北师范大学教材

初等数論选讲

李复中

东北师范大学

说　明

本讲义是以张德馨教授的《整数论》一书为兰本，参考华罗庚教授的《数论导引》等十多本书编写而成的，约18万字。介绍初等数论的基本内容：整除性、同余式、连分数、不定方程、平方剩余和原根。论证详细，收入了108个例题和272个习题（包括基本题和大量的国内外的竞赛题以及自编的题目），附有解答，便于自学。本讲义可供本科60—70学时的数论课教材，删去第三章§7、§8及第五章§4等多为作者近年来得到的新结果，可供师院专修科教材，也可供中学教师阅读。

本讲义是在张德馨教授的亲切指导下编写的，编者表示衷心的谢意。

本讲义虽已在77级和78级讲授过，但欠妥甚至错误之处仍在所难免，请同志们指正。

编　者

82年10月

目　录

第一章　整数的整除性

§1　约数与倍数

自然数是指

$$1，2，3，\cdots\cdots$$

中的数。整数是指

$$\cdots\cdots -3，-2，-1，0，1，2，3，\cdots\cdots$$

中的数。所以自然数就是正整数。显然，二整数之和、差、积仍然是整数。但是，二整数之商却不一定是整数。这就需要研究整数的整除性。

我们约定，如果没有特别声明，将用

$$a，b，c，d，\cdots\cdots$$

等英文字母表示整数。用 ab 表示 $a\times b$。

定义. 设 a、b 为二整数且 $b\neq 0$，如果有一整数 c 使 $a=bc$，我们就说 b 是 a 的约数，a 是 b 的倍数，叫做 b 整除 a，用记号 $b|a$ 表示。而用记号 $b\nmid d$ 表示 b 不能整除 d。

若 $a=bc$，而且 $b\neq a$，$b\neq 1$，则 b 叫做 a 的真约数。即 a 的约数中非 a 非 1 者，叫做 a 的真约数。

我们容易得到如下结论：

1 是任一整数的约数：$1|a$。

0 是任一整数的倍数：$b|0$。

任一整数是其本身的约数，也是其本身的倍数：$a|a$。

定理 1　如果 b，c 都是非零的整数，就有

1）若 $c|b$，$b|a$，则 $c|a$。

2）若 $b|a$，则 $bc|ac$。

3）若 $c|a$，$c|b$，则对于任意的 m，n 有 $c|ma+nb$。

定理 2　若 b 是 a 的真约数。则

$$|<|b|<|a|。$$

这两个定理的证明很容易，读者可作练习。

定理 3　若 a 为任一整数，b 为任一整数，则必有唯一的一对整数 q 与 r 使

$$a=bq+r \qquad 0\leqslant r<b。$$

证明。 I 存在性。

将 b 的倍数按从小到大的次序列出：

……，$-3b$，$-2b$，$-b$，0，$2b$，$3b$，……。

用 a 与之比较，则

1）a 等于某一个倍数 bq，即 $a=bq$，此时 $r=0$。

2）a 大于某一个倍数 bq，而小于 $b(q+1)$，即

$bq<a<b(q+1)$。

也就是

$$0<a-bq<b。$$

令　　$a-bq=r$。　即得

$$a=bq+r。 \qquad 0<r<b$$

II　唯一性

如果有两对这样的商和余数：q、r 与 q_1、r_1，使

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

$$a = bq_1 + r_1 \qquad 0 \leqslant r_1 < b。$$

则有

$$b(q - q_1) + r - r_1 = 0 \qquad (1)$$

即 $$b(q - q_1) = r_1 - r。$$

这说明 $r_1 - r$ 是 b 的倍数。但是 $0 \leqslant |r_1 - r| < b$。绝对值小于 b 而又是 b 的倍数者只能是零。所以，$r = r_1$。将此式代入（1）式得

$$b(q - q_1) = 0$$

故得

$$q = q_1。$$

定理 4　若 $b|a_1$，$b|a_2$，…，$b|a_n$，则 $b|(\pm a_1 \pm a_2 \pm \cdots \pm a_n)$。这可以叙述为：一数之倍数的代数和仍是此数的倍数。

证明。因为 $b|a_1$，$b|a_2$，…，$b|a_n$，故必有 n 个整数 c_1，c_2，…，c_n，可使

$$a_1 = bc_1，\ a_2 = bc_2，\ \cdots，\ a_n = bc_n。$$

故得

$$\pm a_1 \pm a_2 \pm \cdots \pm a_n = \pm bc_1 \pm bc_2 \pm \cdots \pm bc_n$$
$$= b(\pm c_1 \pm c_2 \pm \cdots \pm c_n)$$

即

$$b|(\pm a_1 \pm a_2 \pm \cdots \pm a_n)。$$

例题 1　证明：若一数的末两位数是 4（或 2 5）的倍数，则此数是 4（或 2 5）的倍数。

证明。设此数为 n 位数 $a_{n-1}\ a_{n-2}\cdots\cdots a_1 a_0$，即

$$a_{n-1}a_{n-1}\cdots a_1 a_0 = a_{n-1}a_{n-2}\cdots a_2 \times 100 + a_1 a_0 =$$

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

故若其末两位数 a_1a_0 是4（或25）的倍数，则此 n 位数 $a_{n-1}a_{n-2}\cdots a_1a_0$ 为4（或25）的倍数。

例题2．证明：若一数的奇数位上的数码和与偶数位上的数码和的差是11的倍数，则此数是11的倍数。

证明．把10写成11与1之差，由定理4可得

$10 = 11 - 1 = 11$的倍数$- 1$，

$10^2 = (11-1)^2 = 11$的倍数$+ 1$，

$10^3 = (11-1)^3 = 11$的倍数$- 1$，

$10_4 = (11-1)^4 = 11$的倍数$+ 1$，

$10^5(11-1)^5 = 11$的倍数$- 1$，

……

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

故得

$$a_{n-1}a_{n-2}\cdots a_2a_1a_0 = a_0 + a_1\cdot 10 + a_2\cdot 10^2 + \cdots$$
$$+ a_{n-1}\cdot 10^{n-1} = a_0 + a_1(11\text{的倍数} - 1)$$
$$+ a_2(11\text{的倍数} + 1)$$
$$+ a_3(11\text{的倍数} - 1)$$
$$+ a_4(11\text{的倍数} + 1)$$
$$+ a_5(11\text{的倍数} - 1)$$
$$+ \cdots\cdots$$
$$+ a_{n-1}(11\text{的倍数} + (-1)^{n-1})$$
$$= 11\text{的倍数} + (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)$$

故若 $(a_0 + a_2 + a_4\cdots) - (a_1 + a_3 + a_5 + \cdots)$ 是11的倍数。

则 $a_{n-1}a_{n-2}\cdots a_2a_1a_0$ 就是11的倍数。

例题 3　证明：对于任一整数 n

$$\frac{n}{3}+\frac{n^2}{2}+\frac{n^3}{6}$$

恒是整数。

证明. $\frac{n}{3}+\frac{n^2}{2}+\frac{n^3}{6}=\frac{n}{6}(2+3n+n^2)$

$$=\frac{1}{6}n(n+1)(n+2).$$

因为连续两个整数之积必为 2 的倍数，连续三个整数之积必为 3 的倍数，所以，$6\mid n(n+1)(n+2)$。

即 $\frac{n}{3}+\frac{n^2}{2}+\frac{a^3}{6}=\frac{1}{6}n(n+1)(n+2)$ 必为整数。

例题 4　已知七位数 9 2 □□ 4 2 7 是 9 9 的倍数，求此数。

解。由习题 2 知一自然数的数码和是 9 的倍数则此数也是 9 的倍数。否则不是。因为 92 xy 427是 9 的 倍 数，所以

$$9\mid 9+2+x+y+4+2+7$$

即

$$9\mid x+y+6.$$

因为　　$0\leqslant x,\ y\leqslant 9$　　所以

$$6=0+0+6\leqslant x+y+6\leqslant 9+9+6=24$$

$x+y+6$ 是 9 的倍数又界于 6 与 2 4 之间。所以

$$x+y+6=9 \text{ 或 } x+y+6=18.$$

又因为　92 xy 427为11的倍数，所以

$$11\mid[(9+x+4+7)-(2+y+2)]$$

即　　$11 \mid 5 + x - y$.

因为　　$0 \leqslant x, y \leqslant 9$，所以

$$-4 = 5 + 0 - 9 \leqslant 5 + x - y \leqslant 5 + 9 - 0 = 14$$

$5 + x - y$ 是11的倍数又界于 -4 与14之间，所以

$$5 + x - y = 0 \text{ 或 } 5 + x - y = 11.$$

由

$$\begin{cases} x + y + 6 = 9 \\ 5 + x - y = 0 \end{cases}$$

得　　$2x + 2 = 0$，　即　$x = -1$，不合题意。

由

$$\begin{cases} x + y + 6 = 9 \\ 5 + x - y = 11 \end{cases}$$

得　　$2x = 9$，　即　$x = \frac{9}{2}$，不合题意。

由

$$\begin{cases} x + y + 6 = 18 \\ 5 + x - y = 0 \end{cases}$$

得　　$2x = 7$，　即　$x = \frac{7}{2}$，不合题意。

由

$$\begin{cases} x + y + 6 = 18 \\ 5 + x - y = 11 \end{cases}$$

得　　$2x = 18$，即 $x = 9$，代入得 $y = 3$。

所以，此七位数为9 2 9 8 4 2 7。

例题5．任意一个 n 位数，将其数码按逆序重新排列得一新数，试证新数与旧数之差是9的倍数。

证明。设此 n 位数为

$$a_{n-1}a_{n-2}\cdots a_1a_0 = a_{n-1}\cdot 10^{n-1} + a_{n-2}\cdot 10^{n-2} + \\ + \cdots + a_1\cdot 10 + a_0,$$

则新数为

$$a_0a_1\cdots a_{n-2}a_{n-1} = a_0 10^{n-1} + a_1 10^{n-2} + \cdots + \\ + a_{n-2}\cdot 10 + a_{n-1}.$$

故新数与旧数之差等于

$$a_0(10^{n-1}-1) + a_1\cdot 10\cdot(10^{n-3}-1) + \cdots + \\ + a_{n-2}\cdot 10(1-10^{n-3}) + a_{n-1}(1-10^{n-1}).$$

每一项均为 9 的倍数，所以，其和也是 9 的倍数。

例题 6。 n 为非负整数，证明 $7^{n+2}+8^{2n+1}$ 恒为 57 的倍数。

证明。① 当 $n=0$ 时，$7^2+8=57$，命题成立。

② 当 $n>0$ 时，$7^{n+2}+8^{2n+1} = 49\cdot 7^n + 8\cdot 64^n =$

$$= 57\cdot 7^n + 8\cdot 64^n - 8\cdot 7^n =$$

$$= 57\cdot 7^n + 8(64^n - 7^n),$$ n 为正整数，所以

$$(64-7)\mid(64^n-7^n)$$

故得

$$57\mid 7^{n+2}+8^{2n+1}.$$

例题 7。 t 为正奇数，证明

$$1^t+2^t+\cdots+9^t-3(1^t+6^t+8^t)$$

恒为 18 的倍数。

证明。① $2\mid[2^t+4^t+6^t+8^t-3(6^t+8^t)]$，而

$$1^t+3^t+5^t+7^t+9^t-3\cdot 1^t = 3^t+5^t+7^t+9^t-2$$

也是偶数，这是因为 $3'$，$5'$，$7'$，$9'$ 均为奇数。所以，

$$2|[1'+2'+\cdots+9'-3(1'+6'+8')].$$

② $9'$，$1'+8'$，$2'+7'$，$3'+6'$ 及 $4'+5'$分别为9，$1+8$，$2+7$，$3+6$ 及 $4+5$ 即 9 的倍数。又 $1'+8'$ 与 $6'$ 均为 3 的倍数，因此 $3(1'+6+8')$ 是 9 的倍数。所以

$$9|[1'+2'+\cdots+9'-3(1'+6'+8')].$$

综合①与②得知

$$1'+2'+\cdots+9'-3(1+6'+8')$$

恒为 18 的倍数。

例题 8．证明无限级数

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

无论加到哪一项为止，永不得一整数。

证明。令 2^a 表示不超过 n 的 2 的最高次幂：$2^a \leqslant n < 2^{a+1}$。将

$$\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{2^a}+\cdots+\frac{1}{n}$$

通分。其公分母必为 $2^a k$，k 为奇数。通分后，$\frac{1}{2^a}$ 这一项的分子为奇数 k，而其余各项之分子均为偶数（都至少乘上一个 2），所以其和之分子为奇数，而分母为偶数。因此

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

无论加到哪一项为止，永不得一整数。

§2 素数与复合数

我们把正整数分为三类：

① 1：只有正整数1为其约数。

② p：只有正整数1及p本身为其约数。或者说，p是大于1而无真约数的正整数。

③ n：除1与n为其约数外，还有真约数。也可以这样来叙述：只有一个约数的数即1为第一类，只有两个约数的数即p为第二类，有三个或三个以上的约数的数即n为第三类。

定义：大于1的正整数p只有1及其本身为约数者叫做素数（又叫质数）。例如2，3，5，7，11，13，17，19都是素数。

定义：有真约数的正整数叫做复合数。

我们知道，2的倍数叫做偶数，非偶数的整数叫做奇数。显然，偶素数仅有一个：2。

我们从定义看出：1既不是素数又不是复合数。

定理5．大于1的正整数都可以分解为素因数的乘积。

证明．设$n>1$是正整数。

若n是素数，定理已成立。

若n是复合数，即n有真约数。令q_1为其真约数之最小者。由定理2可知q_1为素数。命

$$n=q_1n_1 \qquad 1<n_1<n.$$

若n_1是素数，则定理已成立。若n_1是复合数，则命q_2为

n_1的最小素因数，得

$$n = q_1 q_2 n_2 \qquad 1 < n_2 < n_1 < n.$$

这样作下去，得 $n > n_1 > n_2 > \cdots > 1$。这样的手续不能超过 n 次，故必得

$$n = q_1 q_2 \cdots q_s ,$$

其中 q_1，q_2，…，q_s 都是素数。

若将素因数排成

$$n = p_1^{\alpha_1} p^{\alpha_2} \cdots p_k^{\alpha_k}, \alpha_1 > 0, \ \alpha_2 > 0, \ \cdots, \ \alpha_k > 0,$$
$$p_1 < p_2 < \cdots < p_k$$

叫做 n 的标准分解式。

标准分解式的唯一性将在 § 4 中证明。

例题 9．10725 的标准分解式为：

$$10725 = 3 \cdot 5^2 \cdot 11 \cdot 13.$$

定理 6．若 $N > 1$，被 $\leqslant \sqrt{N}$ 的所有素数都除不尽，则 N 是素数。

证明．用反证法。若 N 是复合数，且 $N = n_1 n_2$，由假设知，$n_1 > \sqrt{N}$，$n_2 > \sqrt{N}$，则 $n_1 n_2 > \sqrt{N} \cdot \sqrt{N} = N$，这与 $N = n_1 n_2$ 矛盾，所以 N 是素数。

最小的若干个素数为

2，3，5，7，11，13，17，19，23，29，31，37，41，43，…。如果 N 不太大，求小于 N 的各个素数是容易办到的，有爱拉托士散纳（*Eratosthenes*）筛法。

先列出所有 $1 < n \leqslant N$ 的正整数 n：

2，3，4，5，…N.

陆续去掉：

① 4，6，8，10，……即由2^2起的一切2的倍数。

② 9，15，21，27，…，即由3^2起的一切3的倍数。

③ 25,35,55，65，……即由5^2起的一切5的倍数。

……。

继续作下去，直到$\leqslant\sqrt{N}$的素数的倍数都去掉以后，剩下来的就是$\leqslant N$的全部素数。

例题10．造出$\leqslant$150的素数表

作法Ⅰ．①写下2，而将其余的偶数4，6，8，……150均不写出，因为它们都不是素数。

②写下5，而将个位数是5的数（它们是5的倍数）都不写出。（个位数是0的数已在①中被淘汰掉了）。

2,5, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29,
31, 33, 37, 39, 41, 43, 47, 49, 51, 53, 57, 59,
61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89,
91, 93, 97, 99,101,103,107,109,111,113,117,119,
121,123,127,129,130,113,137,139,141,143,147,149,

③ 从9起去掉3的倍数（以3，9，21，27为首的4列）。

④ 从$7^2=49$起去掉7的倍数（49，$7\times11=77$，$7\times13=91$，$7\times17=119$，$7\times19=133$）。

⑤ 从$11^2=121$起去掉11的倍数（121,$11\times13=143$）。

而 $13^2=169>150$。所以，>150的素数表已求出来了。即

2, 3, 5, 7, 11,13,17,19,23, 29, 31, 37,41,43,47, 53.

59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149。

作法Ⅱ，将2，3写出而将2与3的倍数$6n$，$6n+2$，$6n+3$，$6n+4$去掉，只写出$6n+1$，$6n+5$的数。

2，3，5，11, 17, 23, 29, 35, 41, 47, 53, 59, 65, 71, 77, 83, 89, 95, 101, 107, 119, 125, 131，137, 143, 149。

7，13, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85, 91, 97, 103, 109, 115, 121, 127, 133, 139, 145。

① 从25起去掉5的倍数（即个位数为5的数25, 35, 55, 65, 85, 95, 115, 125, 145）。

② 从49起去掉7的倍数（49，$7\times11=77$，$7\times13=91$，$7\times17=119$，$7\times19=133$）。

③ 从121起去掉11的倍数（121，$11\times13=143$）得出≤150的素数表。

2，3，5，7，11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 1077109, 113, 127, 131, 137, 139, 149。

定理7． 素数的个数无限。

证明。假设素数是有限多个。共有n个：p_1，p_2，…，p_r。则

$$a=p_1p_2\cdots p_n+1$$

不是p_1，p_2，…p_n的倍数，所以a必有一素因数不是p_1，p_2…，p_n，即p_1，p_2，…，p_n这有限多个素数以外还有素数，即素数的个数无限。