参赛队员姓名：刘若霆

中学：广东实验中学

省份：广东

国家/地区：中国

指导教师姓名：黎洪键

凌明灿

指导教师单位：华南师范大学数科院

广东实验中学

论文题目：

整数环上一类矩阵方程

$X^n + Y^n = \lambda^n I$

$(n \in N,\ \lambda \in Z,\ \lambda \neq 0)$的解

整数环上一类矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0)$的解

刘若霆

广东实验中学

摘要

设$\mathbb{Z},\mathbb{N}$分别是全体整数和正整数的集合,$M_n(\mathbb{Z})$表示$\mathbb{Z}$上n阶方阵的集合,本文运用Fermat大定理证明了下面的二阶矩阵方程只有平凡解:$X^n+Y^n=\lambda^n I(n\in\mathbb{N},n\geq 3,\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z}))$,其中整数矩阵$X_{2\times 2}$有一个特征值为整数;特别地,当$\lambda=1$时,利用本原素因子的性质可以把二阶矩阵方程$X^n+Y^n=I(n\in\mathbb{N},n\geq 3,X,Y\in M_2(\mathbb{Z}))$的解确定下来.通过构造整数矩阵的方法,证明了下面的整数矩阵方程有无穷多组非平凡解:$X^n+Y^n=\lambda^n I(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_n(\mathbb{Z}))$; $X^n+Y^n=\lambda^n I(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0,n\in\mathbb{N},\gcd(n,6)=1)$; $X^3+Y^3=\lambda^3 I(X,Y\in M_n(\mathbb{Z}),n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0)$.

关键词: Fermet大定理 整数矩阵方程 不定方程 特征值 本原素因子

目录

1 引言

随着人们日益对信息安全重视程度的提高,密码技术也逐渐成为了一门独立的学科-密码学.整数矩阵方程在数论及密码体系的设计方面有着一定的应用.因此,对整数矩阵方程的研究具有十分重要的意义和价值.但目前关于整数矩阵方程的研究结果较少.设$\mathbb{Z},\mathbb{N}$分别是全体整数和正整数的集合,$GL_n(\mathbb{Z})$表示$\mathbb{Z}$上n阶可逆矩阵的集合,文献 [1]– [10]考虑一类特殊的整数矩阵集$S(A)=\left\{A^k|k,m\in\mathbb{N},A\in GL_m(\mathbb{Z})\right\}$上的Fermat方程$X^n+Y^n=Z^n(X,Y,Z\in S(A),n\in\mathbb{N})$的可解性问题,尹倩倩等在文献[11]中得出了与毕达哥拉斯方程相关的一类二阶整数矩阵方程$X^2\pm Y^2=\lambda I(\lambda\in\mathbb{Z},I$为单位矩阵)的全部解$(X,Y)$.本文在尹倩倩的基础上研究更一般的整数矩阵方程$X^n+Y^n=\lambda^nI(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq0,X,Y\in M_m(\mathbb{Z})$的可解性问题.

令$M_n(\mathbb{Z})$表示$\mathbb{Z}$上n阶矩阵的集合,对于整数矩阵方程

$$X^n+Y^n=\lambda^nI\,(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq0,X,Y\in M_m(\mathbb{Z})) \tag{1.1}$$

若$\det(X)=0$或$\det(Y)=0,\forall\lambda\in\mathbb{Z},\lambda\neq0$取矩阵

$$A=\begin{bmatrix}\lambda&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&0&0\end{bmatrix}_{m\times m},B=\begin{bmatrix}0&0&\cdots&0\\0&\lambda&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&\lambda\end{bmatrix}_{m\times m}$$

则(A,B,λ)是矩阵方程1.1的一组解,由于λ是任意的,因此方程1.1有无穷多组解,我们把这类解称为平凡解.本文主要研究整数矩阵方程1.1是否只有平凡解的情形.除特别说明外,本文所取的参数均默认是整数.

符号说明:I:单位矩阵;$\det(A)$:矩阵A的行列式;$\overline{z}$:复数z的共轭复数;$\gcd(a,b)$:整数a,b的最大公因数;ω:$\omega=\dfrac{-1+\sqrt{-3}}{2}$.

2 预备知识

定义1.[12] 设$a_{ij} \in \mathbb{Z}(i=0,1,2,\cdots m; j=1,2,\cdots n)$，则称$A=(a_{ij})_{m\times n}$为整数矩阵.当$m=n$时，称$A=(a_{ij})_{n\times n}$为$n$阶整数矩阵.

定义2. 称$(A,B,\lambda)(A,B\in M_m(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$是整数矩阵方程*1.1*的一组平凡解,若$\det(A)=0$或$\det(B)=0$;否则称为非平凡解.

定义3.[13] 全体$\mathbb{Q}$上的n次代数数组成的集合记作A_n,设$\alpha\in A_n$,它的不可约多项式

$$g(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0\in\mathbb{Q}[x]$$

(i)$g(x)$的n个根$\alpha^{(1)},\cdots,\alpha^{(n)}$称为是$\alpha$在$\mathbb{Q}$上的共轭数,也说是$\alpha$的绝对共轭数;
*(ii)*把

$$T(\alpha)=\alpha^{(1)}+\cdots+\alpha^{(n)}$$

称为是α在$\mathbb{Q}$上的迹或α的绝对迹;把

$$N(\alpha)=\alpha^{(1)}\cdots\alpha^{(n)}$$

称为是α在$\mathbb{Q}$上的范数或α的绝对范数.

我们有

$$T(\alpha+\beta)=T(\alpha)+T(\beta);N(\alpha\beta)=N(\alpha)N(\beta)$$

引理1.[13] 全体$\mathbb{Q}$上的n次代数整数组成的集合记作$\tilde{A}_n$,若$\alpha\in\tilde{A}_n$,则它的共轭数也属于$\tilde{A}_n$,且它的迹与范数都是有理整数.

引理2.[13] 设$d\neq 0,1$是无平方因子的有理整数,令

$$w=\begin{cases}\sqrt{d}, & d\equiv 2,3(\bmod 4)\\ -1/2+\sqrt{d}/2, & d\equiv 1(\bmod 4)\end{cases}$$

那么,α是二次代数整数的充要条件是它可表为

$$\alpha=m+nw, m,n\in\mathbb{Z}, n\neq 0$$

引理3.[14] 设二阶整数矩阵$A=\begin{bmatrix}a & b\\ c & d\end{bmatrix}$的特征值为$x_1,x_2$,记

$$A^n=\begin{bmatrix}f_1^{(n)} & f_2^{(n)}\\ f_3^{(n)} & f_4^{(n)}\end{bmatrix}(n\in\mathbb{N})$$

(1) 当$x_1 = x_2$时,

$$\begin{cases} f_1^{(n)} = \left(1 + \dfrac{n(a - x_1)}{x_1}\right) x_1^n \\ f_2^{(n)} = bnx_1^{n-1} \\ f_3^{(n)} = cnx_1^{n-1} \\ f_4^{(n)} = \left(1 + \dfrac{n(d - x_1)}{x_1}\right) x_1^n \end{cases}$$

(2) 当$x_1 \neq x_2$时,

$$\begin{cases} f_1^{(n)} = \dfrac{a - x_2}{x_1 - x_2} x_1^n - \dfrac{a - x_1}{x_1 - x_2} x_2^n \\ f_2^{(n)} = \dfrac{b}{x_1 - x_2}(x_1^n - x_2^n) \\ f_3^{(n)} = \dfrac{c}{x_1 - x_2}(x_1^n - x_2^n) \\ f_4^{(n)} = \dfrac{d - x_2}{x_1 - x_2} x_1^n - \dfrac{d - x_1}{x_1 - x_2} x_2^n \end{cases}$$

引理4.[15] Fermet 大定理：当$n \geq 3$时，不定方程

$$x^n + y^n = z^n$$

除$xyz = 0$的解外,没有其它的整数解(x, y, z).

引理5.[15] 不定方程

$$x^4 - y^4 = z^2$$

除$xyz = 0$的解外,没有其它的整数解(x, y, z).

引理6.[16] 行列式

$$\begin{vmatrix} x & 0 & 0 & \cdots & 0 & a_0 \\ -1 & x & 0 & \cdots & 0 & a_1 \\ 0 & -1 & x & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x & a_{n-2} \\ 0 & 0 & 0 & \cdots & -1 & x + a_{n-1} \end{vmatrix} = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

推论1. 任意一个n次首一整系数多项式$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$,其中$a_i \in \mathbb{Z}, i = 0, 1, 2, \cdots n-1$, 则存在一个$n$阶整数方阵$A$, 使得矩阵$A$的特征多项式为$f(x)$.

证明: 取矩阵

$$A=\begin{bmatrix}0&0&0&\cdots&0&-a_0\\1&0&0&\cdots&0&-a_1\\0&1&0&\cdots&0&-a_2\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&\cdots&0&-a_{n-2}\\0&0&0&\cdots&1&-a_{n-1}\end{bmatrix}$$

由引理6得,矩阵A的特征多次项式为$f(x)=\det(xI-A)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$. ■

引理7. [16] 设A是数域P上一个$n\times n$矩阵,$f(x)=\det(xI-A)$是A的特征多项式,则$f(A)=0$.

引理8. [16] 每一个n阶复矩阵A都与一个若尔当形矩阵相似.

推论2. 若$(A_{m\times m},B_{m\times m},\lambda)$是矩阵方程$X^n+Y^n=\lambda^nI(m,n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq0,X,Y\in M_m(\mathbb{Z}))$的解,设$\lambda_1,\cdots,\lambda_m(\lambda_1,\cdots,\lambda_m\in\mathbb{C})$ 和$\mu_1,\cdots,\mu_m(\mu_1,\cdots,\mu_m\in\mathbb{C})$分别是矩阵$A$和矩阵$B$ 的特征值,则有$(\lambda_i,\mu_i)(i=1,2,\cdots,m)$是方程

$$x^n+y^n=\lambda^n\,(x,y\in\mathbb{C}) \tag{2.1}$$

的解.

证明: 由引理8可得,存在一个复可逆矩阵$P\in M_m(\mathbb{C})$,使得

$$A=P\begin{bmatrix}\lambda_1&&&\\&\lambda_2&&*\\&&\ddots&\\0&&&\lambda_m\end{bmatrix}P^{-1} \tag{2.2}$$

对于式子2.2,我们只关心对角线上的元素,元素$*$我们不关心（下同）,由$A^n+B^n=\lambda^nI$得,

$$\begin{bmatrix}\lambda_1^n&&&\\&\lambda_2^n&&*\\&&\ddots&\\0&&&\lambda_m^n\end{bmatrix}+P^{-1}Y^nP=\lambda^nI \tag{2.3}$$

因此

$$P^{-1}Y^nP=\begin{bmatrix}\lambda^n-\lambda_1^n & & & \\ & \lambda^n-\lambda_2^n & & * \\ & & \ddots & \\ & 0 & & \lambda^n-\lambda_m^n\end{bmatrix} \tag{2.4}$$

由式子2.4可得,矩阵B^n的特征值为

$$\lambda^n-\lambda_1^n,\cdots,\lambda^n-\lambda_m^n\,(\lambda_1,\cdots,\lambda_m\in\mathbb{C}) \tag{2.5}$$

由矩阵B的特征值为$\mu_1,\cdots,\mu_m,(\mu_1,\cdots,\mu_m\in\mathbb{C}))$ 可知,矩阵B^n的特征值为

$$\mu_1^n,\cdots,\mu_m^n,(\mu_1,\cdots,\mu_m\in\mathbb{C})) \tag{2.6}$$

式子2.5和2.6两者比较可得,

$$\lambda_i^n+\mu_i^n=\lambda^n\,(i=1,2,\cdots,m)$$

即$(\lambda_i,\mu_i)\,(i=1,2,\cdots,m)$是方程2.1的解. ■

引理9. *若矩阵方程1.1有一组非平凡解(A,B,λ),则方程1.1 有无穷多组非平凡解.*

证明: $\forall t\in\mathbb{N}$,我们有$\left(10^tA,10^tB,10^t\lambda\right)$是矩阵方程1.1的一组非平凡解,由于$t$是任意的,因此方程1.1有无穷多组非平凡解. ■

定义4. [17] *设α和β是代数整数,若$\alpha+\beta$和$\alpha\beta$是互素的有理整数,且$\frac{\alpha}{\beta}$不是一个单位根,我们称(α,β)是Lucas数偶;若$(\alpha+\beta)^2$和$\alpha\beta$是互素的有理整数,且$\frac{\alpha}{\beta}$不是一个单位根,我们称(α,β)是Lehmer数偶.*

对于给定的Lucas数偶(α,β),相应的Lucas序列通项可以定义为

$$u_n=u_n(\alpha,\beta)=\frac{\alpha^n-\beta^n}{\alpha-\beta}(n=0,1,2,\cdots)$$

对于给定的Lehmer数偶(α,β),相应的Lehmer序列通项可以定义为

$$\tilde{u}_n=\tilde{u}_n(\alpha,\beta)=\begin{cases}\dfrac{\alpha^n-\beta^n}{\alpha-\beta} & \text{当}n\text{为奇数时,}\\ \dfrac{\alpha^n-\beta^n}{\alpha^2-\beta^2} & \text{当}n\text{为偶数时.}\end{cases}$$

定义5. [17] 设Lucas数偶(α,β),若素数p整除$u_n(\alpha,\beta)$,但是不能够整除$(\alpha-\beta)^2 u_1\cdots u_{n-1}$,则称$p$是Lucas数$u_n(\alpha,\beta)$的本原素因子;设Lehmer数偶$(\alpha,\beta)$,若素数$p$整除$\tilde{u}_n(\alpha,\beta)$, 但是不能够整除$\left(\alpha^2-\beta^2\right)^2\tilde{u}_1\cdots\tilde{u}_{n-1}$,则称$p$是Lehmer数$\tilde{u}_n$的本原素因子.

引理10. [17] (本原素因子的存在性定理)当$n>30$时,第n个Lucas数或Lehmer数都有本原素因子.而且,当$n\leq 30$时,没有本原素因子的Lucas数或Lehmer数能够清楚地决定出来.当$5<n\leq 30$时,文[17]提供了没有本原素因子的Lucas数或Lehmer数的一个完整列表.

3 二阶矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},n\geq 3,\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z}))$的解

定理1. 当矩阵$X_{2\times 2}$有一个特征值为整数时,二阶矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},n\geq 3,\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z}))$只有平凡解.

证明: 不妨设矩阵X和矩阵Y的特征值分别为λ_1,λ_2,和$\mu_1,\mu_2,(\mu_1,\mu_2\in\mathbb{C})$其中$\lambda_1\in\mathbb{Z},\lambda_2\in\mathbb{C},\lambda_1,\lambda_2\neq 0$,由于$\lambda_1\in\mathbb{Z}$,因此$\lambda_2$也是整数, 由于矩阵$B$的特征多项式是首一二次整系数多项式,因此$\mu_1$在某个二次代数数域$\mathbb{Q}[\sqrt{m}]$($m$为不含平方因子的非零整数)上且$\mu_1$为代数整数,由推论2可得,

$$\lambda^n-\lambda_1^n=\mu_1^n\left(\lambda,\lambda_1\in\mathbb{Z},\lambda,\lambda_1\neq 0,\mu_1\in\mathbb{Q}[\sqrt{m}]\right) \tag{3.1}$$

(由于$\lambda_1,\lambda_2\in\mathbb{Z}$,因此其它情形可以类似讨论)

对式子3.1两边同时取范数(在$\mathbb{Q}[\sqrt{m}]$上考虑),得

$$\left(\lambda^n-\lambda_1^n\right)^2=\left(N(\mu_1)\right)^n\left(\lambda,\lambda_1,N(\mu_1)\in\mathbb{Z},\lambda,\lambda_1\neq 0\right) \tag{3.2}$$

(由于μ_1为代数整数,因此$N(\mu_1)$为整数)

下面对式子3.2进行讨论:

(1) 当n为奇数时,由式3.2可知,$N(\mu_1)$为完全平方数,不妨设$N(\mu_1)=X_1^2$,于是式3.2变为

$$\mid\lambda^n-\lambda_1^n\mid=\mid X_1\mid^n\left(\lambda,\lambda_1,N(\mu_1)\in\mathbb{Z},\lambda,\lambda_1\neq 0\right) \tag{3.3}$$

由于$n\geq 3$,由引理4(费马大定理)可得,$X_1=0$,则$N(\mu_1)=0$,于是$\mu_1=0$,此时矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},n\geq 3,\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z}))$只有平凡解.

(2) 当n为偶数时,令$n=2m(m\geq 2)$

① 当$m=2$时,式3.2变为

$$\lambda^4-\lambda_1^4=\left(N(\mu_1)\right)^2\left(\lambda,\lambda_1,N(\mu_1)\in\mathbb{Z},\lambda,\lambda_1\neq 0\right) \tag{3.4}$$

由引理5可知,$N(\mu_1)=0$,于是$\mu_1=0$,此时矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},n\geq 3,\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z}))$只有平凡解.

② 当$m\geq 3$时,式3.2变为

$$\left(\lambda^2\right)^m-\left(\lambda_1^2\right)^m=\left(N(\mu_1)\right)^m\left(\lambda,\lambda_1,N(\mu_1)\in\mathbb{Z},\lambda,\lambda_1\neq 0\right)\tag{3.5}$$

由引理4(费马大定理)可得,$N(\mu_1)=0$,于是$\mu_1=0$,此时矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},n\geq 3,\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z}))$只有平凡解.

综上,当矩阵$X_{2\times 2}$有一个特征值为整数时,矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},n\geq 3,\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z}))$只有平凡解. ■

推论3. 令$\begin{cases} m=2m_1 \\ n=m_1 t \end{cases}(m_1,t\in\mathbb{Z},m_1\geq 1,t\geq 3)$,当矩阵$X_{m\times m}$的特征值全为整数时,矩阵方程$X^n+Y^n=\lambda^n I(\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_m(\mathbb{Z}))$只有平凡解.

证明: 不妨设矩阵X和矩阵Y的特征值分别为$\lambda_1,\cdots,\lambda_m(\lambda_1,\cdots,\lambda_m\in\mathbb{Z},\lambda_1\cdots\lambda_m\neq 0)$和$\mu_1,\cdots,\mu_m,(\mu_1,\cdots,\mu_m\in\mathbb{C})$,由于矩阵$B$的特征多项式是$m$次首一整系数多项式,因此$\mu_1$在某个$m$次代数数域$\mathbb{F}$上且$\mu_1$为代数整数,由推论2可得,

$$\lambda^n-\lambda_1^n=\mu_1^n\left(\lambda,\lambda_1\in\mathbb{Z},\lambda,\lambda_1\neq 0,\mu_1\in\mathbb{F}\right)\tag{3.6}$$

对式子3.6两边同时取范数(在$\mathbb{F}$上考虑),得

$$(\lambda^n-\lambda_1^n)^m=\left(N(\mu_1)\right)^n\left(\lambda,\lambda_1,N(\mu_1)\in\mathbb{Z},\lambda,\lambda_1\neq 0\right)\tag{3.7}$$

(由于μ_1为代数整数,因此$N(\mu_1)$为整数)
即

$$(\lambda^n-\lambda_1^n)^{2m_1}=\left(N(\mu_1)\right)^{m_1 t}\left(\lambda,\lambda_1,N(\mu_1)\in\mathbb{Z},\lambda,\lambda_1\neq 0\right)\tag{3.8}$$

式子3.8可以类似于定理1进行讨论,那么可以得到$\mu_1=0$,于是矩阵方程$X^n+Y^n=\lambda^n I(\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_m(\mathbb{Z}))$只有平凡解. ■

注1. 当$m_1=1$时,即$\begin{cases} m=2 \\ n=t \end{cases}(t\in\mathbb{Z},t\geq 3)$,矩阵方程$X^n+Y^n=\lambda^n I(\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_m(\mathbb{Z}))$就是定理1的情形.

注2. 记矩阵

$$X^n=\begin{bmatrix} f_1^{(n)} & f_2^{(n)} \\ f_3^{(n)} & f_4^{(n)} \end{bmatrix},Y^n=\begin{bmatrix} g_1^{(n)} & g_2^{(n)} \\ g_3^{(n)} & g_4^{(n)} \end{bmatrix}$$

由引理3可知,求解二阶矩阵方程$X^n+Y^n=\lambda^n I\,(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z}))$的问题可以转化为求解方程组

$$\begin{cases} f_1^{(n)}+g_1^{(n)}=\lambda^n \\ f_2^{(n)}+g_2^{(n)}=0 \\ f_3^{(n)}+g_3^{(n)}=0 \\ f_4^{(n)}+g_4^{(n)}=\lambda^n \end{cases}$$

的问题.

定理2. 对于二阶矩阵方程

$$X^n+Y^n=\lambda^n I(n\in\mathbb{N},n\geq 3,\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_2(\mathbb{Z})) \tag{3.9}$$

设$(A_{2\times 2},B_{2\times 2},1)$是方程3.9的一组解,令

$$P=\left\{(\omega,\overline{\omega}),(-\overline{\omega},-\omega),\left(\frac{1+\sqrt{-7}}{2},\frac{1-\sqrt{-7}}{2}\right),\left(\frac{-1+\sqrt{-7}}{2},\frac{-1-\sqrt{-7}}{2}\right)\right\}$$

则

① 矩阵A和矩阵B的特征值分别为(λ,μ)和(μ,λ),其中$(\lambda,\mu)\in P$;

② 矩阵A和矩阵B在复数域$\mathbb{C}$上分别相似于

$$\begin{bmatrix} \lambda & 0 \\ 0 & \mu \end{bmatrix} 和 \begin{bmatrix} \mu & 0 \\ 0 & \lambda \end{bmatrix}.$$

证明: 不妨设矩阵A和矩阵B的特征值分别为λ_1,λ_2和μ_1,μ_2,其中$\lambda_i(i=1,2)$和$\mu_i(i=1,2)$均为二次代数整数,由式子2.1可得,$\lambda_i(i=1,2)$和$\mu_i(i=1,2)$在同一个二次代数数域$\mathbb{Q}[\sqrt{D}]$(D为不含平方因子的非零整数)上,下面分情况进行讨论:

(1) 当$D\equiv 2,3(\bmod 4)$时,由引理2可得$\lambda_1=a+b\sqrt{D}(a,b\in\mathbb{Z})$和$\mu_1=c+d\sqrt{D}(c,d\in\mathbb{Z})$,由式子2.1可得,

$$\left(a+b\sqrt{D}\right)^n+\left(c+d\sqrt{D}\right)^n=1(a,b,c,d\in\mathbb{Z}) \tag{3.10}$$

下面对方程3.10进行讨论:

① 当$D>0$时,

(i) 当n为偶数时,我们可以要求$a\geq,b>0$(我们可以取实共轭)则有

$$\begin{cases}|a+b\sqrt{D}|\leq 1\\ |c+d\sqrt{D}|\leq 1\end{cases} \tag{3.11}$$

由于$D>0,D\equiv 2,3(\bmod 4),a\geq 0,b>0$,因此这种情况是不可能的.

(ii) 当n为奇数时,我们可以考虑$a\geq 0,b>0$的情形,此时方程3.10变为

$$\left(a+b\sqrt{D}\right)^n+\left(c+d\sqrt{D}\right)^n=\pm 1(a,b,c,d\in\mathbb{Z}) \tag{3.12}$$

令

$$\left(a+b\sqrt{D}\right)^n=a_n+b_n\sqrt{D}(a_n,b_n\in\mathbb{Z},a_n\leq 0,b_n>0) \tag{3.13}$$

$$\left(c+d\sqrt{D}\right)^n=c_n+d_n\sqrt{D}(c_n,d_n\in\mathbb{Z}) \tag{3.14}$$

下面对方程3.12,式子3.13和式子3.14进行讨论:

情形一:当$c\leq 0,d>0$时,则有$c_n\leq 0,d_n>0$,这是不可能的.

情形二:当$c\geq 0,d>0$时,则有$c_n\geq 0,d_n>0$,这是不可能的.

情形三:当$c\geq 0,d<0$时,则有$c_n\geq 0,d_n<0$,于是方程3.12变为

$$a_n+c_n=1 \tag{3.15}$$

由于$a_n\geq 0,c_n\geq 1,n\geq 3$,由二项展开式可知,方程3.15是不可能的.

情形四:当$c\leq 0,d<0$时,式子3.12变为

$$\left(a+b\sqrt{D}\right)^n-\left(c_1+d_1\sqrt{D}\right)^n=\pm 1(c_1=-c,d_1=-d,c_1\geq 0,d_1>0) \tag{3.16}$$

我们可以假设$a+b\sqrt{D}\geq c_1+d_1\sqrt{D}$,式子3.16变为

$$\left(a-c_1+(b-d_1)\sqrt{D}\right)(\lambda_1^{n-1}+\cdots+\mu_1^{n-1})=1 \tag{3.17}$$

有理化可得,

$$\frac{(a-c_1)^2-(b-d_1)^2D}{a-c_1-(b-d_1)\sqrt{D}}(\lambda_1^{n-1}+\cdots+\mu_1^{n-1})=1 \tag{3.18}$$

对式子3.17两边取范数可知,

$$N(a-c_1+(b-d_1)\sqrt{D})=(a-c_1)^2-(b-d_1)^2D=\pm 1 \tag{3.19}$$

结合式子3.18和3.19可得,

$$\frac{1}{|a-c_1-(b-d_1)\sqrt{D}|}(\lambda_1^{n-1}+\cdots+\mu_1^{n-1})=1 \tag{3.20}$$

对于式子3.20:

$$|a-c_1-(b-d_1)\sqrt{D}|\leq|a-c_1|+|b-d_1|\sqrt{D}\leq a+c_1+(b+d_1)\sqrt{D}\leq 2(a+b\sqrt{D})=2\lambda_1 \tag{3.21}$$

当$n\geq 4$时,由式子3.20和不等式3.21可知

$$1\geq\frac{\lambda_1^{n-1}+\cdots+\mu_1^{n-1}}{2\lambda_1}>\frac{\lambda_1^{n-1}}{2\lambda_1}=\frac{\lambda_1^{n-2}}{2}\geq\frac{(\sqrt{2})^{n-2}}{2}\geq\frac{(\sqrt{2})^2}{2}=1$$

矛盾!

当$n=3$时,由式子3.20和不等式3.21可知

$$1\geq\frac{\lambda_1^2+\lambda_1\mu_1+\mu_1^2}{2\lambda_1}\geq\frac{\lambda_1^2+2+2}{2\lambda_1}=\frac{1}{2}(\lambda_1+\frac{4}{\lambda_1})\geq\sqrt{4}=2$$

矛盾!

② 当$D<0$时,

(i) 当n为偶数时,可以归结为$n=2$的情形:此时方程3.10变为:

$$\left(a+b\sqrt{D}\right)^2+\left(c+d\sqrt{D}\right)^2=1(a,b,c,d\in\mathbb{Z}) \tag{3.22}$$

由方程3.22可得,

$$\begin{cases}ab+cd=0\\a^2+c^2+(b^2+d^2)D=1\end{cases} \tag{3.23}$$

由方程3.22可得,

$$\begin{aligned}1&=\left|\left(a+b\sqrt{D}\right)^2+\left(c+d\sqrt{D}\right)^2\right|\geq\left|a+b\sqrt{D}\right|^2-\left|c+d\sqrt{D}\right|^2\\&=a^2-b^2D-(c^2-b^2D)\end{aligned} \tag{3.24}$$

(这里不妨设$a^2-b^2D\geq c^2-b^2D$)

下面对式子3.23和不等式3.24进行讨论:

情形一:当

$$\begin{cases}a^2-b^2D=c^2-b^2D\\a^2+c^2+(b^2+d^2)D=1\\ab+cd=0\end{cases} \tag{3.25}$$

时,由式子3.25可以得到,

$$2a^2+2d^2D=1$$

这是不可能的.

情形二：当

$$\begin{cases} a^2-b^2D=c^2-b^2D+1 \\ a^2+c^2+(b^2+d^2)D=1 \\ ab+cd=0 \end{cases} \tag{3.26}$$

时,由式子3.26可以得到,

$$\begin{cases} a^2+d^2D=1 \\ c^2+b^2D=0 \end{cases} \tag{3.27}$$

此时$D=-1$,于是式子3.27变为

$$\begin{cases} a^2-d^2=1 \\ c^2-b^2=0 \\ ab+cd=0 \end{cases} \tag{3.28}$$

由方程3.28可以得到$b=c=d=0$,这是不可能的.

(ii) 当n为奇数时,由方程3.10可以得到

$$\begin{aligned} 1&=\left|\left(a+b\sqrt{D}\right)^n+\left(c+d\sqrt{D}\right)^n\right|\geq\left|a+b\sqrt{D}\right|^n-\left|c+d\sqrt{D}\right|^n \\ &=\left(a^2-b^2D\right)^{\frac{n}{2}}-\left(c^2-b^2D\right)^{\frac{n}{2}}=\frac{(a^2-b^2D)^n-(c^2-b^2D)^n}{(a^2-b^2D)^{\frac{n}{2}}+(c^2-b^2D)^{\frac{n}{2}}} \\ &=\frac{(a^2-b^2D-c^2+d^2D)\left[(a^2-b^2D)^{n-1}+\cdots+(c^2-b^2D)^{n-1}\right]}{(a^2-b^2D)^{\frac{n}{2}}+(c^2-b^2D)^{\frac{n}{2}}} \end{aligned} \tag{3.29}$$

(这里不妨设$a^2-b^2D\geq c^2-b^2D$)

令

$$\begin{cases} t=a^2-b^2D \\ s=c^2-b^2D \end{cases}$$

当$t-s\geq 1(s\geq 1)$时, 下面对不等式3.29进行讨论：

情形一：当$n>3$时,由不等式3.29可得,

$$1\geq\frac{t^{n-1}+\cdots+s^{n-1}}{2t^{\frac{n}{2}}}>\frac{t^{\frac{n}{2}-1}}{2}\geq\frac{2^{\frac{n}{2}-1}}{2}=2^{\frac{n}{2}-2}\geq\sqrt{2}$$

这是不可能的.

情形二：当$n=3$时,由不等式3.29可得,

$$1\geq\frac{t^2+ts+s^2}{t^{\frac{3}{2}}+s^{\frac{3}{2}}}\geq\frac{t^2+3}{2t^{\frac{3}{2}}}(t\geq 2) \tag{3.30}$$

令$f(t)=\dfrac{t^2+3}{2t^{\frac{3}{2}}}(t\geq 2)$,$f'(t)=\dfrac{t^{-\frac{1}{2}}(1-\frac{9}{t^2})}{4}$,

当$t\geq 3$时,$f'(t)\geq 0$,此时,$f(t)\geq f(3)=\dfrac{2\sqrt{3}}{3}>1$, 这与不等式3.30矛盾!

当$t=2$时,$f(t)=f(2)=\dfrac{7\sqrt{2}}{8}>1$,这与不等式3.30矛盾!

综上,$t=s$,即$a^2-b^2D=c^2-b^2D$.

由方程3.10可以得到

$$\left(a+c+(b+d)\sqrt{D}\right)(\frac{\lambda_1^n+\mu_1^n}{\lambda_1+\mu_1})=1 \tag{3.31}$$

对方程3.31两边取范数可得,

$$N(a+c+(b+d)\sqrt{D})=1$$

即

$$(a+c)^2-(b+d)^2D=1 \tag{3.32}$$

注意到方程3.32只有解：$(\pm 1,0,D)$和$(0,\pm 1,-1)$,下面对这两种情形进行讨论：

情形一：当

$$\begin{cases}a+c=1\\ b+d=0\\ a^2-b^2D=c^2-b^2D\end{cases}$$

($a+c=-1$可以同样讨论)

时,可以得到,$2a=1$,这是不可能的.

情形二：当

$$\begin{cases}a+c=0\\ b+d=1\\ D=-1\\ a^2-b^2D=c^2-b^2D\end{cases}$$

($b+d=-1$可以同样讨论)

时,可以得到,$2b=1$,这是不可能的.

综上,当$D\equiv 2,3(\bmod 4)$时,方程3.10不可能成立!

(2) 当$D\equiv 1(\bmod 4)$时,由引理2可得$\lambda_1=\dfrac{a+b\sqrt{D}}{2}(a,b\in\mathbb{Z},2|(a+b))$和$\mu_1=\dfrac{c+d\sqrt{D}}{2}(c,d\in\mathbb{Z},2|(c+d))$, 由式子2.1可得,

$$\left(\frac{a+b\sqrt{D}}{2}\right)^n+\left(\frac{c+d\sqrt{D}}{2}\right)^n=1(a,b,c,d\in\mathbb{Z}) \tag{3.33}$$

下面对方程3.33进行讨论:

① 当$D>0$时,

(i) 当n为偶数时,我们可以要求$a\geq,b>0$(我们可以取实共轭)则有

$$\begin{cases}|a+b\sqrt{D}|\leq 2\\ |c+d\sqrt{D}|\leq 2\end{cases} \tag{3.34}$$

由于$D>0,D\equiv 1(\bmod 4),a\geq 0,b>0$,因此这种情况是不可能的.

(ii) 当n为奇数时,我们可以考虑$a\geq 0,b>0$的情形,此时方程3.33变为

$$\left(\frac{a+b\sqrt{D}}{2}\right)^n+\left(\frac{c+d\sqrt{D}}{2}\right)^n=\pm 1(a,b,c,d\in\mathbb{Z}) \tag{3.35}$$

令

$$\left(\frac{a+b\sqrt{D}}{2}\right)^n=\frac{a_n+b_n\sqrt{D}}{2}(a_n,b_n\in\mathbb{Z},a_n\leq 0,b_n>0) \tag{3.36}$$

$$\left(\frac{c+d\sqrt{D}}{2}\right)^n=\frac{c_n+d_n\sqrt{D}}{2}(c_n,d_n\in\mathbb{Z}) \tag{3.37}$$

下面对方程3.35,式子3.36和式子3.37进行讨论:

情形一:当$c\leq 0,d>0$时,则有$c_n\leq 0,d_n>0$,这是不可能的.

情形二:当$c\geq 0,d>0$时,则有$c_n\geq 0,d_n>0$,这是不可能的.

情形三:当$c\geq 0,d<0$时,则有$c_n\geq 0,d_n<0$,于是方程3.35变为

$$\frac{a_n+c_n}{2}=1 \tag{3.38}$$

若$a=c=0$,则方程3.33变为

$$\left(\frac{b\sqrt{D}}{2}\right)^n+\left(\frac{d\sqrt{D}}{2}\right)^n=1(a,b,c,d\in\mathbb{Z})$$

由于n是奇数,因此这是不可能的.因此$a\geq 1$或$c\geq 1$,不妨设$a\geq 1$, 由式子3.35可得,

当$n\geq 5$时,

$$\begin{aligned} a_n &= \frac{a^n+\binom{n}{2}a^{n-2}b^2D+\binom{n}{4}a^{n-4}b^2D^2+\cdots+\binom{n}{n-1}ab^{n-1}D^{\frac{n-1}{2}}}{2^{n-1}} \\ &\geq \frac{1+\binom{n}{2}D+\binom{n}{4}D^2+\cdots+\binom{n}{n-1}D^{\frac{n-1}{2}}}{2^{n-1}} \\ &\geq \frac{5\left(1+\binom{n}{2}+\binom{n}{4}+\cdots+\binom{n}{n-1}\right)}{2^{n-1}}=5 \end{aligned} \tag{3.39}$$

当$n=3$时,

$$a_3=\frac{a^3+\binom{3}{2}ab^2D}{2^2}=\frac{a^3+3ab^2D}{4}\geq\frac{1+3\cdot 5}{4}=4 \tag{3.40}$$

综合3.39和3.40得,$a_n\geq 4$,因此方程3.38不可能成立.

情形四：当$c\leq 0,d<0$时,方程3.35变为

$$\left(\frac{a+b\sqrt{D}}{2}\right)^n-\left(\frac{c_1+d_1\sqrt{D}}{2}\right)^n=\pm 1(c_1=-c,d_1=-d,c_1\geq 0,d_1>0) \tag{3.41}$$

我们可以假设$a+b\sqrt{D}\geq c_1+d_1\sqrt{D}$,式子3.41变为

$$\frac{\left(a-c_1+(b-d_1)\sqrt{D}\right)}{2}(\lambda_1^{n-1}+\cdots+\mu_1^{n-1})=1 \tag{3.42}$$

有理化可得,

$$\frac{(a-c_1)^2-(b-d_1)^2D}{2\left[a-c_1-(b-d_1)\sqrt{D}\right]}(\lambda_1^{n-1}+\cdots+\mu_1^{n-1})=1 \tag{3.43}$$

对式子3.42两边取范数可知,

$$N\left(\frac{a-c_1+(b-d_1)\sqrt{D}}{2}\right)=\frac{(a-c_1)^2-(b-d_1)^2D}{4}=\pm 1 \tag{3.44}$$

结合式子3.43和3.44可得,

$$\frac{2}{|a-c_1-(b-d_1)\sqrt{D}|}(\lambda_1^{n-1}+\cdots+\mu_1^{n-1})=1 \tag{3.45}$$

对于式子3.45:

$$|a-c_1-(b-d_1)\sqrt{D}|\leq|a-c_1|+|b-d_1|\sqrt{D}\leq a+c_1+(b+d_1)\sqrt{D}\leq 2(a+b\sqrt{D})=4\lambda_1 \tag{3.46}$$

当$n\geq 4$时,由式子3.45和不等式3.46可知

$$\begin{aligned}1&\geq\frac{\lambda_1^{n-1}+\lambda_1^{n-2}\mu_1+\cdots+\lambda_1\mu_1^{n-2}+\mu_1^{n-1}}{2\lambda_1}>\frac{\lambda_1^{n-1}+\lambda_1^{n-2}\mu_1+\cdots+\lambda_1\mu_1^{n-2}}{2\lambda_1}\\&=\frac{\lambda_1^{n-2}+\lambda_1^{n-3}\mu_1+\cdots+\lambda_1\mu_1^{n-2}}{2}>\frac{\lambda_1^{n-2}+\mu_1^{n-2}}{2}\\&\geq\frac{(\frac{\sqrt{5}}{2})^{n-2}+(\frac{\sqrt{5}}{2})^{n-2}}{2}\geq\frac{(\frac{\sqrt{5}}{2})^2+(\frac{\sqrt{5}}{2})^2}{2}=\frac{5}{4}\end{aligned} \tag{3.47}$$

矛盾!

当$n=3$时,由式子3.45和不等式3.46可知

$$1\geq\frac{\lambda_1^2+\lambda_1\mu_1+\mu_1^2}{2\lambda_1}\geq\frac{\lambda_1^2+\frac{5}{2}}{2\lambda_1}=\frac{1}{2}(\lambda_1+\frac{\frac{5}{2}}{\lambda_1})\geq\frac{\sqrt{10}}{2}$$

矛盾!

② 当$D<0$时,

(i) 当n为奇数时,由方程3.33可以得到

$$\begin{aligned}1&=\left|\left(\frac{a+b\sqrt{D}}{2}\right)^n+\left(\frac{c+d\sqrt{D}}{2}\right)^n\right|\geq\left|\frac{a+b\sqrt{D}}{2}\right|^n-\left|\frac{c+d\sqrt{D}}{2}\right|^n\\&=\left(\frac{a^2-b^2D}{4}\right)^{\frac{n}{2}}-\left(\frac{c^2-b^2D}{4}\right)^{\frac{n}{2}}=\frac{\left(\frac{a^2-b^2D}{4}\right)^n-\left(\frac{c^2-b^2D}{4}\right)^n}{\left(\frac{a^2-b^2D}{4}\right)^{\frac{n}{2}}+\left(\frac{c^2-b^2D}{4}\right)^{\frac{n}{2}}}\\&=\frac{\frac{a^2-b^2D-c^2+d^2D}{4}\left[\left(\frac{a^2-b^2D}{4}\right)^{n-1}+\cdots+\left(\frac{c^2-b^2D}{4}\right)^{n-1}\right]}{\left(\frac{a^2-b^2D}{4}\right)^{\frac{n}{2}}+\left(\frac{c^2-b^2D}{4}\right)^{\frac{n}{2}}}\end{aligned} \tag{3.48}$$

(这里不妨设$a^2-b^2D\geq c^2-b^2D$)

令

$$\begin{cases}t=\dfrac{a^2-b^2D}{4}\\ s=\dfrac{c^2-b^2D}{4}\end{cases}$$

当$t-s\geq 1(s\geq 1)$时, 下面对不等式3.48进行讨论：

情形一：当$n>3$时,由不等式3.48可得,

$$1\geq\frac{t^{n-1}+\cdots+s^{n-1}}{2t^{\frac{n}{2}}}>\frac{t^{\frac{n}{2}-1}}{2}\geq\frac{2^{\frac{n}{2}-1}}{2}=2^{\frac{n}{2}-2}\geq\sqrt{2}$$

这是不可能的.

情形二：当$n=3$时,由不等式3.48可得,

$$1\geq\frac{t^2+ts+s^2}{t^{\frac{3}{2}}+s^{\frac{3}{2}}}\geq\frac{t^2+3}{2t^{\frac{3}{2}}}(t\geq 2)\tag{3.49}$$

令$f(t)=\dfrac{t^2+3}{2t^{\frac{3}{2}}}(t\geq 2)$,$f'(t)=\dfrac{t^{-\frac{1}{2}}(1-\frac{9}{t^2})}{4}$,

当$t\geq 3$时,$f'(t)\geq 0$,此时,$f(t)\geq f(3)=\dfrac{2\sqrt{3}}{3}>1$, 这与不等式3.49矛盾!

当$t=2$时,$f(t)=f(2)=\dfrac{7\sqrt{2}}{8}>1$,这与不等式3.49矛盾!

综上,$t=s$,即$a^2-b^2D=c^2-b^2D$. 由方程3.33可以得到

$$\left(\frac{a+c+(b+d)\sqrt{D}}{2}\right)(\frac{\lambda_1^n+\mu_1^n}{\lambda_1+\mu_1})=1\tag{3.50}$$

对方程3.50两边取范数可得,

$$N\left(\frac{a+c+(b+d)\sqrt{D}}{2}\right)=1$$

即

$$(a+c)^2-(b+d)^2D=4\tag{3.51}$$

注意到方程3.51只有解：$(\pm 2,0,D)$和$(\pm 1,\pm 1,-3)$,下面对这两种情形进行讨论：

情形一：当

$$\begin{cases}a+c=2\\ b+d=0\\ a^2-b^2D=c^2-d^2D\end{cases}\qquad\big(\text{对于}a+c=-2\text{可以同样讨论}\big)$$

时,可以得到,

$$\begin{cases}a=c=1\\ b=-d\end{cases}$$

于是方程3.33变为

$$\left(\frac{1+b\sqrt{D}}{2}\right)^n+\left(\frac{1-b\sqrt{D}}{2}\right)^n=1 \tag{3.52}$$

令$\alpha=\frac{1+b\sqrt{D}}{2},\beta=\frac{b\sqrt{D}-1}{2}$,于是方程3.52变为

$$\frac{\alpha^n-\beta^n}{\alpha-\beta}=1 \tag{3.53}$$

令

$$\tilde{u}_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}$$

下面对$\tilde{u}_n$进行讨论: 注意到

$$\begin{cases}(\alpha+\beta)^2=b^2D\\ \alpha\beta=\dfrac{b^2D-1}{4}\end{cases}$$

因此$(\alpha+\beta)^2$和$\alpha\beta$是互素的有理整数,

(I)若$\frac{\alpha}{\beta}$是一个单位根时,由于$D<0,D\equiv 1(\bmod 4)$,因此$D=-3$,可以得到

$$b(1-b)=0$$

于是$b=1(b=0$舍去$)$.此时有

$$\begin{cases}\lambda_1=\dfrac{1+\sqrt{-3}}{2}\\ \mu_1=\dfrac{1-\sqrt{-3}}{2}\end{cases}$$

(II)若$\frac{\alpha}{\beta}$不是一个单位根,则由定义5可知,(α,β)是Lehmer数偶,从而$\tilde{u}_n$是一个Lehmer序列的第n 项.由引理10可知,

当$n>30$时,$\tilde{u}_n$有一个本原素因子,由方程3.53可知,这是不可能的.对于$3\leq n\leq 30$,仅考虑指标$n=3,5,7,9,13,15$.

当$n=7,9,13,15$时,由引理10可知,$\tilde{u}_n$有一个本原素因子,由方程3.53 可知,这是不可能的.

当$n=3$时,方程3.52变为

$$\left(\frac{1+b\sqrt{D}}{2}\right)^3+\left(\frac{1-b\sqrt{D}}{2}\right)^3=1$$

可以得到

$$1+3b^2D=4(D<0,D\equiv 1(\bmod 4))$$

这是不可能的.

当$n=5$时,方程3.52变为

$$\left(\frac{1+b\sqrt{D}}{2}\right)^5+\left(\frac{1-b\sqrt{D}}{2}\right)^5=1$$

可以得到

$$b^2D(2+b^2D)=3(D<0,D\equiv 1(\bmod 4))$$

此时可以得到$D\mid 3$,因此可以得到

$$\begin{cases} D=-3 \\ b=\pm 1 \end{cases}$$

此时有

$$\begin{cases} \lambda_1=\dfrac{1+\sqrt{-3}}{2} \\ \mu_1=\dfrac{1-\sqrt{-3}}{2} \end{cases}$$

情形二：当

$$\begin{cases} a+c=1 \\ b+d=1 \\ D=-3 \\ a-c=3(d-b) \end{cases} \quad \left(\text{对于}\begin{cases} a+c=-1 \\ b+d=-1 \end{cases}\text{可以同样讨论}\right)$$

时,可以得到,

$$\begin{cases} a=3d-1 \\ b=1-d \\ c=2-3d \end{cases} \tag{3.54}$$

此时方程3.33变为

$$\left(\frac{3d-1+(1-d)\sqrt{-3}}{2}\right)^n+\left(\frac{2-3d+d\sqrt{-3}}{2}\right)^n=1 \tag{3.55}$$

下面对方程3.55进行讨论:

(a)当$\mid d\mid\geq 3$时,对方程3.55两边取$\bmod(\mid d\mid)$可得,

$$左\equiv\left(\frac{-1+\sqrt{-3}}{2}\right)^n+1=\omega^n+1 \tag{3.56}$$

当$3\nmid n$时,由方程3.55和式子3.56可知,这是不可能的.

当$3\mid n$时,式子3.56变为

$$左\equiv\left(\frac{-1+\sqrt{-3}}{2}\right)^n+1=\omega^n+1=2(\bmod\mid d\mid)\tag{3.57}$$

由方程3.55可知,这是不可能的.

(b)当$|d|=\pm 1$时,

当$d=1$时,由方程3.55可知,这种情况显然不成立.

当$d=-1$时,方程3.55变为

$$(-1+2\omega)^n+(2+\omega)^n=1\tag{3.58}$$

对方程3.58两边取$\bmod(2)$可得,

$$左\equiv -1+\omega^n(\bmod 2)\tag{3.59}$$

当$3\nmid n$时,由方程3.58和式子3.59可知,这是不可能的.

当$3\mid n$时,式子3.59变为

$$左\equiv -1+\omega^n=-1+1=0(\bmod 2)\tag{3.60}$$

由方程3.58可知,这是不可能的.

(c)当$|d|=\pm 2$时,

当$d=2$时,方程3.55变为

$$\left(\frac{5-\sqrt{-3}}{2}\right)^n+\left(\frac{-4+2\sqrt{-3}}{2}\right)^n=1\tag{3.61}$$

对方程3.61两边取$\bmod(3)$可得,

$$左\equiv 2\left(\frac{-1-\sqrt{-3}}{2}\right)^n=2\overline{\omega}^n(\bmod 3)\tag{3.62}$$

当$3\nmid n$时,由方程3.61和式子3.62可知,这是不可能的.

当$3\mid n$时,式子3.62变为

$$左\equiv 2\overline{\omega}^n=2(\bmod 3)\tag{3.63}$$

由方程3.61可知,这是不可能的.

当$d=-2$时,方程3.55变为

$$\left(\frac{-7+3\sqrt{-3}}{2}\right)^n+\left(\frac{8-2\sqrt{-3}}{2}\right)^n=1\tag{3.64}$$

对方程3.64两边取 mod (3)可得,

$$左\ \equiv 1+\left(\frac{-1+\sqrt{-3}}{2}\right)^n=1+\omega^n(\bmod 3) \tag{3.65}$$

当$3\nmid n$时,由方程3.64和式子3.65可知,这是不可能的.

当$3\mid n$时,式子3.65变为

$$左\ \equiv 1+\left(\frac{-1+\sqrt{-3}}{2}\right)^n=1+\omega^n=1+1=2(\bmod 3) \tag{3.66}$$

由方程3.64可知,这是不可能的.

综上,这种情况是不可能出现的.

(ii) 当n为偶数时,令$n=2^t n_1(t,n_1\in\mathbb{N},2\nmid n_1)$,

(I)若$n_1\geq 3$, 令

$$\begin{cases}\left(\dfrac{a+b\sqrt{D}}{2}\right)^{2^t}=\dfrac{u+v\sqrt{D}}{2}\\ \left(\dfrac{c+d\sqrt{D}}{2}\right)^{2^t}=\dfrac{p+q\sqrt{D}}{2}\end{cases}(u,v,p,q\in\mathbb{Z})$$

此时方程3.33变为:

$$\left(\frac{u+v\sqrt{D}}{2}\right)^{n_1}+\left(\frac{p+q\sqrt{D}}{2}\right)^{n_1}=1\,(u,v,p,q,n_1\in\mathbb{Z},n_1\geq 3) \tag{3.67}$$

这种情况可以归结为$D<0$且n_1为奇数的情形,这时候我们可以得到

$$\begin{cases}\dfrac{u+v\sqrt{D}}{2}=\dfrac{1+\sqrt{-3}}{2}\\ \dfrac{p+q\sqrt{D}}{2}=\dfrac{1-\sqrt{-3}}{2}\end{cases}$$

即

$$\begin{cases}\left(\dfrac{a+b\sqrt{D}}{2}\right)^{2^t}=\dfrac{1+\sqrt{-3}}{2}\\ \left(\dfrac{c+d\sqrt{D}}{2}\right)^{2^t}=\dfrac{1-\sqrt{-3}}{2}\end{cases} \tag{3.68}$$

由方程3.68可得,$D=-3$,且对方程3.68两边取范数,我们可以得到

$$\begin{cases}\left(\dfrac{a^2+3b^2}{4}\right)^{2^t}\mid 1\\ \left(\dfrac{c^2+3d^2}{4}\right)^{2^t}\mid 1\end{cases} \tag{3.69}$$

此时可以得到,

$$\begin{cases} a^2+3b^2=4 \\ c^2+3d^2=4 \end{cases} \tag{3.70}$$

注意到方程3.70有解$(a,b)=(\pm1,\pm1)$和$(c,d)=(\pm1,\pm1)$.(其中$(a,b)=(\pm2,0)$和$(c,d)=(\pm2,0)$舍去).
所以我们只需要考虑

$$\begin{cases} \left(\dfrac{1+\sqrt{-3}}{2}\right)^{2^t}=(-\overline{\omega})^{2^t}=\overline{\omega}^{2^t} \\ \left(\dfrac{1-\sqrt{-3}}{2}\right)^{2^t}=(-\omega)^{2^t}=\omega^{2^t} \end{cases}$$

注意到$\gcd(3,2^t)=1$,因此方程3.68是不可能成立的,因此$n_1=1$.
(II)当$n_1=1$时,即$n=2^t$时,令

$$\begin{cases} \left(\dfrac{a+b\sqrt{D}}{2}\right)^{2^{t-1}}=\dfrac{u+v\sqrt{D}}{2} \\ \left(\dfrac{c+d\sqrt{D}}{2}\right)^{2^{t-1}}=\dfrac{p+q\sqrt{D}}{2} \end{cases} (u,v,p,q\in\mathbb{Z}) \tag{3.71}$$

此时方程3.33变为:

$$\left(\frac{u+v\sqrt{D}}{2}\right)^2+\left(\frac{p+q\sqrt{D}}{2}\right)^2=1(u,v,p,q\in\mathbb{Z}) \tag{3.72}$$

由方程3.72可得,

$$\begin{cases} uv+pq=0 \\ u^2+p^2+(v^2+q^2)D=4 \end{cases} \tag{3.73}$$

由方程3.72可得,

$$\begin{aligned} 1&=\left|\left(\frac{u+v\sqrt{D}}{2}\right)^2+\left(\frac{p+q\sqrt{D}}{2}\right)^2\right| \\ &\geq\left|\frac{u+v\sqrt{D}}{2}\right|^2-\left|\frac{p+q\sqrt{D}}{2}\right|^2=\frac{u^2-v^2D-(p^2-q^2D)}{4} \end{aligned} \tag{3.74}$$

(这里不妨设$u^2-v^2D\geq p^2-q^2D$)

下面对式子3.73和不等式3.74进行讨论：

情形一：当

$$\begin{cases} u^2-v^2D=p^2-q^2D \\ u^2+p^2+(v^2+q^2)D=4 \\ uv+pq=0 \end{cases} \tag{3.75}$$

时,由式子3.75可以得到,

$$\begin{cases} u^2+q^2D=2 \\ p^2+v^2D=2 \\ uv+pq=0 \end{cases} \tag{3.76}$$

由式子3.76可得,

$$\begin{cases} \gcd(u,q)=1 \\ \gcd(p,v)=1 \end{cases}$$

此时可以得到

$$\begin{cases} p=u \\ q=-v \end{cases} \text{或} \begin{cases} p=-u \\ q=v \end{cases}$$

此时,方程3.72变为

$$\left(\frac{u+v\sqrt{D}}{2}\right)^2+\left(\frac{u-v\sqrt{D}}{2}\right)^2=1(u,v,p,q\in\mathbb{Z}) \tag{3.77}$$

由方程3.71可得,

$$\begin{cases} \left(\frac{a+b\sqrt{D}}{2}\right)^{2^{t-1}}=\frac{u+v\sqrt{D}}{2} \\ \left(\frac{c+d\sqrt{D}}{2}\right)^{2^{t-1}}=\frac{u-v\sqrt{D}}{2} \end{cases} \tag{3.78}$$

此时方程3.33变为:

$$\left(\frac{a+b\sqrt{D}}{2}\right)^{2^t}+\left(\frac{a-b\sqrt{D}}{2}\right)^{2^t}=1 \tag{3.79}$$

令

$$u_{2^{t+1}}=\frac{\alpha^{2^{t+1}}-\beta^{2^{t+1}}}{\alpha-\beta}\left(\text{其中}\alpha=\frac{a+b\sqrt{D}}{2},\beta=\frac{a-b\sqrt{D}}{2}\right)$$

下面对$u_{2^{t+1}}$进行讨论:

注意到

$$\begin{cases}\alpha+\beta=a\\ \alpha\beta=\dfrac{a^2-b^2D}{4}\end{cases}$$

下面证明$\gcd(\alpha+\beta,\alpha\beta)=\gcd\left(a,\dfrac{a^2-b^2D}{4}\right)=1$(反证法):

(I)若$\gcd(\alpha+\beta,\alpha\beta)=2$,则有$2|a,2|b$, 令

$$\begin{cases}a=2a_1\\ b=2b_1\end{cases}\quad(a_1,b_1\in\mathbb{Z})$$

此时方程3.79变为:

$$\left(a_1+b_1\sqrt{D}\right)^{2^t}+\left(a_1-b_1\sqrt{D}\right)^{2^t}=1\tag{3.80}$$

令

$$\begin{cases}\left(a_1+b_1\sqrt{D}\right)^{2^t}=A+B\sqrt{D}\\ \left(a_1-b_1\sqrt{D}\right)^{2^t}=A-B\sqrt{D}\end{cases}\quad(A,B\in\mathbb{Z})$$

此时方程3.80变为:

$$2A=1$$

这是不可能的.

(II)若$\gcd(\alpha+\beta,\alpha\beta)=p(p>2)$(其中$p$为素数),则有

$$\begin{cases}p|a\\ p|b^2D\end{cases}$$

若$p|a,p|b$,令$a=pa_1,b=pb_1(a_1,b_1\in\mathbb{Z})$,此时由$2|(a+b)$可得$2|(a_1+b_1)$,由引理2可知,$\dfrac{a_1+b_1\sqrt{D}}{2},\dfrac{a_1-b_1\sqrt{D}}{2}$均为代数整数,此时方程3.79变为:

$$p^{2^t}\left[\left(\frac{a_1+b_1\sqrt{D}}{2}\right)^{2^t}+\left(\frac{a_1-b_1\sqrt{D}}{2}\right)^{2^t}\right]=1$$

于是有$p|1$,这是不可能的.

若$p|a,p|D$,令$a=pa_1,D=pD_1(a_1,D_1\in\mathbb{Z})$,此时方程3.79变为:

$$\left(\frac{a^2+b^2D+2ab\sqrt{D}}{4}\right)^{2^{t-1}}+\left(\frac{a^2+b^2D-2ab\sqrt{D}}{4}\right)^{2^{t-1}}=1$$

即

$$p^{2^{t-1}}\left[\left(\frac{a_1a+b^2D_1+2a_1b\sqrt{D}}{2}\right)^{2^{t-1}}+\left(\frac{a_1a+b^2D_1-2a_1b\sqrt{D}}{2}\right)^{2^{t-1}}\right]=2^{2^{t-1}} \tag{3.81}$$

因为$2|(a+b)$且$D\equiv 1\bmod 4$,因此$2\mid(a_1a+b^2D_1+2a_1b)$,于是$\frac{a_1a+b^2D_1+2a_1b\sqrt{D}}{2},\frac{a_1a+b^2D_1-2a_1b\sqrt{D}}{2}$均为代数整数.由方程3.81可得,$p\mid 2^{2^{t-1}}$,这是不可能的.

综合(I)和(II)可得,$\gcd(\alpha+\beta,\alpha\beta)=\gcd\left(a,\frac{a^2-b^2D}{4}\right)=1$.

(1)若$\frac{\alpha}{\beta}$是一个单位根时,由于$D<0,D\equiv 1(\bmod 4)$,因此$D=-3$,可以得到$a=-b$或$a=b$,即要考虑方程

$$a^{2^t}\left[\left(\frac{1+\sqrt{-3}}{2}\right)^{2^t}+\left(\frac{1-\sqrt{-3}}{2}\right)^{2^t}\right]=1 \tag{3.82}$$

此时有$a^{2^t}|1$,于是可以得到$a^{2^t}=1$,因此方程3.82变为

$$\left(\frac{1+\sqrt{-3}}{2}\right)^{2^t}+\left(\frac{1-\sqrt{-3}}{2}\right)^{2^t}=1 \tag{3.83}$$

即

$$\begin{cases}\alpha=\dfrac{1+\sqrt{-3}}{2}\\ \beta=\dfrac{1-\sqrt{-3}}{2}\end{cases}\text{或}\begin{cases}\alpha=\dfrac{-1+\sqrt{-3}}{2}\\ \beta=\dfrac{-1-\sqrt{-3}}{2}\end{cases}$$

(2)若$\frac{\alpha}{\beta}$不是一个单位根,则由定义5可知,(α,β)是Lucas数偶,从而$u_{2^{t+1}}$是一个Lucas序列的第2^{t+1}项. 注意到

$$\left(\alpha^{2^t}+\beta^{2^t}\right)\cdot u_{2^t}=\left(\alpha^{2^t}+\beta^{2^t}\right)\cdot\frac{\alpha^{2^t}-\beta^{2^t}}{\alpha-\beta}=\frac{\alpha^{2^{t+1}}-\beta^{2^{t+1}}}{\alpha^{2^t}-\beta^{2^t}}\cdot\frac{\alpha^{2^t}-\beta^{2^t}}{\alpha-\beta}=u_{2^{t+1}}$$

因此,当$u_{2^{t+1}}$有本原素因子p的时候,则$p\nmid u_{2^t}$,此时有

$$p\mid\left(\alpha^{2^t}+\beta^{2^t}\right). \tag{3.84}$$

由引理10可知,

当$t\geq 4$时,$u_{2^{t+1}}$有一个本原素因子,由方程3.79和式子3.84可知,这是不成立

的,因此仅考虑指标$t=2,3$.

当$t=2$时,由引理10可得,

$$\begin{cases}\alpha=\dfrac{1+\sqrt{-7}}{2}\\ \beta=\dfrac{1-\sqrt{-7}}{2}\end{cases}\text{ 或 }\begin{cases}\alpha=\dfrac{-1+\sqrt{-7}}{2}\\ \beta=\dfrac{-1-\sqrt{-7}}{2}\end{cases}$$

此时确实有$\alpha^4+\beta^4=1$.

当$t=3$时,由引理10可得,u_{2^4}有一个本原素因子,由方程3.79 和式子3.84可知,这是不成立的.

情形二：当

$$\begin{cases}u^2-p^2+q^2D-v^2D=4\\ u^2+p^2+(v^2+q^2)D=4\\ uv+pq=0\end{cases}\tag{3.85}$$

时,由式子3.85可以得到,

$$p^2+v^2D=0$$

此时$D=-1$,由于$D\equiv 1(\bmod 4)$,这是不可能的.

■

定理3. 当$\gcd(n,6)=1(n\in\mathbb{N})$时,二阶矩阵方程$X^n+Y^n=\lambda^n I(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$有无穷多组非平凡解.

证明: 取矩阵

$$A=\begin{bmatrix}1&1\\-1&0\end{bmatrix},B=\begin{bmatrix}0&-1\\1&1\end{bmatrix}$$

矩阵A的特征值为$\lambda_1=-\omega,\lambda_2=-\overline{\omega}$,其中$\omega=\dfrac{-1+\sqrt{-3}}{2}$,由于$\lambda_1\neq\lambda_2$,因此矩阵$A$在复数域上可以对角化,即存在复可逆矩阵$P\in M_2(\mathbb{C})$,使得

$$A=P\begin{bmatrix}\lambda_1&0\\0&\lambda_2\end{bmatrix}P^{-1}$$

注意到$AB=I$,因此

$$B=A^{-1}=P\begin{bmatrix}\dfrac{1}{\lambda_1}&0\\0&\dfrac{1}{\lambda_2}\end{bmatrix}P^{-1}$$

因此

$$A^n=P\begin{bmatrix}(\lambda_1)^n & 0\\ 0 & (\lambda_2)^n\end{bmatrix}P^{-1}=P\begin{bmatrix}(-\omega)^n & 0\\ 0 & (-\overline{\omega})^n\end{bmatrix}P^{-1}$$

$$B^n=P\begin{bmatrix}\left(\frac{1}{\lambda_1}\right)^n & 0\\ 0 & \left(\frac{1}{\lambda_2}\right)^n\end{bmatrix}P^{-1}=P\begin{bmatrix}(-\overline{\omega})^n & 0\\ 0 & (-\omega)^n\end{bmatrix}P^{-1}$$

因此,

$$A^n+B^n=P\begin{bmatrix}(-\omega)^n+(-\overline{\omega})^n & 0\\ 0 & (-\overline{\omega})^n+(-\omega)^n\end{bmatrix}P^{-1}$$

由于$\gcd(n,6)=1$,因此$(-\omega)^n+(-\overline{\omega})^n=(-\overline{\omega})^n+(-\omega)^n=1$. 于是$A^n+B^n=I$,即$(A,B,1)$是方程$X^n+Y^n=\lambda^n I\,(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$的一组非平凡解.

由引理9得,方程$X^n+Y^n=\lambda^n I\,(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$有无穷多组非平凡解.

■

推论4. 当$\gcd(n,6)=1(n\in\mathbb{N})$时,$r$阶矩阵方程$X^n+Y^n=\lambda^n I(X,Y\in M_r(\mathbb{Z}),r\in\mathbb{N},2|r,\lambda\in\mathbb{Z},\lambda\neq 0)$ 有无穷多组非平凡解.

证明: 令$r=2m,m\in\mathbb{N}$,取矩阵

$$A=\begin{bmatrix}A_1 & & & \\ & A_2 & & 0\\ & & \ddots & \\ 0 & & & A_m\end{bmatrix}_{2m\times 2m}$$

其中矩阵

$$A_i=\begin{bmatrix}1 & 1\\ -1 & 0\end{bmatrix}(i=1,2,\cdots m)$$

同理,取矩阵

$$B=\begin{bmatrix}B_1 & & & \\ & B_2 & & 0\\ & & \ddots & \\ 0 & & & B_m\end{bmatrix}_{2m\times 2m}$$

其中矩阵

$$B_i=\begin{bmatrix}0&-1\\1&1\end{bmatrix}(i=1,2,\cdots m)$$

由命题3得,$A_i^n+B_i^n=I_{2\times 2}(i=1,2,\cdots m)$,因此

$$A^n+B^n=\begin{bmatrix}(A_1)^n+(B_1)^n & & & \\ & (A_2)^n+(B_2)^n & & \\ & 0 & \ddots & 0 \\ & & & (A_m)^n+(B_m)^n\end{bmatrix}_{2m\times 2m}=I_{r\times r}$$

即$(A,B,1)$是方程$X^n+Y^n=\lambda^n I\,(X,Y\in M_r(\mathbb{Z}),r\in\mathbb{N},2|r,\lambda\in\mathbb{Z},\lambda\neq 0)$ 的一组非平凡解.

由引理9得,方程$X^n+Y^n=\lambda^n I\,(X,Y\in M_r(\mathbb{Z}),r\in\mathbb{N},2|r,\lambda\in\mathbb{Z},\lambda\neq 0)$ 有无穷多组非平凡解. ■

推论5. 二阶矩阵方程$X^3+Y^3=\lambda^3 I\,(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$有无穷多组非平凡解.

证明: 取矩阵

$$A=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}\in M_2(\mathbb{Z})$$

假设矩阵A的特征值为$\lambda_1,\lambda_2\,(\lambda_1\neq\lambda_2)$,于是矩阵$A$在复数域上可以对角化,即存在复可逆矩阵$P\in M_2(\mathbb{C})$,使得

$$A=P\begin{bmatrix}\lambda_1&0\\0&\lambda_2\end{bmatrix}P^{-1}$$

取矩阵

$$B=P\begin{bmatrix}\lambda_2&0\\0&\lambda_1\end{bmatrix}P^{-1}$$

经过比较矩阵A,B的元素可得,

$$B=\begin{bmatrix}a_{22}&-a_{12}\\-a_{21}&a_{11}\end{bmatrix}\in M_2(\mathbb{Z})$$

$\forall a_{22}\in\mathbb{Z}$,取$a_{11},a_{12},a_{21}\in\mathbb{Z}$满足下列条件

$$\begin{cases}\lambda_1\equiv 1(\bmod 3)\\ \lambda_2\equiv 1(\bmod 3)\\ a_{11}=\lambda_1^3-a_{22}\\ a_{12}a_{21}=a_{11}a_{22}-\dfrac{\lambda_1^6-\lambda_2^3}{3}\end{cases}\quad(\lambda_1,\lambda_2\in\mathbb{Z})$$

因此

$$A^3+B^3=\begin{bmatrix}\alpha & 0\\ 0 & \alpha\end{bmatrix}$$

其中$\alpha=(a_{11}+a_{22})[(a_{11}+a_{22})^2-3(a_{11}a_{22}-a_{12}a_{21})]=(\lambda_1\lambda_2)^3$,因此

$$A^3+B^3=\begin{bmatrix}(\lambda_1\lambda_2)^3 & 0\\ 0 & (\lambda_1\lambda_2)^3\end{bmatrix}=(\lambda_1\lambda_2)^3 I$$

由于$a_{22},\lambda_1,\lambda_2$是任意的,因此矩阵方程$X^3+Y^3=\lambda^3 I\,(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$有无穷多组非平凡解. ■

例1. 取

$$\begin{cases}\lambda_1=1\\ \lambda_2=-2\\ a_{22}=0\\ a_{11}=1\\ a_{12}=-1\\ a_{21}=3\end{cases}$$

则矩阵

$$A=\begin{bmatrix}1 & -1\\ 3 & 0\end{bmatrix},B=\begin{bmatrix}0 & 1\\ -3 & 1\end{bmatrix}$$

于是$(A,B,-2)$是矩阵方程$X^3+Y^3=\lambda^3 I\,(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$的一组非平凡解.

推论6. 二阶矩阵方程$X^4+Y^4=\lambda^4 I\,(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$有无穷多组非平凡解.

证明: 取矩阵

$$A=\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}\in M_2(\mathbb{Z})$$

假设矩阵A的特征值为$\lambda_1,\lambda_2\,(\lambda_1\neq\lambda_2)$,于是矩阵$A$在复数域上可以对角化,即存在复可逆矩阵$P\in M_2(\mathbb{C})$,使得

$$A=P\begin{bmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{bmatrix}P^{-1}$$

取矩阵

$$B=P\begin{bmatrix}\lambda_2 & 0\\ 0 & \lambda_1\end{bmatrix}P^{-1}$$

经过比较矩阵A,B的元素可得,

$$B=\begin{bmatrix}a_{22} & -a_{12}\\ -a_{21} & a_{11}\end{bmatrix}\in M_2(\mathbb{Z})$$

注意到

$$A^4+B^4=\begin{bmatrix}\alpha & 0\\ 0 & \alpha\end{bmatrix}\left(\alpha=2\left(a_{12}a_{21}\right)^2+4a_{12}a_{21}\left(a_{11}^2+a_{22}^2+a_{11}a_{22}\right)+a_{11}^4+a_{22}^4\right)$$

令

$$\alpha=\lambda^4$$

即

$$2\left(a_{12}a_{21}\right)^2+4a_{12}a_{21}\left(a_{11}^2+a_{22}^2+a_{11}a_{22}\right)+a_{11}^4+a_{22}^4=\lambda^4 \tag{3.86}$$

把式子3.86看作是$a_{12}a_{21}$的一元二次方程,则

$$\frac{\Delta}{4}=2\left[\left(a_{11}+a_{22}\right)^4+\lambda^4\right]$$

由于$a_{12}a_{21}$是一个整数,因此$\dfrac{\Delta}{4}$是一个完全平方数,令

$$\frac{\Delta}{4}=2\left[\left(a_{11}+a_{22}\right)^4+\lambda^4\right]=X_1^2 \tag{3.87}$$

令$X_1=2X$,则式子3.87变为

$$\left(a_{11}+a_{22}\right)^4+\lambda^4=2X^2 \tag{3.88}$$

注意到不定方程$Y^4+Z^4=2X^2(X,Y,Z\in\mathbb{Z})$有解$(t,t,t^2)(t\in\mathbb{Z})$ 因此,令

$$\begin{cases}a_{11}+a_{22}=t\\ \lambda=t \qquad\qquad (t\neq 0)\\ X=t^2\end{cases}$$

因此

$$\begin{cases} a_{11}+a_{22}=t \\ \lambda=t \qquad\qquad (t\neq 0) \\ X_1=2t^2 \end{cases}$$

是方程3.87的一组解,由方程3.86可得,

$$\begin{cases} a_{11}+a_{22}=t \\ a_{12}a_{21}=-\left(a_{11}^2+a_{22}^2+a_{11}a_{22}\right)\pm t^2 \end{cases} (t\neq 0)$$

由于t是任意的,因此矩阵方程$X^4+Y^4=\lambda^4 I\,(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$有无穷多组非平凡解. ■

例2. 取

$$\begin{cases} t=1 \\ a_{11}=1 \\ a_{22}=0 \\ a_{12}=1 \\ a_{21}=-2 \end{cases}$$

则矩阵

$$A=\begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}, B=\begin{bmatrix} 0 & -1 \\ 2 & 1 \end{bmatrix}$$

于是$(A,B,1)$是矩阵方程$X^4+Y^4=\lambda^4 I\,(X,Y\in M_2(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$的一组非平凡解.

4 n阶矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_n(\mathbb{Z}))$的解

定理4. n阶矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_n(\mathbb{Z}))$有无穷多组非平凡解.

证明: $\forall\mu,\lambda\in\mathbb{Z},\lambda\neq 0$,取方阵$A=\mu I_{n\times n}$,

$$B=\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & \lambda^n-\mu^n \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}_{n\times n}$$

由引理6得,矩阵B的特征多项式为$f(x)=x^n+\mu^n-\lambda^n$,由引理7可得,$B^n+(\mu^n-\lambda^n)I=0$,即$B^n=(\lambda^n-\mu^n)I$. 因此,$A^n+B^n=\mu^n I+(\lambda^n-\mu^n)I=\lambda^n I$,由于是μ,λ任意的，因此矩阵方程$X^n+Y^n=\lambda^n I(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_n(\mathbb{Z}))$有无穷多组非平凡解$(A,B,\lambda)$. ■

例3. 对于三阶矩阵方程$X^3+Y^3=\lambda^3 I\,(X,Y\in M_3(\mathbb{Z}),\lambda\in\mathbb{Z},\lambda\neq 0)$:

取

$$\begin{cases}\mu=1\\ \lambda=-2\end{cases}$$

由定理4得,取矩阵

$$A=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},B=\begin{bmatrix}0&0&-9\\1&0&0\\0&1&0\end{bmatrix}$$

于是$(A,B,-2)$是矩阵方程$X^3+Y^3=\lambda^3 I\,(X,Y\in M_3(\mathbb{Z}))$的一组非平凡解.

5 n阶矩阵方程$X^3+Y^3=\lambda^3 I(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_n(\mathbb{Z}))$的解

定理5. n阶矩阵方程$X^3+Y^3=\lambda^3 I(n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0,X,Y\in M_n(\mathbb{Z}))$有无穷多组非平凡解.

证明: 令

$$A=\begin{bmatrix}1&-1\\3&0\end{bmatrix},B=\begin{bmatrix}0&1\\-3&1\end{bmatrix},C=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix},D=\begin{bmatrix}0&0&-9\\1&0&0\\0&1&0\end{bmatrix}$$

由例3和例1可得,

$$\begin{cases}A^3+B^3=(-2)^3I_{2\times 2}\\C^3+D^3=(-2)^3I_{3\times 3}\end{cases}\tag{5.1}$$

(1) 当$n=2m(m\in\mathbb{N})$时,取矩阵

$$A=\begin{bmatrix}A_1&&&\\&A_2&&0\\&&\ddots&\\0&&&A_m\end{bmatrix}_{2m\times 2m}$$

其中矩阵$A_i=A(i=1,2,\cdots m)$ 同理,取矩阵

$$B=\begin{bmatrix}B_1&&&\\&B_2&&0\\&&\ddots&\\0&&&B_m\end{bmatrix}_{2m\times 2m}$$

其中矩阵$B_i=B(i=1,2,\cdots m)$ 由式5.1得,

$$A^3+B^3=\begin{bmatrix}(A_1)^3+(B_1)^3&&&\\&(A_2)^3+(B_2)^3&&0\\&&\ddots&\\0&&&(A_m)^3+(B_m)^3\end{bmatrix}_{2m\times 2m}=(-2)^3I_{n\times n}$$

即$(A,B,-2)$是方程$X^3+Y^3=\lambda^3 I(X,Y\in M_n(\mathbb{Z}),n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0)$的一组非平凡解.

由引理9得,方程$X^3+Y^3=\lambda^3 I(X,Y\in M_n(\mathbb{Z}),n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0)$有无穷多组非平凡解.

(2) 当$n=2m+1(m\in\mathbb{N})$时,取矩阵

$$A=\begin{bmatrix} A_1 & & 0 \\ & \ddots & \\ 0 & & A_{m-1} \\ & & & C \end{bmatrix}_{(2m+1)\times(2m+1)}$$

其中矩阵$A_i=A(i=1,2,\cdots,m-1)$ 同理,取矩阵

$$B=\begin{bmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_{m-1} \\ & & & D \end{bmatrix}_{(2m+1)\times(2m+1)}$$

其中矩阵$B_i=B(i=1,2,\cdots m-1)$ 由式5.1得,

$$A^3+B^3=\begin{bmatrix} A_1^3+B_1^3 & & 0 \\ & \ddots & \\ 0 & & A_{m-1}^3+B_{m-1}^3 \\ & & & C^3+D^3 \end{bmatrix}_{(2m+1)\times(2m+1)}=(-2)^3 I_{n\times n}$$

即$(A,B,-2)$是方程$X^3+Y^3=\lambda^3 I(X,Y\in M_n(\mathbb{Z}),n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0)$的一组非平凡解.

由引理9得,方程$X^3+Y^3=\lambda^3 I(X,Y\in M_n(\mathbb{Z}),n\in\mathbb{N},\lambda\in\mathbb{Z},\lambda\neq 0)$有无穷多组非平凡解.

■

6 参考文献

参考文献

[1] RIBENBOIM.P13 lectures on Fermat's last theorem [M].New York:Springer Verlag,1979.

[2] FREJMAN D.on Fermat's equation in the set of Fibonacci matrices[J].Discussiones Mathematicae,1933,13(1):61-64.

[3] GRYTCZUK A.On Fermat's equation in the set of integral 2×2matrices[J].Period Math Hungral,1995,30(1):79-84.

[4] LE M H,LI Q.On Fermat's equation in integral 2×2 matrices [J].Periodica Mathematica Hugarica,1995,31(2):219-222.

[5] LI Q,LE M H.A note on Fermat's equation in integral 2×2 matrices [J].Discussiones Mathematiace,1995,15(2):135-136.

[6] CHEN X G.On Fermat's equation in the set of generalized Fibonacci matrices [J].Discussiones Mathematicae,1997,17(1):5-8.

[7] GRYTCZUK A.Matrices and diophantine equations [J].Dissertationes Mathematicae,1997,58(1):1-49.

[8] 乐茂华.关于整数矩阵集上的Fermat方程[J].吉首大学学报(自然科学版),1998，19(3):11-12.

[9] 赵院娥,车顺.整数矩阵集上的Fermat方程[J].西北大学学报(自然科学版),2014,44(3):360-362.

[10] 李伟勋.关于2阶整数矩阵的Catanlan方程[J].广东石油化工学院学报,2016,26(4):59-60.

[11] 尹倩倩,梁欣然,袁平之.一类二阶整数矩阵方程的解[J].华南师范大学学报(自然科学版),2019,51(5):104-109.

[12] 张景晓.整数矩阵的性质及应用[J].重庆理工大学学报(自然科学版),2010,24(4):117-118.

[13] 潘承洞,潘承彪.代数数论[M].济南:山东出版社,2001.

[14] 钟祥贵.整数环上一类二阶矩阵方程的解[J].大学数学,2006,22(4):71-74.

[15] Henri Cohen.Number Theory Volume I:Tools and Diophantine Equations[M].2007 Springer Science+Business Media,LLC.

[16] 王萼芳,石生明.高等代数(第三版)[M].北京:高等教育出版社,2003.9.

[17] Voutier P.M.,Primitive divisors of Lucas and Lehmer sequences,Math. Comp.,1995,64:869-888.

7 致谢

本论文的完成得到了多方的支持与帮助，在此特地进行感谢。本论文的灵感来自于华南师范大学数学学报中尹倩倩等人的论文，在此基础上做更加一般化的研究。感谢华南师范大学的黎洪键老师，在本文中提供了方向以及协助进行定理的证明，老师的耐心教导让我受益匪浅。感谢广东实验中学A-LEVEL部的闫月峰老师，在我住宿期间向给我矩阵方面的教导。感谢我的父母在论文进行过程中的关心与支持。感谢广东实验中学凌明灿老师和科工社王剑老师的支持。