中学数学丛书

洪伯阳

整数的性质及其应用

ZHONGXUE SHUXUE CONGSHU

湖北教育出版社

ZHONGXUE SHUXUE CONGSHU

整数的性质及其应用

洪 伯 阳

湖 北 教 育 出 版 社

中学数学丛书
整数的性质及其应用
洪伯阳
*
湖北教育出版社出版　湖北省新华书店发行
黄冈县印刷厂印刷
787×1092毫米32开本　4.75印张　1插页　105,000字
1983年10月第1版　1983年10月第1次印刷
印数：1—18,500
统一书号：7306·35　定价：0.42元

内 容 提 要

本书初步地介绍了整数的一些基本性质。全书共分六章：整除；质数；整除性判别法；同余理论；不定方程的整数解；中国剩余定理。有关内容在中学通用教材的基础上作了拓广、加深和提高。

本书叙述简明，通俗易懂，适合中学生自学，同时，亦可供中学数学教师教学时参考。

出 版 说 明

为了帮助广大中学生更好地掌握中学数学基础知识，扩大视野，提高能力，我们请湖北省暨武汉市数学学会组织编写了一套《中学数学丛书》. 本丛书《逻辑代数初步》、《线性代数初步》、《概率统计初步》、《微积分初步》四册，已经以湖北人民出版社名义出版，其余各册，改由湖北教育出版社出版.

编 者 的 话

为了帮助广大中学生学习数学基础知识，一九八一年秋，湖北人民出版社委托我们湖北省暨武汉市数学学会推荐介绍作者，组织编写了《逻辑代数初步》、《线性代数初步》、《概率统计初步》、《微积分初步》四本小册子，分别介绍中学数学教材中有关高等数学的初步知识．这一工作，得到大中学校教师的热情支持，并希望以中学生为主要对象，编辑出版一套《中学数学丛书》．根据读者的要求和老师们的意见，出版社约请我会在此基础上主编一套《中学数学丛书》．我们认为，这个工作是很有意义的．于是，发动高等院校及中学的广大数学教师以及教学研究工作者共同讨论，决定了二十几个选题，结合出版社组稿的四种．制定了《中学数学丛书》选题计划．

《中学数学丛书》的编写，围绕中学数学教学大纲和全国统编数学教材，从中学生的学习实际出发，对中学数学知识适当作了拓宽和加深．编写这套丛书的目的，是为了帮助中学生巩固基础知识，加强基本训练，熟练掌握基本技能，培养分析和解决数学问题的能力，提高学习质量．

参加这套丛书编写的，有大专院校的老师和教学研究工作者，以及教学经验丰富的中学教师．编写中充分注意中学生的实际，考虑到他们的实际水平和接受能力，力求写得深入浅出．通俗易懂，使一般水平的学生都能看懂，且学有所得．

《中学数学丛书》共计三十余册，多数小册子内容是和教材相对应的，几本综合性的小册子，是为了帮助同学们掌握数学

概念，学会分析与归纳，寻找解题途径并掌握较好的解题方法而编写的．丛书中每本小册子既相对独立又互相联系．同学们既可系统阅读，也可以根据自己的情况有选择地使用．学习中哪一方面比较薄弱，哪一方面存在疑难，便可选择其中的有关部分阅读．另外，丛书各册编有丰富的练习题、复习题，并附有答案与提示，便于同学们自学，同时对中学教师教学亦有一定的参考作用．

这套丛书出版以后，欢迎读者提出批评与建议，以便我们组织力量进一步修改再版，把这套丛书编好．同时，希望读者对进一步编好中学生课外读物提出宝贵意见．

湖北省暨武汉市数学学会

一九八二年五月

目　录

第一章 整 除

一切数学问题最终都离不开数字计算，而一切数字计算都将导致整数的计算．因此，对于整数的一些基本性质我们有必要作一些初步的介绍，它不仅对于每一个优秀的中学生和数学爱好者是必要的，而且对每一个中学数学教师都是很有益的．

所谓整数，不但包括自然数（正整数）

$$1,\ 2,\ 3,\ \cdots\cdots$$

而且包括零与负整数

$$-1,\ -2,\ -3,\cdots\cdots$$

在本书中，常用小写拉丁字母表示整数．

§1. 带余除法

我们容易看到：两个整数 a 与 b 相加、相减、相乘所得的和、差、积还是整数；但 a 用 b 除（此处 $b\neq 0$）所得的商，可能是整数，也可能不是整数．

如果整数 a 用整数 b 除所得的商是整数，即等式 $a=bq$ 成立，这时也说 a 被 b 整除，或者说 b 整除 a，并简记为：

$$b\mid a.$$

此时 a 叫做 b 的倍数，而 b 叫做 a 的约数．例如 7 能整除 21，就记为 $7\mid 21$，故 21 是 7 的倍数，7 是 21 的约数．

如果整数 a 用整数 b 除所得的商不是整数，就说 a 不能被

b 整除，或者说 b 不能整除 a，此时则简记为：

$$b \nmid a.$$

例如 $3 \nmid 5$，$4 \nmid 2$ 等等.

下面讲两条基本性质：

性质 1 如果 a 是 b 的倍数，b 是 c 的倍数，则必 a 是 c 的倍数.

事实上，由于 a 是 b 的倍数，则有

$$a = q_1 b \tag{1}$$

又由于 b 是 c 的倍数，则有

$$b = q_2 c \tag{2}$$

将(2)式代入(1)式中得

$$a = q_1 q_2 c$$

因为 $q_1 q_2$ 也是整数，故性质 1 得证.

性质 2 如果在一个等式

$$k + h + \cdots + n = p + s + \cdots + t \tag{3}$$

中，除开一项以外，其余的项都是 a 的倍数，那么这一项也必是 a 的倍数.

事实上，不妨设那一项是 k，我们令

$$h = h_1 a,\ \cdots,\ n = n_1 a,\ p = p_1 a,\ s = s_1 a,\ \cdots,\ t = t_1 a$$

将它们代入(3)式中并提公因子就有

$$\begin{aligned} k &= p + s + \cdots t - h - \cdots - n \\ &= (p_1 + s_1 + \cdots + t_1 - h_1 - \cdots - n_1)a, \end{aligned}$$

由于括号里的代数和仍为整数，故性质得证.

为简便起见，下面假定所讨论的对象是非负整数（因为若非负整数的性质讨论好了，对于负整数只相差一个符号问题）.现在来讲一个重要的定理.

定理 1(带余除法) 任意给定两个非负整数 a 和 $b(b \neq 0)$，

则必存在唯一的整数 q 和 r，使得

$$a=bq+r, \qquad 0\leqslant r<b. \tag{4}$$

成立.

证明：今先证整数 q，r 的存在性．设 bq 是 b 的倍数中不超过 a 的最大的一个，并令差 $a-bq=r$，这就得到了上面的(4)式.

再证唯一性：如果除了表示式(4)外还有

$$a=bq_1+r_1, \qquad 0\leqslant r_1<b \tag{5}$$

将(4)，(5)两式相减就有

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

或者写为

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

可见 r_1-r 是 b 的倍数，但要注意 $|r_1-r|<b$，故只能有 $r_1-r=0$．这就得到了 $r=r_1$，因而也得到 $q=q_1$，这就证明了唯一性.

上面(4)式中的 q 叫做 a 用 b 除的不完全商，r 叫做 a 用 b 除的剩余.

例如：设 $b=7$，则我们有

$$a=24，\ 24=7\cdot3+3，\ 0<3<7；$$

$$a=0，\ 0=7\cdot0+0，\ 0=0<7；$$

$$a=35，\ 35=7\cdot5+0，\ 0=0<7.$$

在(4)式中，如果 $r=0$，即 $a=bq$，这就是我们前面所说的 a 能被 b 整除的情形，此时 a 就是 b 的倍数.

非常明显，任何非零整数都存在无穷多个倍数，但只存在有穷多个约数.

为叙述简便计，凡 2 的倍数我们叫做偶数，不是 2 的倍数就称为奇数．由此可见，全部整数就恰好分为偶数与奇数两

类．且任一偶数均可以表写为 $2n$（n 为整数）的形式，任一奇数均可以表写为 $2n+1$ 的形式．

容易看出，关于偶数与奇数的运算可得到以下结论：

两偶数相加、相减、相乘所得的和、差、积仍为偶数．

一偶数与一奇数相加、相减所得的和、差均为奇数；而偶数与奇数相乘之积为偶数．

两奇数相加、相减所得的和、差均为偶数，而奇数与奇数相乘之积仍为奇数．

现在我们来举几个例子．

例 1 设 a_0，a_1，a_2，…，a_n 为整数，若方程

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_{n-1}x + a_n = 0 \qquad (6)$$

有整数根，证明任一整数根均可整除 a_n（这里 $a_n \neq 0$）．

证明：设 $x=c$ 为方程（6）的任一整数根，于是将它代入（6）式并移项就有

$$a_n = -(a_0c^{n-1} + a_1c^{n-2} + \cdots + a_{n-1})c$$

即得知 $c \mid a_n$．

例 2 如果 $(a-s) \mid (ab+st)$，则必 $(a-s) \mid (at+bs)$．

证明：我们考虑作差

$$(ab+st) - (at+bs) = b(a-s) - t(a-s),$$

亦即有

$$(ab+st) - (at+bs) = (a-s)(b-t)$$

由题目已设 $(ab+st)$ 是 $(a-s)$ 的倍数，故根据前面讲的性质 2 即知 $(at+bs)$ 必为 $(a-s)$ 的倍数．

例 3 试证对于任意整数 n 均有

$$3 \mid n(n+1)(2n+1). \qquad (7)$$

证明：我们用 3 去除 n，于是根据定理 1 就可得到

$$n = 3q + r, \qquad r = 0, 1, 2.$$

当 $r=0$ 时，n 是 3 的倍数；当 $r=1$ 时，$2n+1$ 是 3 的倍数；当 $r=2$ 时，$n+1$ 是 3 的倍数．可见对任意整数 n 均有（7）式成立．

例 4　设某城共有 1983 部电话机，问能否限制这些电话机中的每部刚好与另外 3 部用电线连成直通电话．

解：我们不妨试探性的来进行讨论一下．今假定可以按限制的条件连成直通电话，于是可设连接所用电线的总条数为k，由于每一条电线的两端连接着两部电话机，故被连接的电话机(包括重复计算的在内)应共有 $2k$ 部．但由于题设 1983 部电话机限制每部刚好只与另外 3 部相连接，于是可推知相连接的电话机总数(重复的也计算在内)应为 1983×3 部．这样一来，我们就得出等式

$$1983\times3=2k$$

此式左边是一个奇数，而右边则是一个偶数．这个矛盾也就证明了题目限制的条件是不能实现的．

习　题　1.1

1．设 m、n 为任意两个整数，则 $m+n$、$m-n$、mn这三者之中至少有一个必为 3 的倍数．

2．如果 a 为任一奇数，则必 $8\mid(a^2-1)$．

3．如果 $p\mid(10a-b)$ 与 $p\mid(10c-d)$，试证必有 $p\mid(ad-bc)$．

4．如果 a 为偶数，则必 $a=4n$ 或 $a=4n+2$．

5．若 k 为自然数，则当且仅当 $n=4k$ 或 $n=4k-1$ 时，$\frac{1}{2}n(n+1)$ 为偶数．

6．试证 $\log_2 3$ 为无理数．

7．对于任意整数 a、b，试证

$$a^2+(a+3)^2=2b^2$$

均不可能成立．

8．当 $n>1$ 时，试证

$$S=1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$$

不是整数．

9．如果整系数多项式

$$f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_{n-1}x+a_n$$

同时使 $f(0)$，$f(1)$ 均为奇数，试证 $f(x)=0$ 没有整数根．

§2．最大公约数

关于整数的约数(也叫因数)、公约数、最大公约数以及倍数、公倍数、最小公倍数的概念，这是读者在小学算术中就已经接触到的内容，这些内容十分重要．整数中很多重要而又深刻的性质，都是建立在这些概念基础之上的．这一节先讲公约数与最大公约数的定义．

设 c 是 a 的约数，同时也是 b 的约数，即 $c\mid a$，$c\mid b$，则 c 就叫做 a，b 的公约数．由于 a，b 全为 0 时，讨论其公约数没有什么意义，故下面均假定 a，b 不全为零．

在 a，b 的一切公约数中，其中最大的公约数就叫做 a，b 的最大公约数．一般将它简记为 (a, b)．

读者也许要问：对于任意两个不全为零的整数 a，b 是否都存在最大公约数呢？如果存在，有几个呢？下面的性质 1 可以回答这些问题．

性质 1　对于不全为零的整数 a，b，其最大公约数存在

而且唯一．

事实上，在§1中我们就指出：任一非零的数的约数只有有穷个，故不全为0的两个数 a，b 的公约数也只有有穷多个．在有限个数中一定存在最大的，这就证明了最大公约数的存在性．为了证明唯一性，设 d 与 d' 都是 a，b 的最大公约数，由于最大公约数也是公约数，可见当视 d 为最大公约数而视 d' 为公约数时，就有 $d \geqslant d'$，另一方面，当视 d' 为最大公约数而视 d 为公约数时又有 $d' \geqslant d$．故有 $d = d'$．性质完全证明．

非常明显，1是任意两整数 a，b 的公约数，如果 $(a, b) = 1$，就说 a，b 互质．不言而喻，1与任何整数 a 互质，即 $(a, 1) = 1$．

由性质1已经知道，(a, b) 是唯一存在的．但怎样去求出 (a, b) 呢？如果整数 a、b 很小，则用视察法易得出其最大公约数．比如 $(9, 12) = 3$，$(4, 15) = 1$；即9，12的最大公约数是3，而4与15互质．

如果 a、b 较大，一般就不能用视察法求出 (a, b) 了．我们将要介绍一般可行的方法．由于 a、b 不全为0，故不妨设 $b \neq 0$．在没有讲 (a, b) 的求法之前，先讲一点预备知识．

性质 2　在表达式

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

中，则必 $(a, b) = (b, r)$．

事实上，由于 $(a, b) \mid r$，又由于 $(a, b) \mid b$，可见 (a, b) 是 b，r 的公约数，故有 $(a, b) \leqslant (b, r)$．另一方面，由(1)式又有 $(b, r) \mid a$，$(b, r) \mid b$，故推知 (b, r) 也是 a，b 的公约数，因而又有 $(b, r) \leqslant (a, b)$．于是不得不有 $(a, b) = (b, r)$．证毕．

现在我们来介绍两个整数 a、b 的最大公约数的求法，这就是通常所说的辗转相除法．由于这个方法首先见之于古希腊数

学家欧几里德(Euclid，公元前三世纪)所著的《几何原本》第七卷第1，2两个命题，故此法也被称为欧几里德算法. 为了让读者了解得更清楚一些，先举一个例子. 比如要求6174与1078的最大公约数，兹用辗转相除法将计算格式列之如下：

5	6174	1078	1
	5390	784	
2	784	294	1
	588	196	
2	196	98	
	196		

进行的步骤是先用较小的数1078去除较大的数6174，得出余数为784；其次又用784去除前次的除数1078，得出余数为294；再次又用294去除784，得出余数为196；又再次用196去除294，得出余数为98；最后用98去除196，此时余数为0. 于是98（即最后一个不为0的余数）即为所求的6174与1078的最大公约数.

在一般情形下，对于任意两个整数a、b，不妨设$b\neq0$，根据带余除法，可得下列一串等式：

$$\left.\begin{array}{ll}
a=bq_1+r, & 0<r_1<b,\\
b=r_1q_2+r_2, & 0<r_2<r_1,\\
r_1=r_2q_3+r_3, & 0<r_3<r_2,\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\
r_{k-3}=r_{k-2}q_{k-1}+r_{k-1}, & 0<r_{k-1}<r_{k-2},\\
r_{k-2}=r_{k-1}q_k+r_k, & 0<r_k<r_{k-1},\\
r_{k-1}=r_kq_{k+1}. &
\end{array}\right\}\qquad(2)$$