



数论经典著作系列

Outline of Number Theory

数论概貌

陈景润 著



哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS



Outline of Number Theory

数论概貌

● 陈景润 著



哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

0156
0015



内容提要

数论是一门研究数的性质的科学,有着丰富的内容。本书旨在通俗地向读者介绍数论的基本内容、典型问题和主要方法,全书共分三章,即:初等数论、解析数论、代数数论。书中结合几个主要问题(例如哥德巴赫猜想、费马大定理)而引进若干概念,介绍一些近代的方法和研究成果,以使读者能从中了解数论这一数学分支的大致面貌。

本书是一本科普书,具有中等文化程度的读者即可读懂,因而可供对数论有兴趣的读者阅读、参考。

图书在版编目(CIP)数据

数论概貌/陈景润著. —哈尔滨:哈尔滨工业大学出版社,2011.3

ISBN 978-7-5603-3200-0

I. ①数… II. ①陈… III. ①数论 IV. ①O156

中国版本图书馆CIP数据核字(2011)第029112号

策划编辑 刘培杰 张永芹

责任编辑 范业婷

封面设计 孙茵艾

出版发行 哈尔滨工业大学出版社

社 址 哈尔滨市南岗区复华四道街10号 邮编 150006

传 真 0451-86414749

网 址 <http://hitpress.hit.edu.cn>

印 刷 哈尔滨市石桥印务有限公司

开 本 787mm×1092mm 1/16 印张 3.5 字数 56千字

版 次 2011年3月第1版 2011年3月第1次印刷

书 号 ISBN 978-7-5603-3200-0

定 价 18.00元

(如因印装质量问题影响阅读,我社负责调换)

数论是研究数的性质的一门科学,是数学的一个分支学科.

人类对数论的研究,渊源久远.早在古希腊时代,就已取得了许多成果.欧几里得(Euclid)的《原本》一书中,就记有素数有无限多个(及其证明)、整数的因数分解、欧几里得除法(即辗转相除法,用以求两个数的最大公因数)、关于完全数的一个著名定理等;作为古希腊的成就,还有寻求素数的埃拉托色尼(Eratosthenes)筛法,阿基米得(Archimedes)对不定方程所作的研究等.亚历山大里亚时代的丢番图(Diophantus)曾对不定方程进行了深入的研究.当然,在数论的发展史上,更应该提到的是法国业余数学家费马(P. S. de Fermat)、德国数学家高斯(C. F. Gauss)以及狄里克雷(P. G. Dirichlet).

我国古代,在数论方面也有极其光辉的成就.例如商高定理(勾股定理)、孙子定理(被西方人称为“中国剩余定理”)都为世人所瞩目.近代,我国数学工作者在解析数论、丢番图方程、一致分布等方面,都作出了重要贡献.特别是华罗庚教授在三角和估计以及堆垒数论方面,成就卓著.近三十多年来,我国的数论研究队伍中新人辈出,在哥德巴赫(C. Goldbach)问题、算术级数中的最小素数问题、L函数的零点问题以及三角和的估计等问题上,更进一步获得了许多优秀的成果.

数论按照所运用的研究方法的不同,又分为初等数论、解析数论、代数数论、几何数论等,下面择要加以介绍.

◎
目
录

第一章 初等数论 //1

1. 整数的整除性 //1
2. 最大公因数和最小公倍数 //3
3. 不定方程 //5
4. 同余 //8
5. 完全剩余系 //11
6. 连分数 //12
7. 素数分布 //17
8. 关于完全数和梅森素数 //20

第二章 解析数论 //22

1. 三角和 //23
2. 古典筛法 //24
3. 大筛法 //25
4. 大筛法在证明哥德巴赫猜想中的应用 //27
5. 黎曼 ζ 函数 //30
6. 狄里克雷特征 //32
7. 狄里克雷 L 函数 //33

第三章 代数数论 //36

编辑手记 //41

初等数论

第

一

章

初等数论是仅仅利用初等数学的方法,而不借助于其他数学工具,去研究整数的性质.它主要包括:整除性、不定方程、同余式、连分数等.

1. 整数的整除性

大家知道,整数对于加法、减法、乘法是封闭的,即:整数加整数、整数减整数、整数乘以整数,其结果仍然是整数.但是,整数除以整数就不一定得到整数了.于是,产生了数论的一个基本问题——研究一个整数能否被另一个整数整除的问题:

如果三个不为零的整数 a, b, c , 满足

$$a = b \cdot c$$

我们就说“ a 能被 b 整除”(或“ a 能被 c 整除”),记为 $b \mid a$ (或 $c \mid a$),并说“ b (或 c) 是 a 的一个因数”;而且,当 b 或 c 不为 a 或 1 时,称 b (或 c) 是 a 的一个真因数.否则,就说“ a 不能被 b (或 c) 整除”,记为 $b \nmid a$ (或 $c \nmid a$).我们把这个基本问题,称为整数的整除性.

我们以 $[\alpha]$ 表示不超过数 α 的最大整数.例如, $[3] = 3, [\sqrt{2}] = 1, [\pi] = 3, [-\sqrt{2}] = -2, [-4.5] = -5$.那么,显然成立下面的不等式:

$$[\alpha] \leq \alpha < [\alpha] + 1$$

对于两个整数 a 和 b (其中 $b > 0$)的商,有

$$\left[\frac{a}{b}\right] \leq \frac{a}{b} < \left[\frac{a}{b}\right] + 1$$

即

$$0 \leq a - b\left[\frac{a}{b}\right] < b$$

于是,我们有

$$a = \left[\frac{a}{b}\right]b + r$$

这里 $0 \leq r < b$.

因此,给定任意两个整数 a, b (其中 $b > 0$),必存在整数 q, r ,使

$$a = qb + r$$

这里 $0 \leq r < b$.

当 $r=0$ 时,就是前面所说的“ b 能整除 a ”;当 $r \neq 0$ 时,即是“ b 不能整除 a ”.

为了研究整数的整除性,人们把正整数分为如下三类:

- (1) 1: 它只有 1 为其因数;
- (2) p : 它只有 1 和 p 为其因数,即 p 大于 1 且无真因数;
- (3) n : 有真因数.

我们把上述第二类数叫做素数(在有些书上也称之为质数),把上述第三类正整数叫做复合数(有些书上也称之为合数).显然,大于 2 的偶数必有真因数 2,都是复合数.

把素数按照大小进行排列,可以得到下面的数列(通常称为素数列):

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, \dots$$

在古希腊,欧几里得就已证明了素数有无穷多个,他采用了反证法:假设素数只有有限个,不妨设这有限个不同的素数是 p_1, p_2, \dots, p_n ;我们来考察整数 $a = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$,依假定, a 显然异于任一素数,因而是一个复合数;于是,根据复合数的定义, a 应该有一个素因数 p ,但 $p \nmid 1$ 而 $p \mid p_1 \cdot p_2 \cdot \dots \cdot p_n$,可知 $p \nmid a$,这就和前面导出的 p 是 a 的素因数产生了矛盾,究其原因,是假设了素数只有有限个是错误的,这就证明了素数有无穷多个.

关于素数分布的研究,是很有趣,又很困难的.本书在下面的章节里还将讲到.

算术基本定理 每一个大于 1 的整数 n ,可唯一地表示为

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_k^{a_k}$$

的形状,这里素数 $p_1 < p_2 < \cdots < p_k$,而 a_1, a_2, \cdots, a_k 是大于 0 的整数.

这个定理的证明,仅用简单的初等方法就可完成,但定理的结论是非常深刻的.它反映了素数在整数中的基本作用,揭示了整数的一个基本性质——积性.

2. 最大公因数和最小公倍数

如果 a, b 是非零整数,而整数 q 同时是 a, b 的因数,我们便把 q 叫做 a, b 的公因数.

显然, q 的绝对值必不大于 a, b 的绝对值的最小者:

$$|q| \leq \min\{|a|, |b|\}$$

上式表明,两个非零整数的公因数必只有有限多个.于是,其中一定有一个最大的;我们把 a 和 b 的所有公因数中的最大一个公因数 d ,叫做 a 和 b 的最大公因数,记作 $d = (a, b)$.

已知两个非零整数 a 和 b ,怎样求出它们的最大公因数呢?当然,可以利用上面的算术基本定理;但是,更简单的办法是采用辗转相除法,这一方法最早见于欧几里得的《原本》(公元前 3 世纪),我国古算书《九章算术》(约成书于东汉初年,公元 1 世纪)也记有这一方法.

用辗转相除法求两个非零整数的最大公因数的具体步骤如下:(不妨设 a 与 b 都是正整数,且 $a > b$)

先用 b 除 a ,得到正整数 q_1 ,使

$$a = q_1 b + r_1 \quad (0 \leq r_1 < b)$$

若 $r_1 = 0$,则由 $a = q_1 b$ 知 a 与 b 的最大公因数是 b .若 $r_1 \neq 0$,由 $0 < r_1 < b$,可再以 r_1 除 b ,于是又可得正整数 q_2 和非负整数 r_2 ,使

$$b = q_2 r_1 + r_2 \quad (0 \leq r_2 < r_1)$$

以 (a, b) 表 a 与 b 的最大公因数,则可知

$$(a, b) = (b, r_1)$$

当 $r_2 = 0$ 时,可知 $(a, b) = (b, r_1) = r_1$.若 $r_2 \neq 0$,由 $0 < r_2 < r_1$,可再以 r_2 除 r_1 ,得正整数 q_3 和非负整数 r_3 ,使

$$r_1 = q_3 r_2 + r_3 \quad (0 \leq r_3 < r_2)$$

于是,当 $r_3 = 0$ 时,有 $(a, b) = (b, r_1) = (r_1, r_2) = r_2$.若 $r_3 \neq 0$,则由 $0 < r_3 < r_2$,又可再以 r_3 除 r_2, \cdots 这样继续辗转相除,由于 $b > r_1 > r_2 > r_3 > \cdots$ 且各 r_i (这里 $i = 1, 2, 3, \cdots$) 皆是非负整数,则一定存在一个正整数 n ,使经过 $n + 1$ 次辗转

相除后,有 $r_{n+1} = 0$ 但 $r_n \neq 0$. 这时,就可得到 $(a, b) = r_n$.

这就通过辗转相除,求出了 a 和 b 的最大公因数.

两个非零整数的最大公因数的性质,主要有:如果 $(a, b) = d$, 则存在整数 m, n , 使

$$ma + nb = d \quad (1)$$

这里的整数 m 和 n , 可由辗转相除法求得 $(a, b) = r_n$ 后, 逐次向上一算式回代而得.

如果 $(a, b) = 1$, 我们称 a 和 b 是互素的. 当然, 互素的整数中, 可以不一定有素数. 例如 $(25, 26) = 1$, 但 25 和 26 都是复合数.

对于非零整数 a, b , 如果 m 同时是 a, b 的倍数, 我们便把 m 叫做 a 和 b 的公倍数.

可以看出, a 和 b 的公倍数有无穷多个. 例如, 它们的积 ab 即是它们的一个公倍数, 而这一乘积的任意倍数都是它们的公倍数. 我们把 a 和 b 的公倍数中的最小的一个数 M , 叫做 a 和 b 的最小公倍数, 记作 $M = \{a, b\}$.

当然, 两个非零整数的最小公倍数, 也可以利用上面的算术基本定理而求得.

下面, 我们来证明关于最大公因数和最小公倍数之间的一个结果: 正整数 a 与 b 的乘积, 可以表示成

$$ab = (a, b) \cdot \{a, b\} \quad (2)$$

证明 因 ab 为 a 与 b 的公倍数, 而 $\{a, b\}$ 为 a 与 b 的最小公倍数, 故存在正整数 q , 使

$$ab = q \cdot \{a, b\}$$

从而 $\frac{a}{q} = \frac{\{a, b\}}{b}$, $\frac{b}{q} = \frac{\{a, b\}}{a}$; 而 $\frac{\{a, b\}}{b}$ 与 $\frac{\{a, b\}}{a}$ 皆为正整数, 所以 $q \mid a, q \mid b$, 即

q 为 a, b 的公因数. 又设 g 为 a, b 的任一公因数, 令 $m = \frac{ab}{g}$. 由于 $\frac{a}{g}$ 及 $\frac{b}{g}$ 都是正

整数, 又 $m = a\left(\frac{b}{g}\right) = b\left(\frac{a}{g}\right)$, 故 m 是 a 和 b 的公倍数, 从而 $\{a, b\} \mid m$, 即 $\frac{m}{\{a, b\}}$ 是一个正整数. 又由

$$\frac{m}{\{a, b\}} = \frac{ab}{g\left(\frac{ab}{q}\right)} = \frac{q}{g}$$

故 $\frac{q}{g}$ 也是正整数, 即 $g \mid q$. 由 g 的任意性, 可知 $q = (a, b)$, 这就证明了式(2)成立.

3. 不定方程

如果未知数的个数多于方程的个数,这样的方程叫做不定方程.例如,方程

$$\begin{aligned} ax + by &= c \\ ax + by + cz &= d \\ ax^2 + bxy + cx + dw &= 0 \end{aligned}$$

等等,都是不定方程.

研究整系数不定方程的整数解,是数论中饶有趣味的问题之一.5世纪末,我国古代数学家张丘建曾编写了一部《算经》,书中提出了一个不定方程问题——世界数学史上有名的“百鸡问题”:

鸡翁一,值钱五.鸡母一,值钱三.鸡雏三,值钱一.百钱买百鸡,问鸡翁、母、雏各几何?

(用现在的白话文来说,就是:每一只公鸡的售价是五个钱,每一只母鸡的售价是三个钱,每三只小鸡的售价是一个钱;现有100个钱,想买100只鸡,问公鸡、母鸡和小鸡各应买几只?)

假设用 x, y, z 分别代表买公鸡、母鸡和小鸡的数目,就得到下面的两个方程

$$\begin{cases} 5x + 3y + \frac{z}{3} = 100 \\ x + y + z = 100 \end{cases}$$

由这两个方程,我们得到

$$\begin{aligned} 200 &= 300 - 100 = 3\left(5x + 3y + \frac{z}{3}\right) - (x + y + z) = \\ &15x + 9y + z - x - y - z = \\ &14x + 8y \end{aligned}$$

也就是

$$7x + 4y = 100$$

我们要解“百鸡问题”,就是要寻求 $7x + 4y = 100$ 的非负整数解.

这里的 $7x + 4y = 100$,是一个二元一次不定方程.二元一次不定方程的一般形式是

$$ax + by = c \quad (3)$$

其中 a, b, c 都是整数.

定理 设二元一次不定方程

$$ax + by = c \quad (3)$$

(其中 a, b, c 都是正整数,而 $(a, b) = 1$)有一组整数解 $x = x_0, y = y_0$,则它的一切

整数解可以表示成

$$x = x_0 - bt, \quad y = y_0 + at \quad (4)$$

的形式,其中 $t = 0, \pm 1, \pm 2, \dots$.

这一定理的证明,可参看一般初等数论书中有关不定方程的讨论,这里从略.

应用这一定理,很容易得出“百鸡问题”的解答.首先,易见 $s = -1, t = 2$ 是不定方程

$$7s + 4t = 1$$

的一组整数解;由此得知 $x = -100, y = 200$ 是

$$7x + 4y = 100$$

的一组整数解.于是, $7x + 4y = 100$ 的一切整数解可以表示成为

$$x = -100 - 4t, \quad y = 200 + 7t$$

的形式,其中 $t = 0, \pm 1, \pm 2, \dots$. 在“百鸡问题”中,由于 x, y 分别代表公鸡、母鸡的只数,所以必有 $x \geq 0, y \geq 0$. 由 $-100 - 4t \geq 0$ 得到 $t \leq -25$, 由 $200 + 7t \geq 0$ 得到 $t \geq -\frac{200}{7}$, 因此有

$$-\frac{200}{7} \leq t \leq -25$$

由于 t 是整数,故有 $t = -28, -27, -26, -25$. 又,小鸡的只数是

$$\begin{aligned} z &= 100 - x - y = \\ &= 100 - (-100 - 4t) - (200 + 7t) = \\ &= -3t \end{aligned}$$

这样,我们就得到了“百鸡问题”的四组解答:

$$x_1 = 12, y_1 = 4, z_1 = 84$$

$$x_2 = 8, y_2 = 11, z_2 = 81$$

$$x_3 = 4, y_3 = 18, z_3 = 78$$

$$x_4 = 0, y_4 = 25, z_4 = 75$$

下面再来介绍人们很早就认识了另一个不定方程:

$$x^2 + y^2 = z^2 \quad (5)$$

其中 x, y, z 为正整数. 上述不定方程,即是通常所谓的求勾股数组的问题. 据史料记载,最简单的一组解 $3^2 + 4^2 = 5^2$ 至迟在四千多年前就已被发现. 古希腊的毕达哥拉斯(Pythagoras)发现了上述不定方程的部分解的公式:设 m 是奇数

$$x = m, \quad y = \frac{m^2 - 1}{2}, \quad z = \frac{m^2 + 1}{2} \quad (6)$$

丢番图也证明了一个部分解的公式:设 m 和 n 是正整数,而 $2mn$ 是一个完全平方数,则

$$\left. \begin{aligned} x &= m + \sqrt{2mn} \\ y &= n + \sqrt{2mn} \\ z &= m + n + \sqrt{2mn} \end{aligned} \right\} \quad (7)$$

现今所用的通解公式则是:设 m 和 n 是正整数, $m > n$, $(m, n) = 1$, $2 \nmid (m + n)$, 则方程(5)的满足条件 $(x, y) = 1, 2 \mid x$ 的一切正整数解可表示成:

$$\left. \begin{aligned} x &= 2ab \\ y &= a^2 - b^2 \\ z &= a^2 + b^2 \end{aligned} \right\} \quad (8)$$

通常认为,式(8)是由罗士琳(1789 ~ 1853)得到的,故被称作罗士琳公式.

上面通过“百鸡问题”,介绍了二元一次不定方程的一种一般解法;又介绍了一个二次不定方程——求勾股数组的解,值得注意的是有不少不定方程,解题的特殊性很强,对一个方程适用的方法往往不再适用于另一个方程,要像二元一次方程那样寻求一种“一般解法”实在是困难的.迄今为止,关于不定方程尚有许多未知领域,真是向人类智慧的挑战.

谈到不定方程,很值得一提的是方程(5)的推广: $x^3 + y^3 = z^3, x^4 + y^4 = z^4, \dots$,一般地, $x^n + y^n = z^n$. 法国业余数学家费马于1637年提出了一则猜想(通常称为“费马大定理”):当 n 是一个大于2的整数时,不定方程

$$x^n + y^n = z^n \quad (9)$$

没有正整数解. 费马的这一猜想迄今还未被人们证明^①. 1976年时瓦格斯塔夫(S. Wagstaff)借助于大型电子计算机证得 $2 < n < 125\,000$ (当然还包括这些数的任何整倍数)情况下这一猜想是成立的. 1983年,联邦德国数学家法尔丁斯(G. Faltings)在《数学创造》杂志上(Invent. Math.)发表了题为《数域上阿贝尔簇的有限性》一文. 在此文章中,他以代数几何为主要工具,证明了莫德尔(L. J. Mordell)1922年提出的一个猜想:数域上任一个亏格 ≥ 2 的非奇异射影曲线仅有有限多个点的坐标在此数域中. 注意到 $n \geq 3$ 时,方程(9)定义的曲线满足莫德尔猜想的条件. 于是,由莫德尔猜想,立即推出方程(9)对每个 $n \geq 3$ 最多只有有限组正整数解. 但是,法尔丁斯的方法并未给出方程(9)中解的个数或上界估计. 因而费马大定理仍然未能解决. 法尔丁斯这一工作荣获1986年度国际数学家大会颁发的菲尔兹奖.

^① 策划编辑注:费马大定理已于1995年被怀尔斯(Wiles)和他的学生成功证明.

4. 同 余

如果 a 与 b 都是整数,而 m 是一个正整数; $(a-b)$ 可以被 m 整除,即 $m \mid (a-b)$ 时,我们称“ a, b 对模 m 同余”,记作 $a \equiv b \pmod{m}$;当 $m \nmid (a-b)$ 时,称“ a, b 对模 m 不同余”,记作 $a \not\equiv b \pmod{m}$.

显然,我们有

$$a \equiv a \pmod{m};$$

若 $a \equiv b \pmod{m}$,则 $b \equiv a \pmod{m}$;

若 $a \equiv b \pmod{m}$ 和 $b \equiv c \pmod{m}$,则 $a \equiv c \pmod{m}$.

关于同余,还有下列结果:若

$$a_1 \equiv b_1 \pmod{m}$$

$$a_2 \equiv b_2 \pmod{m}$$

$$\vdots$$

$$a_n \equiv b_n \pmod{m}$$

则有

$$a_1 \pm a_2 \pm \cdots \pm a_n \equiv b_1 \pm b_2 \pm \cdots \pm b_n \pmod{m} \quad (10)$$

$$a_1 a_2 \cdots a_n \equiv b_1 b_2 \cdots b_n \pmod{m} \quad (11)$$

例如,由式(11)和 $10 \equiv 1 \pmod{9}$,我们有 $10^n \equiv 1^n \pmod{9}$,即

$$10^n \equiv 1 \pmod{9} \quad (12)$$

又,设正整数

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_0$$

(其中 $0 \leq a_i \leq 9, 1 \leq a_n \leq 9; i = 0, 1, 2, \cdots, n-1$),则由式(10)、式(11)和式(12),有

$$a \equiv a_n + a_{n-1} + \cdots + a_0 \pmod{9} \quad (13)$$

根据式(13),我们可以很快地判别一个整数能否被9整除:即只需将这个整数的各位数上的数字加起来,看其数字和能否被9整除.例如221 145 236 415,它的各数位上的数字之和为

$$2 + 2 + 1 + 1 + 4 + 5 + 2 + 3 + 6 + 4 + 1 + 5 = 36$$

36是能被9整除的,故221 145 236 415亦能被9整除.

我们把

$$ax + b \equiv 0 \pmod{m} \quad (14)$$

称为“模 m 的一次同余式”,其中 a, b 是整数,且 $a \not\equiv 0 \pmod{m}$.

显然,如果整数 c 使式(14)成立,即 $ac + b \equiv 0 \pmod{m}$,则满足 $x \equiv c \pmod{m}$ 的一切整数 x 都能使式(14)成立.于是,我们称

$$x \equiv c \pmod{m}$$

为式(14)的一个解. 这就是说, 把适合式(14)的对模 m 相互同余的一切整数, 称为式(14)的一个解.

当 $(a, m) \nmid b$ 时, 一次同余式 $ax + b \equiv 0 \pmod{m}$ (其中 $a \not\equiv 0 \pmod{m}$) 没有整数解. 这可以用反证法来加证明: 若存在一个整数 c , 使 $ac + b \equiv 0 \pmod{m}$, 从而有

$$ac - mn = -b$$

其中 n 为一个整数; 又设 $(a, m) = l$, 则 $a = ld, m = le$ (其中 d 和 e 都是整数); 代入上式, 有

$$-b = ac - mn = cld - len = l(cd - en)$$

从而 $l \mid b$, 这与已知 $(a, m) \nmid b$ 矛盾.

我国古代的《孙子算经》(约公元 400 年) 提出了一个问题:

“今有物不知数, 三三数之剩二, 五五数之剩三, 七七数之剩二, 问物几何?”

对于这个题, 设 x 是所求的“物”的数目, 就可以把这个问题归结为求解下列同余式组

$$x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7} \quad (15)$$

关于求解一般同余式组

$$x \equiv a \pmod{3}, \quad x \equiv b \pmod{5}, \quad x \equiv c \pmod{7} \quad (16)$$

有

$$x \equiv 70a + 21b + 15c \pmod{105} \quad (17)$$

这个一般的解法, 在我国明朝程大位《算法统宗》(1593 年) 里, 有一首歌:

三人同行七十稀,
五树梅花廿一枝,
七子团圆整半月,
除百零五便得知.

可见关于解同余式组的问题, 在我国古代有极光辉的研究成果.

我国古代数学家孙子发明了下面中外驰名的“孙子定理”: 若 $k \geq 2$, 而 m_1, m_2, \dots, m_k 是两两互素的 k 个正整数. 又令

$$M = m_1 m_2 \cdots m_k = m_1 M_1 = m_2 M_2 = \cdots = m_k M_k$$

则同时满足同余式组

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \quad \dots, \quad x \equiv b_k \pmod{m_k} \quad (18)$$

的正整数解是

$$x \equiv b_1 M'_1 M_1 + b_2 M'_2 M_2 + \cdots + b_k M'_k M_k \pmod{M} \quad (19)$$

这里 M'_i 是满足同余式 $M'_i M_i \equiv 1 \pmod{m_i}$ 的正整数解, $i = 1, 2, \dots, k$.

证明 由于当 $i \neq j$ (其中 $i, j = 1, 2, \dots, k$) 时 $(m_i, m_j) = 1$, 故 $(M_i, m_i) = 1$, 即

$$(M_1, m_1) = (M_2, m_2) = \cdots = (M_k, m_k) = 1$$

于是, 存在整数 M'_i 和 n_i (其中 $i = 1, 2, \dots, k$), 使

$$M_i M'_i + m_i n_i = 1$$

即

$$M_i M'_i \equiv 1 \pmod{m_i}$$

又,当 $i \neq j$ 时,由 $(m_i, m_j) = 1$ 和 $M_j = \frac{M}{m_j}$,可知 $m_i \mid M_j$. 故有

$$b_j M'_j M_j \equiv 0 \pmod{m_i}$$

从而有

$$b_1 M'_1 M_1 + b_2 M'_2 M_2 + \cdots + b_k M'_k M_k \equiv b_i M'_i M_i \equiv b_i \pmod{m_i}$$

而 m_1, m_2, \cdots, m_k 两两互素,于是

$$x \equiv b_1 M'_1 M_1 + b_2 M'_2 M_2 + \cdots + b_k M'_k M_k \pmod{M}$$

是满足式(18)的正整数解.

又,若 y 也能同时满足式(18),则有

$$x \equiv y \pmod{m_1}, x \equiv y \pmod{m_2}, \cdots, x \equiv y \pmod{m_k}$$

即 $m_1 \mid (x - y), m_2 \mid (x - y), \cdots, m_k \mid (x - y)$, 所以有 $M \mid (x - y)$, 所以

$$x \equiv y \pmod{M}$$

因此

$$x \equiv b_1 M'_1 M_1 + b_2 M'_2 M_2 + \cdots + b_k M'_k M_k \pmod{M}$$

是式(18)的唯一解.

利用孙子定理,即可得到方程(15)的解. 这里, $m_1 = 3, m_2 = 5, m_3 = 7; b_1 = a, b_2 = b, b_3 = c$. 于是, $M = 105, M_1 = 35, M_2 = 21, M_3 = 15$. 又,设 M'_1 是一个正整数,满足 $M'_1 M_1 \equiv 1 \pmod{3}$, 则有 $1 \equiv M'_1 M_1 = 35 M'_1 \equiv 2 M'_1 \pmod{3}$, 得到 $M'_1 = 2$. 设 M'_2 是一个正整数,满足 $M'_2 M_2 \equiv 1 \pmod{5}$, 则有 $1 \equiv M'_2 M_2 = 21 M'_2 \equiv M'_2 \pmod{5}$, 得到 $M'_2 = 1$. 同理,可得 $M'_3 = 1$. 代入式(19),即可得到式(17).

我国古代所说的“韩信点兵”,就是用孙子定理来解决的一个例子,它是这样一个问题:有兵一列,若列成五行纵队,则末行一人;列成六行纵队,则末行五人;列成七行纵队,则末行四人,列成十一行纵队,则末行十人,求兵数.

对于这个题,设 x 是所求兵数,依题意,有

$$x \equiv 1 \pmod{5}$$

$$x \equiv 5 \pmod{6}$$

$$x \equiv 4 \pmod{7}$$

$$x \equiv 10 \pmod{11}$$

在孙子定理中,取 $m_1 = 5, m_2 = 6, m_3 = 7, m_4 = 11, b_1 = 1, b_2 = 5, b_3 = 4, b_4 = 10$, 此时,有 $M = 5 \times 6 \times 7 \times 11 = 2310, M_1 = 462, M_2 = 385, M_3 = 330, M_4 = 210$.

又,由 $1 \equiv M'_1 M_1 = 462 M'_1 \equiv 2 M'_1 \pmod{5}$, 得 $M'_1 = 3$; 由 $1 \equiv M'_2 M_2 = 385 M'_2 \equiv M'_2 \pmod{6}$, 得 $M'_2 = 1$; 由 $1 \equiv M'_3 M_3 = 330 M'_3 \equiv M'_3 \pmod{7}$, 得 $M'_3 = 1$; 由 $1 \equiv M'_4 M_4 = 210 M'_4 \equiv M'_4 \pmod{11}$, 得 $M'_4 = 1$. 从而

$$x \equiv 3 \times 462 + 5 \times 385 + 4 \times 330 + 10 \times 210 \equiv$$

$$\begin{aligned} 6731 &= \\ 2111 &(\text{mod } 2310) \end{aligned}$$

即可知

$$x = 2111 + 2310k$$

其中 $k = 0, 1, 2, \dots$.

我国古代杨辉的《续古摘奇算法》(1275年)和黄宗宪的《求术通解》等数学书中,还有许多类似“韩信点兵”的题目,这说明了我国古代数学家对初等数论做了大量深入的研究,并取得了丰硕的成果.

5. 完全剩余系

设 m 是一个大于 1 的整数,我们把能被 m 整除的所有整数(即形如 mn 的所有整数,其中 $n = 0, \pm 1, \pm 2, \dots$)划成一类;把被 m 除后余数是 $m-1$ 的所有整数(即形如 $mn + m - 1$ 的所有整数,其中 $n = 0, \pm 1, \pm 2, \dots$)划成一类……这样,我们就把全体整数分成为 m 类.如果从每一类中各取出一个整数,我们把取出的这 m 个整数叫做“模 m 的一个完全剩余系”.而把 $0, 1, \dots, m-1$ 称为“模 m 的非负最小完全剩余系”.

用 $\varphi(m)$ 表示不大于正整数 m 而和 m 互素的正整数的个数(通常把 $\varphi(m)$ 叫欧拉(L. Euler)函数).又设 $1 < a_2 < \dots < a_{\varphi(m)}$ 是不大于 m 而与 m 互素的 $\varphi(m)$ 个正整数.我们把被 m 除后余数是 1 的所有整数(即形如 $mn + 1$ 的所有整数,其中 $n = 0, \pm 1, \pm 2, \dots$)划为一类;把被 m 除后余数是 a_2 的所有整数(即形如 $mn + a_2$ 的所有整数,其中 $n = 0, \pm 1, \pm 2, \dots$)划为一类;……;把被 m 除后余数是 $a_{\varphi(m)}$ 的所有整数(即形如 $mn + a_{\varphi(m)}$ 的所有整数,其中 $n = 0, \pm 1, \pm 2, \dots$)划成一类.这样,我们把所有与 m 互素的整数分成 $\varphi(m)$ 类.从每一类中,各取出一个整数,则这 $\varphi(m)$ 个整数叫做“以 m 为模的一个简化剩余系”.

关于完全剩余系,有一个经过简单推导即可得到的结果:设 m 是一个大于 1 的整数,而 b, c 是两个任意的整数,但满足条件 $(b, m) = 1$. 如果 a_1, a_2, \dots, a_m 是模 m 的一个完全剩余系,则

$$ba_1 + c, \quad ba_2 + c, \dots, \quad ba_m + c$$

也是模 m 的一个完全剩余系.

模 m 的简化剩余系也有一个相应的结果,这虽没有上述结果完美,但却非常有用的:设 m 是一个大于 1 的整数, a 是一个整数,且满足条件 $(a, m) = 1$. 如果 $b_1, b_2, \dots, b_{\varphi(m)}$ 是模 m 的一个简化剩余系,则 $ab_1, ab_2, \dots, ab_{\varphi(m)}$ 也是模 m 的一个简化剩余系.

关于欧拉函数 $\varphi(m)$,有一个定理:设 l 是一个正整数, p 是一个素数,则有

$$\varphi(p^l) = p^{l-1}(p-1) \quad (20)$$

证明 由于 p 是一个素数, 于是 $1, 2, \dots, p-1$ 中的任何一个整数都与 p 互素, 故 $\varphi(p) = p-1$; 而当 $l=1$ 时有 $p^{l-1} = 1$, 所以当 $l=1$ 时定理成立.

现设 $l > 1$, 不大于 4 而和 4 互素的正整数是 1, 3, 共有 2 个, 即 $\varphi(4) = 2$; 不大于 8 而与 8 互素的正整数是 1, 3, 5, 7, 故 $\varphi(8) = 4$; 不大于 9 而和 9 互素的正整数是 1, 2, 4, 5, 7, 8, 故 $\varphi(9) = 6$. 而满足条件 $l > 1$ 及 $p^l \leq 9$ 的 p^l 只有 4, 8, 9 这 3 个数, $\varphi(2^2) = \varphi(4) = 2 = 2^{2-1}(2-1)$, $\varphi(2^3) = \varphi(8) = 4 = 2^{3-1}(2-1)$, $\varphi(3^2) = \varphi(9) = 6 = 3^{2-1}(3-1)$. 故当 $l > 1$ 而 $p^l \leq 9$ 时, 定理亦成立.

现设 $l > 1$ 而 $p^l \geq 10$. 在不大于 p^l 的正整数中, 有 p^{l-1} 个整数:

$$p, 2p, 3p, \dots, p^{l-1}p$$

是 p 的倍数, 其余的不大于 p^l 的正整数都是和 p 互素的. 故不大于 p^l 而和 p^l 互素的正整数是 $p^l - p^{l-1}$ 个, 即

$$\varphi(p^l) = p^l - p^{l-1} = p^{l-1}(p-1)$$

至此, 定理已证完.

对于欧拉函数, 还有著名的欧拉定理: 设 m 是一个大于 1 的整数, a 是一个整数, 且满足条件 $(a, m) = 1$, 则有

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad (21)$$

证明 设 $1 < a_2 < \dots < a_{\varphi(m)}$ 是不大于 m 且和 m 互素的全部正整数. 令 r_1 是一个整数, 且满足条件

$$a \equiv r_1 \pmod{m}, 0 \leq r_1 \leq m-1$$

令 r_i 是一个整数 ($i = 2, 3, \dots, \varphi(m)$) 且满足条件

$$aa_i \equiv r_i \pmod{m}, 0 \leq r_i \leq m-1$$

由于 $1, a_2, \dots, a_{\varphi(m)}$ 是模 m 的一个简化剩余系, 且由 $(a, m) = 1$, 可知 $a, aa_2, \dots, aa_{\varphi(m)}$ 也是模 m 的一个简化剩余系. 从而 $r_1, r_2, \dots, r_{\varphi(m)}$ 和 $1, a_2, \dots, a_{\varphi(m)}$ 只是在次序上可能不同, 所以

$$r_1 r_2 \cdots r_{\varphi(m)} \equiv a_2 \cdots a_{\varphi(m)} \pmod{m}$$

进而得到

$$a^{\varphi(m)} a_2 \cdots a_{\varphi(m)} = a(aa_2) \cdots (aa_{\varphi(m)}) \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m} \equiv a_2 \cdots a_{\varphi(m)} \pmod{m}$$

由于 $a_2, \dots, a_{\varphi(m)}$ 与 m 互素, 可将上式两端的 $a_2 \cdots a_{\varphi(m)}$ 同时消去, 得

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

利用 $\varphi(p) = p-1$ (其中 p 为素数), 在欧拉定理中取 $m=p$, 便得到费马小定理: 设 p 为素数, 又 $p \nmid a$, 则有

$$a^{p-1} \equiv 1 \pmod{p} \quad (22)$$

6. 连分数

我们称分数