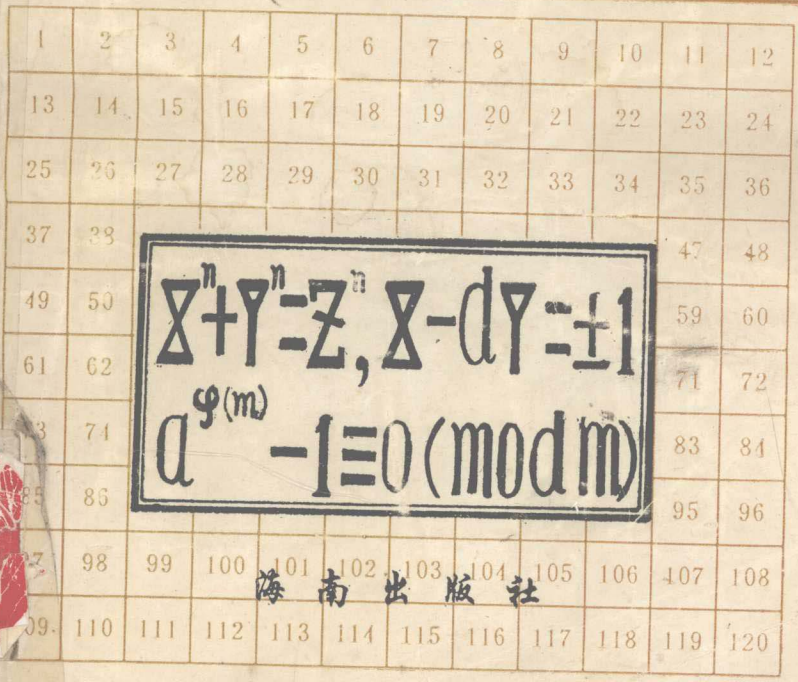
初等数论

何国樑 肖振纲 编



海南出版社

初等数论

何国棵
肖振纲 编

海南出版社

内 容 提 要

本书内容包括整数的整除性、数论函数、不定方程、同余式、二次同余式与平方剩余、原根与指标等七章. 较为详细的介绍了初等数论的基本内容，并紧密联系数学竞赛，书中有较多的例题和习题，书末附有习题的提示与解答. 本书可作为高等师范院校数学专业本、专科学生或综合性大学相应专业学生初等数论课的教材，也可作为数学竞赛的参考资料.

初 等 数 论

何国樑 肖振纲 编著

责任编辑：苏 斌
封面设计：达 维

*

海南出版社出版 湖南省新华书店经销
湖南省统计局机关印刷厂印刷

*

开本：787×1092 1/32 印张：10.5 字数：240千字
1992年12月第1版 1992年12月第1次印刷 印数：1—4000册

*

ISBN7—80590—357—3/G.211
定价：5.95元

序　言

数论是一个古老而又生气盎然的数学分支，察其源可上溯到公元前六世纪或者更早些．按所使用的数学工具，数论又可分为初等数论、解析数论、代数数论和几何数论．

解析数论所使用的是数学分析的工具，它与实变函数有着紧密的联系，其奠基人是大数学家欧拉(Euler)．切比雪夫(Чебышев)、狄里克雷(Dirichlet)、哈代(Hardy)等人发展了欧拉的工作．代数数论的基本概念是代数数，即整系数方程

$$a_0x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0$$

的根．数学大师高斯(Gauss)以及拉格朗日(Lagrange)等人在这方面有巨大的贡献．几何数论研究的对象是空间网格(或说格点、整点)，其创始人是闵科夫斯基(Minkowski)和沃洛诺伊(Вороной)．空间格点对几何学与结晶学有极大的意义，与它的研究紧密相关的是二次型的算术理论．

初等数论所使用的方法主要是算术的，因此许多被喻为"皇冠"的世界著名难题，象哥德巴赫(Goldbach)猜想、费尔马(Fermat)大定理等，只要具有初中文化水平的人经过一番自学都能理解它的含意，正因为如此也就吸引了许多年青人意欲一试摘取"皇冠"的喜悦．这种心情是多么的美好，其勇敢精神实堪嘉许．然而科学来不得半点虚假，要摘取"皇冠"，首先应有扎实的数学基础知识，并研读许多精深的数论文献，再加上刻苦钻研的精神和坚韧不拔的毅力，才有可能从事这方面的研究，问鼎"皇冠"．

尽管如此，数论仍然是一门十分活跃的数学分支.数论研究的发展曾对许多数学分支的发展产生过积极的影响，因此，在它的周围吸引着许多优秀的科学家.特别是这些年来兴起的国际、国内的各种数学竞赛中，数论试题更是屡见不鲜，这无疑对数论研究家族的兴旺发达起了推波助澜的作用.

数论的发展源自古希腊对形数的构思.公元前五、六世纪毕达哥拉斯(Pythagoras)学派创立了原始数论，他们对完全数、亲和数、素数及整除性的讨论对后世的影响是十分著巨的.公元前三世纪欧几里得(Euclid)又证明了素数的个数是无穷的，并给出了计算两个正整数的最大公约数的方法(Euclid 算法).丢番图(Diophantus)增添了不定方程的问题.我国古代的《孙子算经》中给出了解一次同余式组的算法，即著名的孙子定理(国外把它叫做中国剩余定理).多少世纪以来数论研究始终是一个不衰的主题，十七世纪至十九世纪，由于实际的需要促使人们在计算上、数学符号体系上和方程的理论上取得进展，而对纯数学问题的兴趣更激发了对数论的深入研究.正如当代数论大师哈代(Hardy 1877—1947)所说"数论的诞生，比数学中的任一分支都含有更多的实验科学的气味，它的著名定理都是先猜出来的，有时等了一百年甚至百余年才得到证明；它们的提出，也是凭着一大堆计算上的证据.……"这期间几乎所有的主要数学家都在数论方面作出过一些猜想并指出一些事实.如费尔马、欧拉、勒让德(Legendre)、高斯等，他们的工作大大地丰富和发展了数论的内容.特别值得一提的是费尔马和高斯.费尔马是个律师，数学只不过是他的业余爱好，但他对数论这门学科的贡献却是广泛的，也是可观的，他是第一个给数论发展以巨大推动力的欧洲人.高斯于 1801 年出版了著名的《算术探讨》，在这本

书中高斯证明了二次互反律以及原根存在的充要条件等重要结果.也正是他们的这些工作大体上构成了当今初等数论教科书的基本内容.当然，初等数论的内容远非这些，特别是近几十年来，初等数论在计算机科学、组合数学、代数编码、信号的数字处理等领域得到了广泛的应用.

要在一本数论入门书里囊括全部的内容是不切实际也是不可能的，但是我们注意了如下几点：

第一　本书旨在为大专院校数学系学生或中学数学教师提供一本数论的入门书，因此在内容的安排上，力求简捷、通俗易读，除个别地方外，我们不假定读者已具有大学一年级以上的数学修养；

第二　考虑到初等数论的一些基本知识，如整除性、最大公因数与最小公倍数、素数、整数的标准分解式、同余式、简单的不定方程以及某些数论函数都已列入国际或国内的数学竞赛中，本书在叙述这些问题时尽可能朝这个方向靠拢，这也许是本书的最大特点之一；

第三　考虑到许多对数论感兴趣的数学爱好者的自学成才，我们在每节后面配有一定数量的习题，它们是本书内容的延续，或说是有机整体的一部分，读者当不会掉以轻心.书后附有习题的详细解答，我们当然不希望读者一开始就去翻阅它们；

第四　在介绍那些经典结论时，我们力图介绍新的证明方法以及近代的进展.本书是为师范院校本、专科数学系学生一个学期初等数论课而编写的，也可作为其他院校初等数论课的参考书或教材，部分内容还可作为在教师指导下中学生的课外读物，特别是那些有志于参加数学奥林匹克竞赛的学生.

后面所列参考文献，可供读者在阅读本书时参考．我们在编写过程中，亦从它们那里获益匪浅，在此一并致谢．

本书大部分是在我们多年讲授初等数论课的讲义的基础上修改而成的，如果本书的出版能使读者有所得益的话，那将是我们的最大安慰．限于水平，漏误之处敬请读者指正．

作　者

一九九二年二月于湖南师范大学

目　录

第一章　整数的整除性

数论是研究数的性质的一门学科，特别是初等数论，可以说是算术的继续，它所研究的对象是整数. 整数的整除性在数论中有如极限在数学分析中的地位.

本章将由带余除法开始介绍整除性的概念，再由辗转相除法导出最大公约数和最小公倍数，最后介绍素数与合数，从而证明算术基本定理.

§1.1　带余除法

两个整数的和、差、积仍然是整数，然而用一个整数除以另一个非零整数所得的商却不一定是整数.

定义 1　设 a、b 是两个整数，其中 $b\neq 0$，如果存在一个整数 q，使得等式

$$a=bq \tag{1}$$

成立，则称 b 整除 a，记作 $b\mid a$，并称 b 为 a 的因数，a 为 b 的倍数.

如果对于任意的整数 q，(1)式均不成立，则称 b 不整除 a，记作 $b\nmid a$.

如果 $b\mid a$，但 $b\neq \pm 1$、$\pm a$，则 b 叫做 a 的真因数. 特别地，当 $2\mid a$ 时，a 叫做偶数；$2\nmid a$ 时，a 叫做奇数.

容易从定义出发，证明整除的如下基本性质：

定理 1 设 $b\neq 0$，$c\neq 0$，那么

Ⅰ) 若 $b|a$，$c|b$，则 $c|a$；

Ⅱ) 若 $b|a$，则 $bc|ac$；

Ⅲ) 若 $b|a$，则 $b||a|$，反之亦然；

Ⅳ) 若 $b|a$，$a\neq 0$，则 $|b|\leqslant|a|$；

Ⅴ) 若 b 是 a 的真因数，则 $1<|b|<|a|$；

Ⅵ) 若 $b|a_i(i=1,2,\cdots,n)$，则对任意 n 个整数 $k_i(i=1,2,\cdots,n)$恒有

$$b|k_1a_1+k_2a_2+\cdots+k_na_n;$$

Ⅶ) 若 $b|a$，$a\neq 0$，则 $\frac{a}{b}|a$.

证明 仅证Ⅰ)、Ⅵ)，其余的留给读者练习.

Ⅰ) 因 $b|a$，$c|b$，由定义，存在两个整数 q_1，q_2，使得 $a=bq_1$，且 $b=cq_2$. 故有 $a=c(q_1q_2)$，而 q_1q_2 是整数，由定义得 $c|a$；

Ⅵ) 由 $b|a_i$ 知，存在整数 q_i，使得 $a_i=bq_i(i=1,2,\cdots,n)$，因此

$$k_1a_1+k_2a_2+\cdots+k_na_n=b(k_1q_1+k_2q_2+\cdots+k_nq_n)$$

而 $k_1q_1+k_2q_2+\cdots+k_nq_n$ 是整数，故 $b|k_1a_1+k_2a_2+\cdots+k_na_n$. ■

整除的这些基本性质虽然简单，但却应用广泛.

例 1 设 a，b，c，d 都是整数，且 $a-c|ab+cd$. 求证，

$$a-c|ad+bc.$$

证明 因 $a-c|ab+cd$，显然 $a-c|(a-c)(d-b)$，由定理 1 (Ⅵ)即知 $a-c|ab+cd+(a-c)(d-b)$，而 $ab+cd+(a-c)(d-b)=ad+bc$，故 $a-c|ad-bc$. ■

例 2 证明 $7|2222^{5555}+5555^{2222}$.

证明 因 $2222=7\cdot 318-4$，$5555=7\cdot 793+4$，所以

$$2222^{5555}+5555^{2222}$$
$$=(2222^{5555}+4^{5555})+(5555^{2222}-4^{2222})-(4^{5555}-4^{2222})$$

而

$$2222+4\mid 2222^{5555}+4^{5555},\ 7\mid 2222+4,$$
$$5555-4\mid 5555^{2222}-4^{2222},\ 7\mid 5555-4,$$

由定理 1 Ⅰ)，$7\mid 2222^{5555}+4^{5555}$，

$$7\mid 5555^{2222}-4^{2222}$$

又 $4^{5555}-4^{2222}=4^{2222}(4^{3333}-1)$，而 $4^3-1\mid 4^{3333}-1$，$7\mid 4^3-1$，所以 $7\mid 4^{5555}-4^{2222}$. 由定理 1 Ⅴ)即知

$$7\mid 2222^{5555}+5555^{2222}.\ \blacksquare$$

例 3 试求三个大于 1 的整数，使其中任意两个数之积加 1 能被另一个数整除.

解 设所求三整数为 x,y,z，依题意有正整数 a,b,c，使得

$$xy+1=az \tag{2}$$
$$yz+1=bx \tag{3}$$
$$zx+1=cy \tag{4}$$

由此易知 x,y,z 两两不等. 不失一般性，设 $1<x<y<z$，于是，(2)×(4)可得

$$(ac-x^2)yz=xy+zx+1 \tag{5}$$

由于 $1<x<y<z$，所以 $xy+1\leqslant yz$，$xz<yz$，于是 $xy+zx+1<2yz$，再由(5)式得，$(ac-x^2)yz<2yz$，因此

$$ac-x^2<2$$

另一方面，由于 x、y、z 都是正整数，由(5)式可知 $ac-x^2>0$，但 $ac-x^2$ 为整数，因而必有 $ac-x^2=1$，这样，(5)式变为

$$yz=xy+zx+1 \tag{6}$$

代入(3)式，得 $x(b-y-z)=2$，所以 $x\mid 2$，又 $x>1$，故 $x=2$. 将 x

$=2$ 代入(2)式，得 $2y+1=az$，由 $y<z$，知 $y+1\leqslant z$，于是

$$az=2y+1<2y+2\leqslant 2z$$

而 a 为正整数，所以 $a=1$，即有

$$z=2y+1 \tag{7}$$

将(7)及 $x=2$ 代入(6)式得 $y=3$，再由(7)式得 $z=7$，不难验证 2,3,7 三数满足题设要求，故所求三数为 2,3,7. ■

前面对整除的情形作了初步的讨论，一般来说，有

定理 2 (带余除法)设 a、b 是两个整数，其中 $b>0$，则存在唯一的一对整数 q，r，使得

$$a=bq+r,\ 0\leqslant r<b \tag{8}$$

成立.

证明 存在性 当 $a=0$ 时，命题显然成立.

若 $a>0$，由 *Archimedes* 公理，必存在整数 q，使得

$$bq\leqslant a<b(q+1)$$

因而 $0<a-bq<b$，令 $a-bq=r$，即得(8)式；

若 $a<0$，命 $a'=-a$，同样可得(8)式，从而存在性得证.

唯一性 设整数组 q、r 和 q_1、r_1，都满足(8)式，即

$$a=bq+r \qquad 0\leqslant r<b$$

$$a=bq_1+r_1 \qquad 0\leqslant r_1<b$$

从而 $(q-q_1)b=r_1-r$ $(0\leqslant|r_1-r|<b)$. 于是 $|q-q_1|b=|r_1-r|<b$，因此 $0\leqslant|q-q_1|<1$，而 q，q_1 都是整数，所以 $|q-q_1|=0$，即 $q_1=q$，进而 $r_1=r$. 即满足(8)式的整数 q，r 是唯一的. ■

定义 2 在式(8)中，q 叫做 a 除以 b 所得的不完全商；r 叫做 a 除以 b 所得的最小非负剩余，简称余数，记作 $\langle a\rangle_b$.

定理 2 是初等数论中的一个最基本的定理，整数理论中许多命题的证明都是建立在这个定理的基础之上的.

例 4 设 ax_0+by_0 是形如 $ax+by$(x,y 是任意整数，a,b 是两个不全为零的整数)的数中的最小正数，试证，对任意整数 x、y，恒有 $ax_0+by_0 \mid ax+by$.

证明 对任意整数 x,y，由定理 2，存在唯一的一对整数 q，r，使得

$$ax+by=(ax_0+by_0)q+r,\ 0\leqslant r<ax_0+by_0$$

若 $r\neq 0$，则 $0<r<ax_0+by_0$，且

$$r=a(x-x_0q)+b(y-y_0q)$$

而 $x-x_0q$ 与 $y-y_0q$ 皆为整数，这说明 r 是一个比 ax_0+by_0 还要小的形如 $ax+by$ 的正数，这与 ax_0+by_0 的最小性矛盾，因此必有 $r=0$，故 $ax_0+by_0 \mid ax+by$. ■

例 5 设整数 $g>1$，试证任一正整数 a 能够唯一地表示为

$$a=a_ng^n+a_{n-1}g^{n-1}+\cdots+a_1g+a_0 \tag{9}$$

其中整数 $n\geqslant 0$，a_i 为整数，且 $0\leqslant a_i<g$，$i=0,1,\cdots,n$，$a_n>0$.

证明 先用数学归纳法证明 a 可以表示为(9)的形式.

当 $a<g$ 时，令 $n=0$，$a_0=a$ 即有(9)式.

设小于 $a(a\geqslant g)$的任意正整数都可以表示为(9)的形式，须证 a 也可以表示为(9)的形式. 事实上，因 a,g 均为正整数，故由定理 2 知必有两非负整数 q,a_0，使得

$$a=qg+a_0,\ 0\leqslant a_0<g \tag{10}$$

且由 $a\geqslant g>1$ 知，$1\leqslant q<a$，由归纳假设

$$q=a_ng^{n-1}+a_{n-1}g^{n-2}+\cdots+a_2g+a_1$$

其中 $n\geqslant 0$，$a_n>0$，$0\leqslant a_i<g$，$i=1,2,\cdots,n$，代入(10)式即得

$$a=a_ng^n+a_{n-1}g^{n-1}+\cdots+a_1g+a_0$$

这就证明了任一正整数 a 可以表示为(9)式.

再证唯一性，设另有

$$a=b_m g^m+b_{m-1}g^{m-1}+\cdots+b_1 g+b_0 \tag{11}$$

其中 $m\geqslant 0$，$b_m>0$，$0\leqslant b_i<g$，$i=0,1,\cdots,m$，下面证明 $m=n$ 且 $b_i=a_i$，$i=0,1,\cdots,n$.

事实上，若 $m\neq n$，不失一般性，设 $m<n$，则 $m+1\leqslant n$，由于 $0\leqslant b_i\leqslant g-1$，$i=0,1,\cdots,m$，$a_m\geqslant 1$，$a_j\geqslant 0$，$j=0,1,\cdots,n$，有

$$\begin{aligned}a&=b_m g^m+\cdots+b_1 g+b_0\leqslant(g-1)(g^m+\cdots+g+1)\\&=g^{m+1}-1<g^{m+1}\leqslant a_n g^n\leqslant a\end{aligned}$$

矛盾. 因此必有 $m=n$.

将(9)、(11)两式相减可得

$$a_n g^n+\cdots+a_1 g-(b_n g^n+\cdots+b_1 g)=b_0-a_0 \tag{12}$$

由此可知 $g\mid b_0-a_0$，但 $0\leqslant|b_0-a_0|<g$，因而必有 $b_0-a_0=0$，即 $b_0=a_0$，再由(12)式可得

$$a_n g^{n-1}+\cdots+a_2 g-(b_n g^{n-1}+\cdots+b_2 g)=b_1-a_1$$

同理可得 $b_1=a_1$，$\cdots$，$b_n=a_n$. ■

例 4 是数的 g 一进制表示的理论依据.

习 题 1·1

1. 已知 $p\mid 10a-b$，$p\mid 10c-d$，求证：$p\mid ad-bc$.

2. 证明，对任一正整数 n，恒有 $17\mid 3\cdot 5^{2n+1}+2^{3n+1}$.

3. 证明，$7\mid 4444^{3333}+3333^{4444}$.

4. 设 m,n 皆为正整数，求证：$m^2\mid(m+1)^n+m(m-1)n-1$.

5. 设 m,n 都是正整数，且 $n\geqslant 2$. 证明，$(n-1)^2\mid n^m-1$ 的充要条件为 $n-1\mid m$.

6. ξ 是一个 n 次单位根，m 是使得 $\xi^m=1$ 成立的最小正整数，证明 $m\mid n$.

7. 设 a,b 是两个整数，且 $b\neq 0$，则存在两个整数 s,t，使得

$$a=sb+t,\ |t|\leqslant\frac{1}{2}|b|$$

且当 b 是奇数时，s,t 是唯一的，但当 b 是偶数时，s,t 不唯一.

8.（北美数学竞赛试题）证明，每一个整数都可以表示为 $x^2+y^2-5z^2$ 的形式，其中 x,y,z 为整数.

9. 证明，任意 $n(n\geqslant 1)$ 个相继整数中，有且仅有一个数能被 n 整除.

10.（1936 年匈牙利数学竞赛试题）试证，对于任意给定的正整数 n，必有唯一的一对整数 k,l，使得

$$n=\frac{1}{2}k(k-1)+l,\ 0\leqslant l<k.$$

§1.2 最大公因数与辗转相除法

在上一节的基础上，我们来讨论两个或两个以上整数的最大公因数的存在性及其求法.

定义 1 设 $a_1,a_2,\cdots,a_n(n\geqslant 2)$ 是 n 个整数，若整数 d 是这 n 个数中每一个数的因数，则 d 叫做这 n 个整数的一个公因数.

由于 1 是任意整数的因数，且任何非零整数的因数只有有限个，因此，我们有

定义 2 不全为零的 $n(n\geqslant 2)$ 个整数 $a_1,a_2,\cdots,a_n$ 的一切公因数中的最大数叫做这 n 个整数的最大公因数，记作 $(a_1,a_2,\cdots,a_n)$.

显然，$(a_1,a_2,\cdots,a_n)\geqslant 1$.

定义 3 如果 $(a_1,a_2,\cdots,a_n)=1$，则称整数 $a_1,a_2,\cdots,a_n$ 互素，若 $a_1,a_2,\cdots,a_n$ 中任意两个整数都互素，则称 $a_1,a_2,\cdots,a_n$ 两