Des matrices pour la somme des carrés

Tamafumi KANEYAMA

兼　山　瓊　典

Abstract

It is known every 2×2 integral matrix is the sum of three integral squares. So in this paper I prove that which 2×2 integral matrix can be expressed as the sum of two integral squares.

Introduction

Les possibilités d'exprimer une matrice entiere pour la somme de carrés des matrices entieres sont considérées par Carlitz [1], Granville [2], Griffin et Krusemeyer [3] et Newman [5].

Newman a utilisé les fait sur GF(2) dans [5] et a prouveé que toutes 2×2 matrices entieres sont la somme de trois carrés des matrices entieres. En outre il a prouveé qu'il est la meilleur possibilité.

Presque toutes 2×2 matrices entieres sont la somme de trois carrés des matrices entieres, je prouve dans ce dissertation que certains 2×2 matrices entieres peut exprimer des matrices pour la somme de deux carrés des matrices entieres.

Des 2×2 martices entieres

Soit $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ une 2×2 matrice entiere dans $M(2,\mathbf{Z})$. Je prouve beaucoup de lemmes.

Lemme 1 *Si* $a-d\equiv 1 \pmod 2$ *alors une matrice A peut exprimer la matrice pour la somme de deux carrés des matrices entieres.*

Démonstration: Parce que $a-d\equiv 1 \pmod 2$, soit $a-d=2p+1$ $(p\in\mathbf{Z})$ et on met

$$m=p+1,\ n=p.$$

Alors

$$m-n=1,\ m+n=2p+1,$$
$$m^2-n^2=2p+1=a-d.$$

Donc

$$\begin{pmatrix} m & b \\ c & -n \end{pmatrix}^2+\begin{pmatrix} 0 & 1 \\ -n^2-bc+d & 0 \end{pmatrix}^2$$
$$=\begin{pmatrix} m^2+bc & b(m-n) \\ c(m-n) & n^2+bc \end{pmatrix}+\begin{pmatrix} -n^2-bc+d & 0 \\ 0 & -n^2-bc+d \end{pmatrix}$$
$$=\begin{pmatrix} m^2-n^2+d & b(m-n) \\ c(m-n) & d \end{pmatrix}$$

※ E-mail　kaneyama@ha.shotoku.ac.jp

$$= \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

cqfd.

Lemme 2 *Si* $a-d \equiv 0 \pmod 2$ *et b est un nombre impair alors une matrice A peut exprimer la matrice pour la somme de deux carrés des matrices entieres.*

Démonstration: Parce que $a-d \equiv 0 \pmod 2$ et b est un nombre impair, on suppose

$$a-d=2p \quad (p \in \mathbf{Z}),\ b=2k+1 \quad (k \in \mathbf{Z}).$$

Met

$$u=(p+1)^2+(b-k)c-a.$$

Alors

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^2 = \begin{pmatrix} p+1 & b-k \\ c-u & -p \end{pmatrix}^2 + \begin{pmatrix} 0 & k \\ u & 1 \end{pmatrix}^2$$

$$= \begin{pmatrix} (p+1)^2+(b-k)(c-u) & b-k \\ c-u & p^2+(b-k)(c-u) \end{pmatrix} + \begin{pmatrix} uk & k \\ u & uk+1 \end{pmatrix}$$

Donc

$$\begin{aligned} \alpha &= (p+1)^2+(b-k)(c-u)+uk \\ &= (p+1)^2+(b-k)c-u(b-2k) \\ &= (p+1)^2+(b-k)c-\{(p+1)^2+(b-k)c-a\} \times 1 \\ &= a, \\ \beta &= b-k+k=b, \\ \gamma &= c-u+u=c, \\ \delta &= p^2+(b-k)(c-u)+uk+1 \\ &= p^2+(b-k)c-u(b-2k)+1 \\ &= p^2+(b-k)c-\{(p+1)^2+(b-k)c-a\} \times 1+1 \\ &= -2p+a \\ &= -(a-d)+a \\ &= d. \end{aligned}$$

cqfd.

Lemme 3 *Si* $a-d \equiv 0 \pmod 2$ *et c est un nombre impair alors une matrice A peut exprimer la matrice pour la somme de deux carrés des matrices entieres.*

Démonstration: Parce que $a-d \equiv 0 \pmod 2$ et c est un nombre impair, on suppose

$$a-d=2p \quad (p \in \mathbf{Z}),\ c=2h+1 \quad (h \in \mathbf{Z}).$$

Met

$$\upsilon=(p+1)^2+b(h-c)-a.$$

Alors

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} p+1 & b-\upsilon \\ c-h & -p \end{pmatrix}^2 + \begin{pmatrix} 0 & \upsilon \\ h & 1 \end{pmatrix}^2$$

$$= \begin{pmatrix} (p+1)^2+(b-\upsilon)(c-h) & b-\upsilon \\ c-h & p^2+(b-\upsilon)(c-h) \end{pmatrix} + \begin{pmatrix} \upsilon h & \upsilon \\ h & \upsilon h+1 \end{pmatrix}$$

Donc

$$\alpha=(p+1)^2+(b-\upsilon)(c-h)+\upsilon h$$

$$
\begin{aligned}
&= (p+1)^2 + b(c-h) - v(c-2h)\\
&= (p+1)^2 + b(c-h) - \{(p+1)^2 + b(h-c) - a\} \times 1\\
&= a,\\
\beta &= b - v + v = b,\\
\gamma &= c - h + h = c,\\
\delta &= p^2 + (b-v)(c-h) + vh + 1\\
&= p^2 + b(c-h) - v(c-2h) + 1\\
&= p^2 + b(c-h) - \{(p+1)^2 + b(h-c) - a\} \times 1 + 1\\
&= -2p + a\\
&= -(a-d) + a\\
&= d.
\end{aligned}
$$

cqfd.

Lemme 4 *Si $a - d \equiv 0 \pmod 4$ et b, c sont des nombres pairs alors une matrice A peut exprimer la matrice pour la somme de deux carrés des matrices entieres.*

Démonstration: Parce que $a - d \equiv 0 \pmod 4$ et b, c sont des nombres pairs, on suppose

$$a - d = 4p \ (p \in \mathbf{Z}),\ \ b = 2k,\ \ c = 2h \ (k, h \in \mathbf{Z}).$$

Met

$$m = p + 1,\ n = p - 1.$$

Alors

$$m - n = 2,\ m^2 - n^2 = 4p = a - d.$$

Donc

$$
\begin{aligned}
&\begin{pmatrix} m & k \\ h & -n \end{pmatrix}^2 + \begin{pmatrix} 0 & 1 \\ -n^2 - kh + d & 0 \end{pmatrix}^2\\
&\quad = \begin{pmatrix} m^2 + kh & k(m-n) \\ h(m-n) & n^2 + kh \end{pmatrix} + \begin{pmatrix} -n^2 - kh + d & 0 \\ 0 & -n^2 - kh + d \end{pmatrix}\\
&\quad = \begin{pmatrix} m^2 - n^2 + d & 2k \\ 2h & d \end{pmatrix}\\
&\quad = \begin{pmatrix} a & b \\ c & d \end{pmatrix}
\end{aligned}
$$

cqfd.

Lemme 5 *Si $a - d \equiv 2 \pmod 4$ et a, b, c, d sont des nombres pairs alors une matrice A peut exprimer la matrice pour la somme de deux carrés des matrices entieres.*

Démonstration: Parce que $a - d \equiv 2 \pmod 4$ et b est un nombre pair, on suppose

$$a - d = 4p + 2 \ (p \in \mathbf{Z}),\ b = 2k \ (k \in \mathbf{Z}).$$

Met

$$u = 2(p+1)^2 + (b - k + 1)\frac{c}{2} - \frac{a}{2}.$$

Parce que *a, c* sont des nombres pairs, u est un nombre entier.

Alors

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 2p+2 & b-k+1 \\ c-u & -2p-1 \end{pmatrix}^2 + \begin{pmatrix} 0 & k-1 \\ u & 1 \end{pmatrix}^2$$

$$= \begin{pmatrix} 4(p+1)^2+(b-k+1)(c-u) & b-k+1 \\ c-u & (2p+1)^2+(b-k+1)(c-u) \end{pmatrix} + \begin{pmatrix} u(k-1) & k-1 \\ u & u(k-1)+1 \end{pmatrix}$$

Donc

$$\begin{aligned}
\alpha &= 4(p+1)^2+(b-k+1)(c-u)+u(k-1) \\
&= 4(p+1)^2+(b-k+1)c-u(b-k+1-k+1) \\
&= 4(p+1)^2+(b-k+1)c-2u \\
&= 4(p+1)^2+(b-k+1)c-\{4(p+1)^2+(b-k+1)c-a\} \\
&= a, \\
\beta &= b-k+1+k-1=b, \\
\gamma &= c-u+u=c, \\
\delta &= (2p+1)^2+(b-k+1)(c-u)+u(k-1)+1 \\
&= (2p+1)^2+(b-k+1)c-u(b-k+1-k+1)+1 \\
&= (2p+1)^2+(b-k+1)c-2u+1 \\
&= (2p+1)^2+(b-k+1)c-\{4(p+1)^2+(b-k+1)c-a\}+1 \\
&= -4p-2+a \\
&= -(a-d)+a \\
&= d.
\end{aligned}$$

cqfd.

Le lemme suivant a été prouvée essentiallement par Granville [2].

Lemme 6 *Si* $a-d \equiv 2 \pmod 4$ *alors une matrice A peut exprimer la matrice pour la somme de trois carrés des matrices entieres.*

Démonstration: Parce que $a-d \equiv 2 \pmod 4$, on suppose

$$a-d=4p+2 \quad (p \in \mathbf{Z}).$$

Met

$$u=d-bc-1-(2p+1)^2.$$

Alors

$$\begin{aligned}
&\begin{pmatrix} 0 & b \\ c & 1 \end{pmatrix}^2 + \begin{pmatrix} 2p+2 & 0 \\ 0 & 2p+1 \end{pmatrix}^2 + \begin{pmatrix} 0 & 1 \\ u & 0 \end{pmatrix}^2 \\
&= \begin{pmatrix} bc & b \\ c & bc+1 \end{pmatrix} + \begin{pmatrix} (2p+2)^2 & 0 \\ 0 & (2p+1)^2 \end{pmatrix} + \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} \\
&= \begin{pmatrix} bc+(2p+2)^2+u & b \\ c & bc+1+(2p+1)^2+u \end{pmatrix} \\
&= \begin{pmatrix} d+4p+2 & b \\ c & d \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}
\end{aligned}$$

cqfd.

Lemme 7 *Si* $a-d \equiv 2 \pmod 4$ *et a, d sont des nombres impairs et b, c sont des nombres pairs alors une matrice A ne peut pas exprimer la matrice pour la somme de deux carrés des matrices entieres.*

Démonstration: Parce que $a-d\equiv 2\ (\mathrm{mod}\ 4)$, on suppose $a-d=4p+2\ (p\in\mathbf{Z})$.

Parce que

$$a+d=a-d+2d=(4p+2)+2d=2(2p+1+d)$$

et d est un nombre impair, on pout supposer $a+d=4q\ \ (q\in\mathbf{Z})$.

Donc on suppose que la matrice A est exprimée la matrice pour la somme de deux carrés des matrices entieres X et Y. Alors

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}=X^2+Y^2. \tag{1}$$

Soient $t_1=\mathrm{tr}(X),\ d_1=det(X),\ t_2=tr(Y),\ d_2=det(Y)$ tels que

$$X^2=t_1X-d_1I,\ \ Y^2=t_2Y-d_2I$$

où I est la matrice identité.

Alors

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=t_1X-d_1I+t_2Y-d_2I,$$

$$t_1X+t_2Y=\begin{pmatrix} a & b \\ c & d \end{pmatrix}+(d_1+d_2)I=\begin{pmatrix} a+d_1+d_2 & b \\ c & d+d_1+d_2 \end{pmatrix} \tag{2}$$

Prenant trace des deux côtés, on a

$$t_1^2+t_2^2=(a+d)+2(d_1+d_2). \tag{3}$$

Il suit d'après le (3) que comme $a+d=4q$, t_1 et t_2 sont les nombres impairs ou sont les nombres pairs.

Si t_1 et t_2 sont les nombres impairs, soient $t_1=2k_1+1$, $t_2=2k_2+1\ (k_1,\ k_2\in\mathbf{Z})$.

Alors

$$(2k_1+1)^2+(2k_2+1)^2=a+d+2(d_1+d_2),$$

$$d_1+d_2=2(k_1^2+k_1+k_2^2+k_2-q)+1.$$

Donc d_1+d_2 est un nombre impair. D'après le (2), on a

$$t_1X+t_2Y\equiv\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\ (\mathrm{mod}\ 2).$$

Parce que t_1 et t_2 sont des nombres impairs, on a

$$X\equiv Y\ (\mathrm{mod}\ 2),$$

$$X^2\equiv Y^2\ (\mathrm{mod}\ 2).$$

Ce dit que

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\equiv\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\ (\mathrm{mod}\ 2).$$

Ceci est en contradiction avec a, d sont des nombres impairs.

Si t_1 et t_2 sont des nombres pairs, soient $t_1=2k_1,\ t_2=2k_2\ (k_1,\ k_2\in\mathbf{Z})$. Alors

$$4k_1^2+4k_2^2=a+d+2(d_1+d_2),$$

$$d_1+d_2=2(k_1^2+k_2^2-q).$$

Ce dit que d_1+d_2 est un nombre pair.

Parce que t_1 et t_2 sont des nombre pairs, on a

$$t_1X+t_2Y\equiv\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\ (\mathrm{mod}\ 2). \tag{4}$$

Parce que a, d sont des nombres impairs, b, c sont des nombres pairs et d_1+d_2 est un nombre pair, on a

$$\begin{pmatrix} a+d_1+d_2 & b \\ c & d+d_1+d_2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2. \qquad (5)$$

Ceci (4), (5) sont en contradictions avec (2) et achève le démonstration du lemme.

cqfd.

Tout de suite nous rassemblons touts les lemmes, on a le théorème suivre.

Théorème *Soit* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *une* 2×2 *matrice entiere dans* $M(2, \mathbf{Z})$. *Alors*

1. *Si* $a - d \equiv 2 \pmod 4$, *et a, d sont des nombres impairs et b, c sont des nombres pairs alors une matrice A ne peut pas exprimer la matrice pour la somme de deux carrés des matrices entieres. Mais peut exprimer la matrice pour la somme de trois carrés des matrices entieres.*
2. *Sinon une matrice A peut exprimer la matrice pour la somme de deux carrés des matrices entieres.*

BIBLIOGRAPHIE

[1] L. Carlitz: Solution to problem 140 (posed by I. Connell), Canad. Math. Bull., 11 (1968) 615–619
[2] A. Granville: Matrices as the sum of four squares, Linear and Multilinear Algebra, 20 (1987) 247–251.
[3] M. Griffin and M. Krusemeyer: Matrices as sums of square. Linear and Multilinear Algebra, 5 (1977) 33–44.
[4] M. Newman: Integral Matrices, Celsea, New York (1972).
[5] M. Newman: Sums of squares of matrices, Pasific Journal of Mathematics, 118 (1985) 497–506.
[6] O. Taussky: History of sums of squares in algebra, American Mathematics Heritage, Algebra and applied Mathematics, 13 (1981) 73–90.