东北数学
NORTHEAST. MATH. J.
21(3)(2005), 355–364

# Goldbach's Problem in the Matrix Ring over a Principal Ideal Domain*

HU Wei (胡 维)
(*School of Mathematics, Beijing Normal University, Beijing, 100875*)

**Abstract:** In this paper, we consider the Goldbach's problem for matrix rings, namely, we decompose an $n \times n$ $(n > 1)$ matrix over a principal ideal domain $R$ into a sum of two matrices in $\mathrm{M}_n(R)$ with given determinants. We prove the following result:

Let $n > 1$ be a natural number and $A = (a_{ij})$ be a matrix in $\mathrm{M}_n(R)$. Define $d(A) := \mathrm{g.c.d}\{a_{ij}\}$. Suppose that $p$ and $q$ are two elements in $R$. Then

(1) If $n > 1$ is even, then $A$ can be written as a sum of two matrices $X$, $Y$ in $\mathrm{M}_n(R)$ with $\det(X) = p$ and $\det(Y) = q$ if and only if $d(A) \mid p - q$;

(2) If $n > 1$ is odd, then $A$ can be written as a sum of two matrices $X$, $Y$ in $\mathrm{M}_n(R)$ with $\det(X) = p$ and $\det(Y) = q$ if and only if $d(A) \mid p + q$.

We apply the result to the matrices in $\mathrm{M}_n(\mathbb{Z})$ and $\mathrm{M}_n(\mathbb{Q}[x])$ and prove that if $R = \mathbb{Z}$ or $\mathbb{Q}[x]$, then any nonzero matrix $A$ in $\mathrm{M}_n(R)$ can be written as a sum of two matrices in $\mathrm{M}_n(R)$ with prime determinants.

**Key words:** Goldbach's problem, principle ideal domain, matrix ring
**1991 MR subject classification:** 11C20, 11L20, 13G05
**CLC number:** O151.2, O156.1, O153.3
**Document code:** A
**Article ID:** 1000-1778(2005)03-0355-10

## 1 Introduction

As is well known, Goldbach's conjecture is a famous problem in number theory which can be described as follows:

Every even integer $n$ greater than 2 is the sum of two primes.

Goldbach first conjectured this in his famous letter to Leonhard Euler dated June 7, 1742. Since then, many people have been devoted to solve this problem. However, it still remains unverified. In 1966, A Chinese famous mathematician Chen Jingrun proved that any sufficient large even natural number is the sum of a prime and a number with no more than two prime factors. Up to now, this is the best result on the conjecture.

*Received date: Jan. 21, 2004.
Foundation item: The "985 Program" of Beijing Normal University.

As we know, Goldbach's conjecture is discussed over the ring $\mathbf{Z}$, and it is a very hard problem. But if one changes the point of view and considers the similar problem in matrix rings, then things might go smoothly. For example, in [1], Vaserstein proved that given any integer $p$ and any matrix $A$ in the ring $\mathrm{M}_2(\mathbf{Z})$, there are $X, Y$ in $\mathrm{M}_2(\mathbf{Z})$ such that

$$X + Y = A$$

and

$$\det(X) = \det(Y) = p.$$

Here $\mathrm{M}_n(R)$ denotes the $n \times n$ matrix ring over a ring $R$. He also asked the analogous question for $\mathrm{M}_3(\mathbf{Z})$. In [2], Wang answered Vaserstein's question for $\mathrm{M}_n(\mathbf{Z})$ $(n > 1)$, and proved the following result:

(1) If $n > 1$ is even, then for any matrix $A$ in $\mathrm{M}_n(\mathbf{Z})$ and any $p$ in $\mathbf{Z}$, there are two matrices $X$, $Y$ in $\mathrm{M}_n(\mathbf{Z})$ such that

$$X + Y = A$$

and

$$\det(X) = \det(Y) = p.$$

(2) Let $n > 1$ be an odd integer and $p$ a fixed integer. Then for any $A$ in $\mathrm{M}_n(\mathbf{Z})$, there are $X$, $Y$ in $\mathrm{M}_n(\mathbf{Z})$ such that

$$X + Y = A$$

and

$$\det(X) = \det(Y) = p$$

if and only if $d(A)$ divides $2p$, where $d(A)$ is the greatest common divisor of all the entries of the matrix $A$.

In the present paper, we consider the following more general problem.

**Goldbach's Problem** Suppose $R$ is an arbitrary unique factorization domain. Let $A$ be a matrix in $\mathrm{M}_n(R)$ $(n > 1)$ and let $p$, $q$ be two elements in $R$. Are there two matrices $X, Y \in \mathrm{M}_n(R)$ such that $\det(X) = p$, $\det(Y) = q$ and $X + Y = A$?

In this paper, we give a positive answer to the Goldbach's problem for matrices over a principal ideal domain (PID). For a matrix $A$ in $\mathrm{M}_n(R)$, we use $d(A)$ to denote the greatest common divisor of the $n^2$ entries of $A$. Our result is the following theorem.

**Theorem 1.1** *Let two elements $p$, $q$ in a principal ideal domain $R$ and a nonzero matrix $A$ in $\mathrm{M}_n(R)$ be given.*

(1) *If $n > 1$ is even, then $A$ can be written as a sum of two matrices $X$, $Y$ in $\mathrm{M}_n(R)$ with $\det(X) = p$ and $\det(Y) = q$ if and only if $d(A) \mid p - q$;*

(2) *If $n > 1$ is odd, then $A$ can be written as a sum of two matrices $X$, $Y$ in $\mathrm{M}_n(R)$ with $\det(X) = p$ and $\det(Y) = q$ if and only if $d(A) \mid p + q$.*

In particular, we consider matrices over $\mathbf{Z}$ and $\mathbf{Q}[x]$, which are both principal ideal domains. We get the following corollary.

**Corollary 1.1** *Let $R$ be $\mathbb{Z}$ or $\mathbb{Q}[x]$ and let $A$ be a nonzero matrix in $\mathrm{M}_n(R)$ $(n > 1)$. Then there are infinitely many pairs of prime elements $p$, $q$ in $R$ such that the matrix $A$ can be written as a sum of two matrices $X, Y \in \mathrm{M}_n(R)$ with $\det(X) = p$ and $\det(Y) = q$.*

## 2 Definitions and Preliminaries

In this section, we give some basic definitions and two useful lemmas needed in this paper.

Let $R$ be a principal ideal domain (PID). We denote by $\mathrm{M}_n(R)$ the ring of all $n \times n$ matrices over $R$. For a matrix $A \in \mathrm{M}_n(R)$ we denote by $d(A)$ the greatest common divisor of the $n^2$ entries of $A$.

Two matrices $A, B \in \mathrm{M}_n(R)$ are said to be equivalent if there are two matrices $U, V \in \mathrm{M}_n(R)$ with $\det(U) = \det(V) = 1$ such that $B = UAV$.

Now we give the following useful lemma.

**Lemma 2.1**([3], p.26) *Let $R$ be a* PID *and let $A$ be a matrix in $\mathrm{M}_n(R)$. Then $A$ is equivalent to a diagonal matrix*

$$D = \mathrm{diag}[d, d_2, \cdots, d_n]$$

*in $\mathrm{M}_n(R)$, where $d = d(A)$.*

Let $A$ and $B$ be two matrices in $\mathrm{M}_n(R)$ which are equivalent. If we want to decompose the matrix $A$ into a sum of two matrices in $\mathrm{M}_n(R)$ with given determinants, we can deal with $B$ instead of $A$. Thus, by Lemma 2.1, we can assume that $A$ itself is a diagonal matrix with $d(A)$ in its (1,1)-position.

In the proof of Theorem 3.3 below, we shall use the following lemma.

**Lemma 2.2**(Eisenstein's criterion, see [4], p.72) *Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial in $\mathbb{Z}[x]$. If there is a prime number $p$ such that the following three conditions are satisfied:*

(1) $p \nmid a_n$;

(2) $p \mid a_i$ *for* $i = 0, 1, \cdots, n-1$;

(3) $p^2 \nmid a_0$,

*then $f(x)$ is irreducible over $\mathbb{Q}$.*

A polynomial in $\mathbb{Z}[x]$ satisfying the three conditions in Lemma 2.2 is called an Eisenstein polynomial over $\mathbb{Q}$. Hence Lemma 2.2 can be rewritten as "Every Eisenstein polynomial over $\mathbb{Q}$ is irreducible over $\mathbb{Q}$".

## 3 Results and Proofs

In this section, $R$ always denotes a PID. We shall first consider the matrices in $\mathrm{M}_n(R)$ and prove Theorem 3.1 below. Then, we use Theorem 3.1 to investigate matrices in $\mathrm{M}_n(\mathbb{Z})$ and matrices in $\mathrm{M}_n(\mathbb{Q}[x])$ respectively.

Now let us use Lemma 2.1 to prove the following result.

**Theorem 3.1** *Let $n > 1$ be a natural number and let $A$ be a nonzero matrix in $\mathrm{M}_n(R)$. Suppose that $p$ and $q$ are two elements in $R$. Then*

(1) *If $n$ is even, then there are two matrices $X$ and $Y$ in $\mathrm{M}_n(R)$ such that $\det(X) = p$, $\det(Y) = q$ and $A = X + Y$ if and only if $d(A) \mid p - q$.*

(2) *If $n$ is odd, then there are two matrices $X$ and $Y$ in $\mathrm{M}_n(R)$ such that $\det(X) = p$, $\det(Y) = q$. and $A = X + Y$ if and only if $d(A) \mid p + q$.*

*Proof.* By Lemma 2.1, we may assume that $A$ itself is a diagonal matrix with $d(A)$ in its (1,1)-position and denote $A$ by $\mathrm{diag}[d, d_2, \cdots, d_n]$, where $d = d(A)$.

(1) $n > 1$ is an even integer. Suppose $n = 2m$. If there are two matrices $X$ and $Y$ in $\mathrm{M}_n(R)$ such that $\det(X) = p$, $\det(Y) = q$ and $A = X + Y$, then

$$X = A - Y \equiv -Y (\mathrm{mod}\ d).$$

Hence

$$\det(X) \equiv \det(-Y) (\mathrm{mod}\ d).$$

Since $n$ is even, we have

$$\det(-Y) = \det(Y).$$

So

$$p \equiv q (\mathrm{mod}\ d),$$

that is,

$$d \mid p - q.$$

Conversely, suppose $p - q = kd$. Multiplying the first row of $A$ by $k$ and adding it to the second row, we get

$$A' = \begin{pmatrix} d & 0 & 0 & \cdots & 0 \\ p-q & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & d_n \end{pmatrix}.$$

Obviously, $A$ is equivalent to $A'$, so we only need to consider the matrix $A'$. Put

$$X_1 = \begin{pmatrix} d & -1 \\ p & 0 \end{pmatrix}, \qquad Y_1 = \begin{pmatrix} 0 & 1 \\ -q & d_2 \end{pmatrix}$$

and put

$$X_i = \begin{pmatrix} d_{2i-1} & -1 \\ 1 & 0 \end{pmatrix}, \qquad Y_i = \begin{pmatrix} 0 & 1 \\ -1 & d_{2i} \end{pmatrix}$$

for $i = 2, 3, \cdots, m$. Define

$$X = \mathrm{diag}[X_1, X_2, \cdots, X_m], \qquad Y = \mathrm{diag}[Y_1, Y_2, \cdots, Y_m].$$

Then we have

$$\det(X) = p, \qquad \det(Y) = q$$

and

$$A' = X + Y.$$

(2) $n > 1$ is an odd integer. If there are two matrices $X$ and $Y$ in $\mathrm{M}_n(R)$ such that

$$\det(X) = p, \qquad \det(Y) = q$$

and

$$A = X + Y,$$

then

$$X = A - Y \equiv -Y(\mathrm{mod}\ d).$$

Hence

$$\det(X) \equiv \det(-Y)(\mathrm{mod}\ d).$$

Since $n$ is odd, we have

$$\det(-Y) = -\det(Y).$$

So

$$p \equiv -q(\mathrm{mod}\ d),$$

that is,

$$d \mid p + q.$$

Conversely, suppose $p + q = kd$. From the discussion for the case (1), we only need to consider the case $n = 3$. Suppose that

$$A = \mathrm{diag}[d, d_2, d_3]$$

with $d = d(A)$. Multiplying the first row of $A$ by $k$ and adding it to the third row, we get the matrix

$$A' = \begin{pmatrix} d & 0 & 0 \\ 0 & d_2 & 0 \\ p+q & 0 & d_3 \end{pmatrix},$$

which is equivalent to $A$. Thus we need only to consider $A'$ instead of $A$. Let

$$X = \begin{pmatrix} d & 1 & 0 \\ 0 & 0 & 1 \\ p & 0 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -1 & 0 \\ 0 & d_2 & -1 \\ q & 0 & d_3 \end{pmatrix}.$$

Then we have

$$\det(X) = p, \qquad \det(Y) = q$$

and

$$A' = X + Y.$$

**Remark** The above proof of the converse direction does not work for $n = 1$.

Since both $\mathbb{Z}$ and $\mathbb{Q}[x]$ are PIDs, we shall use Theorem 3.1 to investigate matrices in $\mathrm{M}_n(\mathbb{Z})$ and $\mathrm{M}_n(\mathbb{Q}[x])$ respectively and prove Corollary 1.1 mentioned in the introduction. First, we give the definition of prime matrix.

**Definition 3.1** *Let $R$ be a* PID. *A matrix $X$ in $\mathrm{M}_n(R)$ is called a prime matrix if* $\det(X)$ *is a prime element in $R$.*

For our purpose, we also need the following lemmas. For the convenience of the reader, we provide their proofs.

**Lemma 3.1** *Let $m \neq 0$ be an integer. Then there are infinitely many pairs of prime numbers $p$, $q$ such that $m \mid p - q$.*

*Proof.* Clearly, we can assume that $m > 0$. Let $\{p_1, p_2, p_3, \cdots\}$ be the complete set of prime numbers. Then for any $k \in \mathbb{N}$, the set $\{p_{k(m+1)+1}, p_{k(m+1)+2}, \cdots, p_{(k+1)(m+1)}\}$ must contain two prime numbers $p_i$, $p_j$ such that $p_i \equiv p_j \pmod{m}$. Thus $m \mid p_i - p_j$ and this completes the proof.

**Lemma 3.2**(Dirichlet, see [5], p.188) *Let $m$ and $l$ be integers. Suppose that $m \geq 2$, $1 \leq l < m$ and $(m, l) = 1$. Then there are infinitely many prime numbers in the set $\{tm + l | t \geq 0,\ t \in \mathbb{Z}\}$.*

Using Lemma 3.2, we get the following corollary.

**Corollary 3.1** *Let $m \neq 0$ be an integer. Then there are infinitely many pairs of prime numbers $p, q$ such that $m \mid p + q$.*

*Proof.* Clearly, we can assume that $m > 0$. If $m = 1$, it is trivial. We assume that $m \geq 2$. By Lemma 3.2, there are infinitely many prime numbers in the set $A = \{tm + 1 | t \geq 0,\ t \in \mathbb{Z}\}$ since $(m, 1) = 1$. Similarly, there are infinitely many prime numbers in the set $B = \{tm + m - 1 | t \geq 0,\ t \in \mathbb{Z}\}$ since $(m, m - 1) = 1$. Thus for any prime number $p$ in $A$ and any prime number $q$ in $B$, we have

$$p + q \equiv 0 \pmod{m},$$

that is, $m \mid p + q$. Hence the corollary is proved.

By Lemma 3.1 and Corollary 3.1, we are able to prove the following result, which says that the Goldbach's conjecture is true for the matrix ring $\mathrm{M}_n(\mathbb{Z})$, $n > 1$.

**Theorem 3.2** *Let $A$ be a nonzero matrix in $\mathrm{M}_n(\mathbb{Z})$, where $n > 1$. There are infinitely many pairs of prime numbers $p, q$ such that the matrix $A$ can be written as a sum of two prime matrices $X, Y \in \mathrm{M}_n(\mathbb{Z})$ with $\det(X) = p$ and $\det(Y) = q$.*

*Proof.* Let $d = d(A)$. Then $d \neq 0$. To prove the theorem, we consider the following two cases:

(1) $n > 1$ is even. By Lemma 3.1, there are infinitely many pairs of prime numbers $p$, $q$ such that $d \mid p - q$. By Theorem 3.1, we can find two matrices $X, Y \in \mathrm{M}_n(\mathbb{Z})$ with $\det(X) = p$, $\det(Y) = q$ such that

$$A = X + Y.$$

But $\det(X)$ and $\det(Y)$ are prime numbers, and hence $X$, $Y$ are prime matrices.

(2) $n > 1$ is odd. By Corollary 3.1, there are infinitely many pairs of prime numbers $p$, $q$ such that $d \mid p + q$. By Theorem 3.1, we can find two matrices $X, Y \in \mathrm{M}_n(\mathbb{Z})$ with $\det(X) = p$, $\det(Y) = q$ such that

$$A = X + Y.$$

Since $X$ and $Y$ are prime matrices, the theorem is proved.

Now we give an example. Let

$$A = \begin{pmatrix} 3 & -3 & 6 \\ 6 & -3 & 12 \\ 9 & -9 & 27 \end{pmatrix}.$$

Then

$$d(A) = 3.$$

We take $p = 7$ from the set $\{3k+1|k \in \mathbb{Z}\}$ and $q = 11$ from the set $\{3k+2|k \in \mathbb{Z}\}$. Let

$$X = \begin{pmatrix} 3 & -2 & 6 \\ 6 & -4 & 13 \\ -2 & -1 & -4 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 1 & -1 \\ 11 & -8 & 31 \end{pmatrix}.$$

We have

$$\det(X) = 7, \qquad \det(Y) = 11$$

and

$$X + Y = A.$$

In the rest of this section, we consider matrices in $\mathrm{M}_n(\mathbb{Q}[x])$ $(n > 1)$ and prove Theorem 3.4 below. Note that the prime elements in $\mathbb{Q}[x]$ are just the irreducible polynomials in $\mathbb{Q}[x]$.

To prove our next result, we first show the following lemma.

**Lemma 3.3** *Let $p$, $q$ be two prime numbers with $p \neq q$. Then there are two integers $s$, $t$ such that $sp+tq=1$ with $p \nmid s$ and $q \nmid t$.*

*Proof.* Clearly, there are two integers $a, b$ such that

$$ap + bq = 1.$$

If $p \nmid a$ and $q \nmid b$, we define

$$s = a, \qquad t = b.$$

Now we assume that $p \mid a$ or $q \mid b$. To find two required integers $s$ and $t$, we consider the following two cases.

Case 1: One of $p$ and $q$ is 2. Without loss of generality, we assume $p = 2$. Then we again consider two cases:

Case (1): $p \mid a$. If $q \nmid b - p$, we define

$$s = a + q, \qquad t = b - p.$$

It is easy to see that $p \nmid s$, $q \nmid t$ and $sp + tq = 1$.

If $q \mid b - p$, we define

$$s = a + 3q, \qquad t = b - 3p.$$

It is easy to verify that $p \nmid s$, $q \nmid t$ and $sp + tq = 1$.

Case (2): $p \nmid a$. By our hypothesis, we have $q \mid b$. Define

$$s = a + 2q, \qquad t = b - 2p,$$

and we have $s$, $t$ are as required.

Case 2: Both $p$ and $q$ are odd prime numbers. Similarly, we need to consider two cases:

Case (1): $p \mid a$. Clearly,

$$(a+q)p + (b-p)q = 1.$$

If $q \nmid b-p$, we define

$$s = a+q, \qquad t = b-p;$$

If not, we define

$$s = a+2q, \qquad t = b-2p.$$

In either of the two cases, we have $p \nmid s$, $q \nmid t$ and $sp+tq = 1$.

Case (2): $p \nmid a$. By our hypothesis, we have $q \mid b$. Similarly, we can get two required integers $s$, $t$.

Using the above lemma, together with Eisenstein's criterion, we can get the following theorem.

**Theorem 3.3** *For every polynomial $f(x)$ of positive degree in $\mathbb{Q}[x]$, there are infinitely many pairs of irreducible polynomials $p(x)$, $q(x)$ in $\mathbb{Q}[x]$ such that*

$$p(x) + q(x) = f(x)$$

*and*

$$\deg f(x) = \deg p(x) = \deg q(x).$$

*Proof.* Let $f(x)$ be a polynomial in $\mathbb{Q}[x]$ of positive degree. Clearly, $f(x) \neq 0$ and there is a non-zero element $k$ in $\mathbb{Q}$ such that

$$kf(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

is in $\mathbb{Z}[x]$ and $a_n \neq 0$. We shall use Eisenstein's criterion to give two irreducible polynomials

$$g(x) = g_0 + g_1x + \cdots g_nx^n, \qquad h(x) = h_0 + h_1x + \cdots h_nx^n$$

in $\mathbb{Z}[x]$ such that

$$g(x) + h(x) = kf(x).$$

We consider the following two cases:

Case 1: $a_0 = 0$. Clearly, we can find infinitely many pairs of prime numbers $p$, $q$ such that

$$q - p > |a_n| + 1.$$

Now we define

$$g_n = p-1, \qquad h_n = a_n - (p-1).$$

Clearly, $p \nmid g_n$ and $q \nmid h_n$ since $|h_n| \leq |a_n| + 1 + p < q$. Obviously,

$$(p, q) = 1.$$

Thus there are two integers $s$, $t$ such that

$$sp + tq = 1.$$

Now define

$$g_0 = pq, \qquad h_0 = -pq$$

and

$$g_i = a_i sp, \qquad h_i = a_i tq$$

for $i = 1, \cdots, n-1$. We have that both $g(x)$ and $h(x)$ are Eisenstein polynomials over $\mathbb{Q}$. Define

$$p(x) = \frac{1}{k} g(x), \qquad q(x) = \frac{1}{k} h(x).$$

We have that $p(x)$ and $q(x)$ are irreducible. Clearly

$$p(x) + q(x) = f(x), \qquad \deg f(x) = \deg p(x) = \deg q(x).$$

Case 2: $a_0 \neq 0$. Since $a_0$ can only have finite prime factors, we can find infinitely many pairs of prime numbers $p$, $q$ such that

$$p \nmid a_0, \qquad q \nmid a_0$$

and

$$q - p > |a_n| + 1.$$

First, we determine the leading coefficients of $g(x)$ and $h(x)$. We define

$$g_n = p - 1, \qquad h_n = a_n - (p - 1).$$

Clearly, $p \nmid g_n$ and $q \nmid h_n$ since $|h_n| \leq |a_n| + 1 + p < q$. By Lemma 3.3, there are two integers $s$, $t$ with $p \nmid s$ and $q \nmid t$ such that

$$sp + tq = 1.$$

Now define

$$g_i = a_i sp, \qquad h_i = a_i tq$$

for $i = 0, 1, \cdots, n-1$. Then $p$ divides $g_i$ and $q$ divides $h_i$ for $i = 1, 2, \cdots, n-1$. Furthermore, $p^2 \nmid a_0 sp$ and $q^2 \nmid a_0 tq$ since $p$, $q$ are not factors of $a_0$ and $p \nmid s$, $q \nmid t$. By Eisenstein's criterion, $g(x)$ and $h(x)$ are irreducible in $\mathbb{Q}[x]$. Define

$$p(x) = \frac{1}{k} g(x), \qquad q(x) = \frac{1}{k} h(x).$$

$p(x)$ and $q(x)$ are also irreducible. Obviously,

$$p(x) + q(x) = f(x), \qquad \deg f(x) = \deg p(x) = \deg q(x).$$

Now we prove the following theorem, which says that Goldbach's conjecture is true for the matrix ring $\mathrm{M}_n(\mathbb{Q}[x])(n > 1)$.

**Theorem 3.4** *Let $A$ be a non-zero matrix in $\mathrm{M}_n(\mathbb{Q}[x])$ with $n > 1$. Then there are infinitely many pairs of prime elements (irreducible polynomials) $p(x)$, $q(x)$ in $\mathbb{Q}[x]$ such that the matrix $A$ can be written as a sum of two prime matrices $X, Y \in \mathrm{M}_n(\mathbb{Q}[x])$ with $\det(X) = p(x)$ and $\det(Y) = q(x)$.*

*Proof.* Let

$$d(x) = d(A).$$

By hypothesis, $d(x) \neq 0$ and hence $xd(x)$ must have positive degree. By Theorem 3.3, there are infinitely many pair of irreducible polynomials $g(x)$, $h(x)$ in $\mathbb{Q}[x]$ such that

$$xd(x) = g(x) + h(x).$$

If $n$ is even, we define

$$p(x) = g(x), \qquad q(x) = -h(x).$$

Then $p(x)$ and $q(x)$ are irreducible and $d(x) \mid p(x) - q(x)$. By Theorem 3.1, there are two matrices $X, Y \in \mathrm{M}_n(\mathbb{Q}[x])$ such that

$$\det(X) = p(x), \qquad \det(Y) = q(x)$$

and

$$A = X + Y.$$

If $n$ is odd, we define

$$p(x) = g(x), \qquad q(x) = h(x).$$

Then $p(x)$ and $q(x)$ are irreducible and $d(x) \mid p(x) + q(x)$. Again by Theorem 3.1, there are two matrices $X, Y \in \mathrm{M}_n(\mathbb{Q}[x])$ such that

$$\det(X) = p(x), \qquad \det(Y) = q(x)$$

and

$$A = X + Y.$$

**Acknowledgements** This article is completed under the careful supervision of Prof. Changchang Xi. I would like to thank him for suggestions. I also thank Li Weixia for reading the paper and her comments.

# References

[1] Vaserstein, L. N., Non-commutative number theory, *Contemp. Math.*, **83**(1989), 445–449.

[2] Wang, J., Goldbatch's problem in the ring $\mathrm{M}_n(\mathbb{Z})$, *Amer. Math. Soc. Monthly*, **99**(1992), 856–857.

[3] Newman, M., Integral Matrices, Academic Press, New York and London, 1972.

[4] Zhang, H. R. and Hao, B. X., Advanced Algebra (in Chinese), Higher Education Press, Beijing, 1983.

[5] Feng, K. Q., Algebraic Number Theory (in Chinese), Science Publishing House, Beijing, 2000.