世界数学精品译丛

MSRI
Mathematical Sciences Research Institute

5

# 算法数论
## 格、数域、曲线和密码学

# Algorithmic Number Theory
## Lattices, Number Fields, Curves and Cryptography

□ J. P. Buhler, P. Stevenhagen 编

□ 王 元 冯克勤 张 俊 译

高等教育出版社


MSRI
Mathematical Sciences
Research Institute

5

Algorithmic Number Theory
Lattices, Number Fields, Curves and Cryptography

# 算法数论
## 格、数域、曲线和密码学

□ J. P. Buhler, P. Stevenhagen 编

□ 王 元 冯克勤 张 俊 译

高等教育出版社·北京 International Press

图字：01-2018-7304 号



**算法数论**
Suanfa Shulun

**图书在版编目 (CIP) 数据**
算法数论：格、数域、曲线和密码学 /（美）J. P. 布勒（J. P. Buhler）等编；王元，冯克勤，张俊译．
—北京：高等教育出版社，2019.1
书名原文：Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography
ISBN 978-7-04-050123-0
Ⅰ. ①算… Ⅱ. ①J… ②王… ③冯…④张… Ⅲ. ①算法理论 Ⅳ. ①O241
中国版本图书馆 CIP 数据核字 (2018) 第 165799 号

| | | |
|---|---|---|
| 策划编辑　赵天夫 | 责任编辑　赵天夫 | 封面设计　李小璐 |
| 版式设计　马敬茹 | 责任校对　高　歌 | 责任印制　陈伟光 |

出版发行 高等教育出版社
社址 北京市西城区德外大街 4 号
邮政编码 100120
购书热线 010-58581118
咨询电话 400-810-0598
网址 http://www.hep.edu.cn
http://www.hep.com.cn
网上订购 http://www.hepmall.com.cn
http://www.hepmall.com
http://www.hepmall.cn
印刷

开本 787mm×1092mm 1/16
印张 35.25
字数 690 千字
版次 2019 年 1 月第 1 版
印次 2019 年 1 月第 1 次印刷
定价 168.00 元

本书如有缺页、倒页、脱页等质量问题，
请到所购图书销售部门联系调换
版权所有　侵权必究
[物 料 号 50123-00]

# 前言

我们的对象来源于数学思想的两个根基: 对于各种数的特性的探索和对计算的追求. 在二十世纪的后二十五年是数论和计算机科学非常活跃的年代, 这两个学科的交叉也令人印象深刻. 算法数论作为一个引人入胜的领域由此产生, 它具有深刻的观点和令人振奋的应用.

2000 年秋季, 加州大学伯克莱数学所举办了关于算法数论的一学期学术活动. 开始时与 Clay 数学所合办一个讨论班, 组织了许多基础性和综述性的讲座. 会议期间, 人们感到这个领域的新人缺乏信息资源. 会后一部分讲演人愿意根据讲演写出文章, 于是我们编辑了这本书.

有几位作者很快就提交了初稿, 其中有的保持讲稿风格和原来讲演的特点, 另一些则加工成完善的讲义或综述性文章. 另有不少作者 (包括本书的编者) 延误了时间. 恳求到的新文章中需要更好地组织材料, 并且加上不能忽略的一些新结果 (其中最值得指出的是由 Manindra Agrawal, Neeraj Kayal 和 Nitin Saxena 给出的素性判定多项式型算法). 这一切使问题变得复杂, 这本书从而包括了二十篇文章, 十五位作者和 650 页. 经过大家的努力, 我们高兴地看到本书得以问世.

我们对快速提交稿件的作者致以歉意, 希望本书内容的扩大和人们对他们有所贡献的这本书的兴趣来补偿出版稍迟这一不足之处.

大致说来, 本书的文章可分类如下. 前两篇文章为引论, 比后面文章较为初等, 试图带领读者去追寻更深刻的思想. 接下来的八篇是关于中心课题的综述性文章, 包括光滑数, 因子分解, 素性判定, 格, 椭圆曲线, 代数数论和算数运算的快速算法. 其余十篇更深入地讨论专门课题, 包括密码学, 计算代数数论, 模形式和算术几何.

虽然在最广泛的意义上本书中的文章是综述性的, 但这并不意味着这是一本收罗当前通常意义下学问的百科全书. 我们更想用 "俯视" (overview) 这个词, 这些文章均具有独特的甚至有些是非标准的视野.

我们必须要感谢一些机构和人. 显然, 所有作者的文章都是引人入胜的, 定会激励人们投入本学科的研究. 我们感谢 Clay 研究所和美国国家数学科学研究所 (MSRI) 对研讨会的慷慨资助, 他们使本书的出版成为可能. 我们感谢剑桥大学出版社和 MSRI 在本书出版过程中的支持和耐心, 特别感谢 Silvio Levy 对本书所做的大量工作. John

Voight 为研讨会的大多数报告都做了记录 (将 TEX 代码几乎实时地录入笔记本), 这对一些作者来说很有价值.

最后, Hendrik Lenstra 一直是整个算法数论领域灵感与智慧的源泉, 本书也不例外: 除了贡献两篇杰出的文章外, 这些年他为主编和几乎所有作者都给出过令人感激不尽的建议.

Joe Buhler

Peter Stevenhagen

2008 年 5 月于圣迭戈

## 内容简介

近百年来，由于大量计算的例子，数论学家增进了他们的直觉性。计算机和精心研制的算法逐渐导致出现了算法数论这一专门的领域。这个年轻的学科和计算机科学、密码学以及数学的其他分支有很强的联系。数学思想往往导致更好的算法，这是此学科的魅力之一；而对算法的广泛研究也促使数学新思想的产生和新问题的探索。

本书包括由各领域首屈一指的专家对算法数论各个专题所写的二十篇综述性文章：前两篇文章为引论；随后的八篇文章覆盖了该领域的核心内容：因子分解、素性、光滑数、格、椭圆曲线、代数数论和算术运算的快速算法；后十篇文章就某个专门方面综述一些特殊课题，包括密码学、Arakelov 类群、计算类域论、有限域上的 zeta 函数、算术几何与模形式理论。

本书可供数学、计算机科学和密码学等相关专业的读者参考。

# 目录

# 解 Pell 方程

Hendrik W. Lenstra, Jr.

## 1. Pell 方程

Pell 方程即方程

$$x^2 = dy^2 + 1,$$

对给定的非零整数 $d$, 试求正整数 $x, y$ 满足上面方程. 例如 $d = 5$, 我们有解 $x = 9, y = 4$. 我们总可以假定 $d > 0$, 且不是一个平方数, 否则, 方程显然无解.

英国数学家 John Pell (1610—1685) 与这个方程无关. Euler (1707—1783) 错误地将这个方程的一个解法归于 Pell. 实际上, 这个解法是另一个英国数学家 William Brouncker (1620—1684) 为响应 Fermat (1601—1665) 的挑战而发明的, 但是企图改变 Euler 引入的术语总是无效的.

关于 Pell 方程有着丰富的史料, 其中 Weil [1984] 的书是最好的导引; 亦见 [Dickson 1920, Chapter XII; Konen 1901; Whitford 1912]. Brouncker 的方法本质上等同于至少早六个世纪印度数学家就知道的一个方法. 我们将看到, 这个方程也出现在希腊数学中, 但并无令人信服的证据说明希腊人能解出这个方程.

一个非常清楚的 "印度人的" 或 "英国人的" 解 Pell 方程的方法包含在 Euler 的《代数学》[Euler 1770, Abschnitt 2, Capitel 7] 中. 现代教科书则常常用连分数语言来表述, 这种表述也是 Euler 提供的 (例如见 [Niven et al. 1991, Chapter 7]). Euler, 与他的印度及英国的先驱者一样, 确认该方法必能产生一个解. 那是真实的, 但却不是显然的 —— 显然的只是, 若存在一个解, 那么这个方法就能找出一个解来. Fermat 或许证明了, 对于每一个 $d$, 方程皆存在一个解 (见 [Weil 1984, Chapter II, §XIII]), 但 Lagrange (1736—1813) [1773] 第一个发表了这样一个证明[1].

我们可以将 Pell 方程改写为

$$(x + y\sqrt{d}) \cdot (x - y\sqrt{d}) = 1,$$

所以寻求一个解转而为寻求环 $\mathbb{Z}[\sqrt{d}]$ 中范数为 1 的一个非平凡单位, 这里范数 $\mathbb{Z}[\sqrt{d}]^* \to Z^* = \{\pm 1\}$ 表示每一个单位与它的共轭数乘起来, 其中单位 $\pm 1$ 被

[1] 这个证明亦可见华罗庚《数论导引》(科学出版社, 1957) 第十章, §9. —— 译者注

当作 $\mathbb{Z}[\sqrt{d}]$ 的平凡单位[2]. 这个重新表达说明, 当我们得知 Pell 方程的一个解时, 我们就可以找到无穷多个解. 更确切地说, 若将解按其大小排序, 则第 $n$ 个解 $x_n, y_n$ 可以由第一个解 $x_1, y_1$ 表示如下

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

所以, 第一个解 $x_1, y_1$ 被称为 Pell 方程的基本解, 而解 Pell 方程就意味着对于给定的 $d$, 寻求 $x_1, y_1$. 借语言措辞的滥用, 我们亦将用 $x + y\sqrt{d}$ 而不是一对 $x, y$ 指 Pell 方程的解, 并称 $x_1 + y_1\sqrt{d}$ 为基本解.

我们可以将 Pell 方程的可解性看作代数数论中 Dirichlet 单位定理[3]的一个特例, 这一定理给出了一般代数整数环上单位群的结构 [Stevenhagen 2008a]; 对于环 $\mathbb{Z}[\sqrt{d}]$ 来说, 它是 $\{\pm 1\}$ 与一个无限循环群之乘积.

作为一个例子, 考虑 $d = 14$, 我们有

$$\sqrt{14} = 3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \sqrt{14}}}}},$$

所以 $3 + \sqrt{14}$ 的连分数展开式是纯周期的, 其周期长度为 4, 在第一个周期之末将展开式截断, 即得分数

$$3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}} = \frac{15}{4},$$

这是 $\sqrt{14}$ 的一个较好的逼近[4]. 它的分子与分母即导出基本解 $x_1 = 15, y_1 = 4$; 事实上, 我们有 $15^2 = 14 \cdot 4^2 + 1$. 进而言之, 我们有 $(15 + 4\sqrt{14})^2 = 449 + 120\sqrt{14}$, 所以 $x_2 = 449, y_2 = 120$, 等等, 我们有下表:

| $n$ | $x_n$ | $y_n$ |
|---|---|---|
| 1 | 15 | 4 |
| 2 | 449 | 120 |
| 3 | 13455 | 3596 |
| 4 | 403201 | 107760 |
| 5 | 12082575 | 3229204 |
| 6 | 362074049 | 96768360 |

[2]环 $\mathbb{Z}[\sqrt{d}]$ 表示集合 $\{a + b\sqrt{d}; a, b \in \mathbb{Z}\}$, 其中 $\mathbb{Z}$ 表示全体整数所成的集合. 我们称 $\alpha' = a - b\sqrt{d}$ 为 $\alpha = a + b\sqrt{d}$ 的共轭数, 及 $N(\alpha) = a^2 - db^2$ 为 $\alpha$ 的范数. 若 $N(\alpha) = \pm 1$, 则称 $\alpha$ 为 $\mathbb{Z}[\sqrt{d}]$ 的单位. 因此 Pell 方程的解即 $\mathbb{Z}[\sqrt{d}]$ 中的单位. 由于当 $\alpha$ 为单位时, $\alpha^n (n \in \mathbb{Z})$ 亦然, 所以当知道 Pell 方程的一个解, 即知道它的无穷多个解. —— 译者注

[3]关于 Dirichlet 单位定理, 请参看 E. Hecke 著《代数数理论讲义》(科学出版社, 2005), §35. —— 译者注

[4]这里计算有错, 应该是 $\sqrt{14} - 3 = [\dot{1}2\dot{1}6]$. —— 译者注

表的形式反映出随 $n$ 的增长, $x_n$ 与 $y_n$ 呈指数型增长.

对于一般的 $d$, $[\sqrt{d}]+\sqrt{d}$ 的连分数展开式亦为纯周期的, 如同我们见到 $d$=14 时一样, 周期段是对称的. 当周期长度为偶数时, 则可以如上处理; 而当周期的长度为奇数时, 则需在第二个周期之末截断 [Buhler and Wagon 2008].

## 2. 群牛问题

从计算与历史两方面来说, Archimedes (公元前 287—前 212) 提出的群牛问题都是 Pell 方程的一个有趣例子. Lessing (1729—1781) 在 Wolffenbüttel 图书馆里发现了一份含有这个问题的手稿, 并将它于 1773 年发表 (见 [Lessing 1773; Heiberg 1913, pp. 528–234]). 现在一般将这个问题归于 Archimedes 名下 ([Fraser 1972; Weil 1984]). 在 22 行希腊哀歌体的对句诗中, 问题要求求出满足一些算术限制的属于太阳神的白色、黑色、有斑点以及棕色的公牛与母牛的个数, 它的英文对句诗版本取自文献 [Archimedes 1999], 见下页图. 用近代数学记号, 这个问题仍不失其优美. 记白色、黑色、有斑点与棕色的公牛个数分别为 $x, y, z, t$, 则由诗的第 8–16 行可知它们需满足条件

$$x=\left(\frac{1}{2}+\frac{1}{3}\right)y+t,$$

$$y=\left(\frac{1}{4}+\frac{1}{5}\right)z+t,$$

$$z=\left(\frac{1}{6}+\frac{1}{7}\right)x+t.$$

其次, 令 $x', y', z', t'$ 分别表示对应于同样颜色的母牛个数, 则诗的第 17–26 行要求

$$x'=\left(\frac{1}{3}+\frac{1}{4}\right)(y+y'), \qquad y'=\left(\frac{1}{4}+\frac{1}{5}\right)(z+z'),$$

$$z'=\left(\frac{1}{5}+\frac{1}{6}\right)(t+t'), \qquad t'=\left(\frac{1}{6}+\frac{1}{7}\right)(x+x').$$

迄今为止, 任何能够解决这个问题的人将被称为 Archimedes 认定的优胜者, 为了得到这一最高智慧奖, 它们还要满足诗的第 33–40 行所述的条件, 即 $x+y$ 为一个平方数, 而 $z+t$ 为一个三角数[5].

问题的第一部分属于线性代数, 它的确有正整数解. 最前面三个方程的通解由 $(x, y, z, t)=m\cdot(2226, 1602, 1580, 891)$ 给出, 其中 $m$ 表示一个正整数. 于是往下的四个方程可解当且仅当 $m$ 可以被 4657 整除, 即 $m=4657\cdot k$. 我们得到

$$(x', y', z', t')=k\cdot(7206360, 4893246, 3515820, 5439213).$$

[5]所谓三角数为形如 $\frac{n(n+1)}{2}$ 的数, 即 1, 3, 6, 10, $\cdots$ —— 译者注

# PROBLEM

*that Archimedes conceived in verse*
*and posed to the specialists at Alexandria*
*in a letter to Eratosthenes of Cyrene.*

The Sun god's cattle, friend, apply thy care
to count their number, hast thou wisdom's share.
They grazed of old on the Thrinacian floor
of Sic'ly's island, herded into four,
colour by colour: one herd white as cream,
the next in coats glowing with ebon gleam,
brown-skinned the third, and stained with spots the last.
Each herd saw bulls in power unsurpassed,
in ratios these: count half the ebon-hued,
add one third more, then all the brown include;
thus, friend, canst thou the white bulls' number tell.
The ebon did the brown exceed as well,
now by a fourth and fifth part of the stained.
To know the spotted — all bulls that remained —
reckon again the brown bulls, and unite
these with a sixth and seventh of the white.
Among the cows, the tale of silver-haired
was, when with bulls and cows of black compared,
exactly one in three plus one in four.
The black cows counted one in four once more,
plus now a fifth, of the bespeckled breed
when, bulls withal, they wandered out to feed.
The speckled cows tallied a fifth and sixth
of all the brown-haired, males and females mixed.
Lastly, the brown cows numbered half a third
and one in seven of the silver herd.
Tell'st thou unfailingly how many head
the Sun possessed, o friend, both bulls well-fed
and cows of ev'ry colour — no-one will
deny that thou hast numbers' art and skill,
though not yet dost thou rank among the wise.
But come! also the foll'wing recognise.
Whene'er the Sun god's white bulls joined the black,
their multitude would gather in a pack
of equal length and breadth, and squarely throng
Thrinacia's territory broad and long.
But when the brown bulls mingled with the flecked,
in rows growing from one would they collect,
forming a perfect triangle, with ne'er
a diff'rent-coloured bull, and none to spare.
Friend, canst thou analyse this in thy mind,
and of these masses all the measures find,
go forth in glory! be assured all deem
thy wisdom in this discipline supreme!

现在真正的挑战在于选择 $k$ 使得 $x+y=4657\cdot 3828\cdot k$ 为一个平方数且 $z+t=4657\cdot 2471\cdot k$ 是一个三角数. 由素因子分解 $4657\cdot 3828=2^2\cdot 3\cdot 11\cdot 29\cdot 4657$ 可知, 第一个条件等价于 $k=al^2$, 此处 $a=3\cdot 11\cdot 29\cdot 4657$ 并且 $l$ 为一个整数. 由于 $z+t$ 为一个三角数当且仅当 $8(z+t)+1$ 是一个平方数, 我们得到方程 $h^2=8(z+t)+1=8\cdot 4657\cdot 2471\cdot al^2+1$, 这是 Pell 方程 $h^2=dl^2+1$, 其中

$$d=2\cdot 3\cdot 7\cdot 11\cdot 29\cdot 353\cdot (2\cdot 4657)^2=410\,286423\,278424.$$

因此, 由 Lagrange 定理可知群牛问题有无穷多组解.

1867 年, 不那么著名的德国数学家 C. F. Meyer 用连分数方法来解这个方程 [Dickson 1920, p.344]. 在对 $\sqrt{d}$ 作连分数展开 240 步之后, 他仍未能查出其周期, 于是他放弃了. 他可能有一点不耐烦; 以后被发现周期长度为 203254; 见 [Grosjean and De Meyer 1991]. 1880 年, A. Amthor 首先用一个令人满意的方法解决了群牛问题 (见 [Krumbiegel and Amthor 1880]). Amthor 没有直接应用连分数方法; 我们将在下面讨论他是怎么做的. 他既没有写出 Pell 方程基本解的十进位表示, 也没有给出群牛问题的对应解答. 他确实证明了群牛问题的最小解是一个有 206545 位的数, 其中最前面的四个数字是 7766, 但其中第四个数是错误的, 这是由于他用了不够精确的对数引起的. 整个数字占据了 47 页计算机输出打印纸, 用 12 页缩小的字体登于 *Journal of Recreational Mathematics* [Nelson 1980/81] 上, 它的缩写为

$$77602714\cdots 237983357\cdots 55081800,$$

其中六个点之每一点均表示省略了 34420 位数字.

19 世纪有一些德国学者感到困扰, 这么多公牛与母牛可能不适宜放在西西里岛上, 因为这与诗的第 3 行和第 4 行相矛盾, 但是, Lessing 指出牛群的所有者太阳神将能应对它.

群牛问题的故事表明, 连分数方法并非解 Pell 方程的最后语句.

## 3. 效率

我们对 Pell 方程解法的*效率*感兴趣. 那么, 一个解答 Pell 方程的给定算法需要多少时间才能完成? 这里, 时间是用实际的途径来度量的, 例如, 它反映出大正整数所需的运算时耗要比小整数多, 技术上, 我们作比特 (二进位) 计算. 假定将 $d$ 输入运算程序, 则运算时间的估计需被表示为 $d$ 的函数. 若 $d$ 被二进位或十进位表示, 则输入长度近似地与 $\log d$ 成比例. 若存在一个正实数 $c_0$ 使对所有 $d$, 运算时间皆不超过 $(1+\log d)^{c_0}$, 则称算法按*多项式时间*运行, 换言之, 求解 Pell 方程的算法所需时间不多于写下这个方程所需的时间.

连分数方法有多快呢? Pell 方程可否用多项式时间求解呢? 欲回答这类问题需要考虑的中心量为调整子[6](regulator) $R_d$, 其定义为

$$R_d = \log(x_1 + y_1\sqrt{d}),$$

此处, 如前定义, $x_1 + y_1\sqrt{d}$ 表示 Pell 方程的基本解. 调整子与代数数论中的定义是一致的; 在那里, 范数映射 $\mathbb{Z}[\sqrt{d}]^* \to \mathbb{Z}^*$ 的核被称为调整子. 由 $x_1 - y_1\sqrt{d} = 1/(x_1 + y_1\sqrt{d})$ 可得 $0 < x_1 - y_1\sqrt{d} < 1/(2\sqrt{d})$, 再由 $x_1 + y_1\sqrt{d} = \mathrm{e}^{R_d}$, 即得

$$\frac{\mathrm{e}^{R_d}}{2} < x_1 < \frac{\mathrm{e}^{R_d}}{2} + \frac{1}{4\sqrt{d}}, \quad \frac{\mathrm{e}^{R_d}}{2\sqrt{d}} - \frac{1}{4d} < y_1 < \frac{\mathrm{e}^{R_d}}{2\sqrt{d}}.$$

这就证明了 $R_d$ 非常接近于 $\log(2x_1)$ 及 $\log(2y_1\sqrt{d})$. 换言之, 若将 $x_1$ 与 $y_1$ 用二进位或十进位表示出来, 则 $R_d$ 与求解 Pell 方程的任何算法的输出长度是近似成比例的. 由于拼写输出所需的时间是总运行时间的一个下界, 所以我们得到结论: *存在 $c_1$ 使求解 Pell 方程的任何算法所需的时间至少为 $c_1R_d$.* 在此 $c_1$ 以及以下的 $c_2, c_3, \cdots$ 皆表示不依赖于 $d$ 的正实数.

连分数方法几乎达到了这个下界. 令 $l$ 表示 $[\sqrt{d}] + \sqrt{d}$ 的连分数展开之周期长度, 此处周期长度需为偶数, 而当周期长度为奇数时, 则周期长度需为 $l$ 之两倍, 于是有

$$\frac{\log 2}{2} \cdot l < R_d < \frac{\log(4d)}{2} \cdot l$$

(见 [Lenstra 1982, (11.4)]). 所以 $R_d$ 与 $l$ 是近似成比例的, 由此易得直接运用连分数方法所需的时间最多为 $R_d^2 \cdot (1 + \log d)^{c_2}$, 其中 $c_2$ 为某正常数; 依赖于快速 Fourier 变换的改进的连分数方法可将计算量减至 $R_d \cdot (1 + \log d)^{c_3}$, 其中 $c_3$ 为某正常数; 见 [Schönhage 1971]. 连分数方法的后面这个版本除一个对数因子外, 是臻于至善的.

由上述这些结果, 很自然地要问作为 $d$ 的函数, 调整子的增长情况, 它有很大的波动. 我们有

$$\log(2\sqrt{d}) < R_d < \sqrt{d} \cdot (\log(4d) + 2),$$

由上面证明过的不等式 $y_1 < \mathrm{e}^{R_d}/(2\sqrt{d})$, 即得上式的下界估计, 而上界估计则由华罗庚的一个定理得出 [Hua 1942][7]. 这两个界的差别非常巨大, 但却不能避免: 若 $d$ 可取形如 $k^2 - 1$ 的数, 则得 $x_1 = k$, $y_1 = 1$, 从而 $R_d - \log(2\sqrt{d})$ 趋于 0; 我们还可以证明存在一个 $d$ 的无穷集合 $D$ 及一个常数 $c_4$, 使对于所有 $d \in D$ 皆有 $R_d = c_4\sqrt{d}$. 事实上, 若 $d_0, d_1$ 均为大于 1 的整数及 $d_0$ 不是一个平方数, 则存在一个正整数 $m = m(d_0, d_1)$, 使 $D = \{d_0 d_1^{2n} : n \in \mathbb{Z}, n \geqslant m\}$ 对于某常数 $c_4 = c_4(d_0, d_1)$ 具有这个性质.

可以相信, 对于绝大多数 $d$, 上界估计接近于真实. 更精确些, 有一个传统的猜想断言存在一个密率为 1 的非平方数集合 $D$, 即 $D$ 适合 $\lim\limits_{x\to\infty} \#\{d \in D : d \leqslant x\}/x = 1$,

[6]关于调整子的一般定义见注 (3) 提到的 E. Hecke 著的书 §35. —— 译者注

[7]关于华罗庚定理请见脚注 (1) 提到的《数论导引》第 12 章, §13. —— 译者注

满足

$$\lim_{d\in D}\frac{\log R_d}{\log\sqrt{d}}=1.$$

这是一个未解决的猜想, 一个弱得多的猜想仍待解决, 即 $\limsup_d(\log R_d)/\log\sqrt{d}>0$, 此处 $d$ 可取大于 1 的无平方因子数.

如果传统的猜想真实, 则对于绝大多数 $d$, 估计运算时间时, $R_d$ 大约应是 $\sqrt{d}$, 它是输入长度 $\log d$ 的指数函数.

综合上述结果可知, 连分数方法所需运算时间最多为 $\sqrt{d}\cdot(1+\log d)^{c_5}$; 人们猜想, 对于绝大多数 $d$ 为慢指数型; 而求解 Pell 方程的任何方法对于无穷多个 $d$, 全部写出 $x_1$ 与 $y_1$ 的时耗是慢指数型, 从而不能为多项式运算时间.

若想改进连分数方法, 则我们必须有一个比十进位或二进位更简洁的表示 $x_1$ 与 $y_1$ 的途径.

## 4. Amthor 的解法

Amthor 对于群牛问题的解法基于下面的考虑: 数 $d=410\,286423\,278424$ 可以写成 $(2\cdot4657)^2\cdot d'$, 此处 $d'=4\,729494$ 无平方因子. 因此若 $x$, $y$ 是关于 $d$ 的 Pell 方程之解, 则 $x$, $2\cdot4657\cdot y$ 是关于 $d'$ 的 Pell 方程之解, 所以有某个 $n$, 使后面 Pell 方程的第 $n$ 个解 $x'_n, y'_n$ 适合:

$$x+2\cdot4657\cdot y\cdot\sqrt{d'}=(x'_1+y'_1\sqrt{d'})^n.$$

这就将群牛问题归结为两个较容易的问题: 第一个问题为求解关于 $d'$ 的 Pell 方程; 而第二个问题为找出最小的 $n$ 使 $y'_n$ 可以被 $2\cdot4657$ 整除.

因 $d'$ 比 $d$ 小得多, Amthor 可以用连分数程序处理 $d'$ 的方程, 在一个可以用 3 页纸写成的计算中 [Krumbiegel and Amthor 1880], 他发现周期长度为 92 及 $x'_1+y'_1\sqrt{d'}$ 等于

$$\begin{aligned}u=\ &109\,931986\,732829\,734979\,866232\,821433\,543901\,088049\\&+50549\,485234\,315033\,074477\,819735\,540408\,986340\cdot\sqrt{d'}.\end{aligned}$$

为了节省篇幅, 我们可以写成

$$u=(300\,426607\,914281\,713365\cdot\sqrt{609}+84\,129507\,677858\,393258\cdot\sqrt{7766})^2.$$

这是由适合 $x^2-dy^2=1$ 的 $x,y$ 满足的恒等式 $x+y\sqrt{d}=(\sqrt{(x-1)/2}+\sqrt{(x+1)/2})^2$ 推出来的, 调整子满足 $R'_d\doteq102.101583$.

为了决定 $n$ 的最小可行值, Amthor 发展了一个小理论, 我们今天可以用有限域与环的语言来表达. 利用 $p=4657$ 为一个素数及 Legendre[8]符号 $\left(\frac{d'}{p}\right)$ 等于 $-1$, 则由他

[8]关于 Legendre 符号的定义, 请见脚注 (1) 提到的华罗庚著《数论导引》第 3 章, §1. —— 译者注

的理论, 他得出 $n$ 的最小值可以整除 $p+1=4658$; 经更仔细地处理, 他发现 $n$ 必须整除 $(p+1)/2=2329=17\cdot 137$; 见 [Vardi 1998]. 当试少许因子后, 我们即可知 $n$ 的最小值的确等于 2329, 因此 $R_d=2329\cdot R'_d\doteq 237794.586710$.

结论为关于 $d$ 的 Pell 方程的基本解由 $x_1+y_1\sqrt{d}=u^{2329}$ 给出, 此处 $u$ 已于前面定义过. Amthor 未能将各个结果综合起来, 但我做了这件事, 为了读者方便: 这在历史上是首次, 群牛问题的所有无穷多个解被安排在一张方便的小表中! 很自然地, 它不包含任何答案的完全十进位表示, 若要这样做, 则需更多的智慧. 例如, 读者不仅易于验证由最小解给出的牛的头数有 206545 个十进位数字并等于 $77602714\cdots 55081800$, 而且可以发现第 1494 195300 个解中有斑点的公牛的个数为一个有 308 619694 367813 位数字的数, 它等于 $111111\cdots 000000$. (发现中间位置的数字可能相当困难.) 关于大数的表示, Archimedes 曾写了一封长信给 Gelon 国王 (见 [Dijksterhuis 1956] 或 [Heiberg 1913, pp 215–259]), 由下表给出的解答无疑将使他高兴与满意.

Archimedes 群牛问题的所有解

$$w=300\,426607\,914281\,713365\cdot\sqrt{609}+84\,129507\,677858\,393258\cdot\sqrt{7766}$$

$$k_j=(w^{4658\cdot j}-w^{-4658\cdot j})^2/368\,238304\quad(j=1,2,3,\cdots)$$

| 第 $j$ 个解 | 公牛 | 母牛 | 所有牛 |
|---|---|---|---|
| 白色的 | $10\,366482\cdot k_j$ | $7\,206360\cdot k_j$ | $17\,572842\cdot k_j$ |
| 黑色的 | $7\,460514\cdot k_j$ | $4\,893246\cdot k_j$ | $12\,353760\cdot k_j$ |
| 有斑点的 | $7\,358060\cdot k_j$ | $3\,515820\cdot k_j$ | $10\,873880\cdot k_j$ |
| 棕色的 | $4\,149387\cdot k_j$ | $5\,439213\cdot k_j$ | $9\,588600\cdot k_j$ |
| 所有颜色的 | $29\,334443\cdot k_j$ | $21\,054639\cdot k_j$ | $50\,389082\cdot k_j$ |

## 5. 幂乘积

假定人们希望对于一个给定的 $d$, 求解 Pell 方程 $x^2=dy^2+1$, 由 Amthor 关于群牛问题的解法, 我们发现寻求 $d$ 的最小因子 $d'$ 使 $d/d'$ 为一个平方数可能是明智的, 有两个理由: 当执行连分数算法时节省了时间, 而在表示最后结果时, 既节省时间, 又节省空间. 现在还不知道由 $d$ 寻求 $d'$ 要比 $d$ 的因子分解本质上快的算法. 此外, 如果我们想决定关于 $d'$ 的基本解的什么方幂可以导出关于 $d$ 的基本解 —— 即前一节中的数 $n$ —— 我们亦需知道, $\sqrt{d/d'}$ 的素因子分解, 及对于一个 $\sqrt{d/d'}$ 的素因子 $p$, $p-\left(\frac{d'}{p}\right)$ 的素因子分解. 因此, 如果我们想求解 Pell 方程, 首先就要分解 $d$. 已知的素分解算法对于大的 $d$ 可能不是很快, 但对于多数 $d$, 仍可以期待其计算量之阶快于求解 Pell 方程的任何已知方法 [Stevenhagen 2008b].

现在假定 $d$ 无平方因子, 并记 $x_1+y_1\sqrt{d}$ 为 Pell 方法的基本解, 它是 $\mathbb{Z}[\sqrt{d}]$ 一个

单位, 则 $x_1+y_1\sqrt{d}$ 可能亦是 $\mathbb{Z}[\sqrt{d}]$ 的分数域 $\mathbb{Q}(\sqrt{d})$[9]中一个数的某方幂. 例如, 具有 $y_1>6$ 的最小的 $d$ 是 $d=13$, 对于它, 我们有 $x_1=649, y_1=180$, 及

$$649+180\sqrt{13}=\left(\frac{3+\sqrt{13}}{2}\right)^6.$$

1657 年, Fermat 提出一个挑战性问题, 即对于 $d=109$, 基本解为一个六次方幂:

$$158\,070671\,986249+15\,140424\,455100\sqrt{109}=\left(\frac{261+25\sqrt{109}}{2}\right)^6.$$

就目前所知, 这是代数数论中一个初等习题, 即若 $n$ 是个正整数使 $x_1+y_1\sqrt{d}$ 在 $\mathbb{Q}(\sqrt{d})$ 中有 $n$ 次根, 则 $n=1,2,3$ 或 6, 其中仅当 $d\equiv 1$, 2 或 5 mod 8 时, 有可能 $n=2$, 而仅当 $d=5 \bmod 8$ 时, 有可能 $n=3$ 及 6, 因此, 对于大的无平方因子的数 $d$, 我们不可能期望在书写 $x_1+y_1\sqrt{d}$ 时节省很多空间, 就如同我们在做群牛问题那样, 当根被允许位于二次域的复合中时亦是这样.

假定 $d$ 为一个任意非平方正整数, 我们考虑 $\mathbb{Q}(\sqrt{d})$ 中的*方幂积*来代替方幂, 即考虑形如

$$\prod_{i=1}^{t}(a_i+b_i\sqrt{d})^{n_i}$$

的表示式, 此处 $t$ 为一个非负整数, $a_i,b_i,n_i$ 为整数, $n_i\neq 0$, 而对于每一个 $i$, $a_i,b_i$ 中至少有一个非零. 我们定义这样一个表示式的*长度*为

$$\sum_{i=1}^{t}(\log|n_i|+\log(|a_i|+|b_i|\sqrt{d})).$$

这粗略地与表示 $a_i,b_i,n_i$ 诸数所需的比特总和成比例. 每一个幂乘积表示 $\mathbb{Q}(\sqrt{d})$ 中的一个非零元素, 而这个元素可以唯一地表为 $(a+b\sqrt{d})/c$, 其中 $a,b,c\in\mathbb{Z}, \gcd(a,b,c)=1, c>0$. 无论如何, $a,b,c$ 的比特数将随 $|n_i|$ 指数而不是随它们的对数线性地增长, 所以我们避免用后面的表达式而直接用幂乘积.

将元素表示为幂乘积引起了一些基本问题. 例如, 我们是否可以用多项式时间判定两个幂乘积表示 $\mathbb{Q}(\sqrt{d})$ 中的同样的数? 这里如前所述, "多项式时间" 表示运算时间是输入长度的多项式函数, 在这里, 输入长度等于这两个给定幂乘积的长度之和. 类似地, 我们可否用多项式时间决定一个给定的幂乘积表示为形如 $a+b\sqrt{d}$ 的数, 其中 $a,b\in\mathbb{Z}$, 即 $\mathbb{Z}[\sqrt{d}]$ 中的一个元素? 如果可以, 我们能否用多项式时间决定它满足 $a^2-db^2=1$, 其中 $a,b>0$, 从而得到 Pell 方程的一个解, 及能否算出 $a$ 与 $b$ 模一个已给正整数 $m$ 所属的剩余类?

刚刚提出的所有问题的答案都是肯定的, 即使对于一般代数数域来说, 亦是这样. 最近 Guoqiang Ge [1993; 1994] 展示了证明之算法. 特别地, 我们能够有效地决定一个

[9]$\mathbb{Q}(\sqrt{d})$ 表示集合 $\{r+s\sqrt{d}: r,s\in\mathbb{Q}\}$, 其中 $\mathbb{Q}$ 表示全体有理数所成之集合. —— 译者注