

趣味数论

单增著

趣味数论

QUWEI SHULUN

中国青年出版社

趣味数论

单 樽 著

中国青年出版社

封面设计：唐伟杰

趣味数论

单 墀 著

*

中国青年出版社出版 发行

中国青年出版社印刷厂印刷 新华书店经销

*

787×1092 1/32 7.75印张 2插页 156千字

1987年12月北京第1版 1987年12月北京第1次印刷

印数1—4,000册 定价1.60元

序

自然数产生于史前时代，人们对它的研究源远流长，古往今来，数学家们提出和解决了数不清的有关自然数性质的问题，在数学中，形成了一个结构严谨、内容丰富多采的分支——数论。不少问题的解决，思想的深刻和方法的巧妙，足以使世代代的数学爱好者赞赏不已。数论中许多问题叙述简明而难度极大，是富有魅力的。以华罗庚教授为代表的中国数学家在数论研究中令人瞩目的工作，也引起人们对数论更大的兴趣。我们经常与自然数打交道，对自然数的一些简单性质应该有所了解。一个中学生，如果不知道什么是欧几里得算法是一件遗憾的事。青少年朋友们，无论你将来想做什么，学一点数论的基本知识和方法是会有用的。因此，写一本数论普及读物，让更多的人了解数论的基本内容，是很有必要的。

科学昌明，很需要科普工作者播种耕耘。科普工作很重要，但做好不容易。数学的科普读物似乎尤为难写，正如华罗庚教授所说：“深入浅出是真功夫。”在这本书中，没有繁琐的推导和证明，而是通过一个一个有趣的问题，把初等数论中大部分精华浅显地展现在读者面前。单墀同志是下了一番功夫的。

我以为，好的科普作品应当做到四个字：准、新、浅、趣。

准，内容选择确当，有意义，论说正确，史实无讹。

新，有新意，采用新颖材料或用新的观点来处理熟悉的问题，令人耳目为之一新。

浅，通俗易懂而不肤浅，能跳出为“尖子”、“天才”写的小圈子，写得生动活泼，使多数人愿意看。浅，表明作者对问题看得透澈、就象未受污染的水潭，深，然而澄澈见底。

趣，幽默风趣，而不流于油滑，使人能轻松地学到一些知识。

做到以上四个字，当然很不容易。单墀同志请我作序，一时高兴，写了以上的话，他在这几方面做得如何，读过这本书后，读者自然会作出自己的评价。

王 元

一九八六年五月于北京

前 言

数论又名算术，它研究的对象是数。

数论是一个重要的数学分支。

十九世纪的大数学家高斯(1777-1855)有一句名言：“数论是数学的皇后”。

二十世纪的大数学家希尔伯特(1862-1943)称数论是“其他科学的典范”，是“数学知识的永不枯竭的源泉，并且对其他一切领域的研究提供了不断的刺激。”

正因为如此，在当代著名数学家丢多涅的著作《现代数学概观》中，数论被列入最重要的A级。

数论既古老又年轻。它有几千年的历史，欧几里得(约前330-前275)的《原本》、丢番图(约246-330)的《算术》中已经对数论进行了系统的论述，我国古代算书《周髀算经》、《九章算术》等也都讨论了数论问题。但是，尽管人们在这块富矿中采掘了数千年，资源还远远没有耗尽，直到今天，数论仍然生气勃勃，十分活跃。一方面，不少问题还有待解决，正如日本数学家弥永昌吉所说，“这个理论的大部分仍然笼罩在神奇的面纱之下”。另一方面，数论这一数学分支成绩斐然，尤其是近年来取得了不少举世瞩目的重大成果(例如莫德尔猜测的解决、高斯类数猜测的解决等等)。

很多数论问题(例如哥德巴赫问题)可以从经验中归纳出来，并且能用三言两语向任何一个路过的人解释清楚，但

是要证明它们却远非容易。这也正是数论所特有的奇妙的魅力，使得它既被专业数学家所重视，又被业余研究者所宠爱，甚至使有些人象吃了忘忧果似的，“一次吃了这种果实就再也离不开它了。”

这本小册子试图对数论作一点通俗的介绍，希望能使读者对于数论有所了解并感到兴趣。所用知识不超过中学数学，有初中水平的人就可以读懂绝大部分内容，个别章节稍难一些，在第一次阅读时不妨略去。

余红兵同志在本书的写作过程中提出了不少宝贵的意见与建议，作者表示深深的感谢。

作 者

目 录

一 你最熟悉的朋友——自然数…………… (1)

1. 华生的第一个问题 (2)
2. 巨轮的长 (3)
3. 孩子与门牌号码 (3)
4. 荷兰人买猪 (4)
5. 创记录的因数分解 (6)
6. 被 2160 整除的立方数 (7)
7. 哪几盏灯亮着? (8)
8. 何时重逢 (9)
9. 丢番图的墓碑 (10)
10. 请添三个数字 (11)
11. 欧几里得永垂不朽 (12)
12. 因数分解的妙法 (13)
13. 十全数 (15)
14. 十全数的韧性 (17)
15. 分油问题 (18)
16. 辗转相除法与裴蜀恒等式 (19)
17. 货物的单价 (21)
18. 能变成均等吗? (21)
19. 素数的一个特征 (22)
20. 最大公约数的性质 (23)
21. 唯一分解定理的证明 (24)

二 多角数、完全数及其他…………… (27)

1. 三角形与三角数 (27)
2. 等差数列的求和 (29)
3. 正方形与平方数 (29)
4. 平方数与平方式 (31)
5. 五边形与五角数 (32)
6. 立体图形 (33)
7. 一些不难证明的公式 (35)
8. 一个不平凡的结论 (36)
9. 什么数恰好有 60 个因数? (38)
10. 因数的和 (39)
11. 完全数——人们对它的认识并不完全 (40)
12. 亲和数 (42)
13. 高阶亲和数 (43)

三 素数——是永恒的谜吗?…………… (45)

1. 是合数还是素数? (45)
2. 乘法公式大显身手 (46)
3. 爱拉托斯散的筛子 (47)
4. 殆素数与 $1+2$ 的 2 (49)
5. 辛勤劳动的结晶——素数表 (50)
6. 最大的素数 (51)
7. 修道士的工作——梅森数 (51)
8. 费尔马说错了 (53)
9. 正十七边形的尺规作图 (54)
10. 欧几里得的巧妙证明 (55)
11. 费尔马数与素数的无限性 (56)
12. 量与质 (57)
13. 素数定理 (58)

14. 算术级数中的素数 (60) 15. 素数之间的间隙 (61) 16. 一个容易的问题 (62) 17. 几个无理数 (62) 18. “天造地设”的素数幻方 (63) 19. 有表示素数的公式吗? (64) 20. 哥德巴赫猜测 (66) 21. 两个合数的和 (67) 22. 孪生素数 (67) 32. 又一些猜测与问题 (68) 24. 一个被推翻了的猜测 (70)

四 大师的发明——同余…………… (71)

1. 华生的新把戏 (72) 2. 同余 (73) 3. $1+1=0$ (74) 4. 在费尔马失足的地方 (76) 5. 整除的判别法 (76) 6. 一个简单的数字问题 (78) 7. 求余数 (78) 8. 47^{47} 的个位数字 (79) 9. $1 \times 3 \times 5 \times \cdots \times 1989$ 的末三位数字 (80) 10. 华生难倒了福尔摩斯 (81) 11. 整除问题举例 (82) 12. 三角数与偶完全数的末位数字 (84) 13. $11 \cdots 1$ 不是平方数 (85) 14. 平方数的末尾能有几个 4? (85) 15. 平方数的末位数字 (86) 16. 用 1, 2, 3, 4, 5, 6, 7 作成的七位数 (87) 17. 无相同项的两个数列 (88) 18. 完全剩余系 (89) 19. 有超韧性数吗? (91) 20. 抽屉原则牛刀小试 (91) 21. 在不定方程中的应用 (92) 22. 在堆垒问题中的应用 (94)

五 欧拉的 φ 函数…………… (97)

1. 放石子 (98) 2. 空格有了石子 (99) 3. 染色问题 (101) 4. $\varphi(n)$ 的计算公式 (102) 5. 一个求和问题 (103) 6. 副产品 (104) 7. 30 有惊人的性质 (104) 8. $\varphi(n)$ 是积性函数 (106) 9. “我正是这样想的!” (107) 10. 卡片上的数 (108) 11. 欧拉定理 (109) 12. 7 的幂结尾能是 0000001 吗? (110) 13. 数字全不为 0 的倍数 (110) 14. 7^{9999} 的末三位数字 (111) 15. 费尔马小定理 (111) 16. 伪素数 (112) 17. 群、环、域 (113)

六 一些不定方程的解…………… (115)

1. 百鸡问题 (115) 2. 另有妙法 (116) 3. 中国剩余定理 (119) 4. 太阳神的牛 (120) 5. 勾股数 (122) 6. 换一换汤 (124) 7. 复数与勾股数 (125) 8. $x^2 + y^2 = (y+1)^2$ 的解 (126) 9. 单位圆上的有理点 (127) 10. 距离为整数的整点 (128) 11. 成等差数列的三个平方数 (129) 12. 弹子的

个数 (130) 13. 张冠李戴的沛尔方程 (131) 14. 最小解与一般解 (132) 15. 罗马军团问题 (134) 16. 方程 $x^2 - 2y^2 = \pm 1$ (134) 17. 勾股为连续的自然数 (136) 18. 小红家的号码 (138) 19. 方程 $x^2 - dy^2 = n$ (140)

七 机器人与坑 (142)

1. 罗伯特落入坑里 (142) 2. 重蹈覆辙 (143) 3. 结论与问题 (144) 4. 小心地雷! (144) 5. 罗伯特家族 (145) 6. 狄利克雷定理 (147) 7. 克罗内克尔定理 (148) 8. 幂的前 n 位数字 (149) 9. 马勒的定理 (149)

八 形形色色的初等问题 (151)

1. 哥伦布式的问题 (151) 2. 笛卡尔不敢动手 (152) 3. 欧拉的恒等式 (154) 4. -1 是平方和 (155) 5. 递降法 (156) 6. 威尔逊没有证明的威尔逊定理 (157) 7. 两个完系相乘能是完系吗? (159) 8. 平方和及其他 (160) 9. 华林问题 (163) 10. 任意的七个整数 (164) 11. 剩余类相加 (165) 12. 从 7 到 $2n-1$ (168) 13. 美国竞赛题 (170) 14. $n!$ 中 p 的次数 (172) 15. 二项式系数中哪些是奇数? (174) 16. 一道国际数学竞赛题 (176) 17. $\frac{1}{a} + \frac{1}{a+d} + \frac{1}{a+2d} + \cdots + \frac{1}{a+nd}$

不是整数 (178) 18. 最小公倍数的上界 (180) 19. 证明的完成 (181) 20. 解题能手的问题 (184) 21. 数论中的三颗明珠 (186)

九 分析与数论缔结姻缘 (189)

1. 张教授堆砖 (189) 2. 收敛与发散 (191) 3. 这里又出现了欧拉 (193) 4. 黎曼 ζ 函数 (194) 5. “我证明了黎曼假设!” (196) 6. 几乎所有 (197) 7. 圆法 (200)

十 固若金汤的城堡——费尔马大定理 (202)

1. $x^4 + y^4 = z^4$ 无解 (203) 2. 欧拉迈出了第一步 (205) 3. 化名的女数学家 (205) 4. 从欧拉到库麦尔 (207) 5. 什么是整数 (208) 6. 高斯整数 (209) 7. $\mathbb{Z}[i]$ 中的唯一分解定理 (211) 8. 再谈勾股数 (212) 9. 1847 年发生的事 (214) 10. 唯一分

解定理不一定成立 (216) 11. 更通俗的例子 (217) 12. 理想
与青春之梦 (218) 13. 伯努利数与正规素数 (220) 14. 二次
域 (222) 15. 证实高斯猜测的历程 (223) 16. 近年来的两大进
展 (226) 17. 猜测与反例 (228) 18. 费尔马有没有找到证
明 (229)

— 你最熟悉的朋友——自然数

有一位数学家克罗内克尔 (1823-1891) 说: “上帝创造了自然数, 其余的都是人工。” 其实, 自然数也是人类创造出来的, 它是我们最熟悉的朋友。

自然数 (也就是正整数)

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, ... 可以分为三类:

第一类只有一个成员, 就是 1, 称为单位。

第二类中的成员称为素数 (也就是质数), 每个素数恰好有两个因数 (即约数): 1 和这个数本身。例如

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 都是素数。

第三类中的成员称为合数, 每个合数至少有三个因数, 即除了 1 和这个数本身以外还有其他的因数 (这样的因数称为真因数)。例如 4 有三个因数 1、2、4, 其中 2 是真因数, 所以 4 是合数。

每一个自然数 n 都可以分解为质 (素) 因数的乘积, 即有分解式

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}. \quad (1)$$

其中 $p_1, \dots, p_k$ 是不同的素数, $a_1, a_2, \dots, a_k$ 是正整数 (当 $n=1$ 时, 约定 (1) 式右边为 1), 例如

$$12 = 2 \times 2 \times 3, 15 = 3 \times 5.$$

并且除了因数的顺序以外，这种分解是唯一的。这称为算术基本定理，也叫做唯一分解定理。

除非特别申明，本书中的数（字母）都表示自然数。

1. 华生的第一个问题

《福尔摩斯探案》是脍炙人口的故事。

且说，有一天，大侦探歇洛克·福尔摩斯在家里闲着无事，他觉得十分烦闷。

“太无聊了，”福尔摩斯说，“最近一件值得动点脑筋的案子都没有！”

“我知道你又要犯老毛病了，”他的挚友华生医生说，“忧郁症，你得做点体操。”

“对，得做点思维的体操。你出个数学题给我做吧。”

“那好，”华生看了看桌上的纸说，“我这里有三个自然数，它们的和是 338，你能求出这三个数是多少吗？”

“你不觉得条件少了点吗？”

“我再添个条件。嗯，它们的积是 1986。”

“1986？哈哈！你这个条件太有用了。你面前的三个数是 1, 6, 331。”

“你可真行！怎么求出来的？”

“虽然你先说的条件是和，但我解题的时候并不一定非要从第一个条件开始。这类问题得从乘积入手，把它分解为

$$1986 = 2 \times 3 \times 331.$$

你那三个数的和是 338，所以最大的一个一定是 331，不能是 2×331 ， 3×331 ，更不能是 6×331 。另两个呢？如果是 2、3，它们的和是 336，所以只能是 1、6，它们的和恰

好是338。”

2. 巨轮的长

阿道克船长（《丁丁历险记》中的主要人物）远航归来，一些朋友来拜访他，其中一位问道：

“阿道克，你驾驶的这艘巨轮长多少英尺①？”

“英尺数是个整数，”船长回答说，“如果把它乘以我的年龄，再乘以这里的人数，得出的积是32118。”

这位朋友如果懂一点算术，他就会把32118分解为

$$32118 = 2 \times 3 \times 53 \times 101。$$

由此可以得出巨轮长101英尺，阿道克的年龄是53，客人的人数是5。

3. 孩子与门牌号码

主人对客人说：

“院子里有三个小孩在做游戏，他们的年龄的积是72，年龄的和恰好等于我家的门牌号码——这你是知道的。你能求出这些孩子的年龄吗？”

聪明的客人想了一下说：“我不能马上就确定答案。”

他站起来，走到窗前看了看楼下的孩子。

“哦，有两个很小的孩子。我知道他们的年龄了。”

更聪明的读者，你能知道主人的门牌号码是多少吗？

这个问题有点难，不过用到的知识并不多，只要读者弄清题意，仔细思考，就可以解决。

首先，三个孩子年龄的积是72，因此，我们把72分解

① 英尺是英制长度单位， 1英尺=0.3048米。

为三个因数（不一定是质因数）的积，并把各种可能的结果列成下表（表中的每个因数都小于 24，因为它们表示孩子们的年龄）。

年	1	1	1	2	2	2	2	3	3
	4	6	8	2	3	4	6	3	4
龄	18	12	9	18	12	9	6	8	6
和	23	19	18	22	17	15	14	14	13

表中每一列的前三个数表示小孩的年龄，最下面的一个数是它们的和。例如第一列表示三个小孩的年龄分别是 1, 4, 18(乘积为 72)，他们的和是 23。

在表中只有两个和是相等的，都等于 14，14 就是主人的门牌号码。

为什么呢？因为聪明的客人知道主人的门牌号码，也就是三个小孩的年龄的和，如果门牌号码不是 14，他就可以立即确定孩子们的年龄，而不会说“我不能马上就确定答案。”

至于孩子的年龄，我们也能够求出来。因为客人说“有两个很小的孩子”，所以孩子们的年龄应当是 3, 3, 8(和为 14，而不是 2, 6, 6(和也为 14))。

4. 荷兰人买猪

“现在我出一个真正的难题给你做，歇洛克。”

“你出吧！”福尔摩斯躺在沙发上懒懒地说。

“好，你听我说。三个荷兰人 x, y, z 与他们的妻子 $u, v,$

w 上集镇去买猪。每个人买的猪的头数恰好等于他(她)买的每一头猪所用的元数。每个男人比他的妻子多用 63 元,并且 x 比 v 多买 23 头猪, y 比 u 少 19 头猪,问谁是谁的妻子?”

“你的题目中没有肯定 x 的妻子是 u , y 的妻子是 v , z 的妻子是 w ?” 福尔摩斯问。

“当然,当然没有肯定谁的妻子是谁。” 华生说,“否则,我还会问你吗?”

“这道题确实有点难。不过,” 福尔摩斯一跃而起,用铅笔在纸上写了几道式子,“我们可以这样来解:

用 M 表示一位男人买的猪的头数, W 表示他的妻子买的猪的头数,根据题意他们用的钱分别为 M^2 元与 W^2 元,并且

$$M^2 - W^2 = 63。$$

一方面

$$M^2 - W^2 = (M + W)(M - W),$$

另一方面,把 63 表示成两个因数(不一定是质因数)之积,有以下几种方式

$$63 = 63 \times 1 = 21 \times 3 = 9 \times 7。$$

如果

$$M + W = 63,$$

$$M - W = 1,$$

那么

$$M = \frac{63+1}{2} = 32,$$

$$W = \frac{63-1}{2} = 31。$$

其余的两种情况可以同样处理,综合起来得到下面的表

M	32	12	8
W	31	9	1

在表中只有 32 与 9 的差是 23, 因此 x 买了 32 头猪, v 买了 9 头猪。同样, 由于表中只有 31 与 12 的差是 19, 所以 y 买了 12 头猪, u 买了 31 头猪。

表中 32、31 是一对夫妻分别买的猪二头数, 所以 u 是 x 的妻子。同样, v 是 y 的妻子。最后, w 当然是 z 的妻子。

5. 创纪录的因数分解

别以为分解因数容易, 数一大可就不好办了。例如

4294967297

是合数还是质数? 如果是合数, 你能找出它的质因数吗? 你能把它分解为质因数的连乘积吗?

这是一个 10 位数, 如果是 100 位数, 那就更困难了。虽然用超高速计算机不难判别它是不是质数, 但是要找出一个大合数的分解式却极不容易。数太大了, 连计算机对它也无可奈何。因此, 有人建议用 80 位以上的数作为密钥(译解密码的钥匙), 发送密码。已方接收人员预先知道这密钥的因数分解, 可以把密码译出来。敌方即使知道发送密码时所用的密钥(80 位以上的数), 但不知道它的分解式, 借助于计算机也无法在短期内破译, 所以这种密钥称为公开密钥。

但是, 这种想法(利用难分解的大合数作公开密钥)最近受到了严重的冲击。1984 年美国的西蒙斯与沃诺克利用一种新型计算机及新编制的程序, 仅花了三小时十二分钟就把一个 69 位数