Publ. Math. Debrecen
61 / 3-4 (2002), 487–494

On Fermat's problem in matrix rings and groups

By Z. PATAY (Békéscsaba) and A. SZAKÁCS (Békéscsaba)

Abstract. We describe the periodic elements in $GL_2(\mathbb{Z})$ and give the answer to some problems concerning Fermat's equation $X^m+Y^m=Z^m$ (F) in matrix groups and in irreducible elements of matrix rings, proposed by L. N. Vaserstein and A. Khazanov. Namely: (1) equation (F) has solutions in $GL_2(\mathbb{C})$ for every m; (2) if $m=3$ or $m\equiv\pm1 \pmod 3$, then (F) has solutions in $SL_3(\mathbb{Z})$; (3) if m is odd, then equation (F) has solutions in $M_2(\mathbb{Z})$ in irreducible elements; (4) if $m\equiv\pm1 \pmod 3$ or $m=n\geq 2$, then (F) has solutions in irreducible elements of matrix rings $M_3(\mathbb{Z})$ and $M_n(\mathbb{Z})$ respectively.

1. Introduction

We consider the solution of Fermat's equation

$$X^m+Y^m=Z^m \quad (m\in\mathbb{N}) \tag{F}$$

in the ring $M_n(\mathbb{Z})$ of $n\times n$-matrices over the ring $\mathbb{Z}$ of integers.

It is proved in [4] that equation $X^4+Y^4=Z^4$ is solvable in $M_2(\mathbb{Z})$. It is also easy to see that if $n\geq 2$, then there are such idempotent elements A and B that $A+B=E$, where E is the identity matrix, and so $A^m+B^m=E^m$ for every $m\geq 1$.

Equation (F) was studied with distinct restrictions in papers [1]–[14] in the ring $M_n(\mathbb{Z})$ and in $M_n(R)$ over a commutative ring R with unit element.

Mathematics Subject Classification: 11D41, 15A24, 15A36.
Key words and phrases: Fermat equation, irreducible element, matrix equations, groups, rings.
The research was supported (partially) by Hungarian National Foundation for Scientific Research grant No. T037202.

The question about the solvability of (F) in the group $GL_2(\mathbb{Z})$ was studied at first by L. N. Vaserstein in [14].

The solvability of (F) in the set of positive integer powers of a matrix A with elements $a_{11} = 0, a_{12} = a_{21} = a_{22} = 1$ was studied in [5] and [6].

In [8] and [11] a general result has been proved: if $A \in M_2(Z)$ and $n > 2$, then the equation (F) has solution (X, Y, Z) with $X, Y, Z \in \mathcal{A} = \{A^k \mid k \in N\}$ if and only if A is nilpotent or $\operatorname{tr} A = \det A = 1$. Evidently $X, Y, Z \in SL_2(\mathbb{Z})$ and we can (by [8], [10]) determine effectively all such solutions.

Paper [7] contains the following result: let $A \in M_n(\mathbb{C})$, $n \geq 2$ and $A^x + A^y = A^z$ for some positive integers x, y, z. If A has at least one real eigenvalue $\alpha > \sqrt{2}$, then $\max\{x - z, y - z\} = -1$. Many interesting consequences can be obtained from this assertion.

A. Khazanov in [9] proved that in $GL_3(\mathbb{Z})$ solutions do not exist if m is a multiple of either 21 or 96, and in $SL_3(\mathbb{Z})$ solutions do not exist if m is a multiple of 48. Paper [12] gives another proof of Khazanov's result (see [9], Corollary 4) on the solvability of (F) in $SL_2(\mathbb{Z})$.

L. N. Vaserstein proposed the following problem: *how about solutions of the equation (F) in $SL_2(\mathbb{Z})$ or in $GL_3(\mathbb{Z})$; or in irreducibles X, Y, Z of the ring $M_2(\mathbb{Z})$?* Later A. Khazanov called attention to the fact that *the equation $X^3 + Y^3 = Z^3$ is still unsolved in $SL_3(\mathbb{Z})$ and in $GL_3(\mathbb{Z})$ as well as in $SL_3(\mathbb{Q})$.*

We give the answers to some of these questions and their generalizations.

Here $GL_n(\mathbb{Z})$ is the group of units of the ring $M_n(\mathbb{Z})$ and

$$SL_n(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det A = 1\}.$$

An element x of a ring R is called *irreducible*, if it is neither a unit nor the product yz of two elements y, z of R, both not units. A matrix X in $M_n(\mathbb{Z})$ is irreducible if and only if $\det X = \pm p$ for a prime p.

2. Description of the elements in $GL_2(\mathbb{Z})$

In this part we give a description of the elements in $GL_2(\mathbb{Z})$ by proving the following theorem:

Theorem 2.1. *Let $A \in GL_2(\mathbb{Z})$ and A is a periodic element. Then we have:*

1° *if* $\operatorname{ord} A = 1$, *then* $A = E$.

2° *if* $\operatorname{ord} A = 2$, *then either* $\operatorname{tr} A = -2$ *and* $A = -E$, *or* $\operatorname{tr} A = 0$ *and* $A = \pm\begin{pmatrix} 1 & 0 \\ z & -1 \end{pmatrix}$, *or* $A = \begin{pmatrix} z & v \\ (1-z^2)v^{-1} & -z \end{pmatrix}$, *where* $z \in \mathbb{Z}$ *and* $v \mid 1 - z^2$.

3° *if* $\operatorname{ord} A = 3$, *then* $A = \begin{pmatrix} z & -v \\ (1+z+z^2)v^{-1} & -1-z \end{pmatrix}$ *for some* $z \in \mathbb{Z}$ *and* $v \mid 1 + z + z^2$.

4° *if* $\operatorname{ord} A = 4$, *then* $A = \begin{pmatrix} z & -v \\ (1+z^2)v^{-1} & -z \end{pmatrix}$, *where* $z \in \mathbb{Z}$ *and* $v \mid 1 + z^2$.

5° *if* $\operatorname{ord} A = 6$, *then* $A = \begin{pmatrix} -z & -v \\ (1+z+z^2)v^{-1} & 1+z \end{pmatrix}$ *for some* $z \in \mathbb{Z}$ *and* $v \mid 1 + z + z^2$.

Proof. It is well-known (see for example [7] or [9]) that any periodic matrix in $GL_2(\mathbb{Z})$ has order 1, 2, 3, 4 or 6 and if A is an arbitrary matrix of $M_2(\mathbb{Z})$, $t = \operatorname{tr} A$ and $d = \det A$, then for every natural n the n-th power of A can be written in the form $A^n = u_n A - d u_{n-1} E$, where $u_0 = 0$, $u_1 = 1$, $u_2 = t$ and $u_n = t u_{n-1} - d u_{n-2}$ for $n \geq 3$. Therefore, for a nondiagonal matrix $A \in M_2(\mathbb{Z})$ and for some nonzero $k \in \mathbb{Z}$ the equality $A^n = kE$ holds if and only if in the series $u_0, u_1, u_2, u_3, \ldots$ the element u_n is zero. Indeed, suppose $A^n = kE$ and $A = (a_{ij})$. Then $u_n A = A^n + d u_{n-1} E = (k + d u_{n-1})E$ and $u_n a_{12} = u_n a_{21} = 0$. Since $a_{12} \neq 0$ or $a_{21} \neq 0$, we have $u_n = 0$. Conversely, in case $u_n = 0$, $A^n = -d u_{n-1} E = kE$ with $k = -d u_{n-1}$.

Let $\operatorname{ord} A = 2$ and A diagonal. Then $A = -E$ or $A = \pm\begin{pmatrix} 1 & 0 \\ z & -1 \end{pmatrix}$. Let A be a nondiagonal. Then $u_2 = \operatorname{tr} A = 0$, so $A = \begin{pmatrix} z & v \\ u & -z \end{pmatrix}$. If $v = 0$, then $z^2 = 1$ and $A = \pm\begin{pmatrix} 1 & 0 \\ u & -1 \end{pmatrix}$, $u \in \mathbb{Z}$. If $v \neq 0$, then $z^2 + uv = 1$, u and v are divisors of $1 - z^2$ and $A = \begin{pmatrix} z & v \\ (1-z^2)v^{-1} & -z \end{pmatrix}$, where $z \in \mathbb{Z}$ and $v \mid 1 - z^2$.

Let $\operatorname{ord} A = 3$. Then $d \cdot t = -1$, $0 = u_3 = t^2 - d$. This iplies $d = 1$, $t = -1$ and $A = \begin{pmatrix} z & -v \\ u & -1-z \end{pmatrix}$. So $1 = d = -z - z^2 + uv$ and $uv = 1 + z + z^2$.

Let $\operatorname{ord} A = 4$. Then $u_4 = t^3 - 2dt = 0$, $du_3 = d(t^2 - d) = -1$. The case $t \neq 0$ is impossible, since from it $t^2 - 2d = 0$ follows, so $t^2 - d = d$ and $d^2 = -1$. Therefore $t = 0$, $A = \begin{pmatrix} z & -v \\ u & -z \end{pmatrix}$, $A^2 = \begin{pmatrix} z^2 - uv & 0 \\ 0 & z^2 - uv \end{pmatrix} = -E$ and $uv = 1 + z^2$.

Let $\operatorname{ord} A = 6$. Then $0 = u_6 = t^5 - 4dt^3 + 3d^2 t$, $1 = du_5 = d(t^4 - 3dt^2 + d^2)$. Since $A^3 = -E$, $A^2 \neq E$, it follows $d = 1$, $t = 1$. It is easy to prove that in this case A has form $A = \begin{pmatrix} -z & -v \\ (1+z+z^2)v^{-1} & 1+z \end{pmatrix}$, where $z \in \mathbb{Z}$ and $v \mid 1 + z + z^2$. The theorem is proved.

Theorem 2.2. *Let $\mathbb{C}$ be the field of complex numbers. The equation (F) has infinitely many solutions in the group $GL_2(\mathbb{C})$ for every m.*

Proof. Let u be an arbitrary integer. The matrices

$$A = \begin{pmatrix} u & 1 \\ -1-u-u^2 & -1-u \end{pmatrix}, \quad B = \begin{pmatrix} -1-u & -1 \\ 1+u+u^2 & u \end{pmatrix}$$

are elements of order 3 in $GL_2(\mathbb{C})$ and $A + B = -E$. By [3] for every m there exist some A_m, B_m and C_m in $M_2(\mathbb{C})$, for which $(A_m)^m = A$, $(B_m)^m = B$ and $(C_m)^m = -E$. The matrices A_m, B_m and C_m belong to $GL_2(\mathbb{C})$ and (A_m, B_m, C_m) is a solution of the equation (F).

Theorem 2.3. *If $UT_n(\mathbb{Z})$ is the subgroup of upper (or lower) triangular matrices of $GL_n(\mathbb{Z})$ and $m \geq 1$, then the equation (F) has no solutions in $UT_n(\mathbb{Z})$.*

Proof. Suppose that $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ and (A, B, C) is a solution of (F). Since for every $A \in UT_n(\mathbb{Z})$ the equation $\det A = a_{11} a_{22} \cdots a_{nn} = \pm 1$ holds, it follows that $a_{ii} \in \{-1; 1\}$, and similarly, $b_{ii} \in \{-1; 1\}, c_{ii} \in \{-1; 1\}$. From the equation $A^m + B^m = C^m$ it follows that $a_{ii}^m + b_{ii}^m = c_{ii}^m$. Then $c_{ii} \in \{-2; 0; 2\}$, which contradicts $c_{ii} \in \{-1; 1\}$. The theorem is proved.

3. Fermat's equation in $SL_3(\mathbb{Z})$

Theorem 3.1. *If $m \equiv \pm 1 \pmod 3$, then the equation (F) has solutions in $SL_3(\mathbb{Z})$.*

Proof. Obviously

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} -1 & 1 & -1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

are the elements of order 3 in $SL_3(\mathbb{Z})$ and $A + B = C$.

If $m \equiv 1 \pmod 3$, then $A^m + B^m = A + B = C = C^m$ and so (A, B, C) is a solution of (F).

Let $m \equiv -1 \pmod 3$. Then (A^2, B^2, C^2) is a solution of (F). The theorem is proved.

Theorem 3.2. *The equation $X^3 + Y^3 = Z^3$ has solutions in $SL_3(\mathbb{Z})$.*

Proof. It is easy to verify that (A, B, C) with the following elements A, B and C is a solution of the equation $X^3 + Y^3 = Z^3$ in $SL_3(\mathbb{Z})$. We also give the elements A^3, B^3, C^3 below.

1) $$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & -1 \\ -1 & -1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$A^3 = \begin{pmatrix} 0 & -1 & 2 \\ -1 & -3 & 3 \\ 2 & 3 & -1 \end{pmatrix}, \quad B^3 = \begin{pmatrix} 1 & 2 & -1 \\ 1 & 4 & -2 \\ -1 & -3 & 2 \end{pmatrix}, \quad C^3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

and A, B, C are not periodic elements.

2) $$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 1 & 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{pmatrix},$$

$$A^3 = \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad B^3 = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}, \quad C^3 = \begin{pmatrix} 1 & 0 & -1 \\ -1 & 1 & 1 \\ 1 & -1 & 0 \end{pmatrix},$$

A, B are elements of order 4 and C is not a periodic element.

3) $$A=\begin{pmatrix}0&1&0\\-1&0&0\\1&0&1\end{pmatrix},\ B=\begin{pmatrix}0&1&1\\0&0&1\\1&0&0\end{pmatrix},\ C=\begin{pmatrix}0&1&0\\0&0&1\\1&0&1\end{pmatrix},$$

$$A^3=\begin{pmatrix}0&-1&0\\1&0&0\\0&1&1\end{pmatrix},\ B^3=\begin{pmatrix}1&1&1\\0&1&1\\1&0&1\end{pmatrix},\ C^3=\begin{pmatrix}1&0&1\\1&1&1\\1&1&2\end{pmatrix},$$

A is an element of order 4 and B, C are not periodic elements.

4) $$A=\begin{pmatrix}0&0&1\\0&-1&-1\\1&1&0\end{pmatrix},\ B=\begin{pmatrix}1&1&0\\0&-1&0\\0&0&-1\end{pmatrix},\ C=\begin{pmatrix}1&0&0\\0&0&1\\1&-1&0\end{pmatrix},$$

$$A^3=\begin{pmatrix}0&-1&0\\1&1&-1\\0&1&1\end{pmatrix},\ B^3=\begin{pmatrix}1&1&0\\0&-1&0\\0&0&-1\end{pmatrix},\ C^3=\begin{pmatrix}1&0&0\\1&0&-1\\0&1&0\end{pmatrix},$$

A is not a periodic element, B is an element of order 2 and C has order 4.

5) $$A=\begin{pmatrix}0&0&-1\\0&1&0\\1&0&1\end{pmatrix},\quad B=\begin{pmatrix}-1&0&1\\1&1&-1\\-1&1&0\end{pmatrix},\quad C=\begin{pmatrix}0&1&0\\0&0&1\\1&0&-1\end{pmatrix},$$

$$A^3=\begin{pmatrix}-1&0&0\\0&1&0\\0&0&-1\end{pmatrix},\ B^3=\begin{pmatrix}2&0&-1\\-1&0&1\\1&-1&1\end{pmatrix},\ C^3=\begin{pmatrix}1&0&-1\\-1&1&1\\1&-1&0\end{pmatrix},$$

A is an element of order 6, B, C are not periodic elements. The theorem is proved.

4. Fermat's equation in irreducible elements of the rings $M_2(\mathbb{Z})$ and $M_3(\mathbb{Z})$

Let us now consider the solution of (F) in irreducibles X, Y, Z of the rings $M_2(\mathbb{Z})$ and $M_3(\mathbb{Z})$.

Theorem 4.1. *If m is odd, then the equation (F) has solutions in $M_2(\mathbb{Z})$ in irreducible elements.*

Proof. Let

$$A=\begin{pmatrix}-i+1 & -i^2+2i+2\\ 1 & i-1\end{pmatrix},\quad B=\begin{pmatrix}-i-2 & -i^2-4i-1\\ 1 & i+2\end{pmatrix},$$

$$C=\begin{pmatrix}-2i-1 & -2i^2-2i+1\\ 2 & 2i+1\end{pmatrix}.$$

Then $\det A=\det B=\det C=-3$, $A+B=C$ and

$$A^2=B^2=C^2=\begin{pmatrix}3 & 0\\ 0 & 3\end{pmatrix}=3E$$

for every $i\in\mathbb{Z}$. If $m=2k+1$ ($k\in\mathbb{N}$), then (for example) $A^m=A^{2k+1}=(A^2)^kA=(3E)^kA=3^kA$. Therefore $A^{2k+1}+B^{2k+1}=3^kA+3^kB=3^kC=C^{2k+1}$ and the proof is complete.

Theorem 4.2. *If $m\equiv\pm1 \pmod 3$, then the equation (F) has solutions in $M_3(\mathbb{Z})$ in irreducible elements.*

Proof. Let

$$A=\begin{pmatrix}0 & 1 & -i\\ 0 & 0 & 1\\ 2 & 2i & 0\end{pmatrix},\quad B=\begin{pmatrix}i-1 & i^2-i & i+1\\ -1 & -i & -1\\ -2 & -2i-1 & 1\end{pmatrix},$$

$$C=\begin{pmatrix}i-1 & i^2-i+1 & 1\\ -1 & -i & 0\\ 0 & -1 & 1\end{pmatrix}.$$

Then $\det A=\det B=\det C=2$, $A+B=C$ and $A^3=B^3=C^3=2E$ for every $i\in\mathbb{Z}$.

If $m=3k+1$, then (as in the proof of Theorem 4.1)

$$A^{3k+1}+B^{3k+1}=2^kA+2^kB=2^kC=C^{3k+1}.$$

Let $m=3k-1$ ($k=1,2,\dots$). Then A^2, B^2, C^2 is a solution of (F). Indeed, using equation $(A^2)^{3k-1}=A^{6k-2}=A^{3(2k-1)+1}=2^{2k-1}A$ it is easy to see that $(A^2)^{3k-1}+(B^2)^{3k-1}=2^{2k-1}A+2^{2k-1}B=2^{2k-1}C=(C^2)^{3k-1}$. The proof is complete.

Theorem 4.3. *If $m = n \geq 2$, then the equation (F) has solutions in $M_n(\mathbb{Z})$ in irreducible elements.*

Proof. Let E_{n-1} denote the $(n-1) \times (n-1)$ identity matrix, $\mathbf{0}$ the $n-1$-dimensional vector-column, $\mathbf{0}^*$ the $(n-1)$-dimensional vector-line and let p be a prime. Then the element $A_p = \begin{pmatrix} \mathbf{0} & E_{n-1} \\ p & \mathbf{0}^* \end{pmatrix}$ is irreducible in $M_n(\mathbb{Z})$, $\det A_p = p$ and it is easy to prove that $(A_p)^n = pE_n$. Therefore, for example, (A_2, A_5, A_7) is a solution of (F) and the proof is complete.

References

[1] E. D. Bolker, Solutions of $A^k + B^k = C^k$ in $n \times n$ integral matrices, *Math. Notes* (1968), 759–760.

[2] Z. Cao and A. Grytczuk, Fermat's type equation in the set of 2×2 integral matrices, *Tsukuba J. Math.* **22** (1998), 637–643.

[3] P. Damphouse, The arithmetic of powers and roots in $GL_2(\mathbb{C})$ and $SL_2(\mathbb{C})$, *Fibonacci Quart.* **27** (1989), 386–401.

[4] R. Z. Domiaty, Solution of $X^4 + Y^4 = Z^4$ in integral matrices, *Amer. Math. Monthly* **73** (1966), 631.

[5] D. Frejman, On Fermat's equation in the set of Fibonacci matrices, *Discuss. Math.* **13** (1993), 61–64.

[6] A. Grytczuk, On Fermat's equation in the set of integral 2×2 matrices, *Period. Math. Hung.* **30** (1995), 79–84.

[7] A. Grytczuk, Note on Fermat's type equation in the set of $n \times n$ matrices, *Discuss. Math.* **17** (1997), 19–23.

[8] A. Grytczuk, On conjecture about the equation $A^{mx} + A^{my} = A^{mz}$, *Acta Acad. Agriensis, Sect. Math.* **25** (1998), 61–70.

[9] A. Khazanov, Fermat's equation in matrices, *Serdica Math. J.* **21** (1995), 19–40.

[10] M. Le and C. Li, On Fermat's equation in integral 2×2 matrices, *Period. Math. Hung.* **31** (1995), 219–222.

[11] M. Le and C. Li, A note on Fermat's equation in integral 2×2 matrices, *Discuss. Math., Algebra and Stochastic Methods* **15** (1995), 135–136.

[12] H. Qin, Fermat's problem and Goldbach problem over $M_n\mathbb{Z}$, *Linear Algebra Appl.* **236** (1996), 131–135.

[13] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, *Springer Verlag*, 1979, 275–277.

[14] L. N. Vaserstein, Non-commutative Number Theory, *Contemp. Math.* **83** (1989), 445–449.

Z. PATAY AND A. SZAKÁCS
DEPARTMENT OF MATHEMATICS
FACULTY OF ECONOMICS
TESSEDIK SÁMUEL COLLEGE
5600, BÉKÉSCSABA, BAJZA U. 33
HUNGARY

(Received October 5, 2001; revised August 1, 2002)