辽宁科协资助
LIAONING KEXIE ZIZHU
辽宁省优秀自然科学著作

● 佟瑞洲 著

广义费马方程与指数丢番图方程

Fermat Equation in Broad Sense and Index Diophantine Equations

$$x^2-Dy^2=1$$

$$aX^2+D^m=p^z$$

$$x^3+y^3=Dz^2$$

$$x^3+b=Dy^2$$

$$Ax^m+By^n=Cz^l$$

辽宁科学技术出版社
LIAONING SCIENCE AND TECHNOLOGY PUBLISHING HOUSE

辽宁省优秀自然科学著作

广义费马方程与指数丢番图方程

佟瑞洲　著

辽宁科学技术出版社

沈阳

图书在版编目(CIP)数据

广义费马方程与指数丢番图方程/佟瑞洲著. —沈阳:辽宁科学技术出版社,2011.9
(辽宁省优秀自然科学著作)
ISBN 978-7-5381-7113-6

Ⅰ.①广… Ⅱ.①佟… Ⅲ.①丢番图方程-研究 Ⅳ.①O156.7

中国版本图书馆 CIP 数据核字(2011)第 181221 号

出版发行:辽宁科学技术出版社
(地址:沈阳市和平区十一纬路 29 号 邮编:110003)
印 刷 者:沈阳新华印刷厂
经 销 者:各地新华书店
幅面尺寸:185mm×260mm
印 张:13.5
字 数:276 千字
印 数:1~2000
出版时间:2011 年 9 月第 1 版
印刷时间:2011 年 9 月第 1 次印刷
责任编辑:李伟民
特邀编辑:王奉安
封面设计:嵘 嵘
责任校对:刘 庶

书 号:ISBN 978-7-5381-7113-6
定 价:38.00 元

联系电话:024-23284360
邮购热线:024-23284502
http://www.lnkj.com.cn

《辽宁省优秀自然科学著作》评审委员会

序　言

丢番图方程是研究不定方程的整数解、正整数解或有理数解的数论学科，有着悠久的历史，以致内容丰富、方法频出。近代和现代的数学家中，英国的莫德尔(L. J. Mordell)于1969年出版了较为系统总结当时这方面成果的专著《丢番图方程》(Diophantine Equations)。我国最早专门介绍这一学科的著作，是著名数学家柯召与孙琦教授于1980年合作出版的《谈谈不定方程》。我于1989年出版了系统总结这方面的方法和成果的第一本中文专著《丢番图方程引论》。后来，乐茂华于1998年出版了此前Gelfond-Baker方法在丢番图方程中的应用，2000年我出版了当时不定方程的最新成果及其在代数、组合、图论等领域的应用专著。这些专著可以看做是丢番图方程不断发展的总结，为有志于该领域研究的数学爱好者提供了学术价值很高的导引性的范例，推动了丢番图方程的发展。

本书作者就是学习这些著作起步的。他完成的《广义费马方程与指数丢番图方程》一书以两个专题“广义费马方程”和“指数丢番图方程”为切入点，阐述了1989年之后，我国学者在这两个专题方面的主要研究进展情况。第一章分别按二次、三次、四次和高次广义费马方程依次叙述，总结了一些最新结果。二次广义费马方程主要叙述了Pell方程基本解的判定定理和Pell方程解的性质，$x^2-Dy^2=-1$ 的可解性，$lx^2-ky^2=M$ 解的结构，$x^2+my^2=z^2$ 的本原解，二次广义费马方程组及Pell方程的应用。三次广义费马方程主要叙述了 $x^3\pm a^3=Dy^2$，$x^3\pm y^3=Dz^2$ 的研究结果。四次广义费马方程主要叙述了 $x^4+y^4=cz^4$，$x^4+By^4=Cz^2$，$x^4+By^4=Cz^4$，$x^2+By^4=Cz^4$，$x^3+y^3=Cz^4$，$x^2+By^4=Cz^3$，$px^4-(p-1)y^2=z^4$ 等方程的研究结果。高次广义费马方程主要叙述了 $Ax^m+By^n=Cz^r$ 和与 $Ax^m+By^n=Cz^r$ 有关的方程 $ax^4+bx^2y^2+cy^4=dz^2$ 的一些研究结果。第二章分别按 $a^x+b^y=c^z$，$aX^2+D^y=p^z$ 和其他指数丢番图方程依次叙述。在每一章的显著位置均介绍了作者的有关工作。这种专门的叙述和总结对初学者具有一定的启发性、参考性和可读性，对从事相关研究的学者也有一定的借鉴意义。

《广义费马方程与指数丢番图方程》一书虽经我指点，但由于时间和精力问题，未能帮助作者解决更多的问题，不足之处在所难免。希望读者有借鉴地读、更能看出作者用初等方法处理丢番图方程问题的毅力和坚忍不拔的精神。希望本书的出版对数学爱好者有所裨益。也真诚期望广大专家、学者对本书的批评指正。

2011 年 3 月 31 日

目　录

第一章　广义费马方程

设 A,B,C 是两两互素的正整数，m,n,r 是正整数，$\max\{m,n,r\}>1$，称丢番图方程

$$Ax^m+By^n=Cz^r,(x,y,z)=1$$

为广义费马方程.

直到现在，数学工作者们也只是研究了广义费马方程的一些特殊情形. 例如，1637 年费马曾写到，他已经证明方程

$$x^n+y^n=z^n,(x,y)=1,n>2$$

无正整数解，这一命题被称为费马大定理. 但人们一直没有看到费马的证明，直到 1995 年，Andrew Wiles 巧妙地证明了费马大定理成立，终于使这个困扰数学界 350 多年的难题获得圆满解决[1]. 广义费马方程的另一重要情形是方程

$$Ax^m+By^n=Cz^r,(x,y,z)=1,\frac{1}{m}+\frac{1}{n}+\frac{1}{r}<1$$

1989 年，Tijdeman[2] 猜想：方程仅有有限多组整数解 (x,y,z). 稍后 H. Darmon，A. Granville[3] 提出了广义费马猜想：方程在 $A=B=C=1$ 时仅有 10 组整数解：$1+2^3=3^2$，$2^5+7^2=3^4$，$7^3+13^2=2^9$，$2^7+17^3=71^2$，$3^5+11^4=122^2$，$17^7+76\ 271^3=21\ 063\ 928^2$，$1\ 414^3+2\ 213\ 459^2=65^7$，$9\ 262^3+15\ 312\ 283^2=113^7$，$43^8+96\ 222^3=30\ 042\ 907^2$，$33^8+1\ 549\ 034^2=15\ 613^3$.

1997 年，Andrew Beal 为如下的猜想设了大奖：如果 $A=B=C=1$，m,n,r 均大于 2，则上述方程没有正整数解[4].

关于广义费马方程的研究，内容十分丰富，本章分别按二次、三次、四次、高次广义费马方程来叙述这方面的研究成果.

§1　二次广义费马方程

§1.1　方程 $x^2-Dy^2=1$

二次广义费马方程的一个特殊情形是 Pell 方程

$$x^2-Dy^2=1,(x,y)=1,D>0\text{ 非平方数}\tag{1}$$

关于方程(1)的解的存在性及其结构在文献[5-6]中已经研究得很清楚. 但用传统求法求出方程(1)的基本解,有时计算很冗长,例如 Pell 方程 $x^2-1\ 141y^2=1$,当 $1\leqslant y\leqslant 10^{25}$ 时都无解. 然而在一些问题的研究中,常常要确定 Pell 方程(1)的一组解是否是基本解. 因此,判定方程(1)的基本解是一件十分有意义的工作[7].

一、方程(1)基本解的判定

文献[5]曾介绍下面两个判定定理.

定理 1[5]　设 x_1,y_1 是方程(1)的一组正整数解. 如果

$$x_1>\frac{1}{2}y_1^2-1,$$

则 $x_1+y_1\sqrt{D}$ 是方程(1)的基本解.

定理 2[5]　设 $s>0,t>0,D=s(st^2+2)$,则方程(1)的基本解 $x_1+y_1\sqrt{D}=1+st^2+t\sqrt{D}$.

此外,曹珍富在文献[7]中还给出了 $D=s(st^2-2),D=s(st^2\pm1)$ 时方程(1)的基本解.

1951 年,T. Nagell[8] 在他的专著《Introduction to Number Theory》中介绍了störmer 定理,给出了判定 Pell 方程基本解的另一个方法.

定理 3(störmer 定理)　设 x,y 是正整数,$D>0$ 不是平方数,如果 $y\mid{}^*D$,则 $x+y\sqrt{D}$ 是 Pell 方程(1)的基本解. 这里符号 $y\mid{}^*D$ 表示 y 的每一个素因子整除 D.

定理 3 的证明可参见文献[7].

1995 年,梅汉飞等推广了 störmer 定理,获得了定理 4;随后,1997 年又进一步推广为定理 5.

定理 4[9]　设 x,y 是正整数,$D>0$ 是整数,且为非平方数,满足方程(1),式中 $y=p^ny'$,p 是素数,n 是非负整数,$p\nmid D$,但如果 $y'\mid{}^*D$,则

$$x+y\sqrt{D}=\varepsilon\text{ 或 }\varepsilon^2\text{ 或 }\varepsilon^3$$

式中 $\varepsilon=x_1+y_1\sqrt{D}$ 是方程(1)的基本解.

定理 5[10]　设 x,y 是正整数,$D>0$ 不是平方数,满足方程(1),且 $y=p_1^{n_1}p_2^{n_2}y'$,p_1,p_2 均为素数,n_1,n_2 为非负整数,$p_1\nmid D,p_2\nmid D,y'\mid{}^*D$,则 $x+y\sqrt{D}=\varepsilon$ 或 ε^4 或 ε^6 或 ε^{p^r},式中 p 是一个奇素数,r 是正整数,$\varepsilon=x_1+y_1\sqrt{D}$ 是(1)的基本解.

1999 年,罗家贵证明了:

定理 6[11]　设 $D>0$ 不是完全平方数,$x>0,y>0$ 是方程(1)的一个解,$\varepsilon=x_0+y_0\sqrt{D}$ 是(1)的基本解,若 $x\mid{}^*x_0$,则 $x+y\sqrt{D}=\varepsilon$.

二、方程(1)解的性质

利用递推序列方法求解某些四次或高次广义费马方程时,常常需要研究方程(1)解

的性质，下面介绍这方面的研究成果.

2001 年，曹珍富[12]给出方程(1)的一个结果，即证明了下面的定理 7.

定理 7　设$(x_i,y_i)(i=1,2)$是 Pell 方程(1)的两组解，且$(y_1,y_2)=1$，则 $D=x_0^2-1$，$x_0>1$ 是整数.

证明　用 **N** 表示正整数集，由 Pell 方程的解知[6]，式(1)给出

$$y_i=\frac{\varepsilon^{m_i}-\bar{\varepsilon}^{m_i}}{2\sqrt{D}}=\frac{\varepsilon^{m_i}-\bar{\varepsilon}^{m_i}}{\varepsilon-\bar{\varepsilon}}y_0,\ i=1,2$$

这里 $\varepsilon=x_0+y_0\sqrt{D}$ 是 Pell 方程(1)的基本解，$\varepsilon=x_0-y_0\sqrt{D}$，$m_i\in\mathbf{N}(i=1,2)$. 由于$(\varepsilon^{m_i}-\bar{\varepsilon}^{m_i})/(\varepsilon-\bar{\varepsilon})\in\mathbf{N}$，故 $y_0\mid y_i(i=1,2)$，但$(y_1,y_2)=1$，故 $y_0=1$，所以 $D=x_0^2-1$. 证毕.

设(x_1,y_1)为(1)的基本解，由文献[6]知方程(1)的全部非负整数解为(x_n,y_n)，满足

$$x_n+y_n\sqrt{D}=(x_1+y_1\sqrt{D})^n,n=0,1,2,3,\cdots,\tag{2}$$

式中$(x_0,y_0)=(1,0)$为(1)的平凡解.

1992 年，王炳安、佟瑞洲研究了式(2)中(x_n,y_n)，获得了若干性质，为叙述方便，用 $\mathbf{N}_0$ 表示非负整数集.

基本性质　设 $n\in\mathbf{N},k\in\mathbf{N}_0,0\leqslant k\leqslant n$，则有

(Ⅰ)$x_n=x_{n-k}x_k+Dy_{n-k}y_k,y_n=y_{n-k}x_k+x_{n-k}y_k$

(Ⅱ)$x_k=x_{n-k}x_n-Dy_{n-k}y_n,y_k=x_{n-k}y_n-y_{n-k}x_k$

下面将借助于矩阵这个工具给出上述基本性质的一个新的证法.

证明　首先证明$\begin{pmatrix}x_n\\y_n\end{pmatrix}=P^n\begin{pmatrix}1\\0\end{pmatrix}$，式中 $P=\begin{pmatrix}x_1&Dy_1\\y_1&x_1\end{pmatrix}$.

事实上，令 $\lambda_1=x_1+y_1\sqrt{D}$，$\lambda_2=x_1-y_1\sqrt{D}$，则由式(2)易知

$$x_n=\frac{\lambda_1^n+\lambda_2^n}{2},y_n=\frac{1}{2\sqrt{D}}(\lambda_1^n-\lambda_2^n)$$

令 $T=\begin{pmatrix}\sqrt{D}&-\sqrt{D}\\1&1\end{pmatrix}$，则 $P=\begin{pmatrix}\lambda_1&0\\0&\lambda_2\end{pmatrix}T^{-1}$，于是

$$P^n=T\begin{pmatrix}\lambda_1&0\\0&\lambda_2\end{pmatrix}T^{-1}=\frac{1}{2\sqrt{D}}\begin{pmatrix}\sqrt{D}(\lambda_1^n+\lambda_2^n)&D(\lambda_1^n-\lambda_2^n)\\\lambda_1^n-\lambda_2^n&\sqrt{D}(\lambda_1^n+\lambda_2^n)\end{pmatrix}=\begin{pmatrix}x_n&Dy_n\\y_n&x_n\end{pmatrix}$$

显然有 $P^n\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}x_n\\y_n\end{pmatrix}$

其次，证 P^n 可逆. 事实上，$(P^n)^{-1}=\begin{pmatrix}x_n&-Dy_n\\-y_n&x_n\end{pmatrix}$.

再次，有

(A)　$\begin{pmatrix}x_n\\y_n\end{pmatrix}=P^{n-k}\begin{pmatrix}x_k\\y_k\end{pmatrix}$

(B)　$\begin{pmatrix}x_k\\y_k\end{pmatrix}=(P^{n-k})^{-1}\begin{pmatrix}x_n\\y_n\end{pmatrix}$

事实上，$\begin{pmatrix}x_n\\y_n\end{pmatrix}=P^n\begin{pmatrix}1\\0\end{pmatrix}=P^{n-k}\cdot P^k\begin{pmatrix}1\\0\end{pmatrix}=P^{n-k}\begin{pmatrix}x_k\\y_k\end{pmatrix}$

因 P^{n-k} 可逆，故(B)显然成立．由(A)(B)即得基本性质(Ⅰ)(Ⅱ)．

由基本性质很容易得到下面的 7 组关系式：

设 $m,n\in\mathbf{N}_0$，$m\geqslant n$，则

(ⅰ)(加法)：$x_{m+n}=x_mx_n+Dy_my_n$；

$y_{m+n}=x_my_n+y_mx_n$；

$x_{2n}=x_n^2+Dy_n^2=2x_n^2-1=2Dy_n^2+1$；

$y_{2n}=2x_ny_n$．

(ⅱ)(减法)：$x_{m-n}=x_mx_n-Dy_my_n$；

$y_{m-n}=x_ny_m-x_my_n$．

(ⅲ)(负指标)：若 $l\in\mathbf{N}$，则 $x_{-l}=x_l$；

$y_{-l}=-y_l$．

(ⅳ)(积化合差)：$x_mx_n=\dfrac{1}{2}(x_{m+n}+x_{m-n})$

$y_my_n=\dfrac{1}{2D}(x_{m+n}-x_{m-n})$

$y_mx_n=\dfrac{1}{2}(y_{m+n}+y_{m-n})$

$x_my_n=\dfrac{1}{2}(y_{m+n}-y_{m-n})$

(ⅴ)(合差化积)：$x_m+x_n=2x_{\frac{m+n}{2}}x_{\frac{m-n}{2}}$

$y_m+y_n=2y_{\frac{m+n}{2}}x_{\frac{m-n}{2}}$

$x_m-x_n=2Dy_{\frac{m+n}{2}}y_{\frac{m-n}{2}}$

$y_m-y_n=2x_{\frac{m+n}{2}}y_{\frac{m-n}{2}}$

(ⅵ)(递推公式)：

①$x_{n+1}=x_1x_n+Dy_1y_n$，$y_{n+1}=y_1x_n+x_1y_n$

②$x_{n+2}=2x_1x_{n+1}-x_n$，$y_{n+2}=2x_1y_{n+1}-y_n$

式②称为 Pell 序列，探讨 $x_n=Q^2$ 或 $y_n=Q^2$，$Q\in\mathbf{N}_0$ 的解，仍是未完全解决的问题．

由公式(ⅳ)(ⅴ)得到一类很有用的分解公式：

(ⅶ)设 $m,n,k\in\mathbf{N}_0$，$m\geqslant n+k$，则

$x_{m-n}x_k=x_{m+k}x_n-Dy_my_{n+k}=x_mx_{n+k}-Dy_{m+k}y_n$

$y_{m-n}y_k=\dfrac{1}{D}(x_{m+k}x_n-x_mx_{n+k})=y_my_{n+k}-y_{m+k}y_n$

$x_{m-n}y_k=x_my_{n+k}-x_{m+k}y_n=y_{m+k}x_n-y_mx_{n+k}$

$y_{m-n}x_k=y_mx_{n+k}-x_{m+k}y_n=y_{m+k}x_n-x_my_{n+k}$

性质 1　(ⅰ)若 $2\nmid n,k,m,n\in\mathbf{N}$,则

$$x_{mn}=\sum_{k=0}^{\frac{n-1}{2}}C_n^{2k+1}x_m^{2k+1}(Dy_m^2)^{\frac{n-1}{2}-k}$$

$$y_{mn}=\sum_{k=0}^{\frac{n-1}{2}}C_n^{2k}x_m^{2k}y_m^{n-2k}D^{\frac{n-1}{2}-k}$$

(ⅱ)若 $2\mid n,k,m,n\in\mathbf{N}$,则

$$x_{mn}=\sum_{k=0}^{\frac{n}{2}}C_n^{2k}x_m^{2k}(Dy_m^2)^{\frac{n}{2}-k}$$

$$y_{mn}=\sum_{k=0}^{\frac{n-1}{2}}C_n^{2k+1}x_m^{2k+1}y_m^{n-2k-1}D^{\frac{n}{2}-k-1}$$

证明　由式(2)知,$x_{mn}+\sqrt{D}y_{mn}=(x_1+\sqrt{D}y_1)^{mn}=(x_m+\sqrt{D}y_m)^n=\sum_{i=0}^{n}C_n^ix_m^i(\sqrt{D}y_m)^{n-i}$

分 $2\mid n$ 和 $2\nmid n$ 两种情况讨论即得(ⅰ)、(ⅱ).

推论　设 $m,n\in\mathbf{N}$

(ⅰ)若 $n\mid m$,则 $y_n\mid y_m$;

(ⅱ)若 $m=ns,2\nmid s\in\mathbf{N}$,则 $x_n\mid x_m$;

(ⅲ)若 $m=ns,2\mid s,s\in\mathbf{N}$,则 $x_n\mid y_m$.

(ⅳ)$x_{mn}\equiv\begin{cases}x_m(\mathrm{mod}\,y_m) & \text{当 } 2\nmid n \text{ 时}\\ 1(\mathrm{mod}\,y_m) & \text{当 } 2\mid n \text{ 时}\end{cases}$

(ⅴ)当 $2\mid n$ 时,$x_{mn}\equiv(-1)^{\frac{n}{2}}(\mathrm{mod}\,x_m)$

(ⅵ)若 $2\nmid n$ 时,则 $y_{mn}\equiv(-1)^{\frac{n-1}{2}}y_m(\mathrm{mod}\,x_m)$

性质 2　设 $m,n\in\mathbf{N}$,则$(y_m,y_n)=y_{(m,n)}$

证明　令 $d=(m,n)$. 则有 $s,t\in\mathbf{Z}$,使 $ms+nt=d$,于是

$y_d=y_{ms+nt}=y_{ms}x_{nt}+x_{ms}y_{nt}$,由推论(ⅰ)知 $y_m\mid y_{ms},y_n\mid y_{nt}$,故有 $k,l\in\mathbf{Z}$,使 $y_{ms}=ky_m,y_{nt}=ly_n$,于是

$$y_d=ky_mx_{nt}+x_{ms}ly_n \tag{3}$$

因 $y_d\mid y_m,y_d\mid y_n$,又设 w 是 y_m 与 y_n 的任意公因子,由式(3)知 $w\mid y_d$,故$(y_m,y_n)=y_d$.

性质 3　设 $m,n\in\mathbf{N}$,则 $y_n\mid y_m$ 的充要条件为 $n\mid m$.

证明　由推论(ⅰ)知充分性成立. 下证必要性:因 $y_n\mid y_m$,故$(y_n,y_m)=y_n$,由性质 2 知 $n=(m,n)$,　即 $n\mid m$.

性质 4　设 $m,n,k\in\mathbf{N}$,则 $x_n\mid x_m$ 的充要条件为 $m=(2k-1)n$.

证明　由推论(ⅱ)知充分性成立. 下证必要性:

假设 $n\nmid m$，则 $m=nq+r,0<r<n,q\in\mathbf{N}$

(ⅰ)若 $2\mid q$，则 $x_r=x_{m-nq}=x_mx_{nq}-Dy_my_{nq}$ (4)

由推论(ⅲ)，知 $x_n\mid y_{np}$，若 $x_n\mid x_m$，由式(4)知 $x_n\mid x_r$，这与 $x_n>x_1>0$ 矛盾，即 $x_n\nmid x_m$.

(ⅱ)若 $2\nmid q$，则将 $m=nq+r$ 改写为 $n(q+1)-m=n-r,0<n-r<n$. 于是

$$x_{n-r}=x_{n(q+1)}x_m-Dy_{n(q+1)}y_m \tag{5}$$

由于 $x_n\mid y_{n(q+1)}$，若 $x_n\mid x_m$，则由(5)知 $x_n\mid x_{n-r}$，与 $x_n>x_{n-r}>0$ 矛盾. 故 $x_n\nmid x_m$.

即在假设 $n\nmid m$ 的条件下则有 $x_n\nmid x_m$，这与题设 $x_n\mid x_m$ 矛盾. 故必有 $n\mid m$. 证毕.

性质 3、性质 4 推广了文献[13]的推论 1 及推论 2.

性质 5　设 $m,n,d\in\mathbf{N}$，且 $(m,n)=d$.

(ⅰ)若 $2\nmid\frac{n}{d}$，则 $(x_m,y_n)=1$；

(ⅱ)若 $2\mid\frac{n}{d}$，则 $(x_m,y_n)=x_{(m,n)}$.

证明　(ⅰ)由性质 2 知 $(y_{2m},y_{2n})=y_{(2m,2n)}=y_{2d}$，故

$$\left(\frac{y_{2m}}{y_{2d}},\frac{y_{2n}}{y_{2d}}\right)=1,\text{即}\left(\frac{x_my_m}{x_dy_d},\frac{y_nx_n}{y_dx_d}\right)=1 \tag{6}$$

①因 $2\nmid\frac{m}{d}$，则 $x_d\mid x_m$. 由 $2\nmid\frac{n}{d}$，知 $x_d\mid x_n$，而 $y_d\mid y_i(i=m,n)$

由式(6)知 $(\frac{x_m}{x_d},\frac{y_n}{y_d})=1$，由推论(ⅳ)知

$$y_n\equiv(-1)^{\frac{\frac{n}{d}-1}{2}}y_d(\mathrm{mod}x_d)$$

故 $(\frac{y_n}{y_d},x_d)=1$，于是 $\left(x_m,\frac{y_n}{y_d}\right)=1$. 由推论(ⅳ)知 $(x_m,y_d)=1$. 故 $(x_m,y_n)=1$.

②若 $2\mid\frac{m}{d}$，因 $y_{2d}\mid y_m$，故由式(6)知 $\left(x_m,\frac{y_n}{y_d}\right)=1$. 由推论(ⅳ)知 $(x_m,y_d)=1$，故有 $(x_m,y_n)=1$.

(ⅱ)若 $2\mid\frac{n}{d}$，因为 $(\frac{m}{d},\frac{n}{d})=1$，故 $2\nmid\frac{m}{d}$. 于是 $y_{2d}\mid y_n,x_d\mid x_m,y_d\mid y_m$.

由式(6)知 $(\frac{x_m}{x_d},\frac{y_n}{x_dy_d})=1$，由推论(ⅳ)知 $x_m\equiv x_d(\mathrm{mod}y_d)$，故 $(\frac{x_m}{x_d},y_d)=1$，于是 $(\frac{x_m}{x_d},\frac{y_n}{x_d})=1$，即 $(x_m,y_n)=x_d=x_{(m,n)}$.

性质 5 推广了文献[8]的引理 5.

性质 6　设 $m,n,d\in\mathbf{N}$，且 $(m,n)=d$.

(ⅰ)若 $2\nmid\frac{m}{d},2\nmid\frac{n}{d}$，则 $(x_m,x_n)=x_{(m,n)}$；

(ⅱ)若 $\frac{m}{d},\frac{n}{d}$ 一奇一偶，则 $(x_m,x_n)=1$.

证明　(ⅰ)因 $2\nmid\frac{m}{d}$，$2\nmid\frac{n}{d}$，故 $x_d\mid x_i$，$i=m,n$，又 $y_d\mid y_m$，$y_d\mid y_n$. 由式(6)知$\left(\frac{x_m}{x_d},\frac{x_n}{x_d}\right)=1$，此即$(x_m,x_n)=x_d=x_{(m,n)}$.

(ⅱ)不妨设 $2\mid\frac{m}{d}$，$2\nmid\frac{n}{d}$，则 $x_dy_d\mid y_m$，$x_d\mid x_n$. 由式(6)$\left(x_m,\frac{x_n}{x_d}\right)=1$，由推论(Ⅴ)知$(x_m,x_d)=1$. 于是$(x_m,x_n)=1$.

对 $2\nmid\frac{m}{d}$，$2\mid\frac{n}{d}$，同理可证. 因$(\frac{m}{d},\frac{n}{d})=1$，故$\frac{m}{d}$，$\frac{n}{d}$不能同为偶数. 证毕.

性质 7　设 $n,k,t\in\mathbf{N}$，则

(ⅰ)$x_{n+2kt}\equiv(-1)^tx_n(\mathrm{mod}x_k)$；

(ⅱ)$y_{n+2kt}\equiv(-1)^ty_n(\mathrm{mod}x_k)$.

证明　(ⅰ)因 $x_{n+2k}=x_nx_{2k}+Dy_ny_{2k}=x_n(2x_k^2-1)+Dy_n\cdot2x_ky_k\equiv-x_n(\mathrm{mod}x_k)$，故有 $x_{n+2kt}=x_{n+2k(t-1)+2k}\equiv-x_{n+2k(t-1)}\equiv(-1)^2x_{n+2k(t-2)}\equiv\cdots\equiv(-1)^tx_n(\mathrm{mod}x_k)$.

(ⅱ)同理可证. 这便推广了文献[5]及文献[14]的相应的关系式.

1999 年，Walsh[15] 提出猜想：当 $D\neq2^{2r}\cdot1785$，式中 $r\in\{0,1,2\}$ 时，如果

$$y_n=2z^2,n,z\in\mathbf{Z}\tag{7}$$

则必有 $n<4$.

2003 年，钟莉萍，乐茂华[16] 部分地证实了上述猜想，即证明了：

定理 8　当 $D\neq2^{2r}\cdot1785$，$r\in\{0,1,2\}$，而且 y_1 是奇数时，如果(7)成立，则必有 $n=2$.

§1.2　方程 $x^2-Dy^2=M$

二次广义费马方程的另一特殊情形是方程

$$x^2-Dy^2=M,D>0\text{ 非平方数},M\neq0\tag{1}$$

方程(1)的解的结构及存在性在文献[6-7]中已阐述完整，$M=-1,\pm2,\pm4,\pm p$，$\pm2p$(p 为奇素数)时，如果方程(1)有解，则方程(1)的全部正整数解均已给出.

$M=-1$ 时，研究 D 为何值时方程(1)有解或无解，是一件有意义的事情. 设 p 为奇素数，当 $D=p\equiv1(\mathrm{mod}4)$ 及 $D=2p$，$p\equiv5(\mathrm{mod}8)$时方程(1)有整数解. 而 D 含有 $4k+3$ 形因子或 $4\mid D$ 时，方程(1)无整数解. 1978 年，Lienen[17] 证明了

定理 1　设 $p\equiv1(\mathrm{mod}8)$是素数，且 $D=2p=r^2+s^2$，$r\equiv\pm3(\mathrm{mod}8)$，$s\equiv\pm3(\mathrm{mod}8)$，则方程(1)当 $M=-1$ 时无整数解.

定理 2　若 $s=2$ 或 $2\nmid s$，$p_i\equiv1(\mathrm{mod}4)(i=1,2,\cdots,s)$且对任意的 $i\neq j$，$(1\leqslant i,j\leqslant s)$都有 $\left(\frac{p_j}{p_i}\right)=-1$，$D=p_1\cdots p_s$，$p_i(i=1,2,\cdots,s)$为不同的奇素数，$M=-1$，则方程(1)有整数解.

1994 年，袁平之[18-19] 给出了方程(1)，当 $M=-1$ 时不可解的一个充要条件，获得了若干推论，从而拓展了 Lienen 的结果.

引理　(ⅰ)　设 $D>0$,D 非平方数,$4\nmid D$,并有正整数 $k>1,l,(k,l)=1,kl=D$ 使得二次方程 $kx^2-ly^2=1$ 有解,则 k,l 由 D 唯一决定;(ⅱ)　设 $D>0$,D 非平方数,$2\nmid D$,并有正整数 $k,l,(k,l)=1,kl=D$ 使得二次方程 $kx^2-ly^2=2$ 有解,则 k,l 由 D 唯一决定;(ⅲ)　设 $D>0$,D 非平方数,$2\nmid D$,并有正整数 $k>1,l,(k,l)=1,kl=D$ 使得二次方程 $kx^2-ly^2=4$ 有解,则 k,l 由 D 唯一决定.

由引理有:

定理 3　设 $4\nmid D$,D 无模 4 为 3 的素因子,D 非平方数,$M=-1$,则方程(1)不可解的充要条件是存在 $D_1>1,D_2>1,(D_1,D_2)=1,D_1D_2=D$ 使方程 $D_1x^2-D_2y^2=1$ 有解.

推论 1　如果 $M=-1$,整数 $D=m\cdot\dfrac{(mu^2\pm1)}{v^2}$,$D>m>1,(m,v)=1$,则方程(1)无解,特别当 $D=m(mu^2\pm1),m>1,D>2$ 时方程(1)无解.

我们注意到,事实上推论 1 给出了 $M=-1$ 时所有使方程(1)不可解的整数 D.

推论 2　如果 $M=-1,D=2p,p\equiv1(\mathrm{mod}4)$ 为素数,则方程(1)无解的充要条件是 $2x^2-py^2=1$ 或 $2x^2-py^2=-1$ 有解.

推论 3　如果 $p=2x^2\pm1$ 是模 4 为 1 的素数,则方程 $x^2-2py^2=-1$ 不可解.

设 $p=2\cdot13^2-1=337$,由于 $2p=674=25^2+7^2$,故 Lienen 的结果不包含推论 3 的结论.

定理 4[20]　设 $\zeta>0,\eta>0$ 满足 Pell 方程

$$x^2-Dy^2=4,D>0\text{ 不是平方数}\tag{2}$$

若 $\zeta>2\eta^2-1$,则 $\zeta+\eta\sqrt{D}$ 是 Pell 方程(2)的基本解.

定理 5[21]　设 $x,y\in\mathbf{N}$ 满足 Pell 方程

$$x^2-Dy^2=\pm1,D\in\mathbf{N},D\text{ 不是平方数}\tag{3}$$

$\varepsilon=x_0+y_0\sqrt{D}$ 是式(3)的基本解,若 $x\mid^* x_0$ 或 $y\mid^* y_0$,则 $x+y\sqrt{D}=\varepsilon$.

2001 年,董晓蕾、曹珍富研究满足方程 $1+4b^2k^{2n}=da^2$(式中 $a,b,k,n,d\in\mathbf{N},k>1,n>1,d$ 无平方因子)的实二次域 $Q(\sqrt{d})$ 的类数 $h(d)$ 时,证明了下面结果[22]:

定理 6[22]　若 $(x,y)\in\mathbf{N},(x_1,y_1)$ 是方程(1)当 $D=d,M=-1$ 时的解,且 $x_1>\dfrac{y_1^2}{2}$,则 $x_1+y_1\sqrt{d}=x_0+y_0\sqrt{d}$ 是方程(1)的基本解.

设 $\varepsilon=1+\sqrt{2},\bar{\varepsilon}=1-\sqrt{2},x_n=\dfrac{\varepsilon^n+\bar{\varepsilon}^n}{2},y_n=\dfrac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{2}}$,当 $2\nmid n$ 时,如何用初等方法证明 $y_n=Q^2$ 仅有正整数解 $y_1=1,y_7=13^2$,这是一个数论中未解决的问题[23].佟瑞洲给出了数列 x_n,y_n 的若干性质.

定理 7　(1)设 $J_p=\left(\dfrac{y_p}{x_p}\right),J_1=1$,则有:

(ⅰ)若 $2\nmid p$,则 $J_{p-1}=J_p$;

若 $p\equiv 1(\mathrm{mod}4)$，则 $J_p=-J_{p+1}$；

若 $p\equiv 3(\mathrm{mod}4)$，则 $J_p=J_{p+1}$.

(ⅱ)若 $p\equiv 1,6,7,0(\mathrm{mod}8)$，则 $J_p=1$；

若 $p\equiv 2,3,4,5(\mathrm{mod}8)$，则 $J_p=-1$.

(2)$x_n^{\,2}-2y_n^{\,2}=(-1)^n$.

(3)$y_{2m}=2y_mx_m$，$x_{2m}=2x_m^2+(-1)^{m-1}=x_m^2+2y_m^2=4y_m^2+(-1)^m$.

(4)若 $2\mid k$，则

(ⅰ)$y_{2kT+n}\equiv(-1)^Ty_n(\mathrm{mod}x_k)$；

(ⅱ)$y_{2kT+n}\equiv y_n(\mathrm{mod}y_k)$.

(5)若 $2\nmid mn$，则 $x_m\mid x_{mn}$，$y_m\mid y_{mn}$，$x_n\mid x_{mn}$，$y_n\mid y_{mn}$.

(6)若 $2\nmid mn$，则

(ⅰ)$y_{mn}\equiv y_i(\mathrm{mod}x_i)$，$i=m,n$；

(ⅱ)$x_{mn}\equiv(-1)^{\frac{n-1}{2}}x_m(\mathrm{mod}y_m)$；

(ⅲ)$x_{mn}\equiv(-1)^{\frac{m-1}{2}}x_n(\mathrm{mod}y_n)$.

(7)若 $2\nmid n$，n 含有 $8k\pm 3$ 形素因子，则 $y_n\neq Q^2$.

(8)若 p 为素数时，则

(ⅰ)当 $p\equiv\pm 1(\mathrm{mod}8)$时，$y_p\equiv 1(\mathrm{mod}p)$；

(ⅱ)当 $p\equiv\pm 3(\mathrm{mod}8)$时，$y_p\equiv -1(\mathrm{mod}p)$.

(9)$p\equiv 17,23(\mathrm{mod}40)$时，$y_p\neq Q^2$.

(10)$y_{4m+1}=y_{2m+1}^2+y_{2m}^2$，$y_{4m+3}=y_{2m+2}^2+y_{2m+1}^2$.

证明　(1)的证明.　易证 x_n，y_n 有如下性质：

(Ⅰ)若 $n\equiv 1,0(\mathrm{mod}4)$，则 $x_n\equiv 1(\mathrm{mod}4)$；

若 $n\equiv 2,3(\mathrm{mod}4)$，则 $x_n\equiv 3(\mathrm{mod}4)$；

若 $2\mid n$，则 $2\mid y_n$；若 $2\nmid n$，则 $y_n\equiv 1(\mathrm{mod}4)$.

(Ⅱ)$y_{m+n}=x_my_n+x_ny_m$，$n=1$ 时，$y_{m+1}=y_m+x_m$.

(Ⅲ)$x_{m+n}=x_mx_n+2y_my_n$，$n=1$ 时，$x_{m+1}=y_{m+1}+y_m$.

(ⅰ)若 $2\nmid p$，$J_{p-1}=\left(\dfrac{y_{p-1}}{x_{p-1}}\right)=\left(\dfrac{y_{p-1}+x_{p-1}}{x_{p-1}}\right)=\left(\dfrac{y_p}{x_{p-1}}\right)=\left(\dfrac{x_{p-1}}{y_p}\right)=\left(\dfrac{y_p-y_{p-1}}{y_p}\right)=\left(\dfrac{-1}{y_p}\right)\left(\dfrac{y_{p-1}}{y_p}\right)=\left(\dfrac{y_p+y_{p-1}}{y_p}\right)=\left(\dfrac{x_p}{y_p}\right)=\left(\dfrac{y_p}{x_p}\right)=J_p$.

$J_{p+1}=\left(\dfrac{y_{p+1}}{x_{p+1}}\right)=\left(\dfrac{x_{p+1}-y_p}{x_{p+1}}\right)=\left(\dfrac{-y_p}{x_{p+1}}\right)=\left(\dfrac{-1}{x_{p+1}}\right)\left(\dfrac{y_p}{x_{p+1}}\right)=\left(\dfrac{-1}{x_{p+1})}\right)\left(\dfrac{x_{p+1}}{y_p}\right)=\left(\dfrac{-1}{x_{p+1}}\right)\left(\dfrac{x_p+2y_p}{y_p}\right)=\left(\dfrac{-1}{x_{p+1}}\right)\left(\dfrac{x_p}{y_p}\right)=\left(\dfrac{-1}{x_{p+1}}\right)\left(\dfrac{y_p}{x_p}\right)=\left(\dfrac{-1}{x_{p+1}}\right)J_p$.

当 $p\equiv 1(\mathrm{mod}4)$时，$x_{p+1}\equiv 3(\mathrm{mod}4)$，$\left(\dfrac{-1}{x_{p+1}}\right)=-1$，$J_{p+1}=-J_p$.

当 $p\equiv 3(\mathrm{mod}4)$时，$x_{p+1}\equiv 1(\mathrm{mod}4)$，$\left(\frac{-1}{x_{p+1}}\right)=1$，$J_{p+1}=J_p$.

(ⅱ)　由(ⅰ)易推(ⅱ)成立.

(2)～(5)容易证明.

(6)因为 $x_{mn}+\sqrt{2}y_{mn}=(1+\sqrt{2})^{mn}=(x_m+\sqrt{2}y_m)^n$，故

$$x_{mn}=\sum_{i=1}^{\frac{n-1}{2}}C_n^{2i}\cdot 2^i\cdot y_m^{2i}x_m^{n-2i}+x_m^n\equiv x_m^n\equiv x_m(x_m^2)^{\frac{n-1}{2}}\equiv(-1)^{\frac{n-1}{2}}x_m(\mathrm{mod}y_m).$$

而 $y_{mn}=\sum_{i=0}^{\frac{n-1}{2}-1}C_n^{2i+1}\cdot 2^i\cdot y_m^{2i+1}x_m^{n-2i-1}+(2y_m^2)^{\frac{n-1}{2}}y_m\equiv y_m(\mathrm{mod}x_m)$. 同理(ⅰ)～(ⅲ)的其他情形可证.

(7)由假设，$n=mp$，$p=8k\pm 3$，由(6)知，$y_n=y_{mp}\equiv y_p(\mathrm{mod}x_p)$，而由(1)知 $J_p=\left(\frac{y_p}{x_p}\right)=-1$，故 $y_n\neq Q^2$.

显然，只剩下 $2\nmid n$，n 只含 $8k\pm 1$ 形素因子，y_n 是否为平方数的问题.

(8) 因 $y_p=\sum_{i=0}^{\frac{p-1}{2}}C_p^{2i+1}2^i$，当 $0\leqslant i<\frac{p-1}{2}$时，$(2i+1,p)=1$，故$((2i+1)!,p)=1$，因 $C_p^{2i+1}=\frac{p(p-1)\cdots 3\cdot 2\cdot 1}{(2i+1)!}$，而 C_p^{2i+1} 为整数，即$(2i+1)!\mid(p-1)(p-2)\cdots 3\cdot 2\cdot 1$，于是 $p\mid C_p^{2i+1}$. 因此，$y_p\equiv 2^{\frac{p-1}{2}}\equiv\left(\frac{2}{p}\right)(\mathrm{mod}p)$.

(ⅰ)当 $p\equiv\pm 1(\mathrm{mod}8)$时，$\left(\frac{2}{p}\right)=1$；

(ⅱ)当 $p\equiv\pm 3(\mathrm{mod}8)$时，$\left(\frac{2}{p}\right)=-1$.

(9) 由(4)及(8)便知(9)成立.

(10) 易证成立.

§1.3　方程 $kx^2-ly^2=M$

$kx^2-ly^2=M$ 是二次广义费马方程的又一特殊情形，下面讨论其解的结构.

定理 1[24]　设 $k>1$，$l>1$ 为给定的正整数，$(k,l)=1$，kl 非平方数，若丢番图方程

$$kx^2-ly^2=1 \tag{1}$$

有正整数解，并设 $x_1\sqrt{k}+y_1\sqrt{l}$ 是式(1)的所有解 $x>0$，$y>0$ 中使 $x\sqrt{k}+y\sqrt{l}$ 最小的(为方便起见，称 $x_1\sqrt{k}+y_1\sqrt{l}$ 为方程(1)的最小解)，则(1)的全部正整数解 x，y，可由下式给出：

$$x\sqrt{k}+y\sqrt{l}=(x_1\sqrt{k}+y_1\sqrt{l})^n,n>0,2\nmid n \tag{1}_1$$

证明　设 $\varepsilon_1=x_1\sqrt{k}+y_1\sqrt{l}$，$\delta=x\sqrt{k}+y\sqrt{l}$，$\eta=a+b\sqrt{kl}$ 是 Pell 方程 $x^2-kly^2=1$ 的基本解，容易验证 ε_1^2，$\varepsilon_1\delta$ 均为 Pell 方程 $x^2-kly^2=1$ 的解，于是有正整数 t_1，t_2，$t_1>t_2$，使