The Application of Indeterminate Equation

中国数论名家著作选系列

"十三五"国家重点图书

不定方程及其应用

曹珍富 著

非外借

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

中国数论名家著作选系列

"十三五"国家重点图书

不定方程及其应用

The Application of Indeterminate Equation

曹珍富 著

HITP
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书主要介绍著者在不定方程、代数数论、组合设计、整图和有限单群的精细刻画方面的应用的研究成果. 全书共分 8 章:佩尔方程与广义佩尔方程,一些三次与四次不定方程,二次域与不定方程,一些高次不定方程,一些指数不定方程,不定方程对组合设计的应用,用佩尔方程的解构造整图,用不定方程的方法确定单 K_n-群.

本书可作为大专院校理工科高年级学生或研究生的教材,也可作为科技工作者的参考书.

图书在版编目(CIP)数据

不定方程及其应用/曹珍富著. —哈尔滨:哈尔滨工业大学出版社,2019.1

ISBN 978-7-5603-7726-1

Ⅰ.①不… Ⅱ.①曹… Ⅲ.①不定方程 Ⅳ.①O122.2

中国版本图书馆 CIP 数据核字(2018)第 243513 号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 陈雅君
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 哈尔滨市工大节能印刷厂
开 本 787mm×1092mm 1/16 印张 14.75 字数 314 千字
版 次 2019 年 1 月第 1 版 2019 年 1 月第 1 次印刷
书 号 ISBN 978-7-5603-7726-1
定 价 58.00 元

◎前言

不定方程又称为丢番图(Diophantus)方程,是数论的重要分支学科,是历史上最活跃的数学领域之一.1969年,“不定方程之王”莫德尔(L. J. Mordell)系统地总结了当时的成果,写成了著名的《丢番图方程》(*Diophantine Equations*).1980年,著名数学家柯召和孙琦在我国出版了第一部专门研究不定方程的专著《谈谈不定方程》(上海教育出版社).在这两部专著的基础上,作者于1987年完成了全面总结与系统研究不定方程的成果和方法的手稿《丢番图方程引论》,并于1989年由哈尔滨工业大学出版社出版.

近年来,不仅不定方程自身的发展异常活跃,而且全面应用于离散数学的其他各个领域,例如,不定方程在代数数论(二次域类数)、组合设计、整图和有限单群等领域均有应用.这方面的文献资料之多是任何其他数学分支所不能比拟的.鉴于这种情况,为了本书内容的完整性和相关性,在以不定方程作为主线的前提下,将不定方程以及不定方程在离散数学及其他领域的应用有机地结合起来.大量相关文献的出处被加在每章的末尾.

全书共分8章.简介如下:

第1章介绍佩尔(Pell)方程和广义佩尔方程的结果与方法,这在后面各章均有应用.

第2章介绍一些三次与四次不定方程的结果与问题,它们均是近些年的研究成果.其中佩尔方程与佩尔序列的雅可比(Jacobi)符号是基本的工具.

第3章建立了二次域与不定方程的一些关联定理，并用这些定理分别研究了一类虚、实二次域类数的可除性. 这是不定方程的一个重要的应用方面. 这一章的结果与方法是基本的，对于后面的高次与指数不定方程的研究具有重要作用.

第4章研究了一些重要的高次不定方程的解，包括方程 $Ax^2+B=y^n$，$Ax^2+1=By^n$，$x^4\pm y^4=z^p$，$x^p+2^{2m}=py^2$，$x^m-y^n=1$ 和 $\frac{x^m-1}{x-1}=y^q$ 等，及其研究进展，其中指数作为未定元时，这些高次不定方程也可以看成是指数不定方程.

第5章对与 S－单位方程有关的问题做了较为深入的研究，包括不定方程 $Ax^2+By^2=\lambda p^z$，$a^x+b^y=c^z$ 及 Terai-Jesmanowicz 猜想，$x^2+b^y=c^z$ 及有关猜想，有限单群与差集中的某些指数不定方程.

第6章介绍了不定方程的成果对组合设计的一些应用，主要包括四平方和定理与BRC定理的发现，勒让德(Legendre)方程的结果在证明 (v,k,λ)－组态不存在性时的应用，一些指数与高次不定方程在证明有Stanton-Sprott 差集与Storer 差集的循环性中的应用等.

第7章是用佩尔方程的解，构造直径3，4，5，6的若干类整树，这些结果完全解决了 Capobianca，Maurer，McCarthy 和 Molluzzo 的整树问题. 同时，我们还提出了若干新的整树问题有待于进一步研究.

第8章是用不定方程的方法确定单 K_n－群，包括 $3\leqslant n\leqslant 5$ 的结果，以及阶含有一个或两个任意素数幂的单 K_n－群. 同时，讨论了单 K_n－群的个数问题.

在本书定稿之时，作者由衷地感谢中国科学院王元院士与四川大学孙琦教授，他们都是作者的业师，多年来作者得到过他们的热情帮助与指教. 作者还要由衷地感谢上海交通大学沈灏教授，本书初稿完成后，曾得到过他认真的审阅并提出宝贵的修改意见，他的真诚友谊与无私帮助，作者将铭记于心. 同时，作者还要感谢在研究工作中的合作者：波兰的 A. Grytczuk 教授，法国的 Y. Bugeaud 博士和M. Mignotte 教授等，他们提供了一些有价值的文献资料. 最后，还要感谢我的妻子董晓蕾女士，本书的写作自始至终得到了她的帮助与支持.

希望本书的出版会有助于不定方程及其应用领域的进一步研究. 当然，限于作者的能力，本书难免会出现谬误和遗漏，恳望读者批评指正！

常用符号表

（按书中出现的先后顺序排列）

$\mathbf{Z},\mathbf{N},\mathbf{Q},\mathbf{P}$	分别表示整数、正整数[①]、有理数和素数的集合
$\mathbf{P}^{\mathbf{N}}$	素数幂的集合，即 $\mathbf{P}^{\mathbf{N}}=\{p^n \mid p\in\mathbf{P}$ 且 $n\in\mathbf{N}\}$
$\left(\frac{b}{a}\right)$	勒让德－雅可比符号
$a \mid^* b$	a 星整除整数 b，即 a 的每个素因子整除 b
$\gcd(a,b)$	整数 a,b 的最大公约数（当 a,b 是代数整数或理想数时，$\gcd(a,b)$ 仍表示 a,b 的最大公约数）
$\binom{n}{k}$	n 个对象中取 k 个的取法个数，即 $\binom{n}{k}=\frac{n!}{(n-k)!\ k!}$
A^n	n 个集合 A 的笛卡儿积，即 $A^n=\underbrace{A\times\cdots\times A}_{n\text{个}}=\{(a_1,\cdots,a_n) \mid a_i\in A(i=1,\cdots,n)\}$
$\log x$	x 的自然对数
$\mathbf{N}_0$	非负整数的集合，即 $\mathbf{N}_0=\mathbf{N}\cup\{0\}$
$a\equiv b(\bmod m)$	整数 a,b 对模 m 同余
$a\not\equiv b(\bmod m)$	整数 a,b 对模 m 不同余
$a \mid b$	整数 a 整除整数 b
$a\nmid b$	整数 a 不整除整数 b
$p^k \parallel b$	素数 p 的 k 次幂恰整除整数 b，即 $p^k \mid b$ 且 $p^{k+1}\nmid b$
$\mid A \mid$	集合 A 的元素个数
$a\in A$	a 是集合 A 的元素
$a\notin A$	a 不是集合 A 的元素
$\omega(a)$	整数 a 的不同素因子的个数

① 本书成书较早，书中正整数为当时定义的说法.

$\{F_n\},\{Q_n\}$	斐波那契－鲁卡斯序列
$\mathbf{Q}(\sqrt{D})$	二次域，即 $\mathbf{Q}(\sqrt{D})=\{a+b\sqrt{D} \mid a,b\in\mathbf{Q}\}$，这里 $\mid D\mid$ 不是平方数
$h(D)$	二次域 $\mathbf{Q}(\sqrt{D})$ 的类数，即该二次域的理想类群的阶
O_K	表示代数数域 K 的整元环
$[\alpha_1,\cdots,\alpha_m]$	$\alpha_1,\cdots,\alpha_m\in O_K$ 生成的理想数，即 $[\alpha_1,\cdots,\alpha_m]=\{\eta_1\alpha_1+\cdots+\eta_m\alpha_m \mid \eta_i\in O_K(i=1,\cdots,m)\}$
$[\alpha]$	$\alpha\in O_K$ 生成的主理想数，即 $[\alpha]=\{\eta\alpha \mid \eta\in O_K(i=1,\cdots,m)\}$
$\chi(k)$	$K(=\mathbf{Q}(\sqrt{D}))$ 的实特征
$I\sim J$	理想数 I 与 J 等价
$\exp x$	指数函数 e^x
$\mid a\mid$	实数 a 的绝对值
$\{u_n\}$	鲁卡斯序列，即 $u_n=\dfrac{\alpha^n-\beta^n}{\alpha-\beta}$，$\alpha,\beta$ 为方程 $x^2-Px+Q=0$ 的两个根，$P,Q\in\mathbf{Z}$ 适合 $\gcd(P,Q)=1$
$[a_0,\overline{a_1,\cdots,a_s}]$	周期为 s 的简单连分数
$[x]$ 或 $\lfloor x\rfloor$	高斯函数，表示不超过 x 的最大整数
B_n	第 n 个伯努利数
v_p	p-adic 赋值，$p\in\mathbf{P}$
$\max\{a,b,\cdots\}$	$a,b,\cdots$ 中最大者
$\begin{bmatrix}n\\k\end{bmatrix}$	表示形如 $\dfrac{(n-k-1)!\ n}{(n-2k)!\ k!}\left(0\leqslant k\leqslant\left[\dfrac{n}{2}\right]\right)$ 的自然数
$[a_{ij}]_{i,j\in\{1,\cdots,v\}}$	(v,k,λ)－组态的关联矩阵，其中 $a_{ij}=\begin{cases}1 & (\text{当 } a_j\in V_i \text{ 时})\\ 0 & (\text{否则})\end{cases}$
$\det\boldsymbol{A}$ 或 $\mid\boldsymbol{A}\mid$	矩阵 $\boldsymbol{A}$ 的行列式
$\mathbf{F}_{p^a}$	p^a 元的有限域，这里 $p\in\mathbf{P},a\in\mathbf{N}$
$\mathbf{F}_{p^a}^*$	$\mathbf{F}_{p^a}$ 的乘群，即 $\mathbf{F}_{p^a}^*=\mathbf{F}_{p^a}\setminus\{0\}$
C_i^e	第 i 个 e 次分圆类

$(i,j)_e$	e 阶分圆数
$\mathbf{F}_{p^a} \times \mathbf{F}_{p^b}$	$\mathbf{F}_{p^a}$ 与 $\mathbf{F}_{p^b}$ 的笛卡儿积
$K_{1,m}$	星图
$T(m,r)$	用一条新边联结两个星图 $K_{1,m}$，$K_{1,r}$ 的中心得到的图
$S(r,m)$	联结 r 个星图 $K_{1,m}$ 的中心到一个新顶点得到的图
$S(m_1,\cdots,m_r)$	联结 r 个星图 $K_{1,m_1},\cdots,K_{1,m_r}$ 的中心到一个新顶点得到的图
$H(t,m)$	$K_{1,m}$ 的每个顶点各联结 t 个新顶点得到的图
$T_t(m,r)$	$T(m,r)$ 的每个顶点各联结 t 个新顶点得到的图
$L(r,m,t)$	联结 t 个 $S(r,m)$ 的中心到一个新顶点得到的图
$P(G)$	图 G 的特征多项式
$\pi(G)$	群 G 的阶中所有不同素因子的集合
$G_1 \cong G_2$	群 G_1，G_2 同构

目录

佩尔方程与广义佩尔方程

第 1 章

从本章开始，分别用 **Z**，**N**，**Q** 和 **P** 表示整数、正整数、有理数和素数的集合.

通常佩尔方程是指下面四个不定方程

$$x^2 - Dy^2 = \pm 1, \pm 4 \quad (x, y \in \mathbf{Z}) \qquad ①$$

它们的解结构已是数论中的经典结果. 广义佩尔方程是指佩尔方程 ① 的推广，有以下两种基本类型

$$ax^2 - by^2 = \pm 1, \pm 2, \pm 4 \quad (x, y \in \mathbf{Z}) \qquad ②$$

和

$$x^2 - Dy^2 = M \quad (x, y \in \mathbf{Z}) \qquad ③$$

我们统一将方程 ①② 和 ③ 称为佩尔类方程.

众所周知，方程 ① 的解可由其基本解生成，但方程 ① 的基本解是极其不规律的，确定方程 ① 的基本解(或范围) 已成为解析数论(研究基本解的上界) 与代数数论(研究实二次域高斯(Gauss) 类数问题) 的共同课题. 本章通过对方程 ① 的介绍，揭示方程 ① 的基本解的一些基本特征. 特别是建立方程 ② 的基本解与方程 ① 的基本解的联系，从而通过方程 ② 的基本解求出方程 ① 的基本解. 最后给出方程 ③ 的解的结构.

本章的结果对后面各章也是基本的.

1.1 佩尔方程

本节的结果是经典的，一般不加证明，读者可在文献[1] 中找到它们的证明，其中部分结果的证明还可参看文献[8][9]，

而且文献[8]中给出了另一种证明方法——连分数法.

设 $D \in \mathbf{N}$ 不是完全平方数(简称不是平方数),将如下的四个不定方程

$$x^2 - Dy^2 = \pm 1, \pm 4 \quad (x, y \in \mathbf{Z})$$

统称为佩尔方程.熟知,佩尔方程

$$x^2 - Dy^2 = 1 \quad (x, y \in \mathbf{Z}) \tag{1.1.1}$$

总有正整数解.设(x_1, y_1)是方程(1.1.1)所有正整数解(x, y)中使$x + y\sqrt{D}$为最小的一组解,称(x_1, y_1)为佩尔方程(1.1.1)的最小解,或称$x_1 + y_1\sqrt{D}$为佩尔方程(1.1.1)的基本解.设(x, y)为方程(1.1.1)的一组解,有时也说$x + y\sqrt{D}$是方程(1.1.1)的一组解.以后所说的佩尔方程$x^2 - Dy^2 = M$的解与解的结合类中的基本解均如此定义.

定理 1.1.1 设$x_1 + y_1\sqrt{D}$为佩尔方程(1.1.1)的基本解,则方程(1.1.1)的全部解可表示为

$$x + y\sqrt{D} = \pm(x_1 + y_1\sqrt{D})^n \quad (n \in \mathbf{Z}) \tag{1.1.2}$$

显然,如果令

$$\varepsilon_1 = x_1 + y_1\sqrt{D}, \bar{\varepsilon}_1 = x_1 - y_1\sqrt{D}$$

则由式(1.1.2)得

$$x = \pm\frac{\varepsilon_1^n + \bar{\varepsilon}_1^n}{2}, y = \pm\frac{\varepsilon_1^n - \bar{\varepsilon}_1^n}{2\sqrt{D}} \quad (n \in \mathbf{Z})$$

并且方程(1.1.1)的正整数解为

$$x = \frac{\varepsilon_1^n + \bar{\varepsilon}_1^n}{2}, y = \frac{\varepsilon_1^n - \bar{\varepsilon}_1^n}{2\sqrt{D}} \quad (n \in \mathbf{N})$$

对于佩尔方程

$$x^2 - Dy^2 = -1 \quad (x, y \in \mathbf{Z}) \tag{1.1.3}$$

当D含有$4k+3$型素因子或$D \equiv 0 \pmod 4$时,方程(1.1.3)显然无解.但是,如果方程(1.1.3)有解,那么必有无穷多组解.设$\varepsilon_2 = x_1 + y_1\sqrt{D}$为方程(1.1.3)的基本解,则有:

定理 1.1.2 设方程(1.1.3)有解,$\varepsilon_1, \varepsilon_2$分别为方程(1.1.1)与方程(1.1.3)的基本解,则$\varepsilon_1 = \varepsilon_2^2$,且方程(1.1.3)的全部解可表示为

$$x + y\sqrt{D} = \pm\varepsilon_2^{2n+1} \quad (n \in \mathbf{Z}) \tag{1.1.4}$$

讨论方程(1.1.3)何时有解、何时无解是一件有意义的事情.对此,我们有:

定理 1.1.3 设$D = 2p_1 \cdots p_s, p_i (i = 1, \cdots, s)$是不同的奇素数,$p_i \equiv 5 \pmod 8 (i = 1, \cdots, s)$,且当$s > 2$时对任意的$i \neq j (1 \leqslant i, j \leqslant s)$都有勒让德-雅可比(Legendre-Jacobi)符号$\left(\frac{p_j}{p_i}\right) = 1$,则方程(1.1.3)有解.

证明　设 $x_1+y_1\sqrt{D}$ 是方程(1.1.1)的基本解,则有

$$x_1^2-Dy_1^2=1$$

由此易得 $2\mid y_1$,且有

$$\left(\frac{x_1+1}{2}\right)\left(\frac{x_1-1}{2}\right)=D\left(\frac{y_1}{2}\right)^2$$

故得出

$$\frac{x_1+1}{2}=D_1u^2,\frac{x_1-1}{2}=D_2v^2,y_1=2uv \tag{1.1.5}$$

这里 $u,v\in\mathbf{N}$ 且 $\gcd(u,v)=1,D=D_1D_2$. 由式(1.1.5)得

$$D_1u^2-D_2v^2=1 \tag{1.1.6}$$

显然,如果证明了方程(1.1.6)中 $D_2=1,D_1=D$,那么证明了方程(1.1.3)有解. 为此,设 $D_2>1$,如果 $D_1=1$,那么 $u+v\sqrt{D}$ 是方程(1.1.1)的一个解,但

$$u+v\sqrt{D}<x_1+y_1\sqrt{D}$$

与 $x_1+y_1\sqrt{D}$ 是方程(1.1.1)的基本解矛盾,所以 $D_1>1$. 当 D_1 或 $D_2=2$ 时,对方程(1.1.6)取模 p_1,得

$$1=\left(\frac{\pm2}{p_1}\right)=\left(\frac{2}{p_1}\right)=-1$$

矛盾. 当 $D_1>2,D_2>2$ 时,如 $s=2$,则不妨设 D_1 为 $2p_1$,D_2 为 p_2,则方程(1.1.6)给出

$$\left(\frac{2p_1}{p_2}\right)=\left(\frac{p_2}{p_1}\right)=1$$

但 $p_1\equiv p_2\equiv5(\mathrm{mod}\ 8)$,故

$$\left(\frac{2p_1}{p_2}\right)=-\left(\frac{p_1}{p_2}\right)=-1$$

矛盾;如 $s>2$,设 $2\mid D_1$(或 $2\mid D_2$),则任取 D_2(或 D_1)的某个素因子 $p_i(1\leqslant i\leqslant s)$,对方程(1.1.6)取模 p_i,得

$$1=\left(\frac{D_1}{p_i}\right)=\left(\frac{2}{p_i}\right)=-1\quad\left(\text{或 }1=\left(\frac{-D_2}{p_i}\right)=\left(\frac{2}{p_i}\right)=-1\right)$$

仍是矛盾. 这就证明了当 $D_2>1$ 时方程(1.1.6)不成立. 于是 $D_2=1$,给出方程(1.1.3)有解. 证毕.

同样的方法可以证明以下定理.

定理 1.1.4　设 $D=p_1\cdots p_s,p_i(i=1,\cdots,s)$ 是不同的素数且 $p_i\equiv1(\mathrm{mod}\ 4)(i=1,\cdots,s)$. 若 $s=2$ 或 $2\nmid s$,且在 $s>1$ 时,对任意 $i\neq j(1\leqslant i,j\leqslant s)$ 都有 $\left(\frac{p_j}{p_i}\right)=-1$,则方程(1.1.3)有解.

对于 $D=2p,p\equiv1(\mathrm{mod}\ 4)$ 为素数,当 $p\equiv5(\mathrm{mod}\ 8)$ 时,由定理1.1.3知,

方程(1.1.3)有解. 当 $p\equiv 1(\bmod 8)$ 时,方程(1.1.3)是否有解呢? 对此,有如下定理:

定理 1.1.5(Lienen[11]) 设 $D=2p, p\equiv 1(\bmod 8)$ 为素数,如果

$$2p=r^2+s^2, r\equiv\pm 3(\bmod 8), s\equiv\pm 3(\bmod 8)$$

那么方程(1.1.3)无解.

这个结果不难用高斯整数的性质给出一个简短的证明(参看[1],第 160 ~ 161 页).

对于佩尔方程

$$x^2-Dy^2=4 \quad (x,y\in \mathbf{Z}) \tag{1.1.7}$$

与

$$x^2-Dy^2=-4 \quad (x,y\in \mathbf{Z}) \tag{1.1.8}$$

分别设 $\varepsilon_3,\varepsilon_4$ 为方程(1.1.7)和方程(1.1.8)的基本解(假设方程(1.1.8)有解),则有:

定理 1.1.6 方程(1.1.7)总有 $y\neq 0$ 的解. 设 ε_1 为方程(1.1.1)的基本解,则

$$\varepsilon_1=\begin{cases}\dfrac{\varepsilon_3}{2} & (\text{当 } \gcd(x,y)=2 \text{ 时})\\ \left(\dfrac{\varepsilon_3}{2}\right)^3 & (\text{当 } \gcd(x,y)=1 \text{ 时})\end{cases}$$

且方程(1.1.7)的全部解可表示为

$$\frac{x+y\sqrt{D}}{2}=\pm\left(\frac{\varepsilon_3}{2}\right)^n \quad (n\in \mathbf{Z})$$

定理 1.1.7 如果方程(1.1.8)有解,那么有

$$\varepsilon_2=\begin{cases}\dfrac{\varepsilon_4}{2} & (\text{当 } \gcd(x,y)=2 \text{ 时})\\ \left(\dfrac{\varepsilon_4}{2}\right)^3 & (\text{当 } \gcd(x,y)=1 \text{ 时})\end{cases}$$

且方程(1.1.8)的全部解可表示为

$$\frac{x+y\sqrt{D}}{2}=\pm\left(\frac{\varepsilon_4}{2}\right)^{2n+1} \quad (n\in \mathbf{Z})$$

对于方程

$$x^2-Dy^2=\pm 2 \quad (x,y\in \mathbf{Z}) \tag{1.1.9}$$

如果它们有解,可设 $\lambda_\pm$ 为方程(1.1.9)的基本解(即 λ_+ 与 λ_- 分别是对应方程(1.1.9)右端取 $+2$ 与 -2 的基本解).

定理 1.1.8 如果方程(1.1.9)有解,那么除 $x^2-2y^2=-2$ 外,必有 $\varepsilon_1=\dfrac{\lambda_\pm^2}{2}$,且方程(1.1.9)的全部解可表示为

$$x+y\sqrt{D}=\pm\frac{\lambda_{\pm}^{2n+1}}{2^n}\quad(n\in\mathbf{Z})$$

定理 1.1.6 ～ 定理 1.1.8 均可由广义佩尔方程 $x^2-Dy^2=M$ 的结论推出.

1.2 佩尔方程的基本解

佩尔方程的基本解在研究二次域的类数中起关键性作用(参阅 3.1 节和 3.3.2 小节). 但基本解常常是不规律的,例如,$x^2-1\,141y^2=1$,当 $1\leqslant y\leqslant 10^{25}$ 时都无解. 这里,我们只研究一些基本的情况:一是对一些特殊类型的 D,给出佩尔方程的基本解;二是应用广义佩尔方程的结果求佩尔方程的基本解.

定理 1.2.1 设 x_1,y_1 是佩尔方程

$$x^2-Dy^2=1\quad(x,y\in\mathbf{N})\tag{1.2.1}$$

的一组解,且满足 $x_1>\frac{1}{2}y_1^2-1$,则 $x_1+y_1\sqrt{D}$ 是方程(1.2.1) 的基本解.

定理 1.2.2 设 x_1,y_1 是佩尔方程

$$x^2-Dy^2=4\quad(x,y\in\mathbf{N})\tag{1.2.2}$$

的一组解,且满足 $x_1>y_1^2-2$,则 $x_1+y_1\sqrt{D}$ 是方程(1.2.2) 的基本解.

这两个定理的证明是类似的,这里只给出定理 1.2.2 的证明.

证明 如果 $y_1=1$,那么 $x_1+y_1\sqrt{D}$ 显然是方程(1.2.2) 的基本解. 现设 $y_1>1$,如果 $x_1+y_1\sqrt{D}$ 不是方程(1.2.2) 的基本解,那么可令 $x_0+y_0\sqrt{D}$ 是方程(1.2.2) 的基本解,$1\leqslant y_0<y_1$,于是

$$\begin{aligned}x_0^2y_1^2-y_0^2x_1^2&=y_1^2(4+Dy_0^2)-y_0^2x_1^2\\&=4y_1^2-y_0^2(x_1^2-Dy_1^2)\\&=4(y_1^2-y_0^2)>0\end{aligned}$$

令 $x_0y_1+y_0x_1=2\xi,x_0y_1-y_0x_1=2\eta$,则 $\xi\eta=y_1^2-y_0^2,\xi,\eta\in\mathbf{N}$. 所以

$$x_1=\frac{\xi-\eta}{y_0}\leqslant\frac{y_1^2-y_0^2-1}{y_0}=\frac{1}{y_0}\cdot y_1^2-\left(y_0+\frac{1}{y_0}\right)\leqslant y_1^2-2$$

与 $x_1>y_1^2-2$ 矛盾. 这就证明了 $x_1+y_1\sqrt{D}$ 是方程(1.2.2) 的基本解. 证毕.

由定理 1.2.1 和定理 1.2.2 立即得出:

推论 1.2.1 设佩尔方程(1.2.1) 与方程(1.2.2) 的基本解分别为 ε_1 与 ε_3,则有:

(1) 如果 $D=s(st^2+2\delta),s,t\in\mathbf{N},\delta\in\{-1,1\}$ 且当 $\delta=-1$ 时,$st^2>2$,那么

$$\varepsilon_1=st^2+\delta+t\sqrt{D}$$

(2) 如果 $D=s(st^2+\delta)$, $s,t\in\mathbf{N}$, $\delta\in\{-1,1\}$ 且当 $\delta=-1$ 时, $st^2>1$, 那么

$$\varepsilon_1=2st^2+\delta+2t\sqrt{D}$$

(3) 如果 $D=s(st^2+4\delta)$, $s,t\in\mathbf{N}$, $\delta\in\{-1,1\}$ 且当 $\delta=-1$ 时, $st^2>4$, 那么

$$\varepsilon_3=st^2+2\delta+t\sqrt{D}$$

推论 1.2.1 中得到的基本解对决定实二次域的类数起决定作用(参看文献[12]). 同时, 对一类高次不定方程的求解也起重要作用(参看 4.1 节).

设 $a,b\in\mathbf{N}$, $a\mid^* b$ 表示 a 的每个素因子(如果存在的话)整除 b, 读为 a 星整除 b. 例如 $1\mid^* b$, $2^{10}\mid^* 14$ 等.

定理 1.2.3(斯托默(Störmer)[15]) 设 x_1,y_1 是佩尔方程(1.2.1)的一组解, 且满足 $y_1\mid^* D$, 则 $x_1+y_1\sqrt{D}$ 是方程(1.2.1)的基本解.

证明 用反证法. 假设 $x_1+y_1\sqrt{D}$ 不是方程(1.2.1)的基本解, 而设方程(1.2.1)的基本解为 $\varepsilon_1=x_0+y_0\sqrt{D}$, 则由定理 1.1.1 知

$$x_1+y_1\sqrt{D}=\varepsilon_1^n=(x_0+y_0\sqrt{D})^n\quad(1<n\in\mathbf{N})$$

于是

$$x_1=\frac{\varepsilon_1^n+\bar{\varepsilon}_1^n}{2},y_1=\frac{\varepsilon_1^n-\bar{\varepsilon}_1^n}{2\sqrt{D}}\quad(1<n\in\mathbf{N})$$

这里 $\bar{\varepsilon}_1=x_0-y_0\sqrt{D}$. 如果 $2\mid n$, 那么

$$y_1=2\cdot\frac{\varepsilon_1^{\frac{n}{2}}+\bar{\varepsilon}_1^{\frac{n}{2}}}{2}\cdot\frac{\varepsilon_1^{\frac{n}{2}}-\bar{\varepsilon}_1^{\frac{n}{2}}}{2\sqrt{D}}$$

因为 $y_1\mid^* D$, 所以上式给出 $\dfrac{\varepsilon_1^{\frac{n}{2}}+\bar{\varepsilon}_1^{\frac{n}{2}}}{2}\mid^* D$. 又

$$\left(\frac{\varepsilon_1^{\frac{n}{2}}+\bar{\varepsilon}_1^{\frac{n}{2}}}{2}\right)^2-D\left(\frac{\varepsilon_1^{\frac{n}{2}}-\bar{\varepsilon}_1^{\frac{n}{2}}}{2\sqrt{D}}\right)=1$$

故 $\dfrac{\varepsilon_1^{\frac{n}{2}}+\bar{\varepsilon}_1^{\frac{n}{2}}}{2}=1$, 因而 $n=0$, 与 $n>1$ 矛盾.

如果 $2\nmid n$, 因为 $n>1$, 所以可设 p 是 n 的任一奇素数因子. 记 $n=pn_1$, $n_1\in\mathbf{N}$

$$\varepsilon_1^{n_1}=a+b\sqrt{D},\bar{\varepsilon}_1^{n_1}=a-b\sqrt{D}$$

这里 $a,b\in\mathbf{N}$ 且满足

$$a^2-Db^2=1\tag{1.2.3}$$

于是由