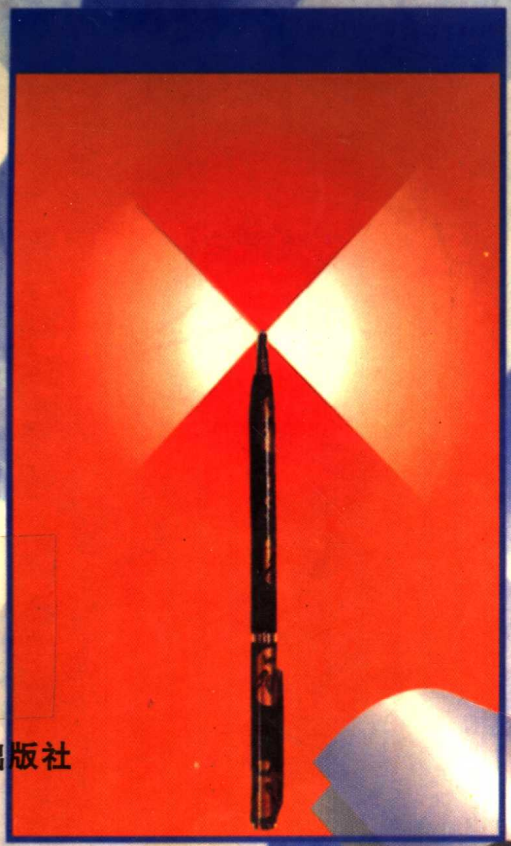
小学教师进修高等师范专科小学教育专业教材
（理科方向）

数论初步

陈肇曾　编



高等教育出版社

小学教师进修高等师范专科小学教育专业教材
（理科方向）

数论初步

陈肇曾　编

高等教育出版社

（京）112号

图书在版编目（CIP）数据

数论初步/陈肇曾编。—北京：高等教育出版社，1996
小学教师进修高等师范专科小学教育专业教材
ISBN 7-04-005705-0

Ⅰ.数… Ⅱ.陈… Ⅲ.初等数论-高等教育：师范教育-教材
Ⅳ.0156.1

中国版本图书馆CIP数据核字（96）第12171号

*

高等教育出版社出版
北京沙滩后街55号
邮政编码:100009 传真:64014048 电话:64054588
新华书店总店北京发行所发行
复旦大学印刷厂印装

*

开本 850×1168 1/32 印张 6.25 字数 160 000
1996年3月第1版 1996年3月第1次印刷
印数 0001—13 092

定价 6.80元

凡购买高等教育出版社的图书，如有缺页、倒页、脱页等
质量问题者，请与当地图书销售部门联系调换

内容提要

本书是根据作者多年的教学经验写成的，主要内容包括整数的整除性、不定方程、同余与同余式等基础知识。在介绍一些经典结果时，给出了它们的背景及应用。

本书结合小学数学的教学内容，使小学数学内容在理论上和观点上得到提高，可供小学教师进修高等师范专科选作教材。

前　言

本教材由上海市教育委员会师资处组织编写，供小学教师进修成人高等师范专科小学教育专业理科方向使用.

设置小学教师进修成人高等师范专科小学教育专业是以中国教育“面向现代化、面向世界、面向未来”为指导，旨在全面提高小学教师的思想政治、职业道德、专业知识、教育理论、教育教学能力、教育教学研究能力等素质，建立一支适应21世纪初等教育改革发展和需要的新型的小学师资队伍.

编写小教育专业的教材，力求从我国社会发展的客观要求和小学在职教师的特点出发，体现时代的先进性和创新性；知识体系的科学性和系统性；师范教育的专业性和综合性；教材内容的应用性和针对性. 编者在编写时尽可能把最新的研究成果吸收并渗透到各课程教材中去；在专业知识的安排上，注意与中等师范及高等师范本科阶段知识结构的衔接；在综合知识方面，针对小学教师既有明确的学科定向，也能兼教其他学科的需要，加强基础，拓宽知识面；在教材的编排体例上，根据小学教师在职、成人、师范教育的特点，安排了学习提要、思考与练习、参考资料等，便于学员业余进修及自学.

为保证教材质量，我们在编写该教材的课程大纲时，请有关专家进行了论证. 在教材完稿后，又请专家进行审定，然后修改完稿.

由于小学教育专业教材的编写是一项全新的工作，不当之处在所难免，希望广大读者和专家给予批评、指正.

上海市教育委员会师资处

1995年6月

目　录

第一章　整数的整除性

整除是数论中的基本概念. 我们将从这个概念出发，引进带余除法与辗转相除法；并以它们为工具，研究最大公约数与最小公倍数的性质. 然后介绍质数的基本性质、算术基本定理及证明. 这些知识是本课程的最基本内容，也是学习后续知识的基础.

第一部分　整除的概念

§1.1　整除、约数与倍数

在小学数学里，我们已经知道，整数 a 除以自然数 b，如果能够得到整数商 q，那么 b 能整除 a. 现在我们把整除概念推广到除数 b 也是整数的情形.

设 a,b 是任意两个整数，其中 $b\neq 0$，如果存在一个整数 q，使得等式 $a=bq$ 成立，我们就说 b 整除 a，或 a 被 b 整除，记作 $b\mid a$.

整数 a 除以整数 $b(b\neq 0)$，如果不能得到整数 q（即对任何整数 q，恒有 $bq\neq a$），那么就叫做 b 不能整除 a（或者说，a 不能被 b 整除），记作 $b\nmid a$.

如果整数 a 能被整数 $b(b\neq 0)$ 整除（即 $b\mid a$），那么 a 就叫做 b 的倍数，b 就叫做 a 的约数.

对于整除、约数和倍数，我们应该注意如下几点：

(1)　整除概念，强调的是整数 a 与整数 b 之间的一种关系——整除关系. 也就是说，a 与 b 之间是否具有整除关系，只要看 a

除以 b 的商是否是整数，而不是看这个整数商的大小.

(2) 约数和倍数是互相依存的，它们不能单独存在. 例如，$18 \div 9 = 2$，$54 \div 18 = 3$，我们不能说“18 是约数”，“18 是倍数”，而应该指出 18 是哪个数的约数，是哪个数的倍数，即必须说成“18 是 9 的倍数”，“18 是 54 的约数”.

(3) 整数 a 的约数个数是有限的，零的约数个数是无限的.

根据约数的定义，对于任意一个整数 a，它的约数只能是绝对值小于、等于 $|a|$ 的整数，而绝对值小于、等于 $|a|$ 的整数的个数是有限的，所以 a 的约数个数是有限的.

对于零来说，由于零除以任何不为零的整数，商都是零，所以任何不为零的整数都是零的约数，而不为零的整数的个数是无限的，因此零的约数个数是无限的.

(4) 对于任何一个整数，它的倍数的个数是无限的.

实际上，对于任何一个整数 a，$0 \cdot a$，$1 \cdot a$，$2 \cdot a$，…，$n \cdot a$(n 为自然数)，… 都是 a 的倍数，所以任意一个整数的倍数的个数是无限的.

由约数与倍数的定义，还可以推得：数 0 是任何不为零的整数的倍数，数 1 是任何整数的约数.

一般地，在整数 a 的约数中，± 1 与 $\pm a$ 叫做整数 a 的当然约数；除 ± 1 与 $\pm a$ 之外，a 的其它约数叫做 a 的真约数(或非当然约数).

根据整除、约数与倍数的定义，可以知道下面六种说法是等价的：

(1) a 能被 b 整除；

(2) b 能整除 a；

(3) b 是 a 的约数；

(4) a 是 b 的倍数；

(5) a 除以 b 的商是整数(即 $a = bq$，q 为整数)；

(6) 存在一个整数 q，使 $a = bq$.

还应该指出的是，在有理数范围内整除与除尽是不同的概念. a 能被 b 整除，a 就一定能被 b 除尽；反之，如果 a 能被 b 除尽，a 不一定能被 b 整除. 实际上，在引进小数之后，两个数（整数或小数）相除，当商是整数或有限小数时，我们就说被除数能被除数除尽，例如，$7 \div 2 = 3.5$，$9 \div 4.5 = 2$，$3.6 \div 0.9 = 4$ 等，这几个算式都说明被除数能被除数除尽，但由于它们不满足“被除数、商是整数，除数是整数”的条件，即不符合整除定义，因此不能说被除数能被除数整除. 但是，如果我们把整除与除尽概念的讨论局限在整数范围内，那么这两个概念是完全一致的，即整除就是除尽，除尽也是整除.

例 1.1　试用列举法写出下列各集合的元素.

$A = \{1$ 的正约数$\}$；　$B = \{18$ 的正真约数$\}$；

$C = \{$不大于 15 的 3 的非负倍数$\}$.

解　$A = \{1\}$；

$B = \{2,3,6,9\}$；

$C = \{0,3,6,9,12,15\}$.

例 1.2　已知非负整数 a 小于整数 $b(b \neq 0)$，且 $b \mid a$，试求 a 的值.

解　因为

$$b \mid a,\ b > a \geqslant 0,$$

所以存在非负整数 q，使

$$a = bq,$$

但是因为 $a < b$，所以有

$$bq < b, b(q-1) < 0,$$

又因为 $b > a \geqslant 0$，所以 $q - 1 < 0$，即 $q < 1$.

因为 q 为小于 1 的非负整数，所以 $q = 0$，因此

$$a = bq = 0.$$

例 1.3　设 a，b 为两个整数，$ab > 0$ 且 $a \mid b$，$b \mid a$，求证：

$$a = b.$$

证明 由 $ab>0$ 可知 a 与 b 同为正整数或同为负整数.

(1) 若 a，b 同为正整数，由 $a|b$，$b|a$ 与整除定义可知，存在整数 q_1,q_2，使得

$$b=aq_1,\quad a=bq_2.$$

由此得
$$b=aq_1=bq_1q_2,\quad q_1q_2=1.$$

因为 a,b 都为正整数，所以 q_1,q_2 是正整数，而 $q_1q_2=1$，因此 $q_1=1,q_2=1$，于是得

$$a=b.$$

(2) 若 a,b 同为负整数，仿(1) 可知存在整数 q_1 与 q_2，使得

$$q_1q_2=1.$$

由于 a,b 同为负整数，所以 q_1,q_2 应同为正整数，所以 $q_1=1$，$q_2=1$，因此 $a=b$.

由例 1.3 可以知道，要证明两个正整数(或负整数)a 与 b 相等，只须证明 a 能被 b 整除，且 b 也能被 a 整除，这就是说，两个互相整除且同号的整数相等. 因此它为我们证明两个整数相等提供了一个方法.

§1.2 带余除法

我们已经知道，一个数除以另一个数，并不一定得到整数商. 如 $14\div5$ 就不存在整数商，它的结果是 $14\div5=2$(余 4). 我们可以把这个式子改写成下面的形式：

$$14=5\times2+4.$$

同时把 14 称为被除数，5 称为除数，2 称为不完全商，4 称为余数.

一般地，我们可以引入下面概念.

已知整数 a 和自然数 b，如果存在整数 q 与 r，使得 $a=bq+r$，并且 $0\leqslant r<b$，那么 a 叫做被除数，b 叫做除数，q 叫做不完全商(有时也简称为商)，r 叫做余数.

求两个数的不完全商 q 和余数 r 的运算叫做带余除法(或有余数除法).

在 $a = bq + r$ 中,如果 $r = 0$,那么 $a = bq$,即 $b|a$; 反之,如果 $a = bq$,那么 $r = 0$. 因此整除可以看作是带余除法中余数为零的特殊情况.

从上面讨论可以看到,带余除法概念是建立在不完全商与余数存在的基础上的. 那么两个数相除,不完全商与余数是否一定存在呢?如果存在,它们是否唯一呢?答案是肯定的. 一般地,我们有下面的结论.

定理 1.1 设 a,b 是两个整数,$b>0$,则一定有并且只有两个整数 q,r 使得

$$a = bq + r, \quad 0 \leqslant r < b$$

成立,而且 q 与 r 是唯一的.

证明 (1) 先证明 q,r 的存在性.

将 b 的倍数由小到大排列,得到如下数列:

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

(i) 如果 a 与数列中某一项,如从 0 起由左到右(或由右到左)第 n 项重合,则取

$$q = n - 1(\text{或 } q = -(n-1)), a = bq,$$

这时 $r = 0$.

(ii) 如果 a 在某两项之间,则存在一个整数 q,使得

$$qb < a < (q+1)b$$

成立. 令 $a - bq = r$,则 $a = bq + r$,而 $0 < r < b$.

由(i),(ii)可知,有两个整数 q,r 使 $a = bq + r$ 成立,这里 $0 \leqslant r < b$.

(2) 再证明 q,r 的唯一性.

设存在另外两个整数 q_1,r_1,等式

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b$$

成立,由于 $a = bq + r$,所以

$$bq + r = bq_1 + r_1,$$

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

两边取绝对值，得

$$b|q - q_1| = |r - r_1|,$$

因为 $0 \leqslant r_1 < b, 0 \leqslant r < b$，所以

$$|r_1 - r| < b,$$

又因为 $b \mid |r_1 - r|, |r_1 - r| < b$，由上面例 1.2 可知

$$|r_1 - r| = 0,$$

故

$$r_1 = r.$$

将 $r_1 = r$ 代入 $b(q - q_1) = r_1 - r = 0$，而 $b \neq 0$，所以

$$q - q_1 = 0,$$

故

$$q = q_1.$$

这就是说，q, r 是唯一的.

由(1),(2) 可知定理成立.

例 1.4　设 m, n 都不是 3 的倍数，$m > n$，求证：$m + n$ 与 $m - n$ 中有一个且仅有一个是 3 的倍数.

证明　因为 m, n 都不是 3 的倍数，所以 m, n 分别被 3 除，余数将是 1 或 2，即

$$m = 3q_1 + 1 \quad 或 \quad m = 3q_1 + 2;$$

$$n = 3q_2 + 1 \quad 或 \quad n = 3q_2 + 2.$$

(1)　如果 m, n 被 3 除后余数相同，则 $m - n = 3(q_1 - q_2)$，这时 $m - n$ 是 3 的倍数，而 $m + n = 3(q_1 + q_2 + 1) \mp 1$，即 $m + n$ 不能被 3 整除.

(2)　如果 m, n 被 3 除后余数不同，则 $m + n = 3(q_1 + q_2) + 3$，这时 $m + n$ 是 3 的倍数，而 $m - n = 3(q_1 - q_2) \mp 1$，即 $m - n$ 不能被 3 整除.

由(1),(2) 可知结论成立.

例 1.5　已知 2761 除以某自然数，余数不为零，不完全商为

95，求除数与余数.

分析　在 $a=bq+r$ 中，已知 $a=2761, q=95$，要求 b 与 r. 考虑到题设 $0<r<b$ 的条件，可确定 b 的可能取值范围，从而确定 b 的整数值.

解　设除数为 b，余数为 r，则有

$$2761=95b+r, 0\leqslant r<b.$$

由题意可得上式的 $r>0$，所以 $95b<2761$，即

$$b<\frac{2761}{95}, \quad \text{或 } b<29\frac{6}{95};$$

在 $2761=95b+r$ 中，由于 $r<b$. 因此，$2761<95b+b$，即

$$b>\frac{2761}{96}, \quad \text{或 } b>28\frac{73}{96}.$$

因此我们有

$$28\frac{73}{96}<b<29\frac{6}{95}.$$

由于 b 为自然数，所以 $b=29$，这时

$$r=2761-95\times 29=6.$$

例 1.6　有一个自然数，用它去除 63，91，129 得到三个余数之和为 25，求这个自然数.

解　设这个自然数为 a，再设用 a 去除 63，91，129 得到的商分别为 q_1, q_2 与 q_3，余数分别为 r_1, r_2, r_3，则由题意得

$$63=aq_1+r_1 \quad (0\leqslant r_1<a),$$

$$91=aq_2+r_2 \quad (0\leqslant r_2<a),$$

$$129=aq_3+r_3 \quad (0\leqslant r_3<a),$$

将上面三式相加，得

$$283=a(q_1+q_2+q_3)+(r_1+r_2+r_3).$$

因为

$$r_1+r_2+r_3=25<3a,$$

所以

$$a>\frac{25}{3},$$

又因为

$$a(q_1+q_2+q_3)$$

$$=283-(r_1+r_2+r_3)$$

$$= 283 - 25 = 258.$$

而 258 正的约数是 1,2,3,6,43,86,129 与 258，即 $258 = 1 \times 258 = 2 \times 129 = 3 \times 86 = 6 \times 43$，$a > \frac{25}{3}$，所以 a 只能是 258,129,86,43 四个数中的一个.

当 $a = 258$ 或 129 或 86 时，用 a 去除 63,91,129 所得的余数之和都大于 25，因此 a 不能取这三个数，即

$$a = 43.$$

例 1.7　若 $ax_0 + by_0$ 是形为 $ax + by$（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

$$(ax_0 + by_0) \mid (ax + by).$$

证明　由有余数除法，可使

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

由此得

$$\begin{aligned} r &= ax + by - (ax_0 + by_0)q \\ &= a(x - x_0q) + b(y - y_0q), \end{aligned}$$

因此 r 也是形如 $ax + by$ 的数，因为 $ax_0 + by_0$ 是这类数中最小的正数，因此在 $0 \leqslant r < ax_0 + by_0$ 中，必有 $r = 0$，即

$$(ax_0 + by_0) \mid (ax + by).$$

习　题　1.1

1. 什么叫做约数、倍数？哪类数的约数只能是当然约数？哪个数一定是任何自然数的倍数？试举例说明.

2. 一个数的约数个数是有限的吗？一个数的倍数的个数是有限的吗？试说明理由.

3. 判断下列说法正确与否，并说明理由：

“被除数是整数，除数是自然数，商是整数，这种除法叫做整除.”

4. 求 1 ～ 500 的自然数中，19 的倍数有多少？

5. 写出下列各集合里的全部元素.

(1)　$A = \{18\text{ 的约数}\} \cap \{30\text{ 的约数}\}$；

(2)　$B = \{18\text{ 的真约数}\} \cap \{42\text{ 的真约数}\}$；

(3) $C=\{$小于100的15正的倍数$\}\cap\{$小于100的45正的倍数$\}$.

6. 求证：若$b|a$，$d|c$，则$bd|ac$.

7. 有四个不同的自然数，它们中的任意两个数之和是2的倍数，任意三个数的和是3的倍数，为使这四个数之和尽可能地小，这四个数应该分别为多少？

8. 在下面括号内填入适当的整数，使得等式成立.

(1) 71 ÷（　　）=（　　）余4；

(2) 189 ÷（　　）=（　　）余2.

9. 两个数相除商为8，余数为16，被除数、除数、商与余数之和为463，求被除数.

10. 对任意两个整数m与n，试证$m+n$，$m-n$，mn三者中至少有一个是3的倍数.

第二部分　整除性定理

§1.3　和、差的整除性定理

定理 1.2　如果两个数都能被同一个自然数整除，那么它们的倍数和(或差)也能被这个数整除，就是

如果$c|a$，$c|b$，m，n是整数，那么

$$c|(am+bn),\ c|(am-bn).$$

证明　因为$c|a$，$c|b$，所以存在整数q_1，q_2，使得

$$a=cq_1,\ b=cq_2,$$

因此
$$am+bn=cq_1m+cq_2n=c(q_1m+q_2n),$$
$$am-bn=cq_1m-cq_2n=c(q_1m-q_2n).$$

由于q_1m+q_2n，q_1m-q_2n都为整数，所以由整除定义，得

$$c|(am+bn),\quad c|(am-bn).$$

推论 1　如果$c|a$，$c|b$，那么$c|(a+b)$，$c|(a-b)$.