

Elements of Number Theory



HIT

数论经典著作系列

数论基础

[俄] И·М·维诺格拉多夫 著 裘光明 译



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



数论经典著作系列

Elements of Number Theory

数论基础

● [俄] И. М. 维诺格拉多夫 著 裘光明 译



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

内 容 提 要

本书系根据前苏联国立技术理论书籍出版社(Государственное издательство технико-теоретической литературы)1952年出版的维诺格拉多夫院士(Академик И. М. Виноградов)著《数论基础》修正第六版译出的.原书经前苏联高等教育部审定综合大学物理数学系的教本.

本书前出第五版译本(由商务印书馆出版)曾得到北京大学闵嗣鹤教授的帮助,同时,中国科学院数学研究所所长华罗庚教授为本书写了指导性的介绍,对读者有很大的帮助.

图书在版编目(CIP)数据

数论基础/(俄罗斯)维诺格拉多夫著;裘光明译. — 哈尔滨:
哈尔滨工业大学出版社,2011.3

ISBN 978 - 7 - 5603 - 3221 - 5

I. ①数… II. ①维… ②裘… III. ①数论 - 基本知识 IV. ①O156

中国版本图书馆 CIP 数据核字(2011)第 038426 号

责任编辑 刘培杰 张永芹
责任编辑 王勇钢
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 9.5 字数 175 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 - 3221 - 5
定 价 18.00 元

(如因印装质量问题影响阅读,我社负责调换)

维诺格拉多夫院士的《数论基础》是数论领域里不可多

得的一本深入浅出的好书,译成中文,对于大学数学系的学生和爱好数论的同志都是极有帮助的.

这本书是不能粗浅地阅读的!特别是习题部分,其中包含着十分丰富的题材,特别是维诺格拉多夫学派的基本技术.如果读这本书而不看不做书后的问题,就好像入宝山而空返,把这书的最重要的部分忽略了!这些问题大部分都是根据有源流的.很多是历史上的著名问题,或是维氏自己的研究工作.他精简地叙述了,他巧妙地安排了,使读者逐步做去,在不知不觉中证明了历史上有名的定理.这些高度的技巧,可能是初读者不易发现的,同时也诚恐国内很少人能够指明给读者关于这些问题的出处.因此我不揣冒昧地,在这里介绍一番.

在第二章的习题中,一开始就谈到两个数论上十分重要而未解决的问题:其中一个是著名的高斯(Gauss)的圆内整点问题.所谓整点是指两个坐标都是整数的点.设 T 是以原点为圆心, r 为半径的圆内的整点的个数.换句话说, T 就是适合

$$x^2 + y^2 \leq r^2$$

的整数 (x, y) 的对数.经过第二章问题1. c,第三章问题6. a,逐步地证明了

$$T = \pi r^2 + O(r^{\frac{2}{3}} \ln r)$$

这是历史上有名的伏乐诺依和谢尔品斯基(Вороной-Sierpinski)的结果.而所谓高斯问题,就是要求出 $T - \pi r^2$ 的最好的上限.这是数论中一个十分困难的问题,近若干年来经过不少数学家的努力,逐步推进,整个的历史可以概括地叙述如下:

设 θ 是最小的正整数适合下面的条件:对于任意 $\alpha > \theta$,总有

$$T = \pi r^2 + O(r^{2\alpha})$$

谢尔品斯基证明 $\theta \leq \frac{1}{3}$;李特伍德(Littlewood)和瓦尔非兹(Walfitz)证明 $\theta \leq \frac{37}{112}$;尼兰德(Nieland)更证明 $\theta \leq \frac{27}{82}$;蒂奇马什(Titchmarsh)用双变数方次数函数和证明 $\theta \leq \frac{15}{46}$.而最好的结果则是 $\theta \leq \frac{13}{40}$.这是华罗庚在1935年所证明的.但是这距离大家所猜测的 $\theta \leq \frac{1}{4}$ 还有些距离.另一方面已经证明了 $\theta < \frac{1}{4}$.如何来决定这个 θ 的数值,在数论中是一个难题.

接着圆内整点问题,维氏还提出迪利克雷(Dirichlet)的约数问题.问题是这样的:求出适合

$$xy \leq n, x > 0, y > 0$$

的整点的个数 T 来.经过第二章问题1. d和第三章问题6. b,可以证明

$$T = n(\ln n + 2E - 1) + O(n^{\frac{1}{3}}(\ln n)^2)$$

这是俄国大数学家伏乐诺依的结果.但是如果读者把维氏的证明与伏乐诺依原来的证明比较一下,不难发现新的证法是便捷得多了.就像圆内整点问题一样,我们引进 θ ,这个 θ 的历史是这样:万·德·考柏(Wan der Corput)先后证明了 $\theta \leq \frac{33}{100}$ 和 $\theta \leq \frac{27}{82}$.最好的结果是迟宗陶同志的 $\theta \leq \frac{15}{46}$.他所用的方法是闵嗣鹤同志所提出的.

在讨论上述两个问题的过程中,维氏引入了一个十分重要的定理:(见第三章问题5. a,它前面一连串的问题都是帮助读者来证明这个定理的.)

设 $A > 2, k \geq 1$,函数 $f(x)$ 在间隔 $Q \leq x \leq R$ 里有连续的二阶导数而且有条件

$$\frac{1}{A} \leq |f''(x)| \leq \frac{k}{A}$$

以 $\{f(x)\}$ 表示 $f(x)$ 的分数部分,则

$$\left| \sum_{Q < x \leq R} \{f(x)\} - \frac{1}{2}(R - Q) \right| \leq (2k^2(R - Q) \ln A + 8kA)A^{-\frac{1}{3}}$$

这是一个十分重要的定理(非常有用的工具).如果把这书中所安排着的

证明和万·德·考柏的相当的工作比较一下,不难发现这里要简捷多了.

在第二章的问题里,一连串地引进了不少关于素数分布的定理.特别是问题 9,那是历史上有名的俄国数学大师切比雪夫(Чебышев)的工作.问题 16 是麦比乌斯(Möbius)函数的若干重要性质,而且也是与素数分布基本上相通的.问题 17. a 中引入了一个重要方法,这方法把“爱拉托赛尼(Eratosthenes)的筛子”公式化了.这与问题 23. c 联系起来,就是素数论上常用的白润(Brun)方法.也就是维氏著名工作“充分大的奇数是三个素数的和”的证明中用着的一端.问题 24 是这个方法的一个简单的应用.

第五章的问题 11 讨论了所谓高斯和数.他算出形式

$$\sum_{x=0}^{m-1} e^{2\pi i \frac{Ax^2+ax}{m}}$$

的和数的绝对值.在第六章问题 11 里更把这结果推进一步.他研究了

$$\sum_{x=0}^{m-1} e^{2\pi i \frac{ax^n}{m}}$$

的绝对值的上限.在问题 15. a 里更讨论了

$$\sum_{x=0}^{m-1} e^{2\pi i \frac{ax^n+bx}{m}}$$

的一个特例.由此引申出来,我们就会发问:和式

$$\sum_{x=0}^{m-1} e^{2\pi i \frac{f(x)}{m}}, f(x) = ax^n + a_1x^{n-1} + \dots + a_n$$

的上限如何?这一个历史上的问题,已经由华罗庚解决了.

不要看轻第六章的问题 13,这是维氏的重要贡献之一.从第四章问题 11 就开始了 n 次剩余的讨论,而第六章问题 13 则是关于 n 次剩余分布情形的优良结果.不等式中 p 的方次数 $\frac{1}{c}$ ($c = 2e^{1-\frac{1}{n}}$) 是应当可以降低的.大家预测,可以用 p^ε (ε 是任意正数) 来代替 $p^{\frac{1}{c}}$,但是这是一个迄未解决的问题.如果读者能得出比 $\frac{1}{c}$ 小的数,也是值得发表的.而如果能解决这个问题,那对于数论的贡献是极大的.

同时第六章问题 12. c 也是维氏的重要贡献,华罗庚曾经把它推进一步.问题 14 也是维氏自己的工作.

第五章问题 9 是前苏联数学家高尔士可夫(Горшков)的结果,是普通书上所找不到的.我们知道,任意 $4m+1$ 形式的素数 p 一定是两个平方数的和 $x^2 + y^2$.但是究竟如何把 x 和 y 写出来?高尔士可夫回答了这个问题

$$p = \left(\frac{1}{2}S(r)\right)^2 + \left(\frac{1}{2}S(n)\right)^2$$

此处 $\left(\frac{r}{p}\right) = 1, \left(\frac{n}{p}\right) = -1$, 而且

$$S(k) = \sum_{x=0}^{p-1} \left(\frac{x(x^2 + k)}{p} \right)$$

此处像第四章问题7引进了克鲁斯脱曼(Kloostermann)和数,第五章问题10解决了佩尔(Pell)方程,第六章问题9引进了特征函数的基本性质,等.仔细地看来,就不难发现维氏的惊人的技巧.他把这许多重要的结果分成若干问题,使读者按部就班地,用做习题的方式,自己证明了这些结果.这是多么引人入胜的方法啊!

维诺格拉多夫院士的全名是伊凡·马脱维也维赤·维诺格拉多夫(Иван Матвеевич Виноградов),生在1892年.他是前苏联科学院院士,斯泰克洛夫数学研究所所长,他还是前苏联的社会主义劳动英雄,1941年获得斯大林奖金,1945年得到列宁勋章.他对数论有划时代的光辉贡献.对于用“三角和式的估值”来研究数论上的问题这一方面,在世界上是首屈一指的权威.特别是关于华林(Waring)问题的不朽的工作,以及震惊全球的关于哥德巴赫(Goldbach)问题的贡献.他的成就证明了社会主义的优越性,这正象征着我们的明天.

华罗庚

历史介绍 // 1

第一章 可除性理论 // 1

- 1.1 基本的概念和定理 // 1
- 1.2 最大公约数 // 2
- 1.3 最小公倍数 // 5
- 1.4 欧几里得算法与连分式的关系 // 6
- 1.5 素数 // 9
- 1.6 素因子分解式的唯一性 // 10
- 问题 // 12
- 计算题 // 13

第二章 重要的函数 // 14

- 2.1 函数 $[x]$ 和 $\{x\}$ // 14
- 2.2 对约数展开的和式 // 15
- 2.3 麦比乌斯函数 // 16
- 2.4 欧拉函数 // 17
- 问题 // 19
- 计算题 // 26

第三章 同余式 // 27

- 3.1 基本概念 // 27
- 3.2 同余式与等式相似的性质 // 28
- 3.3 同余式进一步的性质 // 29
- 3.4 完全剩余组 // 30
- 3.5 与模互素的剩余组 // 31
- 3.6 欧拉定理和费马定理 // 32
- 问题 // 32
- 计算题 // 37

第四章	一个未知数的同余式	// 38
4.1	基本概念	// 38
4.2	一次同余式	// 39
4.3	一次同余式组	// 40
4.4	素数模的任意次同余式	// 42
4.5	复合数模的任意次同余式	// 43
	问题	// 45
	计算题	// 49
第五章	二次同余式	// 51
5.1	一般性定理	// 51
5.2	勒让德符号	// 53
5.3	雅可比符号	// 56
5.4	复合数模的情形	// 59
	问题	// 61
	计算题	// 66
第六章	元根和指数	// 68
6.1	一般性定理	// 68
6.2	模 p^α 和 $2p^\alpha$ 的元根	// 69
6.3	模 p^α 和 $2p^\alpha$ 的元根的求法	// 70
6.4	模 p^α 和 $2p^\alpha$ 的指数	// 71
6.5	前面理论的一些推论	// 73
6.6	模 2^α 的指数	// 75
6.7	任意复合数模的指数	// 77
	问题	// 78
	计算题	// 84
	问题解答	// 86
	第一章	// 86
	第二章	// 90
	第三章	// 102
	第四章	// 111
	第五章	// 116
	第六章	// 124
	计算题答案	// 133
	中文、俄文、英文名词对照表	// 137

可除性理论

第一章

1.1 基本的概念和定理

a. 数论是研究整数的性质的. 我们所说的整数不仅是自然数(正整数) $1, 2, 3, \dots$, 还有零和负整数 $-1, -2, -3, \dots$

通常在作理论的叙述时, 我们用字母表示的只是整数. 当字母所代表的不是整数时, 如果意义并不很明白, 我们会作特别的声明.

两个整数 a 和 b 的和数, 差数和乘积仍然是整数, 但是 a 被 b 除(假如 b 不等于零) 所得到的商数, 可以是整数, 也可以不是整数.

b. 当 a 被 b 除得到的商数是整数时, 假如把它记做 q , 我们就有 $a = bq$, 也就是说, a 等于 b 乘上一个整数. 那么我们就说, a 被 b 除尽或者 b 除尽 a . 这时 a 叫做 b 的倍数而且 b 叫做 a 的约数. b 除尽 a 这个事实, 写做 $b \mid a$.

下面的两个定理成立.

1. 如果 a 是 m 的倍数, m 是 b 的倍数, 则 a 是 b 的倍数.

实际上,从 $a = a_1 m, m = m_1 b$ 推出 $a = a_1 m_1 b$, 这里 a_1, m_1 是整数. 这就证明了定理.

2. 如果在等式 $k + l + \cdots + n = p + q + \cdots + s$ 中, 除掉某一项以外, 所有的项都是 b 的倍数, 则这一项也是 b 的倍数.

实际上, 设这一项是 k , 则因为

$$l = l_1 b, \cdots, n = n_1 b, p = p_1 b, q = q_1 b, \cdots, s = s_1 b$$

所以

$$k = p + q + \cdots + s - l - \cdots - n = (p_1 + q_1 + \cdots + s_1 - l_1 - \cdots - n_1) b$$

这就证明了定理.

c. 在一般情形下, 包括 a 被 b 除尽的特殊情形在内, 我们有下列定理:

每一个整数 a 可以唯一地通过正整数 b 而被表示成

$$a = bq + r \quad 0 \leq r < b$$

实际上, 取 bq 等于不超过 a 的 b 的最大倍数, 我们得到 a 的这种形式的一个表示式. 假定还有 $a = bq_1 + r_1, 0 \leq r_1 < b$, 我们得到 $0 = b(q - q_1) + (r - r_1)$, 由此推出 $r - r_1$ 是 b 的倍数 (b. 2). 但是由于 $|r - r_1| < b$, 所得结果只在 $r - r_1 = 0$, 即 $r = r_1$ 时才可能, 于是还得出 $q = q_1$.

数 q 叫做 a 被 b 除的不完全商数, 数 r 叫做 a 被 b 除的余数.

例子: 设 $b = 14$, 我们有

$$\begin{aligned} 177 &= 14 \times 12 + 9 & 0 < 9 < 14 \\ -64 &= 14 \times (-5) + 6 & 0 < 6 < 14 \\ 154 &= 14 \times 11 + 0 & 0 = 0 < 14 \end{aligned}$$

1.2 最大公约数

a. 以后我们只讨论数的正的约数. 同时除尽整数 a, b, \cdots, l 的每一个整数都叫做它们的公约数. 公约数中最大的一个叫做最大公约数而且用符号 (a, b, \cdots, l) 来表示. 由于公约数的个数是有限的, 最大公约数显然存在. 如果 $(a, b, \cdots, l) = 1$, 则 a, b, \cdots, l 就说是互素的. 如果数 a, b, \cdots, l 中的每一个都与别的每一个互素, 则 a, b, \cdots, l 叫做两两互素的. 明显地, 两两互素的数一定也互素; 而对于两个数来说, “互素” 和 “两两互素” 的概念是一样的.

例子: 数 $6, 10, 15$, 由于 $(6, 10, 15) = 1$, 是互素的. 数 $8, 13, 21$, 由于

$$(8, 13) = (8, 21) = (13, 21) = 1$$

是两两互素的.

b. 我们先来研究两个数的公约数.

1. 如果 a 是 b 的倍数, 则数 a 和 b 的公约数的集合与单独一个 b 的约数的集合重合; 特别地, $(a, b) = b$.

实际上, 数 a 和 b 的每一个公约数都是单独一个 b 的约数. 反之, 因为 a 是 b 的倍数, 所以 (1.1 节, b.1) b 的每一个约数也都是 a 的约数, 这说是说它们都是数 a 和 b 的公约数. 因此数 a 和 b 的公约数的集合与单独一个 b 的约数的集合重合. 而因为数 b 的最大的约数是 b 自己, 所以 $(a, b) = b$.

2. 如果 $a = bq + c$

则数 a 和 b 的公约数的集合与数 b 和 c 的公约数的集合重合; 特别地, $(a, b) = (b, c)$.

实际上, 上面所写的等式表明, 数 a 和 b 的每一个公约数也除尽 c (1.1 节, b.2), 因而也是数 b 和 c 的公约数. 反之, 这一个等式又表明, 数 b 和 c 的约数除尽 a . 因而也是数 a 和 b 的公约数. 因此数 a 和 b 的公约数与数 b 和 c 的公约数是相同的一些数; 特别地, 这些公约数中最大的也应该相同, 即 $(a, b) = (b, c)$.

c. 为了求出最大公约数, 也为了获得它的最重要性质, 用到下面叙述的欧几里得 (Euclid) 算法. 设 a 和 b 是正整数. 按照 1.1 节, c, 我们求得一串等式

$$\begin{cases} a = bq_1 + r_2 & 0 < r_2 < b \\ b = r_2q_2 + r_3 & 0 < r_3 < r_2 \\ r_2 = r_3q_3 + r_4 & 0 < r_4 < r_3 \\ \vdots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = r_nq_n \end{cases} \quad (1)$$

这串等式当我们得到一个 $r_{n+1} = 0$ 时才终止. 这后一点是必然的, 因为 b, r_2, r_3, \dots 是递减的正整数列, 不能包括多于 b 个的正整数.

d. 自上而下来看等式组 (1), 根据 b, 我们可以肯定, 数 a 和 b 的全体公约数与数 b 和 r_2 的全体公约数重合, 也与数 r_2 和 r_3 的, 数 r_3 和 r_4 的, \dots , 数 r_{n-1} 和 r_n 的全体公约数重合, 最后就与单独一个数 r_n 的全体约数重合. 同时我们还有

$$(a, b) = (b, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n) = r_n$$

于是我们得到了下面的一些结果.

1. 数 a 和 b 的公约数的集合与它们的最大公约数的约数集合重合.
2. 这个最大公约数等于 r_n , 也就是等于欧几里得算法最后的不等于零的余数.

例子: 应用欧几里得算法求 (525, 231). 我们求得 (辅助的计算写在右边)

$$\begin{array}{r}
 525 \overline{) 231} \quad 525 = 231 \times 2 + 63 \\
 \underline{462} \\
 231 \overline{) 63} \quad 231 = 63 \times 3 + 42 \\
 \underline{189} \\
 63 \overline{) 42} \quad 63 = 42 \times 1 + 21 \\
 \underline{42} \\
 42 \overline{) 21} \quad 42 = 21 \times 2 \\
 \underline{42} \\
 0
 \end{array}$$

这里最后的正余数是 $r_4 = 21$. 所以 $(525, 231) = 21$.

e. 1. 设 m 表示任意的正整数, 我们有 $(am, bm) = (a, b)m$.

2. 设 δ 表示数 a 和 b 的任意公约数, 我们有 $(\frac{a}{\delta}, \frac{b}{\delta}) = \frac{(a, b)}{\delta}$; 特别地, 我们有 $(\frac{a}{(a, b)}, \frac{b}{(a, b)}) = 1$, 这就是说, 两个数被它们的最大公约数除所得的商数是互素的.

实际上, 等式组(1) 逐项地乘上 m , 我们得到新的等式组, 在其中代替 a, b, r_2, \dots, r_n 的是 $am, bm, r_2m, \dots, r_nm$. 所以 $(am, bm) = r_nm$, 因此命题 1 成立.

应用命题 1, 我们求得

$$(a, b) = (\frac{a}{\delta}, \frac{b}{\delta})\delta = (\frac{a}{\delta}, \frac{b}{\delta})\delta$$

由此推出命题 2.

f. 1. 如果 $(a, b) = 1$, 则 $(ac, b) = (c, b)$.

实际上, 由于 (ac, b) 除尽 ac 和 b , 按照 d. 1 它也除尽 (ac, bc) , 后者根据 e. 1 等于 c ; 而 (ac, b) 又除尽 b , 所以它也除尽 (c, b) . 反之, (c, b) 除尽 ac 和 b , 所以它除尽 (ac, b) . 因此, (ac, b) 和 (c, b) 互相除尽, 因而它们就相等了.

2. 如果 $(a, b) = 1$ 而且 ac 被 b 除尽, 则 c 被 b 除尽.

实际上, 由于 $(a, b) = 1$, 我们有 $(ac, b) = (c, b)$. 但是因为 ac 是 b 的倍数, 所以按照 b. 1 我们有 $(ac, b) = b$, 这说明 $(c, b) = b$, 即 c 是 b 的倍数.

3. 如果 a_1, a_2, \dots, a_m 中的每一个与 b_1, b_2, \dots, b_n 中的每一个互素, 则乘积 $a_1 a_2 \dots a_m$ 也与乘积 $b_1 b_2 \dots b_n$ 互素.

实际上, 从定理 1, 我们有

$$(a_1 a_2 a_3 \dots a_m, b_k) = (a_2 a_3 \dots a_m, b_k) = (a_3 \dots a_m, b_k) = \dots = (a_m, b_k) = 1$$

然后, 简写 $a_1 a_2 \dots a_m = A$, 用同样的方法我们求得

$$(b_1 b_2 b_3 \dots b_n, A) = (b_2 b_3 \dots b_n, A) = (b_3 \dots b_n, A) = \dots = (b_n, A) = 1$$

g. 求两个以上的数的最大公约数的问题, 可以化成求两个数的公约数的问题. 那就是说, 为了求得数 a_1, a_2, \dots, a_n 的公约数, 我们写出下列的一串数

$$(a_1, a_2) = d_2, (d_2, a_3) = d_3, (d_3, a_4) = d_4, \dots, (d_{n-1}, a_n) = d_n$$

数 d_n 就是所有已知数的最大公约数.

实际上,根据 d. 1 数 a_1, a_2 的全部公约数与 d_2 的全部约数重合,所以数 a_1, a_2, a_3 的全部公约数与数 d_2 和 a_3 的全部公约数重合,即与 d_3 的全部约数重合. 然后我们肯定,数 a_1, a_2, a_3, a_4 的全部公约数与 d_4 的全部约数重合,等. 最后,数 a_1, a_2, \dots, a_n 的全部公约数与 d_n 的全部约数重合. 而因为 d_n 的最大约数是 d_n 自己,所以它就是数 a_1, a_2, \dots, a_n 的最大公约数.

看一下上面所引的证明,我们肯定定理 d. 1 对于两个以上的数也对. 定理 e. 1 和 e. 2 也是对的,这是因为用 m 去乘或者用 δ 去除所有的数 a_1, a_2, \dots, a_n , 正像所有 d_2, d_3, \dots, d_n 都被 m 乘或者被 δ 除一样.

1.3 最小公倍数

a. 所有已知数的每一个整倍数都叫做它们的公倍数. 最小的正的公倍数叫做最小公倍数.

b. 我们先来研究两个数的最小公倍数. 设 M 是两个整数 a 和 b 的任意公倍数. 因为它是 a 的倍数,所以 $M = ak$, 这里 k 是整数. 但是 M 又是 b 的倍数,所以

$$\frac{ak}{b}$$

也应该是整数. 假定 $(a, b) = d, a = a_1d, b = b_1d$, 上面的整数就可以表示成 $\frac{a_1k}{b_1}$, 这

里 $(a_1, b_1) = 1$ (1.2 节, e. 2). 所以 k 应该被 b_1 除尽 (1.2 节, f. 2), $k = b_1t = \frac{b}{d}t$, 这里 t 是整数. 由此

$$M = \frac{ab}{d}t$$

反之,明显地,这种形式的每一个 M 既是 a 的倍数,也是 b 的倍数,因此,这是数 a 和 b 的所有公倍数的一般形状.

这些公倍数中的最小正数,即最小公倍数,在 $t = 1$ 时得到. 它就是

$$m = \frac{ab}{d}$$

引用 m , 求 M 的公式可以改写成

$$M = mt$$

最后这两个等式引出下列定理:

1. 两个数的公倍数的集合与它们的最大公约数的某倍数集合重合.
2. 两个数的最小公倍数等于它们的乘积除以它们的最大公约数.

c. 设现在要求出两个以上的数 a_1, a_2, \dots, a_n 的最小公倍数. 一般地用 $[a, b]$ 表示数 a 和 b 的最小公倍数, 我们写下一串数

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \dots, [m_{n-1}, a_n] = m_n$$

用这种方法得到的 m_n 就是所有已知数的最小公倍数.

实际上, 从 b. 1, 数 a_1 和 a_2 的全部公倍数与 m_2 的全部倍数重合, 所以数 a_1, a_2 和 a_3 的全部公倍数与 m_2 和 a_3 的全部公倍数重合, 即与 m_3 的全部倍数重合. 然后我们肯定, 数 a_1, a_2, a_3, a_4 的全部公倍数与 m_4 的全部倍数重合, 等. 最后, 数 a_1, a_2, \dots, a_n 的全部公倍数与 m_n 的全部倍数重合. 而因为 m_n 的最小的正倍数就是 m_n 自己, 所以它就是数 a_1, a_2, \dots, a_n 的最小公倍数.

从上面的证明我们看到, 定理 b. 1 对于两个以上的数也对. 此外, 我们还肯定了下列定理的正确性:

两两互素的数的最小公倍数等于它们的乘积.

1.4 欧几里得算法与连分式的关系

a. 设 α 是任意的实数. 用 q_1 表示不超过 α 的最大整数. 在 α 不是整数时, 我们有

$$\alpha = q_1 + \frac{1}{\alpha_2} \quad \alpha_2 > 1$$

同样地, 在 $\alpha_2, \dots, \alpha_{s-1}$ 不是整数时, 我们有

$$\alpha_2 = q_2 + \frac{1}{\alpha_3} \quad \alpha_3 > 1$$

\vdots

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s} \quad \alpha_s > 1$$

根据这个, 我们得出下列分割成连分式的 α

$$\alpha = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_{s-1} + \frac{1}{\alpha_s}}}} \quad (1)$$

如果 α 是无理数, 则在数列 α, α_2, \dots 中显然不能遇到整数, 以致这种表示的步骤可以无限制地继续下去.

如果 α 是有理数, 则以后在 b 里将会看到, 在数列 α, α_2, \dots 里一定会遇到整数, 而这种表示的步骤是有尽头的.

b. 如果 α 是有理的不可约分数 $\alpha = \frac{a}{b}$, 则分割 α 成连分式, 就与欧几里得算法密切地有联系. 实际上, 我们有

$$\begin{aligned} a &= bq_1 + r_2, \frac{a}{b} = q_1 + \frac{r_2}{b} \\ b &= r_2q_2 + r_3, \frac{b}{r_2} = q_2 + \frac{r_3}{r_2} \\ r_2 &= r_3q_3 + r_4, \frac{r_2}{r_3} = q_3 + \frac{r_4}{r_3} \\ &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{r_n}{r_{n-1}} \\ r_{n-1} &= r_nq_n, \frac{r_{n-1}}{r_n} = q_n \end{aligned}$$

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_n}}}$$

于是

c. 在数 α 所分割成的连分式里出现的数 q_1, q_2, \dots 叫做不完全的商数(按照 b, 当 α 是有理数时, 这就是欧几里得算法中逐次作除法所得的不完全的商数), 分数

$$\delta_1 = q_1, \delta_2 = q_1 + \frac{1}{q_2}, \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}, \dots$$

叫做近似分数.

d. 当我们注意到只要把 δ_{s-1} 里的 q_{s-1} 换成 $q_{s-1} + \frac{1}{q_s}$ 就得到 $\delta_s (s > 1)$ 时, 我们很容易地发现了组成近似分数的非常简单的规律.

实际上, 为了统一起见, 假定 $P_0 = 1, Q_0 = 0$, 我们可以依次把近似分数表示成下列形状(这里等式 $\frac{A}{B} = \frac{P_s}{Q_s}$ 表示 A, B 分别由符号 P_s, Q_s 来代替)

$$\begin{aligned} \delta_1 &= \frac{q_1}{1} = \frac{P_1}{Q_1} \\ \delta_2 &= \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_2q_1 + 1}{q_2 \times 1 + 0} = \frac{q_2P_1 + P_0}{q_2Q_1 + Q_0} = \frac{P_2}{Q_2} \end{aligned}$$

$$\delta_3 = \frac{(q_2 + \frac{1}{q_3})P_1 + P_0}{(q_2 + \frac{1}{q_3})Q_1 + Q_0} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}$$

等,更普遍地

$$\delta_s = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s}$$

因此,近似分数的分子和分母可以依次按着下面的式子来计算

$$\begin{cases} P_s = q_s P_{s-1} + P_{s-2} \\ Q_s = q_s Q_{s-1} + Q_{s-2} \end{cases} \quad (2)$$

这些计算可以用下面的表来做:

q_s		q_1	q_2	...	q_{s-2}	q_{s-1}	q_s	...	q_{n-1}	q_n
P_s	1	P_1	P_2	...	P_{s-2}	P_{s-1}	P_s	...	P_{n-1}	a
Q_s	0	1	Q_2	...	Q_{s-2}	Q_{s-1}	Q_s	...	Q_{n-1}	b

例子:把数 $\frac{105}{38}$ 写成连分式. 这里

$$\begin{array}{r} 105 \overline{) 38} \\ \underline{76} \\ 29 \\ \underline{29} \\ 9 \\ \underline{27} \\ 9 \\ \underline{8} \\ 1 \\ \underline{2} \\ 2 \end{array} \quad \frac{105}{38} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4 + \frac{1}{2}}}}$$

所以上面所说的表是:

q_s		2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

e. 我们来观察邻接的近似分数的差数 $\delta_s - \delta_{s-1}$. 当 $s > 1$, 我们有

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_s}{Q_s Q_{s-1}}$$

这里 $h_s = P_s Q_{s-1} - Q_s P_{s-1}$; 把这式子里的 P_s 和 Q_s 用式(2)来代, 再化简以后, 我们得到 $h_s = -h_{s-1}$. 最后这个式子结合 $h_1 = q_1 \times 0 - 1 \times 1 = -1$, 就有 $h_s = (-1)^s$.