国家出版基金资助项目

高斯——泥瓦匠之子，被誉为数学王子，身为最卓越的古典数学家，为19世纪数学奠基础。

1801年，高斯在《算术研究》中提出三个著名猜想，牵引庞布局中国代数数论组织攻关。

影响数学世界的猜想与问题

陆洪文 著

从高斯到盖尔方特
——二次数域的高斯猜想

From Gauss to Gel'fand
—The Gauss Conjecture of Quadratic Field

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

国家出版基金资助项目

影响数学世界的猜想与问题

陆洪文 著

从高斯到盖尔方特

——二次数域的高斯猜想

From Gauss to Gel'fand

—The Gauss Conjecture of Quadratic Field

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

内 容 简 介

本书系统且完整地阐述了高斯所提出的关于二次数域类数的三个著名猜想，特别着重于近几十年来有关这方面研究的最新成就.

前三章是预备知识，系统阐明了二次数域的算术理论和解析理论. 第四、五、六章分别详细论述了类数问题的一般状况，虚二次数域高斯类数猜想的解决，以及实二次数域的类数问题的难点所在和它的现状. 其中特别介绍了 Baker-Stark 和 Goldfeld-Gross-Zagier 的有关研究的详细情况，包括他们是如何把超越理论和椭圆曲线的 BSD 猜想用在类数问题上的，这两项工作分别获得了 1970 年的 Fields 奖与 1987 年的 Cole 奖.

本书可以作为数学工作者、研究生和大学数学系高年级学生的教材和参考书.

图书在版编目(CIP)数据

从高斯到盖尔方特：二次数域的高斯猜想./陆洪文著.
—哈尔滨：哈尔滨工业大学出版社，2013.8
(影响数学世界的猜想与问题)
ISBN 978-7-5603-4136-1

Ⅰ.①从… Ⅱ.①… Ⅲ.①二次域-类数
Ⅳ.①O153.4

中国版本图书馆 CIP 数据核字(2013)第 144549 号

策划编辑　刘培杰　张永芹
责任编辑　张永芹　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　黑龙江省教育厅印刷厂
开　　本　787mm×1092mm　1/16　印张 24.75　字数 510 千字
版　　次　2013 年 8 月第 1 版　2013 年 8 月第 1 次印刷
书　　号　ISBN 978-7-5603-4136-1
定　　价　198.00 元

序言

Euler 在 1772 年发现了下列有趣的事实：

当 $x = 0,1,\cdots,40$ 时，$x^2 - x + 41$ 均是素数.

这一事实与所谓的 Gauss 的类数 1 问题密切相关，因此我们有命题 A.

命题 A（Rabinovitch[88]） 设无平方因子整数 $D < 0, D \equiv 1 \pmod 4$. 则当 $x = 0,1,\cdots,\frac{|D|-3}{4}$ 时，$x^2 - x + \frac{1+|D|}{4}$ 均表素数的充要条件是虚二次域 $\boldsymbol{Q}(\sqrt{D})$ 的整数环是唯一分解的，即 $\boldsymbol{Q}(\sqrt{D})$ 的类数为 1.

由于虚二次域 $\boldsymbol{Q}(\sqrt{-163})$ 的类数是 1，所以我们由定理 A 立即得出 Euler 断言的真实性.

同样，我们可以有下面的命题 B.

命题 B（陆洪文[46]） 设无平方因子整数 $D = 4N^2 + 1$，其中正整数 $N > 1$. 则当 $x = 1,2,\cdots,N-1$ 时，$N^2 - x - x^2$ 均表素数的充要条件是实二次域 $\boldsymbol{Q}(\sqrt{D})$ 的整数环是唯一分解的，即 $\boldsymbol{Q}(\sqrt{D})$ 的类数为 1.

由于 $N = 13$ 时，$D = 677$，而 $\boldsymbol{Q}(\sqrt{677})$ 的类数为 1，所以我们有下列事实：

当 $x = 1,2,\cdots,12$ 时，$169 - x - x^2$ 均是素数.

这样寻找类数为1的二次数域是一个既古老又很有意义的问题.这个问题是Gauss提出的.Gauss在其名著《Disquisitiones Arithmeticae》(《算术探索》,由哈尔滨工业大学出版社于2011年12月出版)中,提出下列三个著名的猜想,它们用现代语言叙述,即为

1. 当判别式 $D \to -\infty$ 时,虚二次域 $\boldsymbol{Q}(\sqrt{D})$ 的类数 $h(D) \to +\infty$;

2. 正好存在九个类数为1的虚二次域,十八个类数为2的虚二次域和十六个类数为3的虚二次域,等等;

3. 存在无穷多个类数为1的实二次域.

1918 ~ 1934年间,Hecke[43],Deuring[13],Mordell[81]以及Heilbronn[30]等人的工作,完全解决了Gauss的第一个猜想,即有下列的定理C.

定理C(Hecke-Deuring-Mordell-Heilbronn)

$$h(D) \to +\infty, \text{如 } D \to -\infty$$

这里 D 表二次数域 $\boldsymbol{Q}(\sqrt{D})$ 的判别式,$h(D)$ 为其类数.

在Heilbronn和Linfoot[31](1934)工作的基础上,K. Heegner[29],A. Baker[3]和H. Stark[95-96],[99]的工作,完全解决了Gauss关于类数1和2的虚二次域的猜想,即有下列的定理D.

定理D(Heegner-Baker-Stark) 分别正好有九个和十八个类数为1和2的虚二次数域,它们的判别式分别是 $-3, -4, -7, -8, -11, -19, -43, -67, -163$(这些的类数为1)和 $-15, -20, -24, -35, -40, -51, -52, -88, -91, -115, -116, -123, -148, -187, -235, -267, -403, -427$(这些的类数为2).

另外,C. L. Siegel[92](1935)和Tatuzawa[103](1951)的工作给出了下面的定理E.

定理E(Siegel-Tatuzawa) 对任给的正常数 $\delta > 0$,均存在可以有效计算的正常数 C_δ,使得至多除去一个二次数域以外,恒有

$$h(D)R_D > C_\delta \mid D \mid^{\frac{1}{2}-\delta}$$

这里 D,$h(D)$ 分别表示二次数域 $\boldsymbol{Q}(\sqrt{D})$ 的判别式、类数,而 R_D 是1(对虚二次域)或正则子(对实二次数域).

关于虚二次域的Gauss类数猜想,最后是由D. Goldfeld[22](1975),B. Gross和D. Zagier[23](1983)的工作解决的,即有下面的定理F.

定理F(Goldfeld-Gross-Zagier) 对判别式为 D 的虚二次数域 $\boldsymbol{Q}(\sqrt{D})$,其类数

$$h(D) > \frac{1}{55}(\log|D|)\prod_{\substack{p|D| \\ p\neq|D|}}\left(1-\frac{[2\sqrt{p}]}{p+1}\right)$$

其中 p 表素数,$[x]$ 表 x 的整数部分.

我们做了参考文献中的[57](1986),上述常数 55 可以改进为 54.

Goldfeld 的想法是利用椭圆曲线理论中的 BSD 猜想,把上述定理的证明归结为找到一条椭圆曲线,它的 Hasse-Weil L - 函数在 $s=1$ 处有一个三阶零点. Gross 和 Zagier 花了 7 年的功夫完成了后一任务.

这样下一步的任务,理所当然地转向了关于实二次域的 Gauss 类数猜想(3).

由上述的 Siegel-Tatuzawa 定理可以看到,实二次域 $\boldsymbol{Q}(\sqrt{D})$ 有关问题的困难还在于它的所谓的正则子 $\log\varepsilon_D$,其中 ε_D 为 $\boldsymbol{Q}(\sqrt{D})$ 的基本单位.

现在关于实二次域方面的结果还非常不完善,即使在小正则子时的情况,除匈牙利数学家 A. Biro 证明了 Chowla 猜想和 Yokoi 猜想之外,也只相当于虚二次域在20世纪60年代以前的水平上,所以还有许多工作可做. 现在的状况见第六章.

本书的目的,一方面概述虚二次域方面的卓越成果,另一方面着重叙述实二次域方面的情况.

本书第一章讲述实二次无理数的连分数展开,它的本身似乎非常初等和简单,但是却在关于实二次域的研究中起着非常重要的作用,究其原因,还是上述的正则子在作怪.

第二章讲述二元二次型与二次域的一般理论,这些内容是经典的,例如可见华罗庚的《数论导引》,只有个别的新结果,例如关于某些完全特征和的公式和实二次域的初等类数公式.

第三章讲述极限公式. 虚二次域方面的结果是经典的. 实二次域方面的结果为以后的研究作了很好的准备.

从第四章起用三章的篇幅讲述 Gauss 类数问题,其中第四章讲述 20 世纪 50 年代以前的工作,包括 Euclid 域的决定;第五章讲述虚二次域 Gauss 类数问题的完整解决的详细情况;第六章致力于实二次域的 Gauss 类数问题,详细地阐述了近年来国内外在这方面的研究成果.

第七章讲述所谓的 Hirzebruch 和在 Hecke 算子作用下的变化情况,这也和 Gauss 类数问题有关,特别是和实二次域正则子的有关猜想密切相关.

希望本书的出版有助于 Gauss 类数猜想的进一步研究,特别希望能吸引有兴趣的年轻学者来攀登这一个科学高峰. 由于本人能力的限制,本书难免出现

$f(x,y)=ax^2+bxy+cy^2$

谬误和遗漏,请读者不吝指教.

作者对自己的导师,已故数学大师华罗庚教授表示衷心的感谢和深切的怀念;同时对自己的师长王元教授和谷超豪教授,同门冯克勤教授表示由衷的谢忱,他们仔细地审阅了本书的原稿.

最后,我要特别感谢哈尔滨工业大学出版社的刘培杰老师对本书出版的鼎力支持.

陆洪文

2013 年 5 月 8 日

◎常用符号表

$\mathbf{N} = \{1,2,3,\cdots\}$.

$\boldsymbol{Z},\boldsymbol{Q},\boldsymbol{R},\boldsymbol{C},\boldsymbol{F}_q$ 分别代表有理整数环，有理数域，实数域，复数域，q 个元素组成的有限域. 而 M^*（$M = \boldsymbol{Z},\boldsymbol{Q},\boldsymbol{R},\boldsymbol{C}$ 或 $\boldsymbol{F}_q$）表示由 M 的全体非零元素组成的集合.

$A \ll B$ 或 $A = O(B)$ 表示两个变量 A,B 在极限过程中满足 $|A| \leqslant cB$，这里 c 是一个正常数，$B \geqslant 0$，一般在各个具体情况下说明 c 的依赖关系.

$A \overset{\text{def}}{=\!=} B$ 表示 A 由 B 定义.

两个 L - 级数 $A \overset{def}{=\!=} \sum^{\infty} \frac{a_n}{n^s} \overset{def}{=\!=} \sum^{\infty} \frac{b_n}{n^s}$，表示 $b_n \geqslant 0$，且 $|a_n| \leqslant b_n, n \geqslant 1$.

两个有理整数 $A \mid B$，表示 A 是 B 的因子，即 A 除尽 B. $A \nmid B$ 表示 A 不是 B 的因子，即 A 除不尽 B.

$p^n \parallel A$，表示素数 p 的 n 次幂除尽 A，而 $p^{n+1} \nmid A$.

$[x]$ 表示实数 x 的整数部分，除非另有说明.

$[\alpha]$ 表示代数整数 α 生成的主理想.

◎目录

$f(x,y)=ax^2+bxy+cy^2$

连分数与 Pell 方程

第一章

由于实二次域的基本单位为一个 Pell 方程的最小解所确定，而后者又可以用连分数表出，所以连分数对实二次域的研究是一个非常有用的工具. 我们在 §1 中讲述实二次无理数的连分数展开，包括简单连分数、半单连分数和奇异连分数. 在 §2 中讲述 Pell 方程和更一般的二元二次不定方程的解. 有关的结论都是研究实二次域类数问题的必要的准备工作.

§1 实二次无理数的连分数展开

本节中讨论实二次无理数的三种连分数展开式，即简单连分数、半单连分数和奇异连分数. 前两者在实二次域类数问题的研究中起着非常重要的作用，后者则在研究实二次欧氏域时起着关键的作用.

1.1 简单连分数

对一个实数 α，可如下地定义 α 的简单连分数展开式（见华罗庚著《数论导引》第十章，这里为了引用的方便，给出概况）：

令 $\alpha_0 = \alpha$，对 $n \geqslant 0$，归纳地定义

$$a_n = [\alpha_n], \alpha_{n+1} = (\alpha_n - a_n)^{-1}$$

如

$$a_n \neq \alpha_n, a_n \in \mathbf{Z}(n \geqslant 0), a_n \geqslant 1(n \geqslant 1) \qquad (1.1)$$

其中 $[x]$ 表 x 的整数部分.

$f(x,y) = ax^2 + bxy + cy^2$

我们记

$$\alpha = [a_0, a_1, \cdots, a_n, \cdots] \tag{1.2}$$

α_n 称为 α 的第 n 个完全商

$$\frac{p_n}{q_n} = [a_0, a_1, \cdots, a_n] \quad (n \geqslant 0) \tag{1.3}$$

称为 α 的第 n 个渐近分数，其中要求 p_n, q_n 为互素的整数，且 $q_n \geqslant 1 (n \geqslant 0)$. 熟知有

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} \quad (n \geqslant 1) \tag{1.4}$$

$$p_0 = a_0, p_1 = a_0 a_1 + 1, p_n = a_n p_{n-1} + p_{n-2} \quad (n \geqslant 2) \tag{1.5}$$

$$q_0 = 1, q_1 = a_1, q_n = a_n q_{n-1} + q_{n-2} \quad (n \geqslant 2) \tag{1.6}$$

$$\alpha_n = [a_n, a_{n+1}, \cdots] \quad (n \geqslant 0) \tag{1.7}$$

有时还约定

$$p_{-1} = 1, q_{-1} = 0 \tag{1.8}$$

这样 $n = 0$ 时，式(1.4) 仍成立.

设 a, b, c 为有理整数，它们满足

$$0 \leqslant |b| \leqslant a \leqslant c \tag{1.9}$$

且 $d = b^2 + 4ac$ 不是完全平方. 易见

$$1 \leqslant a < \frac{\sqrt{d}}{2} \tag{1.10}$$

实二次无理数

$$\alpha = \frac{b + \sqrt{d}}{2a} > 0 \tag{1.11}$$

满足二次方程

$$ax^2 - bx - c = 0 \tag{1.12}$$

这个方程的另一个根是

$$\alpha' = \frac{b - \sqrt{d}}{2a} \tag{1.13}$$

α' 也是 α 在 Galois 群 $\mathrm{Gal}(\boldsymbol{Q}(\sqrt{d})/\boldsymbol{Q})$ 下的象.

命 α 的简单连分数展开式为

$$\alpha = [a_0, a_1, \cdots, a_n, \cdots], a_n \in \mathbf{Z}, a_0 \geqslant 0, a_n \geqslant 1 (n \geqslant 1) \tag{1.14}$$

并用式(1.1) ~ (1.13) 的记号. 再命

$$Q_0 = a, P_0 = b, P_1 = 2a_0 a - b \tag{1.15}$$

$$Q_n = (-1)^n (a p_{n-1}^2 - b p_{n-1} q_{n-1} - c q_{n-1}^2) \quad (n \geqslant 0) \tag{1.16}$$

$$P_n = (-1)^{n-1} (2a p_{n-1} p_{n-2} - b(p_{n-1} q_{n-2} + p_{n-2} q_{n-1}) - 2c q_{n-1} q_{n-2}) \quad (n \geqslant 1) \tag{1.17}$$

易见诸 $Q_n, P_n (n \geqslant 0)$ 均为有理整数. 且有

引理 1.1

$$P_n^2 + 4Q_nQ_{n-1} = d \quad (n \geqslant 1) \tag{1.18}$$

$$P_{n+1} + P_n = 2a_nQ_n \quad (n \geqslant 0) \tag{1.19}$$

$$Q_{n+1} = Q_{n-1} + a_nP_n - a_n^2Q_n \quad (n \geqslant 1) \tag{1.20}$$

$$1 \leqslant Q_n < \sqrt{d} \quad (n \geqslant 0) \tag{1.21}$$

$$P_n \geqslant 1 \quad (n \geqslant 1) \tag{1.22}$$

$$P_n < \sqrt{d} \quad (n \geqslant 0) \tag{1.23}$$

证明 式(1.18)与式(1.19)由直接计算可得. 式(1.20)是式(1.18)与式(1.19)的推论. 又由定义式(1.16)可得

$$Q_n = (-1)^n aq_{n-1}^2\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right)\left(\frac{p_{n-1}}{q_{n-1}} - \alpha'\right) \quad (n \geqslant 1) \tag{1.24}$$

由式(1.19)与式(1.10)即有 $\alpha' < 0$,再由式(1.4)可得

$$(-1)^n\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right) > 0 \quad (n \geqslant 1) \tag{1.25}$$

这样由式(1.24)即得 $Q_n > 0 (n \geqslant 1)$,从而 $Q_n \geqslant 1 (n \geqslant 0)$,这证明了式(1.21)的前一半.

如 $a_0 \geqslant 1$,则 $P_1 = 2a_0a - b \geqslant 2a - b \geqslant a \geqslant 1$;如 $a_0 = 0$,则 $\alpha < 1$,故由式(1.10)有 $b < 0$,从而仍有 $P_1 = -b \geqslant 1$. 总之有 $P_1 \geqslant 1$. 当 $n \geqslant 2$ 时,由定义(1.17)有

$$P_n = (-1)^{n-1}q_{n-1}q_{n-2}\left(2a\frac{p_{n-1}}{q_{n-1}} \cdot \frac{p_{n-2}}{q_{n-2}} - b\left(\frac{p_{n-1}}{q_{n-1}} + \frac{p_{n-2}}{q_{n-2}}\right) - 2c\right) \tag{1.26}$$

易见有

$$\alpha = \frac{\alpha_np_{n-1} + p_{n-2}}{\alpha_nq_{n-1} + q_{n-2}} \quad (n \geqslant 2) \tag{1.27}$$

由式(1.26),(1.27)有

$$\begin{aligned} P_n = {} & (-1)^{n-1}q_{n-1}q_{n-2}\left(2a\left(\alpha + \frac{(-1)^n}{q_{n-1}(q_{n-1}\alpha_n + q_{n-2})}\right) \cdot \right. \\ & \left(\alpha + \frac{(-1)^{n-1}\alpha_n}{q_{n-2}(q_{n-1}\alpha_n + q_{n-2})}\right) - \\ & \left. b\left(2\alpha + \frac{(-1)^n}{q_{n-1}(q_{n-1}\alpha_n + q_{n-2})} + \frac{(-1)^{n-1}\alpha_n}{q_{n-2}(q_{n-1}\alpha_n + q_{n-2})}\right) - 2c\right) \\ = {} & q_{n-1}q_{n-2}\left((2a\alpha - b)\frac{q_{n-1}\alpha_n - q_{n-2}}{q_{n-1}q_{n-2}(q_{n-1}\alpha_n + q_{n-2})} + \right. \\ & \left. \frac{2a(-1)^n\alpha_n}{q_{n-1}q_{n-2}(q_{n-1}\alpha_n + q_{n-2})}\right) \end{aligned}$$

其中用到 α 是方程(1.12)的一个根,从而得到

$$P_n = \frac{\sqrt{d}(q_{n-1}^2\alpha_n^2 - q_{n-2}^2) + (-1)^n 2a\alpha_n}{(q_{n-1}\alpha_n + q_{n-2})^2} \quad (n \geqslant 2) \tag{1.28}$$

$n = 2$ 时,式(1.28)右边分子的两项均非负,而第二项为正,故 $P_2 \geqslant 1$. 而 $n \geqslant 3$ 时,由于

$$q_{n-1}^2\alpha_n - q_{n-2}\alpha_n^{-1} > q_{n-1}^2 - q_{n-2}^2 \geqslant 2$$

故

$$\text{式(1.28)右边} = \alpha_n(\sqrt{d}(q_{n-1}^2\alpha_n^2 - q_{n-2}^2) + (-1)^n 2a)$$
$$> \alpha_n(2\sqrt{d} - 2a) > 0$$

从而 $n \geqslant 3$ 时,也有 $P_n \geqslant 1$. 引理的其余部分显然成立. 引理证毕.

引理 1.2 我们有

$$\alpha_n = \frac{P_n + \sqrt{d}}{2Q_n} \quad (n \geqslant 0) \tag{1.29}$$

$$\sqrt{d} - P_n < 2Q_n < \sqrt{d} + P_n \quad (n \geqslant 1) \tag{1.30}$$

$$\sqrt{d} - P_{n+1} < 2Q_n < \sqrt{d} + P_{n+1} \quad (n \geqslant 0) \tag{1.31}$$

$$a_n = \left[\frac{P_n + \sqrt{d}}{2Q_n}\right] \quad (n \geqslant 0) \tag{1.32}$$

$$a_n = \left[\frac{2Q_{n+1}}{\sqrt{d} - P_{n+1}}\right] \quad (n \geqslant 1) \tag{1.33}$$

证明 式(1.29)由定义,引理 1.1 及归纳法可得. 式(1.30)的右端显然成立,至于左端用引理 1.1 即有

$$\frac{2Q_n}{\sqrt{d} - P_n} = \frac{\sqrt{d} + P_n}{2Q_{n-1}} > \frac{P_{n-1} + P_n}{2Q_{n-1}} = a_{n-1} \geqslant 1$$

如 $n \geqslant 2$ 或 $n = 1$ 而 $a_0 \geqslant 1$. 但当 $n = 1$ 而 $a_0 = 0$ 时,由引理 1.1 的证明可知 $b < 0$,从而有 $Q_1 = c, P_1 = -b = |b|$,所以由式(1.9)及 a_0 的定义即有

$$2Q_1 = 2c \geqslant 2a > b + \sqrt{d} = \sqrt{d} - P_1$$

这就证明了式(1.30).

式(1.32)是式(1.29)的推论,于是有(注意由式(1.23)知 $\sqrt{d} > P_{n+1}$)

$$\frac{2Q_n}{\sqrt{d} - P_{n+1}} > \left[\frac{2Q_n}{\sqrt{d} - P_{n+1}}\right] = \left[\frac{P_{n+1} + \sqrt{d}}{2Q_{n+1}}\right] = a_{n+1} \geqslant 1 \quad (n \geqslant 0)$$

由此即得式(1.31)的左端. 至于右端用引理 1.1 即有

$$\frac{\sqrt{d} + P_{n+1}}{2Q_n} > \frac{P_n + P_{n+1}}{2Q_n} = a_n \geqslant 1$$

如 $n \geqslant 1$ 或 $n = 0$ 而 $a_0 \geqslant 1$ 时;但当 $n = 0$ 且 $a_0 = 0$ 时,有

$$\frac{\sqrt{d} + P_1}{2Q_0} = \frac{\sqrt{d} + |b|}{2a} > 1$$

所以式(1.31)完全得证. 由式(1.30),(1.19),(1.18)可得

$$a_n = \left[a_n + \frac{\sqrt{d} - P_n}{2Q_n}\right] = \left[\frac{\sqrt{d} + P_{n+1}}{2Q_n}\right] = \left[\frac{2Q_{n+1}}{\sqrt{d} - P_{n+1}}\right] \quad (n \geqslant 1)$$

即得式(1.33). 引理证毕.

由引理 1.2 即知 α 的简单连分数展开式为

$$\alpha = [a_0, \overline{a_1, \cdots, a_k}] \tag{1.34}$$

这个记号意指

$$a_{k+n} = a_n (n \geqslant 1) \tag{1.35}$$

我们取 k 为最小可能的,$\overline{a_1, \cdots, a_k}$ 称为**基本周期**,k 称为**周期的长度**.

这样可有

$$P_{k+1} = P_1, Q_{k+1} = Q_1, a_{k+1} = a_1 \tag{1.36}$$

$$Q_k = \frac{d - P_{k+1}^2}{4Q_{k+1}} = \frac{d - P_1^2}{4Q_1} = Q_0 = a \tag{1.37}$$

$$\begin{aligned} a_k &= \left[\frac{2Q_n}{\sqrt{d} - P_{n+1}}\right] = \left[\frac{\sqrt{d} + P_{n+1}}{2Q_k}\right] = \left[\frac{\sqrt{d} + P_1}{2Q_0}\right] \\ &= \left[\frac{\sqrt{d} + 2a_0 a - b}{2a}\right] = 2a_0 + \left[\frac{\sqrt{d} - 2a_0 a - b}{2a}\right] \\ &= 2a_0 + \left[\frac{\sqrt{d} - P_1}{2Q_0} - \frac{b}{a}\right] \\ &= \begin{cases} 2a_0 \text{ 或 } 2a_0 - 1, \text{当 } b \geqslant 0 \\ 2a_0 \text{ 或 } 2a_0 + 1, \text{当 } b < 0 \end{cases} \end{aligned} \tag{1.38}$$

引理 1.3 当 $b = 0$ 或 $\pm a$ 时,有

$$a_n = a_{k-n} (1 \leqslant n \leqslant k - 1) \tag{1.39}$$

$$Q_n = Q_{k-n} (1 \leqslant n \leqslant k - 1) \tag{1.40}$$

$$P_n = P_{k+1-n} (1 \leqslant n \leqslant k - 1) \tag{1.41}$$

$$a_k = \begin{cases} 2a_0, & \text{当 } b = 0 \text{ 时} \\ 2a_0 - 1, & \text{当 } b = a \text{ 时} \\ 2a_0 + 1, & \text{当 } b = -a \text{ 时} \end{cases} \tag{1.42}$$

并且有:

(1) 如 $P_l = P_{l+1}$ 对某个满足 $1 \leqslant l < l + 1 \leqslant k$ 的 l 成立,则有 $k = 2l$;

(2) 如 $Q_{l-1} = Q_{l+1}$ 对某个满足 $1 \leqslant l - 1 < l + 1 \leqslant k - 1$ 的 l 成立,则有 $k = 2l$;

$f(x,y) = ax^2 + bxy + cy^2$

(3) 如 $Q_l = Q_{l+1}$ 对某个满足 $1 \leqslant l < l+1 \leqslant k-1$ 的 l 成立,则有 $k = 2l+1$.

证明 由式(1.38)及其之前的计算,即得式(1.42). 又有 $Q_k = Q_0, P_{k+1} = P_1$,故由

$$P_k = 2a_k Q_k - P_{k+1} = 2a_k Q_0 - P_1$$

结合式(1.42)分别计算之,即得

$$P_k = P_1$$

于是

$$Q_{k-1} = \frac{d - P_k^2}{4Q_k} = \frac{d - P_1^2}{4Q_0} = Q_1$$

$$a_{k-1} = \left[\frac{2Q_k}{\sqrt{d} - P_k}\right] = \left[\frac{2Q_0}{\sqrt{d} - P_1}\right] = \left[\frac{\sqrt{d} + P_1}{2Q_1}\right] = a_1$$

$$P_{k-1} = 2a_{k-1}Q_{k-1} - P_k = 2a_1 Q_1 - P_1 = P_2$$

如此继续做下去,即得式(1.39) ~ (1.41).

最后三个断言也容易证明. 引理证毕.

附记 这个引理可使在计算 $\alpha = \dfrac{b + \sqrt{d}}{2a}$ 的简单连分数展开式时减少工作量,如果 $a \mid b$ 这一条件成立的话.

引理 1.4 如 $b = 0, a = 1$ 或 $b = a = 1$,则有

$$Q_n \geqslant 2(1 \leqslant n \leqslant k-1), Q_k = Q_0 = 1 \tag{1.43}$$

$$1 \leqslant a_n \leqslant a_0 (1 \leqslant n \leqslant k-1) \tag{1.44}$$

证明 $Q_k = Q_0 = 1$,即式(1.43)的后一式显然成立. 如有 n 满足 $1 \leqslant n \leqslant k-1$,使 $Q_n = 1$,则

$$\alpha_n = \frac{P_n + \sqrt{d}}{2} = \frac{P_n - b}{2} + \alpha$$

又由式(1.18)知 P_n 与 b 同奇偶. 这样,得出

$$\alpha = [a_0, a_1, \cdots, a_{n-1}, \alpha_n] = \left[a_0, a_1, \cdots, a_{n-1}, \overline{\frac{P_n - b}{2} + a_0}\right]$$

这与 k 的定义矛盾. 这样完全证明了式(1.43).

式(1.44)的左端是显然的,至于右端,由式(1.43)即知,对 $1 \leqslant n \leqslant k-1$ 有

$$a_n = \frac{P_n + P_{n+1}}{2Q_n} \leqslant \frac{2[\sqrt{d}]}{4} = \frac{[\sqrt{d}]}{2}$$

故

$$a_n \leqslant \left[\frac{[d]}{2}\right] \leqslant \left[\frac{b + [d]}{2}\right] \leqslant \left[\frac{b + [d]}{2}\right] = a_0$$

引理证毕.

引理1.5 设a,b,c,d仍如上所述,而且$\alpha=\dfrac{b+\sqrt{d}}{2a}$的简单连分数展开式为

$$\alpha=[a_0,\overline{a_1,a_2,\cdots,a_{k-1},a_k}]$$

其中$\overline{a_1,a_2,\cdots,a_{k-1},a_k}$为基本周期.

再令α的第n个完全商为

$$\alpha_n=[a_n,a_{n+1},\cdots]=\frac{P_n+\sqrt{d}}{2Q_n}\quad(n\geqslant 0)$$

则$\beta=-\alpha'=\dfrac{-b+\sqrt{d}}{2a}$的简单连分数展开式为

$$\beta=[a_k-a_0,\overline{a_{k-1},a_{k-2},\cdots,a_2,a_1,a_k}]$$

其中$\overline{a_{k-1},a_{k-2},\cdots,a_2,a_1,a_k}$为基本周期,而且$\beta$的第$n$个完全商

$$\beta_n=\frac{P_{k+1-n}+\sqrt{d}}{2Q_{k-n}}\quad(1\leqslant n\leqslant k)$$

证明 不妨设$b\geqslant 0$(否则可对调α与β). 这样有$a_0\geqslant 1,a_k\geqslant 2a_0-1\geqslant a_0$,即有$a_k-a_0\geqslant 0$. 用引理1.1以及引理1.3之前的计算,我们有

$$\begin{aligned}
\beta&=\frac{-b+\sqrt{d}}{2a}=a_k-a_0+\frac{\sqrt{d}-b-2a(a_k-a_0)}{2a}\\
&=a_k-a_0\frac{\sqrt{d}+P_1-2a_ka}{2a}\\
&=a_k-a_0\frac{\sqrt{d}+P_{k+1}-2a_kQ_k}{2Q_k}\\
&=a_k-a_0\frac{\sqrt{d}-P_k}{2Q_k}\\
&=\left[a_k-a_0,\frac{2Q_k}{\sqrt{d}-P_k}\right]=\left[a_k-a_0,\frac{\sqrt{d}+P_k}{2Q_{k-1}}\right]\\
&=\left[a_k-a_0,a_{k-1}+\frac{\sqrt{d}-P_{k-1}}{2Q_{k-1}}\right]\\
&=\left[a_k-a_0,a_{k-1}+\frac{2Q_{k-1}}{\sqrt{d}-P_{k-1}}\right]=\\
&\vdots\\
&=\left[a_k-a_0,a_{k-1},a_{k-2},\cdots,a_{n+1},a_n,\frac{2Q_n}{\sqrt{d}-P_n}\right]=\quad(1\leqslant n\leqslant k-1)\\
&\vdots
\end{aligned}$$

$f(x,y)=ax^2+bxy+cy^2$