

上海“九五”重点图书

离散数学丛书

不定方程 及其应用

● 曹珍富 著

上海交通大学出版社

上海“九五”重点图书
离散数学丛书

不定方程及其应用

曹珍富 著

上海交通大学出版社

内 容 提 要

本书主要介绍著者在不定方程及其在代数数论、组合设计、整图和有限单群的精细刻画方面的应用的最新研究成果。全书共分八章: Pell 方程和广义 Pell 方程, 一些三次与四次不定方程, 二次域与不定方程, 一些重要的高次不定方程, 有关的指数不定方程, 不定方程对组合设计的应用, 用 Pell 方程的解构造整图, 用不定方程的方法确定单 K_n 群。

本书可作为大中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. —上海: 上海交通大学出版社, 2000
(离散数学丛书)
ISBN 7-313-02468-1

I. 不… II. 曹… III. 不定方程 IV. 0158

中国版本图书馆 CIP 数据核字(2000)第 35326 号

不定方程及其应用

曹珍富 著

上海交通大学出版社出版发行

(上海市番禺路 877 号 邮政编码 200030)

电话: 64071208 出版人: 张天蔚

常熟市印刷二厂印刷 全国新华书店经销

开本: 850mm × 1168mm 1/32 印张: 9 字数: 228 千字

2000 年 10 月第 1 版 2000 年 10 月第 1 次印刷

印数: 1 ~ 500

ISBN 7-313-02468-1/O·127 定价: 15.00 元

版权所有 侵权必究

前 言

不定方程又称为丢番图方程,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”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, Academic Press)。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。这本书的前几章作为哈尔滨工业大学研究生教材已使用十余年。

最近十余年来,不定方程不仅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的其他领域的应用有机地结合起来。大量的相关文献的出处被加在每章的末尾。

全书共分八章。简介如下:

第一章介绍 Pell 方程和广义 Pell 方程的结果与方法,这在后面各章均有应用。

第二章介绍一些三次与四次不定方程的结果与问题,它们均是近几年的最新研究成果。其中 Pell 方程与 Pell 序列的 Jacobi 符号是基本的工具。

第三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

2 前言

的一个重要的应用方面。这一章的结果与方法是基本的,对后面的高次与指数不定方程的研究是重要的。

第四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 $\frac{x^m - 1}{x - 1} = y^n$ 等及其最新的研究进展。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。

第五章对与 S-单位方程有关的问题作了较为深入的研究,包括不定方程 $Ax^2 + By^2 = \lambda p^z$, $a^x + b^y = c^z$ 及 Terai-Jesmanowicz 猜想, $x^2 + b^y = c^z$ 及有关的猜想,有限单群与差集中的某些指数不定方程。

第六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,Legendre 方程的结果在证明 (v, k, λ) 一组态不存在性时的应用,一些指数与高次不定方程在证明 Stanton-Sprott 差集与 Storer 差集的循环性中的应用等。

第七章是用 Pell 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。

第八章是用不定方程的方法确定单 K_n -群,包括 $3 \leq n \leq 5$ 的结果以及阶含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。

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!

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大沈灏教授,在 1996 年本书初稿完成后,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。

曹珍富

2000年1月于哈尔滨

常用符号表

(按书中出现的先后顺序排列)

$\mathbb{Z}, \mathbb{N}, \mathbb{Q}, \mathbb{P}$	分别表示整数、正整数、有理数和素数的集合
$\mathbb{P}^{\mathbb{N}}$	素数幂的集合, 即 $\mathbb{P}^{\mathbb{N}} = \{p^n \mid p \in \mathbb{P} \text{ 且 } n \in \mathbb{N}\}$
$\left(\frac{b}{a}\right)$	Legendre-Jacobi 符号
$a \mid^* b$	a 星整数 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 $A^n = \underbrace{A \times \cdots \times A}_n = \{(a_1, \cdots, a_n) \mid a_i \in A (i = 1, \cdots, n)\}$
$\log x$	x 的自然对数
\mathbb{N}_0	非负整数的集合, 即 $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
$a \equiv b \pmod{m}$	整数 a, b 对模 m 同余
$a \not\equiv b \pmod{m}$	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 $p^{k+1} \nmid b$

2 常用符号表

$ A $	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
$\{F_n\}, \{Q_n\}$	Fibonacci-Lucas 序列
$\mathbb{Q}(\sqrt{D})$	二次域, 即 $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$, 这里 $ D $ 不是平方数
$h(D)$	二次域 $\mathbb{Q}(\sqrt{D})$ 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
$[\alpha_1, \dots, \alpha_m]$	$\alpha_1, \dots, \alpha_m \in O_K$ 生成的理想数, 即 $[\alpha_1, \dots, \alpha_m] = \{\eta_1 \alpha_1 + \dots + \eta_m \alpha_m \mid \eta_i \in O_K (i=1, \dots, m)\}$
$[\alpha]$	$\alpha \in O_K$ 生成的主理想数, 即 $[\alpha] = \{\eta \alpha \mid \eta \in O_K (i=1, \dots, m)\}$
$\chi(k)$	$K (= \mathbb{Q}(\sqrt{D}))$ 的实特征
$I \sim J$	理想数 I 与 J 等价
$\exp x$	指数函数 e^x
$ a $	实数 a 的绝对值
$\{u_n\}$	Lucas 序列, 即 $u_n = (\alpha^n - \beta^n) / (\alpha - \beta)$, α, β 为方程 $x^2 - Px + Q = 0$ 的两个根, $P, Q \in \mathbb{Z}$ 适合 $\gcd(P, Q) = 1$
$[\overline{a_0, a_1, \dots, a_s}]$	周期为 s 的简单连分数
$[x]$ 或 $\lfloor x \rfloor$	Gauss 函数, 表示不超过 x 的最大整数
B_n	第 n 个 Bernoulli 数
v_p	p -adic 赋值, $p \in \mathbb{P}$
$\max\{a, b, \dots\}$	a, b, \dots 中最大者

$\begin{bmatrix} n \\ k \end{bmatrix}$	表示形如 $\frac{(n-k-1)!}{(n-2k)!} \frac{n}{k!}$ ($0 \leq k \leq [n/2]$) 的自然数
$[a_{ij}]_{i,j \in \{1, \dots, v\}}$	(v, k, λ) -组态的关联矩阵, 其中 $a_{ij} = \begin{cases} 1, & \text{当 } a_j \in V_i \text{ 时} \\ 0, & \text{否则} \end{cases}$
$\det \mathbf{A}$ 或 $ \mathbf{A} $	矩阵 \mathbf{A} 的行列式
\mathbb{F}_p^a	p^a 元的有限域, 这里 $p \in \mathbb{P}, a \in \mathbb{N}$
\mathbb{F}_p^*	\mathbb{F}_p^a 的乘群, 即 $\mathbb{F}_p^* = \mathbb{F}_p^a \setminus \{0\}$
C_i	第 i 个 e 次分圆类
$(i, j)_e$	e 阶分圆数
$\mathbb{F}_p^a \times \mathbb{F}_p^b$	\mathbb{F}_p^a 与 \mathbb{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
$S(m_1, \dots, m_r)$	联结 r 个星图 $K_{1,m_1}, \dots, K_{1,m_r}$ 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

第一章 Pell 方程与广义 Pell 方程	1
§ 1.1 Pell 方程	1
§ 1.2 Pell 方程的基本解	6
§ 1.3 广义 Pell 方程 $ax^2 - by^2 = c, c = 1, 2, 4$	16
§ 1.4 广义 Pell 方程 $x^2 - Dy^2 = M$	20
1.4.1 一般的二元二次不定方程	20
1.4.2 方程 $x^2 - Dy^2 = M$ 解的结构	22
§ 1.5 本章评注	26
参考文献	27
第二章 一些三次与四次不定方程	29
§ 2.1 不定方程 $x^3 + a^3 = Dy^2$	29
2.1.1 $a = \pm 1$ 的情形	29
2.1.2 $ a > 1$ 的情形	38
§ 2.2 不定方程 $ax^4 + bx^3 + cx^2 + dx + e = y^2$	49
2.2.1 不定方程 $D_1x^4 - D_2y^2 = \pm 1$	50
2.2.2 不定方程 $ax^4 + bx^3 + cx^2 + dx + e = y^2$	54
§ 2.3 本章评注	64
参考文献	65
第三章 二次域与不定方程	68
§ 3.1 有关的代数数论	68
3.1.1 一般事实	68
3.1.2 二次域, 理想类数与 K 群	71

§ 3.2 不定方程与类数的关联定理	75
3.2.1 关联定理:二元二次型表整数	75
3.2.2 关联定理对 Abel 猜想的一个应用	82
§ 3.3 二次域类数的可除性	85
3.3.1 一类虚二次域类数的可除性	85
3.3.2 一类实二次域类数的可除性	92
§ 3.4 本章评注	102
参考文献	103
第四章 一些高次不定方程	106
§ 4.1 一类高次不定方程的统一解	106
4.1.1 不定方程 $Ax^2 + B = y^n$	106
4.1.2 不定方程 $Ax^2 + 1 = By^n$	113
§ 4.2 两类高次不定方程	116
4.2.1 Ribet-Darmon 定理对广义 Fermat 大定理的一个应用	116
4.2.2 不定方程 $x^p + 2^{2m} = py^2$	121
§ 4.3 Catalan 方程和不定方程 $\frac{x^m - 1}{x - 1} = y^q$	124
4.3.1 柯召定理的简化证明	124
4.3.2 不定方程 $\frac{x^m - 1}{x - 1} = y^q$	128
§ 4.4 本章评注	137
参考文献	137
第五章 一些指数不定方程	142
§ 5.1 不定方程 $Ax^2 + By^2 = \lambda p^z$	142
§ 5.2 不定方程 $a^x + b^y = c^z$ 与 Terai-Jeśmanowicz 猜想	149
§ 5.3 不定方程 $x^2 + b^y = c^z$	158
§ 5.4 有限单群与差集中的一些指数不定方程	166
§ 5.5 本章评注	173

参考文献	173
第六章 不定方程对组合设计的一些应用	176
§ 6.1 (v, k, λ) -组态	176
6.1.1 四平方和定理与 BRC 定理	176
6.1.2 Legendre 方程与 (v, k, λ) -组态的 不存在性	182
§ 6.2 差集	186
6.2.1 Stanton-Sprott 差集与 Hall 问题	187
6.2.2 分圆数与差集	191
6.2.3 乘子 -1 的差集与 McFarland 猜想	195
§ 6.3 本章评注	197
参考文献	198
第七章 用 Pell 方程的解构造整图	201
§ 7.1 直径 3 的整树	201
§ 7.2 直径 4 的整树	206
§ 7.3 直径 5 的整树	216
§ 7.4 直径 6 的整树	222
§ 7.5 本章评注	227
参考文献	228
第八章 用不定方程的方法确定单 K_n-群	230
§ 8.1 有限单群的分类定理	230
§ 8.2 单 K_3 -群和单 K_4 -群	233
§ 8.3 阶只含一个任意素因子的单 K_n -群	240
§ 8.4 阶含两个任意素因子的单 K_n -群	244
§ 8.5 单 K_5 -群	256
§ 8.6 本章评注	268
参考文献	268

第一章 Pell 方程与广义 Pell 方程

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

通常 Pell 方程是指下面四个不定方程:

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

它们的解结构已是数论中的经典结果. 广义 Pell 方程是指 Pell 方程 $\textcircled{1}$ 的推广,有以下两种基本类型:

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

和

$$x^2 - Dy^2 = M (x, y \in \mathbb{Z}). \quad \textcircled{3}$$

我们统将方程 $\textcircled{1}, \textcircled{2}$ 和 $\textcircled{3}$ 称为 Pell 类方程.

众所周知, $\textcircled{1}$ 的解可由其基本解生成,但 $\textcircled{1}$ 的基本解是极其不规律的,确定 $\textcircled{1}$ 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 Gauss 类数问题)的共同课题. 本章通过对方程 $\textcircled{1}$ 的介绍,揭示 $\textcircled{1}$ 的基本解的一些基本特征. 特别是建立 $\textcircled{2}$ 的基本解与 $\textcircled{1}$ 的基本解的联系,从而通过 $\textcircled{2}$ 的基本解求出 $\textcircled{1}$ 的基本解. 最后给出 $\textcircled{3}$ 的解的结构.

本章的结果对后面各章也是基本的.

§ 1.1 Pell 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 $D \in \mathbb{N}$ 不是完全平方数(简称不是平方数),将如下的四个

2 不定方程及其应用

不定方程

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

统称为 Pell 方程. 熟知, Pell 方程

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

总有正整数解. 设 (x_1, y_1) 是 (1.1.1) 式所有正整数解 (x, y) 中使 $x + y\sqrt{D}$ 为最小的一组, 称 (x_1, y_1) 为 Pell 方程 (1.1.1) 的最小解, 或称 $x_1 + y_1\sqrt{D}$ 为 Pell 方程 (1.1.1) 的基本解. 设 (x, y) 为 (1.1.1) 式的一组解, 有时也说 $x + y\sqrt{D}$ 是 (1.1.1) 式的一组解. 以后所说的 Pell 类方程 $x^2 - Dy^2 = M$ 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 Pell 方程 (1.1.1) 的基本解, 则 (1.1.1) 式的全部解可表示为

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

显然, 如果令

$$\epsilon_1 = x_1 + y_1\sqrt{D}, \quad \bar{\epsilon}_1 = x_1 - y_1\sqrt{D},$$

则由 (1.1.2) 式得

$$x = \pm \frac{\epsilon_1^n + \bar{\epsilon}_1^n}{2}, \quad y = \pm \frac{\epsilon_1^n - \bar{\epsilon}_1^n}{2\sqrt{D}}, \quad n \in \mathbb{Z},$$

并且 (1.1.1) 式的正整数解为

$$x = \frac{\epsilon_1^n + \bar{\epsilon}_1^n}{2}, \quad y = \frac{\epsilon_1^n - \bar{\epsilon}_1^n}{2\sqrt{D}}, \quad n \in \mathbb{N}.$$

对于 Pell 方程

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

当 D 含有 $4k+3$ 形素因子或 $D \equiv 0 \pmod{4}$ 时, (1.1.3) 式显然无解. 但是, 如果 (1.1.3) 式有解, 则必有无穷多组解. 设 $\epsilon_2 = x_1 + y_1\sqrt{D}$ 为 (1.1.3) 式的基本解, 则有

定理 1.1.2 设方程 (1.1.3) 有解, ϵ_1, ϵ_2 分别为方程 (1.1.1) 与方程 (1.1.3) 的基本解, 则 $\epsilon_1 = \epsilon_2^2$, 且方程 (1.1.3) 的全部解可

表示为

$$x + y\sqrt{D} = \pm \epsilon_2^{2n+1}, \quad n \in \mathbb{Z}. \quad (1.1.4)$$

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 $D = 2p_1 \cdots p_s$, $p_i (i = 1, \dots, s)$ 是不同的奇素数, $p_i \equiv 5 \pmod{8} (i = 1, \dots, s)$ 且当 $s > 2$ 时对任意的 $i \neq j (1 \leq i, j \leq s)$ 都有 Legendre 符号 $\left(\frac{p_j}{p_i}\right) = 1$, 则方程(1.1.3)有解.

证 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

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

这里 $u, v \in \mathbb{N}$ 且 $\gcd(u, v) = 1$, $D = D_1D_2$. 由(1.1.5)式得

$$D_1u^2 - D_2v^2 = 1. \quad (1.1.6)$$

显然, 如果证明了(1.1.6)式中 $D_2 = 1, D_1 = D$, 则证明了方程(1.1.3)有解. 为此, 设 $D_2 > 1$, 如果 $D_1 = 1$, 则 $u + v\sqrt{D}$ 是(1.1.1)式的一个解, 但

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

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

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

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(1.1.6)式给出

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

但 $p_1 \equiv p_2 \equiv 5 \pmod{8}$, 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 $p_i (1 \leq i \leq s)$, 对 (1.1.6) 式取模 p_i , 得

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

仍是矛盾. 这就证明了当 $D_2 > 1$ 时 (1.1.6) 式不成立. 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 $p_i \equiv 1 \pmod{4} (i = 1, \cdots, s)$, 如果 $s = 2$ 或 $2 \nmid s$, 且在 $s > 1$ 时对任意 $i \neq j (1 \leq i, j \leq s)$ 都有 $\left(\frac{p_j}{p_i}\right) = -1$, 则方程 (1.1.3) 有解.

对于 $D = 2p$, $p \equiv 1 \pmod{4}$ 为素数, 当 $p \equiv 5 \pmod{8}$ 时, 由定理 1.1.3 知, 方程 (1.1.3) 有解. 当 $p \equiv 1 \pmod{8}$ 时, 方程 (1.1.3) 是否有解呢? 对此, 有

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

$$2p = r^2 + s^2, r \equiv \pm 3 \pmod{8}, s \equiv \pm 3 \pmod{8},$$

则方程 (1.1.3) 无解.

这个结果不难用 Gauss 整数的性质给出一个简短的证明 (参看 [1], p160~161).

对于 Pell 方程

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

与

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

分别设 ϵ_3, ϵ_4 为(1.1.7)式和(1.1.8)式的基本解(假设(1.1.8)式有解),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

$$\epsilon_1 = \begin{cases} \frac{\epsilon_3}{2}, & \text{当 } \gcd(x, y) = 2 \text{ 时;} \\ \left(\frac{\epsilon_3}{2}\right)^3, & \text{当 } \gcd(x, y) = 1 \text{ 时;} \end{cases}$$

且方程(1.1.7)的全部解可表达为

$$\frac{x + y\sqrt{D}}{2} = \pm \left(\frac{\epsilon_3}{2}\right)^n, n \in \mathbb{Z}.$$

定理 1.1.7 如果方程(1.1.8)有解,则有

$$\epsilon_2 = \begin{cases} \frac{\epsilon_4}{2}, & \text{当 } \gcd(x, y) = 2 \text{ 时;} \\ \left(\frac{\epsilon_4}{2}\right)^3, & \text{当 } \gcd(x, y) = 1 \text{ 时;} \end{cases}$$

且方程(1.1.8)的全部解可表达为

$$\frac{x + y\sqrt{D}}{2} = \pm \left(\frac{\epsilon_4}{2}\right)^{2n+1}, n \in \mathbb{Z}.$$

对于方程

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

如果它们有解,可设 λ_{\pm} 为(1.1.9)式的基本解(即 λ_+ 与 λ_- 分别是对应(1.1.9)式右端取 +2 与 -2 的基本解).

定理 1.1.8 如果方程(1.1.9)有解,则除 $x^2 - 2y^2 = -2$ 外,必有 $\epsilon_1 = \frac{\lambda_{\pm}^2}{2}$,且方程(1.1.9)的全部解可表达为

$$x + y\sqrt{D} = \pm \frac{\lambda_{\pm}^{2n+1}}{2^n}, n \in \mathbb{Z}.$$

定理 1.1.6~定理 1.1.8 均可由广义 Pell 方程 $x^2 - Dy^2 = M$ 的