整数論

第一卷

張德馨著

科学出版社

內 容 提 要

本書講解了整数論的基础，內容共分八章：第一章——整数的可約性；第二章——数論函数；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。

書末还附有二表：100 以下各質数的原根和标数表；4000 以下的質数和它們的最小原根表。

整　数　論

第一卷

張 德 馨 著

*

科学出版社出版（北京朝阳門大街 117 号）

北京市书刊出版业营业許可証出字第 061 号

中国科学院印刷厂印刷　新华书店总經售

*

1958 年 [illegible] 月第一版　　书号：1194　印张：9 5/8

1960 年 1 月第二次印刷　　开本：850×1168 1/32

（京）2,351—4,850　　字数：234,000

定价：(10) 1.80 元

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軍后的今天实現了．所以我感謝党和政府給我的鼓励和支持．

这本書可供高等师范学校和綜合性大学数学系或数理系作教本用，也可供中学教員和高中畢業生自修之用．

在这本書内有下列几点希讀者注意．

第一章內，关于大公約和小公倍的求法，我曾各提出了五种．輾轉相減法是我在德国柏林大学数学系听老教授 I. Schur 的数論課时学来的．混合求法是我个人提出的．

第四章內，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簡捷．比方第四章第 3 节的例題 1 实际上只用了一行就把問題解决了．若用其它的方法都不会这样地簡捷．

第四章內也曾介紹了孙子定理和黃宗宪的求一术表式．讀者可以看出我国前輩数学家在整数論方面的成就．

关于怎么样解出以質数 $p=4n+1$ 为模的二次同余式問題我在第六章第一节內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．

关于从質数模 p 的原根 g 求出 $p^{\alpha}(\alpha>1)$ 的原根問題，在有些数論書上大致是这样提出的：在 $0, 1, 2, \cdots, p-1$ 这些数內必有适当的 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，

就得試驗 $k=1$ 怎么样. 有的書上是这样提出的: 若 g 不是 p^α 的原根, 则 $g+p$ 一定是 p^α 的原根. 这样就只須試驗 $k=0$ 就够了.

我在第七章第 4 节内証明了, 若 g 不是 p^α 的原根, 則 $g-p$ 一定是 p^α 的原根. 这与 $g+p$ 虽然只差一个符号, 但因我們在选用 g 时, 習慣用正数, 故一定是 $|g-p|<|g+p|$. 这在計算 $(g-p)^2$, $(g-p)^3$, $\cdots$, $(g-p)^{\varphi(p^\alpha)}$ 时, 將会节省若干劳动力.

关于如何肯定一个数 g 是不是模 m 的原根問題, И. М. Виноградов 在他的数論基础第六章第 3 节内提出了一个办法(可参考裘光明的中譯本). 根据这个办法, 他在計算出 2^8, 2^{20}; 3^8; 4^8, 4^{20}; 5^8, 5^{20}; 6^8, 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.

我在这本書第七章第 5 节定理 16 内把这个方法改进了. 根据这个定理, 只計算 3^8 和 6^8 这兩个数对于模 41 的最小正同余数, 就把 6 是 41 的原根肯定了. 这只是兩个 8 次方的数; 而在上边的 9 个数中还有 4 个是 20 次方的数.

写本書时, 我無时無刻不在想, 怎么能使讀者更容易看得懂. 因此在文字方面我曾尽力使它接近口語; 在講解方面我曾力求詳尽, 沒把一些証明过程或計算过程簡化掉或留給讀者, 怕給讀者造成疑虑和麻煩.

虽然尽了很大的努力想把这本書写得淺显通俗, 严密正确, 但是我的能力有限, 很可能还有許多缺点和錯誤, 所以我誠恳地希望讀者提出批評和指正.

本书原稿曾蒙吉林师范大学代数教研室张立仁等同志看过. 他們对本稿都提出了一些宝貴的意見, 特在此表示感謝.

张德馨

1958.11.7.

目　录

第　一　章

整数的可約性

§1. 約数和倍数

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

这些数叫作自然数. 在自然数范圍内,很明显是

自然数＋自然数＝自然数,

自然数×自然数＝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負数. 因此我們又把自然数叫作正整数,并把

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

这些数叫作負整数. 而正整数和負整数再加上零,就統一叫作整数.

整数論是研究整数的性質的. 整数論也叫作数論.

在整数范圍内,我們得

整数＋整数＝整数,

整数－整数＝整数,

整数×整数＝整数.

但是整数除整数不一定得整数,当然更談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? 研究这个問題,就是研究整数的可約性. 这就是数論的开端.

以后若不特別声明,我們將用

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

等字母表示整数，并且有时將把整数叫作数.

定义 1. 設 a, d 是整数，$d\neq 0$. 若有一整数 q，可使 $a=dq$，則 d 叫作 a 的約数，a 叫作 d 的倍数；我們有时說，d 能除尽 a，或 a 能被 d 除尽；也有时說，d 能整除 a，或 a 能被 d 整除.

若 d 能整除 a，我們就用 $d|a$ 这个符号表示它，譬如 $6|(-30)$，$-5|20$.

若 b 除不尽 c，我們就写作 $b\nmid c$，譬如 $3\nmid 8$，$-5\nmid 12$. 若 $b\nmid c$，我們就說，b 不是 c 的約数或 c 不是 b 的倍数. 但为了今后說明問題方便起見，我們有时將把 b 叫作 c 的非約数，c 叫作 b 的非倍数.

若 $a=dq$，$q\neq 0$，当然 q 也是 a 的約数.

若 a 是任意数，則

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

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

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

定理 1. 若 $a|b$，則

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

<u>証明</u>. 因 $a|b$，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 $-a|b$，$a|(-b)$，$-a|(-b)$，$|a|\Big||b|$.

这个定理也可以这样說：若 $a|b$，則 $\pm a|(\pm b)$，在这里 a, b 的正負号可以任意搭配. 故無論 a, b 是正或負，其中自然包括着 $|a|\Big||b|$.

定理 2. 若$a|b$，$b|c$，則$a|c$.

<u>証明</u>. 因$a|b$，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$a|c$.

这个定理也可以这样說：若a是b的約数，b是c的約数，則a是c的約数；或者說，若c是b的倍数，b是a的倍数，則c是a的倍数.

这个定理还可以更簡化成这样：約数的約数还是約数；倍数的倍数还是倍数.

定理 3. 若$a|b$，則$a|bx$，x可以是任意数.

<u>証明</u>. 因$a|b$，而$b|bx$，故$a|bx$.

由此定理可知，若d是a的約数，則d也是0，$\pm a$，$\pm 2a$，$\pm 3a$，… 这些数的約数.

定理 4. （1）若$a|b$，$c\neq 0$，則$ac|bc$.

（2）若$ac|bc$，則$a|b$.

<u>証明</u>. （1）因$a|b$，故$a\neq 0$. 又因$c\neq 0$，故$ac\neq 0$. 又因$b=aq$，故$bc=acq$. 故得$ac|bc$.

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

定理 5. 若$a|b$，$b\neq 0$，則$|a|\leqslant|b|$.

<u>証明</u>. 因$a|b$，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$|a|\leqslant|b|$.

这个定理說明了，任何不为零的数只能有有限多个約数.

定理 6. ± 1是任何数的約数，除此以外再沒有其它的数有此性質.

<u>証明</u>. 設a是任何数. 由于$a=1\cdot a=(-1)(-a)$，故得$\pm 1|a$. 若$|a|>1$，則a根据定理5很明显不能是1的約数. 故除± 1以外，再無其它的数，能是任何数的約数.

定理 7. 零是任何数的倍数，除此以外，再沒有其它的数有此

性質.

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

定理 8. 設 $n>1$ 是整数. 若

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

則

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

証明. 因 $d|a_1$, $d|a_2$, $\cdots$, $d|a_n$, 故必有 n 个数 $\alpha_1, \alpha_2, \cdots, \alpha_n$, 可使

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

故得

$$\begin{aligned}\pm a_1\pm a_2\pm\cdots\pm a_n&=\pm d\alpha_1\pm d\alpha_2\pm\cdots\pm d\alpha_n\\&=d(\pm\alpha_1\pm\alpha_2\pm\cdots\pm\alpha_n).\end{aligned}$$

故

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

这个定理,也可以这样說:若 $a_1, a_2, \cdots, a_n$ 都是 d 的倍数,則它們的任意代数和也是 d 的倍数. 或者更簡短地說: 倍数的代数和还是倍数. 当 $n=2$ 时,这个定理可以这样說:若 a, b 都是 d 的倍数,則它們的和及差也都是 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,則它們的代数和也不是 d 的倍数.

証明. 为了明确起見,設只有 $d\nmid a_n$. 令

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

假若 d 能除尽 b, 則由

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

及根据定理 8 必得 $d|a_n$. 此与題設矛盾. 所以 $d\nmid b$.

这个定理也可以这样說:倍数和一个非倍数的和或者是差是一个非倍数.

要注意,我們不能說:若在 $a_1, a_2, \cdots, a_n$ 这 n 个数中有兩个或兩个以上的数不是 d 的倍数,則它們的代数和就不是 d 的倍数. 比方 $6\nmid 5$, $6\nmid 13$, 但是 6 能除尽 $5+13=18$.

定理 10. 設 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 $m+n$ 个項中有 $m+n-1$ 个項都是 d 的倍数，那么所余的那一項也是 d 的倍数．

證明．設所余的那一項是 b_n．

故得

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

現在可以看出，b_n 是 $m+n-1$ 个数的代数和，这些数都是 d 的倍数，故它們的代数和(就是 b_n)也是 d 的倍数．

这个定理 10 和前边的定理 8 的內容是一致的，只是表現的形式有所不同．因为它們在以后各有各的用处，故分别列出．

定理 11. 在

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

內若有一項不是 d 的倍数，則最少还有一項也不是 d 的倍数．

證明．設 $d \nmid a_1$．若其它 $m+n-1$ 个項都是 d 的倍数，則按定理 10 应得，a_1 也是 d 的倍数．但 a_1 不是，所以其它的項不能都是 d 的倍数．

定理 12. 若 $a_1, a_2, \cdots, a_n$ 都是 d 的倍数，則它們的連乘积 $a_1a_2\cdots a_n$ 很明显是 d^n 的倍数．

定理 13. 若 a, b 是兩个整数，$b\neq0$，則必有而且仅有兩个整数 q, r，可使

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

證明．若 $b>0$，則 b 的倍数按大小列出是

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

若 $b<0$，則 b 的倍数按大小列出是

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

故無論如何只有兩种可能：

I. a 等于一个倍数 qb，故 $r=0$。

II. a 介在一个倍数 qb 和次一个較大的倍数中間．故 $0<a-qb=r<|b|$．故無論如何恒可得

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

現在要証明只有唯一的这样一对 q, r，可使这个关系式成立．假設还有另外一对 q_1, r_1，可使

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

那么这兩个关系式相減得

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

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

因 $0\leqslant r<|b|$， $0\leqslant r_1<|b|$， 故 $|r-r_1|<|b|$．

絕对値小于 $|b|$ 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. 某些数作約数的观察法

为了今后写出来和念起来不至于發生模糊起見，我想把数字与数碼的意义区别开．一般地是把

0, 1, 2, 3, 4, 5, 6, 7, 8, 9

这十个符号叫作“数字”．这个时候必須把“字”字重念．但在平常談話时，也可能談到这个：中国發展国民經济的第一个五年計划的投資总額是 766.4 亿元，折合黃金七万万兩，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，所以我建議把

0, 1, 2, 3, 4, 5, 6, 7, 8, 9

这十个符号叫作“数碼”．“数碼”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"数碼"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.

一个数碼同时是一个数，但是一个数可有許多数碼，比方5083这个数有四个数碼.

若把某数的各个数碼所代表的数加起来，則所得的数將叫作某数的数碼和. 比方5083的数碼和是$5+0+8+3=16$. 而-5083的数碼和也是16.

定理1說：若$d|a$，則$\pm d|(\pm a)$. 故一个正整数a的約数和負整数$-a$的約数是完全相同的. 而任何数a的正約数和負約数是在絕对值相等的情况下一一对应的. 因此在以后我們將只討論正整数的正約数.

在中学算术課本里我們已經学过一些观察約数的方法. 这些約数的观察法在那里是用数的实际例子說明的，現在我們可以引用前一节的定理来証明它們. 我們不打算都証明，只准备作几个例子.

在証明它們以前应該把它們述說出来. 在述說它們以前，对于某些詞彙，我們应該取得一致的理解.

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

一个数的个位上的数碼所代表的数將叫作該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說，已經沒有什么首末之分.

一个数的个位上和十位上的兩个数碼所組成的数，將叫作該数的末兩位数. 故3582的末兩位数是82，35的末兩位数就是35，而8的末兩位数应該說是8，虽然8这个数只有一位.

一个数的个，十，百三位上的数將叫作該数的末三位数，虽然

該数也可能只有三位，兩位或一位.

現在把以 2, 5; 4, 25; 8, 125; 3, 9; 11 等数为約数的观察法述說如下：

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

末位上出現的能被 2 除尽的数有 2, 4, 6, 8, 0. 末位上出現的能被 5 除尽的数有 5, 0. 故从末位上的数来看，以 2 作約数的数有 5 类，以 5 作約数的数有 2 类.

(2)若一数的末兩位数能被 4 (或 25)除尽，則此数是 4 (或 25)的倍数；若除不尽，就不是.

末兩位数能被 4 除尽的有 4, 8, 12, …, 96, 00, 共有 25 类. 末兩位数能被 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，則此数是 8 (或 125)的倍数；若除不尽，就不是.

末三位数以 8 作約数的有 $\frac{1000}{8}=125$ 类，末三位数以 125 作約数的有 $\frac{1000}{125}=8$ 类.

(4)若一数的数碼和是 9 (或 3)的倍数，則此数是 9 (或 3)的倍数；若数碼和不是，則此数也不是. 現在举几个例子說明如下：

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

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

(c) 9456 的数碼和是 $9+4+5+6=24$，所以它不是 9 的倍数，却是 3 的倍数.

若一数的数碼和不是一个一位数，則可以繼續求这个数碼和的数碼和. 这是因为，旣然一个数的数碼和能决定該数是不是 9 (或 3)的倍数，那么这个数碼和的数碼和也能决定該数的数碼和

是不是 9 (或 3)的倍数. 現在再回头看看前边的三个例子:

(a) 534726 的数碼和的数碼和是 $2+7=9$, 是 9 和 3 的倍数.

(b) 8761325 的数碼和的数碼和是 $3+2=5$, 不是 9 和 3 的倍数.

(c) 9456 的数碼和的数碼和是 $2+4=6$, 不是 9 的倍数, 而是 3 的倍数.

可是在实际計算当中, 我們还可以更簡化. 由前边的定理 8 可知, 若一个数是 9 (或 3) 的倍数, 則加上或減去 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, 則加上或減去 9 (或 3)的倍数后, 还不是 9 (或 3)的倍数. 因此我們在計算一个数的数碼和时, 多个 9 或少个 9, 或者是多个 9 的倍数或少个 9 的倍数, 对于結論毫無影响. 所以在实际計算数碼和时, 遇到 9 这个数碼或者遇到能以凑足 9 的几个数碼, 我們就可以把它們去掉. 这將会大大加速观察任务的完成. 再把前边的三个例子拿来試試看.

(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, 数碼和变成零了, 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.

(5)若一数的奇位上的数碼和与偶位上的数碼和的差是 11 的倍数, 則此数是 11 的倍数; 否則就不是.

現在我們可以証明几个約数的观察法. 在开始以前, 我們要作一下这样的按排: 設 $a_1, a_2, \cdots, a_n$ 是 n 个任意数碼, $n \geqslant 1$, 并且一般地 $a_n \neq 0$. 以下我們有时將用 $a_n a_{n-1} \cdots a_3 a_2 a_1$ 表示一个 n 位

数. 所以这时不是

$$a_na_{n-1}\cdots a_2a_1 = a_n \times a_{n-1} \times \cdots \times a_2 \times a_1,$$

而是

$$a_na_{n-1}\cdots a_2a_1 = a_1 + a_2\cdot 10 + a_3\cdot 10^2 + \cdots + a_{n-1}\cdot 10^{n-2} + a_n\cdot 10^{n-1}.$$

例 1. 証若一数的末兩位数是 4 (或 25) 的倍数, 則此数是 4 (或 25) 的倍数.

証明. 設此数是一个 n 位数 $a_na_{n-1}\cdots a_2a_1$. 故

$$a_na_{n-1}\cdots a_2a_1 = a_n\cdots a_4a_3 \times 100 + a_2a_1 = a_n\cdots a_4a_3 \times 4 \times 25 + a_2a_1.$$

故若等号右边的 a_2a_1 是 4 (或 25) 的倍数, 則按着定理 8 可知, 等号左边的数就是 4 (或 25) 的倍数. 又按定理 9 可知, 若 a_2a_1 不是 4 (或 25) 的倍数, 則 $a_n\cdots a_2a_1$ 也不是.

例 2. 証若一数的奇位上的数碼和与偶位上的数碼和的差是 11 的倍数, 則此数是 11 的倍数.

証明. 按着定理 3 和定理 8 可得

$$10 = 11 - 1 = 11\text{ 的倍数} - 1,$$
$$10^2 = (11-1)^2 = 11\text{ 的倍数} + 1,$$
$$10^3 = (11-1)^3 = 11\text{ 的倍数} - 1,$$
$$10^4 = (11-1)^4 = 11\text{ 的倍数} + 1,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$10^{n-1} = (11-1)^{n-1} = 11\text{的倍数} + (-1)^{n-1}.$$

故得

$$\begin{aligned} a_na_{n-1}\cdots a_2a_1 &= a_1 + a_2\cdot 10 + a_3\cdot 10^2 + \cdots + a_n\cdot 10^{n-1} \\ &= a_1 + a_2(11\text{ 的倍数} - 1) \\ &\qquad + a_3(11\text{ 的倍数} + 1) \\ &\qquad + a_4(11\text{ 的倍数} - 1) \\ &\qquad \cdots\cdots\cdots\cdots \\ &\qquad + a_n(11\text{ 的倍数} + (-1)^{n-1}). \end{aligned}$$

去掉括号后, 把 11 的倍数的項合併为一項, 我們就得

$$a_n\cdots a_2a_1 = 11\text{ 的倍数} + a_1 - a_2 + a_3 - a_4 + \cdots$$