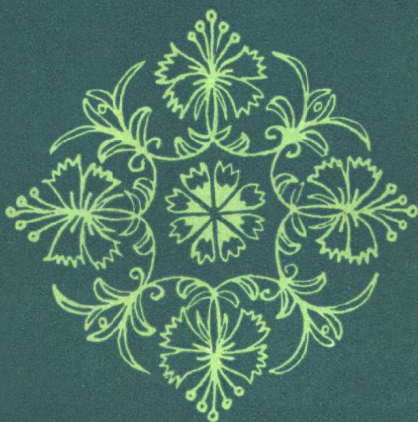


和小学教师谈数论

朱怀新 编著



浙江教育出版社

和小学教师谈数论

朱怀新 编著

浙江教育出版社

和小学教师谈数论

朱怀新编著

浙江教育出版社出版 浙江印校印刷厂印刷

浙江省新华书店发行

开本 787×1092 1/32 印张2.25 插页1 字数47,000 印数00,001—00,000

1984年7月第1版 1984年7月第1次印刷

统一书号：7346·82

定 价：0.21 元

写 在 前 面

先选题目三则：

一、猜数游戏：

小明两只手都捏有一分硬币若干。知道他一手捏的个数为奇数，一手为偶数。而他右手捏的一分硬币个数乘以2，左手捏的个数乘以3，其和为35。请你猜，小明哪一只手捏的一分硬币的个数是奇数？

二、奇妙的数：

某数，用2除余1，用3除余2，
用4除余3，用5除余4，
用6除余5，用7除余6，
用8除余7，用9除余8，
用10除余9。

某数是几？

三、有趣的判断：

四位数：
$$\begin{array}{r} 1000a + 100b + 10c + d \\ + 1000b + 100c + 10d + a \\ \hline 1001a + 1100b + 110c + 11d \end{array}$$
 (a, b, c, d 都是正整数)

能被11整除。为什么？

从上述几则题，给我们一个启示：数论的基本概念已牢固地深入到小学数学领域，事实上，涉及分数的最基本、普

通的计算，都要用到数论的概念。确实，数论是一个使人感兴趣，引人入胜的课题。

我国著名数学家陈景润同志说过：“数论是研究数的性质的一门科学，而初等数论是与算术有极密切的联系的，也可以说是算术的继续。”这就是说，为了培养建设社会主义现代化人才而担负最基础教育的小学教师必须要学一点数论的基本知识。

目 录

写在前面	1
一 数系发展表	1
二 自然数和自然数列	2
三 整除	4
四 因数和倍数	6
五 素数	7
六 哥德巴赫猜想	11
七 素因数	13
八 能被整除的数的判定	21
九 整数解	31
十 数的二进制	37
十一 同余与一次同余式	47
附录：中国剩余定理及其证明	53
习题解答	55

一 数系发展表

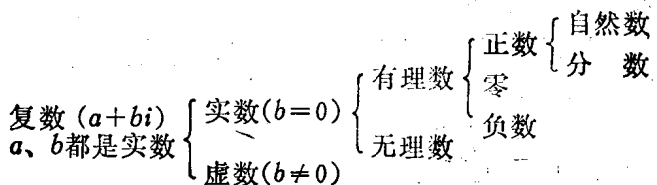
数学是研究现实世界中的空间形式和数量关系的科学。

从数的发展来看，是经过一个漫长的时间的。譬如人们在生产、生活中为了数（shǔ）数（shù），就产生了自然数；要度量部分量，就产生了分数；为了度量具有相反意义的量，就要引进负数，把分数扩大到有理数；要度量连续量（如线段的长度等），就要引进无理数，把有理数扩大到实数；为了度量二维（平面）向量，就要引进虚数，把实数扩充为复数。

因此，建立了有理数集、实数集和复数集。

前两个数集，对于加、减、乘、除四种代数运算是封闭的。复数集使得六种代数运算，尤其是开方这个逆运算永远得以施行。

现将数系发展列表介绍如下：



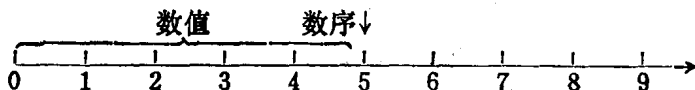
二 自然数和自然数列

一、二、三、四、五、六、七、八、九、……表示物体个数的每一个数，叫自然数。又称正整数。“一”不但是自然数中最小的一个，而且自然数都是由若干个“一”所组成，所以“一”叫自然数的单位。

从一起，顺次加上“一”，就可以顺次得到一、二、三、四、五、六、七、八、九、……这样的一列自然数，叫做自然数列。

数数可以无限的继续下去，所以自然数列是无限的。所有自然数构成一个集合，称为自然数集，则 $A = \{1, 2, 3, 4, 5, \dots\}$ 。在自然数集中，有最小的元素 1，而无最大的元素。任何两个元素相加或相乘，仍然对应着本数集中一个元素，如： $2 + 3 \rightarrow 5$ ， $2 \times 3 \rightarrow 6$ 。

一个自然数具有两方面的意义：一方面是表示事物的多少，即用于计数；另一方面是表示事物的次序，即用于编号。用来表示数量多少的数叫做基数，用来表示事物次序的数叫做序数。



自然数列有三个重要性质：

1. 在自然数列中最前面的一个数是“一”；
2. “一”是自然数的单位；

3. 每一个自然数后面都有一个且只有一个后继数。

在自然数列里，如果两个自然数占有同一个位置，即这两个自然数相等，就是同一个数；如果两个自然数占有不同位置，就说这两个自然数不相等，在前面的小，在后面的大。

例： a 、 b 是两个自然数，则有

$$a < b, a = b, a > b.$$

奇自然数 $2n-1$ 和偶自然数 $2n$ 是一一对应的。即 $2n-1 \leftrightarrow 2n$ ，于是，我们认为奇数和偶数的个数是一样多的。自然数可以用数轴上的点来表示。一个自然数对应着数轴上唯一的一个点。但是，反之不成立。所以，自然数和数轴上的点不是一一对应的。

自然数和它的加法、乘法运算服从下列定律：

1. $a = a$ (自反定律)

2. 若 $a = b$ ，则 $b = a$ (对称定律)

3. 若 $a > b$ ，则 $b < a$ (可逆定律)

4. 若 $a = b, b = c$ ，则 $a = c$ }
或 $a > b, b > c$ ，则 $a > c$ } (传递定律)

5. $\left. \begin{array}{l} a + b = b + a \\ a \cdot b = b \cdot a \end{array} \right\}$ (交换定律)

6. 若 $a = a', b = b'$ 则 $a + b = a' + b', a \cdot b = a' \cdot b'$
(唯一定律)

7. $\left. \begin{array}{l} (a + b) + c = a + (b + c) \\ (a \cdot b) \cdot c = a \cdot (b \cdot c) \end{array} \right\}$ (结合定律)

8. $(a + b)c = ac + bc$ (分配定律)

注：数和数字是有区别的，数字是一种符号，而数则代

表量的多大（有名数和不名数之分），数由数字组成。

习 题 一

1. 自然数列有哪些主要性质？
2. 任意画两条不一样长的线段，怎样来说明这两线段上的点是一样多的？
3. 写出：最小的四位数；最大的五位数。
4. 数的比较大小概念是如何建立起来的？

三 整 除

若我们把零写在自然数列前面，如

$0, 1, 2, 3, 4, 5, \dots$

这就叫扩大的自然数列。

扩大的自然数列的任何一个数叫做整数。因此，任何一整数或是自然数，或是零。

应该强调指出的，“零”是一个数，但“零”不是自然数。

在整数范围内，有

整数 + 整数 = 整数；

整数 - 整数 = 整数；

整数 $\times$ 整数 = 整数。

但是，整数除整数不一定得整数，这就要研究数的整除

问题。

当一个整数 a 除以一个自然数 b ，若能得到整数商 c ，这就说 a 能被 b 整除，或 b 能整除 a ，用 $b|a$ 这个符号表示它。例： $5|30$ ， $7|42$ ，……

当一个整数 a 除以一个自然数 b ，若不能得到整数商 c ，这就说 a 不能被 b 整除，或 b 不能去整除 a ，用 $b \nmid a$ 这个符号表示它。例： $3 \nmid 5$ ， $8 \nmid 17$ ，……但是， $17 \div 8$ 虽不能得到整数商，然而可以得到小数商而无余数。因此，我们说 17 能被 8 除尽。

可见，两数相除，在能整除的情况下，也可以说能够除尽；但在能除尽的情况下，不一定能整除。

关于整除的定理：

1. 若 $a|c$ ， $d|a$ ，则 $d|c$ ；
2. 若 $a|c_1$ ， $a|c_2$ ，则 $a|(c_1+c_2)$ ；
3. 若 $a|c_1$ ， $a|c_2$ ，则 $a|(c_1-c_2)$ (设 $c_1-c_2 \geq 0$)；
4. 若 $a|c_1$ ，而且 c_2 是个整数，那么 $a|c_1 \cdot c_2$ 。

现在来证明定理 2。

已知 $a|c_1$ ， $a|c_2$ 。

求证 $a|(c_1+c_2)$ 。

证明 $\because a|c_1$ ， $a|c_2$ ，根据除法定义，必有整数商 q_1 ， q_2 存在。且

$$c_1 = q_1 a, \quad c_2 = q_2 a.$$

$$\therefore c_1 + c_2 = q_1 a + q_2 a = (q_1 + q_2) a,$$

q_1 与 q_2 是整数，则 $(q_1 + q_2)$ 也必为整数。

$$\therefore (c_1 + c_2) \text{ 能被 } a \text{ 整除，则 } a|(c_1 + c_2).$$

注：这个定理的逆命题不成立，取两数的和能被一个自

然数整除，这两个数不一定能分别被这个自然数整除。

如 $7 \mid (17+11)$ ，但 $7 \nmid 17$ ， $7 \nmid 11$ 。

推论：若两数的和与其中一个加数能被同一个自然数整除，则另一个加数，也能被这个自然数整除。

定理 1、3、4 留给读者自己证明。

四 因数和倍数

设 a, b 是整数， $b \neq 0$ ，如果有一个整数 c ，它使得 $a=bc$ ，则 a 叫做 b 的倍数， b 叫做 a 的因数。当然，也可以说， a 叫做 c 的倍数， c 叫做 a 的因数。

例： $18=2 \cdot 9$ ，则 2, 9 是 18 的因数，18 是 2, 9 的倍数。18 所有的因数组成的集合是：

$\{2, 9, 3, 6, 1, 18\}$ 。

显然，因数和倍数是矛盾的两个方面，它们是不能单独存在的。

“零”可以被任何自然数整除，所以任何自然数都是零的因数，零是任何自然数的倍数。

任何整数都能被 1 整除，所以 1 是任何整数的因数，任何整数都是 1 的倍数。

习 题 二

1. 已知 4205 和 2813 都能被 29 整除，7018 是否能被 29 整

除？为什么？

2. m, n 两个数若都不能被19整除， $m-n$ 能否被19整除？

3. 已知221和323都是17的倍数，544是否是17的倍数？
为什么？

4. 证明任意一个奇数 a 的平方减1都是8的倍数。

五 素 数

一个大于1的整数，只能被1和它本身整除，不能被其他正整数整除，这样的正整数叫素数（又称质数）。简单说，只有1和本身两个因数的数叫做素数。而有多于两个因数的数叫做合数。如17只有两个因数：1和17，所以17是素数；而18，它除了1和18两个因数外，还有因数2、3、6、9，所以它不是素数，是合数。单位“1”既不是素数，也不是合数。

例如，2，3，5，7，11，13，17，19，23，29 都是素数。一般常用 p 或 $p_1, p_2, p_3, \dots, p_n$ 来表示。

寻找素数，有一种方法，叫“厄拉多塞”筛法。这是古希腊数学家与天文学家厄拉多塞设计的一种方法。其方法是这样的：

先列出从2开始的整数。

2，3，4，5，6，7，8，9，10，11，12，13，14，15，
16，17，18，……再把2圈起来，并划去后继的它的所有倍数。

②, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, ……

又把第一个留下来的数 3 圈起来, 并划去后继的所有它的倍数 (有些数在上一次已划过)。

③, 5, 7, 9, 11, 13, 15, 17……再把第一个留下来的数 5 圈起来, 并划去后继的所有它的倍数。……将这个过程一直进行下去, 素数会被圈上。当然, 这种方法或其他方法要得到全部素数表, 那是不可能的。

判断一个正整数 a 是不是素数, 不是说用小于 a 大于 1 的整数——来试除。而是这样判断:

如果 a 是一个大于 1 的正整数, 那么所有 $\leq \sqrt{a}$ 的素数都除不尽 a , 则 a 是素数。

素数有无限多个。这可以用反证法作证明: 假设素数个数有限, 我们可以把它们依次 (从小到大) 排成 2, 3, 5, …… p_n 。

作一整数 $N = 2 \cdot 3 \cdot 5 \cdots p_n + 1$ 。显然 N 也是素数, 这就与假设矛盾。所以素数有无限多个。事实上, 欧几里得 (前 300 年) 早已证明了的。

由于素数的个数无限, 它的变化也无规则可循。我们不能用一种简单的方法直接求出某个素数来。于是只有赖于造素数表。Kalik 曾花 20 年的时间造出了 10^8 以内的素数表。可是, 后来经梅爽 (Mersenne) 检验, 发现有较多的错误。素数表现在最完善的有 Likmes (来梅氏) 素数表, 它罗列了从 2 —— 1006721 诸素数。1876 年 Lucas (路加氏) 曾证得了一个 39 位数的素数。即

$$2^{127} - 1 = 170141183460469231731687303715884105727.$$

目前, 由美国两位十八岁的青年劳拉·尼克爾和柯特诺

尔，经过三年的努力，已求到最大的素数是 $2^{21071}-1$ ，计6533位的数。当然，这是借助电子计算机来证明的。

“梅爽数”：是1644年梅爽(Mersenne)发现了的。所谓“梅爽数”，就是形为 2^n-1 的素数。上面提到那个39位数的素数就是梅爽数中的一个。容易看出，在 2^n-1 中若 n 不为素数，则 2^n-1 也不是素数。因为我们令 $n=a \cdot b (a \neq 1, b \neq 1)$ 即有

$$\begin{aligned} 2^n-1 &= 2^{ab}-1 = (2^a)^b-1 \\ &= (2^a-1)[(2^a)^{b-1} + (2^a)^{b-2} + \dots + 1], \end{aligned}$$

它是个合数。于是 2^n-1 是素数的必要条件是 n 为素数。则梅爽数的公式是：

$$M_p = 2^p - 1 \quad (p \text{ 为素数})$$

在公式 $M_p = 2^p - 1$ (p 为素数) 中，当 $p=11$ 时， $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ ，就不是梅爽数。不难验证。

$$M_{107} = 193707721 \times 761838357287$$

也不是梅爽数。在 $2-257$ 的55个素数中，只有 $p=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$ 所对应的12个数是梅爽数。其余43个都不是梅爽数。

是否有无穷个梅爽数存在？这是一个数学工作者所关心的而尚未证明的问题。

到目前为止，所知道的梅爽数 $M_p = 2^p - 1$ 是素数的已有24个。即当

$p=2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937$ 时即 2^p-1 都是素数。

费尔马数：是在1601—1665年间费尔马(Fermat)所

发现的一种数。则为 2^n+1 的素数。显然， n 不能是奇因数，否则，它就不是素数。因为当 n 有奇因数 a 时，可设 $n=ab$ (a 为奇数， b 为正整数)。

$$\begin{aligned} \text{则} \quad 2^n+1 &= 2^{ab}+1 = (2^b)^a+1 \\ &= (2^b+1)[(2^b)^{a-1} - (2^b)^{a-2} + \cdots + 1] \end{aligned}$$

是个合数。于是 2^n+1 是素数的必要条件是 n 为 2 的乘幂。则费尔马数的公式为：

$$F_n = 2^{2^n} + 1 \quad (n=0, 1, 2, 3, \dots)$$

通过计算，得知 $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ 都是素数。费尔马说：凡 F_n 都是素数。后来 (1732 年) 欧拉 (Euler) 证明 641 可整除 F_5 ，随后又有很多人证明了 $F_6, F_7, F_8, F_9, F_{11}, F_{12}, F_{15}, F_{18}, F_{23}, F_{36}, F_{59}, F_{73}$ ，都非素数。但被发现的有 29 个费尔马数。前些年，又被新发现了 6 个，即： $F_{58}, F_{77}, F_{81}, F_{260}, F_{267}$ 和 F_{1945} 。

再说素数分布简况，如：

在 1 到 100 中间有 25 个素数；

在 1 到 1000 中间有 168 个素数；

在 1000 到 2000 中间有 135 个素数；

在 2000 到 3000 中间有 127 个素数；

在 3000 到 4000 中间有 120 个素数；

在 4000 到 5000 中间有 119 个素数。

从上面的素数分布简况看出，越往上素数个数越稀。

双生素数：相邻两个素数的差是 2，这样成对的素数叫双生素数 (孪生素数)。例如：

3, 5; 5, 7; 11, 13; 17, 19; 29, 31; 41, 43; 59, 61; 71, 73; 101, 103; ……10016957, 10016959 等。越往

上越稀少。

双生素数（即孪生素数）目前知道的最大的 $76 \times 3^{169} - 1$, $76 \times 3^{169} + 1$ 。

习 题 三

1. 什么叫素数？什么叫合数？它们之间有何联系？
2. 任意写出100以内的20个奇数，其中有否素数？有多少个素数？
3. 如何判定一个数是否为素数？试举例说明。
4. 试写出5个形如 $2^n + 1$ 的数（ n 是自然数）其中哪几个是素数？哪几个是合数？

六 哥德巴赫猜想

200多年前，西德数学家哥德巴赫（Goldbach）猜想：“凡相当大的偶数都能分解成两个素数之和。”简称 $(1+1)$ 。

哥德巴赫猜想的根据是充足的。

$$\begin{aligned} 6 &= 3 + 3, 8 = 5 + 3, 10 = 5 + 5, 12 = 5 + 7, \\ 14 &= 7 + 7, 16 = 3 + 13, 18 = 5 + 13, 20 = 7 + 13, \\ 22 &= 5 + 17, 24 = 7 + 17, \dots \end{aligned}$$

哥德巴赫通过大量的实践于1742年写信给数学家欧拉，提出了上面的猜想。后来有人对一个一个的偶数都进行了这样的验算，一直算到三亿三千万，都表明是对的。但是更大