整 数 论

第一卷 第一分册

张德馨 著

中国人民解放军洛阳外国语学院翻印

1980

内 容 提 要

本书讲解了整数论的基础，内容共分八章：第一章——整数的可约性；第二章——数论函数；第三章——同余式；第四章——解同余式；第五章——平方剩余；第六章——解二次同余式；第七章——原根和标数；第八章——一部分不定方程。

书末还附有二表：100以下各质数的原根和标数表；4000以下的质数和它们的最小原根表。

序

多年来想写一本这样的书。这个愿望在中国共产党和中华人民共和国政府号召大力向科学进军和尽可能改善高等知识分子工作条件后的今天实现了。所以我首先应该感谢党和政府给我的鼓励和支持。

这本书可供高等师范学校和综合性大学数学系或数理系作教本用，也可供中学教员和高中毕业生自修之用。

在这本书内有下列几点希读者注意。

第一章内，关于大公约和小公倍的求法，我曾各提出了五种。辗转相减法是我在德国柏林大学数学系听老教授I.Schur的数论课时学来的。混合求法是我个人提出的。

第四章内，关于解一次同余式的第二种解法也是我那时学来的。这个方法在一般的情况下很简捷。比方第四章第3节的例题1实际上只用了一行就把问题解决了。若用其它的方法都不会这样地简捷。

第四章内也曾介绍了孙子定理和黄宗宪的求一术表式。读者可以看出我国前辈数学家在整数论方面的成就。

关于怎么样解出以质数 $p=4n+1$ 为模的二次同余式问题我在第六章第一节内研究出一种求解方法。这个方法能否再改进，希望对此有兴趣的同志共同努力研究。

关于从质数模 p 的原根 g 求出 $p^{\alpha}(\alpha>1)$ 的原根问题，在有些数论书上大致是这样提出的：在0，1，2，…，$p-1$

这些数内必有适当的 k，它能使

$$(g+pk)^{p-1}\not\equiv 1 \pmod{p^2}.$$

这样的数 $g+pk$ 就是 p^α 的原根。这样，若 $k=0$ 满足不了要求时，就得试验 $k=1$ 怎么样。有的书上是这样提出的：若 g 不是 p^α 的原根，则 $g+p$ 一定是 p^α 的原根。这样就只须试验 $k=0$ 就够了。

我在第七章第4节内证明了，若 g 不是 p^α 的原根，则 $g-p$ 一定是 p^α 的原根。这与 $g+p$ 虽然只差一个符号，但因我们在选用 g 时，习惯用正数，故一定是 $|g-p|<|g+p|$。这在计算 $(g-p)^2$，$(g-p)^3$，…，$(g-p)^{\varphi(p^\alpha)}$ 时，将会节省若干劳动力。

关于如何肯定一个数 g 是不是模 m 的原根问题，И.М. Виноградов 在他的数论基础第六章第3节内提出了一个办法（可参考裘光明的中译本）。根据这个办法，他在计算出 2^3，2^{20}；3^3；4^3，4^{20}；5^3，5^{20}；6^3，6^{20} 这9个数对于模41的最小正同余数后，肯定了6是41的原根。

我在这本书第七章第5节定理16内把这个方法改进了。根据这个定理，只计算 3^8 和 6^8 这两个数对于模41的最小正同余数，就把6是41的原根肯定了。这只是两个8次方的数；而在上边的9个数中还有4个是20次方的数。

写本书时，我无时无刻不在想，怎么能使读者更容易看得懂。因此在文字方面我曾尽力使它接近口语；在讲解方面我曾力求详尽，没把一些证明过程或计算过程简化掉或留给读者，怕给读者造成疑虑和麻烦。

虽然尽了很大的努力想把这本书写得浅显通俗，严密正

确，但是我的能力有限，很可能还有许多缺点和错误，所以我诚恳地希望读者提出批评和指正。

本书原稿曾蒙东北师范大学代数教研室张立仁同志看过，又蒙方嘉琳同志于1957年上半年在数学系四年级以本稿作讲义试教过。他们对本稿都提出了一些宝贵的意见，特在此表示感谢。

张德馨

1957.10.31.

目　录

第 一 章

整数的可约性

§ 1. 约数和倍数

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

这些数叫做自然数。在自然数范围内，很明显是

$$\text{自然数}+\text{自然数}=\text{自然数},$$

$$\text{自然数}\times\text{自然数}=\text{自然数}.$$

但是由自然数减去自然数，不一定得自然数。所以在减法中产生零和负数。因此我们又把自然数叫作正整数，并把

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

这些数叫作负整数。而正整数和负整数再加上零，就统一叫作整数。

整数论是研究整数的性质的。整数论也叫作数论。

在整数范围内，我们得

$$\text{整数}+\text{整数}=\text{整数},$$

$$\text{整数}-\text{整数}=\text{整数},$$

$$\text{整数}\times\text{整数}=\text{整数}.$$

但是整数除整数不一定得整数，当然更谈不上正整数除正整数一定得正整数。究竟什么样的整数除什么样的整数才能得整数呢？研究这个问题，就是研究整数的可约性。这就是数论的开端。

以后若不特别声明，我们将用

$$a,\ b,\ c,\ \cdots \text{或} x,\ y,\ z,\ \cdots \text{或} \alpha,\ \beta,\ \gamma,\ \cdots$$

等字母表示整数，并且有时将把整数叫作数。

定义 1．设 a，d 是整数，$d \neq 0$．若有一整数 q，可使 $a = dq$，则 d 叫作 a 的约数，a 叫作 d 的倍数．我们有时说，d 能除尽 a，或 a 能被 d 除尽；也有时说，d 能整除 a，或 a 能被 d 整除。

若 d 能整除 a，我们就用 $d \mid a$ 这个符号表示它，譬如 $6 \mid (-30)$，$-5 \mid 20$。

若 b 除不尽 c，我们就写作 $b \nmid c$，譬如 $3 \nmid 8$，$-5 \nmid 12$．若 $b \nmid c$，我们就说，b 不是 c 的约数或 c 不是 b 的倍数。但为了今后说明问题方便起见，我们有时将把 b 叫作 c 的非约数，c 叫作 b 的非倍数。

若 $a = dq$，$q \neq 0$，当然 q 也是 a 的约数。

若 a 是任意数，则

$$0，\ \pm a，\ \pm 2a，\ \pm 3a，\ \cdots$$

很明显都是 a 的倍数。故零是任意数的倍数。而绝对值小于 $|\pm a|$ 能被 $\pm a$ 除尽的只有零。

由于 $a = a \cdot 1 = (-a)(-1)$ 可知，任何数 a 是本身的约数，也是本身的倍数，而 ± 1 是任何数的约数。

定理 1．若 $a \mid b$，则

$$-a \mid b，\ a \mid (-b)，\ -a \mid (-b)，\ |a| \mid |b|．$$

证明．因 $a \mid b$，故必有一数 q，可使 $b = aq$．故得

$$b = aq = (-a)(-q)，$$
$$-b = a(-q) = (-a)q，$$
$$|b| = |aq| = |a| \cdot |q|．$$

所以 $-a \mid b$，$a \mid (-b)$，$-a \mid (-b)$，$|a| \mid |b|$．

这个定理也可以这样说：若 $a \mid b$，则 $\pm a \mid (\pm b)$，在这里 a，b 的正负号可以任意搭配。故无论 a，b 是正或负，其中自然包括着 $|a| \mid |b|$。

定理 2．若 $a \mid b$，$b \mid c$，则 $a \mid c$。

证明．因 $a \mid b$，故必有一数 q_1，可使 $b = aq_1$。同理必得 $c = bq_2$。故 $c = bq_2 = aq_1q_2$。故 $a \mid c$。

这个定理也可以这样说：若 a 是 b 的约数，b 是 c 的约数，则 a 是 c 的约数；或者说，若 c 是 b 的倍数，b 是 a 的倍数，则 c 是 a 的倍数。

这个定理还可以更简化成这样：约数的约数还是约数；倍数的倍数还是倍数。

定理 3．若 $a \mid b$，则 $a \mid bx$，x 可以是任意数。

证明．因 $a \mid b$，而 $b \mid bx$，故 $a \mid bx$。

由此定理可知，若 d 是 a 的约数，则 d 也是 0，$\pm a$，$\pm 2a$，$\pm 3a$，…这些数的约数。

定理 4．（1）若 $a \mid b$，$c \neq 0$ 则 $ac \mid bc$。

（2）若 $ac \mid bc$，则 $a \mid b$。

证明．（1）因 $a \mid b$，故 $a \neq 0$。又因 $c \neq 0$，故 $ac \neq 0$。又因 $b = aq$，故 $bc = acq$。故得 $ac \mid bc$。

（2）因 $ac \mid bc$，故 $ac \neq 0$。故 $a \neq 0$，$c \neq 0$。故由 $bc = acq$，得 $b = aq$。故得 $a \mid b$。

定理 5．若 $a \mid b$，$b \neq 0$，则 $|a| \leqslant |b|$。

证明．因 $a \mid b$，故 $b = aq$。故由定理 1 得 $|b| = |a| \cdot |q|$。因 $b \neq 0$，故 $q \neq 0$。故 $|q| \geqslant 1$。故 $|a| \leqslant |b|$。

这个定理说明了，任何不为零的数只能有有限多个约

数。

定理 6．± 1 是任何数的约数，除此以外再没有其它的数有此性质。

证明．设 a 是任何数。由于 $a = 1 \cdot a = (-1)(-a)$，故得 $\pm 1 \mid a$。若 $|a| > 1$，则 a 根据定理 5 很明显不能是 1 的约数。故除 ± 1 以外，再无其它的数，能是任何数的约数。

定理 7．零是任何数的倍数，除此以外，再没有其它的数有此性质。

证明．首先是 $0 = a \cdot 0$，a 可以是任何数。若 $a \neq 0$，则 a 被 $|a|+1$ 除不尽；故 a 不能是任何数的倍数。

定理 8．设 $n > 1$ 是整数。若

$$d \mid a_1,\ d \mid a_2,\ \cdots,\ d \mid a_n,$$

则

$$d \mid (\pm a_1 \pm a_2 \pm \cdots \pm a_n).$$

证明．因 $d \mid a_1$，$d \mid a_2$，$\cdots$，$d \mid a_n$，故必有 n 个数 α_1，α_2，$\cdots$，α_n，可使

$$a_1 = d\alpha_1,\ a_2 = d\alpha_2,\ \cdots,\ a_n = d\alpha_n.$$

故得

$$\pm a_1 \pm a_2 \pm \cdots \pm a_n = \pm d\alpha_1 \pm d\alpha_2 \pm \cdots \pm d\alpha_n$$
$$= d(\pm \alpha_1 \pm \alpha_2 \pm \cdots \pm \alpha_n).$$

故

$$d \mid (\pm a_1 \pm a_2 \pm \cdots \pm a_n).$$

这个定理，也可以这样说：若 a_1，a_2，$\cdots$，a_n 都是 d 的倍数，则它们的任意代数和也是 d 的倍数。或者更简短地说：倍数的代数和还是倍数。当 $n = 2$ 时，这个定理可以这样说：若 a，b 都是 d 的倍数，则它们的和及差也都是 d 的倍数。

定理 9．若在 a_1，a_2，$\cdots$，a_n 中只有一个数不是 d 的倍数，则它们的代数和也不是 d 的倍数。

证明。为了明确起见，设只有 $d \nmid a_n$。令

$$b = \pm a_1 \pm a_2 \pm \cdots \pm a_n$$

假若 d 能除尽 b，则由

$$\pm a_n = b \mp a_1 \mp a_2 \mp \cdots \mp a_n$$

及根据定理 8 必得 $d \mid a_n$。此与题设矛盾。所以 $d \nmid b$。

这个定理也可以这样说：倍数和一个非倍数的和或者是差是一个非倍数。

要注意，我们不能说：若在 a_1，a_2，…，a_n 这 n 个数中有两个或两个以上的数不是 d 的倍数，则它们的代数和就不是 d 的倍数。比方 $6 \nmid 5$，$6 \nmid 13$，但是 6 能除尽 $5+13=18$

定理10. 设 m，n 都是正整数，而

$$a_1,\ a_2,\ \cdots,\ a_m \text{ 及 } b_1,\ b_2,\ \cdots b_n$$

都是整数。若

$$a_1+a_2+\cdots+a_m=b_1+b_2+\cdots b_n,$$

并且已知，在这 $m+n$ 个项中有 $m+n-1$ 个项都是 d 的倍数，那么所余的那一项也是 d 的倍数。

证明。设所余的那一项是 b_n。

故得

$$b_n=a_1+a_2+\cdots+a_m-b_1-b_2-\cdots-b_{n-1}.$$

现在可以看出，b_n 是 $m+n-1$ 个数的代数和，这些数都是 d 的倍数，故它们的代数和（就是 b_n）也是 d 的倍数。

这个定理10和前边的定理 8 的内容是一致的，只是表现的形式有所不同。因为它们在以后各有各的用处，故分别列出。

定理11. 在

$$a_1+a_2+\cdots+a_m=b_1+b_2+\cdots+b_n$$

内若有一项不是 d 的倍数，则最少还有一项也不是 d 的倍数。

证明。设 $d \nmid a_1$。若其它 $m+n-1$ 个项都是 d 的倍数，则按定理10应得，a_1 也是 d 的倍数。但 a_1 不是，所以其它的项不能都是 d 的倍数。

定理12. 若 a_1，a_2，$\cdots$，a_n 都是 d 的倍数，则它们的连乘积 $a_1a_2\cdots a_n$ 很明显是 d^n 的倍数。

定理13. 若 a，b 是两个整数，$b\neq 0$，则必有而且仅有两个整数 q，r，可使

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

证明。若 $b>0$，则 b 的倍数按大小列出是

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

若 $b<0$，则 b 的倍数按大小列出是

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

故无论如何只有两种可能：

Ⅰ. a 等于一个倍数 qb，故 $r=0$。

Ⅱ. a 介在一个倍数 qb 和次一个较大的倍数中间。故 $0<a-qb=r<|b|$。故无论如何恒可得

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

现在要证明只有唯一的这样一对 q，r，可使这个关系式成立。假设还有另外一对 q_1，r_1，可使

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

那么这两个关系式相减得

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

故根据定理10得 $b|(r-r_1)$。再根据定理1得 $|b|\,|r-r_1|$。

因 $0\leqslant r<|b|$，$0\leqslant r_1<|b|$，故 $|r-r_1|<|b|$。绝对值小于 $|b|$ 而能被 $|b|$ 除尽的只有零。故 $r-r_1=0$，也就是 $r_1=r$。因而也得 $q-q_1=0$，就是 $q_1=q$。

§2．某些数作约数的观察法

为了今后写出来和念起来不至于发生模糊起见，我想把数字与数码的意义区别开。一般地是把

0，1，2，3，4，5，6，7，8，9

这十个符号叫作“数字”。这个时候必须把“字”字重念。但在平常谈话时，也可能谈到这个：中国发展国民经济的第一个五年计划的投资总额是766.4亿元，折合黄金七万万两，这真是一个了不起的数字。这个时候通常是把“数字”中的“数”重念，而在这个地方“数字”的意思其实就是数。因为“数字”二字的意义不是那么肯定，所以我建议把

0，1，2，3，4，5，6，7，8，9

这十个符号叫作“数码”。“数码”二字念起来明朗，听起来也清楚，这对于教学是有好处的。

“数字”二字的一个意思被“数码”代替了，另一个意思又实际上就是数，所以在这以后不准备再使用了。

一个数码同时是一个数，但是一个数可有许多数码，比方5083这个数有四个数码。

若把某数的各个数码所代表的数加起来，则所得的数将叫作某数的数码和。比方5083的数码和是 $5+0+8+3=16$。而 -5083 的数码和也是16。

定理1说：若$d \mid a$，则$\pm d \mid (\pm a)$。故一个正整数a的约数和负整数$-a$的约数是完全相同的。而任何数a的正约数和负约数是在绝对值相等的情况下一一对应的。因此在以后我们将只讨论正整数的正约数。

在中学算术课本里我们已经学过一些观察约数的方法。这些约数的观察法在那里是用数的实际例子说明的。现在我们可以引用前一节的定理来证明它们。我们不打算都证明，只准备作几个例子。

在证明它们以前应该把它们述说出来。在述说它们以前，对于某些词汇，我们应该取得一致的理解。

一个数的个位有时将叫作第一位，十位叫作第二位，百位叫作第三位，…。而第一位，第三位，…将叫作奇位；第二位，第四位，…将叫作偶位。

一个数的个位上的数码所代表的数将叫作该数的个位数或末位数。故358的末位数是8，而6的末位数是6，虽然对于一个一位数来说，已经没有什么首末之分。

一个数的个位上和十位上的两个数码所组成的数，将叫作该数的末两位数。故3582的末两位数是82，35的末两位数就是35，而8的末两位数应该说是8，虽然8这个数只有一位。

一个数的个，十，百三位上的数将叫作该数的末三位数，虽然该数也可能只有三位，两位或一位。

现在把以2，5；4，25；8，125；3，9；11等数为约数的观察法述说如下：

（1）若一数的末位数能被2（或5）除尽，则此数是2（或5）的倍数；若除不尽，就不是。

末位上出现的能被2除尽的数有2，4，6，8，0。末位上出现的能被5除尽的数有5，0。故从末位上的数来看，以2作约数的数有5类，以5作约数的数有2类。

（2）若一数的末两位数能被4（或25）除尽，则此数是4（或25）的倍数；若除不尽，就不是。

末两位数能被4除尽的有4，8，12，…，96，00，共有25类。末两位数能被25除尽的有25，50，75，00，共有四类。

（3）若一数的末三位数能被8（或125）除尽，则此数是8（或125）的倍数；若除不尽，就不是。

末三位数以8作约数的有$\frac{1000}{8}=125$类，末三位数以125作约数的有$\frac{1000}{125}=8$类。

（4）若一数的数码和是9（或3）的倍数，则此数是9（或3）的倍数；若数码和不是，则此数也不是。现在举几个例子说明如下：

（a）534726的数码和是$5+3+4+7+2+6=27$，所以它是9（也是3）的倍数。

（b）8761325的数码和是$8+7+6+1+3+2+5=32$，所以它不是9（也不是3）的倍数。

（c）9456的数码和是$9+4+5+6=24$，所以它不是9的倍数，却是3的倍数。

若一数的数码和不是一个一位数，则可以继续求这个数码和的数码和。这是因为，既然一个数的数码和能决定该数是不是9（或3）的倍数，那么这个数码和的数码和也能决定该数的数码和是不是9（或3）的倍数。现在再回头看看

前边的三个例子：

（a）534726的数码和的数码和是2＋7＝9，是9和3的倍数。

（b）8761325的数码和的数码和是3＋2＝5，不是9和3的倍数。

（c）9456的数码和的数码和是2＋4＝6，不是9的倍数，而是3的倍数。

可是在实际计算当中，我们还可以更简化。由前边的定理8可知，若一个数是9（或3）的倍数，则加上或减去9（或3）的倍数后，还是9（或3）的倍数。又由定理9可知，若一个数不是9（或3）的倍数，则加上或减去9（或3）的倍数后，还不是9（或3）的倍数。因此我们在计算一个数的数码和时，多个9或少个9，或者是多个9的倍数或少个9的倍数，对于结论毫无影响。所以在实际计算数码和时，遇到9这个数码或者遇到能以凑足9的几个数码，我们就可以把它们去掉。这将会大大加速观察任务的完成。再把前边的三个例子拿来试试看。

（a）在观察534726时，一看就知，5＋4是9，7＋2是9，3＋6是9，都去掉后，数码和变成零了，所以是9和3的倍数。

（b）在8761325内，一眼可以看到，8＋1是9，7＋2是9，6＋3是9，都去掉后，只剩下5了，所以不是9和3的倍数。也可以这样看：（3＋7）＋8＝18，6＋1＋2＝9，都去掉后还是剩个5。

（c）在9456内把9去掉，再把4和5去掉，所以一望就得到6，是3的倍数，不是9的倍数。