mm　1/32
字　　数：184 千
印　　张：7.25
版　　次：2002 年 8 月第 1 版
印　　次：2002 年 8 月第 1 次印刷
印　　数：1—3000
ISBN 7-5304-2610-9/G·183

定　价：18.00 元

张君达　主编

倪斯杰　鲍敬谊　顿继安
李景华　兰　英　王　蓓　编

前　言

初等数论是研究整数性质的一个数论分支，它是数学中历史悠久的分支之一。早在公元前 3 世纪，古希腊数学家欧几里德(Euclid)就已证明了猜想“有无穷多个素数存在”的正确性。我国古代的《孙子算经》中给出了求解一次同余式组的算法——孙子定理，亦称中国剩余定理。1801 年，数学家高斯(Gauss)在其著作《算术研究》中首先提出了二次互反律、原根存在的充分必要条件等重要结果，并对同余理论做了较为系统的研究。通常，高斯的这一名著被认为是数论作为数学的一个独立分支的标志。

古老悠久的数论在数学发展史中占据着不容忽视的一页，不少重大数论课题的研究都创造了极其深刻的新的方法，甚至促进着新的数学分支的发展。例如对不定方程和高次互反律的研究促进了代数数论与类域论的发展。20 世纪以来，人们惊喜地发现：初等数论在当代计算机科学、组合数学、代数编码、信号的数字处理等科学技术领域得到了极其广泛的应用。时至今日，这一古老学科的底蕴仍然洋溢着诱人的青春活力。

初等数论是一门十分重要的基础课。它不仅应该是高等师范院校数学专业、大学数学各专业的必修课，而且也是计算机科学等许多相关专业所需要的课程。初等数论在离散数学以及计算机科学等诸多学科中所起的日益明显的重要作用绝非偶然。事实上，近代数学中许多重要思想、概念、方法与技巧都源于对整数性质的深入研究而不断丰富和发展起来的。学习初等数论不仅可以掌握它的基本观点、内容和方法，还可以从中领悟某些近代数学思想与方法的背景。

“数学是思维的体操”,初等数论是一门绝好的思维训练课程,由于学习初等数论不需要更多的预备知识,因此学习者主要应学习理论并用以解决一些难度较大的问题。思维是智力与能力的核心,初等数论为学习者提供了开发智力与增长能力的系统素材,它不失为一门思维训练课程。被誉为“世界青年智能大赛”的国际数学奥林匹克(IMO)的试题中,数论或与数论相关的试题占总试题的40%左右,这个结果恰好支持了我们的观点。

正基于此,自1988年以来,我为我的三个不同专业方向的六届硕士研究生都开设了“数论基础”课程。“数论基础”在理论上保持了初等数论的主体结构,在内容上加大了思维训练的强度。与通常的大学本科的“初等数论”不同的是在“数论基础”中直接引用了IMO或世界各国的数学奥林匹克试题。希望这样的课程设计更能适应高等师范院校的研究生与本科生的需求。

全书共分七章。第一章重点介绍初等数论的基础—整除理论。为使读者对整数有一个清楚、正确的认识,本章引入时介绍了自然数的基数理论与序数理论。第二章介绍初等数论发生、发展的原始方法——带余除法与算术基本定理。第三章介绍高斯函数$[x]$,$\{x\}$的基本性质与相应的技巧与方法。第四章不定方程与第五章同余的理论与应用是初等数论的最基本的内容。第六章欧拉定理与威尔逊定理介绍了有关定理在二次同余方面的应用。第七章专题选讲重点介绍有关基本概念、方法的引伸与拓广。全书注意到奥林匹克数学的理论与实践的结合,适当地引入了数论的概念、方法在数学奥林匹克领域的应用。

作为“奥林匹克数学的理论与实践”方向的硕士课程建设,初始的讲稿历经几届学生的整理、研讨与反复修改,初步形成了一定的体系。其中,鲍敬谊整理了前五章的讲稿,王蓓演算、核实了前五章的全部习题,倪斯杰负责初稿的部分章、节的审定与修改,李景华、顿继安的硕士论文充实了第七章的部分内容。数论基础的初稿分别由倪斯杰、鲍敬谊、王蓓、兰英、李景华、顿继安各主持一

章的研讨与修改，最后由我终审、定稿。

尽管我们的工作是努力的，数论基础课程的设计尚有一定的新意。但我们深知就我们的力量及短短十余年的时间，要使教材达到预期的目标是很难的。为适应当前教学的需要，权抛“数论基础”为砖，期待更多的“碧玉”问世。

本书可作为高等学校教师、研究生、学生的教学参考用书，也可作为中、小学教师继续教育与进修提高的指导用书。

感谢诸多同仁对本书内容的建议与指导，感谢北京科技出版社领导及刘长梅编辑为本书出版付出的辛勤劳动。

张君达

2002 年 6 月 1 日

目　录

第一章 整 除

§1 自然数

1.1 自然数与整数

自然数具有两方面的意义，一表示数量(多少个)，一表示次序(第几个)。基数理论与序数理论就是由此而抽象出来的两种主要的自然数理论。

1. 基数理论

基数理论是通过集合与映射等概念建立起来的自然数理论，对有限集来说，等价集合的共同特征是它们的元素个数相同，可以利用这一共同特征的集合进行分类，凡等价集合都归入一类，用一个符号表示它。据此，采用集合论的观点可以给出自然数的定义。

定义 1.1 一切等价集合的共同特征叫做基数

定义 1.2 非空有限集合的基数叫做自然数

若认为自然数包括零，则可不加"非空"条件，在此基础上，可以进一步给出自然数集合的大小关系、加法运算和乘法运算。

定义 1.3 设(非空)有限集合 A 和 B 的基数分别是 a 和 b，当

(1) $A\sim B$ 时，则说 a 等于 b，记作 $a=b$；

(2) $A\sim B'\subset B$，则说 a 小于 b，记作 $a<b$；

(3) $A\supset A'\sim B$，则说 a 大于 b，记作 $a>b$.

定义 1.4 设 $A\cap B=\phi$，$A\cup B=C$，如果(非空)有限集合 A、B、C 的基数分别是 a、b、c，则把 c 叫做 a 与 b 的和，记作 $c=a+b$，a 和 b 叫做加数，求两数和的运算叫做加法。

定义 1.5 设 b 个(非空)有限集 A_1、A_2……A_b 的基数都是

a，且 $A_i \cap A_j = \phi$，$1 \leqslant i < j \leqslant b$，如果 $A_1 \cup A_2 \cup \cdots\cdots \cup A_b = c$，则称集合 c 的基数 c 为 a 与 b 的积，记作 $a \times b = c$，a 叫做被乘数，b 叫做乘数。求两数积的运算叫做乘法。

在此基础上，先利用集合的知识论证和与积在自然数集中存在且唯一，以及基本运算定律和基本顺序律成立，然后再利用逆运算来定义减法与除法。在自然数集中讨论减法与除法可以实施的条件是必要的，至于四则运算的其它性质则可以用逻辑推理的方法给出。这样，可以建立并逐渐完善自然数基数理论系统。

2. 序数理论

序数理论是采用公理化方法建立起来的自然数理论。它从两个原理概念：集合与后继以及四条公理出发，确立多种命题，从而建立自然数的理论系统。

定义 1.6 任何一个非空集合 N 的元素叫做自然数，若在 N 中的某些元素间有一个基本关系“后继”（记为“′”），且满足下列公理：

(1) 存在一个元素，记作 1，它不后继于任何元素（即 $1 \in N$，且若 $a' \in N$，则 $a' \neq 1$）

(2) 对任何元素 a，有且仅有一个后继元素 a'（即若 $a = b$，则 $a' = b'$）。

(3) 除 1 以外，任何一个元素仅能是一个元素的后继元素（即若 $a' = b'$，则 $a = b$）

(4) (归纳公理)若 N 的任一子集 M，满足条件：

① $1 \in M$

② 每当 $k \in M$，就有 $k' \in M$，那么 M 含有一切自然数。

自然数定义的四个公理中，前三个公理的论断是很明显的，公理 4 通常称为归纳公理，由此可以导出一个重要的证明方法——数学归纳法。

应用公理化的方法还可以定义自然数的加法和乘法。

定义 1.7 在自然数集中，运算“+”叫做自然数的加法，应满

足：

(1) 对任何自然数 a，有 $a+1=a'$

(2) 对任何自然数 a 和 b，有 $a+b'=(a+b)'$；数 a 和 b 叫做加数，而相加的结果 $a+b$ 称为和。

定义 1.8 在自然数集中，运算“·”叫做自然数的乘法，应满足：

(1) 对任何自然数 a，有 $a\cdot 1=a$；

(2) 对任何自然数 a 和 b，有 $a\cdot b'=a\cdot b+a$，数 a 叫做被乘数，数 b 叫做乘数，而相乘的结果 $a\cdot b$ 叫做积。

定义 1.9 设 a、b 是自然数，若存在一个自然数 k，使 $a=b+k$ 成立，则说 a 大于 b，记作 $a>b$；或者说 b 小于 a，记作 $b<a$。

由此可论证关于自然数的基本顺序定律是成立的，再从逆运算的角度引入减法与除法及其相应的性质与运算定律，那么自然数的序数理论系统就相应建立并趋于完善。

基数理论与序数理论从两个不同侧面刻画了自然数的意义，并建立了统一的运算法则。

自然数又叫正整数，正整数、0 和负整数统称为整数，通常用 Z 表示整数集，N 或 Z^+ 表示自然数集，全体整数对加法构成了一个 *Abel* 群——$(Z,+,0)$，即满足下列性质：

(1) $\forall a,b\in Z$，有 $a\pm b\in Z$

(2) 结合律：$(a+b)+c=a+(b+c)$ a、b、$c\in Z$

(3) 交换律：$a+b=b+a$，$a,b\in Z$

(4) 有单位元 0：$a+0=a$，$a\in Z$

(5) $\forall a\in Z$，$\exists b\in Z$，使得 $a+b=0$，b 即为 a 的逆元，记作 $-a$。

同时，整数集对乘法运算封闭，即 $\forall a$、$b\in Z$，$a\times b\in Z$，但 $a\div b$ 不一定属于 Z，乘法常简记为 $a\cdot b$ 或 ab。乘法运算满足以下性质：

(1) 结合律：$(ab)c=a(bc)$

(2) 交换律：$ab = ba$

(3) 分配律：$(a + b)c = ac + bc$

(4) $\forall a \in Z$，存在单位元 1，使 $a \cdot 1 = a$

由以上性质可知$(Z, +, \cdot, 0, 1)$构成一个可换群。

1.2 最小数原理

定理 1.1 （最小数原理）：任意一个自然数的非空子集中，必有一个最小数存在。

证明：分两种情况讨论，即这个集合为有限集或无限集。

(1) 若这个集合为有限集，则根据基数理论或序数理论，任何两个自然数都可比大小，因此一定存在最小数，从而结论成立。

(2) 若这个集合为无限集，设为 N，则对 $\forall m \in N$，从 1 到 m 共有 m 个自然数，即 N 中不超过 m 的数最多有 m 个。由于 m 是有限数，所以其中必有一个最小数，记为 h。h 对于 N 中不超过 m 的数来说是最小的，而 N 中其余的数都大于 m，因而也大于 h。因此，h 就是 N 中的最小数。

最小数原理对正有理数、正实数并不适用，它是自然数集的一个重要性质，同时也是数学归纳法的理论依据。

运用最小数原理不难得到最大数原理：

定理 1.2 （最大数原理）：设 M 是 N 的非空子集，若 M 有上界（即存在一个整数 a，使得对 $\forall m \in M$ 都有 $m \leqslant a$），那么一定存在 $m_0 \in M$，使得对 $\forall m \in M$ 都有 $m \leqslant m_0$，即 m_0 是 M 中的最大自然数。

证明：考虑由所有这样的自然数 t 组成的集合 $T = \{t \mid$ 对 $\forall m \in M$，有 $m \leqslant t\}$。由已知条件可得 $a \in T$，说明 T 非空，于是由最小数原理知，集合 T 中有最小数 t_0 存在。

下证 $t_0 \in M$。若 $t_0 \overline{\in} M$，则对任意 $m \in M$，有 $m < t_0$，所以 $m \leqslant t_0 - 1$，这说明 $t_0 - 1 \in T$，这与 t_0 的最小性矛盾。

由 $t_0 \in T$ 且 $t_0 \in M$，从而对 $\forall m \in M$，都有 $m \leqslant t_0$，故取 $t_0 = m_0$，即 m_0 是 M 中最大的自然数。

运用最小数原理还可以证明常用的数学归纳法。

定理 1.3 （数学归纳法原理）：设有一个与自然数 n 有关的命题 $P(n)$，如果

（1）当 $n=1$ 时，$P(n)$ 成立。

（2）假设当 $n=k$ 时，$P(n)$ 成立，则当 $n=k+1$ 时 $P(n)$ 也成立。

那么对一切自然数 n，$P(n)$ 成立。

证明：假设 $P(n)$ 不对一切自然数都成立。令 N 表示使 $P(n)$ 不成立的自然数所组成的集合，则 $N\neq\phi$，根据最小数原理，N 中存在一个最小数 h。且 $h\neq 1$（否则与条件（1）矛盾），因此 $h-1$ 是一个自然数。因为 h 是 N 中最小的，从而 $h-1\notin N$，此即 $P(n)$ 对 $h-1$ 成立；但 $h\in N$ 故 $P(n)$ 对 h 不成立，这与条件（2）矛盾，故 $P(n)$ 对一切自然数 n 都成立。

例 1 （第二数学归纳法原理）设有一个与自然数 n 有关的命题 $P(n)$，如果

（1）当 $n=1$ 时，$P(n)$ 成立。

（2）假设当 $n<k$ 时，$P(n)$ 成立，则当 $n=k$ 时 $P(n)$ 也成立

那么对一切自然数 n，$P(n)$ 总成立。

证明（反证法）：反设定理不成立，并设 T 是 $P(n)$ 不成立的所有自然数组成的集合，T 非空。由最小数原理知集合 T 中必有最小自然数 t_0 存在。由于 $P(1)$ 成立，所以 $t_0>1$，对任意 $n\in N$，当 $n<t_0$ 时，据 T 的定义知必然有 $P(n)$ 成立，由条件（2）知，必有当 $n=t_0$ 时，$P(t_0)$ 也成立，这说明 $t_0\notin T$，矛盾。

如果某一命题不是与所有自然数有关的命题，而是与从 k_0（$k_0>1$）开始的自然数有关，只须把数学归纳原理改为：

（1）当 $n=k_0$ 时，$P(k_0)$ 成立。

（2）假设当 $n=k(k\geqslant k_0)$ 时，$P(n)$ 成立，则当 $n=k+1$ 时，$P(n)$ 也成立。

那么对一切不小于 k_0 的自然数 n，$P(n)$ 都成立。

例 2 用数学归纳法证明：当 $n\geqslant 2$ 时，

$$\frac{4^n}{n+1}<\frac{(2n)!}{(n!)^2}$$

证明：(1) 当 $n=2$ 时，由于 $\frac{16}{3}<\frac{24}{4}$，故不等式显然成立。

(2) 假设当 $n=k(k\geqslant 2)$ 时，不等式成立，即

$$\frac{4^k}{k+1}<\frac{(2k)!}{(k!)^2}$$

易证 $$4(k+1)^2<2(2k+1)(k+2)$$

故 $$0<\frac{4(k+1)}{k+2}<\frac{2(k+1)(2k+1)}{(k+1)^2}$$

因此 $$\frac{4^k}{k+1}\cdot\frac{4(k+1)}{k+2}<\frac{(2k)!}{(k!)^2}\cdot\frac{2(k+1)(2k+1)}{(k+1)^2}$$

$$=\frac{(2k+2)!}{[(k+1)!]^2}$$

即： $$\frac{4^{k+1}}{k+2}<\frac{(2k+2)!}{[(k+1)!]^2}$$

这说明当 $n=k+1$ 时，不等式也成立。

根据(1)(2)知不等式当 $n\geqslant 2$ 时均成立。

例 3 设有 2^n 个球分成了许多堆，我们可以任意选择甲、乙两堆按以下规则进行挪动：若甲堆的球数 p 不少于乙堆的球数 q，则从甲堆拿 q 个球放至乙堆，称为一次挪动，证明可以经过有限次挪动把所有的球合并成一堆。

证明：(1)当 $n=1$ 时，只有两个球。若这两个球在一堆，则命题成立；若不在一堆，则需挪动一次即可。

(2) 假设 $n=k$ 时，命题成立，即 2^k 个球经过有限次挪动可合并成一堆。现证 $n=k+1$ 时，2^{k+1} 个球的命题也成立。

2^{k+1} 个球分成的各堆球数或奇或偶，而奇数个球的堆数必为偶数，否则总球数将是奇数，现把个数为奇数的堆两两配对，每两堆挪动一次，就会使多堆的球数变为偶数，这样每一堆都变成偶数个球。于是设想把每两个球粘在一起看成一个大球，这时就把

2^{k+1}个球变成了 2^k 个大球，由归纳假设这 2^k 个球可挪成一堆。这就说明 $n=k+1$ 时，命题也成立。

由(1)(2)知，命题对 $\forall n \in N$ 都成立。

1.3 鸽笼原理

鸽笼原理最早来源于这样一个事实：将一群鸽子放入到一些笼子中，已知笼子的数量小于鸽子的数量，则必有一个笼子中有两只或两只以上的鸽子。鸽笼原理最早是由德国数学家狄利克雷明确提出来的，因此又叫狄利克雷原理，也称抽屉原理。

定理 1.4　鸽笼原理：设有 n 个集合 A_1、A_2、$\cdots A_n$，m 个元素 a_1、a_2、$\cdots a_m$，其中 $A_i \cap A_j = \phi (i \neq j)$，$\bigcup_{i=1}^{n} A_i = \{a_1, a_2 \cdots, a_m\}$，则必有一个集合至少含有 k 个元素，其中

$$K = \begin{cases} \dfrac{m}{n} & \dfrac{m}{n} \text{为整数} \\ \left[\dfrac{m}{n}\right] + 1 & \dfrac{m}{n} \text{不为整数} \end{cases}$$

其中$\left[\dfrac{m}{n}\right]$表示为不超过$\dfrac{m}{n}$的最大整数

用反证法容易得到证明，在此略去。

特别地：当 $m=n+1$ 时，一般称为鸽笼原理Ⅰ：$n+1$ 个物体放入到 n 个抽屉中，则无论怎么放，必有一个抽屉中至少有两件物体。

当 $m=nr+1$ 时，一般称为鸽笼原理Ⅱ：$nr+1$ 个物体放入到 n 个抽屉里，则无论怎么放必有一个抽屉里至少有 $r+1$ 件物体。

例 1　已知整数 $a_1, a_2, \cdots, a_{10}$，求证必存在一个非 0 整数组 $(x_1, x_2, \cdots, x_n)$，使得对所有的 $x_i \in \{-1, 0, 1\}$，和式 $\sum_{i=1}^{10} x_i a_i$，被 1001 整除。

证明：考虑形如 $g = \sum_{i=1}^{10} x_i a_i$，$x_i \in \{0, 1\}$ 的数，这样的数共有 $2^{10} - 1 = 1023 > 1001$，由鸽笼原理知，必有两个数被 1001 除可得的余数相等，而这两个数的差被 1001 整除，其差仍然形如 $\sum_{i=1}^{10} x_i a_i$，

且 $x_i \in \{-1,0,1\}$

例 2 一个旅馆有 90 个房间，住有 100 名旅客，如果每次都恰有 90 名客人同时回来。证明至少要准备 990 把钥匙分给这 100 名客人，才能保证使得每次客人回来时，每个客人都能用自己分到的钥匙打开一个房间住进去；并且避免发生两人住进同一个房间。

证明：如果钥匙数少于 990；则由鸽笼原理知 90 个房间至少有一个房间的钥匙数小于 $\frac{990}{90}=11$。当持有这个房间钥匙的客人（至多 10 人）都未回来时，此房间就打不开，这样 90 个人无论如何也不能按所要求的方式在这 89 个房间内住下来。

另外，当钥匙数为 990 时，就可以按所要求的方式住下来，这只须把 90 把不同钥匙分给 90 个人，剩下 10 人每人拿 90 把钥匙（每一个房间一把），那么任何 90 人返回时，都能按要求住进房间。

例 3 任意给定一个 n^2+1 项的实数列，$a_1, a_2, \cdots, a_{n^2+1}$。证明：可以从中选出 $n+1$ 项单调递增或递减的子数列。

证明：在实数列 $a_1, a_2, \cdots, a_{n^2+1}$ 中，对每一个 a_i，从它开始向右寻找能构成递增子列的那些项，把其中最长的递增子列的长度记为 t_i，则相应地有两个数列。

$a_1, a_2, \cdots, a_{n^2+1}$

$t_1, t_2, \cdots, t_{n^2+1}$

如果已有某个 $t_k \geqslant n+1$，则必可以从 $a_k, a_{k+1}, \cdots, a_{n^2+1}$ 中选出长为 $n+1$ 的递增子列；如果所有的 t_i 均小于 $n+1$，故 t_i 只能至多取值为以下几种情况之一：$1,2,3,\cdots,n$，但共有 n^2+1 个元素 t_i，由鸽笼原理知必有 $n+1$ 个数相同。设这 $n+1$ 个数为 $t_{k_1}=t_{k_2}=\cdots=t_{k_{n+1}}$，其中 $1 \leqslant k_1 < k_2 < \cdots < k_{n+1} \leqslant n^2+1$，其对应的 $a_{k_1}, a_{k_2} \cdots, a_{k_{n+1}}$ 必然满足 $a_{k1} \geqslant a_{k2} \geqslant \cdots \geqslant a_{k_{n+1}}$，否则若当 $k_i < k_j$ 时，有 $a_{ki} < a_{kj}$，则就有 $t_{ki} < t_{kj}$，这与 $t_{ki}=t_{kj}$ 矛盾。由此可知一定存在 $n+1$ 个元素单调递减子列。