

# 主理想环上的矩阵 Goldbach 问题\*

王志雄

(华侨大学管理信息科学系, 泉州 362011)

**摘要** 研究主理想环上的矩阵表示为素阵之和的问题, 证明了阶不小于2的矩阵恒能表示为两个素阵之和. 结果表明, 矩阵环及其子环的表示关系是相当复杂的.

**关键词** 主理想环, 矩阵, 哥德巴赫猜想, 素数

**分类号** O 153.3

整数矩阵是解决图论、组合论、控制论、信息论等问题的重要工具. 整数方阵的分解问题形成一个与传统的矩阵论既有联系又有区别的新课题, 越来越引起人们的兴趣<sup>(1~5)</sup>. 阶数为 $n$ 的整数矩阵全体在通常的加法与乘法运算下, 形成一个与整数环相当类似的环. 以整数环为主要研究对象的许多数论问题都能以自然的方式, 在整数矩阵环中提出并加以研究. 一方面, 整数环作为整数矩阵环的特殊情况(取阶数为1), 整数矩阵环上的数论问题应比整数环上的数论问题远为复杂. 因为当阶数 $n \geq 2$ 时, 整数矩阵环不再是整环, 且其乘法不具备交换律. 另一方面, 出乎人们意料的是困惑几代数学大师的一些数论问题, 在阶 $n \geq 2$ 的整数矩阵环中却不难解决. 著名的 Goldbach 猜想即其一例. 本文将对一般主理想环上的矩阵环进行研究.

## 1 基本概念

设 $R$ 是主理想环, 环 $R$ 上的 $n$ 阶矩阵环记为 $M_n(R)$ . 若矩阵 $A \in M_n(R)$ 的行列式值 $\det(A)$ 为环 $R$ 的可逆元, 则称 $A$ 为么模阵. 显然, 环 $M_n(R)$ 的全体么模阵在矩阵乘法运算下成一个群. 矩阵 $A$ 的一个基本初等变换是指: (1) 交换 $A$ 的某两行(列); (2) 把 $A$ 的某一行(列)乘上一个元素 $a \in R$ , 加到另一行(列)上去; (3)  $A$ 的某一行(列)乘上 $R$ 的一个可逆元. 矩阵 $A$ 的一个初等变换指的是对 $A$ 施行一系列基本初等变换的结果. 显然, 矩阵经一初等变换得矩阵 $B$ , 当且仅当存在么模阵 $P$ 与 $Q$ , 使 $B = PAQ$ . 这时, 称矩阵 $A$ 与 $B$ 等价, 记为 $A \cong B$ . 矩阵 $A$ 的各元素之最大公约数记为 $d(A)$ . 显然, 若 $A \cong B$ , 则 $d(A)$ 与 $d(B)$ 在不计环 $R$ 之可逆因子时是相同的, 且对每个矩阵 $A$ , 存在对角矩阵 $B \cong A$ , 使 $B = \text{diag}(a_1, a_2, \dots, a_n)$ , 式中 $a_1 = d(A) = d(B)$ <sup>(6)</sup>. 非么模阵 $P$ 称为环 $M_n(R)$ 的素阵, 若 $P = AB$  ( $A, B \in M_n(R)$ ) 蕴含 $A, B$ 至少其一么模阵.

**定理1** 矩阵 $P \in M_n(R)$ 为素阵, 当且仅当 $\det(P)$ 为环 $R$ 上的素元, 即不可分解为 $R$ 上两个异于可逆元的元素 $a, b$ 之积的元素.

\* 本文 1994-03-26 收到

证 若  $\det(P)$  为环  $R$  上的素元, 且  $P=AB$ , 则  $\det(A) \cdot \det(B) = \det(AB) = \det(P)$  为  $R$  上的素元. 故  $\det(A), \det(B)$  必至少其一为  $R$  上的可逆元, 从而  $A$  与  $B$  至少其一为么模阵. 反之, 若  $\det(P)$  非  $R$  上的素元, 设  $P \cong N = \text{diag}(a_1, a_2, \dots, a_n)$ , 则  $\det(P) = \epsilon a_1 a_2 \cdots a_n$ , 其中  $\epsilon$  为  $R$  的可逆元,  $a_1 = d(P)$ . 因  $\det(P)$  非  $R$  上的素元, 故仅有如下两种情况: (1) 某元素  $a_i$  非  $R$  上的素元; (2) 某两个元素  $a_i, a_j$  非  $R$  上的可逆元. 对每种情况, 显然  $N$  均可分解为两个非么模阵之积, 从而  $P$  亦然.

## 2 若干引理

**引理 1** 矩阵  $A \in M_2(R)$  能分解为  $X+Y$  ( $X, Y \in M_2(R)$ ) 使  $\det(X)=x, \det(Y)=y$ , 当且仅当  $d(A)$  能被  $x-y$  整除.

证 若  $A=X+Y$ , 则  $\det(X) = \det(A-Y) \equiv \det(-Y) = \det(Y) \pmod{d(A)}$ . 反之, 若  $d(A)$  能被  $x-y$  整除, 设  $A=P \text{diag}(a, b)Q$ , 其中  $P, Q$  为  $M_2(R)$  的么模阵,  $a=d(A)$ , 则  $a|b$ , 且  $a|(x-y)$ . 令  $r=0, s=e$  (环  $R$  的单位元),  $t=-x(\det(P)\det(Q))^{-1}, u=b+\frac{x-y}{a}(\det(P)\det(Q))^{-1}$ , 则

$$X_0 = \begin{bmatrix} r & s \\ t & u \end{bmatrix}, \quad Y_0 = \begin{bmatrix} a-r & -s \\ -t & b-u \end{bmatrix}.$$

$X=PX_0Q, Y=PY_0Q$ , 故  $A=X+Y$ , 且  $\det(X)=x, \det(Y)=y$ . 证毕.

**引理 2** 矩阵  $A \in M_3(R)$  能分解为  $X+Y$  ( $X, Y \in M_3(R)$ ), 使  $\det(X)=x, \det(Y)=y$ , 当且仅当  $d(A)$  能被  $x+y$  整除.

证  $A=X+Y$ , 则  $\det(X) = \det(A-Y) \equiv \det(-Y)\det(Y) \pmod{d(A)}$ . 反之, 若  $d(A)|(x+y)$ , 设  $A=P \text{diag}(a, b, c)Q$ , 其中  $\det(P)=p, \det(Q)=q$  都是环  $R$  的可逆元,  $a=d(A)$ , 故  $a|b, a|c, a|(x+y)$ . 令  $r=yp^{-1}q^{-1}, s=[b+(x+y)p^{-1}q^{-1}]/a, e$  为  $R$  的单位元, 则

$$X_0 = \begin{bmatrix} a & 0 & e \\ 0 & b+r & -s \\ e & e & 0 \end{bmatrix}, \quad Y_0 = \begin{bmatrix} 0 & 0 & -e \\ 0 & -r & s \\ -e & -e & c \end{bmatrix}.$$

$X=PX_0Q, Y=PY_0Q$ , 故  $A=X+Y$ , 且  $\det(X)=x, \det(Y)=y$ . 证毕.

**推论 1** 对任何矩阵  $A \in M_2(R)$  有环  $R$  的任何可逆元  $\epsilon$ , 存在行列式值为  $\epsilon$  的矩阵  $X, Y \in M_2(R)$ , 使  $A=X+Y$ . 对任何矩阵  $A \in M_3(R)$  及环  $R$  的任何可逆元  $\epsilon$ , 存在行列式值为  $\epsilon, -\epsilon$  的矩阵  $X, Y \in M_3(R)$ , 使  $A=X+Y$ .

## 3 主要结果

**定理 2** 矩阵  $A \in M_2(R)$  ( $n \geq 2$ ) 能分解为  $X+Y$ , 使  $\det(X)=x, \det(Y)=y$ , 当且仅当  $d(A)$  能被  $x-(-1)^n y$  整除.

证  $A=X+Y$ , 则  $\det(X) = \det(A-Y) \equiv \det(-Y) = (-1)^n \det(Y) \pmod{d(A)}$ . 另一方面, 若  $d(A)$  能被  $x-(-1)^n y$  整除, 则有以下情况.

(1)  $n=2k$  ( $k \leq 1$ ) 为偶数时, 设么模阵  $P, Q$  使  $PAQ = \text{diag}(a_1, a_2, \dots, a_{2k-1}, a_{2k}), a_1 = d(A)$ . 令  $A_i = \text{diag}(a_{2i-1}, a_{2i})$  ( $1 \leq i \leq k$ ). 由引理 1 及推论 1, 存在  $X_i, Y_i \in M_2(R)$ , 使得  $A_i = X_i +$

$Y_i$ , 且  $\det X_1 = (\det P)(\det Q)x$ ,  $\det Y_1 = (\det P)(\det Q)y$ ,  $\det X_i = \det Y_i = e (2 \leq i \leq k)$ , 其中  $e$  为  $R$  的单位元. 令  $X = \text{diag}(X_1, X_2, \dots, X_k)$ ,  $Y = \text{diag}(Y_1, Y_2, \dots, Y_k)$ , 则  $A = P^{-1}XQ^{-1} + P^{-1}YQ^{-1}$ , 且  $\det(P^{-1}XQ^{-1}) = x$ ,  $\det(P^{-1}YQ^{-1}) = y$ .

(2) 当  $n = 2k + 1 (k \geq 1)$  为奇数时, 同理可证.

**推论 2** 任何矩阵  $A \in M_2(R) (n \geq 2)$  恒能分解为两个素阵之和.

**推论 3** 任何  $n \geq 2$  阶整数方阵  $A$ , 恒可以无限多种方式分解为素的整数方阵  $X, Y$  之和.

**证** 任取素数  $x$ , 使  $(x, d(A)) = 1$ . 由 Dirichlet 定理<sup>[7]</sup>, 存在无限多形为  $d(A)t + (-1)^n x$  的素数  $y$ . 由定理 2, 存在整数方阵  $X, Y$ , 使  $\det X = x, \det Y = y$ , 且  $A = X + Y$ . 证毕.

## 4 子环的情况

若环  $R$  的每一个元素, 恒能分解为  $R$  中至多  $C$  (常数) 个素元之和, 则称环  $R$  为 Goldbach 环. 常数  $C$  之可能的最小值称为环的 Goldbach 数, 记为  $G(R)$ . 显然, 若熟知的 Goldbach 猜想成立, 则  $G(M_1(\mathbb{Z})) = 3$ , 其中  $\mathbb{Z}$  为整数环.

定理 2 表明, 对任何主理想环  $R$ , 当  $n \geq 2$  时,  $G(M_n(R)) = 2$ . 对一般的主理想环  $R$ , 确定  $G(M_1(R)) = G(R)$  的值, 看来是一个十分困难的问题. 我们可以进而考虑  $M_n(R)$  的子环的 Goldbach 数. 环与其子环的 Goldbach 数的关系, 从下面的结果看, 似乎是很复杂的. 设  $\mathbb{Z}$  为整数环,  $n\mathbb{Z}$  为能被  $n$  整除的整数组成的子环.

**定理 3** 设  $p$  为素数, 则  $G(p\mathbb{Z}) = 2$ .

**证** 显然,  $p\mathbb{Z}$  的素元是形为  $pt (p \nmid t)$  的数. 当  $p$  是奇素数时, 对任何整数  $n$ , 设  $n = pm + i (0 \leq i \leq p-1)$ , 则

$$pn = \begin{cases} p + p(n-1), & \text{当 } i \neq 1 \text{ 时,} \\ 2p + p(n-2), & \text{当 } i = 1 \text{ 时,} \end{cases}$$

是把  $pn$  分解为  $p\mathbb{Z}$  上两个素元之和的一种形式.

当  $p=2$  时, 若  $2 \nmid n$ , 则  $2n$  为  $2\mathbb{Z}$  上的素元; 若  $2 \mid n$ , 则  $2n = 2 + 2(n-1)$  是  $2n$  分解为  $2\mathbb{Z}$  上的两个素元之和的一种形式. 形为

$$M(a, b) = \begin{bmatrix} a & b \\ b & a \end{bmatrix}, a, b \in \mathbb{Z}$$

的矩阵全体在普通的矩阵加法与乘法运算下形成一个环, 记为  $H(1)$ , 它是  $M_2(\mathbb{Z})$  的子环.

**引理 3** 环  $H(1)$  的素元素集由如下矩阵组成: (i)  $M(\pm \frac{p+1}{2}, \pm \frac{p-1}{2}), M(\pm \frac{p-1}{2}, \pm \frac{p+1}{2})$ , 其中  $p$  是奇素数; (ii)  $M(\pm(2^n+1), \pm(2^n-1)), M(\pm(2^n-1), \pm(2^n+1))$ , 其中  $n$  为非负整数.

**证** 首先, 因为  $\det M(\pm \frac{p+1}{2}, \pm \frac{p-1}{2}) = p$ ,  $\det M(\pm \frac{p-1}{2}, \pm \frac{p+1}{2}) = -p$  为素数, 故  $M(\pm \frac{p+1}{2}, \pm \frac{p-1}{2})$  与  $M(\pm \frac{p-1}{2}, \pm \frac{p+1}{2})$  均为  $H(1)$  的素元. 又因为  $\det M(\pm(2^n+1), \pm(2^n-1)) = 2^{n+2}$ ,  $\det M(\pm(2^n-1), \pm(2^n+1)) = 2^{n+2}$ , 故若  $M(\pm(2^n+1), \pm(2^n-1)) = M(a, b) M(c, d)$ , 则

$$ac + bd = \pm(2^n + 1), ad + bc = \pm(2^n - 1), (a^2 - b^2)(c^2 - d^2) = 2^{n+2}, \quad (1)$$

从而  $(a \pm b)(c \pm d) = \pm 2$ . 若  $M(a, b)$  与  $M(c, d)$  均非么模阵, 则  $a^2 - b^2$  与  $c^2 - d^2$  均异于  $\pm 1$ . 由式(1)知,  $a$  与  $b, c$  与  $d$  同奇偶, 得  $4 | (a \pm b)(c \pm d)$ , 矛盾, 故  $M(\pm(2^n + 1), \pm(2^n - 1))$  为  $H(1)$  的素元. 同理可证,  $M(\pm(2^n - 1), \pm(2^n + 1))$  为  $H(1)$  的素元. 其次, 若  $M(x, y)$  为  $H(1)$  的素元, 当  $x, y$  有不同的奇偶性时,  $\det M(x, y)$  为奇数. 若  $\det M(x, y)$  是奇素数  $p$ , 即  $x^2 - y^2 = p$ , 则  $M(x, y)$  必取形式(i). 若  $\det M(x, y)$  为奇合数, 设  $p$  为其一素约数, 则  $1 < p < |\det M(x, y)|$ , 且  $p$  是  $x + y$  或  $x - y$  之一素约数. 令

$$u = [(y \mp x)p \pm (x \pm y)]/2p, v = [(x \mp y)p \pm (x \pm y)]/2p,$$

则  $u, v$  为整数, 且  $M(x, y) = M(\frac{p+1}{2}, \frac{p-1}{2})M(u, v)$ , 即  $M(x, y)$  不是  $H(1)$  的素元.

当  $x, y$  均为奇数时, 则  $\det M(x, y)$  能被 8 整除. 若  $\det M(x, y)$  有奇约数  $d > 1$ , 如上可证  $M(x, y)$  不是  $H(1)$  的素元. 若  $\det M(x, y) = \pm 2^{n+2}$  ( $n$  为正整数), 则  $x = \pm(2^n + 1), y = \pm(2^n - 1)$  或  $x = \pm(2^n - 1), y = \pm(2^n + 1)$ . 当  $x, y$  均为偶数时, 显然,  $M(x, y)$  为素阵, 当且仅当  $M(x/2, y/2)$  为么模阵, 即  $M(x, y)$  为形式(ii)取  $n=0$  的情况. 证毕.

**定理 4** 若 Goldbach 猜想成立, 则  $4 \leq G(H(1)) \leq 5$ .

**证** 首先举一反例证  $G(H(1)) > 3$ . 比如,  $M(120, 1)$  不能分解为  $H(1)$  中至多 3 个素阵之和. 否则, 若  $M(120, 1) = \sum_i M(x_i, y_i)$ ,  $M(x_i, y_i)$  是  $H(1)$  的素阵, 则由引理 3 得  $(x_i + y_i, x_i - y_i)$  等于  $(\epsilon_i p_i, \eta_i), (\eta_i, \epsilon_i p_i), (\epsilon_i 2^{n_i+1}, 2\eta_i)$  或  $(2\eta_i, \epsilon_i 2^{n_i+1})$ , 其中,  $p_i$  为奇素数,  $n_i$  为非负整数,  $\epsilon_i, \eta_i$  为  $+1$  或  $-1$ . 设满足上述四个式子的下标  $i$  的集合分别是  $R_1, R_2, R_3, R_4$ , 这四个集合的元素个数分别是  $r_1, r_2, r_3, r_4$ , 则  $r_1 + r_2 + r_3 + r_4 \leq 3$ , 且

$$121 = \sum_{i \in R_1} \epsilon_i p_i + \sum_{i \in R_2} \eta_i + \sum_{i \in R_3} \epsilon_i 2^{n_i+1} + \sum_{i \in R_4} 2\eta_i, \quad (2)$$

$$119 = \sum_{i \in R_1} \eta_i + \sum_{i \in R_2} \epsilon_i p_i + \sum_{i \in R_3} 2\eta_i + \sum_{i \in R_4} \epsilon_i 2^{n_i+1}. \quad (3)$$

由式(2), (3)知,  $r_1$  与  $r_3$  不能同时为零,  $r_2$  与  $r_4$  也不能同时为零, 而  $r_1 + r_2$  为奇数, 故只有如附表所示 8 种情况.

附表 关于  $r_i$  取值的情况

$r_i$	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
$r_1$	1	2	1	0	1	1	0	0
$r_2$	2	1	0	1	0	0	1	1
$r_3$	0	0	0	1	0	1	1	2
$r_4$	0	0	1	0	2	1	1	0

由情况(1)得,  $121 = p + \eta_1 + \eta_2$ , 故  $p$  是  $[119, 123]$  中的奇素数, 矛盾. 其它情况同理可证.

另一方面, 对任何  $M(a, b) \in H(1)$ , 因  $a+b, a-b$  同奇偶, 分下述两种情况讨论.

(1) 当  $a+b, a-b$  同为偶数时, 若 Goldbach 猜想成立, 则存在奇素数  $p_1, p_2, p_3, p_4$ , 使  $a+b-2 = p_1 + p_2, a-b-2 = p_3 + p_4$ . 这时,  $M(a, b) = M((p_1+1)/2, (p_1-1)/2) + M((p_2+1)/2, (p_2-1)/2) + M((p_3+1)/2, (1-p_3)/2) + M((p_4+1)/2, (1-p_4)/2)$ , 即  $M(a, b)$  能分解为  $H(1)$  上的 4 个素阵之和.

(2) 当  $a+b, a-b$  同为奇数时, 若 Goldbach 猜想成立, 则存在奇素数  $p_1, p_2, p_3, p_4, p_5$ , 使  $a+b-2 = p_1 + p_2 + p_3, a-b-3 = p_4 + p_5$ . 这时,  $M(a, b) = M((p_1+1)/2, (p_1-1)/2) + M((p_2+1)/2, (p_2-1)/2) + M((p_3+1)/2, (1-p_3)/2) + M((p_4+1)/2, (1-p_4)/2) + M((p_5+1)/2, (1-p_5)/2)$ , 即  $M(a, b)$  能分解为  $H(1)$  上的 5 个素阵之和.

$+1)/2, (p_2-1)/2)+M((p_3+1)/2, (1-p_3)/2)+M((p_4+1)/2, (1-p_4)/2)+M((p_5+1)/2, (1-p_5)/2)$ , 即  $M(a, b)$  能分解为 5 个素阵之和, 从而  $G(H(1)) \leq 5$ . 证毕.

由定理 3 与定理 4 知, 环的 Goldbach 数可能大于, 也可能小于其子环的 Goldbach 数.

本课题为校科研基金资助项目.

### 参 考 文 献

- 1 Domiaty R Z. Solution of  $x'+y'=z'$  in  $2 \times 2$  integral matrices. The Amer. Math. Monthly, 1966, 73~631
- 2 王志雄. 整数方阵的 Waring 问题. 数学的实践与认识, 1987, (2), 80~84
- 3 Newman M. Sums of squares of matrices. Pacific Journal of Mathematics, 1985, 118(2), 497~506
- 4 Vaserstein L N. Non-commutative number theory. Contemporary Mathematics, 1989, 83, 445~449
- 5 Jun Wang. Goldbach's problem in the ring  $M_n(\mathbb{Z})$ . The American Mathematical Monthly, 1992, 99, 856~857
- 6 Jacobson N B. Asic algebra. I. New York, W. H. Freeman and Company, 1985. 213~257
- 7 Hardy G H, Wright E M. An introduction to the theory of Numbers. New York: Oxford University Press, 1975. 189~227

## The Matrix Goldbach Problem on Principal Ideal Ring

Wang Zhixiong

(Dept. of Manag. Info. Sci., Huaqiao Univ., 362011, Quanzhou)

**Abstract** A study is given to the representation of matrix on principal ideal ring as the sum of prime matrices. It is proved by the author that the matrix with an order not less than two can constantly be represented as the sum of two prime matrices. Some results obtained by the author indicate that the representation relation of matrix ring and its subring is fairly complex.

**Keywords** principal ideal rings, matrices, Goldbach conjecture, prime numbers