理科骨干教师拓展读物

初等数论

主编 晏能中

CHUDENGSHULUN

电子科技大学出版社

理科骨干教师拓展读物

初等数论

主编　晏能中

电子科技大学出版社

初等数论

主编　晏能中

出　　版:电子科技大学出版社(成都建设北路二段四号)
责任编辑:张　俊
发　　行:电子科技大学出版社
印　　刷:北京市朝教印刷厂
开　　本:850mm×1168mm　1/32　　印张:8　　字数:162千字
版　　次:1992年1月第一版
印　　次:2005年10月第二次印刷
书　　号:ISBN 7-81016-361-2/O·9
定　　价:19.00元

前　言

有一位数学家曾这亲说过："用以发现数学天才，在初等数学中再也没有比数论更好的课程了。任何学生，如能把当今一本数论教材中的练习做出，就应受到鼓励，劝他将来去从事数学方面的工作"。近十年来，在国际国内中学数学竞赛题中，都少不了数论方面的题，所以不少师范院校和高等师范专科学校都先后开设了《初等数论》课程。但适合师范（师专）院校的特点，又结合奥林匹克数学竞赛和中学数学教学的实际的《初等数论》教材，却非常匮乏。为了尽快改变这种状况，从师专层次的教学实际出发我们编写了这本教材。在编写过程中，注意了系统性、思想性、科学性、通俗性、应用性；注意了讲清基础知识，基本理论和基本方法，特别注意了理论联系实际和少面精的原则，尤其是联系中学数学和奥林匹克数学竞赛的实际。本书相当一部分例题和习题都是从国内外中不数学竞赛试题中，精选出来的。本书还介绍了数论方面的一些新成就和尚未解决的一些问题以及有关数论方而后的一些历史知识，以开拓学生视野，激发学生的学习热情。本书可作为师专、教院和函数专科数论教材，也可供中学数学师和基他数学工作者参考。

参加本书编写的有达县师专晏能中，去南昆明师专郭卫舵，

万县师专潘杰，宜宾师专王国炳，镇江师专张有德，微州师专孙永铉，重庆教育学院费锡樽，重庆师专姜久亮。

本书最后由宜宾师专五国炳审稿并作了一些修改。

本书在编写过程中，得到了西南蛹大严栋开教授的大力支持和热情指导，在此表示谢意。

限于水平，本书错误和缺点在所难免，欢迎读者批评指正。

编者

目　录

第一章　整数的整除性

整数的整除性是研究整数性质的一个重要内容，很多性质都直接或间接地与可除性有关。本章从整除的概念出发，讲述整除的性质、带余除法、最大公约数与最小公倍数、算术基本定理及几个常见的数论函数，最后介绍逐步淘汰原则和鸽舍原理。

§1　整除概念和性质

形如 1,2,3,…的数称为自然数。

形如…,−3,−2,−1,0,1,2,3,…的数称为整数。

很显然，自然数就是正整数。在正整数范围内，两个正整数之和仍是正整数，两个正整数之积仍是正整数。在整数范围内，两个整数之和仍是整数，两个整数之积仍是整数，两个整数之差仍为整数。但整数除整数之商，就不一定是整数，这正是我们要研究的整数的整除性。

我们常用 $a,b,c,\cdots$ 表示整数，用 ab 表示整数 a 乘以整数 b。下面给出整除的概念。

定义　设 $a,b\in Z$（$\in$ 表示属于，Z 表示整数集）且 $b\neq 0$，如果 $\exists c\in Z$（$\exists$ 表示存在），使得 $a=bc$，我们就称 b 是 a 的约数，a 是 b 的倍数，叫做 b 整除 a，用 $b\mid a$。表示。$b\times a$。表示 b 不能整除 a。

在 $a=bc$ 中，当 $b\neq\pm a, b\neq\pm 1$ 时，则 b 称为 a 的真约数，即 a

的约数除$\pm a$，± 1外，其余的约数称为a的真约数。$\pm a$，± 1称为a的平凡因数，其余的叫a的非平凡因数(如果有的话)。

由整除的定义，我们有：

1)整除具有反身性，即$\forall a(a\neq 0)\in Z$($\forall$表示任意)，有$a|a$。故a是a的约数，也是a的倍数。

2)整除具有传递性，即若$c|b, b|a\Rightarrow c|a$(⇒表示能推出)。

3)整除不具有对称性，即$b|a$，但a不一定能整除b。

另外由整除的定义可得：

(1)1是任意整数的约数，即1|a。

(2)0是任意整数a的倍数，即a|0。

(3)若$b|a\Rightarrow bc|ac$。

(4)若$c|a, c|b\Rightarrow$对$\forall$ m，n$\in$Z有c|$(ma+nb)$(此性质，称为整除的组合性质)。

性质(4)可以推广为：

定理1 若$b|a_1, b|a_2, \cdots, b|a_n$，则$b|(K_1a_1+K_2a_2+\cdots+K_na_n)$，其中$K_i, a_i, b\in Z$，且$b\neq 0, i=1,2,\cdots,n$。

证明 因$b|a_1, b|a_2, \cdots, b|a_n\Rightarrow a_1=c_1b, a_2=c_2b, \cdots, a_n=c_nb$ $(c_i\in Z, i=1,2,\cdots,n)\Rightarrow K_1a_2=K_1c_1b, K_2a_2=K_2c_2b, \cdots, K_na_n=K_nc_nb\Rightarrow(K_1a_1+K_2a_2+\cdots+K_na_n)=b(K_1c_1+K_2c_2+\cdots+K_nc_n)\Rightarrow b|(K_1a_1+K_2a_2+\cdots+K_na_n)$。□(□表示证毕)。

定理2 (带余除法)设$a, b\in Z$且$b\neq 0$，则$\exists .1$($\exists .1$表存在唯一的)的q，r$\in$Z，使得a=bq+r，$0\leqslant r<|b|$。

证明 如果$b>0$，则b的倍数由小到大排列出是：

$\cdots, -4b, -3b, -2b, -b, 0b, b, 2b, 3b, 4b, \cdots,$

如果 $b<0$，则 b 的倍数从小到大排列出是：

$\cdots,4b,3b,2b,b,0b,-b,-2b,-3b,-4b,\cdots$

用 a 与之比较有两种情况：

1) $\exists q\in Z$，使得 $a=qb\Rightarrow r=0$。

2)当 $b>0$ 时，$\exists q\in Z$，使得 $qb\leqslant a<(q+1)b$，即 $qb\leqslant a<qb+b\Rightarrow 0\leqslant a-bq<b$。

当 $b<0$ 时，$\exists q\in Z$，使得 $qb\leqslant a<(q-1)b$，即 $qb\leqslant a<qb-b\Rightarrow 0\leqslant a-qb<-b$。

由此，可得

$$0\leqslant a-qb<|b|=\begin{cases}b & (b>0)\\ -b & (b<0)\end{cases}$$

令 $a-qb=r\Rightarrow a=qb+r,0\leqslant r<|b|$。这就证明了 q 和 r 的存在性，下面证明唯一性。

设 $a=bq+r,0\leqslant r<|b|$，$a=bq_1+r_1,0\leqslant r_1<|b|$，两式相减得：

$$0=b(q-q_1)+(r-r_1)$$

即 $-b(q-q_1)=T-T_1\Rightarrow b|(r-r_1)$，但 $|r-r_1|<|b|\Rightarrow r-r_1=0\Rightarrow r=r_1$，从而 $q=q_1$。□

利用整除的组合性质，我们可以得到一个整数 a 能被 2 和 5，4 和 25，8 和 125，7 和 11、13 整除的特性。

1)被 2 和 5 整除的特征是末位数能被 2 或 5 整除。

2)被 4 和 25 整除的特征是末两位数表示的数能被 4 或 25 整除。

证明 设 a 为 n 位数，即

$$a=a_{n-1}a_{n-2}\cdots a_2a_1a_0$$

$$= a_{n-1}a_{n-2}\cdots a_2 \times 100 + a_1a_0$$
$$= a_{n-1}a_{n-2}\cdots a_2 \times 4 \times 25 + a_1a_0$$

故当 $4 \mid a_1a_0$，或 $25 \mid a_1a_0$ 时，则由定理 1 得 $4 \mid a$ 或 $25 \mid a$。□

3)被 8 和 125 整除特征是末三位数所表示的数能被 8 或 125 整除。证明与 2)相同。

4)被 11 整除的特征是奇数位数字之和与偶数位数字之和的差能被 11 整除。

证明

因 $10 = 11 - 1$

$10^2 = (11-1)^2 = 11$ 的倍数 $+1$

$10^3 = (11-1)^3 = 11$ 的倍数 -1

$10^4 = (11-1)^4 = 11$ 的位数 $+1$

……

$10^{n-1} = (11-1)^{n-1} = 11$ 的倍数 $+(-1)^{n-1}$

故 $a = a_{n-1}a_{n-2}\cdots a_1a_0$

$= a_{n-1}10^{n-1} + a_{n-2}10^{n-2} + \cdots + a_1 10 + a_0$

$= a_{n-1}[11$ 的倍数 $+(-1)^{n-1}] + \cdots$

$+ a_2(11$ 的倍数 $+1)$

$+ a_1(11$ 的倍数 $-1) + a_0$

$= (a_1 + a_2 + \cdots + a_{n-1}) \times 11$ 的倍数

$+ (a_0 + a_2 + a_4 + \cdots)$

$- (a_1 + a_3 + a_5 + \cdots)$

由定理 1 知，若 $11 \mid (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$，则 $11 \mid a = a_{n-1}a_{n-2}\cdots a_1a_0$。□

5)被 7、11 和 13 整除的特征是这个数的末三位数所表示的数与末三位以前的数字所表示的数之差能被 7 或 11 或 13 整除。

证明 设 $a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_110+a_0$

令 $M=a_210^2+a_110+a_0$(是 a 的末三位数字组成的数)。

$N=a_n10^{n-3}+a_{n-1}10^{n-4}+\cdots+a_3$(是 a 载去末三位数字以后,其余数字所组成的数,如 $a=4325321$,$M=321$,$N=4325$)。因而

$$\begin{aligned}a&=N\cdot1000+M\\&=N(1000+1)+(M-N)\end{aligned}$$

如果 N<M,则

$$a=N\cdot1001+(M-N)$$

如果 N>M,则

$$a=N\cdot1001-(N-M)$$

因 $1001=7\times11\times13$,所以 $N\cdot1001$ 能被 7,11 和 13 整除。由定理 1 得:一个整数能被 7,11 和 13 整除的充分必要条件是差 N−M 或 M−N 能被 7、11 和 13 整除。□

6)能被 9 和 3 整除的特征是这个数的各位数字之和能被 9 或 3 整除。

证明 设 $a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_110+a_0$。

因 $10=9+1=9\times1+1$

$10^2=99+1=9\times11+1$

$10^3=999+1=9\times111+1$

……

$10^{n-1}=\underbrace{99\cdots9}_{(n-1个)}+1=9\times\underbrace{11\cdots1}_{(n-1个)}+1$

$$10^n=\underbrace{99\cdots9}_{(n个)}+1=9\times\underbrace{11\cdots1}_{(n个)}+1$$

故 $a=a_n\times9\times\underbrace{11\cdots1}_{(n个)}+\cdots+a_2\times9\times11+a_1\times9\times1+(a_0+a_1+a_2+\cdots+a_n)$

所以 $9|a$ 或 $3|a\Leftrightarrow$(表示当且仅当)$9|(a_0+a_1+\cdots+a_n)$或 $3|(a_0+a_1+\cdots+a_n)$。□

例 1 已知七位数 $a=92xy427$ 是 99 的倍数,求此数。

解 因 $a=92xy427$,而 $99|a\Rightarrow9|a$,又因 $11|99\Rightarrow11|a$。由 $9|a$,$11|a$ 的特征,可以求出 x,y 来。

由 $9|a\Rightarrow9|(9+2+x+y+4+2+7)=18+(x+y+6)9|(x+y+b)$,因 $0\leqslant x\leqslant9,0\leqslant y\leqslant9,\Rightarrow6\leqslant x+y+6\leqslant24$。又因 $x+y+6=9q\Rightarrow q=1,2$(q 只能取 1 和 2)。故得

$$x+y+6=9 \text{ 或 } x+y+6=18$$

由 $11|a\Rightarrow11|(9+x+4+7)-(2+y+2)=11+(5+x-y)\Rightarrow11|(5+x-y)\Rightarrow5+x-y=11q_1$。又因 $0\leqslant x\leqslant9,0\leqslant y\leqslant9\Rightarrow-4\leqslant5+x-y\leqslant14$。故 q_1 只能取 0 和 1,所以 $5+x-y=0$ 或 $5+x-y=11$。

故 $\begin{cases}x+y+6=9\\5+x-y=0\end{cases}$ 解之,得 $x=-1$,不适合。

$\begin{cases}x+y+6=9\\5+x-y=1\end{cases}$ 解之,得 $x=9/2$,不适合。

$\begin{cases}x+y+6=18\\5+x-y=0\end{cases}$ 解之,得 $x=7/2$,不适合。

$$\begin{cases} x+y+6=18 \\ 5+x-y=11 \end{cases}$$ 解之，得 $x=9, y=3$。

所求之数 a=9293427。□

例 2 有一个自然数 n，各位数字之和与 $2n$ 的各位数字之和相同，求证：n 必能被 9 整除。

证明 因 n 与 $2n$ 的各位数字之和相同，所以 9 除 n 与 $2n$ 所得余数相同，因此 $9|(2n-n)=n$，即 $9|n$。□

例 3 设 a 是一个 n 位数，将其数码按逆序重新排列得一新数 a'，试证新数与旧数之差仍是 9 的倍数。

证明 因旧数 a 与新数 a' 的各个数位上数字之和相等，因此 9 除 a 和 a' 所得余数相等，故 $9|(a-a')$。□

例 4 证明如果 n 为奇数，那么 $46^n+296\times13^n$ 能被 1947 整除。

证明 因 $46^n+296\times13^n=46^n-46\times13^{n-1}+46\times13^{n-1}+296\times13^n=46(46^{n-1}-13^{n-1})+(46+296\times13)\times13^{n-1}$。因 n 为奇数，所以 $n-1$ 为偶数，故上式第一个被加数含有 1947 因子，即 $46^{n-1}-13^{n-1}$ 能被 $46^2-13^2=(46-13)(46+13)=1947$ 整除。第二个加数：$46296\times13=2\times1947$，所以 $1947|(46^n+296\times13^n)$。□

习 题 一

1. 证明任一奇数的平方减一恒为 8 之倍数。

2. n 为整数且 $n^2=7q+r, 0\leqslant r<6$，证明 r 只能取 0，1，2，4，而不能取 3，5，6。

3. n 为整数且 $n^3=9q+r, 0\leqslant r<8$，证明 r 只能取 0，1，8。

4. 证明四个连续整数的乘积加 1 恒为完全平方数。

5. n 为正整数，证明 $n^3+(n+1)^3+(n+2)^3$ 必为 9 之倍数。

6. 已知七位数 $62xy427$ 为 99 之倍数，求此数。

7. 已知八位数 $965xyl55$ 是 99 之倍数，求 x，y。

8. n 为任何整数，证明 $3 \mid n(n+1)(2n+1)$。

9. 若 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，则 $(ax_0+by_0) \mid (ax+by)$。

10. 证明 $1+\frac{1}{2}+\cdots+\frac{1}{n}$（$n>1$）及 $\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}$（$n\geqslant 1$）都不是整数。

§2 素数与素数分布

定义 设 $p>1$ 的整数，如果 p 只有 1 和 p 本身为其因数，无其它正整数因数，则称 p 为素数。如果一个正整数除 1 和本身为其因数外，还有其它正整数为其因数，则称这个正整数为复合数。简称合数。

由素数和合数的定义可知，全体正整数分为三类：

(1)1(单位)；

(2)素数；

(3)合数。

素数的概念，可以由自然数集扩充到整数集中去，这样全体整数可以分为四类，除上面三类外，还有零类。

下面我们主要研究一下素数。

1)任何大于 1 的整数 a，都至少有一个素因数。

事实上，如果 a 是一个素数，则 a 的大于 1 的因数，只有一个，就是 a。

如果 a 合数，则 a 除 1 和 a 外，还有其它正因数。假设 b 是这些正因数中最小的，则 b 必为素数，不是合数。先假定 b 不是素数而是合数，所以 b 一定有一个大于 1 的因数 c，由 $c|b, b|a \Rightarrow c|a$，即 c 为 a 的因素。又因 $1<c<b$，这与假设 b 是 a 的大于 1 的最小正因数相矛盾。所以 b 不是合数而为素数。因此 a 的大于 1 的最小因数 b 是素数。

2)如何判断一个正整数 a 是素数?

定理 1 如果 a 是一个大于 1 的整数，而所有$\leqslant\sqrt{a}$的素数都不能整除 a，则 a 为素数。

证明 设 a 为合数，即 $a=a_1a_2$，由假设知：$a_1>\sqrt{a}, a_2>\sqrt{a} \Rightarrow a_1a_2>\sqrt{a}\cdot\sqrt{a}=a$。这与 $a=a_1a_2$ 相矛盾，所以 a 为素数。□

3)如何找出小于某一个正整数的所有素数。

如果 a 是一个不太大的正整数，找出小于 a 的全体素数，其方法较多，我们介绍一种筛选法：

先列出所有 $1<n\leqslant a$ 的整数 n：2,3,4,5,6,7,…,a。

(1)从 2 起，2 以后的 2 的倍数的数划掉。

(2)从 3 起，3 以后的 3 的倍数的数划掉。

(3)从 5 起，5 以后的 5 的倍数的数划掉。

……

这样继续作下去，直到$\leqslant\sqrt{a}$的素数的倍数的数都划掉，剩下来的就是$\leqslant a$ 的所有的素数。

例 找出$\leqslant 50$ 的所有的素数。

解 (1)先列出 2～50 的所有的数。

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50

(2)从 2 起,2 以后的 2 的倍数的数划掉。

(3)从 3 起,3 以后的 3 的倍数的数,全划掉。

(4)从 5 起,5 以后的 5 的倍数的数,全划掉。

(5)从 7 起,7 以后的 7 的倍数的数,全划掉。

因为$\leqslant\sqrt{50}<\sqrt{64}=8$的素数的倍数都划掉,所以余下的:2,3,5,7,11,13,17,19,23,29,31,37,41,43,47 就是要找的全体素数。

4)素数的个数有多少?

定理 2 素数的个数是无限的。

证明 设素数的个数是有限的,共有 n 个,就是 $p_1,p_2,\cdots,p_n$,其中 $p_1=2,p_2=3,p_3=5,\cdots$,令 $a=p_1p_2\cdots p_n+1$,显然 $p_1,p_2,\cdots,p_n$ 不同于 a,也不是 a 的因数,由 1)知:a 必含有素因数 p,且 p 不同于 $p_1,p_2,\cdots p_n$ 中任何一个,这与只有 n 个素数相矛盾。□

5)素数的分布

用前面的筛选法,可以制造出很大的素数表来,由素数表就可以知其素数分布情况:

在 1 到 100 间有 25 个素数;

在 1 到 1000 间有 168 个素数;

在 1000 到 2000 间有 135 个素数;

在 2000 到 3000 间有 127 个素数;